Data Protection

Code of Conduct for Cloud Service Providers

Revised v1.0

22 June 2016

Contents

Introduction

Cloud computing provides significant benefits to both public and private sector customers in terms of cost, flexibility, efficiency, security and scalability. However, cloud customers must be able to trust a cloud service provider (CSP), before they will entrust their data and applications to them. A recurring challenge is to ensure that personal data is processed by the CSP in accordance with the EU Data Protection Directive[1], its national transpositions and subsequent EU data protection laws, in particular the General Data Protection Regulation[2] and any further European data protection legislation.

The purpose of this voluntary Code of Conduct (Code)[3] is to 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 Cloud Computing Strategy[4] states that the European Commission will work with industry to agree a code of conduct for cloud computing providers to support the uniform application of data protection rules. The Code has been prepared by the Cloud Select Industry Group (C-SIG) -Data Protection Code of Conduct Subgroup[5] which was convened by the European Commission (DG Connect and DG JUST). The Code consists principally of a set of requirements for CSPs adhering to the Code, and a governance structure that aims to support the effective

[1] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, see http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:NOT

[2] 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

[3] This Code of Conduct has been prepared to contribute to the proper application of the national data protection provisions adopted by Member States pursuant to Directive 95/46/EC, taking into account the specific features of the cloud computing sector.

[4] See http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF

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

and transparent implementation, management, and evolution of the Code. CSPs should take into account relevant initiatives under the Cloud Computing Strategy[6] where appropriate.

The Code is a voluntary instrument, allowing a CSP to evaluate and demonstrate its adherence to the Code's requirements, either through (i) self-evaluation and self-declaration of compliance, or (ii) through third-party certification[7]. Any CSP may sign up 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 processes provided 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 effectively listed on the website listing all the companies adhering to this Code (www.xxx.eu).

[6] This includes particularly outputs from Cloud Computing Strategy initiatives such as the C-SIG Service Level Agreements Subgroup and the C-SIG on Certification Schemes.

[7] Note that this Code uses the concept of 'certification' generically, to refer to an affirmation provided by an independent third party that confirms compliance with a specific set of defined requirements. The concept should therefore not be understood as complying necessarily with the provisions of Article 42 of the General Data Protection Regulation.

0. Terminology

Any terminology used in this Code of Conduct which is defined in the Data Protection Directive (e.g. personal data, data controller, data processor, data subject, etc.) shall have the meaning and interpretation as defined in accordance with that Directive. Upon the date of application of the General Data Protection Regulation, it shall have the meaning as defined in accordance with that Regulation.

Furthermore, the following concepts[8] 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 services': one or more capabilities offered via cloud computing invoked using a defined interface.
- 'Cloud Service Provider' or 'CSP': party which makes cloud services available.
- 'Cloud customer' or '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 data controller, entrusts to the CSP.
- 'Party': Natural person or legal person, whether or not incorporated, or a group of either.
- 'Services Agreement': a (set of) written agreement(s) between the CSP and the customer, which includes their contractual obligations, including with respect to data protection. The Services Agreement may take the form of general terms and conditions, including those published online, that apply to all customers of the CSP's services.

1. Structure of the Code

[8] 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 'Services Agreement'.

The Code is structured as follows, with each section addressing a particular topic in relation to its use, impact on adhering CSPs, and governance of the Code:

- **Purpose:** describes the ambitions of the Code and its relation to applicable data protection law.
- **Scope:** describes the field of application of the Code, including the use cases for which it is particularly intended and the CSP's services to which it applies.
- **Conditions of adherence:** describes the conditions for CSPs declaring adherence to the Code, including particularly the Code's relationship to the terms of 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 such as purpose delimitations, data transfers, security, auditing, liability, data subject rights, etc.
- **Security requirements:** describes how the adhering CSP must ensure that its services 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 are processed with an appropriate level of data protection and that an adhering CSP has performed the necessary due diligence related to the processing of personal data according to the EU Data Protection Directive, its national transpositions and subsequent EU data protection laws, in particular the General Data Protection Regulation and any further European data protection legislation. Specific governance procedures are foreseen to ensure that the Code is revised and amended to remain fully aligned with the obligations and interpretation of European data protection law over the course of its evolution.

When adhering to this Code, CSPs must commit to the Code's requirements and practices. 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 governance section of the Code may choose to publicly show their adherence by using any of the marks or labels specified in accordance with the governance section.

3. Scope

Any CSP may choose to declare its adherence to the Code, for any types of cloud services in which personal data may be processed, provided that it meets the requirements of EU applicable data protection laws and the terms of this Code.

It is not mandatory for the CSP to choose to declare the adherence of all of its cloud services to the Code. If desired, a CSP can choose to only declare specific services as adhering to the Code. CSPs taking this approach will need to ensure that potential customers are made unambiguously aware of which services the Code applies to.

CSP services may be provided alone or in combination with other CSP services (nested services). Where multiple services are provided in combination, a 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 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 service and another is responsible for support, that should also be made clear to customers, including who to contact for which issues. Where users have directly contracted with multiple cloud services in order to build their own applications and services, then each CSP is only responsible for the contracting and disclosure of the service they provide.

Furthermore, the nature of the service (SaaS, PaaS, IaaS, etc.) provided in public, private or hybrid clouds imply services of different nature which may have different related obligations. Customers should be provided with information necessary to understand the nature of the service. Guidance documents can further help users understand the nature of the service type and the obligations related to it.

For ease of use and comparison the drafters have developed a single Code, which is broad enough in scope to cover all offerings. However, that desire to focus on one Code will mean that not all code provisions may be equally relevant to all services.

While the Code is aimed at CSPs who process personal data on behalf of their customers (and therefore act as data processors for those customers), CSPs that process such personal data for their own purposes (and therefore act as a data controller or as a joint data controller) may also adhere to the Code[9].

[9] In such cases however, the Code primarily applies to the part of the service where the CSP is a processor, and it does not affect the CSP's legal duty as a controller to respect all requirements of applicable data protection law. A CSP acting as a

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 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[10]).

The CSP will ensure that key information in relation to data protection compliance is made available to the customer and kept up to date. As a minimum, such information should include all elements covered by the Declaration of Adherence form in Annex C.

controller in relation to the personal data needs to meet any legal requirements imposed by applicable data protection law on the controller and inform the customer that it processes customer data for its own purposes. In case of co-controllership, both CSP and its customer will need to meet their legal obligations as co-controllers. Declaring adherence to the Code is not sufficient for the CSP to meet its entire obligations when acting as a controller.

