EUSEC
EU SECURITY CERTIFICATION

EUROPEAN SECURITY CERTIFICATION FRAMEWORK

D2.3 PRIVACY CODE OF CONDUCT

VERSION: 1.2

PROJECT NUMBER: 731845

PROJECT TITLE: EU-SEC

DUE DATE:	DELIVERY DATE:
September 30, 2017	December 19, 2018
AUTHORS: ELEFTHERIOS SKOUTARIS, CSA DAMIR SAVANOVIC, CSA DANIELE CATTEDDU, CSA	PARTNERS CONTRIBUTED: PWC GERMANY
DISSEMINATION LEVEL:* PU	NATURE OF THE DELIVERABLE:** R
INTERNAL REVIEWERS: SI-MPA	
*PU = Public, CO = Confidential O = Other	**R = Report, P = Prototype, D = Demonstrator,

This project has received funding This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845

VERSIONING

Version	Date	Comment	Name, Organisation
1.0	30/09/2017	Initial version	Damir Savanovic, Daniele Catteddu, Eleftherios Skoutaris (CSA)
1.1	14/12/2018	Minor editorial changes	Damir Savanovic, Eleftherios Skoutaris (CSA)
1.2	20/05/2019	Content update	Damir Savanovic, Eleftherios Skoutaris (CSA)

EXECUTIVE SUMMARY

The Privacy Level Agreement (PLA) Code of Conduct (CoC) was developed with a twofold objective in mind. The first goal was to provide a guidance and a compliance tool to cloud service providers that need to adhere to the requirements of the General Data Protection Regulation (GDPR). The second goal was to offer to cloud customers a mechanism to evaluate the privacy posture of a cloud service provider and the level of privacy that could be offered by a cloud service.

More in general the PLA CoC aims at increasing the level of transparency and accountability from the privacy and security point of view.

The PLA CoC will play a fundamental role in the context of the EU-SEC framework since it will be the tool that helps addressing one of the main limitations of existing certifications for cloud services, i.e., focusing almost exclusively on information security and not providing a means to show compliance with privacy requirements.

Moreover, it is meant to offer a free tool for those organizations seeking guidance when assessing their level of adherence to GDPR requirements as well as a mechanism of compliance.

PLA CoC is composed of two essential components. The first is the PLA Code of Practice (CoP), which can be considered as the "technical standard" and includes a set of controls that a Cloud Service Provider (CSP) should implement in order to establish adherence to the GDPR requirements. The second component is the governance structure, which describes the governance bodies and the processes in place in order to guide the revision of the PLA technical document, to drive and monitor the mechanisms of adherence to the PLA CoC.

The governance structure plays a key role within the PLA CoC as it ensures consistency, control and proper implementation of the changes required following the possible evolution of the regulatory landscape. In addition, it defines accurately the "if", "when", "how" and by "whom" such changes should be applied to the PLA CoC and related documents and finally aims at ensuring that there is an oversight over the PLA CoC adherence process.

The PLA CoC is a voluntary mechanism of adherence to GDPR requirements and transparency and will provide two levels of assurance, i.e. a PLA CoC Self Attestation and PLA CoC third party certification.

DISCLAIMER

The information and views set out in this publication are those of the author(s) and do not necessarily reflect the official opinion of the European Communities. Neither the European Union institutions and bodies nor any person acting on their behalf may be held responsible for the use which may be made of the information contained therein.

The Cloud Security Alliance PLA Code of Conduct is owned by the Cloud Security Alliance and it is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License (CC-BY-NC-ND 4.0).

The present document represents a derivative of the CSA PLA CoC.

ABBREVIATIONS

AB	(EU-SEC) Advisory Board
AICPA	American Institute of Certified Public Accountants
ANSSI	Agence nationale de la sécurité des systèmes d'information (en. National Cybersecurity Agency of France)
ASEC	AICPA Assurance Services Executive Committee
B2B	Business-to-Business
B2C	Business-to-Consumer
CCM	Cloud Control Matrix
CCRA	Cloud Computing Risk Assessment
CCSM	Cloud Certification Schemes Meta framework
CISPE	Cloud Infrastructure Service Providers in Europe
COBIT	Control Objectives for Information and related Technology (Formerly known as Control Objectives for Information and related Technology (COBIT); now used only as the acronym in its fifth iteration – COBIT 5)
CoC	Code of Conduct
CoP	Code of Practice
CPA	Certified Public Accountant
CSA	Cloud Security Alliance
CSP	Cloud Service Provider
D2.3	Deliverable 2.3 (D2.3 Privacy Code of Conduct)
DPA	Data Protection Authorities
DPO	Data Protection Officer
DSP	Digital Service Provider

EEA	European Economic Area
ENISA	European Union Agency for Network and Information Security
ETSI	European Telecommunications Standards Institute
EU	European Union
EU-SEC	European Security Certification Framework
GDPR	General Data Protection Regulation
IaaS	Infrastructure as a Service
ICT	Information and communication technology
ISO Officer	International Organization for Standardization / Information Security
IT	Information technology
NIS Directive	Directive on security of network and information systems
NIST	National Institute of Standards and Technology
PA	Public administration
PaaS	Platform as a Service
PII	Personally Identifiable Information
PLA	Privacy Level Agreement
SaaS	Software as a Service
SECaaS	Security as a Service
SLA	Service Level Agreement
STAR	Security, Trust & Assurance Registry
TSC	Trust Services Criteria
TSP	Trust Services Principles

TABLE OF CONTENTS

LIST OF FIGURES

TERMINOLOGY AND DEFINITIONS

The deliverable D2.1 uses following terminology. Each used term is explained, while existing defined terms have reference to original standard definition.

Table 1. Terms and definitions.

Term	Definition	Source
Accreditation	Accreditation assures users of the competence and impartiality of the body accredited.	http://www.iaf.nu/
Assessment	Refers in this document to risk assessment, which overall process of *risk identification [ISO Guide 73:2009, definition 3.5.1], risk analysis [ISO Guide 73:2009, definition 3.6.1]* and *risk evaluation [ISO Guide 73:2009, definition 3.7.1]*.	ISO Guide 73:2009, definition 3.4.1
Attestation	An issue of a statement that conveys the assurance that the specified requirements have been fulfilled. Such an assurance does not, of itself, afford contractual or other legal guarantees.	ISO 17000:2004, 5.2
Audit	a systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled	ISO/IEC 19011:2011, 3.1
Audit criteria	Set of policies, procedures or requirements used as a reference against which *audit evidence* is compared Note 1: Policies, procedures and requirements include any relevant Service Qualitative Objectives (SQOs) or Service Level Objectives (SLOs).	ISO/IEC 19011:2011, 3.2

Term	Definition	Source
Audit evidence	Records, statements of fact or other information which are relevant to the *audit criteria* and verifiable. Note: Audit evidence can be qualitative (e.g. a document) or quantitative (e.g. KPIs, thresholds, etc.)	ISO 9000:2005, definition 3.9.4
Auditee	Organization being audited.	ISO 9000:2005, definition 3.9.8
Auditor	Person who conducts an audit.	ISO/IEC 19011:2011, definition 3.8
Authority	A trusted party that is responsible for the correct organization of a certification scheme, including the accreditation of auditors and keeping a registry of certified cloud services.	
Authorized Auditor	An auditing organization/auditor authorized by the certification authority/scheme owner to conduct assessments against the requirements of the scheme. A certification body is considered as an authorized auditor.	
Certification	The provision by an independent body of written assurance (a certificate) that the product, service or system in question meets specific requirements.	https://www.iso.org/certification.html
Certification scheme	The set of rules, requirements and mechanisms that govern the process of certifying a process or a product. NOTE: In this document we use interchangeably "certification scheme" and "compliance scheme" noting that in the real term practise often time the term "certification scheme" is used when referring to ISO-based certification while the term "compliance scheme" is used when referring to ISAE 3000 audits.	EU-SEC D1.4 (this document)

Term	Definition	Source
Cloud Controls Matrix	provides a controls framework that gives detailed understanding of security concepts and principles that are aligned to the Cloud Security Alliance guidance in 13 domains *(CSA, 2016)*. Cloud Control Matrix is used as a central cloud service requirement scheme.	
Cloud service	A software service available in a cloud.	
Cloud service provider (CSP)	A cloud provider is a company that offers some component of cloud computing – _typically Infrastructure as a Service (IaaS), Software as a Service (SaaS) or Platform as a Service (PaaS) – _to other businesses or individuals.	
Cloud service customer	A body that contracted a cloud service.	
Cloud service provider	A third-party company offering a cloud service.	
Competence	Ability to apply knowledge and skills to achieve intended results.	ISO/IEC 19011:2011, definition 3.17
Conformity	Fulfilment of a requirement	ISO 9000:2005, definition 3.6.1
Control	A safeguard or countermeasure requirement prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.	CCM mapping methodology
EU-SEC Security Requirements Repository	A repository of all collected requirements mapped against the CSA CCM, making it a native control framework to address the identified requirements	EU-SEC D1.2 v1.2
Governance Body	A body responsible for governance of the Multi-party recognition framework and for maintenance of its repositories.	

Term	Definition	Source
Information privacy	The relationship between the collection and dissemination of data, tech-nology, the public expectation of privacy, and the legal and political issues surrounding them.	
Information Security	Maintaining on-going awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. Note: The terms "continuous" and "on-going" in this context mean that security and privacy controls and organizational risks are assessed and analyzed at a frequency sufficient to support risk-based security decisions to adequately protect organization information.	NIST SP 800-57
Management system	System to establish policy and objectives to achieve those policies.	ISO 9000:2005, definition 3.2.2
Multi-party recognition	A process for establishing a mutual agreement between certification and compliance scheme owners for recognition of the full or partial equivalence between the certification and/or attestation they govern.	EU-SEC D1.4 (this document)
Nonconformity	Non-fulfilment of a requirement	ISO 9000:2005, definition 3.6.2

Term	Definition	Source
Privacy	The ability (and in modern democracies the right) of an individual or group to seclude themselves, or information about themselves, and thereby express them-selves selectively (Wikipedia[2]). Privacy may be divided into four categories (1) Physical: re-striction on others to experience a person or situation through one or more of the human senses; (2) Informational: restriction on searching for or revealing facts that are unknown or unknowable to others; (3) Decisional: restriction on interfering in decisions that are exclusive to an entity; (4) Dispositional: restriction on attempts to know an individual's state of mind (BusinessDictionary.com[3]).	
Privacy requirement	It is a need or expectation to achieve a level of personal data protection stated in national and international laws and regulations and codes of ethics in cloud compu-ting environment.	
Requirement	A need or expectation that is stated in a standard, law, regulation or other documented information, generally implied (i.e. it is custom or common practice for the organization and interested parties that the need or expectation under consideration is implied), or obligatory (usually stated in laws and regulations)	ISO/IEC 27000:2016
Risk	Effect of uncertainty on objectives, where uncertainty is the state of deficiency of infor-mation related to, understanding or knowledge of, an event, its consequence, or likelihood.	

1 INTRODUCTION

In consideration of the European Data Protection Board's Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679 (12 February 2019)[1], Part 1 of the CSA Code of Conduct for European General Data Protection Regulation (GDPR) Compliance (CoC), as well as the cover letter included with the submission of the CoC, contains the "explanatory statement" providing details as to the purpose of the CoC, the scope of the CoC and how it will facilitate the effective application of the GDPR.

Data protection compliance is becoming increasingly risk-based.[2] Data controllers and processors are accountable for determining and implementing in their organisations appropriate levels of protection of the personal data they process. In such decision, they have to take into account factors such as state of the art of technology; 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.[3] As a result, Cloud Service Providers (CSPs) will be responsible for self-determining the level of protection required for the personal data they process.

It is in this context that the Cloud Security Alliance (CSA) has created the CSA Code of Conduct (CoC) for European General Data Protection Regulation (GDPR) Compliance.

The CSA CoC for GDPR Compliance aims to provide Cloud Service Providers (CSPs) and cloud consumers a solution for GDPR compliance and to provide transparency guidelines regarding the level of data protection offered by the CSP.

The CSA CoC for GDPR Compliance is essentially intended to provide:

- Cloud customers of any size with a tool to evaluate the level of personal data protection offered in connection with services provided by different CSPs (and thus to support informed decisions)[4]

[1] Available at: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-20190219_guidelines_coc_public_consultation_version_en_0.pdf.

[2] See, e.g., Preamble 83 and Articles 25, 32, 33, 34 and 35 of the 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 - GDPR)

[3] See, e.g., Articles 24, 25, 32, 35 and 39 of the GDPR.

[4] All cloud providers offering services in the European Economic Area (EEA) should provide the cloud client with all the information necessary to rightly assess the pros and cons of adopting such services. Security, transparency,

- CSPs of any size and geographic location with a guidance to comply with European Union (EU) personal data protection legislation and to disclose, in a structured way, the level of personal data protection they offer to customers, in connection with their services.

The CSA CoC for GDPR compliance is based on two major components, the Privacy Level Agreement Code of Practice (PLA CoP), which is a technical standard that specifies the requirements included in the GDPR, as well as the adherence mechanisms associated with it.

Since the CSA CoC for GDPR Compliance mainly focuses on legal requirements, CSA proposes the combined adoption of this Code with other CSA best practices and certifications, such as the Cloud Control Matrix (CCM) and the STAR Certification (or STAR Attestation or STAR Self-Assessment), which provide additional guidance around technical controls and objectives for information security.

In such a context, the adoption of technical information security standards such as the Cloud Control Matrix or its equivalents (e.g., ISO 27001 supported by ISO 27017 or 27018, or the AICPA Trust Services Criteria), and the certification schemes related to them (e.g., STAR Certification, STAR Attestation, STAR Self-Assessment, ISO 27001, or SOC2) will provide evidence that CSPs have implemented a security program or an information security management system (ISMS) that adequately protects consumer data from the threats outlined in these risk assessments and the Data Protection Impact Assessment.

The CSA CoC for GDPR Compliance reflects the GDPR requirements that are relevant in the cloud and is a component of the CSA Security, Transparency and Assurance Registry (STAR).

The target audience of the CSA CoC for GDPR Compliance includes all interested stakeholders in cloud computing and EU personal data protection legislation, such as CSPs, cloud customers and potential customers, cloud auditors and cloud brokers.

Finally, it is important to note that any adherence to the CSA Code of Conduct for GDPR Compliance does not reduce the responsibility of the controller or the processor to comply with GDPR and is without prejudice to the tasks and powers of the national Data Protection Authorities (DPAs).

and legal certainty for the clients should be key drivers behind the offer of cloud computing services." Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing ("A.29WP05/2012"), p. 2; "A pre- condition for relying on cloud computing arrangements is for the controller [cloud client] to perform an adequate risk assessment exercise, including the locations of the servers where the data are processed and the consideration of risks and benefits from a data protection perspective." p. 4 id. (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf).

1.1 BACKGROUND INFORMATION

The Privacy Level Agreement Outline for the Sale of Cloud Services in the European Union (PLA [V1]), was released in February 2013 as a self-regulatory harmonization tool that offers a structured way to communicate the level of personal data protection offered by a CSP to current and potential customers. PLA [V1] was based not only on EU personal data protection mandatory legal requirements, but also on best practices and recommendations.

PLA [V1] received the endorsement of a number of EU Supervisory Authorities and was used to develop further EU studies, best practices and codes of conduct on personal data protection matters related to cloud computing.

However, after the release of PLA [V1], the Privacy Level Agreement (PLA) Working Group realized that CSPs, cloud customers and potential customers still struggled to identify the necessary baseline for personal data protection compliance across the EU.

Therefore, the PLA Working Group updated these guidelines to PLA [V2], in order to offer various actors in the cloud computing market a compliance tool rather than only a transparency mechanism.

PLA [V2] was based on actual, mandatory EU personal data protection legal requirements (Directive 95/46/EC and its implementations in the EU Member States).

In May 2016, the Regulation (EU) 2016/679 (GDPR)[5] entered into force, and is directly applicable in all EU Member States from 25 May 2018. With the introduction of GDPR, it was immediately evident to the PLA Working Group that CSPs, cloud customers and potential customers needed guidance in order to comply with the new law in the cloud environment. Therefore, the PLA Working Group developed PLA [V3], a compliance tool that reflects the new obligations set forth by the GDPR.[6]

The PLA shall be considered as a Code of Practice (CoP) for privacy and data protection transparency, assurance and compliance.

This current version of PLA of the CoP, i.e. [V3] will be updated as required on the basis of the development of relevant legislation, opinions, guidelines and recommendations from competent authorities.

[5] http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L:2016:119:FULL&from=IT.

[6] Relevant requirements have been added to the PLA [V2] in order reflect the new duties and obligations set forth in the GDPR.

PLA [V3] is thus designed to create continuity between the EU legal personal data protection requirements set forth in the Directive 95/46/EC and its implementations in the EU Member States, by leveraging the PLA [V2] structure, and the requirements of the GDPR.

The PLA is structured to help CSPs, cloud customers and potential customers manage the transition from the old to the new EU data protection regime, and contributes to the proper application of the GDPR into the cloud sector.

PLA [V3] specifies the application of the GDPR in the cloud environment, primarily with regard to the following categories of requirements:

1. Fair and transparent processing of personal data;
2. The information provided to the public and to data subjects (as defined in Article 4 (1) GDPR);
3. The exercise of the rights of the data subjects;
4. The measures and procedures referred to in Articles 24 and 25 GDPR and the measures to ensure security of processing referred to in Article 32 GDPR;
5. The notification of personal data breaches to Supervisory Authorities (as defined in Article 4 (21) GDPR) and the communication of such personal data breaches to data subjects; and
6. The transfer of personal data to third countries.

Additionally, PLA [V3] contains mechanisms that enable the body referred to in Article 41 (1) GDPR to carry out the mandatory monitoring of compliance with its provisions by the controllers or processors that undertake to apply it, without prejudice to the tasks and powers of competent Supervisory Authorities pursuant to Article 55 or 56 GDPR.

For these reasons, PLA Code of Practice [V3] (Part 2), together with its Governance Section (Part 3), qualify as "draft" Code of Conduct pursuant to Article 40 GDPR ("PLA Code of Conduct" or "PLA CoC").

1.2 SCOPE AND METHODOLOGY

The Code deals only with the Business-to-Business (B2B) scenario, considering cloud customers as companies rather than individuals (as opposed to Business-to-Consumer, or B2C scenarios). The Code addresses specific services provided by a CSP in a B2B context – CSPs may offer a

variety of services, some of which comply with the terms of the Code, and others which do not. The services covered by the Code will typically reflect two types of customer situations:

- The cloud customer is the data "controller"[7] and the CSP is a data "processor"[8]
- Both the cloud customer and the CSP are data controllers (whether joint controllers[9] or not)[10]

As originators of this document, the PLA Working Group recognizes that there may be more complex/ hybrid situations (e.g., such as the situation where, for a single service, a CSP acts as a controller for some activities and a processor for others, or the situation where both the cloud customer and the CSP are data processors). However, what matters for the application of this Code is the compliance posture taken by the CSP. Therefore, where a CSP can act as a controller and as a processor for different processing activities within the same service (this should be specified in Control no. 2.3.), it must comply with the relevant controls within this Code (for

[7] "'[C]ontroller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law." Article 4 (7) GDPR.

[8] "'[P]rocessor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller." Article 4 (8) GDPR.

[9] On this matter, see the Decision of the Court of Justice of the EU of 5 June 2018 (Case C-210/16), available at http://curia.europa.eu/juris/document/document.jsf;jsessionid=EC38522CDAEF4821EC942A5AD2552FA2?text=&docid=202543&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=908200.

In this case, the Court considered the situation of Facebook fan page administrators, who were able to obtain anonymous statistical information on fan page visitors – whether or not these visitors have a Facebook account – by means of the "Facebook Insights" service. This service automatically places "cookies" (i.e., small text files) onto devices used by visitors, containing a unique user code, which can be read and matched to those users by Facebook. The resulting information (which is considered as "personal data") is used to provide aggregated statistics to fan page administrators, and also to enable Facebook to improve its ability to target advertisements over its network.

While the Court noted that merely making use of a social network would not suffice to render the user a joint controller regarding the processing of personal data by that network (along with the network provider, in this case Facebook), they stated that, in this case, fan page administrators - by creating a fan page and relying on the "Facebook Insights" service - effectively enabled Facebook's ability to place cookies on visitors' devices. The fact that administrators were also able to define abstract criteria regarding the "target audience" of their fan page (e.g., age, gender, location, occupation, purchasing habits), based upon which Facebook would collect information and generate statistics on users, lead the Court to consider that those administrators contribute to determining the purposes of processing of personal data on those visitors, even though they did not actually access or receive any such personal data (as they only received aggregated, anonymised statistics from Facebook).

Given the above, CSPs should examine carefully the relationship they have with their cloud customers, in order to accurately determine the role which each party plays regarding a given service. This decision has vastly expanded the understanding of how "joint controllership" should be interpreted, and there may be cases where a CSP previously considered itself as acting as an autonomous controller (e.g., because it uses data provided by a cloud customer for a purpose defined by the CSP) which may, effectively, be more appropriately classified as a case of joint controllership (e.g., potentially, where the processing carried out by the CSP is actually done in order to improve the services provided to a customer).

[10] In this respect, it is worth pointing out that, according to Article 28 (8) GDPR: "Without prejudice to Articles 82, 83 and 84, if a processor infringes this Regulation by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing."

controllers and/or processors) for each respective activity; likewise, where a CSP acts as a sub-processor, it must nonetheless comply with the controls defined for data processors within this Code – this will allow the cloud customer-processor engaging the CSP to take those controls into consideration when crafting any offerings which may include the CSP's services.

In conclusion, it is recommended that users of the CoC carefully evaluate the respective privacy roles of the parties involved on a case-by-case basis to clearly identify related obligations.[11] In complex/hybrid situations, the PLA Code of Practice (CoP) (i.e., the technical standard underlining this Code) serves as a practical tool to specifically allocate those parties' respective obligations already clearly identified either under the "CSP is Data Controller" or "CSP is Data Processor" columns of the PLA [V3] Template in Annex 1[12].

The CoC takes into consideration Article 29 Data Protection Working Party Guidelines on the Right to Data Portability[13] (A.29WP242/16-rev.01), Guidelines on Data Protection Officers[14] (A.29WP243/16-rev.01), Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679[15] (A.29WP248/17-rev.01), Guidelines on the Lead Supervisory Authority[16] (A.29WP244/16-rev.01), Guidelines on the application and setting of administrative fines[17] (A.29WP253/17), Guidelines on Personal data breach notification under Regulation 2016/679[18] (A.29WP250/17-rev.01), Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679[19] (A.29WP251/17-rev.01), Guidelines on Transparency under Regulation 2016/67920 (A.29WP260/17-rev.01), Opinion 05/2012 on Cloud Computing[21]

[11] Users can refer to Article 29 Data Protection Working Party Opinion 1/2010 on the concepts of "controller" and "processor" 'A.29WP01/2010' (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf).

[12] See also the discipline concerning joint controllers set forth in Article 26 GDPR: '1. Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects. 2. The arrangement referred to in paragraph 1 shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects. The essence of the arrangement shall be made available to the data subject. 3. Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under this Regulation in respect of and against each of the controllers.

[13] http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233.

[14] http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048.

[15] http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.

[16] http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611235.

[17] http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237.

[18] http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052.

[19] http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053.

