Data Protection

Code of Conduct for Cloud Infrastructure Service Providers

DRAFT – 26 SEPTEMBER 2016

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 providing a variety of different cloud computing model. Data protection considerations do not 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 data it wants to process on the infrastructure, in which countries, for what purposes and how it wishes to protect this data. IaaS providers are unaware of whether their infrastructure is being used by customers to process personal data. Because of the nature of IaaS, IaaS providers are unable to tailor their services to any individual customer's use case. Instead, IaaS providers provide their services with the same level of security irrespective of whether or not personal data is actually processed by a customer on the IaaS provider's infrastructure.

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 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.

A 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 default level of data protection. This will benefit Small and Medium enterprises (**SMEs**), as users and providers, and public administrations in particular.

The Code consists of a set of requirements for CISPs as data processors in Section 5 (Data Protection Requirements) and Section 6 (Transparency Requirements) (together the **Code Requirements**). It also includes a governance structure at 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. This may be either (i) certification by an independent third party auditors, or (ii) self-assessment by the CISP and self-declaration of compliance.

CISPs that have demonstrated their adherence to the Code in accordance with its governance processes may use the Code's relevant compliance marks.

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

1 Structure of the Code

This Code is structured as follows:

- **Purpose:** describes the focus of the Code relative to applicable EU data protection law.
- **Scope:** describes the field of application of the Code.
- **Adherence:** describes the conditions for CISPs declaring adherence to the Code.
- **Data protection:** describes the substantive rights and obligations of adhering CISPs on the basis of key principles such as purpose limitations, data subject rights, transfers, security, auditing, liability, etc.
- **Security requirements:** describes how the adhering CISP demonstrates an adequate level of security for personal data.
- **Governance:** describes how the Code is managed, applied, and revised, including the roles and obligations of its governing bodies.

2 Purpose

The purpose of this Code is to 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:

- customers can use that service to process personal data in way that complies with applicable EU data protection law; and
- the CISP has met 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 EU data protection law. 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 a written agreement (the **Service Agreement**). CISPs should assess whether the then current Service Agreement that they offer new customers in connection with the services contradicts the Code Requirements especially before declaring their adherence.

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

3 Scope

The Code consists of a set of requirements for CISPs as data processors with a particular focus on security. These are set out in Section 5 (Data Protection Requirements) and Section 6 (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 service complies with the Code Requirements;
- in respect of that service, the CISP complies with all EU data protection laws which are applicable and binding on it, including the EU Data Protection Directive (and any applicable national transpositions thereof) and the General Data Protection Regulation (**GDPR**) when it comes into force; 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 only specific of its cloud infrastructure services as adhering to the Code Requirements. Such CISPs must ensure that potential customers are explicitly and unambiguously informed of the services adhering 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 5 (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). The Code Requirements sets out the principles which CISPs, as data processors, must respect.

The legal obligations of data controllers, as set out in applicable EU data protection law, 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 explain how CISPs, 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 data processed on behalf of a customer using the cloud infrastructure service, the CISP will 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, in particular,

for the purposes of data mining, profiling or direct marketing.

The CISP may act as a data controller in respect of certain personal data provided by the customer to the CISP. 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.

4 Adherence

A CISP that declares adherence with the Code will comply with all the Code Requirements for any service covered by its declaration. CISPs cannot declare to adhere to only a chosen part of the Code Requirements or to exclude certain sections of the Code Requirements.

CISPs can declare their adherence to the Code either through:

- undergoing an independent third party audit and certification; or
- until the entry into force of the GDPR, a self-assessment by the CISP followed by a self-declaration of adherence.

The CISP must inform potential customers of which of the above processes it chose to declare its adherence with the Code.

The CISPs that have declared adherence to the Code commit to submit to Section 7 (Governance) of the Code. If a CISP fails to meet the Code Requirements, it will be subject to the enforcement mechanisms as set out in Section 7 (Governance). This is without prejudice to any possible sanctions from competent supervisory authorities under applicable EU data protection law.