[10] According to article 3(2) of the Directive 95/46/EC, "This Directive shall not apply to the processing of personal data … by a natural person in the course of a purely personal or household activity".

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 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.

In addition, through its declaration of adherence the CSP commits to comply with applicable EU data protection law. However, a declaration of adherence to the Code does not absolve any CSP from having to comply with applicable EU 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. Competent authorities may take notice of declarations of adherence to the Code as an element by which to demonstrate compliance with corresponding requirements of data protection law.

CSPs that meet the requirements set out in the Code may declare that they adhere to the Code, following the process outlined in the governance section. CSPs may choose to do this either through a self-assessment of the Code's requirements followed by a self-declaration of adherence, in accordance with Annex C, or after undergoing a third party audit and third party certification. The customers should carefully consider the declaration of adherence to this Code provided by the CSP before entrusting personal data to a cloud provider.

This Code was drafted to be fully consistent with applicable EU data protection law, and 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 using this Code: CSPs should ensure that their legal or contractual obligations do not contradict any part of the Code before declaring their adherence to its terms, and that their legal or contractual obligations 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 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 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 EU data protection law 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 Governance section of the Code.

5. Data Protection

5.1 Contractual specification of the terms and conditions of the CSP's services

The Code does not replace a contract between the CSP and the customer. Therefore, the CSP and its customer shall define how the cloud service is delivered in a Services Agreement, which must comply with applicable data protection law, including in particular in relation to security measures. In case of disputes on contradictions or ambiguities between the Services Agreement and the Code, complaints may be raised and addressed in accordance with section 5.7 (Cooperation with the customer) and with the complaint mechanisms established in the governance section of the Code.

Unless agreed otherwise in the Services Agreement, the CSP shall act only on behalf of the customer, with respect to data processed pursuant to the Services Agreement. The Services Agreement shall specify the purpose(s) for which the CSP may process personal data on behalf of the customer, as well as the conditions under which the data may be processed. The Services Agreement shall also specify the allocation of responsibilities between the parties.

If the Services Agreement expressly authorizes the CSP to determine purposes and conditions which are not specified in the Services Agreement, the CSP would be qualified as a data controller or as a joint data controller, entailing additional obligations for the CSP.

5.2 Processing Personal data lawfully

The data controller[11] remains responsible for complying with all obligations and duties under applicable data protection law. The customer acting as data controller may need to verify whether the CSP services comply with its legal requirements, taking into account the terms of the Services Agreement and the Code.

[11] In most circumstances, the customer will be the data controller. However, there may be cascaded processors, where the customer is itself acting as a processor on behalf of a data controller. For instance, a company may contract with a cloud provider, who outsources services to another cloud provider that complies with the Code. In that case, the company is the data controller, but the initial cloud provider is the customer in the sense of this Code. In such cases, the relevant data controller (the company in this example) is not in direct contact with the CSP.

The CSP shall at all times execute the services according to the provisions of the Services Agreement[12]. The CSP may not process personal data processed pursuant to the Services Agreement for its own purposes without the express permission of the customer or as agreed by the customer in accordance with the Services Agreement. Incidental processing of personal data by the CSP to ensure the security, operational maintenance, analysis or evaluation of the CSP services for the benefit of all of the CSP's customers and not having any adverse impact on the level of data protection of the data subjects must be clearly specified in the Services Agreement, and shall not be presumed to constitute processing for the CSP's own purposes.

The customer will not use the CSP's services for any unlawful or illegitimate purposes, or in violation of the Services Agreement, the Code, or applicable law. It will not impose obligations on the CSP via or in accordance with the Services Agreement to process personal data for purposes which are not fair and lawful.

The customer shall remain responsible for keeping accurate the personal data processed pursuant to the Services Agreement and, where necessary, up to date, in accordance with its obligations under applicable data protection law[13].

The CSP shall implement measures which satisfy any customer requirements as expressed in accordance with the Services Agreement that personal data processed pursuant to the Services Agreement will not be retained longer than necessary according to the CSP's commitments or applicable law, and shall make any relevant elements of its data retention policy available to the customer.

International transfers of personal data must be conducted by the CSP in accordance with the instructions or the knowledge and consent of the customer in his or her capacity as data controller.

5.3 General principles in relation to the transfer of the customer's personal data

CSP operations may occur across multiple locations at the same time. Customers should also be aware that more than one CSP may be involved in providing service at a single location. For example, one CSP may have provided software as a service while another provides the platform or infrastructure it runs on. The relationships between these parties may vary by

[12] The CSP when acting as a processor shall therefore not process personal data except on instructions from the controller, unless required to do so by law, as specified in Article 16 of the Data Protection Directive.

[13] As required by Article 6.1 d) of the Data Protection Directive: personal data must be kept "accurate and, where necessary, kept up to date".

implementation of such nested services and should be made clear in contracts between the entities[14].

Transfers of the customer's personal data are permissible under the conditions set out in the following section. However, the CSP must always ensure that any entities engaged in the processing of the customer's personal data provide at least an equivalent level of protection to that agreed between the CSP and the customer in the Services Agreement, and that they are not permitted to conduct any processing that exceeds the terms of the Services Agreement. The CSP must put in place the necessary legal and operational arrangements to provide this level of protection. The CSP must be able to demonstrate to the customer through appropriate documentary evidence that it has taken measures to provide this level of protection.

The CSP shall maintain an up-to-date list of entities engaged in the processing of the customer's personal data. This list must include the location, including the address, of the infrastructure that they may use for such processing. The location should be described with a level of detail that complies with applicable legal requirements, including the legal entity responsible for the processing in the case of nested services. This list must be accessible to relevant Data Protection Authorities upon their request.

The customer at the time of acceptance of the Services Agreement, and at any time thereafter, will be able to access the aforementioned list. However, it is recognized that it may be necessary for specific addresses of processing locations to be kept confidential by all parties for security reasons. Therefore, the list as made available to customers will not need to disclose specific addresses of processing locations by default, in order to avoid the security risk of such addresses becoming public knowledge. The information on the list must however permit the customer to identify applicable data protection law and the competent data protection authorities. The customer must be informed of the existence and whereabouts of this information. Where the customer requires more detailed information related to processing locations in to comply with legal requirements or requests from data protection authorities, CSPs shall work constructively to assist the customer to address their compliance needs.