[20] http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227.

[21] http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf.

(A.29WP05/2012), ENISA Technical Guidelines for the implementation of minimum security measures for Digital Service Providers22 (ENISA Guidelines February 16, 2017) and the European Data Protection Supervisor's Guidelines on personal data breach notification for the European Union Institutions and Bodies23 (EDPS Guidelines November 21, 2018).

Therefore, this CoC is not only based on the mandatory legal provisions of the applicable EU personal data protection framework, but also reflects the relevant interpretation by the European Supervisory Authorities and related best practices developed by relevant Agencies. The Code aims to be a horizontal tool that can be used to achieve/assess compliance with the EU personal data protection legislation horizontally across different sectors and domains. The PLA Working Group is aware of the possibility for EU Member States to provide for exemptions or derogations, more specific rules and additional requirements on top of the GDPR;[24] as well as of the existence of EU personal data protection provisions applicable to specific services (e.g., Directive on privacy and electronic communications,[25] and the network and information systems Directive[26]). Hence, the PLA Working Group recommends that users of the Code identify possible Member States' and/or sector-specific additional requirements. The CoC is also written taking into account ISO/IEC 27018,[27] the "Cloud Service Level Agreement Standardisation Guidelines",[28] the works developed by the Cloud Select Industry Group on Code of Conduct[29], by the Cloud Infrastructure Service Providers in Europe (CISPE),[30] and the Cloud Accountability Project.[31]

[22] https://www.enisa.europa.eu/publications/minimum-security-measures-for-digital-service-providers.

[23] https://edps.europa.eu/data-protection/our-work/publications/guidelines/guidelines-personal-data-breach-notification_en.

[24] See, e.g., Article 37 (4) and CHAPTER IX 'Provisions relating to specific processing situations' GDPR.

[25] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, as subsequently amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws. See also the Proposal for a Regulation on Privacy and Electronic Communications, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:0010:FIN.

[26] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L1148&from=MT.

[27] https://www.iso.org/standard/61498.html.

[28] https://ec.europa.eu/digital-single-market/news/cloud-service-level-agreement-standardisation-guidelines.

[29] https://ec.europa.eu/digital-single-market/en/cloud-select-industry-group-code-conduct.

[30] https://cispe.cloud/.

[31] http://www.a4cloud.eu/.

The CoC reflects the GDPR requirements that are relevant in the cloud domain and, following the "territorial scope" of the GDPR, the PLA CoP extends beyond the EU.[32] Additionally, the CoC provides also practical explanations of the importance of each defined control (in Part 2), emphasizing the practical relevance (by means of examples, where appropriate) behind implementing each control, beyond compliance with mandatory requirements (particularly regarding controls which are not legally required).

The target audience for this CoC includes all interested stakeholders in the area of cloud computing and EU personal data protection legislation, such as CSPs, cloud customers and potential customers, cloud auditors and cloud brokers. (…) This process ensured that the CoC considers the nuances of the cloud computing sector in each of its controls.

Additionally, the CoC takes into consideration the needs of small and medium enterprises in the realm of data protection – particularly, the need to clearly understand how the GDPR may apply to them, so that they may allocate their resources for compliance in an effective manner. In this sense, the CoC further specifies controls to prevent GDPR compliance (considering all of the GDPR's inherent duties and obligations, compliance with which requires a significant investment of time, money and effort) from becoming a competitive disadvantage for those enterprises: an example can be found in **Control no. 6**, which relies on the detailed guidance developed by ENISA to allow SMEs to clearly understand the different types and levels of security measures which they may consider implementing. The desired end-result is for the CoC to provide easily understandable guidelines for SMEs, which may allow them to efficiently comply with applicable data protection requirements and level the playing field with larger CSPs – in short, the CoC seeks to develop a consistent approach to data protection in the cloud computing sector, for CSPs of all sizes.

At present, the CoC is not intended to meet the requirements of Art. 46(2)(e) GDPR – i.e., to qualify as an appropriate safeguard which might, following approval, serve as legal grounds for a transfer of personal data from within the EU to outside of the EU (where the receiving country is not covered by an adequacy decision). However, an addendum to this CoC, aimed at meeting these requirements, is currently being considered by the CSA.

[32] See Article 3 GDPR: "2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union."

The lead Supervisory Authority which has been identified for the CoC is the French *Commission Nationale de l'Informatique et des Libertés* ("**CNIL**"). This has been decided on the basis of the following factors:

- **Initiatives developed by the CNIL.** The CNIL has developed several guidelines and initiatives of relevance to the scope of the CoC, including "Recommendations for companies planning to use Cloud computing services"[33] and the guide on "Security of Personal Data"[34]. Furthermore, and most importantly, the CNIL has followed the work developed on the CoC from the first versions of the PLA which were produced, and has to date provided extensive feedback on the CoC in the context of an informal consultation process initiated by the CSA. It results that the CNIL is the natural choice for the lead Supervisory Authority competent to decide on the approval of the CoC. This is compounded by the fact that the other potential candidate for lead Supervisory Authority – the ICO (given the existence of a CSA subsidiary in Scotland) – may be compromised due to the impending possibility of the United Kingdom leaving the European Union.
- **Location of the largest density of the processing activity/sector.** France is home to a significant number of CSPs within Europe, including around 10 CSA corporate members with either their headquarters or a subsidiary settled in France.
- **Location of the largest density of data subjects affected.** Considering that there are no limitations as to the categories of data subjects which may have their personal data processed via services provided by a CSP, France may again be considered as meeting this criterion, given that it is one of the most populated EU countries.

Given that the scope of the CoC is **transnational**, in that it seeks to apply to all manner of CSPs which wish to adhere to its requirements, regardless of their location, all other EU Supervisory Authorities may potentially be considered as concerned Supervisory Authorities:

- The Austrian Österreichische Datenschutzbehörde;
- The Belgian Autorité de la Protection des Données;
- The Bulgarian Commission for Personal Data Protection;
- The Croatian Personal Data Protection Agency;
- The Cypriot Commissioner for Personal Data Protection;
- The Czech Office for Personal Data Protection;

[33] Available at: https://www.cnil.fr/sites/default/files/typo/document/Recommendations_for_companies_planning_to_use_Cloud_computing_services.pdf.

[34] Available at: https://www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle_gb_web.pdf.

- The Danish Datatilsynet;
- The Estonian Data Protection Inspectorate (Andmekaitse Inspektsioon);
- The Finnish Office of the Data Protection Ombudsman;
- The German Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (as well as the Supervisory Authorities of the several Länder which make up Germany[35]);
- The Hungarian National Authority for Data Protection and Freedom of Information;
- The Irish Data Protection Commission;
- The Italian Garante per la Protezione dei Dati Personali;
- The Latvian Data State Inspectorate;
- The Lithuanian State Data Protection Inspectorate;
- The Luxembourg Commission Nationale pour la Protection des Données;
- The Maltese Office of the Information and Data Protection Commissioner;
- The Dutch Autoriteit Persoonsgegevens;
- The Polish Urząd Ochrony Danych Osobowych;
- The Portuguese Comissão Nacional de Protecção de Dados;
- The Romanian National Supervisory Authority for Personal Data Processing;
- The Slovakian Office for Personal Data Protection;
- The Slovenian Information Commissioner;
- The Spanish Agencia Española de Protección de Datos;
- The Swedish *Datainspektionen*; and
- The UK *Information Commissioner's Office*.

1.3 OBJECTIVES

1. The CSA CoC can be adhered to by CSPs regarding one or more of the services provided by that CSP, and may also be referenced or used by adhering CSPs as an appendix to a Cloud Services Agreement, in order to describe the level of privacy protection that the CSP will provide. While Service Level Agreements (SLAs) are generally used to provide metrics and other information on the performance of the services, the CoC will address information privacy and personal data[36] protection practices.

[35] A list of these authorities is available at: https://www.datenschutz-wiki.de/Aufsichtsbeh%C3%B6rden_und_Landesdatenschutzbeauftragte.

[36] "'[P]ersonal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an

2. In the CoC, the CSP would clearly describe the level of privacy and data protection that it undertakes to maintain with respect to relevant data processing, regarding the service(s) it provides to cloud customers which the CSP has aligned with this CoC.[37]

3. The adoption of the CoC worldwide can promote a powerful global industry standard, enhance harmonization and facilitate compliance with applicable EU data protection law. In fact, the CoC seeks to establish a standard of compliance for CSPs, based on the GDPR, which may apply internationally (even outside the EU, given that adherence is not restricted to EU-based CSPs). In this sense, approval of the CoC may lead to it becoming a benchmark for data protection compliance to be followed by CSPs worldwide – just as the GDPR, upon which it is based, is considered a solid international baseline for data protection compliance in general – for the benefit of cloud customers and data subjects within and outside the EU.

4. Furthermore, approval of the CoC will lead to a meaningful co-regulation for data protection practices in the cloud computing sector, with input from the market (in the form of the PLA WG and its participants) and EU Supervisory Authorities (during the approval process).

5. Ultimately, the CoC is intended to provide the following:

    - Cloud customers and potential customers, of any size, with a tool to evaluate the level of personal data protection offered by different CSPs, in connection with the service(s) provided (and thus to support informed decisions);[38] and
    - CSPs of any size with guidance to achieve compliance with EU personal data protection legislation and to disclose, in a structured way, the level of personal data protection they offer to customers, in connection with their service(s).

identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person." Article 4 (1) GDPR.

[37] "'[P]rocessing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction." Article 4 (2) GDPR.

[38] "All cloud providers offering services in the EEA should provide the cloud client with all the information necessary to rightly assess the pros and cons of adopting such services. Security, transparency, and legal certainty for the clients should be key drivers behind the offer of cloud computing services." Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing ("A.29WP05/2012"), p. 2; "A precondition for relying on cloud computing arrangements is for the controller [cloud customer] to perform an adequate risk assessment exercise, including the locations of the servers where the data are processed and the consideration of risks and benefits from a data protection perspective." p. 4 id., http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf.

6. The CoC seeks to create additional value for potential and current cloud customers, as well as for CSPs, data subjects and the cloud computing community at large by:

- Identifying – in an organic, structured and systematic manner – all relevant GDPR provisions which CSPs must comply with when handling personal data;
- Explaining the GDPR provisions and their practical relevance, when applied to the computing environment, considering also the clarifications provided in this respect by the Article 29 Working Party / European Data Protection Board, as well as by EU national Supervisory Authorities which have provided guidance on the subject;
- Raising the bar for data protection and privacy in cloud computing, by adding controls defined on the basis of guidelines produced by the European Union Agency for Network and Information Security, ISO standards (e.g., 27001, 27017, 27018) and additional best practices developed (including controls such as the need for CSPs to identify and provide contact details for their Information Security Officer – **Control no. 2.5** –, defining a timeframe for CSPs to notify cloud customers regarding personal data breaches of which they become aware – **Control no. 8** –, to offer effective and business-friendly remedies to cloud customers in the event of breaches of obligations under the PLA – **Control no. 14.** – and to procure data protection compliance insurance, with coverage over breaches caused by sub-processors, and cyber-insurance, covering also security and data breaches which may occur – **Control no. 15.**);
- **Emphasising the need for transparency and enabling compliance with the principle of accountability for CSPs**, by establishing a disclosure policy and requiring CSPs adhering to the CoC's requirements to provide minimum information and evidence to demonstrate their compliance, in the context of their self-assessment/third-party assessment submissions. Additionally, in requiring this disclosure, the information necessary for cloud customers engaging those CSPs to comply with their own transparency and accountability obligations towards data subjects, around the engagement of CSPs to process personal data, will be made available to them;
- Allowing for **public scrutiny of compliance with the CoC**, by requiring adhering CSPs to disclose their CoC self-assessment/third-party assessment submissions within the CSA STAR Registry (including, e.g., specific details on how those CSPs understand that they meet the minimum requirements set by the CoC), with any deviations from those submissions in practice kept in check by means of the CoC's Complaint Management Process (which may, ultimately, lead to suspension or revocation of adherence seals provided to adherent CSPs, where a complaint is found to be valid).

In this manner, the CoC goes beyond the GDPR's requirements and provides a higher standard for adhering CSPs' data protection practices.

7. The Privacy Level Agreement Code of Practice (PLA) reflects the GDPR requirements that are relevant in the cloud. It also restates and reinforces the requirements of the GDPR, particularly where the exercise of data subjects' rights are concerned – see, for example, **Control no. 3.5.6** (on the need for a CSP to commit, via contractual obligations, to assisting cloud customers in responding to data subject requests), **Control no. 9** (on the need for a CSP to assure the portability of data, including the capability to transmit personal data in a structured, commonly used, machine-readable and interoperable format directly to data subjects) and **Control no. 10** (on the need for a CSP to explain to cloud customers how it allows for the restriction of processing of personal data). Moreover, it raises the bar for data protection and privacy in cloud computing, by adding controls defined on the basis of guidelines produced by the European Union Agency for Network and Information Security, ISO standards and additional best practices developed – in particular, in **Control no. 6**, the CoC provides a solid baseline for technical and organisational security measures to be implemented by CSPs, through the ENISA Technical Guidelines for the Implementation of Minimum Security Measures for Digital Service Providers[39], which allows CSPs to declare their compliance with varying sophistication levels (1 to 3), thereby affording to CSPs the possibility to calibrate the security measures proposed by the CoC in line with their own assessment of the risks inherent to their services, in full compliance with Article 32 GDPR. The PLA reflects all of the GDPR requirements and goes beyond, by providing a higher standard for adhering CSPs' data protection practices; hence it may, materially, qualify also as a certification mechanism under Article 42 GDPR.

8. The CoC, through the PLA, does not only seek to promote lawful behaviour on the part of adhering CSPs, but also ethical behaviour. The CoC's requirements include obligations upon CSPs which, while not strictly required by the applicable law, are necessary to guarantee a fair balance in the relationship between CSPs and cloud customers, eventually aiming to ensure that data subject rights can effectively be respected. For example: the requirement for a CSP to provide a transitional period to customers upon customer termination (as a result of an objection to a change of data processing locations or of sub-processors), during which services will continue to be provided to customers as they seek an alternative solution. This requirement seeks to prevent harm which might arise for customers, as well as for the data subjects whose data are processed by those customers, if the services provided by a CSP were abruptly ended, as a result of the customer's exercise of their right of

[39] Available at: https://www.enisa.europa.eu/publications/minimum-security-measures-for-digital-service-providers.

objection/termination (see **Control no. 3.2.3** and **Control no. 3.3.5**). One further example is **Control no. 14**, which requires CSPs to offer remediation to cloud customers in the event that a CSP breaches its obligations under the PLA, thereby ensuring compensation to the customer and preventing the occurrence and escalation of disputes.

9. It is worthwhile to mention that the terminology "**Privacy Level Agreement**" is used in the sense that the approach to privacy and data protection from adherents to the CoC is not a "one-size-fits-all" matter; rather, there are different levels of assurance in terms of compliance (e.g., regarding different security measures put in place, or different technical means to assist in addressing data subjects' requests) which may be offered by adhering CSPs, which still meet the requirements of the CoC. As such, by means of an analogy with the term "Service Level Agreement", referring to "privacy levels" is deemed appropriate.

1.4 ASSUMPTIONS

Before entering into a contract for the provision of cloud services, or when such a contract needs to be reviewed in light of GDPR requirements, both the current and potential cloud customer are recommended to conduct internal and external due diligence assessments, respectively. For example:

- Internal due diligence could be leveraged to identify restrictions and constraints that may accompany or prevent potential use of cloud services (e.g., is the cloud actually a viable solution for the type of data the entity wishes to process in a cloud?).
- External due diligence determines whether the proposed cloud provider(s) offerings meet the potential customer's needs and compliance obligations. It could help to evaluate the level of personal data protection that a CSP would provide. For example, does the proposed CSP provide the level of privacy and data protection and the level of compliance with applicable EU law needed by the company, either because this level has been determined by the company itself, or because it is required by applicable law?[40]

[40] For more on this issue, see CSA Guidance Version 3 (https://cloudsecurityalliance.org/research/security-guidance/)

1.4.1 CLOUD CUSTOMER INTERNAL DUE DILIGENCE

As part of its internal due diligence, an entity that intends to move personal data to the cloud may consider, among other things:

1. Defining its security, data protection and compliance requirements.
2. Identifying what data/processes/services it will want to move to the cloud.
3. Reviewing its own internal security and privacy/data protection policies and other restrictions on its use of personal data, such as pre-existing contracts, applicable laws and regulations, guidelines and best practices.
4. Analysing and assessing risks (e.g., performing a Data Protection Impact Assessment to the extent required by Article 35 GDPR[41]).
5. Identifying which security controls and certifications are required or useful to achieve adequate protection of its employees or customers' personal data while processed in the cloud.
6. Defining responsibilities and tasks for security controls implementation (i.e., understand which security controls are under the direct governance of the organisation and which security controls are under the responsibility of the CSP).
7. Determining which CSP activities the entity should monitor (e.g., are onsite visits required, or is it sufficient to rely on a certification or attestation from a third party?).

1.4.2 CLOUD CUSTOMER EXTERNAL DUE DILIGENCE

The cloud customer may also consider conducting a due diligence evaluation of the practices of the proposed CSP. This may include, among other things:

1. Evaluating whether the CSP - including its (sub)contractors/processors - fulfils the cloud customer's requirements with respect to privacy and data protection, using the PLA.
2. Determining whether the CSP holds any relevant certification or attestation based on an independent third-party assessment.[42]
3. Understanding whether and how to have visibility of, and the ability to monitor, the security controls and practices implemented by the CSP.

[41] See, for practical guidelines, A.29WP248/17

[42] See Articles 40 ff. GDPR.

1.5 EXPLANATORY NOTES

A CSP may offer a variety of services to cloud customers. The Code does not apply to a CSP in itself (as an entity), but rather to one or more of the services it offers. It is thus possible for a CSP to fulfil the requirements of this Code for a number of its services, but still provide other offerings which are not covered by this Code.

Moreover, this Code may leave room, or point to other documents, for further clarification of specific subject and time frame of the cloud service to be provided, and the extent, manner and purpose of the processing of personal data by the CSP, as well as the types of personal data that will be processed. Such information should be gathered and agreed upon with the customer.[43]

Though the obligations assumed by a CSP adhering to the Code are independent from those which that CSP assumes towards its customers (e.g., in data processing agreements signed with those customers), CSPs may choose to include the Code within their contractual documentation offered to customers. In this case, to avoid duplication, references can also be made to appropriate provisions in the Master Services Agreement, Service Level Agreement (SLA) or other document that is part of the contract for cloud services. For example, SLAs typically include information about data security. The use of cross-references between documents is intended to simplify things for both customers and CSPs (as opposed to disorient customers). Clarity and transparency are critical.

1.6 STRUCTURE OF THE DOCUMENT

The rest of this document is organized as follows:

- Section 2 describes PLA Privacy Requirements which includes the set of controls that CSP should put in place in order to show adherence to the EU-SEC privacy requirements.
- Section 3 describes the PLA Code of Conduct's (CoC) governance and adherence mechanisms in order to guide the revision of the EU-SEC privacy controls repository required by the possible evolution of the regulatory landscape.
- Section 4 concludes the document.

[43] A.29WP05/2012, Section 3.4.2, p. 13.

2 PLA PRIVACY REQUIREMENTS

Part 2 of this document shall be used in conjunction with Annex 1: PLA [V3] Template.

In the description of the requirements of the PLA Code of Practice (CoP), it is specified with a [C] if the requirement is applicable to the CSP as a controller; with a [P] if applicable to the CSP as a processor or [C&P] if the requirement is applicable to both.

Notice that if a processor determines the purposes and means of processing, the processor is considered a controller in respect of such processing.

2.1 CSP DECLARATION OF COMPLIANCE AND ACCOUNTABILITY

The CSP declares to the cloud customers and ensures:

1. To comply with the applicable EU data protection law and with the terms of this Code of Conduct, also with respect to technical and organisational security measures, and to safeguard the protection of the rights of the data subject. Where there is a material change in applicable EU data protection law which may imply new or conflicting obligations regarding the terms of this Code of Conduct, the CSP commits to complying with the terms of the applicable EU data protection law. [C & P]

   Relevance: By providing such a declaration, CSPs extend what is already a legal obligation – i.e., to comply with EU data protection law – by means of an additional commitment to complying with the terms of this CoC. If changes in EU data protection law imply a conflict with the CoC, the CSP commits to complying with EU data protection law (regardless of the fact that the CoC will be promptly revised to meet the new legal standards, following the processes described further in Part 3). The CoC exists independently and alongside any data processing agreements which an adhering CSP may have entered into with its customers. Adhering to the Code creates an obligation for the CSP to comply with its terms, lest its adherence seal under the Code be removed or suspended.

2. To be able to demonstrate compliance with the applicable EU data protection law and with the terms of this Code of Conduct. (accountability).[44] [C & P]

[44] See in this respect the fundamental principle of "accountability" in Articles 5.2. and 28.3 (h) GDPR.

Relevance: In this manner, CSPs guarantee that they will be able, at any time, to prove that they comply with their legal obligations, as well as their additional obligations under this CoC, for the benefit of cloud customers and data subjects, which are thus empowered to ask for tangible evidence of compliance from the CSPs they engage (see also below controls, as well as Control no. 3.5.9, Control no. 4., Control no. 7. and Control no. 12.2. for specifications of this).

The CSP must describe to the cloud customers:

3. What policies and procedures the CSP has in place to ensure and demonstrate compliance by the CSP itself and its subcontractors (see also Control no. 3.3., below) or business associates, with the applicable EU data protection law and with the terms of this Code of Conduct. [C & P]

Relevance: Providing cloud customers with the CSP's internal policies and procedures on the protection of personal data is a fundamental step in empowering cloud customers to selecting a CSP which they consider will handle the personal data for which they are responsible in an appropriate manner, thereby complying with the internationally recognized data protection principle of transparency. Furthermore, these policies and procedures should accurately describe to cloud customers how compliance will be demonstrated, both with respect to the CSP, as well as its subcontractors and business associates engaged to provide services (thereby offering reassurance over the entire processing chain used).

The CSP must identify:

4. The elements that can be produced as evidence to demonstrate such compliance.[45],[46] Evidence elements can take different forms, such as self-certification/attestation,

[45] The definition of accountability from the EDPS glossary reads: "Accountability requires that controllers put in place internal mechanisms and control systems that ensure compliance and provide evidence – such as audit reports – to demonstrate compliance to external stakeholders, including supervisory authorities." Source: European Data Protection Supervisor (EDPS) (2012), Glossary of terms, https://edps.europa.eu/data-protection/data-protection/glossary_en#accountability.