5 Data Protection Requirements

EU data protection law makes a distinction between (a) the "data controller" – the party which determines the purposes and means of the processing of personal data, and (b) a "data processor" – a party which processes personal data on behalf of the controller.

CISPs provide self-service, on-demand infrastructure that is completely under the customers' control – including with respect to whether any personal data is uploaded to the cloud infrastructure service and, if so, how that personal data is "processed".

Customer as controller or processor

Cloud infrastructure services are used as part of a variety of different business operations, and there may be multiple parties involved in a chain of supply. As a general guide, however, where a customer stores or otherwise processes personal data using a CISP's services:

- The customer will be the controller in relation to that personal data if the customer determines the purpose for which the data will be processed and has chosen how it will be processed.

- The customer will be a processor in relation to that personal data if the customer is merely processing the personal data on the CISP's service on behalf of and according to the wishes of a third party (who may be the controller or another third party in the supply chain).

CISP as processor

Where the customer chooses to store or otherwise process personal data using a CISP's services, the CISP will be that customer's processor.

The purpose of this Data Protection Requirements section of the Code

The purpose of this Section 5 (Data Protection Requirements) is to clarify the CISP's role as a processor under applicable EU data protection law in the context of cloud infrastructure services.

The Code pursues this objective by:

(a) identifying requirements for processors under applicable EU data protection law (the **DP requirement**); and

(b) applying the DP requirement to the cloud infrastructure services context, 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**).

In addition to the Code, CISPs and customers are encouraged to consider all the requirements of applicable EU data protection law in their provision and use of cloud infrastructure services, respectively.

A key objective of the Code is that it will address the key requirements for CISPs under then current EU data protection law. In particular, this includes the GDPR when it comes into force and requirements in the Code are defined by reference to the GDPR. The Code will 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).

5.1 Processing Personal Data lawfully

DP requirement:

The **controller** must ensure that personal data is processed lawfully. Processing is lawful only if certain conditions apply. Except where required to comply with law, the **processor** may process personal data only on documented instructions from the controller (GDPR Art 28(3)(a)).

Requirement for CISP:

The CISP will process personal data in accordance with the customer's instructions. The Service Agreement 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.

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, for what purpose and if/how it is protected. Accordingly, CISPs are not able to ascertain whether there may be a lawful basis for the processing. As such, their responsibility is limited to (a) complying with the customer's instructions as provided for or reflected in the Service Agreement and (b) providing information about the service in accordance with Section 6 (Transparency Requirements) of the Code.

5.2 Contractual terms and conditions of the CISP's services

DP requirement:

Processing by a processor shall be governed by a written contract that is binding between the **processor** and 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. The contract may be in electronic form. (GDPR Art 28(3)).

Requirement for CISP:

The CISP shall define the features of the service and how it is delivered and the rights and obligations of the customer in the Service Agreement as set out in sections (a) and (b) below.

CISPs provide 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 infrastructure whenever they wish.

(a) Description of processing

To facilitate these features of cloud infrastructure services and to avoid the need to amend the Service Agreement or enter a new Service Agreement 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 Agreement should be drafted in a way that accommodates customers changing their use cases.

For flexibility, Service Agreements 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".

(b) Form of Service Agreement

Provided it is in writing (including in electronic form) and legally binding between the CISP and the customer, the Service Agreement may take any form, 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.

5.3 Security

DP requirement:

Both controller and processor must, 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, 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 will implement and maintain appropriate technical and organisational measures for the 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 (the **CISP Network**). Those technical and organisational measures should be designed to help customers secure personal data against unauthorized processing and accidental or unlawful loss, access or disclosure.

Cloud infrastructure services are 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.