Any changes to the aforementioned list must be made available to the customer in a timely fashion, including by announcing them to the customer through automated notices where appropriate. The customer may object to any changes in the list on reasonable grounds based on data protection or security. The CSP and the customer may define in the Services Agreement in which cases an objection from the customer to the use of a new entity or

[14] Where the user contracts with a nested CSP service then the contracting CSP bears the responsibility of disclosure of the nested services. Where the user contracts with multiple CSPs, then each CSP bears the requirements of disclosure related to the service they are providing.

jurisdiction would be unreasonable. The customer may give his consent to changes of entities or jurisdictions, including through general consent given at the beginning of the use of the CSP service through the Services Agreement. If the customer's objection is reasonable, the customer may terminate the Services Agreement in accordance with the terms therein or, if agreed by the customer and the CSP, terminate the relevant service which cannot be provided by the CSP without the use of the objected-to new entity or jurisdiction.

5.4 Transfer of the customer's personal data within the CSP's Group

Unless agreed otherwise between the CSP and the customer, the CSP may entrust all or some of its processing activities as set out in the Services Agreement to other members of the CSP's Group, under the conditions specified above and in this section of the Code. A "Group" includes any legal entity:

- in which the CSP directly or indirectly owns a legal or de facto controlling interest; or
- which directly or indirectly owns a legal or de facto controlling interest in the CSP; or
- which belongs to the same corporate structure as the CSP (i.e. there is a parent company that directly or indirectly owns a legal or de facto controlling interest in both that legal entity and the CSP).

5.4.1 Group transfers within the EU/EEA or subject to an adequacy finding

If the CSP transfers personal data to another entity of the Group located in an EU or EEA Member State or subject[15] to an adequacy finding pursuant to article 25.2 through 25.6 of the Directive 95/46/EC, the CSP may entrust all or some of its processing activities to these other Group entities without prior consent from the customer[16].

Demonstration keys

[15] See http://ec.europa.eu/justice/data-protection/document/international-transfers/index_en.htm for a list of countries that satisfy the requirements.

[16] Note that the "consent" as discussed here does not relate to the consent of the data subject, but to the contractual consent of the customer (who will typically be the data controller) on the terms of the CSP's services to engage Group affiliates. The data controller may ensure the legitimacy of data processing on the basis of the consent of any data subjects, or on any other legal foundations permitted under applicable data protection law, but this issue is separate from the contractual consent of the customer.

A CSP that is part of a Group may inform on group transfers by demonstrating that a Group Data Protection Policy is in place that is compliant with the requirements of applicable data protection law, the applicable data privacy related requirements of the Services Agreement, and the requirements of the Code.

Alternatively, a Data Transfer Agreement between the relevant Group entities may be adopted to define the terms and conditions of the processing by the different Group entities, which must be compliant with applicable data protection law, the applicable data privacy related requirements of the Services Agreement, and the requirements of the Code.

Alternatively, transfers within the Group as envisaged above are also permissible if all receiving entities in the Group confirm to the CSP that they will respect the applicable data privacy related terms of the Services Agreement and applicable data protection law, provided that the receiving entities have been identified in a declaration of adherence to the Code in accordance with Annex C, so that the terms of the Code apply in the same way to these Group entities as to the CSP itself.

5.4.2 Group transfers outside the EU/EEA in countries not covered by a European Commission adequacy decision.

If the CSP transfers personal data to another entity of the Group located outside of an EU or EEA Member State and not otherwise subject to an adequacy finding pursuant to Article 25.2 – 25.6 of the Data Protection Directive, then the transfer can take place under the conditions hereunder. If these conditions are satisfied, the CSP may entrust all or some of its processing activities to these other Group entities without prior consent from the customer.

Demonstration keys

The Group entities are bound by Binding Corporate Rules for Processors depending on the setup which have been adopted and approved in accordance with the processes established under EU data protection law[17].

[17] Notably Working Papers 74, 107, 108, 133, 153, 154 and 155, and Opinion 8/2003 on the draft standard contractual clauses submitted by a group of business associations; see http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/tools/index_en.htm

Alternatively, the transfer may take place if the Group entities are bound by Data Transfer Agreements that comply with the EU Model Clauses, as approved by the European Commission[18].

Alternatively, the transfer may take place on the basis of other legal derogations as permitted under the Data Protection Directive[19], provided that these have a basis under applicable law, or that are permitted under specific decisions by a competent data protection authority or by the European Commission.

5.5 Transfer of the customer's personal data to a third party subcontractor

Unless agreed otherwise between the CSP and the customer, the CSP may entrust all or some of its processing activities as set out in the Services Agreement to one or more third party subcontractors, under the conditions specified above and in this section of the Code.

5.5.1 Transfers to subcontractors within the EU/EEA or which ensures an adequate level of protection officially recognized by the European Commission

The CSP may subcontract its processing activities under the Services Agreement to a third party with the customer's prior consent to do so. Such consent can take the form of a prior general consent for the CSP to use subcontractors that may be given by the customer at the

[18] See http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm

[19] Notably Article 26.1 of the Directive, stating that transfers are permitted if:

(a) the data subject has given his consent unambiguously to the proposed transfer; or

(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request; or

(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or

(d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or

(e) the transfer is necessary in order to protect the vital interests of the data subject; or

(f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.

beginning of the Services Agreement. The CSP shall not be required to obtain new or additional consents from the customer for changes to the list of subcontractors, provided that they meet the requirements in relation to subcontractors as set out in this Code, and provided that the customer is informed of the change in subcontractors, including specifically by updating the aforementioned list.

5.5.2 Transfers to subcontractors outside of the EU/EEA not covered by a European Commission adequacy decision

In those circumstances, the transfer may only take place under the conditions hereunder, in addition to the general requirement of the customer's prior consent in accordance with the provisions of section 5.4.1.

Demonstration keys.

The transfer may take place if the third party is bound by processing agreements that comply with the EU Model Clauses, as approved by the European Commission[20].

Alternatively, the transfer may take place on the basis of other legal derogations as permitted under the Data Protection Directive[21], provided that these have a basis under applicable law, or that they are permitted under specific decisions by a competent data protection authority or by the European Commission.

[20] See http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm

[21] Notably Article 26.1 of the Directive, stating that transfers are permitted if:

(a) the data subject has given his consent unambiguously to the proposed transfer; or

(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request; or

(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or

(d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or

(e) the transfer is necessary in order to protect the vital interests of the data subject; or

(f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.