[46] A.29WP05/2012, section 3.4.4.7, p. 16 introduces the notion of (documentary) evidence to be provided to back up the asserted compliance to the data protection principles, "[…] cloud providers should provide documentary evidence of appropriate and effective measures that deliver the outcomes of the data protection principles".

third-party audits[47] (e.g., certifications,[48] attestations,[49] and seals), logs, audit trails, system maintenance records, or more general system reports and documentary evidence of all processing operations under its responsibility. These elements need to be provided at the following levels:

i. Organisational policies level to demonstrate that policies are correct and appropriate;

ii. IT controls level, to demonstrate that appropriate controls have been deployed; and

iii. Operations level,[50] to demonstrate that systems are behaving (or not) as planned. Examples of evidence elements pertaining to different levels are data protection certifications, seals and marks.[51] [C & P]

Relevance: This control further specifies Control no. 1.2. above, by establishing specific forms in which CSPs may produce evidence of their compliance to cloud customers. It covers also the subject-areas which must be addressed by this evidence, to provide a complete and clear

[47] "Independent verification or certification by a reputable third party can be a credible means for cloud providers to demonstrate their compliance with their obligations as specified in this Opinion. Such certification would, as a minimum, indicate that data protection controls have been subject to audit or review against a recognised standard meeting the requirements set out in this Opinion by a reputable third-party organisation. In the context of cloud computing, potential customers should look to see whether cloud services providers can provide a copy of this third party audit certificate or indeed a copy of the audit report verifying the certification including with respect to the requirements set out in this Opinion." See A.29WP05/2012, Section 4.2, p. 22.

[48] E.g., CSA STAR certification, ISO/IEC 27001 certifications (possibly augmented with the controls from ISO/IEC 27018),

[49] E.g., CSA STAR Attestation, SOC 2 attestation.

[50] Evidence at Operations level can be defined as "collection of data, metadata, routine information and formal operations performed on data and metadata which provide attributable and verifiable account of the fulfilment of relevant obligations with respect to the service and that can be used to support an argument shown to a third party about the validity of claims about the appropriate and effective functioning (or not) of an observable system." Source: Wlodarczyk, Pais (eds.), A4Cloud Project Public Deliverable D38.2, "Framework of Evidence," March 2015.

[51] See Article 42 GDPR. Moreover, note that the CSP may be requested a general obligation to provide assurance that its internal organisation and data processing arrangements (and those of its sub-processors, if any) are compliant with the applicable national and international legal requirements and standards, as per A.29WP05/2012, Section 3.4.2 p. 14. See also Article 17(2) of Directive 95/46/EC and A.29WP05/2012, Section 3.4.3 p. 14 and Section 3.4.4.7. See also, e.g., CNIL's Recommendations p. 12: "a) Observance of French principles on the protection of personal data. [The following model clause may be used when the service provider is a data processor] The Parties undertake to collect and process all personal data in compliance with any current regulation applicable to the processing of these data, and in particular with Law 78-17 of 6 January 1978 amended. Ac- cording to this law, the Customer is data controller for the Processing carried out under the Contract. [The following model clause may be used when the service provider is a joint data controller] The Parties undertake to collect and process all personal data in compliance with any current regulation applicable to the processing of these data, and in particular with Law 78-17 of 6 January 1978 amended. According to this law, the Parties are joint data controllers for the Processing carried out under the Contract."

picture to data subjects – i.e., compliance regarding the CSP's organizational policies (addressed also in Control no. 1.3. above), IT controls and practical operations.

2.2 CSP RELEVANT CONTACTS AND ITS ROLE

The CSP must specify to the cloud customers:

1. The CSP's identity and contact details (e.g., name, address, email address, telephone number and place of establishment); [C & P]

   Relevance: This control requires CSPs to correctly identify the legal entity which will be responsible not only for providing the services, but for ensuring that the services provided are and remain compliant with applicable data protection legislation.

2. The identity and contact details (e.g., name, address, email address, telephone number and place of establishment) of the CSP's local representative(s) (e.g., a local representative in the EU);[52] [C & P]

   Relevance: In order to afford cloud customers and data subjects with effective means of addressing the CSP with matters related to the services or the processing of personal data inherent to the services, as well as to comply with the requirements of Art. 27 GDPR (when applicable), CSPs are to identify any local representatives which those customers and data subjects may address in the stead of the entity identified in Control no. 2.1. above (including, for non-EU CSPs, a local representative in the EU).

[52] See Article 27 GDPR: "Representatives of controllers or processors not established in the Union. 1. Where Article 3(2) applies, the controller or the processor shall designate in writing a representative in the Union. 2. The obligation laid down in paragraph 1 of this Article shall not apply to: (a) processing which is occasional, does not include, on a large scale, processing of special categories of data as referred to in Article 9(1) or processing of personal data relating to criminal convictions and offences referred to in Article 10, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing; or (b) a public authority or body. 3. The representative shall be established in one of the Member States where the data subjects, whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored, are. 4. The representative shall be mandated by the controller or processor to be addressed in addition to or instead of the controller or the processor by, in particular, supervisory authorities and data subjects, on all issues related to processing, for the purposes of ensuring compliance with this Regulation. 5. The designation of a representative by the controller or processor shall be without prejudice to legal actions which could be initiated against the controller or the processor themselves."

3. The CSP's data protection role for each of the relevant processing activities inherent to the services (i.e., controller, joint-controller[53], processor or subprocessor);[54] [C & P]

[53] On this matter, see the Decision of the Court of Justice of the EU of 5 June 2018 (Case C-210/16), available at http://curia.europa.eu/juris/document/document.jsf;jsessionid=EC38522CDAEF4821EC942A5AD2552FA2?text=&docid=202543&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=908200.

In this case, the Court considered the situation of Facebook fan page administrators, who were able to obtain anonymous statistical information on fan page visitors – whether or not these visitors have a Facebook account – by means of the "Facebook Insights" service. This service automatically places "cookies" (i.e., small text files) onto devices used by visitors, containing a unique user code, which can be read and matched to those users by Facebook. The resulting information (which is considered as "personal data") is used to provide aggregated statistics to fan page administrators, and also to enable Facebook to improve its ability to target advertisements over its network.

While the Court noted that merely making use of a social network would not suffice to render the user a joint controller regarding the processing of personal data by that network (along with the network provider, in this case Facebook), they stated that, in this case, fan page administrators - by creating a fan page and relying on the "Facebook Insights" service - effectively enabled Facebook's ability to place cookies on visitors' devices. The fact that administrators were also able to define abstract criteria regarding the "target audience" of their fan page (e.g., age, gender, location, occupation, purchasing habits), based upon which Facebook would collect information and generate statistics on users, lead the Court to consider that those administrators contribute to determining the purposes of processing of personal data on those visitors, even though they did not actually access or receive any such personal data (as they only received aggregated, anonymised statistics from Facebook).

Given the above, CSPs should examine carefully the relationship they have with their cloud customers, in order to accurately determine the role which each party plays regarding a given service. This decision has vastly expanded the understanding of how "joint controllership" should be interpreted, and there may be cases where a CSP previously considered itself as acting as an autonomous controller (e.g., because it uses data provided by a cloud customer for a purpose defined by the CSP) which may, effectively, be more appropriately classified as a case of joint controllership (e.g., potentially, where the processing carried out by the CSP is actually done in order to improve the services provided to a customer).

[54] A.29WP05/2012 has been written considering the situation in which the customer is a controller and the CSP is a processor, see Section 1, p. and Section 3.4. In our opinion, the respective roles need to be carefully assessed on a case-by-case basis, as also confirmed by the Information Commissioner's Office in its Guidance on the use of cloud computing ("ICO Guidance"), p. 7. In this respect, see the Sopot Memorandum (http://www. datenschutz-berlin.de/attachments/875/Sopot_Memorandum.12.6.12.pdf?1339501499) adopted by the Berlin International Working Group on Data Protection in Telecommunications in April 2012 ("Sopot Memorandum") p. 8: "A commonly recognised data protection principle is that the processor must not process personal data to a greater extent than that which follows from the explicit instructions from the controller. For CC [Cloud Computing], this implies that a cloud service provider cannot unilaterally make a decision or arrange for personal data (and its processing) to be transmitted more or less automatically to unknown cloud data centres. This is true whether the cloud service provider justifies such a transfer as a reduction of operating costs, management of peak loads (overflow), load balancing, copying to backup, etc. Nor may the cloud service provider use personal data for his own purposes."; A.29WP05/2012 p. 23: "The draft proposal clarify that a processor failing to comply with controller's instructions qualifies as a controller and is subject to specific joint controllership rules"; CNIL's Recommendations for companies planning to use Cloud Computing Services (CNIL's Recommendations: http://www.cnil.fr/fileadmin/documents/en/Recommendations_for_companies_planning_to_use_Cloud_computing_ser- vices.pdf) pp. 5-6: "When a customer uses a service provider, it is generally accepted that the former is the data controller and the latter is the data processor. However, CNIL finds that in some cases of public PaaS and SaaS, customers, although responsible for the choice of their service providers, cannot really give them instructions and are not in a position to monitor the effectiveness of the security and confidentiality guarantees given by the service providers. This absence of instructions and monitoring facilities is due particularly to standard offers that cannot be modified by customers, and to standard contracts that give them no possibility of negotiation. In such situations the service provider could in principle be considered as joint controller pursuant to the definition of "data controller" given in Article 2 of Directive 95/46/EC, he contributes to the definition of the purposes and means for personal data processing. In cases where there are joint controllers, the responsibilities of each party

Relevance: It is fundamental, in practice, for both parties to understand and agree upon the roles that they perform in the data processing relationship inherent to the provision of the services, given the significantly different practical implications and legal obligations for a party depending on the role it plays (such as the differences in autonomy, liability and responsibilities towards data subjects between a CSP which acts as a controller – joint or not – and a CSP which acts as a processor). Therefore, CSPs are required to perform their own assessments in light of the services they provide and communicate the roles which they understand as applicable to them to cloud customers, in order to allow these customers to understand what to expect and what they can demand from CSPs (assuming that, in most cases, B2B cloud customers will act as controllers).

To the extent that a service provided may involve different processing activities for which the CSP may undertake different roles (e.g., as a processor for certain activities, and as a controller for others), CSPs must comply with the relevant legal and CoC obligations referring to processors and/or controllers.

4. The contact details of the CSP's Data Protection Officer (DPO)[55] or, if there is no DPO, the contact details of the individual in charge of privacy matters to whom the customer may address requests; [C & P]

   Relevance: By requiring CSPs to provide information as to the Data Protection Officer they have appointed or, in the absence of such an appointment, of the "privacy contact" within each CSP, it is ensured that cloud customers are able to quickly and effectively reach the correct contact persons within the CSP to address privacy and data protection concerns which may come up.

5. The contact details of the CSP's Information Security Officer (ISO) or, if there is no ISO, the contact details of the individual in charge of security matters to whom the customer may address requests. [C & P]

   Relevance: Given that CSPs may segregate internal roles related to privacy and information security (e.g., by having separate individuals acting as DPO / privacy contact and ISO / security contact), and that more technical security matters raised by cloud customers might be better handled by the CSP's ISO (or equivalent function – "security contact"), the CoC requires CSPs to disclose their contact details for this

should be clearly defined." Following the indications of the Italian Data Protection Authority, the CSP is a processor, Cloud Computing: il Vademecum del Garante (http://www.garantepri-vacy.it/garante/document?ID=1895296&DOWNLOAD=true, pp. 14-15). See also ICO Guidance, pp. 7-9 on the privacy roles in different cloud service deployment models.

[55] See Article 13 (1) (b) GDPR and Articles 37 ff. GDPR. Moreover, see A.29WP243/16-rev.01.

individual, in order to ensure a correct and swift resolution of any concerns related more precisely to technical and organisational security measures raised by customers.

2.3 WAYS IN WHICH DATA WILL BE PROCESSED

2.3.1 GENERAL INFORMATION

CSPs that are controllers must provide details to cloud customers regarding the following[56]:

1. Categories of personal data concerned in the processing; [C]
2. Purposes of the processing for which data are intended and the necessary legal basis to carry out such processing in a lawful way;[57] [C]
3. Recipients or categories of recipients of the data; [C]
4. Existence of the right to request access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing, as well as the right to data portability; [C]
5. Where applicable, the fact that the CSP intends to transfer personal data to a third country or international organisation and the absence of an adequacy decision by the European Commission, or reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available; [C]
6. The period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period; [C]
7. Where the processing is based on consent, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal; [C]
8. The right to lodge a complaint with a Supervisory Authority[58] (as defined in Article 4 (21) GDPR); [C]

[56] See A.29WP260/17-rev.01.

[57] Including the legitimate interests pursued by the controller or by a third party, where the processing is based on point (f) of article 6 (1) GDPR. See Article 7 Directive 95/46/EC and Article 6 GDPR.

[58] For the list of Supervisory Authorities, please see: http://ec.europa.eu/justice/data-protection/article-29/structure/data-protection-authorities/index_en.htm.

9. Whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data; [C]

10. The existence of automated decision-making, including profiling,[59] and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject; where automated decision-making is in place (under Art. 22 GDPR), the CSP must explain to cloud customers the safeguards which are put in place to ensure respect for the rights and freedoms of data subjects – including, but not limited to, how data subjects can contest any automated decisions related to them, and how human review or other relevant intervention pertaining to an automated decision can be triggered; [C]

11. Where the CSP intends to further process the personal data for a purpose other than that for which the personal data is being collected, information on that other purpose, prior to the relevant further processing; [C]

12. Where personal data has not been obtained from the data subject, from which source the personal data originated, and if applicable, whether the data came from publicly accessible sources;[60] [C]

Relevance: The above requirements mirror those of Arts. 13 and 14 GDPR. This will increase cloud customers' awareness of the specific terms under which the CSP will process personal data in connection with its services and, as such, empower the cloud customer to make a more informed decision when selecting a CSP. Furthermore, by providing this information to its cloud customers, the CSP ensures that the cloud customer is able, when necessary, to relay this information to the data subjects concerned – this will allow the customer to fulfil its own information obligations regarding the use of the CSP's services, but also those of the CSP (in the event that the CSP acts as a controller, whether joint or not).

Concerning automated decision-making, under Art. 22 GDPR, the requirement goes beyond what is strictly asked by Arts. 13 and 14 GDPR. CSPs must ensure that they clearly explain to cloud customers not only whether or not automated decision-making is in place, as well as the logic involved, the significance and potential consequences for data subjects[61], but also the safeguards implemented to protect the

[59] See Article 22 (1) and (4) GDPR and A.29WP251/17-rev.01.
[60] See Articles 13 and 14 GDPR.
[61] Please refer to A.29WP251/17-rev.01, pp. 24-26, for further guidance on what information should be provided in this respect.

rights, freedoms and legitimate interests of data subjects, as required by Art. 22(3) GDPR. These should include, but not be limited to, the possibility for a data subject to contest an automated decision and to trigger the review, or other significant intervention, related to that decision by a human[62].

13. activities that are conducted to provide the agreed cloud service(s) (e.g., data storage), activities conducted at the customer's request (e.g., report production) and those conducted at the CSP's initiative (e.g., backup, disaster recovery, fraud monitoring). [C]

Relevance: This control – which arguably goes beyond what is strictly required by the GDPR – focuses on having CSPs provide a clear demarcation of the roles, responsibilities and obligations which fall upon the CSP and the cloud customer. This will support the definition of roles carried out under Control no. 2.3. and will allow the CSP to advance an allocation of duties and obligations between the CSP and the customer (in the event of joint controllership) or to clearly indicate the activities which will be carried out at the CSP's own initiative, autonomously from the processing purposes defined by the customer / provision of the services (in the event of autonomous controllership).

CSPs that are processors must provide to cloud customers details on:

14. The extent and modalities in which the customer-data controller can issue its binding instructions to the CSP-data processor.[63] [P]

Relevance: This control addresses the important matter of how cloud customers can issue instructions to CSPs. Given that, in the cloud computing domain, it is typical for

[62] Please refer to A.29WP251/17-rev.01, pp. 27-28 and 32, for further guidance on appropriate safeguards which may be implemented, and which should be clearly explained to cloud customers.

[63] See Articles 28 and 29 GDPR. A.29WP05/2012, Section 3.4.2, p. 12: "The agreement should explicitly state that the cloud service provider may not use the controller's data for the cloud service provider's own purposes," Sopot Memorandum, p. 4. See also ICO Guidance, p. 12: "The DPA requires the data controller to have a written contract (Schedule 1 Part II Paragraph 12(a)(ii)) with the data processor requiring that the "data processor is to act only on instructions from the data controller" and "the data processor will comply with security obligations equivalent to those imposed on the data controller itself." The existence of a written contract should mean that the cloud provider will not be able to change the terms of data processing operations during the lifetime of the contract without the cloud customer's knowledge and agreement. Cloud customers should take care if a cloud provider offers a 'take it or leave it' set of terms and conditions without the opportunity for negotiation. Such contracts may not allow the cloud customer to retain sufficient control over the data in order to fulfil its data protection obligations. Cloud customers must therefore check the terms of service a cloud provider offer to ensure they adequately address the risks discussed in this guidance." and p. 17: "The cloud customer should ensure that the cloud provider only processes personal data for the specified purposes. Processing for any additional purposes could breach the first data protection principle. This might be the case if the cloud provider decides to use the data for its own purposes. Contractual arrangements should prevent this."

terms of service and associated contractual documentation to be defined unilaterally by the CSP, it is important that this specific point is clearly addressed in the information given to cloud customers, so that customers will be in a position to confirm upfront whether the terms offered by the CSP are aligned with Art. 28 GDPR. This requirement goes beyond what is strictly needed under the GDPR, in that it obliges CSPs to detail how and to what extent customers will be able to instruct the CSP regarding the use of the personal data provided, and ties in to the declarations and commitments made under Control no. 1.1. – given that CSPs which act as processors are legally obliged to comply with controllers' instructions regarding personal data processing, this control requires CSPs to delve deeper into the details of how this obligation will be performed, by clearly informing customers of how they will be able to exercise this right.

The CSP must specify to cloud customers:

15. How the cloud customers will be informed about relevant changes concerning relevant cloud service(s), such as the implementation or removal of functions.[64] [C & P]

Relevance: This control arguably exceeds the requirements of the GDPR, born out of the Article 29 Working Party's recommendations in A.29WP05/2012[65]. There, WP29 stresses that, to ensure legal certainty, CSPs acting as processors must provide certain safeguards in the contracts they sign with cloud customers, among which is the obligation to inform customers where relevant changes are to be implemented in the services provided, such as the addition of functions to those services. This control goes beyond WP29's recommendations, by expressly identifying also the removal of functions as a relevant change to be communicated to customers and, more importantly, by extending this obligation to all CSPs which adhere to the CoC, regardless of whether they act as processors in relation to a given processing activity or cloud customer.

Changing features can have a relevant impact on the cloud customer's data governance. As this is not expressly handled by the GDPR, and the WP29 Opinion recommending it predates the GDPR, the CoC seeks to re-establish this best practice into the current legal framework.

[64] A.29WP05/2012, Section 3.4.2, p. 13. See also the 'Legal' Section of ICO Guidance Checklist, p. 22: "How will the cloud provider communicate changes to the cloud service which may impact on your agreement?" Note that CSP-controllers do not need to have changes approved by customers, whereas, CSP-processors do, and failure to do so may result in the CSP acting as controllers (see A.29WP01/2010').
[65] A.29WP05/2012, pp. 12-13.

2.3.2 PERSONAL DATA LOCATION

The CSP must specify to cloud customers:

1. The location(s) of all data centres or other data processing locations (by country) where person- al data may be processed,[66] and in particular, where and how data may be stored, mirrored, backed up, and recovered (this may include both digital and non-digital means). [C & P]

The CSP must also:

2. Notify cloud customers of any intended changes to these locations once a contract has been entered into, in order to allow the cloud customer to acknowledge or object. [C & P]

3. Allow cloud customers to terminate the contract in the event that an objection cannot be satisfactorily resolved between the CSP and the cloud customer, and afford the cloud customer sufficient time to procure an alternative CSP or solution (by establishing a transition period during which an agreed-upon level of services will continue to be provided to the cloud customer, under the contract). [C & P]

Relevance: Given the disparity in legal and material circumstances which may affect the security of personal data between countries – in particular, where those countries are outside of the EU and not covered by an adequacy decision given by the European Commission – it is vital for CSPs to clearly inform cloud customers of the locations where their personal data may be processed, both initially and during the course of the provision of the services. Without this information, cloud customers will not be given a full, clear picture of the implications in engaging a CSP – which is why the CoC obliges CSPs to disclose this information.

Customers should also be informed when changes of location are to take place after the performance of services has begun, and allowed to acknowledge or object to these changes. In the event that an objection cannot be resolved, the cloud customer may terminate the contract. In this case, the cloud customer and CSP must agree on a transitional period during which the CSP will continue to provide a set level of services to the customer, while the customer procures a suitable alternative to the services

[66] A.29WP05/2012, Section 3.4.1.1, p. 11 and Section 3.4.2, p. 13. See also the principle of 'location transparency,' Sopot Memorandum," p. 4 and CNIL's Recommendations, p. 14. See also the 'Legal' Section of ICO Guidance Checklist, p. 22: "Which countries will your cloud provider process your data in and what information is available relating to the safeguards in place at these locations? Can you ensure the rights and freedoms of data sub- jects are protected? You should ask your cloud provider about the circumstances in which your data may be transferred to other countries. Can your cloud provider limit the transfer of your data to countries you consider appropriate?"

offered by the CSP, in order to prevent damages which may occur from an abrupt end to the provision of services for the cloud customer (e.g., sudden lack of availability of personal data).

2.3.3 SUBCONTRACTORS

The CSP must identify:

1. Subcontractors and subprocessors that participate in the data processing, along with the chain of accountabilities and responsibilities used to ensure that data protection requirements are fulfilled.[67] [C & P]

The CSP declares to cloud customers, and further ensures, that:

2. The CSP will not engage another processor without prior specific or general written authorization of the cloud customer.[68] [P]

The CSP declares to cloud customers, and further ensures, that the CSP:

3. Imposes on other processors the same data protection obligations stipulated between the CSP and the cloud customer, by way of a contract (or other binding legal act), in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of EU applicable law; [P]

4. Remains fully liable to the cloud customer for the performance of other processors' obligations, in case the other processors fail to fulfil their data protection obligations. [P]

The CSP must identify:

5. the procedures used to inform the cloud customer of any intended changes concerning the addition or replacement of subcontractors or subprocessors with customers retaining at all times the possibility to object to such changes or terminate the contract.[69] In the event of termination by the cloud customer, the cloud customer must be afforded sufficient time to procure an alternative CSP or solution (by establishing a transition period during which an agreed-

[67] See the concept of "layered services" in ICO Guidance, pp. 6-8.
[68] See Article 28.2. GDPR.
[69] A.29WP05/2012, Section 3.3.2, p. 10: "There should also be clear obligation of the cloud provider to name al the subcontractors commissioned (e.g., in a public digital register)." A.29WP05/2012, Section 3.4.2, p. 13. See also A.29WP05/2012 Section 3.4.1.1, pp. 10-11; ICO Guidelines, p.11; and Article 10 of the Directive 95/46/EC.

upon level of services will continue to be provided to the cloud customer, under the contract). [C & P]

Relevance: By means of these controls, the CoC imposes upon CSPs the unavoidable obligation to disclose clear information to customers on the processing / subcontracting chain which they may engage in order to provide the services, and to subject this to an authorisation (specific or general) from the customer. This was deemed vital to deal with the general practice of not disclosing this information within the cloud computing domain, in spite of the legal obligation under the GDPR to do so. The CoC seeks to ensure that this information is delivered to customers in a manner which is clear and truly accessible to them.

