Data Protection Code of Conduct
for Cloud Infrastructure Service Providers

9 February 2021

Table of Contents

Introduction

Cloud computing services provide benefits to public and private sector users including cost savings, flexibility, efficiency, security, and scalability. For customers who want to use cloud computing services to process personal data, a key consideration is that the processing is carried out in accordance with applicable EU data protection law.

There is a wide spectrum of cloud services providers who provide a variety of different cloud computing models, and because of this, data protection considerations cannot apply to all cloud models in the same way. The extent to which cloud computing services providers process personal data and the extent of their control over the handling of that data depends on the type of cloud computing services being offered. As such, providers of different types of cloud computing services necessarily have different roles and responsibilities, particularly in relation to data protection and data security.

For example:

- A provider of Software-as-a-Service **(SaaS)** typically offers a software application service that is specifically intended to process personal data (e.g. an e-mail service, ERP software, marketing services, etc.). A SaaS provider has the ability to exercise a wide range of controls in relation to the personal data processed using its SaaS and how that data is processed. It is, therefore, able to provide its customers with technical and contractual commitments that are tailored to the specific SaaS it provides and reflect the degree of control SaaS providers have over data protection compliance.

- A provider of Infrastructure-as-a-Service **(IaaS),** on the other hand, only provides virtualised hardware or computing infrastructure. Its customers have the flexibility to choose how to use that infrastructure. For example, a customer using IaaS has the freedom to choose what applications it wants to deploy on the infrastructure, what data it wants to process on the infrastructure, in which countries to process that data and for what purposes, and how it wishes to protect this data. As set out in Section 4.2 the Service Contract should be drafted in a way that reflects the features of cloud infrastructure services used by customers. However, as the customer is solely responsible for choosing what data it processes on the infrastructure, IaaS providers will be unaware of whether their infrastructure is being used at any specific point in time by customers to process personal data. Because the nature of IaaS is providing automated services at scale, IaaS providers propose standard services for all their customers. These services offer standardised options to customers, allowing the customer to select the service which is best suited to its activities.

This Code of Conduct **(Code)** focusses on IaaS providers. IaaS providers are referred to in this Code as Cloud Infrastructure Services Providers **(CISPs).** The purpose of the Code is to help CISPs to ensure compliance with GDPR and guide customers in assessing whether cloud infrastructure services are suitable for the processing of personal data that the customer wishes to perform. The very different nature of cloud infrastructure services – compared to other types of cloud computing services – means that a specific Code tailored for IaaS is required.

This separate Code will improve the understanding of IaaS in the European Union by creating transparency. In so doing it will contribute to an environment of trust and will encourage a high bar for the default level of data protection. This will benefit Small and

Medium enterprises (SMEs), as both customers and cloud providers, and public administrations in particular.

The Code contains of a set of requirements for CISPs as data processors in Section 4 (Data Protection Requirements) and Section 5 (Transparency Requirements) (together the **Code Requirements).** These requirements elaborate on and clarify how CISPs will meet their obligations under the GDPR, clarify transparency requirements between the CISP and customer and describe the minimum standards customers can expect from Code-compliant CISPs. The Code helps to demonstrate to customers that a CISP has implemented appropriate technical and organisational measures to provide "sufficient guarantees" that processing by the CISP will meet the requirements of the GDPR and ensure the protection of data subject rights, as per Art 28(1) GDPR. While in an IaaS environment, data protection compliance is a shared responsibility between customers and CISPs, the Code does not impose any obligation on customers.

The Code also includes in Annex A technical and organisational security practices and responsibilities allowing CISPs, whatever their size, to not only raise their security bar by adopting security best practices but also to share a common security baseline for their IaaS offerings. This baseline will assist the customer with assessing compliance with its obligations under Art 25 GDPR. While Annex A refers to some practices from ISO/IEC 27001, 27017 and 27018, the objective of the Code is not to replicate such security standards given that the implementation and certification of these standards may generally not be affordable for small and medium-sized CISPs. The aim of the Code is to set out pragmatic and ready-to-use guidance that all CISPs can use to ensure compliance of their IaaS offerings. The Compliance Checklist included within Annex B will facilitate CISPs' efforts to achieve compliance with the Code Requirements and adopt the relevant security measures of Annex A. The Code also includes a governance structure in Section 7 (Governance) that aims to support the implementation, management, and evolution of the Code.

The Code is a voluntary instrument, allowing a CISP to evaluate and demonstrate its adherence to the Code Requirements for one or several of its services. Adherence may be either via (i) the self-Assessment process, or (ii) Controlled Adherence, as set out in Section 6.

CISPs that have demonstrated their adherence to the Code may use the Code's compliance mark.

Customers are invited to verify that the Code Requirements, additional contractual assurances provided by the CISP, and the customer's own policies comply with their obligations under applicable EU data protection law. Customers can verify a CISP's adherence to the Code through the website listing all the organisations that have declared their adherence to this Code (https://cispe.cloud) **(CISPE Public Register).**

The **Designated Supervisory Authority** for the Code is the Commission Nationale Informatique et Libertés (CNIL), which has indicated its acceptance of this designation. CISPE has identified the CNIL as the Designated Supervisory Authority for the purposes of seeking approval of the CISPE Code. CISPE members are established and active in a number of EU member states, with nine CISPE members headquartered in France and many more with active customers and investments in France. Officers of CISPE, including the Treasurer and the Chairman have companies with headquarters in France and are based in Paris. Importantly, the CNIL has been closely involved in the development of the CISPE Code, providing analysis and guidance on the CISPE Code throughout the drafting process, and has developed a valuable understanding of the infrastructure cloud industry

and its technical features. It makes it best placed to become the competent Supervisory Authority for the CISPE Code.

The Development of the Code

The CISPE Code has been prepared through a collaborative process between the CISPE members, all of whom are CISPs providing cloud infrastructure services to European customers. CISPE is intended to represent CISPs and includes representatives from market leading CISPs offering services throughout Europe, across many EU member states. CISPE members range from SMEs to large multinational organisations, with each having a vote in the General Assembly. A list of CISPE members can be accessed on the CISPE website: https://cispe.cloud/

Throughout the process of developing the CISPE Code, CISPE established the CISPE Code of Conduct Task Force ("**CCTF**") in order to embed a variety of stakeholders in the development of the CISPE Code. The CCTF is composed of representatives of CISPs, academic researchers, customer representatives, Data Protection Officers and trade associations. In addition, CISPE members have consulted with a variety of stakeholders, including customers, experts in cloud computing, DG Justice of the European Commission, representatives from EU Supervisory Authorities, the Article 29 Working Party, and organisations who may potentially act as monitoring bodies under the Code. A summary of these stakeholder consultations is included at Annex E.

1 Structure of the Code

This Code is structured as follows:

- **Purpose:** this section describes the focus of the Code relative to 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 ("**General Data Protection Regulation**" or "**GDPR**").
- **Scope:** this section describes the field of application of the Code.
- **Data protection requirements:** this section describes the substantive rights and obligations of adhering CISPs on the basis of key principles of GDPR such as purpose limitations, data subject rights, transfers, security, auditing, liability, etc.
- **Transparency requirements:** this section describes how the adhering CISP demonstrates an adequate level of security for personal data.
- **Adherence:** this section describes the conditions for CISPs declaring adherence to the Code.
- **Governance:** this section 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 guide customers in assessing whether the cloud infrastructure service that it wishes to use is suitable for the data processing activities that the customer wishes to perform. Ultimately, the focus of this Code is to help customers to choose the right cloud infrastructure service for their specific needs.

A CISP's declaration of adherence to this Code for a specific service:

- should instil trust and confidence among customers that in respect of that service, the CISP complies with its obligations as a processor under GDPR; and
- means that the CISP has agreed to be bound by the Code Requirements in respect of that service.

When using any cloud infrastructure service, customers are encouraged to complete their own assessment of their specific processing activities and their compliance based on applicable laws, and especially data protection laws such as the GDPR. This Code is intended to assist customers in such assessments, but is not a substitute for them.

The Code does not replace a contract between the CISP and the customer. The CISP and its customer are free to define how the service is delivered in the Service Contract (as defined in Section 4.2) and to determine their shared responsibilities. CISPs must assess whether the then current Service Contract that they offer new customers in connection with the services contradicts the Code Requirements before declaring their adherence.

At present, the Code itself does not act as a mechanism to validate the transfer of personal data to outside the European Economic Area (EEA). Where European personal data[1] is transferred outside the EEA, a recognised mechanism for transfers under Chapter V of the GDPR must be used.

The Code is not legal advice. Adherence to the Code will not guarantee a CISP's or a customer's compliance with applicable law, including the GDPR. CISPs and customers are encouraged to obtain appropriate advice on the requirements of applicable law.

The nature of the processing by cloud infrastructure services is highly specific, so both CISPs and their customers benefit from more detailed consideration of the relevant provisions of the GDPR as applied in that context.

The Code focuses on the specific features of processing by IaaS providers. It seeks to bring clarity as to what GDPR means in practice when applied to IaaS providers, and what are the actual measures which CISPs will take to ensure compliance with GDPR. This helps CISPs to understand clearly what their obligations are under the GDPR, and will facilitate best practice compliance by IaaS providers. Further, the operation of a Monitoring Body, which will carry out annual reviews of CISP compliance, will facilitate and monitor CISP compliance to ensure adherence to Code Requirements and transparency for customers. The Code Requirements set out throughout the Code assist Monitoring Bodies in their evaluation and monitoring of CISP compliance. In some cases it seeks to go beyond what GDPR requires, for example, the obligation on CISPs to offer their customers the option to ensure that all data is processed within the EEA.

[1] This means personal data which is processed by an entity that is established in the EU or is not established in the EU, but is offering goods or services to EU residents or monitoring the behaviour of EU residents.

This means the Code can more specifically apply the GDPR to processing by CISPs and detail a set of requirements applicable in the IaaS context. Ultimately, the Code will enhance transparency with respect to the responsibilities of CISPs and their customers and facilitate the proper application of data protection requirements to these types of services.

3 Scope

The Code consists of a set of requirements for CISPs as data processors with a particular focus on security measures. These are set out in Section 4 (Data Protection Requirements) and Section 5 (Transparency Requirements). These requirements are referred to collectively in the Code as the Code Requirements.

Any CISP may declare its adherence to the Code Requirements for any cloud infrastructure service if:

- the applicable service complies with the Code Requirements;
- in respect of that service, the CISP complies with its obligations as a processor under GDPR; and
- the service provides the customer the ability to choose to use the service to store and process its data entirely within the EEA.

A CISP may choose to declare that only some (not all) of its cloud infrastructure services adhere to the Code Requirements. Such CISPs must ensure that potential customers are explicitly and unambiguously informed of which services adhere to the Code Requirements. Any CISP declaring its compliance with the Code must be able to comply with all the Code Requirements for each service covered by its declaration.

The proper identification of the data controller and of any data processors is vital for EU data protection law. These concepts are explained in Section 4 (Data Protection) of this Code.

In the cloud infrastructure service context, the CISP will act as a data processor to the customer (who may itself be a controller or a processor). As set out below, the Code only applies to the extent that the CISP acts as a data processor. The Code Requirements set out the principles which CISPs, as data processors, must respect.

Both data controllers and data processors have legal obligations under the GDPR. The obligations of data controllers are broader than those of data processors; data processors can play a supporting role in the fulfilment of the data controller's obligations. The Code endeavours to set out the obligations of CISPs and explain how they, as data processors, can support those of their customers who are either data controllers or themselves data processors in the supply chain.

In respect of personal data processed on behalf of a customer using the cloud infrastructure service (**Customer Data**), the CISP must not (a) access or use such data except as necessary to provide and maintain the services to the customer, or (b) process such data for the CISP's own purposes, including, e.g., for the purposes of data mining, profiling or direct marketing.

The CISP may act as a data controller in respect of certain personal data used by the CISP in order to administer the customer's account. This includes, for example, account information (such as usernames, email addresses and billing information), which the customer provides to the CISP in connection with the creation or administration of the customer's account used to access the CISP's service.

This Code does not apply where the CISP processes such data as a data controller.

The Code is transnational in scope and is intended to apply across the EEA. CISPs who may not be subject to the GDPR may also choose to voluntarily comply with the Code. A list

of the Supervisory Authorities for all EEA countries is included at Annex D.

While the focus of the Code is the GDPR, it is acknowledged that CISPs will often also be subject to security requirements and incident notification obligations under the Network and Information Systems Directive (2016/1148), as transposed into Member States law. Such obligations complement and supplement similar requirements under the GDPR and addressed in this Code.

4 Data Protection Requirements

In accordance with Article 4 GDPR, (a) the "data controller" is the party which "*determines the purposes and means of the processing of personal data*", and (b) the "data processor" is the party which "*processes personal data on behalf of the controller*".

CISPs provide self-service, on-demand cloud infrastructure. It is the customer who chooses if and how to use this infrastructure, including whether any personal data is uploaded to the cloud infrastructure service, and if so, how that personal data is "processed".

Where the customer chooses to store or otherwise process personal data using a CISP's services, and determines the purposes and means of such processing, the CISP will be that customer's processor and the customer the data controller.

For example:

- Cloud infrastructure services such as virtual server services are content and data agnostic. They typically provide the customer with the ability to deploy onto a virtual server or cloud infrastructure the customer-created applications and data for storage only by the CISP, with no further interaction by the CISP.
- A dedicated server service is another type of cloud infrastructure service, but is a server that is entirely dedicated to a customer. The server is deployed and hosted by the CISP which will, for example, replace failed hardware components, reboot the server and maintain the network. However, the applications and data are deployed by the customer.

In addition, the CISP may act as a sub-processor. This will be the case if the customer, as processor, is processing personal data on the CISP's service on behalf of and according to the instructions of a third party, as data controller. This will typically happen when the CISP customer is providing an application service to its own end customer (e.g. SaaS). In this scenario, the CISP is a sub-processor, the CISP's customer is a processor, and the third party is the data controller.

As set out in Section 3 (Scope), a CISP may also act as a data controller in the context of its own processing activities (e.g., in respect of certain personal data provided by the customer to the CISP for customer management purposes). The Code does not apply where the CISP processes such data as a controller; it only applies to describe and clarify the CISP's commitments where it acts as processor.

The purpose of this Data Protection Requirements section of the Code

The purpose of this Section 4 (Data Protection Requirements) is to clarify the CISP's role as a processor or sub-processor under GDPR in the context of cloud infrastructure services.

The Code pursues this objective by:

(a) identifying requirements for processors under GDPR (the **GDPR Requirement)** by referencing the underlying obligations in the GDPR**;** and

(b) applying the GDPR Requirement in the context of cloud infrastructure services, allocating responsibility for these requirements between the CISP and the customer, and defining the specific requirements for the CISP under the Code (the **Requirement for CISP)**;

Through this approach, the Code provides both an interpretation and an application of the GDPR Requirement to CISPs, which gives more clarity to the customer on what it can expect to receive and sets a high bar for compliance by the CISP. In addition to adhering to the Code, CISPs and customers shall consider all the requirements of applicable EU and national data protection law in their provision and use of cloud infrastructure services, respectively.

A key objective of the Code is that it shall address the key requirements for CISPs under the GDPR. The Code shall be reviewed and updated as necessary to consider changes in applicable EU data protection law in accordance with Section 7 (Governance) (including any binding specification which may be provided by the competent Supervisory Authorities concerning GDPR).

Explanatory note on interpretation

In the Code Requirements set out below, where there are references to "reasonable", "reasonable" in this context means what is objectively reasonable in the circumstances taking account of the context between the CISP and relevant customer(s).

4.1 Processing Personal Data lawfully

GDPR Requirement:

The **controller** must ensure that personal data is "*processed lawfully*" (GDPR Art 5(1)(a)). Processing is lawful only if certain conditions apply. Except where required to comply with European Union or Member State law to which the processor is subject, the **processor** shall process personal data "*only on documented instructions from the controller*" (GDPR Art 28(3)(a) and GDPR Art 29).

Requirement for CISP:

The CISP shall only process personal data in accordance with the customer's instructions. The Service Contract and use by the customer of the features and functionalities made available by the CISP as part of the service are the customer's complete and final instructions to the CISP in relation to processing of personal data. The Service Contract describes the parameters of the service and the processing which the CISP may therefore undertake: the features and functionalities and any available support services allow for additional instructions to be given by the customer to the CISP. For example, via the customer's use of the service configuration tools to determine how certain aspects are set up. Such new instructions must be within the overall parameters of the Service Description. To the extent the CISP is required to process personal data by European Union or Member State law, the processor will be required to comply with such law. The GDPR sets out that in this case, the CISP must inform the customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

Explanation:

CISPs have no control over what content the customer chooses to upload to the service (including whether or not it includes personal data). CISPs have no role in the decision- making as to whether or not the customer uses the cloud infrastructure service for processing personal data and for what purpose. Accordingly, CISPs are not able to ascertain whether there may be a lawful basis for the processing. As such, their responsibility is to (a) comply with the customer's instructions as

provided for in the Service Contract and (b) provide information about the service in accordance with Section 5 (Transparency Requirements) of the Code.

4.2 Contractual terms and conditions of the CISP's services

GDPR Requirement:

> "*Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets 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*" (GDPR Art 28(3)).

Requirement for CISP:

A contract between the CISP and the Customer shall define the features of the service and how it is delivered and the respective rights and obligations of the CISP and the customer (the **Service Contract**) as set out in sub-sections (a) and (b) below. The CISP shall ensure that the Service Contract is legally binding on the CISP with regard to the customer. The CISP shall not process Customer Data without such a Service Contract in place.

Explanation:

CISPs provide cloud infrastructure. Customers have the flexibility to choose how to use that infrastructure and they can also choose to change how and for what purpose they use that cloud infrastructure at any time. The Service Contract should have appropriate descriptions, without inhibiting the customer's flexibility to choose how to use the infrastructure.

(a) Description of processing

To facilitate these features of cloud infrastructure services and to avoid the need to amend the Service Contract or enter a new Service Contract every time the customer or any customer end-user chooses to change the way it uses the service, the description of processing in the Service Contract should be drafted in a way that reflects the features of cloud infrastructure services used by customers.

For flexibility, Service Contracts may address the description of the processing using the cloud infrastructure services on a generic basis, for example, "compute, storage and content delivery on the CISP's network" and referring to the documentation such as service descriptions or user guides for additional details. The processing activities carried out by the CISP via its provision of the service must be clear from this documentation, for example, through the provision of a detailed service description.

(b) Content of Service Contract

The Service Contract must be in writing (including in electronic form) and be legally binding between the CISP and the customer. The Service Contract shall stipulate processor's obligations as provided by Article 28(3) GDPR and must contain, at a minimum, provisions which address those requirements which are stated as applying to the CISP under:

- CISP Requirements under Section 4.1 (Processing Personal Data lawfully) (GDPR Art 28(3)(a));
- CISP Requirements under Section 4.3 (Security) (GDPR Art 28 (3)(c));
- CISP Requirements under Section 4.4 (Transfer of personal data to third countries);
- CISP Requirements under Section 4.5 (Sub-processing) (GDPR Art 28(2) and (4));

- CISP Requirements under Section 4.6 (Demonstrating Compliance) (GDPR Art 28(3)(h));
- CISP Requirements under Section 4.7 (Data subject rights) (GDPR Art 28(3)(e));
- CISP Requirements under Section 4.8 (CISP personnel) (GDPR Art 28(3)(b));
- CISP Requirements under Section 4.9 (Data breach) (GDPR Art 28(3)(a) and (f));
- CISP Requirements under Section 4.10 (Deletion or return of personal data) (GDPR Art 28(3)(g)); and
- CISP Requirements under Section 5 (Transparency).

(c) Form of Service Contract

The Service Contract must be in writing, including electronic form, but may be structured in any way, including:

- a single contract;
- a set of documents such as a basic services contract with relevant annexes (data processing agreements, SLAs, service terms, security policies, etc.); or
- standard online terms and conditions.

4.3 Security

GDPR Requirement:

> *"Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the* ***controller and the processor*** *shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk*" (GDPR Art 32(1)).

Requirement for CISP:

(a) Security Measures

The CISP shall implement and maintain appropriate technical and organisational measures for the CISP's data center facilities, servers, networking equipment and host software systems that are within the CISP's control and are used to provide the CISP's service (the **CISP Network**).

Annex A of this Code (Security Responsibilities) sets out the minimum standards for security and contains the security responsibilities which must be adopted by the CISP in order for a service to adhere to the Code. The technical and organisational measures implemented by the CISP must: (a)be designed to help customers secure personal data against unauthorised processing and accidental or unlawful loss, access or disclosure, and (b) address each of the security responsibilities of the CISP as set out in Annex A (Security Responsibilities).

CISPs should actively seek to ensure that the security measures they implement do not prevent customers from deploying their own best security practices. For example, customers must be free to securely encrypt their personal data.

Explanation:

Cloud infrastructure services are generally content agnostic. They offer the same technical and organisational measures and level of security to all customers, irrespective of whether they are processing personal data or not or the nature, scope, context and purposes of processing the customer is using the service to perform. Standardised options may be made available by a CISP to allow the customer to select additional measures to be applied. For example, CISPs will provide information on any enhanced features that are available so where the customer is processing special categories of data, customer will be able to select additional security options to satisfy the relevant requirements for processing such data. It is the customer's responsibility to adopt, on a risk-based approach, technical and organisational measures to secure the data, by selecting the appropriate options made available by the CISP. The CISP, in turn, is responsible for implementing the relevant technical and organisational measures set out in each standardised option.

Security and compliance, including the technical configuration of the environment, is a shared responsibility between the CISP and the customer. This shared model can help relieve customer's operational burden as the CISP operates, manages and controls the components from the *host* operating system and virtualisation layer down to the physical security of the facilities in which the service operates. The customer assumes responsibility and management of the *guest* operating system (including updates and security patches), other associated application software, and the configuration of the CISP security measures according to the Service Contract. Annex A (Security Responsibilities) defines the security responsibilities of both the CISP and the customer in the context of a cloud infrastructure service. The specific security and data protection controls on the CISP and the customer will be set out in each Service Contract.

It is essential to distinguish between:

- the security of the infrastructure provided by the CISP on which this data is processed; and
- the security of the data being processed.

Security of the infrastructure

The CISP is responsible for protecting the infrastructure that runs all of the services offered in the cloud infrastructure service. This infrastructure is composed of the hardware, Host Operating Software (if applicable to that service offering), networking, and facilities that run cloud infrastructure services. For example, the CISP is responsible for the deployment, operation and security of any physical hardware used to provide the cloud infrastructure service. Annex A (Security Responsibilities) provides further details as to the scope of these responsibilities.

The CISP must make available a mechanism to filter data flows, such as a firewall, around the perimeter of the cloud infrastructure as a whole and/or a firewall around the service instance which is deployed.

Where there are a filter mechanisms (such as a firewall) to protect the CISP

infrastructure, the CISP will be responsible for configuring these mechanisms.

Whether a firewall will be available for each service instance will be service-dependent. Some services may not have instance-specific firewalls, in which case the customer will be responsible for applying its own instance-specific firewall.

Security of the data processed

In the context of a customer's use of the cloud infrastructure service, some key aspects of security are the customer's responsibility (and not the CISP's responsibility).

In the context of cloud services as a whole, a customer's responsibility varies depending on the services that a customer selects. The customer's choice of service(s) determines the amount of configuration work the customer must perform as part of their security responsibilities.

In IaaS, the customer is responsible for performing security configuration and management tasks, for example if a customer deploys a cloud infrastructure service instance, they are responsible for management of the guest operating system (including updates and security patches), any application software or utilities installed by the customer on the instances, and the configuration of the CISP-provided firewall on each instance. In addition, the customer is responsible for the security of data in transit and the customer's log-in credentials and permissions policies for customer personnel using the service. Annex A (Security Responsibilities) provides further details as to the scope of these responsibilities. CISPs should ensure there is transparency between CISPs and customers regarding their security responsibilities, for example, providing information on default settings which a customer may be required to configure. As set out in Section 5.1 of the Code, the Service Contract must address the division of responsibilities between the CISP and the Customer for the security of the service.

CISPs are responsible for making information on data security in respect of the services available to customers. Further, CISPs must assign a point of contact within the CISP to handle questions from customers regarding data protection or security issues relating to the service (see Section 5 (Transparency Requirements). This should allow customers to review: (a) the Annex A security responsibilities of the CISP, (b) the information made available by the CISP relating to data security in respect of the services (see Section 5 (Transparency Requirements) below), (c) the customer's chosen configuration of the cloud infrastructure service and use of the features and controls available in connection with the cloud infrastructure service, and (d) the security measures that the customer will put in place for the aspects of security under its responsibility, and then make an independent determination that together those measures provide an appropriate level of security for the processing that the customer will use the service to perform. This determination should be based on the nature, scope, context, and purposes of the customer's intended processing, which only the customer will be aware of in sufficient detail.

(b) Information security program

The CISP shall maintain an information security program with the aim to: (a) identify reasonably foreseeable risks to the security of the CISP Network, and (b) minimize security risks, including through risk assessments and regular testing.

The CISP shall designate one or more CISP personnel to coordinate and be responsible for the information security program.

(c) Continued evaluation

The CISP shall conduct periodic reviews of the security of the CISP Network and the adequacy of the CISP's information security program. The CISP may choose to review its information security program against one or more industry security standards (e.g. ISO 27000 series) or state-of-the-art-measures. The CISP shall continually evaluate the security of the CISP Network to determine if additional or different security measures are required to respond to new security risks or the results generated by the CISP's own periodic reviews.

The CISP may modify against which security standards its information security program may be assessed from time to time, but shall continue throughout the term of the Service Contract to provide at least the same level of security as is described in the CISP's security standards at the effective date of the Service Contract.

The CISP must inform the customer of any changes which it considers objectively to have an impact on the scope of its information security program or on the technical and organizational security measures under CISP's responsibilities at the effective date of the Service Contract. This notification should take place prior to the change in the CISP's security standards, unless the CISP can demonstrate that the change needed to be made urgently in order to address a security vulnerability. The customer shall be able to verify the effect of any such changes in accordance with Section 4.6 of the Code.

4.4 Transfer of personal data to third countries

GDPR Requirement:

"*Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in*" the Chapter V of the GDPR "*are complied with* ***by the controller and processor***[…]' (GDPR Art 44).

"Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to" Chapter V of the GDPR (GDPR Art 48).