5.6 Right to audit

The customer must be able to assess whether the CSP complies with the obligations of applicable data protection law and the Code. The Code ensures that compliance can be assessed by the customer, either through an exchange of information between the CSP and the customer on prior audit results, or by permitting audits to be conducted on behalf of the customer. In that way, appropriate evidence with respect to compliance is available to the customer, including where appropriate through audits by an independent third party, or – if no such audits by an independent third party have been undertaken – as directed by the customer itself under the conditions set out below. In this manner, the Code ensures that auditing is possible while mitigating the security and privacy risks inherent in permitting a potentially large number of customers to access a CSP's data processing infrastructure. These audit rights ensured by the Code do not affect the competence of data protection authorities to monitor compliance with data protection law in accordance with their legal mandate.

If the CSP has not received a Certificate from a Competent Monitoring Body in accordance with the governance section of the Code, then the CSP shall permit the customer to request an audit by a mutually agreed auditor or shall conduct an audit on behalf of the customer if this right has been granted to the customer through the Services Agreement, or if the customer demonstrates the need for such an audit in light of his regulatory requirements as controller of personal data.

If the CSP has received a Certificate from a Competent Monitoring Body in accordance with the governance section of the Code, the audit results are presumed to meet the audit requirements of the customer in the field of data protection, unless agreed otherwise in the Services Agreement.

A summary report describing the outcomes of audits conducted for the purposes of obtaining a Certificate in accordance with the Code, shall be made available to the customers upon their request, free of charge.

Audits and related reports should not endanger the security and protection of personal data in the CSP infrastructure. Requests for audits should be on appropriate notice and be carried out in a way not to be disruptive to normal business operations.[22]

The CSP and the customer may specify any arrangements in relation to the cost allocation for audits in the Services Agreement. In the absence of any arrangements in relation to the costs and cost allocation, the costs must be borne by the requesting party.

[22] Investigatory audits may have an urgency related to them that may not always allow as much notice or consideration of business operations as desired.

5.7 Liability

Where the CSP fails to meet its legal obligations under applicable law, the Services Agreement or the Code, including specifically when the CSP has acted outside[23] or contrary to lawful instructions of the controller, the customer shall have the right to avail themselves of the liability regime that applies as set forth in the Services Agreement. The CSP and the customer shall ensure that the Services Agreement unambiguously identifies this liability regime, and that it unambiguously identifies any limitations on liability, exceptions, exclusions or liability caps. The CSP must not limit its obligations and liability or restrict the customer's rights to an extent that unduly disadvantages the customer contrary to applicable law.

The CSP shall ensure that, when the execution or the interpretation of the Services Agreement is subject to European data protection law, the liability regime for any violations by the CSP of its data protection obligations shall be that of at least one EU Member State.

5.8 Cooperation with the customer

CSPs adhering to the Code shall implement the necessary organizational measures within their cloud infrastructure (including any parts of the infrastructure entrusted to Group entities or third parties) which enables them to monitor the effective application of the commitments undertaken by the CSP on the basis of applicable law, the Services Agreement and this Code of Conduct. The CSP shall document these measures and will make these available to the customer at the customer's request, free of charge, for example by providing evidence of an audit of compliance with any or all requirements of this Code.

The CSP shall provide a mechanism that may support the customer for any questions or requests it may have regarding data protection issues in the frame of the service covered by the Services Agreement and this Code. Such mechanisms may take the form of phone numbers, e-mail addresses, chat systems, or any other methods that allow the customer to establish direct communications with a representative of the CSP.

The CSP shall cooperate in good faith with the customer to provide information about the services provided which is reasonably needed by the customer to enable the evaluation of risks to the data protection rights of individuals and in the determination of appropriate

[23] I.e. when the CSP has engaged in processing activities that exceed its contractual mandate as given by the customer through the Services Agreement.

measures to be implemented by the CSP, taking into account the usage of the CSP's services as determined in the Services Agreement.

5.9 Data Subject rights and complaint handling

The CSP and the customer recognize that the first point of contact for data subjects to exercise their rights shall be the data controller, typically the customer, in accordance with applicable data protection law.

If the CSP is a controller or a joint controller, it shall ensure that data subjects are clearly informed of how their rights can be exercised and how their complaints will be addressed, including by which party, in accordance with applicable data protection law.

If the CSP is a data processor, then the CSP will promptly notify, to the extent legally permitted, the customer if the CSP becomes aware of any data subject requests or complaints which have been addressed to the CSP, and will await instructions from the customer.

The CSP shall cooperate in good faith with the customer to help the customer to address any data subject requests made by a data subject to the customer for rectification or erasure, complaints, the right to data portability or any other efforts to exercise data subject rights in a timely and efficient manner.

For the avoidance of doubt, the data subject will retain the right to exercise his or her rights under applicable data protection law, including via the intermediation of courts or data protection authorities, as permitted by law.

5.10 Data Protection Authority request handling

The CSP shall cooperate in good faith with the customer and assist the customer to handle a request from a competent data protection authority.

The CSP shall also cooperate in good faith with all data protection authority requests it receives directly, in particular to ensure adequate and timely responses. The CSP shall notify the customer in the most expedient time possible under the circumstances of any such requests received from a data protection authority that relate to the Services rendered specifically to the customer under the Services Agreement, unless such notifications are not permitted under applicable law.

5.11 Confidentiality obligations

The CSP shall ensure that any of the 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 Group entities or subcontractors involved in the data processing) are aware of their obligation to respect the confidentiality of the personal data as described within the Services Agreement, this Code and applicable law, and required to respect this obligation. Such persons shall specifically not be permitted to collect process or use personal data unless this is necessary for the performance of the services in accordance with the Services Agreement. This obligation of confidentiality shall continue as long as reasonably required, taking into account the confidentiality of the data and the applicable legislation, after their employment ends.

The CSP shall implement and enforce clear access controls to personal data to ensure that personnel can only access and, as the case may be, take actions in relation to the personal data which are required as a consequence of their job functions. When the personnel no longer needs certain rights, these shall be revoked as soon as possible.

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 Law enforcement/governmental requests

The CSP will inform the customer in the most expedient time possible under the circumstances of any legally binding request for which the CSP is compelled to disclose the personal data by a law enforcement or governmental authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation.

Furthermore, before responding to any request from a court, tribunal or administrative authority of a third country to transfer or disclose any customer's personal data, the CSP shall verify whether the request is based on an international agreement in force between the requesting third country and the European Union or a Member State, without prejudice to other grounds for transfer set out under applicable data protection law.

5.13 Data breach

In the event that the CSP becomes aware that there has been a breach of the customer's personal data, it shall, pursuant to the timeframes specified in the Services Agreement and in any event without undue delay, alert and inform the customer about the security breach.