Furthermore, the CoC imposes upon CSPs obligations related to the "cascade of liability" (i.e., to assume full liability to the cloud customer for the performance of their processors and subcontractors), and strictly requires CSPs to impose upon those processors and subcontractors the same data protection obligations as stipulated with the customer – to combat the practice of generally stating that processors will be bound to some similar obligations, and to ensure that such obligations are materially equivalent, thereby adhering to the terms of Art. 28(4) GDPR. This is true also of the obligation to notify the customer of any intended addition or replacement of subcontractors or processors, allowing customers to object (in line with the general authorisation given) or refuse to authorise this change – ultimately, a stalemate here (where the customer and CSP cannot agree on how to resolve an objection) must allow the customer (and not the CSP) to terminate the agreement, providing the cloud customer sufficient time to adjust to the changes required.

2.3.4 INSTALLATION OF SOFTWARE ON CLOUD CUSTOMER'S SYSTEM

The CSP must indicate to cloud customers:

1. Whether the provision of the service requires the installation of software on the cloud customer's system (e.g., browser plug-ins) [C & P]

2. The software's implications from a data protection and data security point of view.[70] [C & P]

Relevance: This control is supported by a similar justification to Control no. 3.1.15., in that requiring software to be installed on customers' systems for services to be provided can have an impact on the customers' data governance (e.g., where this may imply an

[70] A.29WP05/2012, Section 3.4.1.1, p. 11.

additional collection or transfer of data), and is also born out of A.29WP05/2012[71]. Note that, although WP29 states that cloud customers should raise this matter ex ante (where not sufficiently addressed by the CSP), the CoC eliminates the need for this by requiring all CSPs to disclose implications for any software to be installed, from a data protection and data security point of view (such as whether any additional data will be collected, transferred or retained by the CSP via this software, and what security measures the software is subjected to, in as much detail as needed for customers to understand how relevant this installation may be from a compliance perspective) – regardless, it should be noted, of whether the CSP acts as a controller or processor.

2.3.5 DATA PROCESSING CONTRACT (OR OTHER BINDING LEGAL ACT)

2.4 RECORDKEEPING

The CSP must share with the cloud customers:

1. The model data processing contract (or other binding legal act) which will govern the processing carried out by the CSP on behalf of the cloud customer and set out the subject matter and duration of the processing, the type of personal data and categories of data subjects and the obligations and rights of the cloud customer. [P]

The contract or other legal act must stipulate, in particular, that the CSP will do the following:

2. Process personal data only upon documented instructions from the cloud customer, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the CSP is subject; in such a case, the CSP will inform the cloud customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest; [P]

3. Ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality, and that they do not process personal data except upon

[71] A.29WP05/2012, p. 11.

instructions from the cloud customer, unless otherwise required by Union or Member State law;[72] [P]

4. Implement all technical and organizational security measures which the CSP deems adequate, in light of the available technology, the state of the art, the costs in implementing those measures and the processing activities inherent to the services provided, to ensure that the CSP's services are covered by a level of security which is appropriate, considering the potential risks to the interests, rights and freedoms of data subjects;[73] [P]

5. Respect the conditions for engaging another processor[74] (see Control no. 3.3., above); [P]

6. Taking into account the nature of the processing, assist the cloud customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the cloud customer's obligation to respond to requests for exercising the data subject's rights;[75] [P]

7. Assist the cloud customer in ensuring compliance with obligations related to security of processing,[76] notification of a personal data breach to the Supervisory Authority;[77] communication of a personal data breach to the data subject,[78] and data protection impact assessment;[79] taking into account the nature of processing and the information available to the processor; [P]

8. At the choice of the cloud customer, delete or return all personal data to customer after end of the provision of services relating to processing; and delete existing copies unless Union or Member State law requires storage of the personal data; (see Control no. 11., below) [P]

9. Make available to the cloud customer all information necessary to demonstrate compliance with relevant data protection obligations; and allow for and contribute to audits, including inspections, conducted by the cloud customer or another auditor mandated by the customer. [P]

Relevance: This control is a formal requirement, seeking, as a first goal, to reproduce the formal obligations contained within Art. 28 GDPR, in order to ensure that all

[72] See Article 32.4. GDPR.
[73] See Article 32 GDPR.
[74] See Article 28.2 and 28.4.
[75] See Chapter III GDPR.
[76] See Article 32 GDPR.
[77] See Article 33 GDPR.
[78] See Article 34 GDPR.
[79] See Article 35 GDPR.

contracts entered into by CSPs with cloud customers will meet the minimum legal requirements. However, the CoC goes beyond this, by not only reaffirming these requirements but also further specifying them – as seen, e.g., in the commitment to respect the conditions required in order to engage other processors (wherein the CoC, under Control no. 3.3., imposes upon CSPs the obligation to provide clear and transparent information on their entire processing chain – both initially and regarding any subsequent intended changes – and to offer customers the ability to terminate the agreement in the event that their objection to a change in processors cannot be resolved) and in the requirement to delete or return all personal data to customers after services have ended (which, under Control no. 11.4., also obliges CSPs to offer information as to the methods in place to delete or return the data).

2.4.1 RECORDKEEPING FOR CSP-CONTROLLER

A CSP-controller confirms to the cloud customers and commits:

1. To maintain a record of processing activities under CSP responsibility and make it available to the Supervisory Authority on request. [C]

The record must contain the following information:

2. Name and contact details of controller and, where applicable, the joint controller, the controller's representative and the data protection officer; [C]

3. The purposes of the processing; [C]

4. A description of the categories of data subjects and of the categories of personal data; [C]

5. Categories of recipients to whom the personal data have been or will be disclosed, including recipients in third countries or international organisations; [C]

6. 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 the documentation of suitable safeguards; [C]

7. Where possible, the envisaged time limits for erasure of different categories of data or, if that is not possible, the criteria used to determine that period; [C]

8. A description of technical and organisational security measures in place (see also Control no. 6., below).[80], [81] [C]

2.4.2 RECORDKEEPING FOR CSP-PROCESSOR

A CSP-processor confirms to the cloud customers and commits:

1. To maintain a record of all categories of processing activities carried out on behalf of a controller and make it available to the Supervisory Authority upon request. [P]

The record must contain the following information:

2. 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; [P]

3. Categories of processing carried out on behalf of each controller; [P]

4. 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 the documentation of suitable safeguards; [P]

5. A description of technical and organisational security measures in place (see also Control no. 6., below).[82],[83] [P]

[80] See Control no. 6., below; and Article 35 GDPR.

[81] See Article 30.1. GDPR and Article 30.5. GDPR which set forth the following limitation: "The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9 (1) or personal data relating to criminal convictions and offences referred to in Article 10.". However, see also the clarification provided by the Article 29 Working Party in their Position Paper on the derogations from the obligation to maintain records of processing activities pursuant to Article 30(5) GDPR (available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=624045), in which the applicability of this limitation is restricted.

[82] See Section 6 "Data security measures", below; and Article 35 GDPR.

[83] See Article 30.2. GDPR and Article 30.5. GDPR, which set forth the following limitation: "The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9 (1) or personal data relating to criminal convictions and offences referred to in Article 10." However, see also the clarification provided by the Article 29 Working Party in their Position Paper on the derogations from the obligation to maintain records of processing activities pursuant to Article 30(5) GDPR (available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=624045), in which the applicability of this limitation is restricted.

Relevance: This control seeks to extend recordkeeping obligations, by requiring all CSPs – acting as controllers or processors – to keep detailed records containing the above information, regardless of whether the exception laid down in Art. 30(5) GDPR might apply to a CSP or not (considering also WP29's latest position on this exception, in their Position Paper on the derogations from the obligation to maintain records of processing activities pursuant to Article 30(5) GDPR[84] which dramatically reduced its scope of application). This is required of all CSPs due to the keeping of complete records being a fundamental tool in ensuring transparency and increasing controls on the CSPs compliance, as well as being a primary means of allowing the CSP to demonstrate compliance under the principle of accountability.

2.5 DATA TRANSFER

The CSP must clearly indicate:

1. Whether data is to be transferred, backed up and/or recovered across borders, in the regular course of operations or in an emergency. [C & P]

Relevance: The purpose of this control, in practice, is to allow cloud customers to clearly understand the flows of data inherent to the provision of a CSP's services. The CoC sees this control as important in order to shed light on practices which, in the cloud computing domain, are generally unclear to data subjects. CoC adherents remain free to comply with this control in the manner that they see as most adequate, provided that the end result is a clear and complete indication to cloud customers of how personal data will flow across borders in connection with the services – for instance, the use of pictures and data flow diagrams, accompanying a verbal explanation, may help to make the provision of this information transparent to customers.

If such transfer is restricted under applicable EU law, the CSP must clearly identify:

2. The legal ground for the transfer (including onward transfers through several layers of subcontractors),[85] e.g., European Commission adequacy decision, model contracts/standard data protection clauses,[86] approved codes of

[84] Available at: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=624045.
[85] See ICO Guidance p. 18.
[86] See Article 44 ff. GDPR. See A29WP05/2012, Section 3.5.3, p. 18.

conduct[87] or certification mechanisms,[88] binding corporate rules (BCRs),[89] and Privacy Shield.[90] [C & P]

Relevance: It is further important for CSPs to clearly identify the legal mechanisms relied on for any transfers of personal data from within the EU to outside the EU (and onward transfers outside the EU), under Arts. 45 to 49 GDPR, in order for cloud customers to be able to properly evaluate whether such mechanisms are adequate and fit for the purposes the customer wishes to achieve in engaging the CSP. Certain customers may wish to engage CSPs relying on certain transfer mechanisms (e.g., favouring model contracts / standard data protection clauses over the Privacy Shield, when data are transferred to the US). The bottom line is that CSPs must provide to cloud customers all information related to the legal mechanisms which support the transfers disclosed, so that customers are able to make an informed decision on whether these are appropriate or not.

2.6 DATA SECURITY MEASURES

Preliminarily, the CSP should note that: "… [C]loud computing services are considered as Digital Service Providers (DSPs) in the context of the recently adopted Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union."[91] In completing this section, which is based on A.29WP05/2012, CSPs are required to follow the ENISA Guidelines of February 16, 2017[92] as a minimum acceptable baseline (controls provided below). Moreover,

[87] Pursuant to Article 40 GDPR.
[88] Pursuant to Article 42 GDPR.
[89] See A29WP05/2012, Section 3.5.4, p. 19.
[90] The European Commission adopted on 12 July 2016 its decision on the EU-U.S. Privacy Shield: http://ec.europa.eu/justice/data-protection/international-transfers/eu-us-privacy-shield/index_en.htm; Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield (notified under document C(2016) 4176). See https://www.privacyshield.gov/welcome. Please note that on 6 October 2015 the European Court of Justice declared invalid the Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46 on the adequacy of the protection provided by the Safe Harbor privacy principles and related frequently asked questions issued by the U.S. Department of Commerce (OJ 2000 L 215, p. 7), Judgment of the Court - 6 October 2015 Schrems Case C-362/14. (http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=876554).
[91] See ENISA Guidelines, February 16, 2017, p. 6.
[92] See also National Cyber Security Centre: Guidance Implementing the Cloud Security Principles (https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles) and The CNIL's Guides – 2018 Edition: Security of Personal Data (https://www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle_gb_web.pdf)

evidence of data security compliance may also be provided to cloud customers by way of adherence to relevant codes of conduct, and certification mechanisms.[93]

Taking into account the state of the art, costs of implementation and the nature, scope, context and purposes of processing, as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the CSP must:[94]

1. Specify to cloud customers the technical, physical and organisational measures that are in place to protect personal data against accidental or unlawful destruction; or accidental loss, alteration, unauthorised use, unauthorised modification, disclosure or access; and against all other unlawful forms of processing;[95] [C & P]

2. Describe to cloud customers the concrete technical, physical, and organisational measures (protective, detective and corrective) that are in place to ensure the following safeguards:[96] [C & P]

    i. Availability[97] - processes and measures in place to manage risk of disruption and to prevent, detect and react to incidents, such as backup Internet network links, redundant storage and effective data backup, restore mechanisms and patch management;[98] [C & P]

[93] See Articles 32.3, 40 and 42 GDPR.
[94] See Article 32 GDPR.
[95] See Article 32 GDPR. "Security of processing: 1. 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, including inter alia as appropriate: (a) the pseudonymisation and encryption of personal data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. 2. In assessing the appropriate level of security, account shall be taken in particular of the risks presented by processing from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed. 3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article. 4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law."
[96] A.29WP05/2012, Section 3.4.2, p. 13. See also ICO Guidance, pp. 13-14.
[97] See the 'Availability' Section of ICO Guidance Checklist, p. 22: "Does the cloud provider have sufficient capacity to cope with a high demand from a small number of other cloud customers? How could the actions of other cloud customers or their cloud users impact on your quality of service? Can you guarantee that you will be able to access the data or services when you need them? How will you cover the hardware and connection costs of cloud users accessing the cloud service when away from the office? If there was a major outage at the cloud provider how would this impact on your business?"
[98] A.29WP05/2012, Section 3.4.3.1, p.14.

ii. Integrity[99] - methods by which the CSP ensures integrity[100] (e.g., detecting alterations to personal data by cryptographic mechanisms such as message authentication codes or signatures, error-correction, hashing, hardware radiation/ionization protection, physical access/compromise/destruction, software bugs, design flaws and human error, etc.);[101] [C & P]

iii. Confidentiality[102] - methods by which the CSP ensures confidentiality from a technical point of view in order to assure that only authorised persons have access to data; Including, inter alia as appropriate, pseudonymisation and encryption of personal data[103] "in transit" and "at rest",[104] authorisation mechanism and strong authentication;[105] and from a contractual point of view, such as confidentiality agreements, confidentiality clauses, company policies and procedures binding upon the CSP and any of its employees (full time, part time and contract employees), and subcontractors who may be able to access data; [C & P]

iv. Transparency - technical, physical and organisational measures the CSP has in place to support transparency and to allow review by customers (see, e.g., Control no. 7., below);[106] [C & P]

[99] See the 'Integrity' Section of ICO Guidance Checklist, p. 22: "What audit trails are in place so you can monitor who is accessing which data? Make sure that the cloud provider allows you to get a copy of your data, at your request, in a usable format. How quickly could the cloud provider restore your data (without alteration) from a back-up if it suffered a major data loss?"

[100] The description should concern all data layers within the CSP, from the customer's information context, through to physical data components and software codes.

[101] A.29WP05/2012, Section 3.4.3.2, p.15. See also ICO Guidance, p. 22: "Make sure that the cloud provider allows you to get a copy of your data, at your request, in a usable format."

[102] See the 'Confidentiality' Section of ICO Guidance Checklist, p. 22: Can your cloud provider provide an appropriate third-party security assessment? Does this comply with an appropriate industry code of practise or other quality standard? How quickly will the cloud provider react if a security vulnerability is identified in their product? What are the timescales and costs for creating, suspending and deleting accounts? Is all communication in transit encrypted? Is it appropriate to encrypt your data at rest? What key management is in place? What are the data deletion and retention timescales? Does this include end-of-life destruction? Will the cloud provider delete all of your data securely if you decide to withdraw from the cloud in the future? Find out if your data, or data about your cloud users will be shared with third parties or shared across other services the cloud provider may offer.

[103] See Article 32.1 (a) GDPR.

[104] Please note: "Encryption of personal data should be used in all cases when 'in transit' and when available to data 'at rest.' … Communications between cloud provider and client, as well as data centres, should be encrypted." A.29WP05/2012, Section 3.4.3.3, p.15. See also ICO Guidance, pp. 14-15.

[105] A.29WP05/2012, Section 3.4.3.3, p. 15.

[106] A.29WP05/2012, Section 3.4.3.4, p. 15. Moreover, "Transparency is of key importance for a fair and legitimate processing of personal data. Directive 95/46/EC obliges the cloud client to provide a data subject from whom data relating to himself are collected with information on his identity and the purpose of the processing. The cloud client should also provide any further information such as on the recipients or categories of recipients of the data, which can also include processors and sub-processors in so far as such further information is necessary to guarantee fair processing in respect of the data subject (see Article 10 of the Directive) Transparency must also be ensured in the relationship(s) between cloud client, cloud provider and subcontractors (if any). The cloud client is only capable of assessing the lawfulness of the processing of personal data in the cloud if the provider informs

v. Isolation (purpose limitation) - how the CSP provides appropriate isolation to personal data (e.g., adequate governance of the rights and roles for accessing personal data (reviewed on a regular basis), access management based on the "least privilege" principle; hardening of hypervisors;[107] and proper management of shared resources wherever virtual machines are used to share physical resources among cloud customers);[108] [C & P]

vi. Intervenability - methods by which the CSP enables data subjects' rights of access, rectification, erasure ("right to be forgotten"),[109] blocking, objection, restriction of processing[110] (see Control no. 10., below), portability[111] (see Control no. 9., below) in order to demonstrate the absence of technical and organisational obstacles to these requirements, including cases when data are further processed by subcontractors[112] (this is also relevant for Control no. 9., below); [C & P]

vii. Portability - see Control no. 9., below; [C & P]

viii. Accountability - see Control no. 1., above. [C & P]

Relevance: As the GDPR does not provide a clear structure or prescriptive rules on the implementation of specific security measures, the CoC leverages relevant guidelines from multiple competent authorities and relevant agencies / bodies – such as WP29/EDPB, the CNIL, the ICO, ENISA and ISO – in order to impose upon CSPs a structured manner in which to disclose information on the technical and organisational measures in place to ensure the security of processing inherent to their services.

It is understood that providing specific, "one-size-fits-all" security measures to be implemented, regardless of the risks to the rights and freedoms of the data subjects and technological developments, would run counter to the idea behind Art. 32 GDPR. It must also be noted that all adherents to the CoC will have access to the CSA's knowledge and

the client about all relevant issues. A controller contemplating engaging a cloud provider should carefully check the cloud provider's terms and conditions and assess them from a data protection point of view. Transparency in the cloud means it is necessary for the cloud client to be made aware of all subcontractors contributing to the provision of the respective cloud service as well as of the locations of all data centre personal data may be processed. If the provision of the service requires the installation of software on the cloud client's systems (e.g., browser plug-ins), the cloud provider should as a matter of good practise inform the client about this circumstance and in particular about its implications from a data protection and data security point of view. Vice versa, the cloud client should raise this matter ex ante, if it is not addressed sufficiently by the cloud provider." A.29WP05/2012, Section 3.4.1.1, pp. 10-11.

[107] "[H]ardening of hypervisors" is also relevant to 'Integrity', see Section 6 'Data security measures', above.

[108] A.29WP05/2012, Section 3.4.3.5, p. 16. See also ICO Guidance p. 20.

[109] Article 17 GDPR.

[110] Article 18 GDPR.

[111] Article 20 GDPR.

[112] A.29WP05/2012, Section 3.4.3.5, p. 16.

resources on data and information security, which will allow those CSPs to become aware of and implement the most relevant measures in light of the offerings on the market, the costs of implementation, the characteristics of the processing operations carried out and the inherent risks which those operations present to data subjects. Thus, CSPs will be required, under Art. 32 GDPR, to take responsibility for establishing the most appropriate security measures to be implemented given the resources made available to them, and to disclose information on the measures chosen and put in place following the structure within this control – this will allow a more coherent and clear provision of information to cloud customers, which will more easily understand exactly what is offered by each CSP in terms of security.

In any case, it is inherent to the scope of the CoC to provide as much guidance as possible, in order to establish best practices on data protection. Accordingly, the following control provides guidelines on minimum acceptable security measures which all CSPs must have in place, by reference to the ENISA's Technical Guidelines on the matter.

3. As a minimum acceptable baseline, this CoC requires CSPs to comply with the controls set out in ENISA's Technical Guidelines for the implementation of minimum security measures for Digital Service Providers; for each control, the tables on sophistication levels regarding security measures provided in the ENISA's Technical Guidelines will apply, and the CSP must indicate the appropriate sophistication level complied with per each control (1 to 3), taking into account the state of the art, costs of implementation and the nature, scope, context and purposes of processing, as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons[113]: [C & P]

   It shall be noted that not all the minimum security measures listed in the ENISA's Technical Guidelines are directly applicable to all the CSPs. For instance, the requirements SO08 or SO09 cannot be directly implemented by a PaaS or SaaS providers. In any case, if some of the below mentioned security measures cannot be directly implemented by a CSP, the CSP in question shall nonetheless guarantee their implementation through their providers.

   i. (SO 01) – Information security policy: The CSP establishes and maintains an information security policy. The document details information on main assets and processes, strategic security objectives. [C & P]

   ii. (SO 02) – Risk Management: The CSP establishes and maintains an appropriate governance and risk management framework, to identify and address risks for the security of the offered services. Risks management procedures can include

[113] CSPs may also take into consideration the CNIL's Guide on Security of Personal Data (2018), available at https://www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle_gb_web.pdf.