Requirement for CISP:

(a) Location

The CISP's service shall provide the customer the ability to choose to use the service to store and process its data entirely within the EEA, thereby avoiding the application of the GDPR rules governing the transfer of personal data outside the EEA.

(b) Information

The CISP shall provide to the customer information about the region and country where its data is stored and processed by or on behalf of the CISP (regardless of whether the data is stored and processed entirely within the EEA, or in a third country). If the CISP sub-contracts part of the processing to sub-processors, the CISP shall also provide the information set out in Section 4.5 below.

For security reasons, only a general location (such as a city or city region area) needs to be provided. This general description shall, at least, allow the customer to identify which EU Member State has jurisdiction over the customer for processing performed by the customer using the service.

The CISP shall communicate to the competent Supervisory Authority the exact address of the relevant facilities, if such information is required by a competent Supervisory Authority to discharge its obligations under applicable EU data protection law. In light of the sensitive nature of that information and the security risks that would arise if it was disclosed publicly, the CISP may request that the competent Supervisory Authority take into account this sensitivity in making any further disclosures of the information.

For services which can be run indifferently within several different locations in the CISP Network, CISPs must make the information easily accessible to the customer (for example, on the CISP's website) and enable customers to select the location(s) within the CISP Network where their data will be processed. As set out above, CISPs must provide their customers with the ability to choose to use the service entirely within the EEA. If a customer chooses not to use the service entirely within the EEA, whether a CISP allows customers to select the countries (outside the EEA) where the storing and processing of their data will be performed will be dependent on the CISP's service offering.

(c) Level of protection

Any transfer of personal data to a country outside the EEA for the provision of CISP services, including access from a third country outside the EEA, may only occur upon instructions to the CISP from the customer.

The CISP shall assist customers, as exporters, in complying with their obligations under Chapter V of the GDPR for the lawful transfer of personal data to the relevant country, including transfers pursuant to an adequacy decision from time to time in force (for example, currently, to Switzerland, Israel and others) (GDPR Art 45) or subject to appropriate safeguards (such as, currently, Binding Corporate Rules or standard data protection clauses adopted by the Commission (GDPR Art 46)), if:

(i) the customer transfers data from within the EEA to be stored using the CISP's service, including when data is transferred for the purposes of providing "back-up" services to EEA data centers in the case of a force majeure or continuity event by CISP, in any country outside the EEA which is not recognised by the European Commission as providing an adequate level of protection for personal data; or

(ii) the customer has chosen to allow CISP upon its instructions to access data stored using the CISP's service within the EEA from such country referred to in (i) above.

The Service Contract between the CISP and the customer must make clear the circumstances in which there may be a transfer of data to outside the EEA upon customer instructions (including the provision of instructions via the CISP's configuration tools and APIs for the CISP's services) as well as the delineation of responsibilities between the customer (as

exporter) and the CISP (as an importer) regarding such transfer.

In addition, the CISP shall provide the customer with appropriate information including about the location of the relevant processing in order to enable the customer to verify on a case by case basis, prior to any transfer, whether the law or practice of the third country concerned ensures the level of data protection required in the EEA, so as to determine if the guarantees provided by the chosen appropriate safeguards can be complied with in practice.

If this is not the case, the responsibility of identifying and implementing, supplementary measures in addition to the relevant appropriate safeguard to ensure to data transferred an essentially equivalent level of protection as provided in the EEA lies on the customer, if needed with the help of the CISP (as data importer). The European Data Protection Board has published a Recommendation [insert link] on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data which can assist the CISP in the assessment relating to the third country and for identifying appropriate supplementary measures.

No transfer of personal data to a country outside of the EEA will be initiated by CISP as part of the provision of the services, if the CISP is not instructed to do so by its customer.

The CISP shall verify on a case by case basis, prior to any transfer or disclosure of personal data in response to a judgment of a court or tribunal or to any decision of an administrative authority of a third country, that such judgement or decision can be recognised or enforceable on the basis of an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, in order to ensure the lawfulness of such transfer or disclosure. If this is not the case, and without prejudice to other grounds for transfer pursuant to Chapter V of the GDPR, the CISP must identify and implement measure to ensure that transfer or disclosure not authorised by Union law are refused to the requesting third country.

Explanation:

The GDPR restricts transfers of personal data to countries outside the EEA or international organisations without an appropriate safeguard.

In the context of cloud infrastructure services, transfers of personal data outside the EU may occur, for example, where:

- the customer has agreed to allow data to be stored outside the EU and the CISP uses data centers outside the EEA to provide the services; or
- the CISP has data centers located outside of the EEA and data is transferred to these locations for the purposes of providing "back-up" services to EEA data centers in the case of a force majeure or continuity event.

To comply with GDPR, restricted transfers of personal data must either be covered by an "adequacy decision" or subject to appropriate safeguards.

Adequacy decisions: These are findings by the European Commission that the legal framework in place in a particular country, territory, sector or international organisation provides 'adequate' protection for individuals' rights and freedoms for their personal data. If a transfer is covered by an adequacy decision, the restricted transfer may go ahead. An up to date list of the countries which have an adequacy finding is published by the European

Commission's on its data protection website.

Safeguards: If no adequacy decision exists for the country, territory or sector for the restricted transfer, transfers must be subject to an appropriate safeguard. Safeguards recognised under the GDPR include:

Safeguard	Description
1. A legally binding and enforceable instrument between public authorities and bodies	A public authority or body may transfer to another public authority or body, if a signed a contract or another legal instrument which is legally binding and enforceable is in place and contains enforceable rights and effective remedies for individuals whose personal data is being transferred. This safeguard is not effective if either the giving or receiving party are private bodies or individuals, so it is unlikely to be an appropriate safeguard for CISPs.
2. Binding corporate rules	Binding Corporate Rules are internal codes of conduct operating within a multinational group. Binding Corporate Rules must be submitted for approval to a Supervisory Authority in an EEA country where a CISP is based. A CISP may make a restricted transfer if both the data exporter and data importer have signed up to the Binding Corporate Rules document in respect of restricted transfers of personal data from the group's EEA entities to non-EEA group entities.
3. Standard data protection clauses	Standard contractual clauses or "model clauses" are data protection clauses which have been adopted by the European Commission under Directive 95/46/EC. There are two sets of standard contractual clauses for restricted transfers between a controller and controller, and two sets between a controller and processor. The clauses contain contractual obligations on the data exporter and data importer, and rights for the individuals whose personal data is transferred. A CISP may make a restricted transfer if both the data exporter and data importer have entered into the standard contractual clauses. Standard data protection clauses are the safeguard most commonly used by CISPs and are likely to be most appropriate.
4. Standard data protection clauses adopted by a Supervisory Authority and approved by the Commission	In principle, a restricted transfer may be made if a CISP enters into a contract incorporating standard data protection clauses adopted by the relevant Supervisory Authority and approved by the European Commission. To date, no Supervisory Authority has adopted any standard data protection clauses.

5. An approved code of conduct	In principle, a restricted transfer may be made if the receiver has signed up to a code of conduct, which has been approved by a Supervisory Authority. The code of conduct must include appropriate safeguards to protect the rights of individuals whose personal data transferred, and which can be directly enforced. To date, no approved codes of conduct are in use as transfer tools. For the avoidance of doubt, at present, the CISPE Code is not intended to be used as a safeguard for cross-border transfers of personal data.
6. An approved certification mechanism	In principle, a restricted transfer may be made if the receiver has a certification, under a scheme approved by a Supervisory Authority. The certification scheme must include appropriate safeguards to protect the rights of individuals whose personal data transferred, and which can be directly enforced. To date, no approved certification schemes are in use.

In a judgment of 16 July 2020 Data Protection Commissioner v. Facebook Ireland LTD, Maximillian Schrems, C- 311/18, the Court of Justice of the European Union, examined the validity of the European Commission's Standard Contractual Clauses (Decision 2010/87/EC) and considered they are valid. In particular, the Court stated that the SCCs provide for effective mechanisms which, in practice, ensure that the transfer to a third country of personal data is suspended or prohibited where the recipient of the transfer does not comply with those clauses or is unable to comply with them. Nevertheless, the Court clarified that due to their contractual nature, SCCs cannot bind the public authorities of third countries, since they are not party to the contract. As a consequence, data exporters, where appropriate together with the data importer, need to verify, on a case-by-case basis and taking into account the circumstances of the transfer, whether the law or practice in the third country of destination prevents from complying with the commitments of the SCCs and where necessary to supplement those with additional measures in order to ensure to data transferred a level of protection essentially equivalent to that in the EEA. If the data exporter is not able to take appropriate supplementary measures to guarantee an essentially equivalent level of protection under EEA law, the data exporter or, failing that, the competent supervisory authority, are required to suspend or end the transfer of personal data to the third country concerned. The position set by the Court applies to all appropriate safeguards under Article 46 of the GDPR.

Transfers or disclosures not authorised by Union law: In line with Article 48 GDPR, a third country request to transfer or disclose personal data does not, as such, make a transfer or disclosure lawful under GDPR. A request from a third country court or authority does not in itself constitute a legal ground for such transfer or disclosure. A judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data can only be recognised or enforceable if based on an international agreement such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to Chapter V GDPR.

In the absence of such framework provided by an international agreement or another legal basis under the GDPR together with a ground for transfer pursuant to Chapter V GDPR, service providers subject to EU law cannot legally base the disclosure and transfer of personal data on such requests.

4.5 Sub-processing

GDPR Requirement:

> *"The processor shall not engage another processor without specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes". (GDPR Art 28(2)).*
>
> *"Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor […] shall be imposed […] Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations". (GDPR Art 28(4)).*

Requirement for CISP:

(a) Consent

The CISP shall obtain the customer's authorisation before permitting a third party sub-processor to process Customer Data. This authorisation shall either be:

Specific: in this situation the CISP shall inform the customer in writing, including in electronic writing, the specific sub-processors which it will use. It is only if the controller gives its authorisation to the sub-processing that the CISP can engage the targeted sub-processor to process the Customer Data; or

General: in this situation the customer's consent may instead be given generally through the Service Contract. In particular, the Service Contract shall define cases and conditions in which the CISP may enlist sub-processors for carrying out specific processing activities on behalf of the customer without the requirement to obtain specific authorisation from the customer.

In either case, the CISP must inform the customer of any intended changes to its sub-processors in writing (including in electronic form), giving reasonable notice of the proposed change to allow the customer to consider the change and object to the sub-processor. If the customer objects to a sub-processor, the customer may immediately by giving notice in writing terminate the Service Contract for convenience or, if agreed by the customer and the CISP, immediately terminate the service or that part of the service which is provided by the CISP using the relevant sub-processor.

(b) Information

The CISP shall maintain an up-to-date list of sub-processors which process Customer Data. This list must include the location of the sub-processor and must be easily accessible to the customer at the time of acceptance of the Service Contract and during its term. The updated list must either be accessible to the customer via a URL, or otherwise be provided in writing following a customer request. Only a general location (such as a country or specific regional area) needs to be provided. This general description shall, at least, allow the customer to identify which EU Member State has jurisdiction over the customer for processing performed by the customer using the service.

Before authorising a new sub-processor to access Customer Data:

(i) if the CISP is obtaining general authorisation for sub-processors from the customer, the CISP shall make available to the customer: the identity and general location (such as a country or regional area) of the new sub-processor; the customer's right to object to the new sub-processor (as set out above in (a)); and the deadline by which the customer must exercise their right to object. Such deadline must give the customer a reasonable time to consider the change.

(ii) if the CISP is obtaining specific authorisation for sub-processors, it shall make available to the customer the identity and general location (such as a country or regional area) of the new sub-processor and request specific authorisation from the customer before engaging that sub-processor.

While the location of data processing may depend on customer's service selection and how the customer configures the respective service, the customer may request the CISP to provide relevant information on involved sub-processors and their processing of Customer Data (including location).

(c) Sub-processing arrangements

The CISP shall impose the same data protection contractual obligations to those set out in the Service Contract between the CISP and the customer on its sub-processor.

The CISP must put in place operational arrangements in respect of its sub-processor to provide the same or a higher level of data protection to the level of data protection under the Service Contract. The CISP must be able to demonstrate to the customer through appropriate documentary evidence that it has taken such measures.

The CISP shall restrict the sub-processor's processing of Customer Data to processing that is necessary to provide or maintain the services.

The CISP shall remain fully liable to the customer for compliance with its data protection obligations and the performance of the sub-processor's data protection obligations under the Service Contract.

Notwithstanding sub-sections (a) - (c) above, CISPs may freely use subcontractors or suppliers which do not process Customer Data (such as energy suppliers, equipment suppliers, transport, technical service providers, IP Carriers, transit providers, hardware vendors, etc.) to perform the CISP's duties under the Service Contract without having to inform or seek prior authorisation from the customer, **provided that** the applicable security measures from Section 4.3 and Annex A (Security Responsibilities) are put in place by the CISP to ensure that such subcontractors, suppliers or other third parties are prevented from accessing or processing Customer Data.

4.6 Demonstrating compliance

GDPR Requirement:

> *"The processor […] makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller" (GDPR Art 28(3)(h)).*

Requirement for CISP:

In order to enable the customer to exercise its rights under Article 28(3)(h) GDPR, the CISP

will: (i) provide the customer with appropriate information and documentation as set forth in Section 4.6(a) and (ii) submit its data processing facilities to audits by an independent third party as set forth in Section 4.6(b).

(a) Information

CISPs shall comply with the Transparency Requirements set out in Section 5 and shall make necessary information about the security controls in place for the services available to customers so that customers can understand the relevant security controls and reasonably verify the CISP's compliance with the security obligations in the Service Contract.

Where information is non-confidential or non-sensitive it shall be made accessible by customers via a straight-forward process (e.g., via the CISP's website). Where information is confidential, the CISP may make it available to customers upon request but may require the customer to first execute a non-disclosure agreement. With such non-disclosure agreement, the CISP will ensure that access to the confidential information will be restricted to the customer and cannot be disclosed by the customer without the prior approval in writing of the CISP. The non-disclosure agreement shall not prevent customer from communicating with its Supervisory Authority where such communication is mandatory. Notwithstanding the security information to be provided under Section 5, the CISP may in its sole discretion choose not to disclose certain high-sensitive security information (e.g. information which, if available, would prejudice the security of the services which are provided by the CISP).

Where such information is considered too sensitive to disclose, the CISP shall provide the customer with a basic understanding of the position, if this is necessary for the customer to understand the CISP's adopted security measures.

The table below contains some examples of high-sensitive security information which a CISP may choose not to disclose.

Examples of high-sensitive security information which a CISP may choose not to disclose:
• Identity and location of security operations personnel • Detailed results of internal penetration testing • Threat model, where sharing a complete model may adversely impact the security of the CISP infrastructure • Source code of services where access to the source code would not materially improve the customer's security

CISPs may require customers to pay an additional fee for information or may choose to provide such information for no additional fee. Any additional fee shall be reasonable, cost based, proportionate to the effort involved in providing that information, and shall not be used to prevent customers from assessing compliance for the purposes of GDPR Article 28. CISPs shall be clear with customers which information is available without further payment, and which information is only available for further payment. The table below contains some examples of matters for which additional payment would typically be expected.

Examples of matters for which additional payment would typically be expected:
• Communication of audit reports including specific audit report requested by customer that are not generally made available by the CISP • Internal or external support (e.g. security consultants/auditors) for any inspection activity requested by the customer(if needed) • Attendance of security meetings, workshops or testing exercises requested by the customer • Responding to security surveys, questionnaires, interviews requested by customers

The CISP may publish current information on service availability and/or updates about security and compliance details relating to the services on the CISP's website. The relevant service may itself, as part of its functionality, give customer access to reports and logs which allow the customer to check compliance.

The CISP shall provide a mechanism (whether free of charge or for a reasonable fee) for customers that have questions regarding data protection or security issues relating to the service to request to be put in contact with the then-current CISP personnel or representative assigned by the CISP to handle such matters. These mechanisms should assist the customer in fulfilling its obligations as a controller and should be appropriate and proportionate for the cloud infrastructure service in question. These mechanisms may take the form of phone numbers, e-mail addresses, chat systems, or any other methods that allow the customer to establish communications with the relevant representative of the CISP. Access to or knowledge of Customer Data is not required to fulfil this obligation. The CISP should also give a commitment on response times, in conformance with agreements defined in the Service Contract.

(b) Audit

In addition to the information requirements above, the CISP may use independent third party auditors to verify the adequacy of the security and data protection controls that apply to the service.

If offered by the CISP, these audits:

- shall be performed according to a recognised security standard (including, for example, ISO 27001, 27017, 27018);
- shall be performed periodically as provided under the applicable standard;
- shall be performed by independent third party security professionals who are qualified to perform such audit (based on a recognised certification or experience) and recognised in the market as having competence to do so; and
- shall result in the generation of an audit report.

At the customer's written request, the CISP may provide the customer with a copy of such

full audit report so that the customer, the customer's auditor and competent Supervisory Authorities with jurisdiction over the customer can audit and verify the CISP's compliance with its security and data protection obligations under the Service Contract. Such report shall be dated within the previous 12 months. The CISP may choose to charge customers an additional fee, as set out in Section 4.6(b) above, for the provision of the audit report.

The report will be the CISP's confidential information. Before sharing the report with the customer, the CISP may require the customer to first execute a non-disclosure agreement. With such non-disclosure agreement, the CISP will ensure that access to the confidential information will be restricted to the customer and cannot be disclosed by the customer without the prior approval in writing of the CISP. The non-disclosure agreement shall not prevent customer from communicating to its Supervisory Authority where such communication is mandatory, e.g. a formal request for information on matters which are necessary in order to provide evidence of a complaint that GDPR is not being complied with.

The customer shall also, upon request, be provided with the annual report produced by the CISP's Monitoring Body pursuant to Section 7.2 (a) of the Code. Taking into account the nature of cloud infrastructure services and the inherent risks of multi-tenant environments, the annual report and the third party audits (including the reports, attestations and/or certifications resulting from them) are intended to demonstrate the compliance of the CISP (as a processor) under Article 28(3)(h) of the GDPR.

If the information provided by the CISP (including information provided under Section 4.6(a) above and the annual report prepared by the Monitoring Body in the course of its functions described in Section 7.2(a)) is not sufficient to verify the CISP's compliance with its obligations under GDPR as reflected in the Code Requirements, then the customer may choose to exercise its rights under Article 28(3)(h) GDPR as follows:

- the customer may request in writing to the CISP that the Monitoring Body perform verification, as strictly necessary to demonstrate compliance with the Code Requirements, to the extent not already demonstrated (including by any report already prepared by the Monitoring Body in the course of its functions described in Section 7.2(a));
- the CISP shall permit the Monitoring Body to perform such verification;
- in light of the potential security risks to other customers and the service generally, direct access to CISP sites or systems by the Monitoring Body shall be permitted only if there is no other reasonable means of demonstrating compliance, and performed under controlled conditions (mutually agreed between CISP and Monitoring Body) which minimise disruption to the CISP, do not cause risk to the security and continuity of service to other customers, and do not cause the CISP to be in breach of any legal obligation or duty it may have; and
- following such verification, the Monitoring Body shall generate a report which shall be provided to the customer, but shall be treated as confidential information of the CISP and be treated in the same way as any third party audit report described above.

The report generated by the Monitoring Body, insofar as it reveals any non-compliance with the Code:

- may be cited in a complaint from a customer about the compliance of services with

the Code in accordance with the Complaints Process set out in Section 7.2(a) below; and

- shall be used by the Monitoring Body to impose the appropriate sanction in accordance in Section 7.2(b) below.

The information provided to the customer under Section 4.6(a) above (the annual report provided by the CISP's Monitoring Body, the third-party audit reports and certifications provided by the CISP, and the additional verification report performed by the Monitoring Body) shall not limit any rights under GDPR Art 28(3)(h). Where the information provided by the CISP under this Section 4.6 is insufficient to demonstrate compliance as required under GDPR Article 28(3)(h), the customer may request the CISP to take additional steps as necessary to demonstrate such compliance which may include further requests to the Monitoring Body. If the CISP's or Monitoring Body's response to such request is not sufficient to demonstrate the CISP's compliance with its obligations under GDPR Art 28, the customer may request additional information from the CISP through an additional audit, including inspections, by an auditor mandated by the customer from a list of approved auditors provided by the CISP in advance. Such audit shall be conducted in the least intrusive manner possible for the CISP to verify compliance with its obligations under GDPR Art 28, and shall be subject to (i) reasonable controls determined by the CISP to avoid risks to other customers or the CISP, in particular to the security of the CISP's facilities and maintaining the CISP's uninterrupted business operations; (ii) acceptance by the customer of terms protecting confidential information of the CISP; and (iii) the customer's obligation to pay for the reasonable costs of the audit. The customer and the CISP will in good faith discuss and agree the scope of audit activities in advance of conducting any such audit.

For the purpose of the above paragraph, "auditor" means an independent third party security professional who is qualified to perform such audit (based on a recognised certification or experience) and recognised in the market as having competence to do so.

Explanation:

Cloud infrastructure services are multi-tenant environments. This means that the data of potentially all the CISP's customers could be hosted in the same premises or facilities. Physical access to the CISP's facilities by a single customer or third party introduces a potential security risk for all other customers of the CISP whose data is hosted within the same premises or facilities. This risk can be controlled if, where possible to do so, instead of an on-site audit, customers use the information provided by the CISP, or through Monitoring Body inspection activity, to verify the CISP's compliance with the security and data protection obligations in the Service Contract.

4.7 Data subject rights

GDPR Requirement:

*"Taking into account the nature of the processing", the **processor** "assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights […]" (GDPR Art 28(3)(e)).*

Data subject rights under chapter III of GDPR are the right to transparent information (Art. 12, Art. 13 and Art. 14), the right to access (Art. 15), the right to rectification (Art. 16), the right to erasure (Art. 17), the right to restriction of

processing (Art. 18), the right to notification in respect of rectification or erasure of data or restriction of processing (Art 19), the right to data portability (Art. 20), the right to object (Art. 21) and the rights on automated individual decision-making, including profiling (Art. 22).

Requirement for CISP:

The CISP shall provide the customer with the ability to rectify, erase, restrict, access or port (in a structured, commonly used and machine-readable format) Customer Data as part of the service or by enabling customers to design and deploy their own solutions using the service.

The customer may use this ability to perform its obligations in responding to requests made by data subjects. The CISP shall provide an explanation of how these abilities will be provided to the customer as part of the information required pursuant to Section 5 (Transparency). The information provided under Section 5 (Transparency) will also assist the customer in fulfilling its own transparency obligations to data subjects.

Explanation:

Providing the customer with the ability to rectify, erase, restrict, access or port Customer Data, is expected to be limit of what a CISP can do to support data subject requests, although the CISP and customer may choose to define further responsibilities between them. This is because the customer (and not the CISP) is responsible for managing the data processed by that customer using the service. Therefore, the CISP will not know what data customers are uploading to the service and, in particular, who the data subjects are in connection with any personal data being processed.

4.8 CISP personnel

GDPR Requirement:

"Processor […] ensures that persons authorised to process personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality" (GDPR Art 28(3)(b)).

Requirement for CISP:

(a) Confidentiality:

The CISP shall impose appropriate contractual obligations requiring any personnel authorised by the CISP to access Customer Data to protect the confidentiality of that Customer Data.

(b) Access controls:

The CISP shall implement and maintain access controls and policies in order to limit its personnel processing Customer Data to those CISP personnel who need to process Customer Data to provide the services to the customer. The CISP shall select appropriate access controls, which shall include: (i) restricting physical access to data center facilities to authorised personnel; (ii) restricting technical access to host software and networks to authorised personnel

(iii) logging of CISP personnel access to Customer Data. When CISP personnel no longer need to process Customer Data, the CISP shall promptly revoke that personnel's access privileges.

Explanation:

CISP's personnel may have the need to access Customer Data in order to perform the services. Access shall only be permitted as needed to manage the service. Personnel who do not need to access Customer Data to manage the service shall be subject to appropriate access controls designed to prevent them doing so.

4.9 Data breach

GDPR Requirement:

*"The **processor** shall notify the controller without undue delay after becoming aware of a personal data breach". (GDPR Art 33(2)).*

*"[**The processor**] assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor" (GDPR Art 28(3)(f)).*

Requirement for CISP:

(a) Security incident management policy

The CISP shall implement a security incident management policy that specifies the procedures for identifying, and responding to personal data breaches of which the CISP becomes aware.

This policy must include:

- guidance on how incidents should be addressed, including who is responsible for security incident management within the CISP;
- guidance on what constitutes a personal data breach under GDPR, including guidance for deciding which type of incidents have to be notified to the customer based on the potential impact on Customer Data;
- a requirement to perform expeditious investigations when a CISP becomes aware of a suspected data breach to ascertain whether a breach has occurred, and which Customer Data may be affected;
- a process for the implementation of remediation activity to mitigate the impact of a data breach, and address vulnerabilities exposed by security incidents;
- a process to notify without undue delay the customer when the CISP has ascertained that a data breach has occurred which relates to the Customer Data of that customer;
- classifications of incident type by severity, and indicative timelines for key investigatory steps, and planned notification to customer(s) (if applicable), appropriate to the severity of the incident;
- appropriate escalations, within the CISPs own governance, of incident response issues;
- a specification of the information that must be made available to the customer following the data breach; and
- a process for cooperating with customers in circumstances where the customer informs the CISP of a data breach, such as providing any preliminary information

that is available in order to assist the customer's compliance with its obligations under Article 33(1) of the GDPR.

(b) Security breach notification

Scope and timing of notification

If the CISP becomes aware of the accidental or unlawful destruction, loss, alteration or unauthorised disclosure of, or access to, any Customer Data on the CISP's equipment or in the CISP's facilities, the CISP shall notify the customer without undue delay.

Content of notice

The notification shall, to the extent the CISP has knowledge of such information as a data processor: (i) describe the nature of the security breach, (ii) describe the consequences of the breach, (iii) describe the measures taken or proposed to be taken by the CISP in response to the incident and (iv) provide a contact point at the CISP. A sample template for security breach notification is set out in Annex F. It is not mandatory for CISPs to use this template, though it provides an example of the format a CISP may use and the types of information a CISP may include in a security breach notification to a customer. The European Data Protection Board has issued guidelines on personal data breach notification under the GDPR which could help CISPs define their policy and templates for security breaches. These guidelines are available at http://ec.europa.eu/newsroom/document.cfm?doc_id=47741

4.10 Deletion or return of personal data

GDPR Requirement:

> *"[**The processor**] at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data"* (GDPR Art 28(3)(g)).