The CSP shall implement a data breach management policy which will specify the procedures for establishing and communicating data breaches, including clear guidance on how incidents are addressed, and a specification of the information to be made available to the customer subsequently of the data breach incident. This policy shall be made available to the customer upon request. The CSP shall not be responsible for verifying that this data breach management policy is compliant with any legal requirements that may apply to the customer.

The CSP and customer will cooperate in good faith to meet any regulatory requirements to communicate the breach to the public and/or to public authorities to the best of their ability.

If the CSP is a controller or a joint controller, it shall in any event adhere to any breach notification obligations incumbent upon it under applicable data protection law. In the case of joint controllership, notification obligations may be allocated to either the customer or the CSP via the Services Agreement.

5.14 Termination of the Services Agreement

When the Services Agreement terminates or upon the customer's request, the CSP shall where specified in the Services Agreement, enable the customer to make a copy of the customer's personal data stored by the CSP's services and/or to otherwise transmit its data out of the CSP's infrastructure. The scope of which personal customer data is stored and available for return, the formats available for return, and the mechanism for return should be described in the Services Agreement or in related documentation made available by the CSP to the customer. The CSP will not be required to ensure that such copying remains possible after the termination of the Services Agreement, unless otherwise agreed in the Services Agreement.

After the termination of the Services Agreement, the CSP shall delete or otherwise render unrecoverable any remaining copies of the customer's personal data within the timescale specified in the Services Agreement or (if no timescale was specified in the Services Agreement) no later than one year after the termination of the Services Agreement, unless prevented from doing so by applicable law or contract (such as retention obligations related to record keeping for taxes, warranties, etc.). This duty shall also apply to any personal data derived from the personal data processed pursuant to the Services Agreement.

6. Security requirements

The security objectives and requirements set out below are intended to reflect the commitments made by CSPs in their role to support the Code.

6.1 Objective of security requirements for cloud service providers

> *The CSP shall implement technical and organizational information security measures sufficient to ensure the security, integrity, confidentiality and availability of the personal data being processed.*

The nature of the technical and organizational information security measures implemented by the CSP should take into account information they have received from the controller concerning the sensitivity of the personal data being processed and the impact of any security breach, both on the data subjects and on the cloud service customer, insofar as this is known to the CSP. 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 a corresponding range of security measures which the CSC can opt to employ when using the cloud service. The range of security measures should be made available publicly when offering the cloud service.

6.2 Implementation guidance to meet the security objective

6.2.1 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 outlined in Annex B.

6.2.2 Method to achieve the security objectives

Different security measures can be put in place to achieve the security objectives of this section. Security measures can also change over time, as security best practices and security threats evolve. Purposely, compliance with standards and good security practices in general requires monitoring, reviewing, maintenance and improvement of the security measures.

International standards provide an adequate manner to assess the information security risks of the cloud service being provided and to establish adequate security measures to address these risks and achieve the security objectives of Annex B.

One way to establish the security measures adequate to achieve these objectives, is for the CSP to plan to address its information security risk as prescribed in appropriate standards that support information security risk management processes[24]. The purpose is to ensure that the information security risks of the cloud service offered by the CSP are appropriately addressed.

The CSP shall also take into consideration the regulatory requirements for the protection of personal data, and in particular the EU Data Protection Directive 95/46 and subsequent EU data protection laws, which may be applicable within the context of the information security risk environment(s) of a provider of public cloud services. To that end, the guidelines and security controls provided in appropriate standards should be used as a reference for selecting adequate controls. The customer and/or the CSP (as appropriate) should also consider methods of de-identification including anonymizing[25] or pseudonymizing[26] the personal data where practicable on the basis of the objectives and operational requirements of the processing, in accordance with applicable data protection law, relevant guidance from data protection authorities and generally accepted business practices.

Finally, the Services Agreement must indicate which technical and organizational measures are incumbent on the CSP in order to protect the personal data, or allow the customer in his or her capacity as data controller to provide instructions on this point to the CSP.

6.3 Transparency

The CSP should describe the level of security provided by the CSP to protect customers' data in the cloud by providing appropriate information about the technical, physical and organizational measures it has in place.

The CSP should also provide the cloud customer with up-to-date information, with an appropriate level of detail, about the security measures that are in place. The CSP should inform the customer in a timely manner of any changes to those measures that would materially weaken or reduce the level of security.

---

[24] The most widely referenced standards today are those within the ISO 27001 series, including ISO27018. Other equivalent standards exist or may be released in the future; see notably http://www.etsi.org/images/files/Events/2013/2013_CSC_Delivery_WS/CSC-Final_report-013-CSC_Final_report_v1_0_PDF_format-.PDF

[25] In accordance with the techniques set out in the Article 29 Working Party Opinion 05/2014 on Anonymization Techniques; see http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

[26] It should be noted that pseudonymization is only a risk mitigation measure and does not remove any requirement to meet the obligations in respect of data processing under applicable EU data protection law.

564

565 **Demonstration keys**

566 The CSP can meet this requirement by providing copies of:

567 • A document comprising the list of controls and security measures meant to
568 address the risk identified in a risk assessment, or

569 • Audit reports and/or certificates of compliance to ISO or other generally
570 recognized international standards, especially in relation to information security.

571 However, the Cloud Service Provider should not be required to disclose any business
572 confidential or commercially sensitive information to the cloud customer. Furthermore,
573 CSP disclosures must not be of a nature that could be used to compromise system
574 security or integrity.

575 Such information can be provided in:

576 • The template provided in Annex A, or

577 • An appropriate International Standard, or

578 • An accepted industry guideline

579

7. Governance

This Code of Conduct has been drafted based on inputs from a wide range of stakeholders, containing representatives with expertise in data protection, self- and co-regulation, ICT in general and cloud computing specifically, including SME providers. This multistakeholder approach is a key element of the Code's genesis, which should also be reflected in its future governance. This section of the Code strives to enable a sustainable model of governance at multiple levels:

- Firstly, the governance of the organizational framework of the Code itself and its bodies, through a General Assembly as a consultative body, a Steering Board with operational decision making power, a Secretariat for administrative support, and 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 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 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 changes in EU data protection law and in particular the enactment and implementation of the General Data Protection Regulation, 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. Organizations interested in being part of the governance will be invited to express their interest to the European Commission and the C-SIG.

The European Commission will be invited to remain a facilitator of the Code once approved by the Article 29 Working Party.

7.1 Governance of the organizational framework of the Code and its bodies - Governance Bodies and Administration

The Code of Conduct Governance Bodies are independent organizations set up by industry for the implementation and administration of the Code.