(but are not limited to), maintaining a list of risks and assets, using Governance Risk management and Compliance (GRC) tools and Risk Assessment (RA) tools etc. [C & P]

iii. (SO 03) – Security Roles: The CSP assigns appropriate security roles and security responsibilities to designated personnel. (i.e. CSO, CISO, CTO etc.). [C & P]

iv. (SO 04) – Third party management: The CSP establishes and maintains a policy with security requirements for contracts with suppliers and customers. SLAs, security requirements in contracts, outsourcing agreements etc., are established to ensure that the dependencies on suppliers and residual risks do not negatively affect security of the offered services. [C & P]

v. (SO 05) – Background checks: The CSP performs appropriate background checks on personnel (employees, contractors and third party users) before hiring, if required, for their duties and responsibilities provided that this is allowed by the local regulatory framework. Background checks may include checking past jobs, checking professional references, etc. [C & P]

vi. (SO 06) – Security knowledge and training: The CSP verifies and ensures that personnel have sufficient security knowledge and that they are provided with regular security training. This is achieved through for example, security awareness raising, security education, security training etc. [C & P]

vii. (SO 07) – Personnel changes: The CSP establishes and maintains an appropriate process for managing changes in personnel or changes in their roles and responsibilities. [C & P]

viii. (SO 08) – Physical and environmental security: The CSP establishes and maintains policies and measures for physical and environmental security of datacentres such as physical access controls, alarm systems, environmental controls and automated fire extinguishers etc. [C & P]

ix. (SO 09) – Security of supporting utilities: The CSP establishes and maintains appropriate security measures to ensure the security of supporting utilities such as electricity, fuel, HVAC etc. For example, this may be through the protection of power grid connections, diesel generators, fuel supplies, etc. [C & P]

x. (SO 10) – Access control to network and information systems: The CSP established and maintains appropriate policies and measures for access to business resources. For example, zero trust model, ID management,

authentication of users, access control systems, firewall and network security etc. [C & P]

xi. (SO 11) – Integrity of network components and information systems: The CSP establishes, protects, and maintains the integrity of its own network, platforms and services by taking steps to prevent successful security incidents. The goal is the protection from viruses, code injections and other malware that can alter the functionality of the systems or integrity or accessibility of information. [C & P]

xii. (SO 12) – Operating procedures: The CSP establishes and maintains procedures for the operation of key network and information systems by personnel. (i.e. operating procedures, user manual, administration procedures for critical systems etc.). [C & P]

xiii. (SO 13) – Change management: The CSP establishes and maintains change management procedures for key network and information systems. These may include for example, change and configuration procedures and processes, change procedures and tools, procedures for applying patches etc. [C & P]

xiv. (SO 14) – Asset management: The CSP establishes and maintains change management procedures for key network and information systems. These may include for example, change and configuration procedures and processes, change procedures and tools, procedures for applying patches etc. [C & P]

xv. (SO 15) – Security incident detection & Response: The CSP establishes and maintains procedures for detecting and responding to security incidents appropriately. These should consider detection, response, mitigation, recovery and remediation from a security incident. Lessons learned should also be adopted by the service provider. [C & P]

xvi. (SO 16) – Security incident reporting: The CSP establishes and maintains appropriate procedures for reporting and communicating about security incidents. [C & P]

xvii. (SO 17) – Business continuity: The CSP establishes and maintains contingency plans and a continuity strategy for ensuring continuity of the services offered. [C & P]

xviii. (SO 18) – Disaster recovery capabilities: The CSP establishes and maintains an appropriate disaster recovery capability for restoring the offered services in case of natural and/or major disasters. [C & P]

xix. (SO 19) – Monitoring and logging: The CSP establishes and maintains procedures and systems for monitoring and logging of the offered services (logs of user actions, system transactions/performance monitors, automated monitoring tools etc.). [C & P]

xx. (SO 20) – System test: The CSP establishes and maintains appropriate procedures for testing key network and information systems underpinning the offered services. [C & P]

xxi. (SO 21) – Security assessments: The CSP establishes and maintains appropriate procedures for performing security assessments of critical assets. [C & P]

xxii. (SO 22) – Compliance: The CSP establishes and maintains a policy for checking and enforcing the compliance of internal policies against the national and EU legal requirements and industry best practices and standards. These policies are reviewed on a regular basis. [C & P]

xxiii. (SO 23) – Security of data at rest: The CSP establishes and maintains appropriate mechanisms for the protection of the data at rest. [C & P]

xxiv. (SO 24) – Interface security: The CSP should establish and maintain an appropriate policy for keeping secure the interfaces of services which use personal data. [C & P]

xxv. (SO 25) – Software security: The CSP establishes and maintains a policy which ensures that the software is developed in a manner which respects security. [C & P]

xxvi. (SO 26) – Interoperability and portability: The CSP uses standards which allow customers to interface with other digital services and/or if needed to migrate to other providers offering similar services. [C & P]

xxvii. (SO 27) – Customer Monitoring and log access: The CSP grants customers access to relevant transaction and performance logs so customers can investigate issues or security incidents when needed. [C & P]

2.7 MONITORING

The CSP must indicate to cloud customers:

1. The options that the CSP has in place to allow the customer to monitor and/or audit in order to ensure appropriate privacy and security measures described in the PLA are

met on an on-going basis (e.g., logging, reporting, first- and/or third-party auditing[114] of relevant processing operations performed by the CSP or subcontractors).[115] Any audits carried out which imply that an auditor will have access to personal data stored on the systems used by the CSP to provide the services will require that auditor to accept a confidentiality agreement. [C & P]

Relevance: This control further specifies Art. 28(3)(h) GDPR, by imposing upon CSPs the obligation to inform cloud customers as to their specific options for effectively monitoring CSPs' compliance and to audit the privacy and security measures they have implemented regarding the processing activities inherent to the services. CSPs are given options as to how this can be done – such as maintaining logs which customers can monitor, periodic reporting to customers or relying upon first-party or third-party audits performed upon their operations, and those of subcontractors or processors engaged. This control also goes beyond the minimum required by the GDPR in that it imposes this obligation also upon CSPs acting as controllers (joint or not), by subjecting them also to monitoring and audits towards cloud customers as if they acted as processors.

2.8 PERSONAL DATA BREACH

"Personal data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed,[116] in connection with the provision of a service provided by a CSP.[117]

The CSP must specify to cloud customers:

1. How the customer will be informed of personal data breaches affecting the customer's data processed by the CSP and/or its subcontractors, without undue delay and, where feasible[118], no later than 72 hours from the moment on which the CSP

[114] See the 25 August 2014 Decision of CNIL, which evokes the lack of a security audit: http://www.cnil.fr/nc/linstitution/actualite/article/article/la-societe-orange-sanctionnee-pour-defaut-de-securite-des-donnees-dans-le-cadre-de-campagnes/; http://www.cnil.fr/fileadmin/documents/approfondir/deliberations/Formation_contentieuse/D2014-298_avertissement_ORANGE.pdf.

[115] See Article 28.3 (h) GDPR and Section 1 "CSP declaration of compliance and accountability." See A.29WP05/2012, Section 3.4.2, p. 13 and Section 3.4.1.2, p. 11. See also ICO Guideline, pp. 13.14.

[116] Article 4.(12) GDPR.

[117] See A.29WP250/17-rev.01.

[118] As further detailed in the 'Relevance' section of this control, the investigation of a potential personal data breach by a CSP may take some time, particularly in terms of correcting identifying the scope of the breach. Aside from practical and technical complications in the identification and assessment of breaches, there may also be similar complications in the notification of those breaches, particularly where a large number of cloud customers may

becomes aware of the incident in question[119,120]. A CSP will be considered as "aware" of a personal data breach on the moment that it detects (e.g., directly, or due to a notification received from a subcontractor/sub-processor) an incident which qualifies as a personal data breach **and** establishes that that incident has affected data processed by the CSP and/or its subcontractors on behalf of a given customer. Should it not be feasible to inform a given customer of a personal data breach within the 72-hour deadline, the CSP will inform that customer of the personal data breach as soon as possible and accompany this communication to the customer with reasons for the delay. [C & P]

In this respect, the details given to a customer regarding a personal data breach must, at least and to the maximum extent possible, include the below information:

2. Describe the nature of the personal data breach including, where possible, the categories and approximate number of personal data records concerned; [C & P]

3. Communicate the name and contact details of the data protection officer or other contact point where more information can be obtained (see Section 2, "CSP relevant contacts and its role", above); [C & P]

4. Describe the likely consequences of the personal data breach; [C & P]

5. Describe the measures taken (or proposed to be taken) to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.[121] [C & P]

6. Where it is not feasible to provide all of the above information in an initial notification, the CSP must provide as much information to the customer as possible on the reported incident, and provide any further details needed to meet the above requirement as soon as possible (i.e., provision of information in phases).[122] [C & P]

have been affected. In order to avoid premature, unnecessary and incomplete notifications to the greatest extent possible, and to make this Control practically implementable for CSPs, it was considered reasonable to set for CSPs the same notification deadline to customers as the GDPR sets for controllers to notify Supervisory Authorities – i.e., 72 hours from the moment on which a CSP becomes aware of a personal data breach, where feasible.

[119] See Articles 33 and 34 GDPR. Moreover, in Germany there is a statutory data breach notification requirement that went into effect on September 1, 2009; see Section 42 (a) of the German Federal Data Protection Act. See also "Frequently Asked Questions about the German statutory data breach notification requirement": http://www.datenschutz-berlin.de/content/themen-a-z/informationspflicht-nach-42-a-bdsg. In the Netherlands, on 1 January 2016, a data breach notification obligation entered into force; See https://autoriteitpersoonsgegevens.nl/en/news/data-breach-notification-obligation. See also A.29WP05/2012, Section 3.4.2, p. 13.

[120] See EDPS Guidelines November 21, 2018, p. 15.

[121] See Article 33 GDPR.

[122] See A.29WP250/17-rev.01, pp. 13-14: "The GDPR does not provide an explicit time limit within which the processor must alert the controller, except that it must do so "without undue delay". Therefore, WP29 recommends

The CSP must also specify:

7. How the competent Supervisory Authority/ies will be informed of personal data security breaches, in less than 72 hours of becoming aware of a personal data breach); [C]

8. How data subjects will be informed, without undue delay, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.[123] [C]

Relevance: CSPs are required to specify how and when customers will be informed that a personal data breach has occurred, in order to provide transparency to customers over a procedure which must be made very clear to customers (particularly because cloud customers will typically act as data controllers and may rely on CSPs to provide them the necessary information for customers to comply with their own notification, communication and recording obligations relative to breaches). CSPs must not only identify that a breach has taken place, but also provide the information which EU Supervisory Authorities will request in connection with notifications of a breach taken place, to the greatest extent feasible – where it is not possible to provide all required information at once, CSPs should nonetheless provide as much as possible in the first notification to customers and follow this up with the missing details as soon as this is possible.

A timeframe for CSPs to notify affected customers of a detected personal data breach has been defined as a baseline, which must be met whenever feasible. There are several practical circumstances which may lead to delays in the CSP's ability to properly identify, assess and communicate a personal data breach to cloud customers. Given that CSPs are required to notify actual personal data breaches, rather than all incidents which might potentially qualify as a breach, CSPs will be required to investigate security incidents occurred and correctly identify their scope. This work may be more arduous and time-consuming for smaller CSPs, which may not have the staff or processes in place to allow an immediate identification or assessment of a potential breach (including where incident handling may have been outsourced to third parties). Finally, there are also technical circumstances to be considered regarding the actual notification, as where an actual personal data breach affects a large number of cloud customers for a CSP, the process of setting up and issuing the notifications to be sent out may take time (in particular due to the need to avoid spamming filters, or other mechanisms designed to stop

the processor promptly notifies the controller, with further information about the breach provided in phases as more details become available. This is important in order to help the controller to meet the requirement of notification to the supervisory authority within 72 hours".

[123] See Article 33 GDPR. See also Article 34 GDPR.

mass emails). Furthermore, large-scale breach notifications may also have relevant effects with respect to the application of other legislation – e.g., accidental notification to certain cloud customers may put them at risk of insider trading; certain local laws may require CSPs to notify law enforcement authorities directly in the event of breaches of criminal relevance (possibly without notifying the cloud customer) – which therefore requires a series of prior legal checks to be carried out before such external communications are completed.

These and other examples are considered as supporting the argument that CSPs should be subjected, regarding their obligation to report breaches to cloud customers, to the same timeframe that the GDPR affords to controllers vis-à-vis Supervisory Authorities: i.e., 72 hours from the moment on which the CSP becomes 'aware' of the breach (i.e., where it has identified that a breach has taken place and has affected a given customer), whenever feasible. In any case where the 72-hour deadline cannot feasibly be met, the CSP should nonetheless inform the customer as soon as possible, and provide reasons for this delay. Naturally, CSPs may also wish to provide shorter deadlines for incident response in their agreements with customers, particularly where their customers belong to specific sectors (including EU institutions and agencies[124]) which may be subjected to tighter notification requirements.

This requirement goes far beyond the GDPR's legal requirements, also in that it is extended to CSP-controllers (not just processors), which must provide the above information to cloud customers as well as clearly identify how the CSPs themselves will handle the process of notifying Supervisory Authorities (e.g., by filling out online forms provided by the authorities and reaching out to authorities directly, over a phone call or in-person meeting) and communicating to data subjects, where relevant (e.g., by creating a dedicated website to provide information and regular updates on the status of a breach and its mitigation). CSPs may also inform customers that they rely on expert third parties, such as privacy consultants, to manage any breaches which take place.

[124] Entities that are subject to compliance with Regulation (EU) 2018/1725 of the European Parlliament and of the Council, of 23 October 2018.

2.9 DATA PORTABILITY, MIGRATION, AND TRANSFER BACK

The CSP must specify to cloud customers:

1. How the CSP assures data portability, in terms of the capability to transmit personal data in a structured, commonly used, machine-readable and interoperable format:[125] [C & P]

    i. To the cloud customer ("transfer back", e.g., to an in-house IT environment); [C & P]

    ii. Directly to the data subjects; [C & P]

    iii. To another service provider ("migration"), e.g., by means of download tools or Application Programming Interfaces, or APIs).[126] [C & P]

[125] See Recital 68 GDPR.

[126] The right to data portability is granted to data subjects, who, in most cases, are customers of the cloud customer. More precisely, pursuant to Article 20 GDPR, "The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where: (a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and (b) the processing is carried out by automated means. 2. In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible." This means that the cloud customer must make sure CSPs, which process personal data on behalf of the controller-cloud customer, assure data portability. Obviously, data portability must be assured by the CSPs when they process data as data controllers. See A.29WP242/16-rev.01 for practical guidelines, best practises and tools that support compliance with the right to data portability. The right to data portability is a new right introduced by the GDPR. However, even before the GDPR will be directly applicable in the EU Member States (25 May 2018), there seems to be enough ground for considering data portability as a mandatory requirement pursuant to general EU personal data protection principles, such as "data accuracy" (Article 6.1.d of Directive 95/46/EC), "data availability" and possibility to grant data subjects' rights per Sections 11.1.c and 12 of Directive 95/46/EC. See also A29WP05/2012, Section 3.4.3.6, p.16 and ICO Guidance, p. 22: "Make sure that the cloud provider allows you to get a copy of your data, at your request, in a usable format. Moreover, see Section 5.4 of the Data Portability of the Cloud Service Level Agreement Standardisation Guidelines: "5.4. Data Portability.

Description of the context or of the requirement

The following list of SLOs is related with the CSP capabilities to export data, so can still be used by the customer e.g., in the event of terminating the contract.

Description of the need for SLOs, in addition to information available through certification

In related security controls frameworks and certifications the implementation of data portability controls usually focuses on the specification of applicable CSP policies, which makes it difficult (and sometimes impossible) for cloud service customers to extract the specific indicators related with available formats, interfaces and transfer rates. The following list of SLOs focuses on these three basic aspects of the CSP data portability features, which can be used by the customer e.g., to negotiate the technical features associated with the provider's termination process.

The CSP must describe to cloud customers:

2. How and at what cost the CSP will assist customers in the possible migration of data to another provider or back to an in-house IT environment.[127] Whatever the procedure implemented, the CSP must cooperate in good faith with cloud customers, by providing a reasonable solution. [C & P]

Relevance: This control does not merely mirror the obligations relative to the right to data portability in the GDPR. It goes further, by extending this right to cloud customers themselves (which, in a B2B context, will not be data subjects). The CSPs must assure that the right to portability can be triggered by cloud customers even in the absence of a request from a data subject, which reflects a vast extension of the GDPR's terms for the right to data portability. The key for cloud customers is that, in doing business with CSPs which have adhered to the CoC, they will be in control of their data.

The above this applies not only to portability, per se, but also to the migration of data to other providers and the "transfer-back" of data to the cloud customer's in-house IT environment.

2.10 RESTRICTION OF PROCESSING

The CSP must explain to cloud customers:

1. How the possibility of restricting the processing of personal data is granted; considering that where processing has been restricted, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims, or for the protection of the rights of another natural or legal person, or for rea- sons of important public interest of the Union or of a Member State.[128] [C & P]

Description of relevant SLOs

Data portability format: electronic format(s) in which cloud service customer data can be transferred to/accessed from the cloud service.

Data portability interface: mechanisms can be used to transfer cloud service customer data to and from the cloud service. This specification potentially includes the specification of transport protocols and the specification of APIs or of any other mechanism.

Data transfer rate: minimum rate at which cloud service customer data can be transferred to/from the cloud service using the mechanism(s) stated in the data interface."

[127] See A.29WP05/2012, Section 3.4.3.6, p. 16.

[128] See Article 18 GDPR. "Methods by which to restrict the processing of personal data could include, inter alia, temporarily moving the selected data to another processing system, making the selected personal data unavailable to users, or temporarily removing published data from a website. In automated filing systems, the restriction of processing should in principle be ensured by technical means in such a manner that the personal

Relevance: CSPs are required to clearly explain how the right to restriction of processing of personal data will be implemented in practice, for the specific situations in which it applies, under Art. 18 GDPR. Cloud customers should be able to understand not only when the right may be triggered (with reference to Art. 18 GDPR), but how the CSP will block use of the restricted data beyond storage or the other exceptions set out in the GDPR (e.g., exercise and defence of legal claims), as well as how the data will be marked as restricted within CSPs' systems.

2.11 DATA RETENTION, RESTITUTION, AND DELETION

2.11.1 DATA RETENTION, RESTITUTION, AND DELETION POLICIES

The CSP must describe to the cloud customers:

1. The CSP's data retention policies, timelines and conditions for returning personal data or deleting data once the service is terminated, [C & P]

2. As well as these policies, timelines and conditions for their subcontractors. [C & P]

2.11.2 DATA RETENTION

The CSP must indicate and commit to comply with:

1. The time period for which the personal data will or may be retained, or if that is not possible, the criteria used to determine such a period.[129] [C & P]

When defining retention periods, the CSP must consider the following criteria:

2. Necessity – Personal data is retained for as long as necessary in order to achieve the purpose for which it was collected, so long as it remains necessary to achieve that purpose (e.g., to perform the services); Legal Obligation –

data are not subject to further processing operations and cannot be changed. The fact that the processing of personal data is restricted should be clearly indicated in the system." Preamble 67 GDPR.

[129] Note that "[P]ersonal data must be erased [or anonymised] as soon as their retention is not necessary anymore." A.29WP05/2012, Section 3.4.1, 10 and "If this data cannot be erased due to legal retention rules (e.g., tax regulations), access to this personal data should be blocked." Section 3.4.1.3, pp. 11; and "Since personal data may be kept redundantly on different servers at different locations, it must be ensured that each instance of them is erased irretrievably (i.e., previous versions, temporary and even file fragments are to be deleted as well)." See Article 6 of the Directive 95/46/ EC, Articles 5 and Article 13.2 (a), 14.2 (a) GDPR. See also A.29WP05/2012, Section 3.4.2, p. 13.

Personal data is retained for as long as necessary in order to comply with an applicable legal obligation of retention (e.g., as defined in applicable labour or tax law), for the period of time defined by that obligation; Opportunity – Personal data is retained for as long as permitted by the applicable law (e.g., processing based on consent, processing for the purpose of establishing, exercising or defending against legal claims – based on applicable statutes of limitations regarding legal claims related to the performance of the services). [C & P]

2.11.3 DATA RETENTION FOR COMPLIANCE WITH SECTOR-SPECIFIC LEGAL REQUIREMENTS

The CSP must indicate to the cloud customers:

1. Whether and how the cloud customer can request the CSP to comply with specific sector laws and regulations.[130] [C & P]

2.11.4 DATA RESTITUTION AND/OR DELETION

The CSP must indicate to the cloud customers:

1. The procedure for returning to the cloud customers the personal data in a format allowing data portability (see also Control no. 9., above); [C & P]
2. The methods available or used to delete data, whether at the request of the cloud customer or upon a valid request for erasure from a data subject; [C & P]
3. Whether data may be retained after the cloud customer has deleted (or requested deletion of) the data, or after the termination of the contract; [C & P]
4. The specific reason for retaining the data; [C & P]
5. The period during which the CSP will retain the data. [C & P]

Relevance: In requiring CSPs to provide all information above, this control seeks to provide transparency to cloud customers as to the retention periods for which CSPs – whether controllers or processors – may hold onto their data. Furthermore, in specifying the methods available or used to delete data, CSPs must also clarify how

[130] See ICO Guidance, pp. 16-17.

they will provide evidence of this, such as by providing a certified statement that no further copies of the customers' data have been retained in the CSPs systems, or those of its processors / subcontractors.

In particular, CSPs must inform cloud customers as to the means by which they will allow personal data stored on their systems to be deleted, either where this is done at the initiative of the customer (for example, as a result of the termination of services) or a data subject (validly exercising his/her right to erasure, under Art. 17 GDPR). In this manner, cloud customers will be made aware of how a CSP will allow them to comply with their obligation, as a controller, to address valid data subject requests for erasure, by also ensuring the deletion of personal data related to those data subjects which may be further stored on the CSP's systems.

2.12 COOPERATION WITH THE CLOUD CUSTOMER(S)

The CSP must specify:

1. How the CSP will cooperate with the cloud customers in order to ensure compliance with applicable data protection provisions, e.g., to enable the customer to effectively guarantee the exercise of data subjects' rights (rights of access, rectification, erasure ("right to be forgotten"), restriction of processing, portability and rights concerning automated decision-making), to carry out data protection impact assessments and requests for prior consultation with Supervisory Authorities, and to manage incidents including forensic analysis in case of security/data breach.[131] See also Controls no. 6. and 8., above. [C & P]

The CSP undertakes towards cloud customers:

2. To make available to the cloud customer and the competent Supervisory Authorities the information necessary to demonstrate compliance (see also Control no. 1., above).[132] [C & P]

Relevance: The obligation for a CSP to cooperate with its cloud customers is not directly spelled out in the GDPR (other than the references in Art. 28 GDPR), but it is nonetheless fundamental for cloud customers to properly comply with their obligations regarding personal data breaches, responding to data subject rights and, in general, ensuring that they can

[131] A.29WP05/2012, Section 3.4.2 p. 13. Note that the CSP is obliged to support the customer in facilitating exercise of data subjects' rights and to ensure that the same holds true for any subcontractor. A.29WP05/2012, Section 3.4.3.5, p. 16.
[132] Articles 5.2. and 28.3 (h) GDPR.

demonstrate that the CSPs they engage to process personal data maintain compliant practices. CSPs also commit to make available not only to customers, but also to inquiring Supervisory Authorities, the information which may be required in order to demonstrate their compliance with applicable legal obligations and with the terms of the CoC. It should be noted also that cooperating with cloud customers in this manner may be the only way for those customers to have access to all information needed to complete a DPIA concerning their use of the CSP's services.

CSPs must pay particular attention to the need to provide clear and specific information to cloud customers as to how they will assist those customers in addressing data subject requests which relate to personal data stored on the CSPs' systems (or otherwise processed by those CSPs), including the right to data portability (Control no. 9), the right to restriction of processing (Control no. 10), the right to erasure (Control no. 11.4.2) and the rights afforded to data subjects concerning automated decision-making, in the form of safeguards implemented by the CSP concerning those automated decisions (Control no. 3.1.10). This should include information on the specific processes in place to ensure that data subjects' rights can be addressed, as well as whether any costs for cloud customers may be involved in the provision of this assistance.

2.13 LEGALLY REQUIRED DISCLOSURE

The CSP must describe to cloud customers:

1. The process in place to manage and respond to requests for disclosure of personal data by Law Enforcement Authorities, including to verify the legal grounds upon which any such requests are based prior to responding to them, with special attention to the notification procedure to interested customers, unless otherwise prohibited, such as a prohibition under criminal law to preserve confidentiality of a law enforcement investigation.[133] [C & P]

Relevance: The CoC's emphasis on transparency towards cloud customers implies that they must have clear visibility on the circumstances under which a CSP will disclose personal data processed to authorities upon request, thereby allowing a customer not only to assess this procedure a priori, but also affording possibilities for the customer to intervene (e.g., in order

[133] A.29WP05/2012, Section 3.4.2 pp. 13-14. See extensively Article 29 Data Protection Working Party Opinion 04/2014 on "Surveillance of electronic communications for intelligence and national security purposes" http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_en.pdf) and ICO Guidance, pp. 19-20. See also Preamble 115 GDPR.

to limit the disclosure or contest the request), to the extent that the applicable law allows this. This procedure must include an explanation of how the CSP will assess the lawfulness of these requests itself, and under what circumstances customers may not be notified of such requests and disclosures (which must strictly be based on applicable laws preventing this).

2.14 REMEDIES FOR CLOUD CUSTOMER(S)

The CSP must indicate to cloud customers:

1. What remedies the CSP makes available to the cloud customer in the event the CSP – and/or the CSP's subcontractors (see Control no. 3., above and, more specifically, Control no. 3.3., above) – breach the obligations under the PLA. Remedies could include service credits for the cloud customer and/or contractual penalties for the CSP.[134] [C & P]

Relevance: To further stress CSPs' commitment to maintaining their compliance with the applicable law and with the terms of this CoC, CSPs are required to offer remedies to cloud customers in the event of their non-compliance (or of their processors / subcontractors) which are business-friendly (such as the example given of service credits and contractual penalties), in order to allow compensation for cloud customers without the need to resort to litigation. It must be understood that, in the event of non-compliance for which the CSP holds liability, the cloud customer will retain all rights under the contract with the CSP and additionally gain the agreed-upon compensation. Any such compensation will not prejudice customers' rights to bring legal action against the CSP if so desired.