Requirement of CISP:

The CISP shall provide the customer with the ability to retrieve and delete Customer Data in its entirety. The customer may use this ability to retrieve or delete Customer Data at any time.

Depending of the type of service, the CISP may provide the customer with the ability to retrieve and delete Customer Data (a) as part of the service, or (b) by enabling customers to design and deploy their own deletion and retrieval solutions using the service. The CISP shall provide, in the information required pursuant to Section 5 (Transparency), an explanation of how these abilities will be provided to the customer. At all times, the CISP shall comply with any instructions given by the customer in respect of retrieval or deletion of Customer Data.

In the absence of instructions from the customer, CISP shall by default delete Customer Data within a reasonable period of time following the expiry or termination of the service

Explanation:

The CISP does not manage or choose to delete a customer's data on the customer's behalf. Therefore, it is the customer's responsibility to manage deletion and retrieval of data on the service taking into account any process triggered by the termination or expiry of the Service Contract, using the ability provided by the CISP although the

CISP and customer may choose to define further responsibilities between them.

4.11 Records of processing

GDPR Requirement:

"Each processor and, where applicable, the processor's representative, shall maintain a record of all categories of processing activities carried out on behalf of a controller containing:

(a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;

(b) the categories of processing carried out on behalf of each controller;

(c) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;

(d) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).." (GDPR Art 30(2))

"The records…shall be in writing, including in electronic form." (GDPR Art 30 (3))

"The controller or the processor and, where applicable the controller's or the processor's representative, shall make the record available to the supervisory authority on request" (GDPR Art 30(4))

Requirement of CISP:

The CISP shall maintain a written record (which may be electronic) of processing activities it carries out on behalf of its customers who are controllers, including:

- the name and contact details of the customer;
- the categories of processing carried out by the customer (these categories may be stated by reference to the services provided by the CISP);
- whether the CISP has implemented or otherwise makes available to the customer a mechanism for transfers which is recognised under Chapter V of the GDPR; and
- a general description of the security measures in place(for example, such as the measures adopted to comply with Annex A).

The CISP must make the record available to a Supervisory Authority on request.

Explanation:

Due to the nature of IaaS, only the customer will have visibility and control over the specific categories of processing. The CISP will maintain records of the services used by its customers as required under the GDPR; however, the customer is the only party with visibility into the specific details of the personal data it chooses to process using these services (and is separately required to maintain records pursuant to GDPR Article 30(1)).

The CISP will also likely need to keep a separate record of processing in accordance

with Article 30.1 of the GDPR where it is acting as a data controller, such as in the context of its own personnel records or customer management systems. However, given that the focus of the Code is on the CISP's obligations as a processor, this particular obligation on data controllers is not included within the scope of the Code.

5 Transparency Requirements

Customers need to be able to perform reliable security risk and data protection impact assessments for personal data processed on cloud infrastructure services.

The CISP shall help the customer to achieve this objective by providing transparency about the security measures implemented by the CISP for its services. To provide adequate transparency the CISP shall comply with Section 4.6 of the Code, "Demonstrating Compliance" and Article 28(3)(h) GDPR, and, as a minimum, provide the following information to customers:

1. A Service Contract that addresses the division of responsibilities between the CISP and the customer for the security of the service.
2. A high level statement on the security objectives and standards that apply to the service concerning at least Confidentiality, Availability, Integrity.
3. Information on the design and management of the service to help customers understand potential threats and vulnerabilities for the customer's use of the service.
4. Information validating the risk management processes, considered threats model and risk management criteria of the CISP for the service.
5. Information on the security measures implemented by the CISP for the service.
6. Documentation covering the CISP's information security management system.
7. Information on the service functionality which allows the customer to i) rectify, erase, restrict, access or port Customer Data (as set out in Section 4.7); and ii) retrieve and delete Customer Data (as set out in Section 4.10).

The CISP shall also, either alone or in combination with others, (whether internal or external) appoint a data protection point of contact or Data Protection Officer, where required by the GDPR or applicable law (the Article 29 Working Party has issued Guidelines on Data Protection Officers which may help CISPs with this assessment. These guidelines are available at https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048). If a CISP is not required to appoint a data protection point of contact or Data Protection Officer, the CISP still must assign a point of contact within the CISP to handle questions from customers regarding data protection or security issues relating to the service, under the mechanism described in Section 4.6(a).

The sub-sections below describe what steps the CISP shall take to ensure the adequate level of transparency for each service declared as adhering the Code.

The CISP may achieve these objectives by implementing an information security management system covering these 7 objectives (as set out in sub-sections 5.1-5.7 below). The Code encourages CISPs to implement state-of-the-art information security management systems based on one or more recognised industry standards. Except for requirements specifically for the Service Contract, the CISP may choose to communicate the information referred to in this Section 5 (Transparency Requirements) to customers by:

- providing information about the CISP's security and control practices; and/or
- obtaining industry certifications and/or independent third-party attestations; and/or
- providing certificates, reports and other documentation directly to customers.

Where the CISP considers information is confidential, the CISP may make it available to customer upon request but may require the customer to first execute a non-disclosure agreement. With such non-disclosure agreement, the CISP will ensure that access to the confidential information will be restricted to the customer and cannot be disclosed by the customer without the prior approval in writing of the CISP. The non-disclosure agreement shall not prevent customer from communicating with its Supervisory Authority where such communication is mandatory.

5.1 A Service Contract that addresses the division of responsibilities between the CISP and the Customer for the security of the service

The Service Contract shall define the security responsibilities of the CISP and the customer for the duration of the term of the Service Contract. Notwithstanding the relevant EU and member state legal obligations that apply to the CISP, the customer, as data controller, will generally remain responsible for any aspect of security under its responsibility as data controller, which is not covered by the Service Contract.

In addition to the Service Contract, the CISP may choose to make available for consultation further documentation for the service which describes the division of responsibility for security between the CISP and the customer. For example, the CISP could provide a matrix describing responsibilities of both parties based on their shared control of the IT environment and controls when using the service.

5.2 A high level statement on the security objectives and standards that apply to the service

The CISP shall state (a) the objectives that the security measures implemented by the CISP for the service are designed to pursue, and if applicable (b) the standards the CISP will follow when implementing those security measures. See Annex A (Security Responsibilities) for further details.

The CISP may modify the applicable security standards from time to time provided that the service continues to provide at least the same level of security as was described in the applicable standards at the effective date of the Service Contract.

The CISP shall inform customers if a cloud infrastructure service is intended by the CISP to assist customers to comply with a recognised standard or legal requirement applicable to a specific type of processing (e.g. processing healthcare data). This information may be communicated by the CISP to customers within the Service Contract, a service description and/or via the CISP's website or other publicly available material.

5.3 Information on the design and management of the service

The CISP shall provide information to customers on the infrastructure available to the customer and how it is used to deliver the service (i.e. the facilities, network, hardware and operational software that support the provisioning and use of the services).

This information may, for example, include:

- High-level architecture of the infrastructure
- General location of the CISP's hosting facilities relevant to the customer
- Hardware configuration, if relevant
- Subcontractor's authorised by the CISP to access Customer Data

- Security features of the service
- Options the customer can use to add to further security to the service

5.4 Information validating the risk management processes and criteria of the CISP

The CISP shall provide information to customers validating the existence and suitability of the CISP's risk management program, including its considered threats model and risk management criteria, to assist customers to incorporate the CISP's controls in the customer's own risk management framework. This information may, for example, include internal and/or external risk assessments performed or commissioned by the CISP and covered in one or more audit reports.

The Code encourages the CISP to follow a risk assessment methodology based on recognised industry standards such as ISO/CEI 27005, OCTAVE or EBIOS.

5.5 Information on the security measures implemented by the CISP for the service

The CISP shall make necessary information about the security measures in place for the services available to customers to assist customers to understand the controls in place for the service that they use and how those controls have been validated.

This information is intended to help customers evaluate if they can use and configure the services in a way that provides an appropriate level of security for the processing the customer will use the services to perform.

Specifically, the CISP shall describe:

- the physical and operational security processes for the network and server infrastructure under the CISP's management; and
- the security features and controls available for use and configuration by customers on the service (on each of which the CISP shall maintain a secure by default posture).

This information shall, for example, include information about:

- physical and environmental security;
- network security;
- logical or physical controls to ensure isolation of customer's data, such as network segmentation of data storage principles;
- business continuity management;
- change management; and
- account security features.

5.6 Documentation covering the CISP's information security management system

The CISP shall make sufficient information about the information security management system in place for the services available to customers so that customers can reasonably verify the CISP's compliance with the security obligations in the Service Contract as described in Section 4.6 (Data Protection; Demonstrating Compliance) of this Code.

5.7 Information on the service functionality which allows the customer to i) rectify, erase, restrict, access or port Customer Data; and ii) retrieve and delete Customer Data.

The CISP shall provide the customer with information about the capabilities available to them to enable them to:

- rectify, erase, restrict, access or port Customer Data as set out in Section 4.7 of this Code (Data subject rights); and
- retrieve and delete Customer Data as set out in Section 4.10 of this Code (Deletion or return of personal data).

6 Adherence

A CISP that declares adherence with the Code must comply with all the Code Requirements for any service covered by its declaration and may then use the Mark (as defined in Section 6.4 below). CISPs cannot declare to adhere to only a chosen part of the Code Requirements or to exclude certain sections of the Code Requirements.

The CISPs that have declared adherence to the Code must also commit to submit to Section 7 (Governance). If a CISP fails to meet the Code Requirements, it shall be subject to the enforcement mechanisms as set out in Section 7 (Governance). Adherence to Section 7 by a CISP is without prejudice to any possible sanctions from competent Supervisory Authorities under applicable EU data protection law.

6.1 Declaring a service adherent to the Code

There are two possible routes for initially declaring a service adherent to the Code: Self-Assessment and Controlled Adherence:

(a) <u>Self-Assessment</u>

For Self-Assessment, a CISP must complete a self-assessment of its service against the Code Requirements and present to the Secretariat:

- its Declaration of Adherence; and
- a completed Compliance Checklist as set out at Annex B of the Code, and any supporting information.

Further information on the relevant documents to be submitted is set out in Section 6.2 below.

Following submission, the Secretariat shall review the documentation. (For the avoidance of doubt, the Secretariat has an administrative function, and shall only confirm that the documentation is complete. Assessment of a service's Code compliance may only be carried out by a Monitoring Body).

Within 40 working days of receipt of the submission, the Secretariat shall notify the CISP whether the submission is complete. If the submission is not complete, the Secretariat may request that the CISP provide any missing document or additional information required to complete its submission.

If the submission is complete, the Secretariat shall incorporate the Declaration of Adherence into the CISPE Public Register within 10 working days of the Secretariat notifying the CISP of its acceptance. The CISPE Public Register will clearly indicate that the relevant service has not yet been assessed and approved by a Monitoring Body and the service will be described as “Candidate to the Code” until a Monitoring Body has confirmed that the service is compliant pursuant to its Initial Review as set out in Section 6.3 below.

CISPs that have followed the Self-Assessment process shall:

only be entitled to have the self-assessed service into the CISPE Public Register as “Candidate to the Code”, for a maximum period of 12 months following the date of incorporation of the Declaration of Adherence into the CISPE Public Register; and

ensure its designated Monitoring Body reviews and verifies the service's Code compliance within 12 months of the date of that incorporation.

Following Monitoring Body assessment of the service's Code compliance through its Initial Review, if the service is confirmed to be Code compliant by the Monitoring Body, the CISP shall submit written confirmation from its Monitoring Body that the CISP service adheres to the Code. Following receipt by the Secretariat of such written confirmation, the CISP service shall have the same status as if the CISP had followed the Controlled Adherence process set out below:

  - it may use the Compliance Mark, as noted in Section 6.4 below; and
  - the CISPE Public Register shall be updated to clarify that the CISP service has now been assessed and approved by its Monitoring Body,

- if the service is found not to be Code compliant, the relevant CISP service and Declaration of Adherence shall be removed from the CISPE Public Register.

The Self-Assessment process is an interim process. The CISP's service(s) shall not be deemed Code compliant until the service(s) have been assessed and approved by its Monitoring Body. The Self-Assessment process is intended to facilitate SME participation in the Code, to give CISPs additional time to become familiar with the Code process and requirements, put a contract in place with a Monitoring Body and organise relevant internal resource to facilitate ongoing Code adherence.

(b) <u>Controlled Adherence</u>

For Controlled Adherence, a CISP must first submit the relevant service for Monitoring Body assessment and verification, and present to the Secretariat:

- its Declaration of Adherence;
- a completed Compliance Checklist as set out at Annex B of the Code, and any supporting information; and
- written confirmation from its Monitoring Body that the CISP service adheres to the Code.

Further information on the relevant documents to be submitted is set out in Section 6.2 below.

Following submission, the Secretariat shall review the submission. (For the avoidance of doubt, the Secretariat has an administrative function, and shall only confirm that all relevant documentation is complete. Assessment of a service's Code compliance may only be carried out by a Monitoring Body).

Within 40 working days of receipt by the Secretariat of the submission, the Secretariat shall notify the CISP whether the submission is complete. If the submission is not complete, the Secretariat may request that the CISP provide any missing document or additional information required to complete its submission.

If the submission is complete, the Secretariat shall incorporate the Declaration of Adherence into the CISPE Public Register within 10 working days of the Secretariat notifying the CISP of its acceptance.

Once the Declaration of Adherence is incorporated into the CISPE Public Register:

- the CISP is entitled to use the Declaration of Adherence and the Compliance Mark, as noted in Section 6.4 below, exclusively for the services covered by the Declaration of Adherence and so long as it remains valid and subject to any

enforcement measures under Section 7.2 (Monitoring, Complaints and Enforcement); and

- if any material change to the service occurs which may impact the CISP's current Declaration of Adherence, then (i) the CISP must, without undue delay, notify the Secretariat and Monitoring Body; (ii) cooperate with the Secretariat to update those materials; and (iii) comply with any requirement by the Monitoring Body to submit such updates for further assessment.

6.2 Documentation

(a) Declarations of Adherence

The current form of the Declaration of Adherence is set out in Annex C. This may be updated by the CCTF from time to time. The Secretariat shall publish and maintain an up to date version of the Declaration of Adherence on the CISPE Public Register. In submitting its Declaration of Adherence the CISP is confirming that the service complies with Code Requirements. The CISP's designated Monitoring Body shall be responsible for monitoring and assessing the CISP's compliance with the provisions of the Code, as set out above in respect of the initial Declaration of Adherence and under Section 7.2 below in respect of ongoing assessment.

(b) Compliance Checklist and supporting documentation

The Compliance Checklist is set out in Annex B. The Compliance Checklist sets out the Code requirements and suggested guidance to CISPs on how compliance with the Code Requirements can be achieved and how the technical and organisational security practices of Annex A can be implemented.

When submitting its completed Compliance Checklist, CISPs are encouraged to include supporting documentation. For example: the current Services Agreement; the CISP's internal policies and procedures; examples of contracts with CISP personnel, contractors etc.; information about the CISP's services; information about the CISP's security and control practices; and/or industry certifications and/or independent third party attestations, are all documents which may support a CISP's Compliance Checklist and may, at the sole discretion of the Monitoring Body, be used in assessing Code compliance. The Monitoring Body shall be entitled to ask the CISP for any further material which it requires to verify compliance by the CISP with the Code Requirements.

(c) Written confirmation from the Monitoring Body

Where a CISP is following the Controlled Adherence process, it must submit written confirmation of the service's assessment and verification by its Monitoring Body. Such confirmation may take the form of a letter or other signed document prepared by the Monitoring Body.

6.3 Renewal and Review

For CISPs following the Self-Assessment process, the Monitoring Body must assess and verify the service's Code compliance within 12 months of the date of incorporation of the CISP's Declaration of Adherence in the Public Register. For CISPs following the Controlled Adherence process, the Monitoring Body's assessment and verification of the service will take place prior to the incorporation of the CISP's Declaration of Adherence in the Public Register. In both cases, the Monitoring Body will be provided with the relevant Declaration of

Adherence and Compliance Checklist on which to base its assessment and verification, and the approach taken to assessment by the Monitoring Body will be the same. The Monitoring Body shall be entitled to ask the CISP for such further information as it deems necessary to assess compliance.

In either case, this is the Monitoring Body's "**Initial Review**". For the avoidance of doubt, assessment, verification and ongoing review of Code compliance shall be carried out in respect of *each service* that is declared to be Code compliant. Where a CISP has multiple services which are declared to Code compliant, the Monitoring Body must assess each service.

Following the Initial Review, Monitoring Body assessment of Code Compliance shall take place annually, in accordance with Section 7.2(a) of the Code. To allow such reviews to reflect any existing annual audit cycles of the CISP, the second review may take place at any time within 18 months of the date of the Initial Review. Thereafter, annual reviews must be completed within 12 months of the anniversary of the previous annual review.

In carrying out reviews, the Monitoring Body may use existing relevant materials available to it (including those materials used to support the CISP's Declaration of Adherence), but further review by the Monitoring Body may be required if the existing materials are not sufficient to verify the CISP's adherence to the Code.

At least two weeks prior to the date of each annual review, the CISP shall submit to the Secretariat and Monitoring Body: an updated Declaration of Adherence; or, if neither the service covered by the original Declaration of Adherence nor the Code, have been materially changed since submission, written confirmation of the continued accuracy of the Declaration of Adherence and any supporting information provided on submission. The maximum period of validity of a Declaration of Adherence is three years. Once this three year period has expired, the CISP must submit a new Declaration of Adherence.

The Monitoring Body shall re-approve the CISP's Code compliance each year via its annual review: An annual review does not require a full audit of Code compliance. The annual reviews will be performed as followed:

- In the first annual review following the Initial Review, or last audit cycle, the Monitoring Body will review the Code requirements for compliance related to Section 4 of the Code except Section 4.3;
- In the second annual review following the Initial Review or last audit cycle, the Monitoring Body will review the Code requirements for compliance related to Section 4.3 of the Code;;
- In the third annual review following the Initial Review, or last audit cycle, the Monitoring Body will review the Code requirements for compliance related to Section 5 of the Code.

However, the Monitoring Body must carry out a full review of the service's Code compliance at a minimum:

- following any material modifications to the service or the Code; or,
- absent any material modifications to the service or the Code, once every three years.

In addition to the above, During each three year audit cycle, the Monitoring Body shall carry

out a full audit of Code compliance:

If the Code has been materially modified, CISPE will specify a reasonable timeframe within which the CISP must make any necessary updates to ensure the CISP services meet the new Code Requirements, following which, the CISP must present a new or revised Declarations of Adherence, Compliance Checklist, and any supporting information, setting out how the CISP services meet the new Code Requirements. The timeframe specified by CISPE will take into account the relevant modifications made to the Code, but in any event shall be no longer than six months.

Material modifications to the service include any modifications which could have an impact on the service's Code compliance. For example, changes to how the services are designed and implemented. Further guidance on what constitutes a "material modification" under the Code may be published by the CCTF in the future, reflecting feedback from Monitoring Bodies on what matters have a material impact on their assessment of compliance.

Every three years, the Monitoring Body shall prepare a written audit report for the CISP service and shall share this report with CISPE. The audit report will include details regarding the audit methodology, findings, analysis, conclusions and recommendations or any equivalent commensurate with the state-of-the-art of conformity assessment methodology such as in the context of ISO 27001 audit.

6.4 Mark

The CCTF shall develop a Compliance Mark to be used as a public-facing symbol of a service's adherence to the Code Requirements (the Mark). The Mark shall be approved by the Executive Board.

CISPs which choose the self-Assessment route are not allowed to use the Compliance Mark until the Monitoring Body has completed its Initial Review and verified the CISP's Code compliance. This is to increase transparency for customers and distinguish between CISP services which: (a) are within the self-Assessment process, and (b) have obtained Monitoring Body approval.

The CCTF shall develop and keep under review guidelines for the use of the Mark by CISPs **(Compliance Mark Use Guidelines).** The Secretariat shall publish and maintain an up to date version of the Compliance Mark Use Guidelines on the CISPE Public Register. The Compliance Mark Use Guidelines will as a minimum address the following:

- Requirement that the Mark be applied only to specific services which the Monitoring Body has confirmed as adherent under its Initial Review
- Requirement that the Mark be used in a manner which is clear and does not mislead the market in respect of the CISPs actual adherence
- Ability for CISPE to suspend or terminate the use of the Mark if a CISP has used it materially outside the requirements of the Compliance Mark Use Guidelines
- Suspension of rights of use of the Mark in case of any suspension of the CISPs adherence in respect of a service, and termination of rights of use of the Mark in case of any exclusion of the CISPs adherence in respect of a service

Once the CISP's Declaration of Adherence is incorporated into the CISPE Public Register, the CISP will be entitled to use the Mark so long as its Declaration of Adherence remains

valid and provided that the CISP uses the Mark: (a) exclusively for the services covered by their Declaration of Adherence, and (b) in accordance with the Compliance Mark Use Guidelines. If the CISP provides different cloud infrastructure services and not all the CISP's services are covered by a Declaration of Adherence, the CISP must ensure that their use of the Marks unambiguously identifies the specific services covered by the CISP's Declaration of Adherence.

For the avoidance of doubt, displaying the Compliance Mark is not a substitute for GDPR compliance and does not signify compliance with a code of conduct with binding and enforceable commitments pursuant to Art 46 GDPR.

The Secretariat shall send a communication to the CNIL twice a year as the Designated Supervisory Authority under the Code, identifying new CISP services which have been declared to be Code compliant by a Monitoring Body during the relevant six month period and are entitled to use the Compliance Mark.

7 Governance

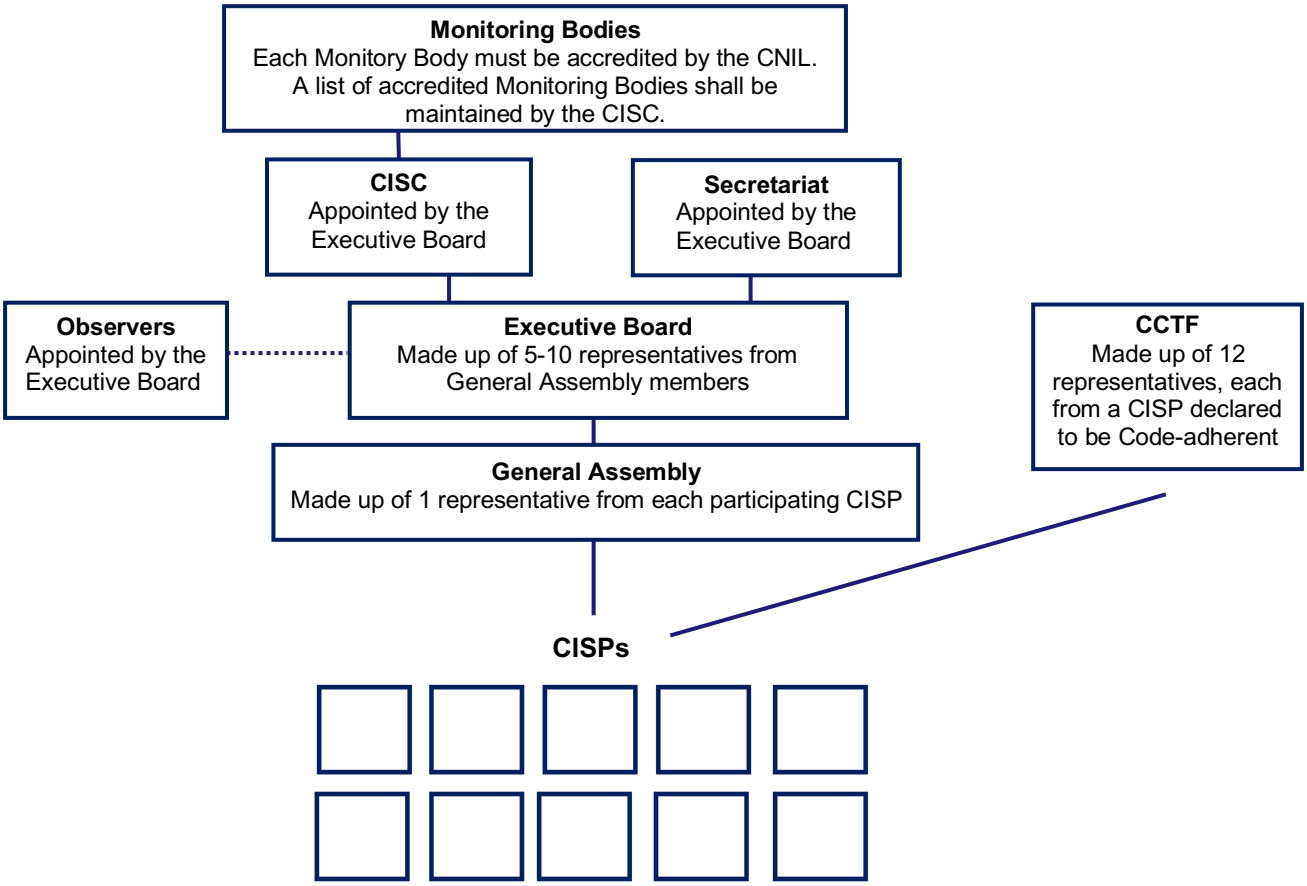
7.1 Governance Structure

The Association of Cloud Infrastructure Service Providers of Europe **(CISPE)** is responsible for the governance of the Code. The table and structure chart below provide an overview of the current structure of CISPE, including its key bodies, how those bodies are comprised and their key responsibilities.