At the same time, the CISP is not solely responsible for security in the context of a customer's use of the cloud infrastructure service. There are certain key aspects of security that are the customer's responsibility (and not the CISP's responsibility). For example, the customer (and not the CISP) is responsible for the security of guest operating systems, applications hosted on the service, data in transit and at rest, customer's service log-in credentials and permissions policies for customer personnel using the service.

Annex A (Security Responsibilities) defines the security responsibilities of (a) the CISP, and (b) the customer in the context of a cloud infrastructure service.

Customers should review (a) the information made available by the CISP relating to data security in respect of the services (see Section 6 (Transparency Requirements) below), (b) 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 (c) the security measures that the 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 service to perform. This determination should be based on the nature, scope, context and purposes of the customer's intended processing.

Because it is the customer who decides what processing (i.e. what data and for what purposes) it will use the service to perform, only the customer can determine what level of security is "appropriate" for the personal data it stores and processes using the service. The CISP is not in a position to make this assessment because the CISP does not monitor, limit or otherwise control what processing the customer may use the service to perform.

(b) Information security program

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

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

(c) Continued evaluation

The CISP will 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. The CISP will 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 the CISP's security standards from time to time, but will continue throughout the term of the Service Agreement 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 Agreement.

5.4 Transfer of personal data to third countries

DP requirement:

Both **controller and processor** must ensure that any transfer of personal data undergoing processing to a third country shall take place only if certain conditions under applicable EU data protection law are complied with (GDPR Art 44).

Requirement for CISP:

(a) Location

The cloud infrastructure service will provide the customer the ability to choose to use the service to store and process its data entirely within the EEA.

(b) Information

The CISP will provide to the customer information about the region and country where its data is stored and processed by or on behalf of the CISP, including if the CISP sub-contracts part of the processing to third parties.

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.

If necessary to discharge a competent supervisory authority's obligations under applicable law in respect of the customer's use of the service and provided that the information is protected by adequate confidentiality obligations binding on the authority, the CISP shall communicate to the competent supervisory authority the exact address of the relevant facilities.

For services which can be run indifferently within several different locations in the CISP Network, CISPs will make the information easily accessible to the customer and enable customers to select the location(s) within the CISP Network where their data will be processed.

(c) Level of protection

The CISP will implement or otherwise make available to customers a recognized compliance standard under applicable EU data protection law for the lawful transfer of personal data to the relevant country (including, for example, the EU Standard Contractual Clauses, Binding Corporate Rules or the EU-US Privacy Shield for transfers of personal data to the United States of America) if:

i. the customer transfers data from within the EEA to be stored using the CISP's service in any country outside the EEA which is not recognized by the European Commission as providing an adequate level of protection for personal data; or
ii. the CISP is authorized to access data stored using the CISP's service within the EEA from such country referred to in (i) above.

5.5 Sub-processing

DP 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 the intended changes giving the controller the opportunity to object (GDPR Art 28(2)).

The **processor** must impose the same obligations as required under applicable EU data

protection law in the contract with its controller with its sub-processors. The **processor** must remain fully responsible to the controller for the performance of their sub-processor's obligations (GDPR Art 28(4)).

Requirement for CISP:

(a) Consent

Subject to applicable law, the CISP shall obtain the customer's consent before authorising a third party sub-processor to access and process customer data.

The customer's consent may be given generally through the Service Agreement. In particular, the Service Agreement may 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 additional consents from the customer.

If the customer objects to a sub-processor, the customer may immediately terminate the Service Agreement 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 authorised by the CISP to access 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 Agreement and during its term. 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.

Before authorising a new sub-processor to access customer data, the CISP will make available to the customer the information about that new sub-processor specified in the paragraph above.

(c) Sub-processing arrangements

The CISP will impose data protection contractual obligations equivalent to those set out in the Service Agreement 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 an equivalent level of data protection to the level of data protection under the Service Agreement. 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 responsible for its compliance with its data protection obligations in the Service Agreement and for any acts or omissions of the sub-processor that cause the CISP to breach any of its obligations under the Service Agreement.