2.15 CSP INSURANCE POLICY

The CSP must describe to cloud customers:

1. The scope of the CSP's relevant insurance policy/ies (e.g., data protection compliance-insurance,[135] including coverage for sub-processors that fail to fulfil their data protection obligations[136] and cyber-insurance, including insurance regarding security/data breaches). [C & P]

[134] A.29WP05/2012, Section 3.4.2 p. 12.
[135] See Articles 58, 77 ff. GDPR.
[136] See Article 28.4. GDPR.

Relevance: This control seeks to reassure customers that CSPs will be adequately covered in terms of damages they may suffer as a result of breaches on the part of the CSP or processors / subcontractors, or of personal data breaches suffered (though not covering consequent administrative fines or sanctions, which are generally uninsurable in Europe). CSPs must disclose the perimeter of their insurance coverage to cloud customers, in order to grant them visibility of how this insurance can serve as a guarantee of business continuity in these cases (avoiding failures to perform due to, e.g., bankruptcy or sudden changes of control).

3 PLA CODE OF CONDUCT (COC) GOVERNANCE AND ADHERENCE MECHANISMS

The cloud security certification landscape is not static and is likely to change rapidly. Cloud service providers and customers must promptly address all new laws and regulations compliance requirements with respect to personal data protection. Related parties and existing certification schemes must adapt to ensure the security and privacy measures in place evolve, and that any new regulatory requirements are continuously met.

This CoC falls under the aforementioned evolving landscape. In this context, a governance structure is required, in order to ensure consistency, control and proper implementation of required changes, and define as well accurately the "if", "when", "how" and by "whom" such changes should be applied to the PLA CoC and related documents.

Pertaining to the governance structure of the PLA CoC, the following important elements shall be considered:

1. technical components: components that over time will be affected by changes in the legal, regulatory and technological environment or by changes within CSA;
2. governance bodies: the key governing bodies, along with their roles and responsibilities
3. processes: the governance process and relevant activities as related to the definition, revision and implementation per PLA's component.

3.1 TECHNICAL COMPONENTS

Components of the PLA CoC governance structure include:

1. PLA Code of Practice
2. CoC mechanisms of adherence;
3. Code of Ethics;
4. Privacy Level Agreement (PLA) and Open Certification Framework (OCF) Working Groups' charter documentation.

3.1.1 PLA CODE OF PRACTICE

The PLA Code of Practice presented Part 2 of this document is the legal-technical standard that identifies the relevant personal data protection compliance requirements in the European Union, and defines clauses and controls to manage compliance with those requirements. The PLA Code of Practice constitutes the fundamental legal-technical component of this CoC.

3.1.2 COC ADHERENCE MECHANISMS

CSPs and cloud customers who are willing to adhere to the requirements of the PLA CoP shall submit a Statement of Adherence (See Annex 2) to the Cloud Security Alliance in accordance to the principles, policies and guidelines established in this document and in subsequent updates of the CoC adherence scheme developed by the CSA OCF Working Group and issued by the Cloud Security Alliance.

The Statement of Adherence shall be signed by either the company/organisation legal representative or by the appointed Data Protection Officer (DPO) and must be supported by the PLA [3] Template (see Annex 1) either in the form of a self-assessment (self-attestation) or in the form of third-party assessment.

The CSA CoC for GDPR Compliance Adherence Template summarises in a table structure the requirements included in the PLA CoP.

It shall remain clear that a CSP and/or Cloud Customer must take into consideration all the PLA CoP requirements and it cannot declare adherence only to a chosen subset of them.

The CSA CoC for GDPR compliance is a component of the CSA certification framework, i.e., STAR Program/ Open Certification Framework (OCF; see Annex 3 below). The Code foresees two mechanisms of adherence, which correspond to two (2) levels of assurance:

1. CoC self-attestation;
2. CoC third-party assessment.

The process for achieving a CSA CoC Self-Attestation is defined in this Section 3, paragraph 1.2.1.

This document provides also the initial input that will be used by the CSA OCF Working Group in order to define the scheme for a third-party certification (which may, ultimately, be intended to be approved as an established certification mechanism under Article 42 of the GDPR, once relevant criteria / guidelines have been formally approved by competent Supervisory Authorities). Such a certification scheme will comply with the ISO/IEC 17065-2012 standards.[137]

The CoC adherence scheme defines the objective, policy, mechanisms, scope, rules, requirements and processes for adhering to this CoC, and includes the following:

a) Scope and objective of adherence;
b) Auditing rules and mechanism;
c) The auditor qualification process;
d) The condition for revocation and complaint mechanism;
e) Adherence fees.

1. CoC Self-Attestation

The CoC self-attestation is the voluntarily publication by a CSP or cloud customer on the CSA STAR Registry (see Annex 3) of two (2) key documents:

- The CoC Statement of Adherence (Annex 2) and
- PLA Template (Annex 1).

The PLA Template and the CoC Statement of Adherence are submitted to CSA to verify that:

- The Code has been completed in all its sections,
- The details provided are sufficient to support an informed evaluation from a current or potential customer (i.e. the submitter of self-attestation), and

[137] ISO/IEC 17065:2012 Conformity assessment -- Requirements for bodies certifying products, processes and services.

- To make sure that a "good faith" effort to completely address PLA CoP requirements was made.

CSA will also verify the submitter has provided a public notice of compliance to the Code on its website. Once verified that all the necessary conditions are satisfied, CSA will publish the results of the self-attestation on the CSA STAR registry and provide the adherent to the Code a self-attestation compliance seal.

The CoC self-attestation compliance seal will have a validity of 12 months from the day of its issuance and it should be renewed after this period. A renewal implies a new and updated submission of both the CoC Statement of Adherence (Annex 2) and PLA Template (Annex 1). Moreover, the CoC self-attestation must be revised, and a new submission made, every time there's a change in the CSP's relevant policies or practices.

The publication of the self-attestation results on the CSA STAR registry, which, as described in Annex 4, is a public website, freely accessible by anyone, is meant to ensure that CoC Self-Attestations receive the necessary level of public scrutiny and to generate a high level of transparency concerning the privacy posture of CSPs in the delivery of their services. The public scrutiny over the published self-assessment is intended to be a mechanism for monitoring the implementation Code results.

The conditions for revoking a seal and the mechanism of complaints are described in sections 3.3. "CoC seals issuing and Statement of Adherence publication" and 3.4, "Complaints Management Process".

It shall be noted that the publication on CSA STAR Registry and issuing of the adherence seal will be subject to an administrative fee.

2. CoC Third Party Assessment

A CoC third-party assessment is obtained via the validation of a CSP's adherence to the PLA CoP requirements by a qualified CoC auditing partner (described in more detail below). The validation process aims to verify the following:

- The correct use of the CoC (e.g., did the data controller/data processor complete all sections in the PLA CoP? Does the content included in every section provide the necessary information on data handling and processing?);
- The accuracy of information included in the Code (e.g., is the information included in the submission truthful? Are statements supported by evidence?).

The third-party audit will be based on a combination of a paper-based analysis and in-person assessment.

As mentioned above, the validation must be performed by a qualified CoC auditing partner, which is an organisation that has signed the "Qualified CoC Auditing Partnership Agreement" with CSA. Among the notable requirements in the partnership agreement are the following:

- Partner employs at least one qualified CoC auditor
- Partner either employs or engages with at least one qualified CoC security expert for the relevant portions of the audit engagement. (This person could also be the qualified CoC auditor)

Please note that CSA corporate members who are also qualified CoC auditing partners will receive a complimentary listing on the CSA website.

Qualified CoC Auditors are professionals who comply with the following requirement:

1. Minimum 2 years' experience on data protection legal compliance or the possession of a relevant professional certification (e.g., IAPP CIPP/E, ECPC-B DPO Certification, CSA CoC training and certification).

Qualified CoC Security Experts are professionals who comply with the following requirements (please note that the requirement varies depending upon the audited company's information security certification status):

1. Audited company has a relevant information security certification (e.g., CSA STAR Certification/Attestation, ISO 27001):

   Minimum 1 year experience in cloud security compliance or the possession of a relevant professional certification (e.g., CSA CCSK, ISC(2) CCSP).

2. Audited company does NOT have a relevant information security certification (e.g., CSA STAR Certification/Attestation, ISO 27001):

   Minimum 3 years' experience on technical, physical and organisational compliance with respect to relevant information security certifications (e.g., CSA STAR Certification/Attestation, ISO27001) or the possession of a relevant certification (e.g., ISACA CISA, CSA STAR Certification Auditor, ISO 27001 Lead Auditor).

Following the successful completion of the audit, if it is verified that all the necessary conditions are satisfied, the Qualified Auditing Partner will issue an assessment for the CSP in question. At the same time, the Qualified Auditing Partner will inform the CSA of the successful completion

of the auditing process and provide CSA with the CoC Statement of Adherence (Annex 2) and PLA Template (Annex 1), on behalf of the adherent.

CSA will then proceed with the publication of the CoC Statement of Adherence (Annex 2) and PLA Template (Annex 1) on the CSA STAR Registry, and will issue a CoC third-party assessment seal to the adherent.

The CoC third-party assessment seal will have a validity of 12 months from the day of its issuance and it should be renewed after this period. A renewal implies that the adherent has to undergo a new audit and that an updated CoC Statement of Adherence (Annex 2) and PLA Template (Annex 1) are provided to CSA. Moreover, the CoC third-party assessment seal must be revised every time there is a change in the CSP's relevant policies or practices.

The conditions for revoking the seal and the mechanism of complaints are described in Sections 3.3. "CoC seals issuing and Statement of Adherence publication" and 3.4, "Complaints Management Process".

It shall be noted that the publication on CSA STAR Registry and issuing of the adherence seal will be subject to an administrative fee.

The final version of the CoC third-party audit-based adherence scheme will be produced by the CSA OCF WG in adherence with the requirements defined in Article 42 GDPR. Nonetheless, it should be stressed that the approach sought within this CoC is **not** to seek approval of any adherence schemes as a certification mechanism under Article 42 GDPR at present; rather, the third-party assessment mechanism has been designed to materially align with certification mechanism requirements, in order to ensure that the highest standards for this sort of assessment are met.

3.1.3 1.3 CODE OF ETHICS

See Annex 4, below, for a description of the Code of Ethics.

3.1.4 1.4 PLA AND OCF WORKING GROUP CHARTERS

See Annex 5 and Annex 6, below, respectively for descriptions of PLA and OCF Working Group charters.

3.2 GOVERNANCE BODIES, ROLES AND RESPONSIBILITIES

The governance of the CoC and its components (PLA Code of Practice, mechanisms of adherence and code of ethics) is a shared responsibility between the PLA and the OCF Working Groups, and CSA.

3.2.1 PLA WORKING GROUP

The PLA Working Group (WG) is responsible for defining, approving and updating changes to the technical standard/code of practice i.e., the PLA Code of Practice (currently in its third version, i.e., PLA [V3]). This body also provides expert opinion to CSA when complaints about CoC Self-Attestation or Third-Party Assessment are submitted. The PLA WG Charter defines the objectives and scope, membership, structure and responsibilities; the relations with other relevant CSA WGs; and relevant external activities, operations, communications methods, decision-making processes, activities, deliverables, duration and Intellectual Property Right (IPR) policy of the WG. Each member has the right to propose changes to the CoC.

Participation in the PLA WG is voluntary and open to anyone that wishes to contribute.

3.2.2 OCF WORKING GROUP

This body is responsible for the definition of the certification scheme(s) adopted within the CSA STAR Program. The OCF WG defines, reviews and approves changes in certification schemes already existing within the CSA OCF/STAR Program; and defines, reviews and approves any new certification scheme. It is further responsible for defining, reviewing and approving changes in the CoC adherence scheme.

The OCF WG Charter (see Annex 6, below) defines the objectives, scope, membership, structure and responsibilities; relations with other relevant CSA WGs; and relevant external activities, operations, communications methods, decision-making processes, activities, deliverables, duration and IPR policy of the WG. Each member has the right to propose changes to the certification schemes included under the CSA STAR Program, as well as to the CoC adherence scheme.

3.2.3 CLOUD SECURITY ALLIANCE (CSA)

CSA supports and oversees implementation of the CoC adherence scheme as a component of the STAR Program. These activities include, but are not limited to the following:

- Maintaining a public registry of issued CoC adherence seals. Each entry includes as minimum the following information: (i) name and description of organisation, (ii) name and description of service for which the CoC is relevant, (iii) CoC entry, (iv) version of the CoC used (currently V3), (v) validity of seals, (vi) name of auditing organisation/auditor (if applicable);
- Maintaining a public registry of qualified CoC auditors;
- Maintaining a web site where information and guidelines about the CoC concept, approach and technical standards are provided, together with the requirements, process and cost of the adherence scheme;
- Developing and maintaining the CoC:
    - Defining guidelines on how to submit and how to review the CoC Self Attestation;
    - Reviewing CoC self-attestations and verifying minimum requirements are met;
    - Maintaining a mechanism for filing complaints;
    - Providing guidance on handling conflicts;
    - Creating an advisory body to support CSA in the implementation and oversight of the scheme;
    - **Through the Monitoring Committee**, verifying complaints, proactively monitoring compliance with the CoC and taking appropriate actions (e.g., revoke Self Attestation seals, removing a CoC entry and seal from the Registry; removing a qualified CoC auditing partner from the Registry, etc.).
    - Assuring transparency and integrity throughout the development of standards, implementation of seals and management;
    - Approving the OCF charter revision and extension;
    - Approving the PLA charter revision and extensions;
    - Setting and reviewing the adherence fee;
    - Approving CoC qualified auditor training partners;
    - Providing a public accounting of all fees and other revenues collected and their disposition in the management of this program.

3.2.4 COLLABORATION AND SUPPORTING ACTIONS TOWARD DATA PROTECTION SUPERVISORY AUTHORITIES

The CoC governance bodies agree to collaborate and support national data protection authorities (DPAs) in matters related to personal data protection in the cloud according to the terms below.

With respect to collaboration, and upon request by a national DPA or the European Data Protection Board, the CoC governance bodies may provide the following:

- Guidelines and awareness initiatives addressed to companies and individual users of cloud computing services;
- Advice on opinions to be issued regarding relevant data protection laws (e.g., opinions due by law from a national DPA toward the relevant national parliament and/or public authorities).

With respect to supporting actions, and upon request by a national DPA or the European Data Protection Board, the CoC governance bodies also may do the following:

- Promote awareness between the CoC self-attested and third-party-assessed companies about measures issued by national DPAs (general provisions, as well as specific provisions - when issued towards a CoC self-attested or third-party-assessed company);
- If a national DPA carries out an inspection of a CoC-adherent company, provide DPA with all information and evidence available in CSA about the CoC-adherent company. In these cases, CoC governance bodies will act as the CSA point of reference.
- Review and, if necessary, withdraw the CoC adherence seal of a company subject to penalties issued by a national DPA.
- Inform the European Data Protection Board and/or relevant National DPAs in case a CoC Self-Attestation and/or Third-Party Assessment seal is revoked.

3.2.5 COC MONITORING BODY

In order to ensure and verify the ongoing compliance of adhering CSPs with the requirements of the CoC, CSA has established an internal committee (the "**Monitoring Body**") which is tasked with the active and effective monitoring of adhering CSPs' data protection practices.

This section describes how the Monitoring Body (MB) meets the requirements for its accreditation by the lead Supervisory Authority, under the terms of Art. 41 GDPR and the EDPB Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679, of 12 February 2019[138].

[138] Version for public consultation available at: https://edpb.europa.eu/sites/edpb/files/consultation/edpb-20190219_guidelines_coc_public_consultation_version_en.pdf.

1. Independence

The MB is an internal body established by CSA, which is functionally separated from other CSA functions or departments. The MB is appropriately independent from any CSP (whether code members or not), other functions or departments within CSA and the cloud computing sector. Independence is achieved by the following means:

- The MB has its own staff and is autonomous in its own management;
- MB staff may not assume other accountabilities or functions within CSA which may create a conflict of interests with the tasks they perform within the MB;
- The MB has its own separate[139] and adequate budget;
- The appointment, remuneration and removal/dismissal of the Monitoring Body Management Representative (MBMR) is subject to approval of the Board;
- Members of the MB cannot be dismissed or penalised in any way as a result of the performance of their tasks;
- The MBMR directly (functionally) reports to and interacts with the Board;
- The activities of the MB are free from interference, whether internal or external to CSA. The MB is free to perform its tasks without taking instructions from CSA or suffering any sort of sanctions or interference from CSA in the performance of its tasks (e.g., the MB is free to decide on the management of complaints, the performance of audits and their scopes, its working procedure and the communication of its results, as well as on the imposition of sanctions against code members).

In order to achieve organizational independence, the MBMR functionally reports to the Board (as mentioned above). The Board is involved in:

- Approving this Policy and Procedure and any amendments to it;
- Approving the annual risk-based (monitoring) plan of the MB;
- Approving the budget and resource plan of the MB;
- Receiving communications of the MBMR as to the achievement of the goals and activities as mentioned in its (monitoring) plan;
- Approving decisions of the MB with regard to the appointment, remuneration, replacement and/or dismissal of the MBMR.

The MB also acts independently from code members in performing its tasks and exercising its powers.

[139] CSA has different sources of revenue which make up its funding. In order to ensure the continued Independence and impartiality of the MB, CSA undertakes to allocate an appropriate budget to the MB (approved by the Board on the basis of annual budget and resource plans) which is kept appropriately independent from the source of revenue represented by the CoC submission and renewal fees paid by code members.

The MB is responsible for continuously assessing its status as an independent monitoring body, in order to identify any potential risk to its independence in the performance of its tasks. If a risk to its independence is identified and cannot be removed or dismissed by the MB itself, the MBMR will report this risk to the Board and suggest how such risk could be removed or minimised. The MBMR shall – at least annually – confirm the organizational independence of the MB to the Board.

Where required by the Lead Supervisory Authority (CompSA) or otherwise, the MB will produce the results of its continuous assessment and will demonstrate how any such risks it may have identified are removed or minimised, so as to safeguard the MB's independence.

2. Absence of a conflict of interests

The MB has implemented review systems to ensure its activities do not result in a conflict of

interest, and that the MB will remain free from external influence, whether direct or indirect.

These systems serve also to document and demonstrate the MB's posture towards preventing any actions which are incompatible with its tasks and duties (e.g., favouring code members by showing undue leniency in the imposition of sanctions for breach of the CoC's terms) and to mitigate the risk of a conflict of interest arising within the MB or related to any of the MB members.

If a risk to the impartiality of the MB is identified, the MBMR reports this risk to the Board and mentions how the MB removed or minimised such risk. The MBMR shall – at least annually – confirm the impartiality of the MB to the Board of CSA.

The MB and its members must warrant that they do not have any stake or standing related to CSP's which could compromise their judgement or create a conflict of interest with their monitoring role. Furthermore, the MB and its members must refrain from any action that is incompatible with their tasks and duties. They shall neither seek nor take instructions from any person, organisation or association (including CSA or any CSP) in the performance of their tasks and duties.

The members of the MB may perform the tasks assigned to the MB in relation to CSPs to which they have previously provided consulting or other services, insofar as the nature of those services does not impair their objectivity in the performance of the tasks assigned to the MB.The individual objectivity of MB members is managed by the MBMR when assigning members to perform specific tasks.

The members of the MB must refrain from assessing or reviewing specific operations for which they were previously responsible. Objectivity is presumed to be impaired if the member had such responsibility within the previous year.

Where required by the CompSA or the Board, the MB will produce the results of its continuous assessment and demonstrate how any such risks it may have identified are removed or minimised, so as to safeguard the MB's impartiality.

Each member of the MB and each third party working for the MB signs this policy statement. Any violation of this policy is subject to appropriate disciplinary action or may lead to contractual liability.

3. Expertise

CSA is responsible for monitoring and retaining records related to training and competency of the Members of the MB and all third parties and persons that carry out (sub-)activities on behalf of the MB. This in order to demonstrate that the MB has the requisite level of expertise to carry out its role in an effective manner. The MBMR performs these assurance activities and reports its findings to the Board.

The MBMR shall – at least annually – confirm the required expertise of the MB to the Board of CSA.

Members of the MB and any third parties contracted by the MB to perform tasks on its behalf must have sufficient knowledge and skills to be able to duly perform their individually assigned tasks.

The MB, collectively, is required to meet the following minimum criteria, while performing its tasks:

- In-depth understanding of data protection issues;
- Expert knowledge of the cloud computing industry and other related activities which are the subject matter of the CoC;
- Appropriate operational experience and training in the carrying out of compliance monitoring activities (e.g. auditing), preferably in the domain of privacy and data governance;
- Successful completion of the CSA GDPR Certification – Lead Auditor Training course;
- Care and skills needed in order to perform their tasks in a reasonably prudent and competent manner.

The MB members assigned to tackle the management of a specific complaint or monitoring process, or parts thereof, must, collectively, meet the requirements listed above. If this is not possible, due to insufficient availability of MB members, the MBMR is responsible for obtaining competent and sufficient external advice and/or support so that those requirements may be met. In the absence thereof, the MB must postpone these activities until it is possible to comply with these requirements.

The MB and its members must exercise due professional care in the tasks and duties performed, by considering:

- the extent of work needed for the activity to be performed;
- the relative complexity, materiality or significance of the subject matter;
- adequacy and effectiveness of governance, risk management and control processes;
- probability of significant errors, fraud or noncompliance;
- assurance costs in relation to potential benefits.

Members of the MB must seek to continuously enhance their knowledge, skills and other competencies on a frequent basis (through training courses, conferences and certifications, for example), so as to ensure that the expertise requirements above are maintained. The budget of the MB should be adequate to meet this requirement.

The initial members making up the MB have been chosen by CSA on the basis of their expertise and the lack of a stake or standing related to CSPs which might be considered incompatible with the role. Following this, the MB has full autonomy to decide on its own composition, provided that no members are brought on which do not have the required expertise on data protection/information security matters or which may be in a position of conflict of interests. Decisions with regard to the appointment, remuneration, replacement and/or dismissal of the MBMR, however, are taken by the MB and need approval of the Board. Those decisions of the Board shall be documented and substantiated.

4. Resources and staffing

The MB must be provided with sufficient resources and staffing, so that it can perform its tasks in an appropriate manner. These resources must be proportionate to the expected number and size of the code members which the MB is to supervise, as well as the complexity and degree of risk of the data processing activities which those code members may carry out. The Board is responsible for ensuring this and keeping documentation to demonstrate that the above is complied with.

In order to be able to make that assessment, the MBMR provides the Board with all necessary information, including an annual risk-based (monitoring) plan.

5. Established procedures and structures

Appropriate governance structures and procedures are in place which adequately assess the eligibility of CSPs to sign up to and comply with the CoC. This specific assessment is not carried out by the MB, but instead by the CSPs themselves (through self-assessment) or by APs (through third-party assessment). CSA will formally assess CoC adherence submissions to ensure that adequate responses to all CoC controls are given (while not materially auditing the answers given to each control), and may rely on external consultants to assist in this assessment.