General Assembly **Representation**: Each participating organisation is permitted one voting representative in the General Assembly. There is no limit on the number of participating organisations. **Eligibility**: To be eligible for membership of the General Assembly, an organisation must (a) provide a cloud infrastructure service to customers in the EEA, (b) that service must provide customers with the ability to choose to use the service to store and process its data entirely in the EEA, and (c) have at least one service declared as adherent to the Code by its Monitoring Body (i) prior to joining the General Assembly if the CISP follows the Controlled Adherence process, or (ii) within one year of joining the General Assembly, if the CISP follows the Self-Assesment process. **Key responsibilities**: Elect representatives to the Executive Board; at least 10% of members acting together may propose changes to the Code to the Executive Board; adopt changes to the Code.
Executive Board **Representation**: Between 5 and 10 representatives each from a different General Assembly member. Board representatives are elected by the General Assembly. **Eligibility**: To be eligible to present a candidate for election to the Executive Board a member must either (a) be a founding member or (b) both (i) derive a significant part of their income from cloud infrastructure services, and (ii) own or exercise effective control of underlying physical computing infrastructure for such cloud infrastructure services. **Key responsibilities**: Approves: (a) admission of new General Assembly members, (b) Marks, (c) guidelines for adherence to the Code, and (d) reviews and makes changes to the Code. Appoints: (a) non-voting representatives of the CCTF, (b) CISC Members, (c) the Secretariat, and (d) Observers.
Code of Conduct Task Force ("CCTF") **Representation**: Each organisation with at least one service declared as adherent to the Code (whether or not it is a General Assembly member) may appoint one voting representative to the CCTF. The CCTF shall be composed of **a maximum of twelve (12) individuals** that have proven (i) expertise related to cloud computing and/or data protection, and/or (ii) understanding of cloud computing business models. Each General Assembly member and the Executive Board may appoint non-voting representatives to the CCTF (e.g. academics or experts, representatives of cloud infrastructure service user associations, representatives of the European Commission). Any third party (including any end customer) wishing to have a non-voting representative may send a written request to the Executive Board requesting an invitation. **Eligibility**: Representatives must have proven: (a) expertise related to cloud computing and/or data protection, and/or (b) understanding of cloud computing business models. **Key responsibilities**: Evaluate Code based on changes to applicable EU data protection law; propose changes to the Code to the Executive Board; produce guidelines for adherence to the Code; express a non-binding opinion on proposed changes to the Code presented by the Executive Board, recommend auditors, norms and certification schemes suitable for demonstrating adherence to the Code by entities; develop Marks; and develop compliance mark use guidelines.
Code Independent Supervisory Committee ("**CISC**") **Representation**: Three members appointed by the Executive Board. **Eligibility**: External independent experts drawn from academia, technical or legal backgrounds. These experts should be experienced in engaging with Supervisory Authorities, businesses, and data subjects. **Key responsibilities**: Maintain the list of organisations accredited as Monitoring Bodies by the CNIL; provide support to Monitoring Bodies in reviewing the application of the Complaints Process; provide support to Monitoring Bodies in achieving a consistent application of the Code by each Monitoring Body; periodically review the operation of the Code via annual workshops with Monitoring Bodies.
Monitoring Body **Representation**: Appointed in respect of any CISP from a list maintained by the CISC. **Eligibility**: See below

Key responsibilities: Monitor CISPs' compliance with the Code; consider complaints about non-compliance of services with the Code; impose enforcement action against a non- compliant CISP ; report any concerns about the operation of the Code to any competent Supervisory Authority.	
Secretariat **Representation**: Appointed by the Executive Board. **Key responsibilities**: Review declarations of adherence to the Code; publish and maintain information on the CISPE Public Register; day-to-day administration of CISPE.	**Observers** The Executive Board may invite representatives who are not affiliated with General Assembly members to participate as non-voting observers.

Structure chart



7.2 Monitoring, Complaints and Enforcement

(a) Monitoring Structure and Monitoring Bodies

The monitoring of the Code shall be structured as follows:

- All Monitoring Bodies must be accredited by the CNIL as the Designated Supervisory Authority.
- The CISC shall maintain a list of the organisations which have been accredited by the CNIL. Such organisations may be appointed by CISPs as their Monitoring Body;
- The Monitoring Body shall be responsible for mandatory monitoring of compliance by CISPs with the Code. Each CISP shall choose a Monitoring Body from the list maintained by the CISC;
- A Complaints Process shall be established in accordance with the principles set out below; and
- The CISC shall support Monitoring Bodies to ensure consistency in the application of the Code by each Monitoring Body, and monitor the application of the Complaints Process.

Code Independent Supervisory Committee ("CISC")

The CISC shall periodically review the implementation of the Code itself, including the Compliance Checklist, and make recommendations to the CCTF and Executive Board for any changes to the Code which may be required.

The CISC shall compile and maintain a list of independent competent third-party organisations that may be selected by CISPs to be their Monitoring Body because they are duly accredited by the competent Supervisory Authority. Those organisations shall demonstrate:

a) an appropriate level of expertise in relation to the subject-matter of the Code and the cloud environment. A Monitoring Body may show such competencies by demonstrating: (i) experience in certifying against relevant industry standards such as ISO 27001, 27017 and 27018 or other equivalents; or (ii) other equivalent auditing experience in information security or privacy;

b) they are accredited to be a Monitoring Body by the CNIL as the designated Supervisory Authority;

c) independence in relation to the subject-matter of the Code to the satisfaction of a competent Supervisory Authority;

d) established procedures which allow them to assess the eligibility of the CISP's concerned to apply the Code, to monitor the CISP's compliance with the Code's provisions and to periodically review the CISP's operations. A Monitoring Body may show such procedures by demonstrating: (i) existing procedures for certifying against relevant industry standards such as ISO/IEC 27001, 27017 and 27018 or other equivalents; or (ii) other equivalent auditing experience in information security or privacy;

e) established procedures and structures to handle complaints in relation to

infringements of the Code or the manner in which the Code has been, or is being, implemented by a CISP as described below;

f) procedures and structures referred to in section e) above and make these procedures and structures transparent and available to data subjects and the public; and

g) to the satisfaction of a competent Supervisory Authority, that its tasks and duties do not result in any conflicts of interest.

For the avoidance of doubt, Monitoring Body eligibility is determined by the Designated Supervisory Authority's accreditation process. The above criteria are intended to indicate the independence, experience and qualifications expected of Monitoring Bodies by CISPE itself. However, in event of any inconsistency between the above criteria and the CNIL's accreditation criteria for Monitoring Bodies, the CNIL's accreditation criteria shall prevail.

The list of Monitoring Bodies shall be published and maintained on the CISPE Public Register. Organizations may only be included in the CISPE Public Register following accreditation by a designated Supervisory Authority.

The CISC shall liaise with and support Monitoring Bodies in ensuring consistent application of the Code by each Monitoring Body. It shall organise and facilitate annual workshops to be attended by Monitoring Bodies to discuss each Monitoring Body's Annual Auditing Report (see Section 7.2(c)), including any practical issues Monitoring Bodies have encountered in assessing the application of the Code (the "**Monitoring Body Workshops**"). Following each Monitoring Body Workshop, the CISC shall share the outcomes of the workshops, including agreed best practice, and examples of enforcement decisions by Monitoring Bodies, including any potential conflicts and the resolutions identified. These guidance documents shall be shared with new and existing Monitoring Bodies to facilitate consistent application of the Code.

The CISC will also issue guidance where needed by Monitoring Bodies, either pro-actively, or in response to a request from a Monitoring Body. Such guidance is not intended to be binding on the Monitoring Body, but is intended to support the Monitoring Body in its application of the Code and maintain consistency between Monitoring Body approaches.

The CISC shall be composed of 3 external independent experts drawn from academia, technical or legal backgrounds (the **CISC Members**). The CISC Members should be experienced in engaging with Supervisory Authorities, businesses, and data subjects. CISC Members shall be appointed by the CISPE Executive Board for fixed terms of three years. CISC Members must not have any existing consulting arrangements with a CISP, and may not be members of the CISPE Executive Board. The Executive Board will keep under review the expertise and performance of the CISC Members and replace them if they no longer meet the above requirements.

Each CISC Member shall be under an obligation to avoid a situation in which they have, or could have, a direct or indirect interest that conflicts, or possibly may conflict, with the interests of the Code. If a CISC Member, or the Executive Board, becomes aware of such a conflict of interest, the CISC Member must recuse themselves from the CISC, and the Executive Board shall appoint a replacement. If the Executive Board is aware of such a conflict, the Executive Board shall request that the CISC Member recuse themselves. If the CISC Member fails to recuse themselves, the Executive Board shall revoke such CISC membership. Any member of CISPE may notify the Executive Board of a suspected conflict of interest on the part of a CISC Member at any time.

The CISPE General Secretary shall carry out a general observer role in respect of the

business of the CISC and support administrative tasks in the conduct of the business of the CISC and the Monitoring Bodies in respect of the Code.

Monitoring Bodies, proactive monitoring

Article 40(4) of the GDPR states that a body which meets the criteria of Article 41(1) of the GDPR, is required to carry out mandatory monitoring of compliance with the Code's provisions by CISPs that undertake to apply it and adhere to it.

Each CISP that undertakes to apply the Code is subject to monitoring by its chosen Monitoring Body in order to verify that the CISP has complied with the Code's provisions. The Monitoring Body shall be selected by the CISP from the list maintained by the CISC. The CISP shall be free to choose any Monitoring Body from the list maintained by the CISC. It is at the Monitoring Body's discretion whether it agrees to act as the Monitoring Body for a relevant CISP. The CISP shall pay its Monitoring Body for all activities it performs in monitoring that CISP's compliance with the Code, and in dealing with complaints against that CISP. Each Monitoring Body shall be accredited by the CNIL, and payment from the CISP to the Monitoring Body shall not impede the independence and the effectiveness of the Monitoring Body. In the case where a CISP is not able to appoint a Monitoring Body as result of a refusal from that latter based on objective criteria, the CISC will organize a mediation between the CISP and the Monitoring Body so that they can find a solution to solve their potential issues. If such mediation fails, the CISC will use ask another Monitoring Body from the list maintained by the CISC to assist the CISP or will use its reasonable effort to add other Monitoring Bodies to the list that could become the Monitoring Body for the CISP. If at the end of this process, no Monitoring Body accepts the mission to become the Monitoring Body for the CISP, the CISC will seek advice from the Competent Supervisory Authority.

The Monitoring Body shall assess each of its monitored CISPs' compliance with the provisions of the Code. Such assessment should be performed by a team of professionals who (collectively) are able to demonstrate technical and legal competency.

Technical expertise would, without limitation, be demonstrated by the following:

- a minimum of three years' experience in the field of information security including relevant information security certifications (e.g. ISO/IEC 27001 Lead Auditor, ISACA Certified Information Systems Auditor (CISA), ISACA Certified Information Security Manager (CISM)); or
- education in the field of information security plus a minimum of one year experience in information security.

Legal expertise would, without limitation, be demonstrated by the following:

- a minimum of two years' demonstrated experience in the field of data protection and privacy and possession of relevant certifications (e.g. IAPP CIPP/E), or
- legal educational background accompanied with a relevant data protection certification (e.g. CIPP/E).

The assessment of Code compliance can be divided into two aspects: assessment of technical and organisational security measures; and assessment of the other data protection and transparency Code requirements:

1. **Assessment of technical and organisational security measures:** Annex A

(Security Responsibilities) sets out the security responsibilities which must be adopted by CISPs. If appropriate measures are adopted by the CISP to meet these responsibilities and can be assessed positively against ISO/IEC 27001/27018 (or an equivalent recognised industry standard), this will demonstrate adequate implementation of the technical and organisational security responsibilities required by the Code. For CISPs which are not ISO/IEC 27001/ ISO/IEC 27018 certified, assessment will be made against the Code requirements set out in Annex B in accordance with a defined assessment methodology developed by the Monitoring Body.

2. Assessment of other data protection and transparency Code requirements: The Code sets out data protection and transparency requirements for CISPs under Section 4 and 5.

The method for assessment of (i) the data protection and transparency requirements of the Code and (ii) technical and organizational security measures of Annex A will be based on the control framework in Annex B of the Code, which utilises similar assessment methodologies to ISO/IEC 27001 / ISO/IEC 27018, or equivalent recognised industry standards.

As set out in Section 6, the Monitoring Body's initial assessment of Code compliance will take place prior to submission of the CISP's Declaration of Adherence, or within one year of submission, depending on the CISP's chosen process of adherence. Thereafter, the Monitoring Body shall verify each CISP's compliance with the provisions of the Code on an annual basis. Following each assessment, the Monitoring Body shall generate a report summarising its findings in relation to the CISP's compliance ("**Report**") and shall provide the Report to the CISP and CISPE. If the Report verifies the CISP's compliance with the provisions of the Code, CISPE shall confirm the CISP's Declaration of Adherence under section 6.

If the Report does not verify the CISP's compliance with the Code, the Monitoring Body shall follow the Enforcement Matrix set out in sub-section 7.2(b) below to determine the appropriate sanction.

Any decision taken by a Monitoring Body shall be documented. This will include the decision itself, the circumstances in which it was made and a statement of reasons why, including any matters of interpretation of the Code. Monitoring Bodies may request support from the CISC at any time in respect of matters of interpretation of the Code.

CISPs shall cooperate with their Monitoring Body with respect to providing information to the Monitoring Body which is reasonably required for the Monitoring Body to fulfil its duties under the Code.

Complaints Process

Any complaints from any customer, data subject, or any other CISP about the compliance of services covered by a CISP's Declaration of Adherence with the Code Requirements will be addressed as follows:

(a) Complaints shall initially be submitted to both the Monitoring Body and to CISPE for administrative ease. If the complaint is only addressed to CISPE, CISPE shall then transmit the complaint to the relevant Monitoring Body for review: CISPE will not exercise any discretion or instruction in the selection of complaints to pass to a Monitoring Body. If the complaint is only addressed to the Monitoring Body, the Monitoring Body shall share a copy of the complaint with CISPE for tracking purposes;

(b) The Monitoring Body will investigate the specific services and/or measures which are alleged to be non-compliant by the complaint in accordance with its own investigation processes and make a determination;

(c) The Monitoring Body shall provide the Executive Board with its determination on the complaint, including details of any enforcement action to be taken against a non-compliant CISP;

(d) Enforcement action shall be taken in accordance with the Enforcement Matrix in sub-section (b) below.

The CISPE Executive Board shall provide the CISC with a copy of all complaints received and complaints reports provided by Monitoring Bodies, but the CISC shall not have any role in the determination of individual complaints. The CISC shall review the functioning of the Complaints Process and provide a yearly report to the CISPE Executive Board on complaints received and how they were dealt with. The report shall detail for example, statistics on the number of complaints submitted and any key themes emerging about the types of complaints which have been filed. The CISC shall also provide administrative support to the Monitoring Bodies in ensuring a consistent application of the Code by each Monitoring Body in accordance with sub-section (c) below, and in accordance with the following principles in respect of any specific complaint:

- The Monitoring Body may ask for general guidance in respect of any matter of interpretation of the Code if necessary to deal with a complaint, without reference to the specific facts of that complaint
- The CISC shall be entitled to provide the Monitoring Body with general information on the handling of equivalent matters in the context of other reviews or complaints handing by Monitoring Bodies; if necessary because no equivalent matter exists, the CISC may a general, non-binding view, without reference to the specific facts of the complaint
- It shall be the Monitoring Body's right alone to determine each individual complaint.

(b) Enforcement

If, in preparing its determination in response to a complaint, or in its preparation of an annual Report on a relevant CISP, the Monitoring Body requires additional documentation or clarification, it may request such additional information from the CISP. The CISP must respond to a request for such additional information within the reasonable timeframe specified by the Monitoring Body in its request.

If in its determination in response to a complaint, or in an annual Report on a relevant CISP, the Monitoring Body finds that a CISP is non-compliant with the Code Requirements, then the Monitoring Body shall follow the Enforcement Matrix below to determine the appropriate sanction:

Enforcement Matrix:

Step	Situation	Sanction
1. First Written Warning	Monitoring Body makes	The Monitoring Body shall provide a written warning (by post or in electronic form) with proof of receipt, to

	an assessment that the CISP is not compliant with any requirement under the Code.	the CISP, setting out: • the area of non-compliance and details of the Monitoring Body's findings in that regard; • remediating measures to be taken by the CISP; and • that the remediating measures must be taken within 60 days of receipt of the written warning or a finding of non-compliance will be published, (the "**First Written Warning**"). Within 60 days of the CISP's receipt of the First Written Warning, the CISP shall: (i) submit itself to re-assessment by the Monitoring Body to determine the CISP's compliance with the relevant requirement; or (ii) make a written submission to the Monitoring Body with further evidence, or submissions in reply, which, if taken into account would demonstrate its compliance. If, following re-assessment: a) the Monitoring Body finds that the CISP has remedied its non-compliance, or concludes based on such other representations that the CISP is compliant, the matter will be closed. b) the Monitoring Body finds that the CISP is still not Code compliant, the Monitoring Body shall take the action set out in Step 2.
2. Second Written Warning and publication of non-compliance	Monitoring Body makes an assessment that the CISP is not compliant with the requirements of the Code within 60 days following its receipt of the First Written Warning.	The Monitoring Body shall provide a second written warning (by post or in electronic form) with proof of receipt, to the CISP, setting out: • the area which remains non-compliant with the Code and details of how any remediating measures to date have not been adequate; • remediating measures to be taken by the CISP, • that a finding of non-compliance will be published; and • that remediating measures must be taken within 30 days of receipt of the second written warning or the CISP's Declaration of Adherence will be suspended, (the "**Second Written Warning**").

		Following delivery of the Second Written Warning, the Monitoring Body shall provide to the CISPE Executive Board, a written statement explaining that the CISP has been found to be non-compliant with the Code and that it has 30 days to remedy such non-compliance. CISPE shall publish this statement on the CISPE website. Within 30 days of the CISP's receipt of the Second Written Warning, the CISP shall submit itself to re-assessment by the Monitoring Body to determine the CISP's compliance with the relevant requirement. If, following re-assessment: a) the Monitoring Body finds that the CISP has remedied its non-compliance, the matter will be closed and a notice of the closure shall be published on the CISPE website. b) the Monitoring Body finds that the CISP is still not Code compliant, the Monitoring Body shall take the action set out in Step 3.
3. Suspension of a CISP's Declaration of Adherence	Monitoring Body makes an assessment that the CISP is not compliant with the requirements of the Code within 30 days following its receipt of the Second Written Warning.	The Monitoring Body shall inform the CISPE Executive Board in writing that the CISP's Declaration of Adherence be suspended. Such suspension shall continue in effect until the CISP can demonstrate to the Monitoring Body that it has remedied the relevant non-compliance.
4. Exclusion of a CISP service from the Code	For severe or persistent Code breaches, the Monitoring Body may decide to exclude a CISP service from the Code.	The Monitoring Body shall inform the CISPE Executive Board in writing that the CISP service has been excluded from the Code. The CISP's Declaration of Adherence and supporting documents shall expire immediately.

In each case, the Monitoring Body shall communicate the relevant sanction to the CISP via

the provision of a written report.

Where the CISP's Declaration of Adherence is to be suspended or the CISP service is to be excluded from the Code, the Monitoring Body shall inform the CISPE Executive Board in writing and the CISPE Executive Board must ensure the suspension or exclusion is implemented. The CISPE Executive Board will share such sanction notices with the CISC.

If a CISP's Declaration of Adherence is suspended or a CISP service is excluded from the Code:

- the Secretariat shall promptly remove the affected service(s) from the CISP's Declaration of Adherence on the CISPE Public Register and inform the Designated Supervisory Authority for the Code of such suspension or exclusion;
- the Monitoring Body shall notify the CISP in writing that its Declaration of Adherence will be suspended, or the service will be excluded from the Code within 7 business days and the CISP must stop using the Compliance Mark in respect of the relevant service within 7 business days of receipt of such notice; and
- the CISP shall stop using the Compliance Mark in respect of the relevant service within 7 business days of receipt of notice from the Monitoring Body. CISPE is the owner of the Compliance Mark and any use of the Compliance Mark without permission will be considered trade mark infringement. CISPE will take active steps to enforce any such misuse of Compliance Mark.

In the case of suspension, these measures shall apply until such suspension is lifted. When a CISP's Declaration of Adherence is suspended, the CISP will effectively be excluded from the Code until such non-compliance has been remedied and verified by the Monitoring Body.

In the case of exclusion, the relevant Declaration of Adherence shall expire permanently. Following exclusion of a CISP service, a CISP may resubmit the service to the Code. In this case, a new application must be made via the adherence process set out in Section 6. The CISP must disclose the fact that the CISP service has previously been excluded from the Code when submitting its new Declaration of Adherence.

The enforcement measures above are:

- the sole and exclusive remedies for a CISP's non-compliance with the Code Requirements;
- without prejudice to the customer's rights under applicable EU data protection law or the Service Contract; and
- without prejudice to the CISP's right to contest the decision of the Monitoring Body by any means available as a matter of law.

The ability for a customer to make a complaint does not of itself give the customer any direct rights or remedies against the CISP or CISPE under or in connection with the Code. CISPE does not accept any responsibility for a CISP's compliance with the Code. Nor will CISPE be liable to any party under any cause of action or theory of liability for any loss or damages arising from an act or omission of CISPE or a CISP in connection with the Code.

Where the Monitoring Body issues a Second Written Warning, a CISP's Declaration of Adherence is suspended or a CISP service is excluded from the Code, the Monitoring Body shall report such cases to the CNIL, as the competent Supervisory Authority. Such reports shall include information on the CISPs non- compliance, the failure by the CISP to implement remediating measures requested by the Monitoring Body, and the action the

Monitoring Body has taken in response. Where, following the issuance of a Second Written Warning, the Monitoring Body finds that the CISP has remedied its non-compliance, the Monitoring Body shall notify the CNIL of the closure of the matter.

(c) Monitoring reports

To facilitate the development of the Code and its effective assessment, the Monitoring Body shall submit an Annual Monitoring Report to the CISPE Executive Board and the CNIL as the Designated Supervisory Authority. The Annual Monitoring Report will detail the Monitoring Body's control and audit methodologies, statistics on the outcome of complaints which it has handled and reviews it has performed (including the number of first written warnings issued to CISPs), and any practical issues it has encountered in assessing application of the Code by its monitored CISPs (for example, issues with assessing how a CISP implements the requirements of Annex A).

Every three years (unless otherwise agreed between the CISC and the Monitoring Bodies), the CISC shall undertake a consistency analysis, assessing the Annual Monitoring Reports of each Monitoring Body to align best practice assessment and enforcement of Code requirements and shall make appropriate recommendations to the Monitoring Bodies to increase alignment.

7.3 Review of the Code

(a) Review of the Code

The CCTF will continue to review the Code based on changes to applicable EU data protection law and, in particular, the interpretation of the GDPR after its coming into force.

The CCTF shall aim to complete a full review of the Code every two years to take into account legal and technological developments as well as developments to industry best practice. For example, the CCTF shall consider relevant developments in best practices from cloud market-adopted certifications, such as ISO/IEC 27701, or other new standards.

The Executive Board may initiate a specific review of the Code by the CCTF by a joint request to the CCTF from at least two members of the Executive Board. The Executive Board may initiate such a review of their own initiative or because it has been requested to do so by:

- at least 10% of General Assembly members;
- a Monitoring Body;
- a competent Supervisory Authority acting in an official capacity; or
- an association representing the interests of cloud infrastructure service users acting in an official capacity.

Any suggestion for changes to the Code must be reviewed and considered expeditiously.

(b) Changes to the Code

After a review, the CCTF may recommend changes to the Code to the Executive Board. Changes to the Code must be adopted by CISPE before they take effect.

To be adopted by CISPE, any change to the Code must be:

- presented to the Executive Board and the General Assembly;

- approved by the Executive Board; and
- adopted by the General Assembly by a special resolution.

Before adoption by CISPE, the Executive Board shall submit any amendment or extension to the Code to the Designated Supervisory Authority for the Code, for approval. In addition, the Executive Board may also choose to submit a change to the Code for consideration and comment to an association representing the interests of cloud infrastructure service users.

As soon as practicable after a change to the Code has been adopted by CISPE, the Secretariat shall publish an updated version of the Code on the CISPE Public Register.

CISPs are required to renew or re-confirm their Declarations of Adherence within a year of the updated version of the Code being published on the CISPE Public Register. A CISP who shows that its service adheres to the Code Requirements by presenting an existing Monitoring Body approval and Compliance Checklist, together with its Declaration of Adherence may rely on the existing approval and Compliance Checklist to show that the service adheres to the updated version of the Code without having to undergo a new or separate audit to obtain a new approval or report, provided the existing approval and Compliance Checklist demonstrates compliance with the requirements of the updated Code.

Annex A – Technical and organizational security practices and security responsibilities

Introduction

This Annex defines a minimum set of technical and organisational security practices and the security responsibilities that the CISP shall take into account to define and adopt a set of measures to secure personal data against unauthorised processing and accidental or unlawful loss, access or disclosure. CISP services which are declared adherent to the Code must comply with these practices and responsibilities, document the measures taken and will be subject to the assessment of the Monitoring Body. Specific examples of the measures the CISP may take to comply with its security responsibilities are included in the tables at the end of each sub-section. These examples are illustrative only rather than prescriptive or mandatory. The specific measures, technologies and controls a CISP implements to adhere to its security responsibilities will be dependent on the size and complexity of each CISP, and such security measures are likely to be adjusted over time to keep pace with technological developments, however CISP adhering to this Code of Conduct are encouraged to take ISO/IEC 27002 as a guidance document for implementing commonly accepted information security controls. CISPs who demonstrate compliance with the relevant requirements under ISO/IEC 27001 / ISO/IEC 27018 / ISO/IEC 27017, or an equivalent recognised industry standard, will be deemed to meet the requirements of this Annex A. The Code recognises that new recognised industry standards will become relevant from time to time, taking into account developments in the market, and the Code will be reviewed to provide further guidance on relevant security standards to be taken into account from time to time. Examples of the ISO controls which would meet the relevant requirement under this Annex A are set out below.

(1) Information Security Management

(a) CISP responsibilities

The CISP shall have clear management-level direction and support for the security of the service.

The CISP shall have in place a management-approved set of information security policies that govern the security of the service.

The CISP shall implement an information security management system or equivalent. The scope of the information security management system shall cover the service.

The CISP shall designate one or more personnel to coordinate and be accountable for the information security management system.

(b) Customer responsibilities

The customer should designate a customer point of contact for security issues in respect of the customer's use of the cloud infrastructure service.

The customer should perform a risk assessment to assess the suitability of the cloud infrastructure service for the data processing activities that the customer wishes to perform based on applicable EU data protection law.

(c) Examples of measures which may be taken by the CISP

The following table lists examples of measures which may be taken by the CISP to address

its security responsibilities in relation to information security management:

Examples:
• Ensuring information security policies and procedures cover, at a minimum: (a) the scope and boundaries of the information security program, including business, organisation, locations, assets and technology; (b) usage policies defining appropriate usage for critical technologies such as mobile devices, wireless technologies, e-mail and internet usage; and (c) roles and responsibilities to manage and implement the information security policies. • Ensuring the CISP's security policy framework covers, at a minimum, the following areas: (a) asset management; (b) human resources; (c) access controls; (d) physical and environmental security; (e) system development lifecycle; (f) incident management; (g) business continuity; (h) compliance; and (i) mobile device usage. • Communicating information security policies to all CISP personnel (including vendors and business partners), including regular updates. • Developing operational procedures to provide guidance for the operation of systems and services within the CISP environment, where necessary.