Notwithstanding sub-sections (a) - (c) above, and subject to applicable law, CISPs may freely use subcontractors or suppliers (such as energy suppliers, equipment suppliers, transport, technical service providers, IP Carriers, transit providers, hardware vendors, etc.) to perform its duties under the Service Agreement without having to inform or seek prior authorisation from the customer, provided that such subcontractors or suppliers are not authorised to access nor process customer data.

5.6 Demonstrating compliance

DP requirement:

The **processor** must make available to the controller all information necessary to demonstrate the processor's compliance with its data protection obligations and allow for audits, including inspections, conducted by the controller or an auditor mandated by the controller (GDPR Art 28(3)(h)).

Requirement for CISP:

(a) Information

CISPs shall make sufficient information about the security controls 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 Agreement.

Where information is non-confidential or non-sensitive it will 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 which is acceptable to the CISP. The CISP may in its sole discretion choose not to disclose certain high-sensitive security information.

CISPs may require customers to pay an additional fee for information. This additional fee will be reasonable and will not be used to prevent customers from accessing information about the security controls for the service.

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 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. Mechanisms should be appropriate and proportionate for the cloud infrastructure service in question and 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.

(b) Audit

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

If offered by the CISP, these audits:

- will be performed according to a recognised security standard (including, for example, ISO 27001);
- will be performed periodically as provided under the applicable standard;
- will be performed by qualified and reputable independent third party security professionals; and
- will result in the generation of an audit report.

If the CISP uses independent third party auditors to verify the adequacy of the security controls that apply to the service, then at customer's written request the CISP may provide the customer with a copy of the audit report so that the customer, the customer's auditor and competent supervisory authorities with jurisdiction over the customer can reasonably audit and verify the CISP's compliance with its security obligations under the Service Agreement. The CISP may choose to charge customers an additional fee for the provision of the audit report provided such fee should not be used as a deterrent.

The report will be the CISP's confidential information. Before sharing the report with customer, the CISP may require the customer to first execute a non-disclosure agreement which is acceptable to the CISP.

The Code does not require the CISP to authorise the customer or any third party to conduct an on-site audit of the CISP's premises or facilities. 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, instead of an on-site audit, customers use the information provided by the CISP to reasonably verify the CISP's compliance with the security obligations in the Service

Agreement.

5.7 Data Subject requests

DP requirement:

Taking into account the nature of the processing, the **processor** must assist 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 data subject's rights (GDPR Art 28(3)(e)).

Requirement for CISP:

The CISP will provide the customer with the ability to rectify, erase, restrict or retrieve customer data. The customer may use this ability to assist customer in the fulfilment of its obligations to respond to requests for exercising data subject's rights.

The CISP may provide the customer with the ability to rectify, erase, restrict or retrieve customer data (a) as part of the service, or (b) by enabling customers to design and deploy their own solutions using the service.

Beyond providing the customer the ability to rectify, erase, restrict or retrieve customer data, the CISP is not required to provide further assistance to the customer with data subject requests. This is because the customer (and not the CISP) is responsible for managing data processed by the customer using the service. Therefore, the CISP does not know what data customers are uploading to the service and, in particular, who are the data subjects of that data.

5.8 CISP personnel

DP requirement:

Processors must ensure that persons authorised by the processor 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:

Confidentiality:

The CISP will impose appropriate contractual obligations regarding confidentiality on any personnel authorised by the CISP to access customer data.

Access controls:

The CISP will implement and maintain access controls and policies in order to restrict CISP personnel processing customer data to those CISP personnel who need to process customer data to provide the services to the customer. When CISP personnel no longer need to process customer data, the CISP will promptly revoke that personnel's access privileges.