Code of Conduct General Assembly

The Code of Conduct General Assembly is composed of:

- the CSPs which, during the initial twelve months after the adoption of this Code, are members of the C-SIG; and thereafter any CSPs which have a valid Declaration of Adherence in the Public Register of the Code;

- any representatives of user groups, cloud providers, or other representative bodies which have applied for membership to the Code of Conduct General Assembly, and which have been admitted to the Code of Conduct General Assembly on the basis of a simple majority vote of the Code of Conduct Steering Board.

The GA may requests experts to provide information to the GA or attend meetings as invited guests to their deliberations.

The Code of Conduct General Assembly has to approve, by a majority of two third of votes, any changes to the Code.

All Code of Conduct General Assembly members will be required to pay a nominal annual membership fee, determined by the Code of Conduct Steering Board.

Code of Conduct Steering Board

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

- monitor changes in the EU data protection laws and propose changes to the Code for approval by the Code of Conduct General Assembly. The Steering Board shall aim to propose relevant changes to the Code within three months of material changes in the EU data protection laws, taking into account the extent and complexity of the changes. In particular, the Steering Board shall propose amendments to the Code to reflect the General Data Protection Regulation before its date of application;

- define and propose the content of the Code Declaration of Adherence and respective guidelines for self-assessment;

- define and propose guidelines for Code Certification by audits, 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 endeavor 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 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 applicable data protection law;

- adopt Compliance Marks that may be used by adhering CSPs;
- approve Code of Conduct Competent Monitoring Bodies and withdraw or suspend an approval in case of factual indications that a body no longer meets the requirements defined in this Code;
- approve external third party auditors;
- approve, when required, Code of Conduct General Assembly members;
- propose the membership fees for Code of Conduct General Assembly members;
- define a range of appropriate actions in case of an infringements of the Code or in case a CSP is not providing the information necessary to review a possible infringement of the Code to a Competent Monitoring Body; including sanctions like 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 European Commission, and, where necessary, by developing proposals for the improvement of the governance, subject to approval by the General Assembly by a majority of two third of votes.

Any proposals for a decision of the Steering Board as enumerated above must be adopted through approval by a majority of two third of votes of the Code of Conduct General Assembly.

The Code of Conduct Steering Board will work on particular issues and new developments impacting the Code, and, where necessary, develop and improve the governance, either on its own initiative, on the initiative of the 2/3 members of the Code of Conduct General Assembly, or on the request from the European Commission.

The C-SIG and the European Commission will launch a call for application to create the Code of Conduct Steering Board, with a view of having a balanced representation of stakeholders interested in participating to the Code from both the private and public sectors. In particular, it should be ensured where possible that the Code of Conduct Steering Board includes neutral representatives of:

- Cloud computing providers and cloud computing customers and their representative organisations (including representatives of the public and private sector);
- Academics or experts in data protection and cloud computing;

In addition, the European Commission should participate as an observer to the Code of Conduct Steering Board.

Should the need arise in view of the future evolutions of the Code, the Code of Conduct Steering Board may decide to appoint a drafting team of qualified experts to prepare amendments to the Code. The drafting team should include observers from the European Commission.

The Code of Conduct Steering Board should be established within three months from the approval of the Code by the Article 29 Working Party. Before the Code of Conduct Steering Board is established, governance will be ensured by the C-SIG and the European Commission, as facilitators.

Individuals who represent their organisations in the Code of Conduct 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 Code of Conduct Steering Board shall elect, by simple majority vote, a Chairman and a Vice-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 Code of Conduct Steering Board shall meet twice a year.

The Code of Conduct 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 of Conduct Steering Board. The Code of Conduct 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 organizations or competent bodies.

Code of Conduct Competent Monitoring Bodies

Code of Conduct Competent Monitoring Bodies perform the following functions:

- review and approve Declarations of Adherence by cloud providers or review audits performed by external auditors with a view of issuing Certificates to CSPs;
- serve as a first point of contact for CSPs and customers in relation to any disputes which cannot be resolved amicably between the CSPs and customers, including for the purposes of reconciliation in case of disputes;
- review and decide about possible infringements of the Code in case there are factual indications of a possible infringement, including as a result of complaints from customers or data subjects that have not been appropriately addressed by the CSP. To

this end, Competent Monitoring Bodies must implement an alternative dispute resolution and complaints handling process whereby any customer can lodge complaints against CSPs adhering to the Code with an independent panel of experts (a Complaints Panel) that will make decisions to settle such disputes;

- take appropriate action, selecting from among the sanctions permitted under the Code, against a CSP in case of an infringement of the Code or in case a CSP is not providing the information necessary to review a possible infringement of the Code to a Competent Monitoring Body;

- inform the competent supervisory authority of final actions taken against CSPs and the reasons for taking them;

- ask a CSP to provide the information necessary to review a possible infringement of the Code, and take appropriate action, selecting from among the sanctions permitted under the Code, in case a CSP is not providing this information within an appropriate time;

- ask the CSP to provide the information necessary to periodically review if the operations of the CSP are still in accordance with the Code of Conduct.

A Code of Conduct Competent Monitoring Body shall be approved by the Code of Conduct Steering Board, after the Code of Conduct Steering Board has determined that the Code of Conduct Competent Monitoring Body:

- has demonstrated its independence and expertise in relation to the subject-matter of the Code, notably in terms of data protection, ICT, certification and self-regulatory initiatives, to the satisfaction of the Code of Conduct Steering Board;

- has established procedures which allow it to assess the eligibility of CSPs to apply the Code, to monitor their compliance with the Code's provisions and to periodically review the CSPs operation if needed;

- has established 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 a CSP, and to make these procedures and structures transparent to customers as required by the Code;

- demonstrates to the satisfaction of the Code of Conduct Steering Board that its tasks and duties do not result in a conflict of interests.

Once the European General Data Protection Regulation has entered into force, only bodies, which are accredited as a monitoring body pursuant to Article 41 of this Regulation, can apply for an approval as a Code of Conduct Competent Monitoring Body. Bodies, which were already approved as a Code of Conduct Competent Monitoring Body by the Code of Conduct Steering

Board before this Regulation has entered into force, will be obliged to apply for an accreditation pursuant to Article 41 of the European General Data Protection Regulation 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.

The Competent Monitoring Body is allowed to use the information obtained during a review process only for purposes related to its responsibilities pursuant to the Code of Conduct. The Competent Monitoring Body and any persons working on its behalf in the context of its activities under the Code shall be bound by an obligation of confidentiality ensuring that all information received in the context of these activities has to be kept undisclosed and adequately protected from unauthorized access during the whole process and has to be deleted unhesitatingly when no longer necessary for the purpose it was obtained for.