(d) Corresponding ISO requirements

CISPs adhering to the Code are encouraged to take into consideration the ISO controls listed below when implementing their security measures. A CISP who has verified compliance against these standards can use this verification to demonstrate compliance with the requirement of this sub-section (1) of Annex A.

Relevant ISO controls:

- ISO/IEC 27001: A.5
- ISO/IEC 27017: 5
- ISO/IEC 27018: 5

(2) Human Resource Security

(a) CISP responsibilities

The CISP shall have in place an organisational structure to manage the implementation of information security within the CISP's services with clearly defined roles and responsibilities.

The CISP shall establish an information security organisation managed by the CISP's security team and led by the CISP's Chief Information Security Officer (CISO) or equivalent. The CISP's security organisation shall establish and maintain formal policies and

procedures to delineate standards for logical access on the CISP's system and infrastructure hosts. The policies also identify functional responsibilities for the administration of logical access and security. The CISP shall be responsible for training its employees and contractors on these policies and procedures.

Procedures shall exist so that the CISP's employee and contractor user accounts are added, modified, or disabled in a timely manner and are reviewed on a regular basis. In addition, password complexity settings for user authentication to CISP systems are managed in compliance with the CISP's corporate password policy which has to be aligned with state-of-the-art password standard such as minimum complexity, length, password history, lock out in the event of multiple authentication failure or multi-factor authentication.

Requests for changes in access shall be captured in a permissions management tool audit log or equivalent. The CISP shall employ the concept of least privilege, allowing only the necessary access for users to accomplish their job function. User accounts are created to have minimal access. Access above these least privileges requires appropriate authorisation.

(b) Customer responsibilities

The customer is solely responsible for its personnel and for any third party who accesses or uses the cloud infrastructure services provided to the customer (including without limitation contractors, agents or end users), and for training its personnel or third parties which access or use the cloud infrastructure services.

(c) Examples of measures which may be taken by the CISP

The following table lists examples of measures which may be taken by the CISP to address its security responsibilities in relation to human resource security:

Examples:
• Ensuring the board of directors of the CISP receives updates as to incidents, threats and status of security improvement deliverables. • Implementing a security awareness program for CISP personnel to ensure they understand the necessary behaviours and skills to help ensure the security of the CISP. • Updating the CISP's security awareness program to address new technologies, threats, standards, privacy & data protection, and business requirements. • Providing role-based security training based on assigned responsibilities to CISP and customer personnel before authorising access to CISP systems or performing assigned duties. • Tracking completion of security training activities by CISP personnel for compliance with training requirements as set out by the Code and GDPR. • Ensuring CISP and customer personnel acknowledge that they have read and understood the CISP information security policy and

procedures.

- Ensuring that all users with administrative account access use a dedicated or secondary account for elevated activities, with specific security measures (e.g: password complexity, multi-factor authentication; traceability of relevant events, etc.). This account should only be used for administrative activities and not internet browsing, email, or similar activities.

- Limiting CISP personnel access, so CISP personnel are only able to access information related to the structural elements of the cloud infrastructure, its configurations and the configuration of logical environments assigned to customers. Having controls in place so CISP personnel do not have access to customer information and application data, unless there is an explicit customer request for assistance, maintenance or updates.

- Implementing controls so CISP personnel cannot keep infrastructure sessions open during their absence.

- Having in place policies where CISP personnel cannot keep the credentials needed to access CISP physical infrastructure in writing, with the exception of a superuser password, known by the system administrator and kept by the operational manager.

(d) Corresponding ISO requirements

CISPs adhering to the Code are encouraged to take into consideration the ISO controls listed below when implementing their security measures. A CISP who has verified compliance against these standards can use this verification to demonstrate compliance with the requirement of this sub-section (2) of Annex A.

Relevant ISO controls:

- ISO/IEC 27001: A.6.1, A.7.2
- ISO/IEC 27017: 6.1, 7.2
- ISO/IEC 27018: 6.1, 7.2

(3) User Access Management

(a) CISP responsibilities

The CISP shall provide the customer with an access control management system for customer user access to the cloud infrastructure service as part of the service. The access control management system shall include, for example, individual accounts (which could be a user or service account), role based access and passwords or other authentication policy means. The CISP shall explain to customer how the access control management system works so that the customer can use and configure it as set out below.

The CISP is not responsible for access solutions for the systems and applications deployed by the customer using the cloud infrastructure service.

(b) Customer responsibilities

The customer is solely responsible for the use and configuration of the access control management systems provided by the CISP. The customer is responsible for assigning access rights to the appropriate personnel.

The customer is responsible for access solutions to the systems and applications deployed by the customer using the cloud infrastructure service.

(c) Examples of measures which may be taken by the CISP

The following table lists examples of measures which may be taken by the CISP to address its security responsibilities in relation to user access management:

Examples:
• Actively managing the life cycle of accounts, including the creation, use and deletion of accounts, in order to minimise opportunities for attackers to leverage them. • Disabling dormant CISP user accounts after a set period of inactivity. • Ensuring CISP user sessions automatically lock after a standard period of inactivity. • Actively managing access management systems by implementing role and profile. • Providing administrative access to customers for logical environment configuration with secure and encrypted connections on explicit customer request.

(d) Corresponding ISO requirements

C CISPs adhering to the Code are encouraged to take into consideration the ISO controls listed below when implementing their security measures. A CISP who has verified compliance against these standards can use this verification to demonstrate compliance with the requirement of this sub-section (3) of Annex A.

Relevant ISO controls:

- ISO/IEC 27001: A.9
- ISO/IEC 27017: 9
- ISO/IEC 27018: 9

(4) Physical and environmental security

(a) CISP responsibilities

The CISP shall implement and maintain state-of-the-art physical and environmental security measures for the cloud infrastructure service designed (i) to help customers secure personal data against unauthorised processing and accidental or unlawful loss, access or disclosure and (ii) to prevent reasonable environmental threats such as fire and water damages.

(b) Customer responsibilities

Customer does not have an active role in maintaining physical and environmental security for the cloud infrastructure service. Customers should however review (a) the information made available by the CISP relating to physical and environmental security in respect of the service, (b) the customer's chosen configuration of the service and use of the features and controls available in connection with the cloud infrastructure service, and (c) the security measures that customer will put in place for the aspects of security under its responsibility, and make an independent determination that together those measures provide an appropriate level of security for the processing customer will use the services to perform.

(c) Examples of measures which may be taken by the CISP

The following table lists examples of measures which may be taken by the CISP to address its security responsibilities in relation to physical and environment security:

Examples:
• Zoning of hosting areas based on criticality. Implementing and controlling such zoning with walls, fences, doors and mantraps under access controls, video-monitoring and guarding. • Using physically or logically segregated systems to isolate and run software that incurs higher risk for the customer. • Managing access to datacenters and cages by a visual authentication or badge system and restricting permanent access to CISP facilities and secure areas to authorised and approved personnel. • Having a system in place whereby visitor (i.e., any persons without a persistent need for access) access requests to CISP facilities and secure areas must be submitted and documented using an approved CISP mechanism, and will only be approved by authorised CISP personnel. • Verifying the identify of any visitors to CISP facilities and secure areas by means of a government issued photo ID (e.g., driver's license, passport, etc.) or a CISP corporate picture ID.

(d) Corresponding ISO requirements

CISPs adhering to the Code are encouraged to take into consideration the ISO controls listed below when implementing their security measures. A CISP who has verified compliance against these standards can use this verification to demonstrate compliance with the

requirement of this sub-section (4) of Annex A.

Relevant ISO controls:

- ISO/IEC 27001: A.11.1, A.11.4.1, A.13.1
- ISO/IEC 27017: 11.1, 13.1
- ISO/IEC 27018: 11.1, 13.1

(5) Physical servers and equipment, including firewalls

(a) CISP responsibilities

The CISP is solely responsible for the deployment, operation and security of any physical hardware, *host* operating system, and virtualisation layer, used to provide the cloud infrastructure service, including any configuration needed for the provision of the service.

The CISP shall make available a mechanism to filter data flows such as a firewall around the perimeter of the cloud infrastructure as a whole and/or a firewall around the service instance which is deployed. Where there is a filter mechanism (such as a firewall) to protect the CISP entire global infrastructure, the CISP will be responsible for configuring this mechanism.

(b) Customer responsibilities

The customer is solely responsible for managing the appropriate configuration of any system and application deployed by the customer on the cloud infrastructure service, including any *guest* operating system, and is solely responsible for the security of data in transit. Whether a firewall will be available for each service instance will be service-dependent. Some services may not have instance-specific firewalls, in which case the customer will be responsible for applying its own instance-specific firewall.

(c) Examples of measures which may be taken by the CISP

The following table lists examples of security measures which may be taken by the CISP to address its security responsibilities in relation to physical servers and equipment:

Examples:
• Implementing a configuration management database covering all physical servers and equipment and managing the lifecycle of such assets. • Implementing security controls to ensure the security of the supply chain and that operations are trackable. • Installing and configuring data plane filtering on wired and wireless environments to protect the CISP network from external networks such as the internet. For example using a network based firewall. • Ensuring data plane policies, for example, firewall rules, adhere to approved configurations. For example, (a) unnecessary ports, protocols, and services must be restricted on network devices; (b) devices should be configured for HA (High

Availability) mode; and (c) data plane policies (e.g., firewall device configurations) must have “extended ip deny” for the access-list border-net, which denies anything not specifically approved in the access control lists.

- Ensuring changes to data plane policies are approved by CISP management and tested prior to implementation.
- Ensuring firewall configurations and access control lists ("ACL") are managed by a network engineer in accordance with approved rule sets. For example: (a) the ACL management tool must be used to deploy approved ACLs to firewalls on the production network; and (b) if a firewall or network device cannot be reached by the ACL management tool, this must be reviewed and remediated.
- Ensuring firewall rule sets are reviewed and approved by the information security team.
- Pushing data plane polices to network devices based on platform, location and network.

(d) Corresponding ISO requirements

CISPs adhering to the Code are encouraged to take into consideration the ISO controls listed below when implementing their security measures. A CISP who has verified compliance against these standards can use this verification to demonstrate compliance with the requirement of this sub-section (5) of Annex A.

Relevant ISO controls:

- ISO/IEC 27001: A.8.1, A.13.1, A.15.1
- ISO/IEC 27017: 8.1, 13.1, 15.1
- ISO/IEC 27018: 8.1, 13.1, 15.1

(6) Malware protection management

(a) CISP responsibilities

The CISP shall implement malware protection on sensitive systems (i.e. commonly affected or targeted systems) that are part of the cloud infrastructure service.

(b) Customer responsibilities

The Customer is responsible for malware protection management on the systems and applications deployed by the customer using the cloud infrastructure service.

(c) Examples of measures which may be taken by the CISP

The following table lists examples of measures which may be taken by the CISP in relation to malware protection management on sensitive systems that are part of the cloud infrastructure service:

Examples:
• Installing anti-virus protection on servers on the network and workstations. • Configuring anti-virus protection to: (a) scan electronic mail, electronic mail attachments, web accesses, and removable media; (b) perform critical system file scans during system boots; and (c) block and quarantine malicious code and send alerts to the CISP security administrator. • Configuring systems to automatically update anti-virus software. • Ensuring all software installed on a platform is system software downloaded from authenticated sources.

(d) Corresponding ISO requirements

CISPs adhering to the Code are encouraged to take into consideration the ISO controls listed below when implementing their security measures. A CISP who has verified compliance against these standards can use this verification to demonstrate compliance with the requirement of this sub-section (6) of Annex A.

Relevant ISO controls:

- ISO/IEC 27001: A.12.2, A.12.5, A.12.6
- ISO/IEC 27017: 12.2, 12.5, 12.6
- ISO/IEC 27018: 12.2, 12.5, 12.6

(7) Vulnerability management

(a) CISP responsibilities

The CISP shall define the level of engagement (distribution of tasks between CISP and customer, delay between patch and patching, etc.) for the cloud infrastructure service. The CISP shall, unless it specifically notifies the customer otherwise in the Service Contract, be responsible for patching within hardware, networking between hardware, virtualisation layer and *host* operating systems.

(b) Customer responsibilities

The Customer is responsible for vulnerability management of the systems and applications deployed by the customer and hosted on the cloud infrastructure service, including *guest* operating systems.

(c) Examples of measures which may be taken by the CISP

The following table lists examples of measures which may be taken by the CISP to address its security responsibilities in relation to vulnerability management:

Examples:
• Subscribing to a vulnerability watch service and mapping any vulnerability to the CISP configuration management database. Assessing any applicable vulnerability in the context of the vulnerable asset to prioritise patching activities. • Ensuring that host operating systems are running the most recent security updates provided by the software vendor. • Conducting penetration tests to identify vulnerabilities and attack vectors that could be used to exploit enterprise systems.

(d) Corresponding ISO requirements

CISPs adhering to the Code are encouraged to take into consideration the ISO controls listed below when implementing their security measures. A CISP who has verified compliance against these standards can use this verification to demonstrate compliance with the requirement of this sub-section (7) of Annex A.

Relevant ISO controls:

- ISO/IEC 27001: A.6.1.4, A.12.6, A.14.2
- ISO/IEC 27017: 6.4, 14.2
- ISO/IEC 27018: 6.4, 14.2

(8) Logging and Monitoring

(a) CISP responsibilities

The CISP shall provide the customer with monitoring (e.g. level, scope, reporting, interfaces, API) and logging (e.g. access, records, duration of recording) tools and/or reports on request for the cloud infrastructure service.

(b) Customer responsibilities

The customer is solely responsible for the logging and monitoring systems and tools deployed by the customer on the cloud infrastructure service, including the use and configuration of the monitoring and logging tools provided by the CISP

(c) Examples of measures which may be taken by the CISP

The following table lists examples of measures which may be taken by the CISP to address its security responsibilities in relation to logging and monitoring:

Examples:
• Defining a list of system events that should be logged to include the following: (a) successful and unsuccessful authentication and authorisation attempts; (b) account management events; (c) privileged functions; (d) system start-up and shutdown; (e)

data deletions, data access, and data changes; and (f) unsuccessful events (for example, calls not authorised).

- Implementing logs on systems to record the following information, at a minimum, for each system event (including user events, system events and security events): (a) user identification (including service, caller and user); (b) type of event or API called; (c) date and time zone; (d) source of system event; (e) outcome of system event; and (f) identity of affected system component or resource.

- Collecting logs from all systems, devices and network components to a centralised logging service which allocates audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded and retains audit records for a defined period of time.

- Aggregating, correlating, reviewing and analysing logs to identify anomalies and other potentially malicious events.

- Monitoring systems and facilities for potential security events, and configuring such systems and facilities to automatically generate alerts notifying appropriate personnel.

- Protecting logs from unauthorised access. For example, by restricting log access to authorised CISP personnel and implementing tamper resistant/evident or change detection software to detect tampering of log information.

(d) Corresponding ISO requirements

CISPs adhering to the Code are encouraged to take into consideration the ISO controls listed below when implementing their security measures. A CISP who has verified compliance against these standards can use this verification to demonstrate compliance with the requirement of this sub-section (8) of Annex A.

Relevant ISO controls:

- ISO/IEC 27001: A.12.4
- ISO/IEC 27017: 12.4
- ISO/IEC 27018: 12.4

(9) Equipment end-of life

(a) CISP responsibilities

The CISP shall conduct a storage media decommissioning process prior to final disposal of storage media used to store Customer Data when such media has reached the end of its useful life, to prevent Customer Data from being exposed to unauthorised individuals. The decommissioning process will be conducted in accordance with industry standard practices (such as described in ISO/IEC 27002; or NIST 800-88) designed to ensure that Customer Data cannot be retrieved from the applicable type of storage media by any data or information retrieval tools or similar means.

(b) Customer responsibilities

Customer does not have an active role in decommissioning end of life storage media used by the CISP. Customers should however review (a) the information made available by the CISP relating to storage media decommissioning, (b) the customer's chosen configuration of the service and use of the features and controls available in connection with the cloud infrastructure service, and (c) the security measures that customer will put in place for the aspects of security under its responsibility, and make an independent determination that together those measures provide an appropriate level of security for the processing customer will use the services to perform.

(c) Examples of measures which may be taken by the CISP

The following table lists examples of measures which may be taken by the CISP to address its security responsibilities in relation to equipment end-of life:

Examples:
• Using the techniques detailed in e.g. DoD 5220.22-M ("National Industrial Security Program Operating Manual ") or e.g. NIST 800-88 ("Guidelines for Media Sanitization") to destroy data as part of the decommissioning process. • Degaussing and physically destroying all decommissioned magnetic storage devices in accordance with industry standard practices. • Protecting media from unauthorised disclosure or misuse until the media is destroyed. • Tracking all media handling and custody. • Ensuring storage media used in one host or system is never reused in another host or system. • Storing all media in a secure, locked/tamper-proof, bin immediately after their removal from source devices. The bin should reside within the cage or pod where the relevant hard drives were removed. • Ensuring media is not taken off-site without prior authorisation and that any media removed from CISP premises is not left unattended in public places. • Protecting media during transportation beyond CISP physical boundaries and ensuring activities associated with the transport of media are restricted to authorised personnel, who are monitored and documented.

(d) Corresponding ISO requirements

CISPs adhering to the Code are encouraged to take into consideration the ISO controls listed below when implementing their security measures. A CISP who has verified

compliance against these standards can use this verification to demonstrate compliance with the requirement of this sub-section (9) of Annex A.

Relevant ISO controls:

- ISO/IEC 27001: A.8, A.11.2.5, A.11.2.6, A.11.2.7
- ISO/IEC 27017: 8, 11.2.5, 11.2.6, 11.2.7
- ISO/IEC 27018: 8, 11.2.5, 11.2.6, 11.2.7

Annex B – Compliance Checklist

This Compliance Checklist sets out the requirements that a CISP shall meet in order to comply with the Code. It also provides suggested guidance to CISPs on how compliance with the Code Requirements can be achieved and technical and organisational security practices of Annex A can be implemented. For clarity, the CISP's obligation is to comply with the Code Requirements: the columns below setting out expected controls to be applied, and questions for the CISP, are to provide examples for how a CISP could comply and how their compliance could be assessed, but do not replace or change the relevant Code Requirement.

The Compliance Checklist is also intended to ensure a consistent verification approach for all Monitoring Bodies by providing them with (i) the requirements with which compliance with the Code will have to be verified and (ii) the questions/materials or equivalent that should be used to perform an assessment of Code compliance. The Compliance Checklist is not intended to replace or alter the Service Contract between a CISP and a customer.

CISP COC Control Framework						GDPR articles		
	Section of the CISPE Code	**Code Requirements** **(To be implemented by the CISP and verified by the Monitoring Body)**	**Expected controls to achieve the Code Requirements** **(Control title & control description aligned with the Code Requirements)**	**Sample Questions to be answered by the CISP** **(included in the CISPE and Privacy readiness check)**	**Evidence (or equivalent) to verify compliance with the Code requirements (to be documented by the CISP – to be verified by the Monitoring Body onsite or offsite depending on the relevance for the control at stake)**	**Article #**	**Name**	**Comments on the mapping (where partially covered by ISO27001)**
1	Section 3 Scope	- In respect of personal data processed on behalf of a customer using the cloud infrastructure service (**Customer Data**), the CISP must not (a) access or use such data except as necessary to provide and maintain the services to the customer, or (b) process such data for the CISP's own purposes, including, e.g., for the purposes of data mining, profiling or direct marketing.	In respect of personal data processed on behalf of a customer using the cloud infrastructure service (**Customer Data**), the CISP must not (a) access or use such data except as necessary to provide the services to the customer or (b) process such data for the CISP's own purposes, including, e.g., for the purposes of data mining, profiling or direct marketing.		Service documentation, Privacy policies, Security policies and/or Service Contract describing the scope and use of Customer Data.			

CISP COC Control Framework						GDPR articles		
	Section of the CISPE Code	**Code Requirements** **(To be implemented by the CISP and verified by the Monitoring Body)**	**Expected controls to achieve the Code Requirements** **(Control title & control description aligned with the Code Requirements)**	**Sample Questions to be answered by the CISP** **(included in the CISPE and Privacy readiness check)**	**Evidence (or equivalent) to verify compliance with the Code requirements (to be documented by the CISP – to be verified by the Monitoring Body onsite or offsite depending on the relevance for the control at stake)**	**Article #**	**Name**	**Comments on the mapping (where partially covered by ISO27001)**
2	Section 4.1. Processing Personal Data Lawfully	- The CISP shall only process personal data in accordance with the customer's instructions. - CISPs must: (a) comply with the customer's instructions as provided for in the Service Contract and (b) provide information about the service in accordance with Section 5 (Transparency Requirements) of the Code.	4.1.1 CISP complies with customer instructions when processing personal data: CISP shall strictly comply with: (i) the customer's written specific instructions contained or referenced in the signed Service Contract or; (ii) generic instructions that are documented by the CISP in a predefined list of services (Named 'Service Catalog'), that the customer may use.	(i) Are all specific processing of Personal data documented as "instructions" in the current Service Contracts with each customer or in appendices? How does the CISP ensure that the personal data is processed for the customer in accordance with specific documented instructions? (ii) Are all non-specific processing of personal data of the customer done in accordance with the documented service catalog? Is the service catalog updated in a way to cover all non-specific personal data processing?	Documentation of the Instructions for specific Processing in Service Contracts or in appendices to Service Contracts. Documentation of the Service catalog and proof of their regular update.	28(3)(a)	Data Processing agreement	

CISP COC Control Framework						GDPR articles		
	Section of the CISPE Code	**Code Requirements** **(To be implemented by the CISP and verified by the Monitoring Body)**	**Expected controls to achieve the Code Requirements** **(Control title & control description aligned with the Code Requirements)**	**Sample Questions to be answered by the CISP** **(included in the CISPE and Privacy readiness check)**	**Evidence (or equivalent) to verify compliance with the Code requirements (to be documented by the CISP – to be verified by the Monitoring Body onsite or offsite depending on the relevance for the control at stake)**	**Article #**	**Name**	**Comments on the mapping (where partially covered by ISO27001)**
3	Section 4.2. Contractual terms and conditions of the CISP's services	- The CISP shall only process personal data in accordance with the customer's instructions. - A contract between the CISP and the Customer shall define the features of the service and how it is delivered and the respective rights and obligations of the CISP and the customer (the Service Contract) - The Service Contract must be in writing (including in electronic form). - The Service Contract must be legally binding between the CISP and the customer. - The Service Contract shall stipulate processor's obligations as provided by Article 28(3) GDPR and must contain, at a minimum, provisions which address those requirements which are stated as applying to the CISP under CISP Requirements under Sections 4.1, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8, 4.10, 4.11 and 5. - The CISP shall not process Customer Data without such a Service Contract in place.	4.2.1 Data processing is covered by service agreement. Any personal data processing made by the CISP must be covered by a formal written service contract signed with the customer. The Service Contracts must contain provisions which address CISP requirements (Processing Personal Data lawfully, Security, Transfer of personal data to third countries, sub-processing, Data subject requests, CISP personnel, Data breach, Deletion or return of personal data). 4.2.2. Processing is described in a Service Contract Service contracts should be drafted in a way that accommodates customer changing their use cases and the services they use. In any case, traces must be generated and archived, detailing which services are being used by the customer, and when.	Do the Service Agreements address the description of the processing of personal data performed using the cloud infrastructure Services on a generic basis? Is the customer able to change how and for what purpose they use that infrastructure for personal data processing whenever they wish? When specific purchases of services related to personal data processing are performed, are traces generated and archived? Are the traces detailed enough on the services purchased by the customer?	Signed Service Contract with the terms and conditions annexed to it. The Service Contract may be structured in any way, including: 1. A single contract; 2. A set of documents such as a basic services contract with relevant annexes (data processing agreements, SLAs..); OR 3. Standard online terms and conditions. Traces of any specific purchase of services performed by the customer.	28 (3)	Processor	

CISP COC Control Framework						GDPR articles		
	Section of the CISPE Code	**Code Requirements** **(To be implemented by the CISP and verified by the Monitoring Body)**	**Expected controls to achieve the Code Requirements** **(Control title & control description aligned with the Code Requirements)**	**Sample Questions to be answered by the CISP** **(included in the CISPE and Privacy readiness check)**	**Evidence (or equivalent) to verify compliance with the Code requirements (to be documented by the CISP – to be verified by the Monitoring Body onsite or offsite depending on the relevance for the control at stake)**	**Article #**	**Name**	**Comments on the mapping (where partially covered by ISO27001)**
	Section 4.3. Security	- The CISP shall implement and maintain appropriate technical and organisational measures for the CISP's data center facilities, servers, networking equipment and host software systems that are within the CISP's control and are used to provide the CISP's service. - Annex A of this Code (Security Responsibilities) sets out the minimum standards for security and contains the security responsibilities which must be adopted by the CISP in order for a service to adhere to the Code. -The technical and organisational measures implemented by the CISP must: (a) be designed to help customers secure personal data against unauthorised processing and accidental or unlawful loss, access or disclosure, and (b) address each of the security responsibilities of the CISP as set out in Annex A (Security Responsibilities). - CISPs should actively seek to ensure that the security measures they implement do not prevent customers from deploying their own best security practices. For example, customers must be free to securely encrypt their personal data.	4.3.1. Organisational and technical measures are Implemented. Technical and organisational measures for the CISP's data center facilities, servers, networking equipment and host software systems must: (a) be designed to help customer secure personal data against unauthorised processing and accidental or unlawful loss, access or disclosure, and (b) address the security responsibilities of the CISP as set out in Annex A (Security Responsibilities). Annex A defines the security responsibilities of a CISP and the customer in the context of cloud infra services. Annex A sets out a minimum standard for security responsibilities. 4.3.2. technical and organisational measures are maintained to ensure security Technical and organisational	What are the security measures (technical and organisational) put in place by the CISP in order to secure the unauthorised processing and accidental or unlawful loss, access or disclosure? Has the CISP implemented the types of security measures set out in Annex A? Is a documented information security program implemented by the CISP? Who is accountable? Are the security of the CISP and the CISP's information security programs regularly evaluated and reviewed?	Documentation of the security measures under the responsibilities of the CISP, including documentation of the security measures adopted to comply with Annex A. Documentation of the CISP information security program in place (with a description of identified risks and how risks are reduced), and related responsibilities. Materialisation of the review and the evaluation of the security of the CISP as well as the CISP's information security program.	32 (1)	Security of processing	

CISP COC Control Framework						GDPR articles		
	Section of the CISPE Code	**Code Requirements** **(To be implemented by the CISP and verified by the Monitoring Body)**	**Expected controls to achieve the Code Requirements** **(Control title & control description aligned with the Code Requirements)**	**Sample Questions to be answered by the CISP** **(included in the CISPE and Privacy readiness check)**	**Evidence (or equivalent) to verify compliance with the Code requirements (to be documented by the CISP – to be verified by the Monitoring Body onsite or offsite depending on the relevance for the control at stake)**	**Article #**	**Name**	**Comments on the mapping (where partially covered by ISO27001)**
		- The CISP must make available a mechanism to filter data flows, such as a firewall, around the perimeter of the cloud infrastructure as a whole and/or a firewall around the service instance which is deployed. - CISPs must assign a point of contact within the CISP to handle questions from customers regarding data protection or security issues relating to the service. - The CISP shall maintain an information security program with the aim to: (a) identify reasonably foreseeable risks to the security of the CISP Network, and (b) minimize security risks, including through risk assessments and regular testing. - The CISP shall designate one or more CISP personnel to coordinate and be responsible for the information security program. - The CISP shall conduct periodic reviews of the security of the CISP Network and the adequacy of the CISP's information security program. - The CISP shall continually evaluate the security of the CISP Network to determine if additional or different security measures are	measures shall be in place to ensure security (e.g. access management, threat & vulnerability management, etc.). A security program shall be documented with CISP personnel accountable. 4.3.3. Regular audits and tests on CISP security program are performed The CISP's information security program should be subject to continuous and regular evaluation and review. The CISP must inform the customer of any changes which it considers a downgrade of the CISP's security standards at the effective date of the Service Contract, giving information on (i) the nature of the change, (ii) the purpose of the change and the date of its effect.					