5.9 Law enforcement/governmental requests

DP requirement:

Processors may only give effect to a court judgment or administrative decision of a third country requiring personal data to be transferred or disclosed if based on an international agreement (e.g. MLAT) between that third country and the EU or a Member State (GDPR Art 48).

Requirement for CISP:

The CISP will not disclose customer data to a third country law enforcement agency unless it is necessary to comply with a valid and legally binding court judgment, order or request. The CISP will not disclose more customer data than is necessary to comply with the relevant court judgment, order or request.

If the CISP receives a valid and legally binding court judgment or order or request from any law enforcement or governmental authority to disclose customer data, then, unless prohibited by law, the CISP will inform the customer before disclosure to provide the customer with the opportunity to seek protection from disclosure.

The CISP may maintain public guidelines intended for use by law enforcement when seeking information from the CISP and produce at least annual reports on the types and volume of information requests the CISP has processed.

5.10 Data breach

DP requirement:

Processors must notify a data breach to the controller without undue delay after becoming aware of it (GDPR Art 33(2)).

Taking into account the nature of the processing and the information available to the processor, the **processor** must assist the controller in ensuring compliance with its obligations to notify data breach to the supervisory authority and data subjects (GDPR Art 28(3)(f)).

Requirement for CISP:

Security incident management policy

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

This policy will include:

- guidance for deciding which type of incidents have to be notified to the customer based on the potential impact on data;
- guidance on how incidents should be addressed; and
- a specification of the information to be made available to the customer following the data breach incident.

Security breach notification

Scope and timing of notification

If the CISP becomes aware of unauthorised access to any customer personal data on the CISP's equipment or in the CISP's facilities and such unauthorised access results in loss, disclosure or alteration of that data, the CISP will notify the customer without undue delay.

Content of notice

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.

5.11 Deletion or return of personal data

DP Requirement:

At the controller's option, the **processor** must delete or return all personal data to the controller (and delete existing copies) at the end of service provision (GDPR Art 28(3)(g)).

Requirement of CISP:

The CISP will provide the customer with the ability to retrieve and delete customer data. The customer may use this ability to retrieve or delete customer data at the end of service provision.

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 does not manage or choose to delete a customer's data on the customer's behalf. Nor is the CISP required to provide the customer with exit assistance beyond the ability for the customer to retrieve or delete the customer's data. 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 Agreement.

6 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 can 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 will pursue the following 6 objectives:

1. A Service Agreement 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 and criteria of the CISP for the service.

5. Information on the security measures implemented by the CISP for the service.

6. Assurance documentation covering the CISP's information security management system.

The sub-sections below describe what steps the CISP should 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 6 objectives. The Code encourages CISPs to implement such information security management systems based on one or more recognised industry standards.

Except for requirements specifically for the Service Agreement, the CISP may choose to communicate the information referred to in this Section 6 (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 which is acceptable to the CISP.

6.1 A Service Agreement that addresses the division of responsibilities between the CISP and the Customer for the security of the service

The Service Agreement should define the security responsibilities of the CISP and the customer for the duration of the term of the Service Agreement provided that the customer shall remain responsible for any aspect of security which is not covered by the Service Agreement.

In addition to the Service Agreement, 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.

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

The CISP should 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.

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 Agreement.

The CISP will 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 Agreement, a service description and/or via the CISP's website or other publicly available material.

6.3 Information on the design and management of the service

The CISP should 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
- 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

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

The CISP should provide information to customers validating the existence and suitability of the CISP's risk management program 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.

6.5 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.

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 should 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.

This information may, for example, include information about:

- physical and environmental security;
- network security;
- business continuity management;
- change management; and

- account security features.

6.6 Assurance 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 Agreement as described in Section 5.6 (Data Protection; Demonstrating Compliance) of this Code.

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 diagram below provides 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 within 6 months of joining the General Assembly.