There are also appropriate governance structures and procedures to ensure that the provisions of the CoC are capable of being met by the code members and compliance with its provisions is monitored. These procedures are outlined in the complaints handling (2.5.5.) and monitoring sections (2.5.11).

6. Transparent complaints handling

If a code member infringes the terms of the CoC, in particular by maintaining practices which are incompatible with the statements made by the code member in the submissions made to apply for a CoC adherence seal (whether under the framework of self-assessment or third-party assessment), the MB will take immediate corrective measures, as deemed appropriate by the MB, to address the situation. If any relevant issues arise regarding an AP, the MB will investigate the matter and report its findings to the Board, which will take the corrective measures deemed appropriate to each case.

In particular, the MB may act against an adhering CSP or an AP as a result of an infringement detected through a complaint submitted by for example a cloud customer, a data subject or another CSP.

If such a complaint is received, the MB will investigate this complaint. If the investigation of the complaint leads to the conclusion that the code member violated one or more provisions of the CoC, the MB will take such immediate corrective measures, as deemed appropriate by the MB to address the situation. The measures to be taken should aim at stopping the infringement and preventing recurrence of the same or similar infringements in the future. Such remedial actions and sanctions may take various forms and could include, but are not limited to:

- A formal notice requiring the implementation of specific actions within a specified deadline;
- Temporary suspension of the member from the STAR Registry, until remedial action is taken;
- Definitive exclusion of such member from the CoC and revocation of the seal.

These measures may be made public by the monitoring body, especially where there are serious infringements of the CoC.

Where required, the MB shall inform CSA, the code member, the CompSA and all other concerned supervisory authorities about the measures taken and their reasoning, without undue delay.

The MB will generate periodic reports under the supervision of the MBMR to document the results of the investigation of complaints, and at least one annual report encompassing all complaint-related activities carried out during that year. This annual report will be shared with the Board, the CompSA and other concerned supervisory authorities, where relevant.

7. Communication with the competent Supervisory Authority

The monitoring body framework allows for the effective communication of any actions carried out by the MB to the CompSA and other supervisory authorities in respect of the code.

The MB reports at least once a year to the CompSA. Its report includes at least the following topics:

- Audits carried out;
- Specific important review or audit findings;
- Complaint management activities carried out;
- Decisions concerning the actions taken in cases of infringement of the CoC by a code member;
- Any relevant changes in code members;
- The future agenda of the MB and any other relevant information about its functioning;
- Technological, legal or other developments which may be relevant for the interpretation and/or functioning of the CoC.

Furthermore, the MB will promptly and directly communicate to the CompSA any specific cases where it decides to suspend or revoke adherence seals granted to CSPs, as a result of a failure to properly comply with the requirements of the CoC.

In addition, the MB shall promptly cooperate with the CompSA and provide any and all information necessary in relation to the CoC and its activities, in order to ensure that the CompSA is not prejudiced or impeded in its role.

8. Review mechanisms

Appropriate review mechanisms shall be in place to ensure that the CoC remains relevant and continues to contribute to the proper application of the GDPR. The PLA Working Group establishes and performs review mechanisms to adapt to any changes in the application and interpretation of the law or the occurrence of new technological developments which may have an impact upon the data processing carried out by code members.

In addition, a process of periodic[140] review is applied to all CSA services and processes to identify possible improvement opportunities.

All changes will be handled via change management through the CSA management committee.

Changes to this Policy and Procedure may be triggered by an initiative presented by the MBMR to the Board.

9. Legal status

As an internal body, the MB does not have autonomous legal standing to be held liable for the performance of its tasks and duties, under Art. 83(4)(c) GDPR. As such, CSA will assume full liability for any breaches of the MB's obligations under Art. 41(4) GDPR.

10. Continuous improvement

The MBMR develops and maintains a quality assurance and improvement program with respect to all tasks of the MB. The effectiveness of the MB and the monitoring process is continually improved through regular reviews carried out by the MB, covering the complaints handling, monitoring and other procedures, as well as the very governance structure of the MB. These reviews – carried out under the supervision of the MBMR – will consider the results of audits carried out on CSPs and APs, feedback received from Supervisory Authorities, cloud customers, CSPs and data subjects, complaints and all other associated information.

[140] At least once a year, but could be more frequent depending on the legal and industry landscape.

Suggestions for improvement may be submitted to the MB by any of the CoC stakeholders, including code members and staff. Actions for improvement will be assessed and documented as an output of these regular reviews.

Such reviews must be held at least once annually; ad hoc reviews can be triggered whenever the MB deems necessary. The MBMR reports the outcome of those reviews to the Board.

11. Monitoring

There are two parts to the monitoring process. One is complaints management (see section 5.6 above, and Appendix A below), and the other is the duty upon the MB to actively monitor. The MB has a process in place that allows for random checking of CSPs, to annually audit their compliance and effectiveness of the process as attested to by the CSP upon their adherence to the CoC. Upon the detection of irregularities, the sanctioning process will be followed.

There is also a process in place to sample of reports and third-party assessments provided by APs, along with their adherence to the requirements for APs laid down in the CoC. Upon the detection of irregularities, the Board will be notified to take any action deemed appropriate.

A review of key processes is conducted through audit or if indicated by special circumstances. This review is used to identify and eliminate potential nonconformities.

The MB monitors code members through procedures that will ensure compliance with the CoC, and monitors APs through procedures that will ensure compliance with the relevant requirements of the CoC which address them. The MB has powers to take immediate corrective measures if a code member acts outside the terms of the CoC, which may even lead to suspension or exclusion from the CoC (see section 5.6 above). Additionally, the MB has the authority to report any findings to the Board, which may take action to suspend or exclude an AP from performing third-party assessments, if through the MB's review it is found that and AP does not comply with the requirements to qualify as an AP under the CoC, or with associated accreditation standards (i.e. ISO/IEC 17065).

All reports are reviewed periodically between the MB and the Board in formal meetings and the need for action to prevent future nonconformities or make changes is evaluated.

3.3 GOVERNANCE PROCESSES AND RELATED ACTIVITIES

The governance process of the CoC defines the relationship between the governance bodies and a set of activities with which they are required to comply, in order to maintain a consistent management process for every CoC component.

3.3.1 CHANGE PROCESS OF EU-SEC PRIVACY CONTROL REPOSITORY

As a main result from Working Package of EU-SEC project, the Privacy control repository is the knowledge database of state-of-art privacy relevant requirements in EU, which are collected from international and national standards, legislations, best practices, etc. Due to the rapid change of the cloud technology and dynamic of the cloud certification scheme, it is essential to keep the EU-SEC privacy control repository always in state-of-art to reflect the market requirements, and furthermore to provide valuable insights for all stakeholders.

The change process aims to detect, assess, and eventually implement changes to EU-SEC privacy control repository, to ensure the knowledge database includes all the relevant information for EU region from the outside world.

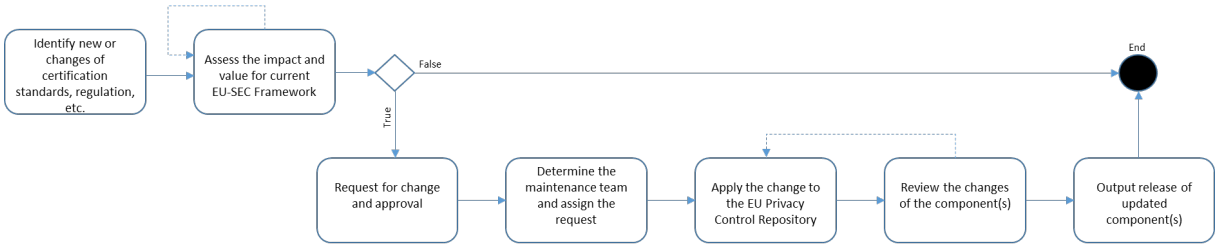


Figure 1: Change Process of EU-SEC Privacy Control Repository Activity Diagram

Change process includes following activities:

- Identify new or changes of privacy certification standards, regulation, etc.

As Input for the change process, news and changes on privacy certification standards, regulation, etc. shall be continuously monitored. When there is new or changes of privacy certification standards or regulations in the market, they shall be reported to the governance

office[141] and trigger the change management process. Both user and contributor of the PLA and the relevant stakeholders could identify and report the new and changes of privacy standards, or regulations. A change can also be identified from outcomes of reviews, meetings, updates, identified enhancements and/or inconsistencies of the contributors of the PLA or other stakeholders.

- Assess the impact and value for current EU privacy control repository

Identified news and changes on privacy certification standards, regulation shall be assessed on its impact and value for the current EU privacy control repository, to decide whether new information shall be included.

The impact assessment activity identifies as precisely as possible the parts/sections of the designated component(s) (e.g. PLA Code of Practice, Code of Ethics, PLA and OCF Working Group Charters that are affected by the change in the privacy control repository documentation) that are impacted by the new input, and the impact rate (e.g. major, significant, and minor).

After the assessment of changes and their estimated impact, a decision is made and a Request for Change will be created to implement the change.

- Request for Change (RfC) and approval

A Request for Change (RfC) will be created and documented along with assessment results, and justified with rational of the proposed change. The RfC shall be approved by approver (e.g. Change Advisory Board) before pass to the maintenance team.

- Determine the maintenance team and assign the request

The approver determines the maintenance team that is the most relevant to implement the changes based on the identified impacts of the validated change. Help from any relevant expert or advisor (e.g. Qualified PLA Auditing Partners) can be also requested.

Finally, the change request is assigned to the designated maintenance team.

- Apply the change to the EU privacy control repository

The maintenance team is responsible for the updates (addition, suppression, modification) of privacy control repository based on the change request and with respect to identified changes at the underlying privacy requirements. In addition, it will be ensured that the requested

[141] To be defined within T2.4. EU-SEC Framework.

updates are done in a timely fashion in order to limit the possible risk of organizations adhering to an incomplete set of requirements.

- Review the change

This activity reviews the updated privacy controls and related elements after the requested change has been implemented. During this review, the approver and the maintenance team are responsible for reviewing the applied changes based on the comparison between the previous version and the updated version of the given component(s) is performed.

- Output release of updated components

The output of the change process will involve an updated documentation of the privacy control repository. This released documentation could become the input for further PLA Code of Practice review process, and furthermore trigger the change on PLA.

3.3.2 PLA CODE OF PRACTICE REVIEW PROCESS

The PLA CoP will be subject to periodic reviews, since it is subject to changes in the European Union personal data protection-related legal framework. The PLA CoP review process falls under the responsibilities of the PLA WG. The CSA undertakes, through the PLA WG, to timely reflect any relevant legislative changes in the PLA CoP, and to promptly notify adhering CSPs to comply with these changes.

The PLA CoP review process can be triggered by any member of the CSA community (volunteers, corporate members, members of the PLA WG, etc.) based on the need to align PLA CoP requirements to the most current relevant legislations.

Any request to update the PLA CoP [V3] shall be assessed and decided upon by PLA WG members (refer to the PLA Charter in Annex 5, below).

CSA and PLA WG members will ensure PLA updates are done in a timely fashion in order to limit possible risk of an organisation adhering to an incomplete set of requirements. As such, the terms on reviews triggered by legislative changes or by CSA community member requests notwithstanding, the CSA commits to reviewing the PLA CoP, via the PLA WG, at least every twelve (12) months from the last review carried out.

CSPs adhering to the PLA CoP will be promptly notified of any changes and requested to make the necessary internal adjustments in order to comply with them in practice. CSPs will be given a timeframe within which to apply these adjustments, depending on the impact of changes

made to the PLA CoP – thirty (30) days for minor changes, sixty (60) days for relevant changes, and ninety (90) days for critical changes.

Any changes to the PLA CoP, once approved as a Code of Conduct under Art. 40 GDPR, will be notified to the competent Supervisory Authority, under Art. 40(5) GDPR.

The current version of PLA CoP [V3] focuses both on the actual (Directive 95/46/EC and its implementations in the EU Member States) and forthcoming European Union relevant legislation concerning the protection of personal data (Regulation (EU) 2016/679, GDPR).

The PLA WG charter also includes the extension of the current geographical scope of the PLA CoP. PLA WG also foresees the development of a CoC that addresses privacy/data protection requirements at the global level.

3.3.3 COC ADHERENCE SCHEME REVIEW PROCESS

The OCF WG is responsible for triggering the review of the CoC certification scheme, as well as assessing and approving review requests and implementing proposed changes.

OCF WG members have the right to propose changes to the certification schemes in the CSA STAR Program, including the CoC certification.

3.3.4 COC SEALS ISSUING AND STATEMENT OF ADHERENCE PUBLICATION

CSA is responsible for reviewing, approving and managing CoC Self Attestation and Third Party Certification Marks issuing, the Statement of Adherence submission processes and relevant complaints. More specifically:

1. **PLA CoC Self-Attestation**

CSA is responsible for reviewing any PLA Self Attestation and relevant complaints submitted by any third parties. In the former case, CSA shall verify that minimum requirements have been satisfied. In the latter case, CSA shall verify the validity of the complaint and based on the input of the PLA WG, shall take relevant actions.

Upon validation, CSA shall ensure that the CoC Self Attestation is published at the online CSA Registry.

If minimum requirements are not satisfied or if a complaint is deemed valid, CSA will take one of the following actions: a) request an amendment to the PLA Self Attestation, or b) Remove the Self Attestation from the CSA Registry and revoke the seal.

2. **CoC third-party assessment**

CSA is responsible for publishing the PLA Certification at the STAR Registry, upon notification from a qualified CoC Auditor that the auditee has passed the audit.

CSA is also responsible for notifying a qualified PLA Auditor that issued a CoC Certification if a related complaint was filed. In that case, the Qualified PLA Auditor shall verify the validity of the complaint and provide feedback to CSA.

If the complaint is deemed valid, the qualified CoC Auditor shall temporarily suspend certification or revoke it. Accordingly, CSA shall remove the certification from its Registry and revoke the seal.

3.3.5 COMPLAINT MANAGEMENT PROCESS

The complaint management process defines how the Monitoring Body will receive, manage and address complaints received which are related to the CSA Code of Conduct self-attestation and third-party assessment mechanisms.

This complaint procedure will be made available on the CSA website and, in particular, on the CSA STAR registry page.

The main purpose of the complaint management process is to allow any individual to report issues related to CSA Code of Conduct, such as (but not limited to):

- Notifying inconsistencies between the information reported in a CoC Self-Attestation and/or CoC Third-Party Assessment for a CSP and the conditions/terms applied by that CSP in the provision of the service;
- Notifying about misleading or inaccurate information reported in the CoC Self-Attestation and/or CoC Third-Party Assessment for a CSP;
- Notifying behaviour which represents a breach of the CSA Code of Ethics;
- Notifying cases of conflict of interest related to members of the CoC Governance Bodies;
- Notifying issues concerning a Qualified CoC Auditing Partner;

- Notifying issues concerning a Qualified CoC Auditor.

1. Ordinary complaint management process

All complaints related to the CoC will be relayed without undue delay to the Monitoring Body (where they are not directly addressed to the Monitoring Body). It must be ensured that the members of the Monitoring Committee tasked with the handling of a complaint (or an appeal) are different from members which have previously been tasked with auditing or taking relevant decisions (e.g., related to corrective actions or sanctions) regarding the CSP or the Qualified CoC Auditing Partner to which the complaint relates.

The submission of complaints or appeals, as well as their subsequent investigation and potential decisions made by the Monitoring Body will not result in any discriminatory actions against the complainant or appellant.

Any complaints filed will be acknowledged to the complainant within two (2) working days. Once a complaint is filed, the Monitoring Body will begin processing the complaint within five (5) working days. Depending on the nature of the compliant, relevant bodies (e.g., the PLA WG) will be engaged. Every effort will be taken to close the complaint within sixty (60) days from its filing, where feasible.

While processing the complaint, the Monitoring Body may request additional information from the complainant, in order to better assess the matter.

In the case a complaint received concerns inaccuracies, inconsistencies or any other issues related to the CoC Self-Attestation mechanism, the Monitoring Body may request additional information from the CSP in question (i.e., the CSP which is the subject of the complaint). If the information made available by the CSP to the Monitoring Body is not sufficient to reach a final decision on the complaint, or if the nature of the complaint concerns a "major" issue, the CSP may be requested to undergo a third-party audit, in order to be able to maintain their adherence seal.

In the event that the Monitoring Body accepts a complaint submitted regarding an adhering CSP, the Monitoring Body will take immediate suitable measures. The aim of these measures will be to stop the infringement and prevent its future recurrence. Measures taken may range from formal warnings requiring the implementation of corrective actions within a specified deadline, to temporary suspension or definitive revocation of the CSP's CoC adherence seal:

- For very minor issues, the Monitoring Body may issue a formal warning to the CSP and provide a timeframe during which the detected non-compliance must be cured;

- For minor issues, or where the Monitoring Body does not respond adequately and in a timely manner to a formal warning issued by the Monitoring Body, the Monitoring Body may temporarily suspend the CSP's CoC adherence seal until the Monitoring Body is satisfied that the issue has been fully resolved;
- For major issues, the Monitoring Body may revoke the CSP's CoC adherence seal.

In case of suspension or revocation, the lead Supervisory Authority and/or European Data Protection Board will be notified.

In case a complaint received concerns inaccuracies, inconsistencies or any other issues related to the CoC Third-Party Assessment mechanism, CSA may request additional information from the CSP in question (i.e., the CSP which is the subject of the complaint) and will immediately notify the Qualified CoC Auditing Partner that has issued the seal. Based on the complaint report produced by the Qualified CoC Auditing Partner, CSA will proceed with the suspension or revocation of the CoC Third-Party Assessment seal. In case of revocation, the relevant national DPA and/or European Data Protection Board will be notified.

The PLA WG will issue guidelines to define the categories of "very minor", "minor" and "major" issues.

The CSP and the complainant will be notified of the outcome of the investigation of a complaint, without undue delay.

The Monitoring Body may also decide to make public the actions or sanctions imposed upon an infringing CSP, particularly where the issue is deemed "major".

The Monitoring Body will relay the results of complaint investigation processes concerning a Qualified CoC Auditing Partner to CSA. CSA reserves the right to suspend, withdraw or terminate the certification of a Qualified CoC Auditing Partner as such, based on the outcome of those investigations – in particular, where these entities fail to properly implement any corrective actions which are imposed upon them by CSA.

The Monitoring Body will generate periodic reports to document the results of the investigation of complaints, and at least one annual report encompassing all complaint-related activities carried out during that year. This annual report will be shared with CSA, the lead Supervisory Authority and other concerned Supervisory Authorities, where relevant.

All processed complaints will be reviewed during the Monitoring Body's regular reviews (see Section 2.5.9 above).

2. Appeal process

Where a CSP or Qualified CoC Auditing Partner wishes to dispute the conclusions and/or the sanctions or corrective actions imposed upon it, as notified upon conclusion of the investigation of a complaint, the CSP must file an appeal with the Monitoring Body within forty-eight (48) hours of the notice. If an appeal is filed, no corrective actions will be enforced until the appeal process has been completed and a final decision has been handed down by the Monitoring Committee.

The Monitoring Body will consult with all parties involved, in order to determine the facts and obtain all supporting information within agreed timelines. Any communications made to the Appellant will be in writing and served to the address provided by the Appellant as their contact office, or otherwise any other address indicated by the Appellant.

An Appeal Panel will be appointed for each appeal case, by the Chair of the Monitoring Body. The Appeal Panel will consist of three (3) Monitoring Committee members, one of which will act as the Chairman. These members must not have participated in the specific complaint management process which is the object of the appeal, and must have no relevant connection to any of the parties involved (i.e., Appellant and complainant).

The Appeal Panel will schedule a meeting at the time of earliest convenience for the Appellant, the complainant and other involved parties. The Appellant will be given prior notice of at least seven (7) working days of the date, time and place of the meeting, and will be informed of the names of the Appeal Panel members. The Appellant may object, in writing and on reasonable grounds, to the appointment of one or more of the Appeal Panel members. Any such objections will be assessed by the Director of the Monitoring Body; if deemed valid, the objected-to Appeal Panel members will be replaced with other Monitoring Committee members meeting the same requirements of independence and impartiality as stated above. The Chair of the Monitoring Body must justify any decision made regarding such an objection in writing and notify the Appellant of this without undue delay.

The Appeal Panel Chairman will be tasked with ensuring that the Appeal Panel meeting takes place in an orderly and appropriate fashion. In particular, it must be ensured that:

- The Appeal Panel hears, in confidence, the evidence and opinion presented by the Appellant;
- The Appeal Panel hears, in confidence, the evidence and opinion presented by the Monitoring Body and/or the complainant;

- The Appeal Panel evaluates the representations made by all parties and, after due consideration (and further questioning, if required), makes a final decision. The decision will be taken by majority of the Appeal Panel and is final and conclusive.

The lead Supervisory Authority, as well as other Supervisory Authorities, may intervene in the Appeal Panel meeting or during an appeal process in general, by submitting written observations on the matter under dispute.

The Appeal Panel Chairman is tasked with recording the proceedings and the decision of the Appeal Panel, as well as notifying the Monitoring Body, CSA, the lead Supervisory Authority and other Supervisory Authorities (where relevant) of the decision, in writing, within five (5) working days from the date of the Appeal Panel meeting.

In the event that the Appeal Panel decides to reverse the decision made by the Monitoring Committee, the Appellant's redress shall be limited to a declaration, by the Monitoring Committee, of the revised decision, in the same manner as the original decision was declared. There will be no liability for any losses or damages suffered by the Appellant as a result of the original decision.

3.3.6 ONGOING MONITORING PROCESSES

Other than handling the Complaint Management Process (see Section 3.4 above), the Monitoring Body is also tasked with the duty to actively monitor compliance with the CoC. This is achieved through a process allowing for random checking of adhering CSPs during annual audits, in order to assess their compliance with the terms of their CoC submissions, on the basis of which their CoC adherence seal was issued. Any irregularities detected will trigger the sanctioning process described in Section 3.4 above.

The Monitoring Body is charged not only with auditing adhering CSPs, but also the Qualified CoC Auditing Partners which are responsible for facilitating Third Party Assessment submissions for CSPs.

The Monitoring Body will generate periodic reports to document the results of audit exercises carried out, and at least one annual report encompassing all monitoring activities carried out during that year. This annual report will be shared with CSA, the lead Supervisory Authority and other concerned Supervisory Authorities, where relevant.

1. **Monitoring process**

The MB will use generally recognized best practices for monitoring/auditing self-assessment and third-party assessment CoC adherence submissions to provide a high-level of confidence that:

A. The code member's processes, in relation to the relevant services for which it applied for CoC adherence, comply with the requirements of the CoC, as stated in the Self-Assessment Statement of Adherence / Third-Party Assessment Statement of Adherence and PLA Code of Practice (CoP) Template - Annex 1 submitted to the STAR Registry; and

B. The code member has kept their submission updated to stay current with any updates and revisions of the PLA Code of Practice (CoP) Template - Annex 1.