CISP COC Control Framework						GDPR articles		
	Section of the CISPE Code	**Code Requirements** **(To be implemented by the CISP and verified by the Monitoring Body)**	**Expected controls to achieve the Code Requirements** **(Control title & control description aligned with the Code Requirements)**	**Sample Questions to be answered by the CISP** **(included in the CISPE and Privacy readiness check)**	**Evidence (or equivalent) to verify compliance with the Code requirements (to be documented by the CISP – to be verified by the Monitoring Body onsite or offsite depending on the relevance for the control at stake)**	**Article #**	**Name**	**Comments on the mapping (where partially covered by ISO27001)**
		required to respond to new security risks or the results generated by the CISP's own periodic reviews. - The CISP may modify against which security standards its information security program may be assessed from time to time, but shall continue throughout the term of the Service Contract to provide at least the same level of security as is described in the CISP's security standards at the effective date of the Service Contract. - The CISP must inform the customer of any changes which it considers objectively to have an impact on the scope of its information security program or on the technical and organizational security measures under CISP's responsibilities at the effective date of the Service Contract. This notification should take place prior to the change in the CISP's security standards, unless the CISP can demonstrate that the change needed to be made urgently in order to address a security vulnerability.						

CISP COC Control Framework						GDPR articles		
	Section of the CISPE Code	**Code Requirements** **(To be implemented by the CISP and verified by the Monitoring Body)**	**Expected controls to achieve the Code Requirements** **(Control title & control description aligned with the Code Requirements)**	**Sample Questions to be answered by the CISP** **(included in the CISPE and Privacy readiness check)**	**Evidence (or equivalent) to verify compliance with the Code requirements (to be documented by the CISP – to be verified by the Monitoring Body onsite or offsite depending on the relevance for the control at stake)**	**Article #**	**Name**	**Comments on the mapping (where partially covered by ISO27001)**
	Section 4.4. Transfer of personal data to third countries	- The CISP's service shall provide the customer the ability to choose to use the service to store and process its data entirely within the EEA, thereby avoiding the application of the GDPR rules governing the transfer of personal data outside the EEA. - The CISP shall provide to the customer information about the region and country where its data is stored and processed by or on behalf of the CISP (regardless of whether the data is stored and processed entirely within the EEA, or in a third country). If the CISP sub-contracts part of the processing to sub-processors, the CISP shall also provide the information set out in Section 4.5. For security reasons, only a general location (such as a city or city region area) needs to be provided. This general description shall, at least, allow the customer to identify which EU Member State has jurisdiction over the customer for processing performed by the customer using the service. - The CISP shall communicate to the competent Supervisory Authority the exact address of the relevant facilities, if such information is required by a competent Supervisory Authority to discharge its obligations under applicable EU	4.4.1. Policies and Procedures for (personal) data transfer mechanisms are documented A framework for the desired regulation of the data transfer mechanism shall be made available by the CISP, including mechanisms covering: - Transfers on the basis of an adequacy decision - Binding corporate rules - Standard Data Protection Clauses 4.4.2. Data processing of personal data. Customer shall have the possibility to choose and enforce limitation to the use of the personal data exclusively in the EU. 4.4.3. The location of data is communicated by the CISP. A general location (City or country) of the personal data processed by or on behalf of the CISP (including sub-contracts) shall be communicated to the customer.	Has the CISP documented a framework of policies and procedures in regards to personal data transfer mechanisms, that the customer can use to ensure lawfulness of personal data transfer or that the CISP can use to ensure lawfulness of its own operations on personal data? Has the CISP provided to the customer information about the region where the personal data is stored? Has the CISP provided the customer with the possibility of choosing the location where the personal data is stored?	Documented policies and procedures detailing personal data transfer mechanisms. Communication/documentation/management interface/website on which: (a) the CISP provides the customer with the region where the personal data is stored. (b) The CISP provides the customer with the possibility of choosing the location of the personal data storage. Evidences regarding data transfer mechanisms such as the Service Contract and addendums/appendixes, the SCCs, BCR, statement where available.	44	Principles for transfer	ISO/IEC 27001: A.13.2.1 A.13.2.2 ISO/IEC 27018: 12.1

CISP COC Control Framework						GDPR articles		
	Section of the CISPE Code	**Code Requirements** **(To be implemented by the CISP and verified by the Monitoring Body)**	**Expected controls to achieve the Code Requirements** **(Control title & control description aligned with the Code Requirements)**	**Sample Questions to be answered by the CISP** **(included in the CISPE and Privacy readiness check)**	**Evidence (or equivalent) to verify compliance with the Code requirements (to be documented by the CISP – to be verified by the Monitoring Body onsite or offsite depending on the relevance for the control at stake)**	**Article #**	**Name**	**Comments on the mapping (where partially covered by ISO27001)**
		data protection law. - For services which can be run indifferently within several different locations in the CISP Network, CISPs must make the information easily accessible to the customer (for example, on the CISP's website) and enable customers to select the location(s) within the CISP Network where their data will be processed. - CISPs must provide their customers with the ability to choose to use the service entirely within the EEA. Any transfer of personal data to a country outside the EEA for the provision of CISP services, including access from a third country outside the EEA, may only occur upon instructions to the CISP from the customer. The CISP shall assist customers, as exporters, in complying with their obligations under Chapter V of the GDPR for the lawful transfer of personal data to the relevant country, including transfers pursuant to an adequacy decision from time to time in force (for example, currently, to Switzerland, Israel and others) (GDPR Art 45) or subject to appropriate safeguards (such as, currently, Binding Corporate Rules or standard data protection clauses adopted by the Commission (GDPR Art 46)), if: i. the customer transfers data from within the	4.4.4. Customer is able to choose the location of data The customer shall have the possibility to choose the location where the personal data is stored.					

CISP COC Control Framework						GDPR articles		
	Section of the CISPE Code	**Code Requirements** **(To be implemented by the CISP and verified by the Monitoring Body)**	**Expected controls to achieve the Code Requirements** **(Control title & control description aligned with the Code Requirements)**	**Sample Questions to be answered by the CISP** **(included in the CISPE and Privacy readiness check)**	**Evidence (or equivalent) to verify compliance with the Code requirements (to be documented by the CISP – to be verified by the Monitoring Body onsite or offsite depending on the relevance for the control at stake)**	**Article #**	**Name**	**Comments on the mapping (where partially covered by ISO27001)**
		EEA to be stored using the CISP's service, including when data is transferred for the purposes of providing "back-up" services to EEA data centers in the case of a force majeure or continuity event by CISP, in any country outside the EEA which is not recognised by the European Commission as providing an adequate level of protection for personal data; or ii. the customer has chosen to allow CISP upon its instructions to access data stored using the CISP's service within the EEA from such country referred to in (i) above. The Service Contract between the CISP and the customer must make clear the circumstances in which there may be a transfer of data to outside the EEA upon customer instructions (including the provision of instructions via the CISP's configuration tools and APIs for the CISP's services) as well as the delineation of responsibilities between the customer (as exporter) and the CISP (as an importer) regarding such transfer. In addition, the CISP shall provide the customer with appropriate information including about the location of the relevant processing in order to enable the customer to verify on a case by case basis, prior to any transfer, whether the law or						

CISP COC Control Framework						GDPR articles		
	Section of the CISPE Code	**Code Requirements** **(To be implemented by the CISP and verified by the Monitoring Body)**	**Expected controls to achieve the Code Requirements** **(Control title & control description aligned with the Code Requirements)**	**Sample Questions to be answered by the CISP** **(included in the CISPE and Privacy readiness check)**	**Evidence (or equivalent) to verify compliance with the Code requirements (to be documented by the CISP – to be verified by the Monitoring Body onsite or offsite depending on the relevance for the control at stake)**	**Article #**	**Name**	**Comments on the mapping (where partially covered by ISO27001)**
		practice of the third country concerned ensures the level of data protection required in the EEA, so as to determine if the guarantees provided by the chosen appropriate safeguards can be complied with in practice. If this is not the case, the responsibility of identifying and implementing, supplementary measures in addition to the relevant appropriate safeguard to ensure to data transferred an essentially equivalent level of protection as provided in the EEA lies on the customer, if needed with the help of the CISP (as data importer). The European Data Protection Board has published a Recommendation [insert link] on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data which can assist the CISP in the assessment relating to the third country and for identifying appropriate supplementary measures. No transfer of personal data to a country outside of the EEA will be initiated by CISP as part of the provision of the services, if the CISP is not instructed to do so by its customer. The CISP shall verify on a case by case basis, prior to any transfer or disclosure of personal data in response to a judgment of a court or tribunal or to any decision of an administrative						

CISP COC Control Framework						GDPR articles		
	Section of the CISPE Code	**Code Requirements** **(To be implemented by the CISP and verified by the Monitoring Body)**	**Expected controls to achieve the Code Requirements** **(Control title & control description aligned with the Code Requirements)**	**Sample Questions to be answered by the CISP** **(included in the CISPE and Privacy readiness check)**	**Evidence (or equivalent) to verify compliance with the Code requirements (to be documented by the CISP – to be verified by the Monitoring Body onsite or offsite depending on the relevance for the control at stake)**	**Article #**	**Name**	**Comments on the mapping (where partially covered by ISO27001)**
		authority of a third country, that such judgement or decision can be recognised or enforceable on the basis of an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, in order to ensure the lawfulness of such transfer or disclosure. If this is not the case, and without prejudice to other grounds for transfer pursuant to Chapter V of the GDPR, the CISP must identify and implement measure to ensure that transfer or disclosure not authorised by Union law are refused to the requesting third country.						
	Section 4.5. Sub-processing	- The CISP shall obtain the customer's authorisation before permitting a third party sub-processor to process Customer Data. - This authorisation shall either be: Specific: in this situation the CISP shall inform the customer in writing, including in electronic writing, the specific sub-processors which it will use. It is only if the controller gives its authorisation to the sub-processing that the CISP can engage the targeted sub-processor to process the Customer Data; or General: in this situation the customer's	4.5.1 Customer's CISP authorisation is obtained The CISP shall obtain the customer authorisation before authorising a sub-processor to access / process customer personal data. Consent shall be obtained through (1) service agreements describing the sub processors used by the CISP and through (2) specific written communication. 4.5.2 Information about sub processor is available	Has the CISP obtained the customer consent before authorising a sub-processor accessing and processing customer personal data? Is this consent obtained through in the Service Contract? Is the CISP maintaining and publishing an up-to-date list of sub-processors Authorised to access customer personal data?	Documentation showing customer consent before authorising a third party sub-processor to access and process customer personal data Service Contract signed by the customer and describing which list of sub contractors used by the CISP and accessing/processing personal data, along with their locations. Service Contracts	28 (2) and 28 (4)	Processor	Implementing guidance ISO/IEC 27018: 8.1 ISO/IECC 27001: A.13.2.2 A.15

CISP COC Control Framework						GDPR articles		
	Section of the CISPE Code	**Code Requirements** **(To be implemented by the CISP and verified by the Monitoring Body)**	**Expected controls to achieve the Code Requirements** **(Control title & control description aligned with the Code Requirements)**	**Sample Questions to be answered by the CISP** **(included in the CISPE and Privacy readiness check)**	**Evidence (or equivalent) to verify compliance with the Code requirements (to be documented by the CISP – to be verified by the Monitoring Body onsite or offsite depending on the relevance for the control at stake)**	**Article #**	**Name**	**Comments on the mapping (where partially covered by ISO27001)**
		consent may instead be given generally through the Service Contract. In particular, the Service Contract shall define cases and conditions in which the CISP may enlist sub-processors for carrying out specific processing activities on behalf of the customer without the requirement to obtain specific authorisation from the customer. - In either case, the CISP must inform the customer of any intended changes to its sub-processors in writing (including in electronic form), giving reasonable notice of the proposed change to allow the customer to consider the change and object to the sub-processor. - The CISP shall maintain an up-to-date list of sub-processors which process Customer Data. This list must include the location of the sub-processor and must be easily accessible to the customer at the time of acceptance of the Service Contract and during its term. The updated list must either be accessible to the customer via a URL, or otherwise be provided in writing following a customer request. Before authorising a new sub-processor to access Customer Data: (i) if the CISP is obtaining general	An up-to-date list of sub processors accessing/processing customer personal data, including their specific role and location, must be accessible by the customer. In addition the CISP shall inform through a written communication of any significant changes or update of the processor list. 4.5.3 Service Contracts with subcontractors are established When the CISP enters in a relationship with a sub contractor accessing and processing customer personal data, this relationship must be governed by a contract binding the CISP to the subcontractor 4.5.4. Security measures Applicable security measures from Section 4.3 and Annex A (Security Responsibilities) are put in place by the CISP to ensure that such subcontractors, suppliers or	In case of sub contracting relationship involving access/processing of personal data, is a service contract in place between the CISP and the subcontractor?	between the CISP and the subcontractors.			

CISP COC Control Framework						GDPR articles		
	Section of the CISPE Code	**Code Requirements** **(To be implemented by the CISP and verified by the Monitoring Body)**	**Expected controls to achieve the Code Requirements** **(Control title & control description aligned with the Code Requirements)**	**Sample Questions to be answered by the CISP** **(included in the CISPE and Privacy readiness check)**	**Evidence (or equivalent) to verify compliance with the Code requirements (to be documented by the CISP – to be verified by the Monitoring Body onsite or offsite depending on the relevance for the control at stake)**	**Article #**	**Name**	**Comments on the mapping (where partially covered by ISO27001)**
		authorisation for sub-processors from the customer, the CISP shall make available to the customer: the identity and general location (such as a country or regional area) of the new sub-processor; the customer's right to object to the new sub-processor (as set out above in (a)); and the deadline by which the customer must exercise their right to object. Such deadline must give the customer a reasonable time to consider the change. (ii) if the CISP is obtaining specific authorisation for sub-processors, it shall make available to the customer the identity and general location (such as a country or regional area) of the new sub-processor and request specific authorisation from the customer before engaging that sub-processor. - The CISP shall impose the same data protection contractual obligations to those set out in the Service Contract between the CISP and the customer on its sub-processor. - The CISP must put in place operational arrangements in respect of its sub-processor	other third parties which do not process Customer Data are prevented from accessing or processing Customer Data.					

CISP COC Control Framework						GDPR articles		
	Section of the CISPE Code	**Code Requirements** **(To be implemented by the CISP and verified by the Monitoring Body)**	**Expected controls to achieve the Code Requirements** **(Control title & control description aligned with the Code Requirements)**	**Sample Questions to be answered by the CISP** **(included in the CISPE and Privacy readiness check)**	**Evidence (or equivalent) to verify compliance with the Code requirements (to be documented by the CISP – to be verified by the Monitoring Body onsite or offsite depending on the relevance for the control at stake)**	**Article #**	**Name**	**Comments on the mapping (where partially covered by ISO27001)**
		to provide the same or a higher level of data protection to the level of data protection under the Service Contract. The CISP must be able to demonstrate to the customer through appropriate documentary evidence that it has taken such measures. - The CISP shall restrict the sub-processor's processing of Customer Data to processing that is necessary to provide or maintain the services. - The CISP shall remain fully liable to the customer for compliance with its data protection obligations and the performance of the sub-processor's data protection obligations under the Service Contract.						
	Section 4.6. Demonstrating compliance	- In order to enable the customer to exercise its rights under Article 28(3)(h) GDPR, the CISP will: (i) provide the customer with appropriate information and documentation as set forth in Section 4.6(a) and (ii) submit its data processing facilities to audits by an independent third party as set forth in Section 4.6(b). - CISPs shall comply with the Transparency Requirements set out in Section 5 and shall	4.6.1. Description of the CISP security controls is documented The CISP shall provide sufficient information about the security controls in place for the services available to customer so that the customer can ensure that the security controls, at the design level, are appropriate. 4.6.2. The CISP security controls are audited by trustable third	Are sufficient information and documentation about security controls in place available to customer which enable them to reasonably verify the CISP's compliance with the security obligations in the Service Agreement? Has an external audit taken place to ensure	Documentation detailing the CISP security controls and the CISP compliance with the security obligations as detailed in the Service agreement. External audit reports covering the operating effectiveness of the CISP Security controls.	28 (3) (h)	Processor	The Audit of the security controls of the service provider by a third party is not enforced by the ISO27001.

CISP COC Control Framework						GDPR articles		
	Section of the CISPE Code	**Code Requirements** **(To be implemented by the CISP and verified by the Monitoring Body)**	**Expected controls to achieve the Code Requirements** **(Control title & control description aligned with the Code Requirements)**	**Sample Questions to be answered by the CISP** **(included in the CISPE and Privacy readiness check)**	**Evidence (or equivalent) to verify compliance with the Code requirements (to be documented by the CISP – to be verified by the Monitoring Body onsite or offsite depending on the relevance for the control at stake)**	**Article #**	**Name**	**Comments on the mapping (where partially covered by ISO27001)**
		make sufficient information about the security controls in place for the services available to customers so that customers can understand the relevant security controls an reasonably verify the CISP's compliance with the security obligations in the Service Contract. - Where information is non-confidential or non-sensitive it shall be made accessible by customers via a straight-forward process (e.g., via the CISP's website). - Where such information is considered too sensitive to disclose, the CISP shall provide the customer with a basic understanding of the position, if this is necessary for the customer to understand the CISP's adopted security measures. - CISPs may require customers to pay an additional fee for information or may choose to provide such information for no additional fee. Any additional fee shall be reasonable, cost based, proportionate to the effort involved in providing that information, and shall not be used to prevent customers from accessing information about the security controls for the service. CISPs shall be clear with customers which information is available without further payment, and which information is only available for	parties. The adequacy and the operating effectiveness of the CISP security controls could be verified through external audits. If such audits are performed they must follow a framework such as recognised Security framework, performed under applicable standard, performed by qualified security professionals and generated a report. 4.6.3. CISP shall provide the customer with a source material which allow the customer to verify the adequacy of the security controls. 4.6.4. If the customer can demonstrate that the existing third party audit and/or source material referred to above is not sufficient to verify the adequacy of the security controls which apply to the service, then a proportionate approach will be taken to achieve further assurance under controlled conditions, including through the use of the Monitoring Body which	adequacy of the operating effectiveness of the CISP Security controls? If such audits are performed, do they comply with the listed conditions: recognised Security framework, performed under applicable standard, performed by qualified security professionals and generated a report				

CISP COC Control Framework						GDPR articles		
	Section of the CISPE Code	**Code Requirements** **(To be implemented by the CISP and verified by the Monitoring Body)**	**Expected controls to achieve the Code Requirements** **(Control title & control description aligned with the Code Requirements)**	**Sample Questions to be answered by the CISP** **(included in the CISPE and Privacy readiness check)**	**Evidence (or equivalent) to verify compliance with the Code requirements (to be documented by the CISP – to be verified by the Monitoring Body onsite or offsite depending on the relevance for the control at stake)**	**Article #**	**Name**	**Comments on the mapping (where partially covered by ISO27001)**
		<u>further payment.</u> - The CISP shall provide a mechanism (whether free of charge or for a reasonable fee) for customers that have questions regarding data protection or security issues relating to the service to request to be put in contact with the then-current CISP personnel or representative assigned by the CISP to handle such matters. These mechanisms should assist the customer in fulfilling its obligations as a controller and should be appropriate and proportionate for the cloud infrastructure service in question. The CISP should also give a commitment on response times, in conformance with agreements defined in the Service Contract. - The customer shall also, upon request, be provided with the annual report produced by the CISP's Monitoring Body pursuant to Section 7.2 (a) of the Code. - If the information provided by the CISP (including information provided under Section 4.6(a) and the annual report prepared by the Monitoring Body in the course of its functions described in Section 7.2(a)) is not sufficient to verify the CISP's compliance with its obligations under GDPR as reflected in the Code Requirements, then the customer may	is responsible for monitoring the CISP's compliance with the Code.					

CISP COC Control Framework						GDPR articles		
	Section of the CISPE Code	**Code Requirements** **(To be implemented by the CISP and verified by the Monitoring Body)**	**Expected controls to achieve the Code Requirements** **(Control title & control description aligned with the Code Requirements)**	**Sample Questions to be answered by the CISP** **(included in the CISPE and Privacy readiness check)**	**Evidence (or equivalent) to verify compliance with the Code requirements (to be documented by the CISP – to be verified by the Monitoring Body onsite or offsite depending on the relevance for the control at stake)**	**Article #**	**Name**	**Comments on the mapping (where partially covered by ISO27001)**
		choose to exercise its rights under Article 28(3)(h) GDPR as follows: • the customer may request in writing to the CISP that the Monitoring Body perform verification, as strictly necessary to demonstrate compliance with the Code Requirements, to the extent not already demonstrated (including by any report already prepared by the Monitoring Body in the course of its functions described in Section 7.2(a)); • the CISP shall permit the Monitoring Body to perform such verification; • in light of the potential security risks to other customers and the service generally, direct access to CISP sites or systems by the Monitoring Body shall be permitted only if there is no other reasonable means of demonstrating compliance, and performed under controlled conditions (mutually agreed between CISP and Monitoring Body) which minimise disruption to the CISP, do not cause risk to the security and continuity of service to other customers, and do not cause the CISP to be in						

CISP COC Control Framework						GDPR articles		
	Section of the CISPE Code	**Code Requirements** **(To be implemented by the CISP and verified by the Monitoring Body)**	**Expected controls to achieve the Code Requirements** **(Control title & control description aligned with the Code Requirements)**	**Sample Questions to be answered by the CISP** **(included in the CISPE and Privacy readiness check)**	**Evidence (or equivalent) to verify compliance with the Code requirements (to be documented by the CISP – to be verified by the Monitoring Body onsite or offsite depending on the relevance for the control at stake)**	**Article #**	**Name**	**Comments on the mapping (where partially covered by ISO27001)**
		breach of any legal obligation or duty it may have. • Where the information provided by the CISP under this Section 4.6 is insufficient to demonstrate compliance as required under GDPR Art 28(3)(h), the customer may request the CISP to take additional steps as necessary to demonstrate such compliance, which may include further requests to the Monitoring Body. If the CISP's or Monitoring Body's response to such request is not sufficient to demonstrate the CISP's compliance with its obligations under GDPR Art 28, the customer may request additional information from the CISP through an additional audit, including inspections, by an auditor mandated by the customer from a list of approved auditors provided by the CISP in advance. Such audit shall be conducted in the least intrusive manner possible for the CISP to verify compliance with its obligations under GDPR Art 28, and shall be subject to (i) reasonable controls determined by the CISP to avoid risks to other customers or the CISP, in particular to the security of the						

CISP COC Control Framework						GDPR articles		
	Section of the CISPE Code	**Code Requirements** **(To be implemented by the CISP and verified by the Monitoring Body)**	**Expected controls to achieve the Code Requirements** **(Control title & control description aligned with the Code Requirements)**	**Sample Questions to be answered by the CISP** **(included in the CISPE and Privacy readiness check)**	**Evidence (or equivalent) to verify compliance with the Code requirements (to be documented by the CISP – to be verified by the Monitoring Body onsite or offsite depending on the relevance for the control at stake)**	**Article #**	**Name**	**Comments on the mapping (where partially covered by ISO27001)**
		CISP's facilities and maintaining the CISP's uninterrupted business operations; (ii) acceptance by the customer of terms protecting confidential information of the CISP; and (iii) the customer's obligation to pay for the reasonable costs of the audit. The customer and the CISP will in good faith discuss and agree the scope of audit activities in advance of conducting any such audit.						
	Section 4.7. Data Subject Rights	- The CISP shall provide the customer with the ability to rectify, erase, restrict, access or port (in a structured, commonly used and machine-readable format) Customer Data as part of the service or by enabling customers to design and deploy their own solutions using the service. - The CISP shall provide an explanation of how these abilities will be provided to the customer as part of the information required pursuant to Section 5 (Transparency).	4.7.1 Procedures/tools enabling necessary actions on personal data are implemented Procedures and tools shall be implemented by the CISP to enable the customer to timely and adequately respond to requests related to data subject rights (information, rectification, limitation, erasure...). Alternatively, the CISP must enable the customer to deploy its own solution to answer to such requests. 4.7.2. Transparency of the information provided by the CISP	Are procedures/tools in place to answer requests from the customer related to data subject rights? Does the CISP provide the customer with the ability to deploy their own solution in order to perform the actions necessary to respond to the data subject request on their data?	Documentation of the procedures/tools in place enabling to handle requests related to data subject rights.	28 (3) (e)	Data Processing agreement	

CISP COC Control Framework						GDPR articles		
	Section of the CISPE Code	**Code Requirements** **(To be implemented by the CISP and verified by the Monitoring Body)**	**Expected controls to achieve the Code Requirements** **(Control title & control description aligned with the Code Requirements)**	**Sample Questions to be answered by the CISP** **(included in the CISPE and Privacy readiness check)**	**Evidence (or equivalent) to verify compliance with the Code requirements (to be documented by the CISP – to be verified by the Monitoring Body onsite or offsite depending on the relevance for the control at stake)**	**Article #**	**Name**	**Comments on the mapping (where partially covered by ISO27001)**
			Information is provided by the CISP to the customer in a transparent manner on how those procedures and tools enabling to timely and adequately respond to requests related to data subject rights.					
	Section 4.8. CISP personnel	- The CISP shall impose appropriate contractual obligations requiring any personnel authorised by the CISP to access Customer Data to protect the confidentiality of that Customer Data. - The CISP shall implement and maintain access controls and policies in order to limit its personnel processing Customer Data to those CISP personnel who need to process Customer Data to provide the services to the customer. - The CISP shall select appropriate access controls, which shall include: (i) restricting physical access to data center facilities to authorised personnel; (ii) restricting technical access to host software and networks to authorised personnel (iii) logging of CISP personnel access to Customer Data. When CISP personnel no longer need to process Customer Data, the CISP shall promptly revoke that personnel's access privileges.	4.8.1. Confidentiality agreements are signed by CISP employees handling personal data All CISP employees with access to such data, shall sign a confidentiality agreement, unless this matter is not addressed in their job contract. 4.8.2. Access management process are in place Access control policies and procedures shall be documented and mechanisms shall be in place in order the restrict CISP personnel processing customer data from accessing what is not necessary/legitimate for them to access, and when it is no more necessary.	Is confidentiality of personal data handled by the CISP employees covered by document signed by each CISP employee manipulating personal data (job contract, NDA)? Has the CISP documented access control policies and procedures in order to restrict CISP personnel processing customer data to only personnel who need to process customer data to provide the services to the customer?	Signed job contract/NDA by each CISP employee manipulating personal data. CISP access control policies and procedures on personal data	28 (3) (b)	Processor	Documentation and Signature of a confidentiality agreements by the users of the personal data is not covered by the ISO27001. The restriction of the sensitive data (personal data) is not covered by the ISO27001.