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 13 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 membermust 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) compliance marks, (c) the Code complaints process, (d) enforcement action for non-compliance of services adhering to the Code, (e) guidelines for adherence to the Code, and (f) reviews and changes to the Code. Appoints: (a) non-voting representatives of the CCTF, (b) the Complaints Committee, (b) the Secretariat, and (c) 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. 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).

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; recommend auditors, norms and certification schemes suitable for demonstrating adherence to the Code by entities; develop compliance marks; and develop compliance mark use guidelines.

Complaints Committee	Secretariat	Observers
Representation: Appointed by the Executive Board. **Key responsibilities:** (a) consider complaints about non-compliance of services with the Code, and (b) take enforcement action against a non-compliant CISP and, where necessary, recommend enforcement action to the Executive Board.	**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.	The Executive Board may invite representatives who are not affiliated with General Assembly members to participate as non-voting observers.

7.2 Declaration of Adherence of a service to the Code

(a) Declarations of Adherence

To use Compliance Marks (as defined in Section 7.3 below) for a service the CISP must complete and submit a declaration of adherence (**Declaration of Adherence**) in accordance with the guidelines for adherence to the Code produced by the CCTF and approved by the Executive Board (**Code Adherence Guidelines**). The current form of the Deed of Adherence is set out in Annex B. This may be updated by the CCTF from time to time. The Secretariat will publish and maintain an up to date version of the Declaraction of Adherence and the Code Adherence Guidelines on the CISPE Public Register.

The Declaration of Adherence confirms that the service complies with the Code Requirements.

The CISP's Declaration of Adherence must be supported by evidence of the adherence of the service to the Code Requirements. The CISP may choose between the following two evidential procedures:

- Certification by an independent third party auditor; or
- Self-assessment by the CISP.

Different Compliance Marks apply to Declarations of Adherence supported by each of these two procedures. Both procedures are explained in more detail in sub-sections (b) and (c) below.

The Secretariat shall review a CISP's Declaration of Adherence according to the Code Adherence Guidelines. Within 40 working days of receipt by the Secretariat of the Declaration of Adherence, the Secretariat will notify the CISP whether the Declaration of Adherence is complete.

If the Declaration of Adherence is not complete, the Secretariat may request that the CISP provide any missing document or information required to complete its Declaration of Adherence.

If the Declaration of Adherence is complete, the Secretariat shall incorporate the Declaration of Adherence into the CISPE Public Register within 10 working days of the CCTF 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 appropriate Compliance Mark, as noted in Section 7.3 below, exclusively for the services

covered by the Declaration of Adherence so long as it remains valid and subject to any enforcement measures under Section 7.4 (Complaints and Enforcement); and

- if any change to the service means a material update to the CISP's current Declaration of Adherence is required, then (i) the CISP must promptly notify the Secretariat, and (ii) cooperate with the Secretariat to update those materials.

(b) Certification by independent third party auditors

Process

A CISP can show that one or more of its services adhere to those Code Requirements which are technical and operational security and/or data protection behaviours which are recognised in the industry as auditable and as specified in the Code Adherence Guidelines (**Auditable Code Requirements**) by presenting one or more appropriate certificates covering all the Auditable Code Requirements for those services and prepared by an independent third party auditor (**Certificate**).

A CISP which chooses this procedure must submit a Certificate(s) covering all the Auditable Code Requirements together with its Declaration of Adherence to the CCTF Secretariat in accordance with the Code Adherence Guidelines. The CISP must also submit any supporting information specified in the Code Adherence Guidelines in respect of those Code Requirements which are not Auditable Code Requirements.

A CISP must obtain a Certificate by engaging one or more qualified and reputable audit and professional accountancy firms to perform an audit and prepare one or more reports or certificates on the compliance of the relevant service(s) with one or more recognised industry norms and/or certifications schemes which cover all the Auditable Code Requirements. The reports or certificates prepared by the approved auditor(s) will amount to a Certificate for the purposes of this section of the Code.