CSPs are required to update their Declarations of Adherence when necessary, and to cooperate in good faith with any requests for assistance made by the Code of Conduct Competent Monitoring Bodies in respect to the evaluations of their Declarations of Adherence.

Code of Conduct Competent Monitoring Bodies shall likewise 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 of Conduct Competent Monitoring Body. The Code of Conduct Competent Monitoring Body will also create a mechanism to hear complaints of potential conflicts as well as appropriate appellate procedures related to decisions that impact organizations.

Code of Conduct Secretariat

The Code of Conduct Secretariat performs the following functions:

- maintain a public register of Code of Conduct Competent Monitoring Bodies;
- maintain a public register of Declarations of Adherence by cloud providers;
- maintain a public register of Certificates;
- maintain a public register of Code guidelines;
- maintain a public register of external auditors;
- prepare meetings of the Code of Conduct Steering Board;
- promote the Code in Member States;

- maintain the Code website;

The C-SIG and the European Commission will launch a call for application and select a suitable organization to perform the Code of Conduct Secretariat tasks on the basis of nondiscriminatory and objective criteria.

The Code of Conduct Secretariat function is performed by C-SIG and the European Commission until a permanent Secretariat is appointed by the C-SIG and the European Commission.

7.2 Governance of the CSPs that have chosen to adhere to the Code

7.2.1 Procedure for Declarations of Adherence by cloud providers

CSPs submit their Declaration of Adherence in accordance with Annex C to a Code of Conduct Competent Monitoring Body[27], listed in the public register.

The Code of Conduct Competent Monitoring Body should endeavour to review the Declaration of Adherence according to the respective guidelines within 30 working days. Once approved, the Code of Conduct Secretariat incorporates the Declaration of Adherence into the public register. The CSP is then entitled to use the Declaration of Adherence and the Compliance Mark, as noted below. The fee for filing a Declaration of Adherence for CSPs should be cost-based and is approved by the Code of Conduct Steering Board.

A CSP whose Declaration of Adherence has been rejected by a Code of Conduct Competent Monitoring Body may submit a revised Declaration of Adherence or refer the application to the Code of Conduct Steering Board for review. The Code of Conduct Competent Monitoring Body shall issue a report on the issues and its assessment of them along with the referral.

7.2.2 Procedure for Certificates by external auditors

As an alternative to self-assessment and self-declaration of adherence, CSPs can choose any Code of Conduct Competent Monitoring Body that is listed in the public register to apply for a Certificate. Certification will be done at the level of the service.

The award of a Certificate is conditional upon the successful completion of a compliance audit or certification process, conducted by an external auditor that has been approved by the Steering Board, against an existing standard or certification schemes that has similarly been approved by the Steering Board. Since a standard or certification scheme may cover the

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

compliance requirements of all or only a part of the Code, the Certificate shall indicate the scope of the audit(s) that have been conducted, and this may also be reflected in the Compliance Mark which the CSP is permitted to use.

The review mechanisms to be applied by the Competent Monitoring Bodies and external auditors shall be approved by the Code of Conduct Steering Board, after the Code of Conduct Steering Board has determined that they have the required expertise in data protection, ICT security, certification and self- and co-regulatory initiatives.

Upon receipt of a Certificate from a Competent Monitoring Body, the CSP must provide a Declaration of Adherence in accordance with Annex C for publication in the public register.

The Certificate and the summary findings of the audit report shall be published in the public register by the Code of Conduct Secretariat. The CSP is then entitled to use the Certificate, the Declaration of Adherence and the corresponding Compliance Mark, to show its high level of data protection.

A CSP that objects to a decision made by a Code of Conduct Competent Monitoring Body or to the procedures it has applied in the context of its tasks under the Code may refer its objection to the Code of Conduct Steering Board for review. The Code of Conduct Steering Board will decide on the Competent Monitoring Body's compliance with the requirements established in relation to the Code and, where applicable, on the procedures to be applied in the future by the Competent Monitoring Body. The Steering Board however cannot decide itself to issue a Certificate to a CSP.

CSPs are obliged to inform on a timely basis the Code of Conduct Competent Monitoring Body and Code of Conduct Secretariat of any changes in their covered services, that may affect the content of the audit report and the Certificate, as appropriate.

7.2.3 Compliance Marks

Any CSP that has been duly registered in the Code's public register is entitled to use the applicable Compliance Mark adopted by the Code of Conduct Steering Board. Separate Compliance Marks will be foreseen in order to provide transparency to the customers on the adherence choices of the CSP, and notably whether the CSP has elected to conduct a self-assessment followed by self-declaration in accordance with section 7.2.1, or whether the CSP has elected to undergo certification by third party auditors in accordance with section 7.2.2 (and in the latter case, which type of Certificate has been obtained).

Should a dispute concerning non-compliance arise, an organization is entitled to continue using the Compliance Mark until that organization has received a final decision from their Competent Monitoring Body or from a competent court or data protection authority.

Any organization with a final finding of non-compliance with the Code must cease to use the Compliance Mark.

7.2.4. Monitoring and enforcement

The compliance of any CSP that has declared its adherence to the Code will be monitored by a Competent Monitoring Body as noted above. If a customer or authority has doubts on such a CSP's compliance with the terms of this Code, it is invited to contact the CSP first in order to obtain a mutually satisfactory solution.

If no such solution can be found, the customer or authority can file a complaint that relates to an alleged non-compliant behaviour with the Code of Conduct Competent Monitoring Body that reviewed and approved the respective Declaration of Adherence or issued the respective Certificate.

The Code of Conduct Competent Monitoring Body shall review the complaint, require the CSP to provide any relevant information for the purposes of fact finding, and either attempt to reconcile the parties involved or to initiate a complaint handling process, in which an independent panel of experts (a Complaints Panel) will make decisions to settle such disputes. The Complaints Panel will process complaints, establish whether violations of the Code have occurred and decide on possible sanctions and remedies as defined by the Steering Board. Panel members will be appointed by the Competent Monitoring Body. The Complaints Panel shall render a decision within four weeks, or longer if the investigation requires, but in those cases shall notify all parties of the delay and provide a time frame for decision.

During this review, the Code of Conduct Competent Monitoring Body can request the cloud provider to take specific measures to become compliant with the Code. In extreme cases of non-compliance the Code of Conduct Competent Monitoring Body may revoke a Certificate or a Declaration of Adherence.