CISP COC Control Framework						GDPR articles		
	Section of the CISPE Code	**Code Requirements** **(To be implemented by the CISP and verified by the Monitoring Body)**	**Expected controls to achieve the Code Requirements** **(Control title & control description aligned with the Code Requirements)**	**Sample Questions to be answered by the CISP** **(included in the CISPE and Privacy readiness check)**	**Evidence (or equivalent) to verify compliance with the Code requirements (to be documented by the CISP – to be verified by the Monitoring Body onsite or offsite depending on the relevance for the control at stake)**	**Article #**	**Name**	**Comments on the mapping (where partially covered by ISO27001)**
		- CISP's personnel may have the need to access Customer Data in order to perform the services. Access shall only be permitted as needed to manage the service. Personnel who do not need to access Customer Data to manage the service shall be subject to appropriate access controls designed to prevent them doing so.						
	Section 4.9. Data breach	- The CISP shall implement a security incident management policy that specifies the procedures for identifying, and responding to personal data breaches of which the CISP becomes aware. This policy must include: • guidance on how incidents should be addressed, including who is responsible for security incident management within the CISP; • guidance on what constitutes a personal data breach under GDPR, including guidance for deciding which type of incidents have to be notified to the customer based on the potential impact on Customer Data;	4.10.1. A Security incident management policy is documented The CISP shall implement a security incident management policy including: a/ guidance for deciding which type of incidents have to be notified to the customer based on the potential impact on data; b/ guidance on how incidents should be addressed; and c/ a specification of the information to be made available to the customer following the data breach incident. 4.10.2 A Data Breach response	Is a security incident management policy implemented by the CISP? Is a Data Breach response plan and Incident detection defined and documented by the CISP? How a Security breach is notified to the customer? What is the content of the notification?	Documentation of the security incident management policy implemented by the CISP. Documentation of the data Breach response plan Example of Security Breach notification	33 and 28 (3)(f)	Notification of breach to authority	

CISP COC Control Framework						GDPR articles		
	Section of the CISPE Code	**Code Requirements** **(To be implemented by the CISP and verified by the Monitoring Body)**	**Expected controls to achieve the Code Requirements** **(Control title & control description aligned with the Code Requirements)**	**Sample Questions to be answered by the CISP** **(included in the CISPE and Privacy readiness check)**	**Evidence (or equivalent) to verify compliance with the Code requirements (to be documented by the CISP – to be verified by the Monitoring Body onsite or offsite depending on the relevance for the control at stake)**	**Article #**	**Name**	**Comments on the mapping (where partially covered by ISO27001)**
		• a requirement to perform expeditious investigations when a CISP becomes aware of a suspected data breach to ascertain whether a breach has occurred, and which Customer Data may be affected; • a process for the implementation of remediation activity to mitigate the impact of a data breach, and address vulnerabilities exposed by security incidents; • a process to notify without undue delay the customer when the CISP has ascertained that a data breach has occurred which relates to the Customer Data of that customer; • classifications of incident type by severity, and indicative timelines for key investigatory steps, and planned notification to customer(s) (if applicable), appropriate to the severity of the incident; • appropriate escalations, within the CISPs own governance, of incident	plan is defined and documented A data breach and incident detection/response plan must be defined by the CISP, that covers: - identification of a personal data breach - determination of the relevant mitigating controls - assessment of the impact of the personal data breach 4.10.3 The Customer is notified in case of data breach In case of a data breach, the CISP has to notify the customer of a data breach within a reasonable timeframe after becoming aware of the breach and without undue delay. The notification will (i) describe the nature of the security breach, (ii) describe the consequences of the breach, (iii) describe the measures taken or proposed to be taken by the CISP in response to the incident and (iv) provide a contact point at the CISP.					

CISP COC Control Framework						GDPR articles		
	Section of the CISPE Code	**Code Requirements** **(To be implemented by the CISP and verified by the Monitoring Body)**	**Expected controls to achieve the Code Requirements** **(Control title & control description aligned with the Code Requirements)**	**Sample Questions to be answered by the CISP** **(included in the CISPE and Privacy readiness check)**	**Evidence (or equivalent) to verify compliance with the Code requirements (to be documented by the CISP – to be verified by the Monitoring Body onsite or offsite depending on the relevance for the control at stake)**	**Article #**	**Name**	**Comments on the mapping (where partially covered by ISO27001)**
		response issues; • a specification of the information that must be made available to the customer following the data breach; and • a process for cooperating with customers in circumstances where the customer informs the CISP of a data breach, such as providing any preliminary information that is available in order to assist the customer's compliance with its obligations under Article 33(1) of the GDPR. - If the CISP becomes aware of the accidental or unlawful destruction, loss, alteration or unauthorised disclosure of, or access to, any Customer Data on the CISP's equipment or in the CISP's facilities, the CISP shall notify the customer without undue delay. - The notification shall, to the extent the CISP has knowledge of such information as a data processor: (i) describe the nature of the security breach, (ii) describe the consequences of the breach, (iii) describe the measures taken or proposed to be taken by the CISP in response to						

CISP COC Control Framework						GDPR articles		
	Section of the CISPE Code	**Code Requirements** **(To be implemented by the CISP and verified by the Monitoring Body)**	**Expected controls to achieve the Code Requirements** **(Control title & control description aligned with the Code Requirements)**	**Sample Questions to be answered by the CISP** **(included in the CISPE and Privacy readiness check)**	**Evidence (or equivalent) to verify compliance with the Code requirements (to be documented by the CISP – to be verified by the Monitoring Body onsite or offsite depending on the relevance for the control at stake)**	**Article #**	**Name**	**Comments on the mapping (where partially covered by ISO27001)**
		the incident and (iv) provide a contact point at the CISP.						
	Section 4.10 Deletion or return of personal data.	- The CISP shall provide the customer with the ability to retrieve and delete Customer Data in its entirety. - The CISP shall provide, in the information required pursuant to Section 5 (Transparency), an explanation of how these abilities will be provided to the customer. - At all times, the CISP shall comply with any instructions given by the customer in respect of retrieval or deletion of Customer Data. - In the absence of instructions from the customer, CISP shall by default delete Customer Data within a reasonable period of time following the expiry or termination of the service.	4.11.1. Technical and organisational measures for removal personal data are documented and are in place The CISP shall provide the customer with the ability to retrieve and delete the personal data for which the customer is the controller, (a) as part of the service, or (b) by enabling the customer to design and deploy their own deletion and retrieval solutions using the service. 4.11.2. Transparency of the information provided by the CISP Information is provided by the CISP to the customer in a transparent manner on how those procedures and tools enabling to timely and adequately respond to requests related to data subject rights.	Has the customer the ability to retrieve and delete personal data for which it is the controller? Is it as part of the service or by enabling customer to deploy their own retrieval /deletion tool?	Documentation of the procedures/tools in place enabling customer to retrieve/delete personal data.	28(3)(g)	Processor	

CISP COC Control Framework						GDPR articles		
	Section of the CISPE Code	**Code Requirements** **(To be implemented by the CISP and verified by the Monitoring Body)**	**Expected controls to achieve the Code Requirements** **(Control title & control description aligned with the Code Requirements)**	**Sample Questions to be answered by the CISP** **(included in the CISPE and Privacy readiness check)**	**Evidence (or equivalent) to verify compliance with the Code requirements (to be documented by the CISP – to be verified by the Monitoring Body onsite or offsite depending on the relevance for the control at stake)**	**Article #**	**Name**	**Comments on the mapping (where partially covered by ISO27001)**
	Section 4.11. Records of Processing	- The CISP shall maintain a written record (which may be electronic) of processing activities it carries out on behalf of its customers who are controllers, including: • the name and contact details of the customer; • the categories of processing carried out by the customer (these categories may be generally stated, such as by reference to the services provided by the CISP); • whether the CISP has implemented or otherwise makes available to the customer a mechanism for transfers which is recognised under Chapter V of the GDPR; and • a general description of the security measures in place(for example, such as the measures adopted to comply with Annex A). - The CISP must make the record available to a Supervisory Authority on request.	Maintenance of appropriate records of the processing activities the CISP carries out on behalf of its customers. Such records shall include: - the name and contact details of the customer; - the categories of processing carried out by the customer (these categories may be generally stated, such as by reference to the services provided by the CISP); -whether the CISP has implemented or otherwise made available to the customer a mechanism for transfers which is recognised under Chapter V of the GDPR; and - a general description of the security measures in place(for example, such as the measures adopted to comply with Annex A).	Does the CISP have up-to-date records of the processing activities it carries out on behalf of its customers?	Documentation of records of processing activities.	30(2)	Records of processing activities	

CISP COC Control Framework						GDPR articles		
	Section of the CISPE Code	**Code Requirements** **(To be implemented by the CISP and verified by the Monitoring Body)**	**Expected controls to achieve the Code Requirements** **(Control title & control description aligned with the Code Requirements)**	**Sample Questions to be answered by the CISP** **(included in the CISPE and Privacy readiness check)**	**Evidence (or equivalent) to verify compliance with the Code requirements (to be documented by the CISP – to be verified by the Monitoring Body onsite or offsite depending on the relevance for the control at stake)**	**Article #**	**Name**	**Comments on the mapping (where partially covered by ISO27001)**
		- The CISP will maintain records of the services used by its customers as required under the GDPR; however, the customer is the only party with visibility into the specific details of the personal data it chooses to process using these services (and is separately required to maintain records pursuant to GDPR Article 30(1)).						
	Section 5.1 A Service Contract that addresses the division of responsibilities between the CISP and the Customer for the security of the service	- The Service Contract shall define the security responsibilities of the CISP and the customer for the duration of the term of the Service Contract.	5.1. The division of responsibilities is defined and documented The division of responsibilities between the CISP and the customer shall be defined and documented in the Service Contract. It should be documented through a matrix based on a recognized framework (ISO27001 or NIST) in which responsibilities of the CISP as well as the customer are highlighted, as well as the non-allocated responsibilities (if any).	Does the service agreement clearly address the division of responsibilities between the CISP and the customer for the security of the Service? Is the description of the division of responsibilities between the CISP and the customer made available for consultation by the CISP to the customer?	Documentation of the service or service agreement which describes the division of responsibilities for security between the CISP and the customer. Additional documentation accessible to the customer on the division of responsibilities for security between the CISP and the customer.	28(3)(a)	Data Processing agreement	Division of responsibilities between the customer and service provider not fully covered by the ISO27001. The documentation of the division of responsibilities is not required by the ISO27001

CISP COC Control Framework						GDPR articles		
	Section of the CISPE Code	**Code Requirements** **(To be implemented by the CISP and verified by the Monitoring Body)**	**Expected controls to achieve the Code Requirements** **(Control title & control description aligned with the Code Requirements)**	**Sample Questions to be answered by the CISP** **(included in the CISPE and Privacy readiness check)**	**Evidence (or equivalent) to verify compliance with the Code requirements (to be documented by the CISP – to be verified by the Monitoring Body onsite or offsite depending on the relevance for the control at stake)**	**Article #**	**Name**	**Comments on the mapping (where partially covered by ISO27001)**
	Section 5.2 A high level statement on the security objectives and standards that apply to the service	- The CISP shall state (a) the objectives that the security measures implemented by the CISP for the service are designed to pursue, and if applicable (b) the standards the CISP will follow when implementing those security measures. See Annex A (Security Responsibilities) for further details. - The CISP shall inform customers if a cloud infrastructure service is intended by the CISP to assist customers to comply with a recognised standard or legal requirement applicable to a specific type of processing (e.g. processing healthcare data).	5.2. Security objectives and security standards are documented The CISP shall document the objectives of the implemented security measures for each service provided as well as the standards followed during the implementation. The documented procedures should be regularly updated by the CISP. The CISP shall inform customer if a specific service is intended to assist customers to comply with a recognised standard or legal requirement applicable to a specific type of processing (e.g. processing healthcare data).	Are the objectives of the implemented security measures documented by the CISP? Are the standards used by the CISP during the implementation of the security measures defined and documented by the CISP? Is the documentation of applicable security standards updated when needed by the CISP? Are specific services intended to assist customer to comply with a recognised standard or legal requirement applicable to a specific type of processing, documented and communicated to customers.	Documentation, accessible to the customer, on the security measures implemented by the CISP, Documentation, accessible to the customer, on the standards used by the CISP during the implementation of the security measures. Documentation, accessible to the customer, on specific standards or legal requirements that the cloud infrastructure is compliant with.			The security measures are covered by the ISAE3000 control framework but the documentation of the objectives if the implemented measures are required by ISO27001.

CISP COC Control Framework						GDPR articles		
	Section of the CISPE Code	**Code Requirements** **(To be implemented by the CISP and verified by the Monitoring Body)**	**Expected controls to achieve the Code Requirements** **(Control title & control description aligned with the Code Requirements)**	**Sample Questions to be answered by the CISP** **(included in the CISPE and Privacy readiness check)**	**Evidence (or equivalent) to verify compliance with the Code requirements (to be documented by the CISP – to be verified by the Monitoring Body onsite or offsite depending on the relevance for the control at stake)**	**Article #**	**Name**	**Comments on the mapping (where partially covered by ISO27001)**
	Section 5.3. Information on the design and management of the service	- The CISP shall provide information to customers on the infrastructure available to the customer and how it is used to deliver the service (i.e. the facilities, network, hardware and operational software that support the provisioning and use of the services).	5.3. The service provided by the CISP is documented CISP shall provide information to customer on the service provided (architecture, location of hosting, subcontractors, security features, security options)	Has the CISP provided information to customer on the service provided? (architecture, location of hosting, subcontractors, security features, security options)	Documentation, accessible to the customer, detailing the infrastructure provided to the customer. Documentation, accessible to the customer, detailing the use of this infrastructure by the CISP. This information may, for example, include: -High-level architecture of the infrastructure -General location of the CISP's hosting facilities -Subcontractor's authorised by the CISP to access customer data -Security features of the service -Options the customer can use to add to further security to the service			The ISO27001 does not enforce the communication of the services provided by the service provider (CISP)

CISP COC Control Framework						GDPR articles		
	Section of the CISPE Code	**Code Requirements** **(To be implemented by the CISP and verified by the Monitoring Body)**	**Expected controls to achieve the Code Requirements** **(Control title & control description aligned with the Code Requirements)**	**Sample Questions to be answered by the CISP** **(included in the CISPE and Privacy readiness check)**	**Evidence (or equivalent) to verify compliance with the Code requirements (to be documented by the CISP – to be verified by the Monitoring Body onsite or offsite depending on the relevance for the control at stake)**	**Article #**	**Name**	**Comments on the mapping (where partially covered by ISO27001)**
	Section 5.4. Information validating the risk management processes and criteria of the CISP	- The CISP shall provide information to customers validating the existence and suitability of the CISP's risk management program, including its considered threats model and risk management criteria, to assist customers to incorporate the CISP's controls in the customer's own risk management framework.	5.4. CISP risk management program is documented The CISP shall provide information to the customer demonstrating the existence and suitability of the CISP's risk management program so that the customer could use and incorporate the CISP's controls in its own risk management framework.	Has the CISP provided information to the customer demonstrating the existence and suitability of the CISP's risk management program?	Documentation, accessible to the customer, of the CISP risk management framework (methodology, tools, metrics, risk universe, etc.) Reports on Internal and/or external risk assessments performed or commissioned by the CISP, accessible to the customer			
	Section 5.5. Information on the security measures implemented by the CISP for the service	- The CISP shall make sufficient information about the security measures in place for the services available to customers to assist customers to understand the controls in place for the service that they use and how those controls have been validated. - Specifically, the CISP shall describe: • the physical and operational security processes for the network and server infrastructure under the CISP's management; and	5.5. CISP security measures are documented Security measures in place for the service available to the customers must be documented and provided by the CISP. This information should cover the security measures under CISP management (enforced for each customer) and security measures that can be selected by the customer as an option.	Is sufficient information about the security measures in place for the service available to the customers, documented and provided by the CISP? Is this information covering the security measures under CISP management (enforced for each customer) as well as the security measures that might be selected by the customer as an option?	Documentation, accessible to the customer, about security measures in place (procedures, guide, technical map, etc.), covering for instance: physical and environmental security; network security;business continuity management; change management; and account security features.			ISO 27001 is not Enforcing the communication of the security measures to third parties by the service provider.

CISP COC Control Framework						GDPR articles		
	Section of the CISPE Code	**Code Requirements** **(To be implemented by the CISP and verified by the Monitoring Body)**	**Expected controls to achieve the Code Requirements** **(Control title & control description aligned with the Code Requirements)**	**Sample Questions to be answered by the CISP** **(included in the CISPE and Privacy readiness check)**	**Evidence (or equivalent) to verify compliance with the Code requirements (to be documented by the CISP – to be verified by the Monitoring Body onsite or offsite depending on the relevance for the control at stake)**	**Article #**	**Name**	**Comments on the mapping (where partially covered by ISO27001)**
		• the security features and controls available for use and configuration by customers on the service (on each of which the CISP shall maintain a secure by default posture). - This information shall, for example, include information about: • physical and environmental security; • network security; • logical or physical controls to ensure isolation of customer's data, such as network segmentation of data storage principles; • business continuity management; • change management; and account security features.						
	Section 5.6. Documentation covering the CISP's information	The CISP shall make sufficient information about the information security management system in place for the services available to customers so that customers can reasonably verify the CISP's compliance with the security obligations in the Service Contract as described	CISP's information security management system is documented Information about the CISP's information security management system must be provided to the customer so that it	Is information about CISP's information security management system documentation provided to customer detailed enough that enables it to verify the	Documentation, accessible to the customer, detailing the CISP security information management program.			

CISP COC Control Framework						GDPR articles		
	Section of the CISPE Code	**Code Requirements** **(To be implemented by the CISP and verified by the Monitoring Body)**	**Expected controls to achieve the Code Requirements** **(Control title & control description aligned with the Code Requirements)**	**Sample Questions to be answered by the CISP** **(included in the CISPE and Privacy readiness check)**	**Evidence (or equivalent) to verify compliance with the Code requirements (to be documented by the CISP – to be verified by the Monitoring Body onsite or offsite depending on the relevance for the control at stake)**	**Article #**	**Name**	**Comments on the mapping (where partially covered by ISO27001)**
	security management system	in Section 4.6 (Data Protection; Demonstrating Compliance) of this Code.	can verify the CISP's compliance with the security responsibilities of the CISP as detailed in the service contract.	CISP's compliance with the security responsibilities of the CISP as detailed in the service contract?				
	Section 5.7 Information on the service functionality which allows the customer to i) rectify, erase, restrict, access or port Customer Data; and ii) retrieve and delete Customer Data.	- The CISP shall provide the customer with information about the capabilities available to them to enable them to: - rectify, erase, restrict, access or port Customer Data as set out in Section 4.7 of this Code (Data subject rights); and - retrieve and delete Customer Data as set out in Section 4.10 of this Code (Deletion or return of personal data).	**Communication of the CISP capabilities** The CISP shall provide the customer with information about the capabilities available to them to enable them to: • rectify, erase, restrict, retrieve or transfer Customer Data ; and retrieve and delete Customer Data.	Is information about CISP's information capabilities provided to customer detailed enough that enables customer to verify that the CISP service enables them to rectify, erase, restrict, retrieve or transfer Customer Data?	Documentation which provides the customer with information about the CISP capabilities available to them to enable them to: - rectify, erase, - restrict, retrieve or transfer Customer Data ; and - retrieve and delete Customer Data.			ISO/IEC 27018: 2.1

Compliance checklist specific to Annex A

CISP COC Control Framework – Specific to Annex A – Security Responsibilities					GDPR articles		
Reference in	**Code Requirements**	**Expected controls**	**Questions to be**		**Article**	**Name**	**Comments on the**

CISPE Code	(To be implemented by the CISP and verified by the Monitoring Body)	(Control title & control description)	(included in the CISPE and Privacy readiness check)	Evidence (or equivalent) to verify compliance with the Code requirements (to	#		mapping (where partially covered by ISO27001)
(1)Information Security Management	- The CISP shall have clear management-level direction and support for the security of the service. - The CISP shall have in place a management-approved set of information security policies that govern the security of the service. - The CISP shall implement an information security management system or equivalent. The scope of the information security management system shall cover the service. - The CISP shall designate one or more personnel to coordinate and be accountable for the information security management system.	• Ensuring information security policies and procedures cover, at a minimum: (a) the scope and boundaries of the information security program, including business, organisation, locations, assets and technology; (b) usage policies defining appropriate usage for critical technologies such as mobile devices, wireless technologies, e-mail and internet usage; and (c) roles and responsibilities to manage and implement the information security policies. • Ensuring the CISP's security policy framework covers, at a minimum, the following areas: (a) asset management; (b) human resources; (c) access controls; (d) physical and environmental security; (e) system development lifecycle; (f) incident management; (g) business continuity; (h) compliance; and (i) mobile device usage. • Communicating information security policies to all CISP personnel (including vendors and business partners), including regular updates. • Developing operational procedures to provide guidance for the operation of systems and services within the CISP environment, where necessary.		Documentation, accessible to the customer, on the standards used by the CISP during the implementation of the security measures. Documentation, accessible to the customer, on specific standards or legal requirements that the cloud infrastructure is compliant with			ISO/IEC 27001: A.5
(2) Human Resource Security	- The CISP shall have in place an organisational structure to manage the implementation of information	• Ensuring the board of directors of the CISP receives updates as to incidents, threats and status of		Security policies, HR security policies, security trainings			ISO/IEC 27001: A.6.1 A.7.2

	security within the CISP's services with clearly defined roles and responsibilities. - The CISP shall establish an information security organisation managed by the CISP's security team and led by the CISP's Chief Information Security Officer (CISO) or equivalent. The CISP's security organisation shall establish and maintain formal policies and procedures to delineate standards for logical access on the CISP's system and infrastructure hosts. The policies also identify functional responsibilities for the administration of logical access and security. The CISP shall be responsible for training its employees and contractors on these policies and procedures. Procedures shall exist so that the CISP's employee and contractor user accounts are added, modified, or disabled in a timely manner and are reviewed on a regular basis. In addition, password complexity settings for user authentication to CISP systems are managed in compliance with the CISP's corporate password policy which has to be aligned with state-of-the-art password standard such as minimum complexity, length, password history, lock out in the event of multiple authentication failure or multi-factor authentication. -Requests for changes in access shall be captured in a permissions management tool audit log or equivalent. The CISP shall employ the	security improvement deliverables. • Implementing a security awareness program for CISP personnel to ensure they understand the necessary behaviours and skills to help ensure the security of the CISP. • Updating the CISP's security awareness program to address new technologies, threats, standards, privacy & data protection, and business requirements. • Providing role-based security training based on assigned responsibilities to CISP and customer personnel before authorising access to CISP systems or performing assigned duties. • Tracking completion of security training activities by CISP personnel for compliance with training requirements as set out by the Code and GDPR. • Ensuring CISP and customer personnel acknowledge that they have read and understood the CISP information security policy and procedures. • Ensuring that all users with administrative account access use a dedicated or secondary account for elevated activities, with specific security measures (e.g: password complexity, multi-factor authentication; traceability of		(onsite/online), IT policies, password policies.			