Where the CISP holds an existing certificate or report covering a service satisfying the requirements in the paragraph above, then the CISP may rely on that existing certificate or report as a Certificate to show that the service(s) adheres to the Auditable Code Requirements without having to undergo a new or separate audit to obtain a new certificate or report.

The CCTF may recommend certain audit and professional accountancy firms and/or industry norms or certification schemes for generating a Certificate. If so, the Secretariat will publish and maintain a list of such firms and/or norms and certification schemes on the CISPE Public Register. However, this will not prevent the CISP from relying on other firms or

norms and certification schemes.

Renewal

A Declaration of Adherence obtained via Certificate is only valid for one year from the date it is incorporated into the CISPE Public Register.

However, if neither the service covered by the original Certificate nor the Code have been materially modified since the Certificate was issued, the CISP can automatically extend the validity of the Declaration of Adherence by an additional year at no cost, by confirming the continued accuracy of the Certificate and the supporting information provided with that Certificate (if any) to the Secretariat.

In other cases, to continue to use the Compliance Mark, a CISP relying on a Declaration of Adherence obtained via Certificate must renew that Declaration of Adherence each year.

(c) Self-assessment by the CISP

Process

A CISP can show that one or more of its services adhere to the Code Requirements by completing a self-assessment in accordance with the Code Adherence Guidelines

A CISP which chooses this procedure must submit its Declaration of Adherence to the Secretariat together with any required supporting information in accordance with the Code Adherence Guidelines.

Renewal

A Declaration of Adherence obtained via self-assessment is only valid for one year from the date it is incorporated into the CISPE Public Register.

To continue to use the Compliance Mark, a CISP relying on a Declaration of Adherence obtained via self-assessment must renew that Declaration of Adherence each year.

7.3 Compliance Marks

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

To increase transparency for customers, the CCTF will develop at least two visually different Compliance Marks to distinguish between CISPs who have evidenced the adherence of their service to the Code Requirements by: (a) certification by an independent third party auditor, and (b) self-assessment by the CISP.

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

Once the CISP's Declaration of Adherence is incorporated into the CISPE Public Register, the CISP will be entitled to use the appropriate Compliance Mark so long as its Declaration of Adherence remains valid and provided that the CISP uses the Compliance Marks: (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 Compliance Mark unambiguously identifies the specific services covered by the CISP's Declaration of Adherence.

7.4 Complaints and Enforcement

(a) Complaints Committee

The Executive Board will appoint a Complaints Committee. The Complaints Committee will be responsible for: (a) considering complaints about the compliance of services covered by a CISP's Declaration of Adherence with the Code Requirements, and (b) taking enforcement action against a non-compliant CISP and, where necessary, recommending such enforcement action to the Executive Board.

(b) Complaints Process

The Complaints Committee will propose to the Executive Board rules and a process to make, decide, appeal and publish complaints about the compliance of services covered by a CISP's Declaration of Adherence with the Code Requirements (**Complaints Process**).

Once approved by the Executive Board, the Complaints Committee will publish, implement and administer and keep under review the Complaints Process. The Secretariat will publish and maintain up to date information on the Complaints Process on the CISPE Public Register

A CISPE member, a customer or a competent supervisory authority can make a complaint to the Complaints Committee in accordance with the Complaints Process. The Complaints

Committee shall review and decide on that complaint in accordance with the Complaints Process.

(c) Enforcement

If in its final decision the Complaints Committee finds that a CISP is non-compliant with the Code Requirements, then the Complaints Committee may:

- request the CISP to take specific remediating measures within a reasonable timeframe to comply the Code; and
- in extreme or repeated cases of non-compliance, or in case of failure by the CISP to implement the requested remediating measures (at all or in time), recommend to the Executive Board that the CISP's Declaration of Adherence be suspended or revoked in respect of the non-compliant service.