Irrespective of any enforcement actions taken as described above, customers retain any rights to address their complaints to competent data protection authorities and/or courts as permitted under applicable law.

In the event that a Certificate or Declaration of Adherence is revoked, the Code of Conduct Secretariat shall delete that particular cloud service from the public register. The CSP shall cease to make reference to the Code or the Compliance Mark in any of its documentation or publications, including its website.

7.3 Governance of the 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[28].

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

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

A revised version of the Code needs to be approved first by a two thirds qualified majority vote of the Code of Conduct General Assembly.

The Code of Conduct Steering Board then submits the revised Code to the Art. 29 Working Party for endorsement. Comments from the Working Party should be incorporated as appropriate, approved by the Code of Conduct General Assembly and published.

After publication, CSPs should renew their Declarations of Adherence and Certificates within two years.

7.4 Finances

The costs for the Code of Conduct Secretariat should be covered by fees paid by adhering CSPs and by the nominal annual membership fee from all Code of Conduct General Assembly members.

A CSP that has signed a Declaration of Adherence or that has obtained a Certificate will pay a fee to cover the running cost of the Code of Conduct Secretariat.

The costs for the Code of Conduct Competent Monitoring Bodies should be covered by the fees that CSPs pay to obtain a Certificate or the approval of a Declaration of Adherence.

Any fees to be applied in relation to the governance of this Code must be transparently communicated and agreed in advance with the customer.

[28] This may include finalized or updated outputs from the C-SIG Service Level Agreements Subgroup , the C-SIG on Certification Schemes , the Safe and Fair Cloud Contract initiative , and ENISA's meta-framework of security measures for cloud providers, or any follow-up initiatives to this work.

ANNEX A

Transparency Form

The CSP shall maintain the information listed in this Annex and provide this information to customers, both current and prospective, in accordance with the requirements of the Code.

A. Ways in which the customer's data will be processed

The CSP shall confirm one of the following:

- That it will not process the customer's data for any purpose independent of the customer's instructions
- That it may process the customer's data for any purpose independent of the customer's instructions

B. Physical location (e.g. country) of infrastructure

All infrastructure used by CSP services covered by this Declaration (including any parts of the infrastructure that have been subcontracted to any third parties, or which are operated by CSP Group entities identified in the CSP's Declaration of adherence) is located in (tick and complete as appropriate; multiple checkboxes are possible):

- The CSP's country of establishment
- Any country of establishment of the CSP Group entities identified in the CSP's Declaration of adherence
- Any EU Member State or EEA country, or a country which is subject to an adequacy finding pursuant to article 25.2 through 25.6 of the Directive 95/46/EC
- Any other country

C. Policies regarding customer personal data

The CSP has established the following policies in relation to the CSP services covered by this Declaration:

- Mechanism for data breach notification: [CSP to explain]
- CSP's policy in respect of return, transfer and destruction of personal data: [CSP to explain]

D. Data portability services

The customer shall be able to use the following data portability services in relation to the CSP services:

- Scope of personal data which is available: [to be described]
- Data formats available: [to be described]
- Communication / transmission mechanisms available: [to be described]

ANNEX B

Security Objectives

B.1 Introduction

The objectives below are intended to define a minimum set of information security objectives to be achieved by a cloud service.

The Cloud Service Provider (CSP) shall in any case make a detailed analysis to further define and implement the sufficient security measures and thus address the identified information security risks.

B.2 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 CSP's cloud services.

The CSP shall have in place a management-approved set of information security policies that govern the security of cloud customers' personal data in the CSP's cloud services.

B.3 Organisation of information security

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

B.4 Human resources security

The CSP shall take all reasonable steps to ensure that all employees, contractors and other individuals within the CSP's 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.

B.5 Asset management

The CSP shall take all reasonable steps to ensure the security and confidentiality of the CSP's assets and facilities associated with the processing of customers' data, with policies for the deletion of personal data.

B.6 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.

B.7 Cryptography

Where technically feasible and operationally practicable, the CSP shall develop and implement cryptographic controls at minimum for any transit of data to protect the confidentiality of customers' personal data in the cloud, where provided for in the Services Agreement or where considered necessary on the basis of a risk analysis.

B.9 Physical and environmental security

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

B.10 Operational security

The CSP shall take all reasonable steps to ensure the secure operation of facilities and services that are involved in processing cloud customer' personal data; among the procedures to be highlighted: redundancy or back-up of customer personal data and controls on changes to data processing facilities and systems that affect customers' personal data security.

B.11 Communications security

The CSP shall take all reasonable steps to ensure the protection of cloud customers' personal data in networks and in the CSP's information processing facilities and to ensure the secure transfer of such data.

B.12 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.

B.13 Suppliers

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

B.14 Information security incident management

The CSP shall develop, implement and manage policies and procedures enabling an effective response to and necessary communication about security events and incidents.

B.15 Information security in business continuity

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.

ANNEX C

Template Declaration of adherence

Through this Declaration, the CSP identified below formally declares that all information contained herein is truthful, accurate, complete and up to date, and that all 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, seat of establishment, VAT number]

B. Identification of the Competent Monitoring Body that verified this Declaration

[Name of Competent Monitoring Body, legal form, seat of establishment]

C. CSP Group entities covered by this Declaration (other than the entity specified under A)

- Entity 1: Name, legal form, seat of establishment, VAT number
- Entity 2: Name, legal form, seat of establishment, VAT number
- Etc.

D. CSP services covered by this Declaration

- Service 1: Commercial name, summary free form description
- Service 2: Commercial name, summary free form description
- Etc.

E. Controllership with respect to the CSP services covered by this Declaration

For all of the CSP services covered by this Declaration (tick only one option):

- The CSP declares itself to be the data 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 data controller for any of the purposes of processing.

F. Third party certifications (if any)

All CSP services covered by this Declaration have undergone the following certifications in the last 12 months prior to submitting this declaration, 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 D

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 Services Agreement (including any terms and conditions or privacy policies) in relation to any services for which a declaration 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 to allow them to make an informed decision on the suitability of the CSP services for the purposes envisaged by the customer;
- Decide on whether it wishes to notify only itself, or also any CSP Group members;
- If data transfers are contemplated to Group members or to subcontractors, the CSP should ensure that the demonstration keys specified by the Code are available;
- Assess whether and how the CSP 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 C) to a Competent Monitoring Body;
    - Undergoing a third party certification and providing a Declaration of adherence

  And ensuring that any certifications are appropriately reflected in the Code's public register.
- Ensure that the services for which adherence has been declared are unambiguously identified as such.