	concept of least privilege, allowing only the necessary access for users to accomplish their job function. User accounts are created to have minimal access. Access above these least privileges requires appropriate authorisation.	relevant events, etc.). This account should only be used for administrative activities and not internet browsing, email, or similar activities. • Limiting CISP personnel access, so CISP personnel are only able to access information related to the structural elements of the cloud infrastructure, its configurations and the configuration of logical environments assigned to customers. Having controls in place so CISP personnel do not have access to customer information and application data, unless there is an explicit customer request for assistance, maintenance or updates. • Implementing controls so CISP personnel cannot keep infrastructure sessions open during their absence. • Having in place policies where CISP personnel cannot keep the credentials needed to access CISP physical infrastructure in writing, with the exception of a superuser password, known by the system administrator and kept by the operational manager.					
(3) User Access Management	- The CISP shall provide the customer with an access control management system for customer user access to the cloud infrastructure service as part of the service. The access control management system shall include, for example, individual accounts (which	• Actively managing the life cycle of accounts, including the creation, use and deletion of accounts, in order to minimise opportunities for attackers to leverage them. • Disabling dormant CISP user accounts		User access management policies.			ISO/IEC 27001: A.9

	could be a user or service account), role based access and passwords or other authentication policy means. The CISP shall explain to customer how the access control management system works so that the customer can use and configure it as set out below.	after a set period of inactivity. • Ensuring CISP user sessions automatically lock after a standard period of inactivity. • Actively managing access management systems by implementing role and profile. • Providing administrative access to customers for logical environment configuration with secure and encrypted connections on explicit customer request.					
(4) Physical and environmental security	- The CISP shall implement and maintain state-of-the-art physical and environmental security measures for the cloud infrastructure service designed (i) to help customers secure personal data against unauthorised processing and accidental or unlawful loss, access or disclosure and (ii) to prevent reasonable environmental threats such as fire and water damages.	• Zoning of hosting areas based on criticality. Implementing and controlling such zoning with walls, fences, doors and mantraps under access controls, video-monitoring and guarding. • Using physically or logically segregated systems to isolate and run software that incurs higher risk for the customer. • Managing access to datacenters and cages by a visual authentication or badge system and restricting permanent access to CISP facilities and secure areas to authorised and approved personnel. • Having a system in place whereby visitor (i.e., any persons without a persistent need for access) access requests to CISP facilities and secure areas must be submitted and documented using an approved CISP mechanism, and will only be approved by authorised CISP personnel.		Physical and environmental security policies.			ISO/IEC 27001: A.11.1 A.11.1.4 A.13.1

		• Verifying the identify of any visitors to CISP facilities and secure areas by means of a government issued photo ID (e.g., driver's license, passport, etc.) or a CISP corporate picture ID.					
(5) Physical servers and equipment, including firewalls	- The CISP is solely responsible for the deployment, operation and security of any physical hardware, *host* operating system, and virtualisation layer, used to provide the cloud infrastructure service, including any configuration needed for the provision of the service. - The CISP shall make available a mechanism to filter data flows such as a firewall around the perimeter of the cloud infrastructure as a whole and/or a firewall around the service instance which is deployed. Where there is a filter mechanism (such as a firewall) to protect the CISP entire global infrastructure, the CISP will be responsible for configuring this mechanism.	• Implementing a configuration management database covering all physical servers and equipment and managing the lifecycle of such assets. • Implementing security controls to ensure the security of the supply chain and that operations are trackable. • Installing and configuring data plane filtering on wired and wireless environments to protect the CISP network from external networks such as the internet. For example using a network based firewall. • Ensuring data plane policies, for example, firewall rules, adhere to approved configurations. For example, (a) unnecessary ports, protocols, and services must be restricted on network devices; (b) devices should be configured for HA (High Availability) mode; and (c) data plane policies (e.g., firewall device configurations) must have “extended ip deny” for the access-list border-net, which denies anything not specifically approved in the access control lists. • Ensuring changes to data plane policies are approved by CISP management and tested prior to implementation.		Physical servers and equipment policies.			ISO/IEC 27001: A.8.1 A.15.1 A.13.1

		• Ensuring firewall configurations and access control lists ("ACL") are managed by a network engineer in accordance with approved rule sets. For example: (a) the ACL management tool must be used to deploy approved ACLs to firewalls on the production network; and (b) if a firewall or network device cannot be reached by the ACL management tool, this must be reviewed and remediated. • Ensuring firewall rule sets are reviewed and approved by the information security team. • Pushing data plane polices to network devices based on platform, location and network.					
(6) Malware protection management	- The CISP shall implement malware protection on sensitive systems (i.e. commonly affected or targeted systems) that are part of the cloud infrastructure service.	• Installing anti-virus protection on servers on the network and workstations. • Configuring anti-virus protection to: (a) scan electronic mail, electronic mail attachments, web accesses, and removable media; (b) perform critical system file scans during system boots; and (c) block and quarantine malicious code and send alerts to the CISP security administrator. • Configuring systems to automatically update anti-virus software. • Ensuring all software installed on a platform is system software downloaded from authenticated sources.		Malware protection management policies.			ISO/IEC 27001: A.12.2 A.12.5 A.12.6
(7) Vulnerability management	-The CISP shall define the level of engagement (distribution of tasks between CISP and customer, delay	• Subscribing to a vulnerability watch service and mapping any vulnerability to the CISP configuration		Vulnerability management policies.			ISO/IEC 27001: A.6.1.4 A.12.6

	between patch and patching, etc.) for the cloud infrastructure service. - The CISP shall, unless it specifically notifies the customer otherwise in the Service Contract, be responsible for patching within hardware, networking between hardware, virtualisation layer and *host* operating systems.	management database. Assessing any applicable vulnerability in the context of the vulnerable asset to prioritise patching activities. • Ensuring that host operating systems are running the most recent security updates provided by the software vendor. • Conducting penetration tests to identify vulnerabilities and attack vectors that could be used to exploit enterprise systems.					A.14.2
(8) Logging and Monitoring	- The CISP shall provide the customer with monitoring (e.g. level, scope, reporting, interfaces, API) and logging (e.g. access, records, duration of recording) tools and/or reports on request for the cloud infrastructure service.	• Defining a list of system events that should be logged to include the following: (a) successful and unsuccessful authentication and authorisation attempts; (b) account management events; (c) privileged functions; (d) system start-up and shutdown; (e) data deletions, data access, and data changes; and (f) unsuccessful events (for example, calls not authorised). • Implementing logs on systems to record the following information, at a minimum, for each system event (including user events, system events and security events): (a) user identification (including service, caller and user); (b) type of event or API called; (c) date and time zone; (d) source of system event; (e) outcome of system event; and (f) identity of affected system component or resource. • Collecting logs from all systems, devices and network components to a centralised logging service which		Logging and Monitoring policies.			ISO/IEC 27001: A.12.4

		allocates audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded and retains audit records for a defined period of time. • Aggregating, correlating, reviewing and analysing logs to identify anomalies and other potentially malicious events. • Monitoring systems and facilities for potential security events, and configuring such systems and facilities to automatically generate alerts notifying appropriate personnel. • Protecting logs from unauthorised access. For example, by restricting log access to authorised CISP personnel and implementing tamper resistant/evident or change detection software to detect tampering of log information.					
(9) Equipment end-of life	The CISP shall conduct a storage media decommissioning process prior to final disposal of storage media used to store Customer Data when such media has reached the end of its useful life, to prevent Customer Data from being exposed to unauthorised individuals. The decommissioning process will be conducted in accordance with industry standard practices (such as described in ISO/IEC 27002; or NIST 800-88) designed to ensure that Customer Data cannot be retrieved from the applicable type of storage media by any data or information retrieval tools	• Using the techniques detailed in e.g. DoD 5220.22-M ("National Industrial Security Program Operating Manual ") or e.g. NIST 800-88 ("Guidelines for Media Sanitization") to destroy data as part of the decommissioning process. • Degaussing and physically destroying all decommissioned magnetic storage devices in accordance with industry standard practices. • Protecting media from unauthorised disclosure or misuse until the media is destroyed.		Equipment end-of life policies.			ISO/IEC 27001: A.8 A.11.2.5 A.11.2.6 A.11.2.7

	or similar means.	• Tracking all media handling and custody. • Ensuring storage media used in one host or system is never reused in another host or system. • Storing all media in a secure, locked/tamper-proof, bin immediately after their removal from source devices. The bin should reside within the cage or pod where the relevant hard drives were removed. • Ensuring media is not taken off-site without prior authorisation and that any media removed from CISP premises is not left unattended in public places. • Protecting media during transportation beyond CISP physical boundaries and ensuring activities associated with the transport of media are restricted to authorised personnel, who are monitored and documented.					

Key

Covered by ISO27001
Partially covered by ISO27001
Not covered by ISO27001

Together the requirements covered by ISO27001 and requirements partially covered by ISO27001 constitute the Auditable Code Requirements.

Annex C – Template Declaration of Adherence

This is a Declaration of Adherence ("**Declaration**") with the Data Protection Code of Conduct for Cloud Infrastructure Service Providers (the "**Code**"). Unless they are otherwise defined, capitalised terms used in this Declaration will have the meaning given to them in the Code.

(1) Services covered by this Declaration

This Declaration covers the cloud infrastructure service(s) below (the "**Services**"). If this Declaration is being made for more than one service, please include details for each service below.

	Service Name (Will appear on CISPE Public Register)	**Further information** (Optional and will not appear on CISPE Public Register)
Service 1	[Insert]	[Insert]
Service 2	[Insert]	[Insert]
etc		

(2) CISP making the Declaration

This Declaration should be made by an entity which is a seller of record of the Service(s) (the "**CISP**"). If this Declaration is being made by more than one CISP, please include details for each CISP below and in the declaration at Section 5. This information will appear on the CISPE Public Register.

	Legal name	**Address**
Seller of Record 1	[Insert]	[Insert]
Seller of Record 2	[Insert]	[Insert]
etc		

(3) Declaration Process

This Declaration is made in accordance with the:

- Self-Assessment process.
- Controlled Adherence process.

Your choice will determine which Mark the CISP is eligible to use for the Service(s). In each case the supporting evidence must include a completed Compliance Checklist and demonstrate compliance by reference to the Compliance Checklist.

(4) Compliance Checklist

The Code Requirements listed in the Compliance Checklist as being auditable are the Auditable Code Requirements. Please attach the Compliance Checklist and copies of all referenced supporting documentation in respect of the Auditable Code Requirements.

Please indicate if supporting documents only apply to specific Services. If you are relying on different supporting documents for different services, you may complete the Compliance Checklist separately for each Service.

(5) Proposed Monitoring Body

Please insert the full name and address of your proposed Monitoring Body:

	Legal name	**Address**
Monitoring Body	[Insert]	[Insert]

(6) Monitoring Body Confirmation (for Declarations following the Controlled Adherence process only)

Please attach written confirmation from the Monitoring Body that the CISP service adheres to the Auditable Code Requirements. (Such confirmation should be signed by the relevant Monitoring Body.)

(7) Declaration

By signing below the CISP(s) confirms that:

(a) as of the date of this Declaration the Services adhere to the Code Requirements;

(b) if following the Self-Adherent Process, the CISP shall submit the Service for Monitoring Body review within 12 months of incorporation of this Declaration in the CISPE Public Register;

(c) the CISP shall comply with the Monitoring Body review, complaints and enforcement procedures in Section 7(Governance) of the Code; and

(d) if any change to the Service(s) or the Code means a material update to this Declaration is required, then (i) the CISP must promptly notify the Secretariat, and (ii) cooperate with the Secretariat to update those materials.

[CISP 1 NAME]

By: _____

Name: _____

Title: _____

Date: _____

[CISP 2 NAME]

By: _____

Name: _____

Title: _____

Date: _____

Annex D – EEA Supervisory Authorities

Austria	Österreichische Datenschutzbehörde
Belgium	Commission de la protection de la vie privée; Commissie voor de bescherming van de persoonlijke levenssfeer
Bulgaria	Commission for Personal Data Protection
Croatia	Croatian Personal Data Protection Agency
Cyprus	Commissioner for Personal Data Protection
Czech Republic	The Office for Personal Data Protection
Denmark	Datatilsynet
Estonia	Estonian Data Protection Inspectorate (Andmekaitse Inspektsioon)
Finland	Office of the Data Protection Ombudsman
France	Commission Nationale de l'Informatique et des Libertés – CNIL
Germany	Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Greece	Hellenic Data Protection Authority
Hungary	National Authority for Data Protection and Freedom of Information
Iceland	The Icelandic Data Protection Authority
Ireland	Data Protection Commissioner
Italy	Garante per la protezione dei dati personali
Latvia	Data State Inspectorate
Liechtenstein	Data Protection Office
Lithuania	State Data Protection
Luxembourg	Commission Nationale pour la Protection des Données
Malta	Office of the Data Protection Commissioner
Netherlands	Autoriteit Persoonsgegevens
Norway	Datatilsynet
Poland	The Bureau of the Inspector General for the Protection of Personal Data - GIODO
Portugal	Comissão Nacional de Protecção de Dados - CNPD
Romania	The National Supervisory Authority for Personal Data Processing
Slovakia	Office for Personal Data Protection of the Slovak Republic
Slovenia	Information Commissioner
Spain	Agencia de Protección de Datos

Sweden	Datainspektionen
United Kingdom	The Information Commissioner’s Office

Annex E – Summary of Stakeholder Consultations

CISPE's consultations have fallen into a number of categories: (i) internal consultation within CISPE membership (ii) consultation with CCTF task force established by CISPE to peer review the Code, with participation of external and industry experts (iii) regular exchanges with government and regulatory agencies (iv) holding and participating in public meetings (v) consultations with external data security experts and assurance/audit providers, including potential Monitoring Body candidates. These consultations have been carried on in the spirit of transparency and openness to improve the Code for the benefit of cloud infrastructure users.

1. Internal consultation within CISPE membership

CISPE has 27 members representing a range of sizes of enterprise with main establishments across more than 14 EU Member States. At each stage of the drafting of the Code, the members have been consulted on and asked to approve the latest draft.

In addition, a number of organisations are not members of CISPE, but have declared services to be adherent to the Code. At present over 107 cloud infrastructure services have been declared as adherent to the Code in its prior (unapproved) form. Discussions have taken place with a number of these adherent CISPs regarding the requirements of the Code. Adherent organisations have advertised their adherence to the Code, for instance on their company websites, and reactions from their customer base have been taken account of.

CISPE has also sought the external expertise of law firm Baker McKenzie in drafting the Code and assessing market positioning of the Code, including from the perspective of customer organisations.

Auditing firms recognized internationally have interacted with CISPE membership in developing the substance of the Code.

Analyst firms IDC and Gartner have interviewed CISPE membership about the development of the Code and its relevance to cloud infrastructure users in Europe and beyond. Both issued reports assessing the CISPE Code.

2. CCTF (Code of Conduct Task Force)

The Code of Conduct Task Force was established as statutory body within CISPE in early 2017 as a deliberate mechanism to enable peer review and external feedback on the Code as its drafting has evolved. The CCTF brings together: 1) representatives of CISPE members who were charged specifically with peer review of the Code from the perspective of the market (including from Dada, SolidHost, Ikoula, OVH, Outscale and Amazon Web Services);2) external experts not otherwise associated with CISPE who were asked to give their independent views (including from law firms, academics, data protection policy think tanks, ISPs, and cloud providers not members of CISPE. EuroCIO, the association of European CIOs has also accepted to become Observer in the CCTF.

The CCTF has met regularly and been consulted on all iterations of the Code drafting as it is has evolved since its formation, with meetings as follows:

22/5/2017 – Meeting of CCTF

First meeting of CCTF to review CISPE Code and provide feedback on latest draft.

23/06/2017 – CISPE CCTF Meeting with Guests

Meeting in Florence between CCTF members and Italian CISPE customers, including EuroCIO Italian chapter, to understand customers view on the CISPE Code.

.

20/10/2017 – CISPE CCTF Meeting

Meeting of CCTF in Spain to discuss CISPE Code latest draft and provide feedback on.

28/11/2017 - CISPE CCTF Meeting

Further meeting to discuss about the recent A29WP letter and specific aspects of the CISPE Code and provide feedback on areas for improvement.

17/12/2017 – CISPE Call with CCTF participation

Call with CCTF to discuss feedback from CCTF on draft CISPE Code.

08/01/2018 - CISPE CCTF Call

Discussion of specific aspects of the Code for improvement.

05/2/2018 – CISPE CCTF Call

Further detailed discussion of areas for improvement of the draft CISPE Code.

27/2/2018 – CISPE CCTF Call

Analysis and discussion of feedback from Article 29 Working Party on the draft CISPE Code and direction for further drafting improvements to the Code.

22/3/2018 – CISPE Joint Board and CCTF Meeting

Two day workshop to discuss further revisions to the draft CISPE Code in light of Article 29 Working Party feedbacks.

26/4/2018 - CISPE CCTF Call

Further detailed discussion of latest drafting iterations of CISPE Code and feedback to CISPE on specific elements.

3/5/2018 – CISPE CCTF Call

Further CCTF call to discuss drafting improvements to specific aspects of the Code.

28/6/2018 – CISPE CCTF Meeting

Meeting to discuss a new draft version of the Code addressing WP29 comments.

30/10/2018 - CISPE CCTF Meeting

Meeting to discuss in detail CNIL's comments on draft CISPE Code and potential improvements to address them, resulting in feedback to CISPE on drafting improvements.

10/04/2019 – CISPE CCTF Call

Call to discuss in detail CNIL's comments on draft CISPE Code and potential improvements to address them, resulting in feedback to CISPE on drafting improvements.

3. Consultations with government and regulatory agencies

Since the first drafts of the CISPE Code, numerous exchanges took place with representatives of Data Protection Authorities (DPAs), the European Commission, and Members States.

- **Data Protection Authorities**: CISPE and its members have interacted with numbers of DPAs in countries where CISPE members are headquartered and active. The Code has been specifically submitted for comment initially to the Article 29 Working Party in March 2017, which commented on it in February 2018. A hearing took place on specific elements with the Article 29 Working Party, in May 2018. The attendees included Supervisory Authorities from Italy, Sweden, France, Czech Republic, Hungary, Luxembourg, Germany, Netherland, United Kingdom, Spain, Latvia, Ireland, Greece as well as the European Data Protection Supervisor. The Code was then submitted for further informal feedback to the CNIL.

- **European Commission:** CISPE and its members have regularly interacted with European Commission officials on the CIPSE Code since February 2016. The Directorate Generals concerned include: DG JUST, DG CONNECT, DG GROW, DG IT and DG HOME.

- **Member States:** CISPE members have regularly met with Member States, in countries where they are operating, including France, Germany, Spain, Poland, Denmark/Nordic Council, UK, Ireland, Malta and Italy. CISPE was also invited to present the CISPE Code at the Germany-France Digital Summit on December 13th 2016.

4. Public Meetings

CISPE members have actively participated in, and presented the core concepts of the Code, in various general stakeholder meetings including the EC Digital Single Market (DSM) Cloud Stakeholder Group, the Cloud Select Industry Group meetings (CSIG), and cloud security workshops. These have been opportunities to discuss the content of the CISPE Code and obtain feedbacks from cloud users and other stakeholders.

Date	Location	Meeting	Comments
27 June 2016	Belgium, Brussels	EC Cloud Select Industry Group (CSIG)	First plenary meeting of the C-SIG group during which CISPE presented its draft CISPE Code.
27 Sept. 2016	Belgium, Brussels	European Parliament	Public announcement of the CISPE Code.
20 Sept. 2016	The Netherlands, Amsterdam	HostingCon	Public presentation of the CISPE Code.
24 Jan. 2017	France, Lille	International Forum on Cybercrime (FIC 2017)	Plenary session / GDPR panel. Presentation of the CISPE Code.
07 Feb. 2017	Belgium, Brussels	Xupery workshop "The GDPR : How codes of conduct will meet the challenges"	CISPE participated in the discussion and introduced the CISPE Code.
15 Feb. 2017	Belgium, Brussels	EC Cloud Select Industry Group (CSIG)	Presentation of the CISPE Code.
28. March 2017	Germany, Rust	World Hosting Days	Presentation of the CISPE Code.
27-30 March 2017	Germany, Rust	World Hosting Days	CISPE shared information about the CISPE Code.

25 April 2017	France, Paris	French Association of Healthcare Data Hosting Services Providers (AFHADS)	Presentation of the CISPE Code of Conduct.
14 June 2017	The Netherlands, Amsterdam	Board EuroCIO	Exchange of views on the CISPE Code.
23 June 2017	Italy, Florence	CISPE	Meeting with Italian cloud users.
29 June 2017	Belgium, Brussels	EC DSM Cloud Stakeholder Meeting	CISPE presented on the state of play of the CISPE Code.
05 July 2017	France, Paris	Cloud Week Paris	GDPR Panel Session. Presentation of the CISPE Code.
22 August 2017	Uruguay, Montevideo	Personal Data Protection Forum	Presentation of the CISPECode..
22 Sept. 2017	France, Paris	CYGAL/Systematic	Presentation of the CISPE Code .
17 Oct. 2017	France, Paris	OVH Summit	Market analysts working session on the CISPE Code.
6-7 Nov. 2017	Belgium, Brussels	IAPP Europe Data Protection Congress 2017	Presentation of the CISPE Code as part of two sessions: “Accountability Made Easy with the GDPR Tools” and .” Deciphering GDPR: DPIA, Data Breach Notification, Portability and Security"
17 Nov. 2017	Poland, Lodz	The Convent of Data Protection Poland	Presentation of the CISPE Code.
23 Nov. 2017	Denmark, Copenhagen	Cloud Forum Denmark	Presentation of the CISPE Code.
06 Dec. 2017	United Kingdom, London	FinTech Connect	Presentation of the CISPE Code.
07 Dec. 2017	Belgium, Brussels	EBF Cloud Banking Forum	Presentation of the CISPE Code in a panel session.
10 March 2018	Germany, Rust	Cloud Fest (previously World Hosting Days)	Presentation of the CISPE Code.
19 April 2018	France, Sophia Antipolis	ETSI	Summit – “Releasing the flow - data protection & privacy” Presentation of the CISPE Code ina panel session.
19 April 2018	Belgium, Brussels	AWS Public Sector Summit	Presentation of the CISPE Code during the session “GDPR: Security and data protection at the core of your strategy”.
20 Sept. 2018	France, Paris	Cloud study trip	Presentation of the CISPE Code tof Dutch and Danish cloud trade associations.
6 Dec. 2018	Austria, Vienna	EC DSM Cloud Stakeholder Group	Panel presentation on Codes of Conduct - Presentation of the CISPE Code

Annex F – Template of Security Breach Notification

This form can be used by a CISP to notify a security breach to its customers. This form is intended to be an example only, providing an illustration of the format and types of information which may be included in a CISP security breach notification to its customers. It is not mandatory for a CISP to use this template.

1. CISP Identification

Organisation name (CISP):

Registered organisation address:

Point of contact available to answer additional request concerning the beach:

Name:

Title:

Email:

Phone:

Data protection officer (only if appointed and if different from the point of contact):

Name:

Email:

Phone:

2. Nature of the Notification

Initial Notification:

Follow-up notification:

In case of follow-up report please provide the initial report date:

3. Description of the security breach

[Based on the information available to the CISP, provide details as to what occurred and/or what went wrong]

4. Consequences of the breach

[Based on the information available to the CISP, provide information on known/potential consequences of the breach]

5. Measures taken or proposed to be taken by the CISP in response to the breach

[Describe the steps/measures taken by the CISP and proposed additional measures to be taken by the CISP and the customer]

Annex G - Glossary

ACL means access control lists.

Auditable Code Requirements means those Code Requirements which are recognised in the industry as auditable and specified in the Compliance Checklist.

CCTF or **CISPE Code of Conduct Task Force** means a maximum of twelve individuals, appointed by CISP members, that have proven (i) expertise related to cloud computing and/or data protection, and/or (ii) understanding of cloud computing business models, as set out in sub-section 7.1 of the Code.

CISC, **Code Independent Supervisory Committee**, or **CISC Members** means the Code Independent Supervisory Committee which comprises three external individual experts drawn from academia, technical or legal background appointed by the Executive Board, as set out in sub-section 7.1 of the Code.

CISP Network means a CISP's data centre facilities, servers, networking equipment and host software systems that are within the CISP's control and are used to provide the CISP's service.

CISPE means the Association of Cloud Infrastructure Service Providers of Europe.

CISPE Public Register means the website listing the CISP's that have declared their adherence to this Code which can be found at https://cispe.cloud.

CISPs mean cloud infrastructure services providers.

Code means this Code of Conduct.

Code Requirements means the Data Protection Requirements and Transparency Requirements as set out in sections 4 and 5 of the Code.

Competent Authority means the independent data protection authority designated by each EU Member States to be responsible for monitoring the application of GDPR.

Complaints Process means the process set out in Section 7.2(a) of the Code whereby complaints from any customer, data subject, or any other CISP about the compliance of services with the Code Requirements will be addressed.

Compliance Checklist means the checklist set out in Annex B of the Code.

Compliance Mark Use Guidelines means the guidelines for the use of Mark by CISPs.

Compliance Mark means the public-facing symbol of a service's adherence to the Code Requirements.

Customer Data means personal data processed on behalf of a customer using a cloud infrastructure service.

Declaration of Adherence means the form set out at Annex C to the Code which a CISP must submit to confirm that its service complies with the Code Requirements.

Designated Supervisory Authority means the Supervisory Authority for the Code, which is Commission Nationale de l'Informatique et des Libertés (CNIL).

DPAs means data protection authorities.

DSM means the European Comission's Digital Single Market.

EEA means the European Economic Area.

Enforcement Matrix means the table set out in sub-section 7.2(b) of the Code.

Executive Board means the 5 to 10 representatives elected by the General Assembly, as set out in sub-section 7.1 of the Code

First Written Warning means the Monitoring Body's first written warning to a CISP if it makes an assessment that a CISP is not compliant with any requirement under the Code, as set out in sub-section 7.2(b) of the Code.

GDPR Requirement means requirements for processors under the GDPR.

General Assembly means the group of voting representatives from each CISP participating in the Code, as set out in sub-section 7.1 of the Code.

General Data Protection Regulation or **GDPR** means 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.

Host Operating Software means the software used by the CISP to provide the cloud infrastructure services to customers.

IaaS means infrastructure-as-a-service.

Mark(s) means the Compliance Mark and/or the Self-Adherent Mark.

Member State means a member state of the European Union.

Monitoring Body means the organisation appointed by a CISP from a list maintained by the CISC to monitor its compliance with the Code.

Monitoring Body Workshop means the annual workshops to be organised by the CISC and attended by Monitoring Bodies to discuss practical issues Monitoring Bodies have encountered in assessing the application of the Code.

Observers means representatives who are not affiliated with the General Assembly but are appointed by the Executive Board to participate as non-voting observers.

Report means the report generated by a Monitoring Body following each of its assessments of a CISP's Code compliance, which summarises its findings in relation to such compliance.

Requirement for CISP means the explanation of the relevant GDPR Requirement in the context of cloud infrastructure services.

SaaS means software-as-a-service.

Second Written Warning means the Monitoring Body's second written warning to a CISP if it makes an assessment that a CISP is not compliant with the requirements of the Code within 60 days following the CISP's receipt of a First Written Warning, as set out in sub-section 7.2(b) of the Code.

Secretariat means the body appointed by the Executive Board to manage the day-to-day administration of the Code.

Service Contract means the contract between the CISP and the customer which defines the features of the service, how it is delivered and the rights and obligations of the customer.

Services means the cloud infrastructure services specified in Annex C.

SMEs means small and medium enterprises.