If a CISP's Declaration of Adherence is suspended or revoked:

- the Secretariat shall promptly remove the affected service(s) from the CISP's Declaration of Adherence on the CISPE Public Register;
- the Complaints Committee shall specify a reasonable timeframe for when the CISP must stop using the Compliance Mark in respect of the relevant service; and
- the CISP shall stop using the Compliance Mark in respect of the relevant service within the timeframe specified by the Complaints Committee.

In the case of suspension, these measures shall apply until such suspension is lifted.

The enforcement measures above are:

- the sole and exclusive remedies for a CISP's non-compliance with the Code Requirements; and
- are without prejudice to the customer’s rights under applicable EU data protection law or the Service Agreement.

The option for a customer to make a complaint does not 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.

7.5 Review of the Code and Guidelines

(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 coming into force of the GDPR.

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.

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 competent supervisory authority acting in an official capacity; or
- an association representing the interests of cloud infrastructure service users acting in an official capacity.

(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 may decide to submit a change to the Code for consideration and comment to:

- a competent supervisory authority; and/or
- 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 a Certificate together with its Declaration of Adherence may rely on an existing Certificate 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 certificate or report.

ANNEX A

Security Responsibilities

Introduction

This Annex defines the security responsibilities of (a) the CISP, and (b) the customer in the context of a cloud infrastructure service.

The CISP is responsible for the cloud infrastructure service it provides and not the systems and applications deployed by the customer using the cloud infrastructure service, which are the customer's responsibility.

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

(b) Customer responsibilities

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

The customer shall 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.

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.

(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).

User Access Management

(a) CISP responsibilities

The CISP shall provide the customer with an access control management system for the cloud infrastructure service as part of the service. The access control management system shall include nominative accounts, role based access and passwords or other authentication policy means.

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 shall be 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.

Physical and environmental security

(a) CISP responsibilities

The CISP shall implement and maintain physical and environmental security measures for the cloud infrastructure service designed to help customers secure personal data against unauthorised processing and accidental or unlawful loss, access or disclosure.

(b) Customer responsibilities

Customers shall 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.

Physical servers and equipment

(a) CISP responsibilities

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

(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.

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.

Vulnerability management

(a) CISP responsibilities

The CISP shall define the level of engagement (distribution of tasks between CISP, delay between patch and patching, etc.) for the cloud infrastructure service.

(b) Customer responsibilities

The Customer is responsible for vulnerability management the systems and applications deployed by the customer and hosted on the cloud infrastructure service.

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 for the cloud infrastructure service.

(b) Customer responsibilities

The customer is solely responsible for the use and configuration of the monitoring and

logging tools provided by the CISP.

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. The decommissioning process will be conducted in accordance with industry standard practices 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

Customers shall 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.

ANNEX B

Template Declaration of Adherence

A. **Declaration**

The CISP identified in Section B formally declares that:

i. the service(s) identified in Section C adhere to the Code Requirements; and
ii. the information referenced in Section D and contained in this Declaration is accurate.

The CISP will ensure that this Declaration will be updated as necessary to ensure it is up to date.

B. Identification of the CISP

[Name, legal form, seat of establishment, VAT number]

C. CISP services covered by this Declaration

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

D. **Supporting evidence provided by the CISP**

This Declaration is supported by:

[A self-assessment by the CISP in accordance with the Code Adherence Guidelines. The supporting information specified in the Code Adherence Guidelines is attached at the Annex to this Declaration.]OR

[Certification by an independent third party auditor. The relevant Certificate(s) are attached at the Annex to this Declaration. The relevant information is as follows:

- Certificate 1: Prepared by [name of independent third party auditors] under [name of norm or certification scheme] and is valid from [date].
- Certificate 2: Prepared by [name of independent third party auditors] under [name of norm or certification scheme] and is valid from [date].]
- Etc.

The supporting information (if any) specified in the Code Adherence Guidelines is attached at the Annex to this Declaration.]

Annex to Declaration of Adherence

[Insert supporting evidence]