Monitoring will be carried out by means of a graduating sampling format. When triggering an annual audit exercise, the Monitoring Body will randomly select a sample of 5 CSPs submissions or 2% of all CSP submissions (whichever is greater):

Population	Sample Size	Corrected Sample Size
10	0,2	Minimum sample must be 5
20	0,4	Minimum sample must be 5
30	0,6	Minimum sample must be 5
50	1	Minimum sample must be 5
75	1.5	Minimum sample must be 5
100	2	Minimum sample must be 5
150	3	Minimum sample must be 5
200	4	Minimum sample must be 5
250	5	5
300	6	6
400	8	8
500	10	10
600	12	12
700	14	14
800	16	16
900	18	18
1,000	20	20
1,200	24	24
1,500	30	30
2,000	40	40
2,500	50	50
3,500	70	75

5,000	100	100

Each code member included within a sample will be assessed in terms of their compliance with the CoC's controls, in order to verify the effectiveness of the implementation of those controls in practice. As a minimum, 10% of the CoC's controls will be assessed randomly, based on the scope and complexity of the code members in question. If further questions arise regarding the compliance and effectiveness of the measures put in place by a code member to address some or all of the CoC's controls, the MB may increase the sample of assessed controls until there is sufficient evidence to determine the code member's overall compliance or non-compliance with the CoC.

Numbers will be rounded based on standard mathematical rules. Samples will be pulled annually on a random basis. Reviews may be pulled more frequently depending on past reviews and the outcome of those reviews. Any code members that had non-conformities[142] must submit written corrective action and be included in the next sampling plan to confirm implementation and effectiveness of the corrective action.

2. **Specific objectives of the monitoring exercises**

When carrying out an annual audit exercise, the MB seeks to meet the following goals:

- Obtain evidence from the code members that they have correctly interpreted and implemented the requirements of the CoC;
- Confirm that the manner in which the code members have implemented the requirements of the CoC is aligned with the contents of the published Self-Assessment / Third-Party Assessment submissions made by those members.

The MB will, within the scope of the review:

a) Require the code member to demonstrate that the terms of its self-assessment / third-party assessment submission are materially accurate and implemented in relation to the service(s)

142 **Major Non-Conformity:** Based on objective evidence, the absence of, or a significant failure to implement and/or maintain conformance to the controls of the CoC (i.e., the absence of, or failure to implement, a CoC control); or a situation which would, on the basis of available objective evidence, raise significant doubts as to the capability of the measures implemented by the code member to achieve the stated policy and objectives of a control.
Minor Non-Conformity: Represents either a system weakness or minor issue that could lead to a major non-conformance if not addressed. Each minor non-conformity should be considered for potential improvement and to further investigate any system weaknesses, for possible inclusion in the corrective action program.

for which the assessment was submitted[143], using the sampling process as defined in Section 7.1;

b) Establish whether the code member's procedures for the identification, examination and evaluation of privacy requirements under the CoC and their related risks as well as the results of their implementation are consistent with the CoC and the code member's policy, objectives and targets;

c) Establish whether any and all procedures employed by the code member and within the scope of the review are sound and properly implemented.

3. **Audit reports**

All audit exercises carried out over a code member will result in the drafting of an audit report. This report must be of sufficient detail to facilitate and support any decision made by the MB regarding that code member.

The draft report of the MB shall be subject to review by at least one other MB member (who did not participate in the actual review). After completion, the draft report is sent the code member and a period of at least 7 days is given for a formal reaction. Any comments made by the code member are reviewed by the MB before finalizing its report. The final report is issued under the responsibility of the MBMR. If a final report contains a significant error or omission, the MBMR needs to rectify this by informing all relevant parties in writing.

The report shall contain:

a) The names of the members of the MB that performed the review;
b) Significant audit trails followed, and audit methodologies utilized;
c) Observations made, both positive (e.g. noteworthy features) and negative (e.g. potential nonconformities) regarding the requirements of the CoC and the effectiveness of it interpretation;
d) Opportunities for improvement of compliancy (if appropriate);
e) Comments on the conformity of the code member's practices with the requirements of the CoC. This should include a clear statement of conformity or nonconformity, referring to the applicable CoC controls and, where relevant, drawing comparisons with the results of previous audits carried out over that CSP.
f) A summary of the most important observations, positive as well as negative, regarding the implementation and effectiveness of the requirements of the CoC; and
g) A recommendation as to whether the code member should be considered in full/partial compliance with the CoC and, where relevant, corrective measures which should be enforced against that code member, along with supporting reasoning. Measures

[143] Typically virtually but the right for an on-site assessment is reserved and will be exercised at the discretion of the MB in cases of continued non-conformance or high-risk environments

proposed, as well as timeframes to be afforded to the code member in order to correct detected irregularities (where relevant), must be adequate in light of the severity of the irregularities and the associated risks for cloud customers and data subjects.

For minor-nonconformities, the MB may issue a formal warning to the code member and provide a timeframe during which the detected non-compliance must be cured.

For minor-nonconformities, where the code member does not respond adequately and in a timely manner to a formal warning issued by the MB, the MB may temporarily suspend the code member's CoC adherence seal until the MB is satisfied that the issue has been fully resolved.

For major-nonconformities, the MB may revoke the code member's CoC adherence seal.

The MB holds the right to require a full 3rd party on-site assessment of a code member if 1.) a major non-conformity is detected, or 2.) a number of minor non-conformities are detected, and this presents sufficient evidence that there is a breakdown of the code member's data privacy systems. The cost of these 3rd party assessments will be fully borne by the code member.

4. Qualified CoC auditing partner monitoring process

The Monitoring Committee must also monitor and assess Qualified CoC Auditing Partners on an annual basis, considering the requirements indicated in Section 1.2.2 above and the terms of ISO/IEC 17065. All Qualified CoC Auditing Partners must be audited at least once during a three-year span.

These exercises must abide by the following terms:

- Audits may be carried out on-site or remotely, depending on the scope of the audit.
- Audits will take place by random sampling of Qualified CoC Auditing Partners, under the same terms as described above (Section 3.5.1), with the necessary adaptations;
- There must be continuous monitoring of Qualified CoC Auditing Partners, including via the performance of at least one updated accreditation visit every two years, on-site or remotely, and one witness or review audit every two years.
- Witness audits must be performed periodically at a representative site, in order to verify proper delivery under the terms of the CoC and ISO/IEC 17065;
- Accreditation visits, witness audits or review audits may be performed in the same year for a Qualified CoC Auditing Partner, as long as there is at least one annual accreditation visit to review the following documentation:

- The management system of that Qualified CoC Auditing Partner;
- The expertise and competence of the personnel of that Qualified CoC Auditing Partner tasked with facilitating Third Party Assessment submissions for CSPs (as indicated in Section 1.2.2 above);
- The process followed by that Qualified CoC Auditing Partner to assess CSPs seeking to apply for a Third Party Assessment submission;
- The records and procedures used by that Qualified CoC Auditing Partner to track and report on CSPs they have assessed under the CoC.

The results of these audits will be reported to CSA. CSA reserves the right to suspend, withdraw or terminate the certification of a Qualified CoC Auditing Partner as such, based on the outcome of the audit exercises – in particular, where these entities fail to properly implement any corrective actions which are imposed upon them by CSA.

3.3.7 CODE OF ETHICS REVIEW PROCESS

The Statement of Ethics is reviewed and updated annually by the CSA Board of Directors. Any changes to the Statement of Ethics shall be communicated to all CSA Parties.

3.3.8 PLA AND OCF WG CHARTERS DOCUMENTS REVIEW PROCESS

CSA is responsible for approving any OCF and PLA charter revision and extension requests.

4 CONCLUSIONS

The work presented in this document constitutes the development of an important tool within the EU-SEC framework, covering a missing component in the EU compliance landscape, that is, the lack of an EU certification scheme for privacy and data protection that is tailored to cloud computing market and that satisfies the requirements of the GDPR.

The PLA CoC provides guidance to cloud service providers and customers (and other stakeholders) for ensuring compliance and transparency with respect to data protection privacy based on EU's regulatory landscape.

Equally important, the presented PLA CoC governance structure and its integrated management processes will assist towards the maintenance and constant alignment of the tool in two ways. First, internally to the EU-SEC framework, it will provide consistency and updates

with respect to any changes to the EU-SEC privacy control/requirements repository. Secondly, it will establish a trust and compliance transparency with the various external stakeholders within the cloud computing industry by employing coherent communication management and adherence mechanisms.

Certainly, there is space for further improvements to the current PLA framework since the legislation landscape is constantly evolving both at EU level and internationally, following the technological and legal advances toward data privacy and human rights protection. In addition, future work will dictate a necessity for continuous evaluation and improvement of the tool's governance structure as well as its capability and efficiency to integrate new technical and non-technical requirements with respect to data privacy.

APPENDIX A - PLA TEMPLATE AND STATEMENT OF ADHERENCE

Requirement	Requirement ID	Control	Control ID	Specification	CSP is Data Controller	CSP is Data Processor
1. CSP DECLARATION OF COMPLIANCE AND ACCOUNTABILITY.	**DCA**	**1. Declaration of compliance and accountability**	**DCA-1.1**	*1. Declare and ensure to comply with the applicable EU data protection law and with the terms of this Code of Conduct, also with respect to technical and organisational security measures, and to safeguard the protection of the rights of the data subject. Where there is a material change in applicable EU data protection law which may imply new or conflicting obligations regarding the terms of this Code of Conduct, the CSP commits to complying with the terms of the applicable EU data protection law.*	Applicable	Applicable
			DCA-1.2	*2. Declare and ensure to be able to demonstrate compliance with the applicable EU data protection law and with the terms of this Code of Conduct (accountability).*	Applicable	Applicable
			DCA-1.3	*3. Describe what policies and procedures the CSP has in place to ensure and demonstrate compliance by the CSP itself and its subcontractors (see also Controls no. WWP-3.1 to 3.5, below) or business associates, with the applicable EU data protection law and with the Terms of this Code of Conduct.*	Applicable	Applicable
			DCA-1.4	*4. Identify the elements that can be produced as evidence to demonstrate such compliance. Evidence elements can take different forms, such as self-certification/attestation, third-party audits (e.g., certifications, attestations, and seals), logs, audit trails, system maintenance records, or more general system reports and documentary evidence of all processing operations under its responsibility. These elements need to be provided at the following levels:* *(i) organisational policies level to demonstrate that policies are correct and appropriate;* *(ii) IT controls level, to demonstrate that appropriate controls have been deployed; and* *(iii) operations level, to demonstrate that systems are behaving (or not) as planned. Examples of evidence elements pertaining to different levels are data protection certifications, seals and marks.*	Applicable	Applicable
2. CSP RELEVANT CONTACTS AND ITS ROLE.	**CAR**	**1. CSP relevant contacts and its role**	**CAR-1.1**	*1. Specify CSP's identity and contact details (e.g., name, address, email address, telephone number and place of establishment);*	Applicable	Applicable
			CAR-1.2	*2. Specify the identity and contact details (e.g., name, address, email address, telephone number and place of establishment) of the CSP's local representative(s) (e.g., a local representative in the EU);*	Applicable	Applicable

Requirement	Requirement ID	Control	Control ID	Specification	CSP is Data Controller	CSP is Data Processor
			CAR-1.3	*3. Specify the CSP's data protection role for each of the relevant processing activities inherent to the services (i.e., controller, joint-controller, processor or subprocessor);*	Applicable	Applicable
			CAR-1.4	*4. Specify the contact details of the CSP's Data Protection Officer (DPO) or, if there is no DPO, the contact details of the individual in charge of privacy matters to whom the customer may address requests;*	Applicable	Applicable
			CAR-1.5	*5. Specify the contact details of the CSP's Information Security Officer (ISO) or, if there is no ISO, the contact details of the individual in charge of security matters to whom the customer may address requests.*	Applicable	Applicable
3. WAYS IN WHICH THE DATA WILL BE PROCESSED.	**WWP**	**1. General Information**	**WWP-1.1**	*CSPs that are **controllers** must provide details to cloud customers regarding: 1. categories of personal data concerned in the processing;*	Applicable	Not Applicable
			WWP-1.2	*2. purposes of the processing for which data are intended and the necessary legal basis to carry out such processing in a lawful way;*	Applicable	Not Applicable
			WWP-1.3	*3. recipients or categories of recipients of the data;*	Applicable	Not Applicable
			WWP-1.4	*4. existence of the right to request access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing, as well as the right to data portability;*	Applicable	Not Applicable
			WWP-1.5	*5. where applicable, the fact that the CSP intends to transfer personal data to a third country or international organisation and the absence of an adequacy decision by the European Commission, or reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available;*	Applicable	Not Applicable
			WWP-1.6	*6. the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;*	Applicable	Not Applicable
			WWP-1.7	*7. where the processing is based on consent, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;*	Applicable	Not Applicable
			WWP-1.8	*8. the right to lodge a complaint with a supervisory authority (as defined in Article 4 (21) GDPR);*	Applicable	Not Applicable
			WWP-1.9	*9. whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;*	Applicable	Not Applicable
			WWP-	*10. the existence of automated decision-*	Applicable	Not

Requirement	Requirement ID	Control	Control ID	Specification	CSP is Data Controller	CSP is Data Processor
			1.10	*making, including profiling, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject;*		Applicable
			WWP-1.11	*11. where the CSP intends to further process the personal data for a purpose other than that for which the personal data is being collected, information on that other purpose, prior to the relevant further processing;*	Applicable	Not Applicable
			WWP-1.12	*12. where personal data has not been obtained from the data subject, from which source the personal data originated, and if applicable, whether the data came from publicly accessible sources;*	Applicable	Not Applicable
			WWP-1.13	*13. activities that are conducted to provide the agreed cloud service(s) (e.g., data storage), activities conducted at the customer's request (e.g., report production) and those conducted at the CSP's initiative (e.g., backup, disaster recovery, fraud monitoring).*	Applicable	Not Applicable
			WWP-1.14	*CSPs that are **processors** must provide to cloud customers details on:* *14. the extent and modalities in which the customer-data controller can issue its binding instructions to the CSP-data processor (General Information - applicable to CSPs that are processors).*	Not Applicable	Applicable
			WWP-1.15	*15. Specify how the cloud customers will be informed about relevant changes concerning relevant cloud service(s), such as the implementation or removal of functions (General Information - applicable to both CSPs that are controllers and CSPs that are processors).*	Applicable	Applicable
2 Personal data location			**WWP-2.1**	*1. Specify the location(s) of all data centres or other data processing locations (by country) where personal data may be processed, and in particular, where and how data may be stored, mirrored, backed up, and recovered (this may include both digital and non-digital means).*	Applicable	Applicable
			WWP-2.2	*2. Notify cloud customers of any intended changes to these locations once a contract has been entered into, in order to allow the cloud customer to acknowledge or object.*	Applicable	Applicable
			WWP-2.3	*3. Allow cloud customers to terminate the contract in the event that an objection cannot be satisfactorily resolved between the CSP and the cloud customer, and afford the cloud customer sufficient time to procure an alternative CSP or solution (by establishing a transition period during which an agreed-upon level of services will continue to be provided to the cloud customer, under the contract).*	Applicable	Applicable

Requirement	Requirement ID	Control	Control ID	Specification	CSP is Data Controller	CSP is Data Processor
3 Subcontractors			**WWP-3.1**	*1. Identify subcontractors and subprocessors that participate in the data processing, along with the chain of accountabilities and responsibilities used to ensure that data protection requirements are fulfilled.*	Applicable	Applicable
			WWP-3.2	*2. Declare to cloud customers and further ensure that the CSP will not engage another processor without prior specific or general written authorisation of the cloud customer.*	Not Applicable	Applicable
			WWP-3.3	*3. Declare to cloud customers and further ensure that the CSP imposes on other processors the same data protection obligations stipulated between the CSP and the cloud customer, by way of a contract (or other binding legal act), in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of EU applicable law;*	Not Applicable	Applicable
			WWP-3.4	*4. Declare to cloud customers and further ensure that the CSP remains fully liable to the cloud customer for the performance of other processors' obligations, in case the other processors fail to fulfil their data protection obligations.*	Not Applicable	Applicable
			WWP-3.5	*5. Identify the procedures used to inform the cloud customer of any intended changes concerning the addition or replacement of subcontractors or subprocessors with customers retaining at all times the possibility to object to such changes or terminate the contract. In the event of termination by the cloud customer, the cloud customer must be afforded sufficient time to procure an alternative CSP or solution (by establishing a transition period during which an agreed-upon level of services will continue to be provided to the cloud customer, under the contract).*	Applicable	Applicable
4 Installation of software on cloud customer's system			**WWP-4.1**	*1. Indicate to cloud customers whether the provision of the service requires the installation of software on the cloud customer's system (e.g., browser plug-ins).*	Applicable	Applicable
			WWP-4.2	*2. Indicate to cloud customers the software's implications from a data protection and data security point of view.*	Applicable	Applicable
5 Data processing contract (or			**WWP-5.1**	*1. Share with the cloud customers the model data processing contract (or other binding legal act) which will govern the processing carried out by the CSP on behalf of the cloud*	Not Applicable	Applicable

Requirement	Requirement ID	Control	Control ID	Specification	CSP is Data Controller	CSP is Data Processor
other binding legal act)				*customer and set out the subject matter and duration of the processing, the type of personal data and categories of data subjects and the obligations and rights of the cloud customer.*		
			WWP-5.2	*The contract or other legal act must stipulate, that the CSP will do the following: 2. process personal data only upon documented instructions from the cloud customer, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the CSP is subject; in such a case, the CSP will inform the cloud customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;*	Not Applicable	Applicable
			WWP-5.3	*3. ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality, and that they do not process personal data except upon instructions from the cloud customer, unless otherwise required by Union or Member State law;*	Not Applicable	Applicable
			WWP-5.4	*4. implement all technical and organizational security measures which the CSP deems adequate, in light of the available technology, the state of the art, the costs in implementing those measures and the processing activities inherent to the services provided, to ensure that the CSP's services are covered by a level of security which is appropriate, considering the potential risks to the interests, rights and freedoms of data subjects;*	Not Applicable	Applicable
			WWP-5.5	*5. Respect the conditions for engaging another processor (see Controls no. WWP-3.1 to 3.5, above).*	Not Applicable	Applicable
			WWP-5.6	*6. taking into account the nature of the processing, assist the cloud customer by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the cloud customer's obligation to respond to requests for exercising the data subject's rights;*	Not Applicable	Applicable
			WWP-5.7	*7. assist the cloud customer in ensuring compliance with obligations related to security of processing, notification of a personal data breach to the supervisory authority; communication of a personal data breach to the data subject, and data protection impact assessment; taking into account the nature of processing and the information available to the processor;*	Not Applicable	Applicable
			WWP-5.8	*8. at the choice of the cloud customer, delete or return all personal data to customer after end of the provision of services relating to processing; and delete existing copies unless*	Not Applicable	Applicable

Requirement	Requirement ID	Control	Control ID	Specification	CSP is Data Controller	CSP is Data Processor
				Union or Member State law requires storage of the personal data (see Controls no. RRD-1.1 to 4.5, below).		
			WWP-5.9	*9. make available to the cloud customer all information necessary to demonstrate compliance with relevant data protection obligations; and allow for and contribute to audits, including inspections, conducted by the cloud customer or another auditor mandated by the customer.*	Not Applicable	Applicable

4. RECORD-KEEPING.	**REC**	**1. Recordkeeping for CSP-controller**	**REC-1.1**	*1. CSP controller confirms to cloud customers and commits to maintain a **record** of processing activities under CSP responsibility and make it available to the supervisory authority on request.*	Applicable	Not Applicable
			REC-1.2	*Record contains:* *2. name and contact details of controller and, where applicable, the joint controller, the controller's representative and the data protection officer;*	Applicable	Not Applicable
			REC-1.3	*3. the purposes of the processing;*	Applicable	Not Applicable
			REC-1.4	*4. a description of the categories of data subjects and of the categories of personal data;*	Applicable	Not Applicable
			REC-1.5	*5. categories of recipients to whom the personal data have been or will be disclosed, including recipients in third countries or international organisations;*	Applicable	Not Applicable
			REC-1.6	*6. 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 the documentation of suitable safeguards;*	Applicable	Not Applicable
			REC-1.7	*7. where possible, the envisaged time limits for erasure of different categories of data or, if that is not possible, the criteria used to determine that period;*	Applicable	Not Applicable
			REC-1.8	*8. a description of technical and organisational security measures in place (see also Controls no. SEC-1.1 to 1.3.xxvii, below).*	Applicable	Not Applicable
		2 Recordkeeping for CSP-processor	**REC-2.1**	*1. CSP processor confirms to cloud customers and commits to maintain a record of all categories of processing activities carried out on behalf of a controller and make it available to the supervisory authority upon request.*	Not Applicable	Applicable
			REC-2.2	*Record contains:* *2. 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;*	Not Applicable	Applicable

Requirement	Requirement ID	Control	Control ID	Specification	CSP is Data Controller	CSP is Data Processor
			REC-2.3	*3. categories of processing carried out on behalf of each controller;*	Not Applicable	Applicable
			REC-2.4	*4. 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 the documentation of suitable safeguards;*	Not Applicable	Applicable
			REC-2.5	*5. a description of technical and organisational security measures in place (see also Controls no. SEC-1.1 to 1.3.xxvii, below).*	Not Applicable	Applicable
5. DATA TRANSFER.	**DTR**	**1. Data transfer**	**DTR-1-1**	*1. Clearly indicate whether data is to be transferred, backed up and/or recovered across borders, in the regular course of operations or in an emergency.*	Applicable	Applicable
			DTR-1-2	*If transfer restricted under applicable EU law:* *2. Clearly identify the legal ground for the transfer (including onward transfers through several layers of subcontractors), e.g., European Commission adequacy decision, model contracts/standard data protection clauses, approved codes of conduct or certification mechanisms, binding corporate rules (BCRs), and Privacy Shield.*	Applicable	Applicable
6. DATA SECURITY MEASURES.	**SEC**	**1. Data security measures**	**SEC-1.1**	*1. Specify to cloud customers the technical, physical and organisational measures that are in place to protect personal data against accidental or unlawful destruction; or accidental loss, alteration, unauthorized use, unauthorised modification, disclosure or access; and against all other unlawful forms of processing;*	Applicable	Applicable
			SEC-1.2	*2. Describe to cloud customers the concrete technical, physical, and organisational measures (protective, detective and corrective) that are in place to ensure the following safeguards:*	Applicable	Applicable
			SEC-1.2.i	*(i) availability - processes and measures in place to manage risk of disruption and to prevent, detect and react to incidents, such as backup Internet network links, redundant storage and effective data backup, restore mechanisms and patch management;*	Applicable	Applicable
			SEC-1.2.ii	*(ii) integrity: - methods by which the CSP ensures integrity (e.g., detecting alterations to personal data by cryptographic mechanisms such as message authentication codes or signatures, error-correction, hashing, hardware radiation/ionization protection, physical access/compromise/destruction, software bugs, design flaws and human error, etc.);*	Applicable	Applicable

Requirement	Requirement ID	Control	Control ID	Specification	CSP is Data Controller	CSP is Data Processor
			SEC-1.2.iii	*(iii) confidentiality - methods by which the CSP ensures confidentiality from a technical point of view in order to assure that only authorised persons have access to data; including, inter alia as appropriate, pseudonymisation and encryption of personal data 'in transit' and 'at rest,' authorisation mechanism and strong authentication; and from a contractual point of view, such as confidentiality agreements, confidentiality clauses, company policies and procedures binding upon the CSP and any of its employees (full time, part time and contract employees), and subcontractors who may be able to access data;*	Applicable	Applicable
			SEC-1.2.iv	*(iv) transparency - technical, physical and organisational measures the CSP has in place to support transparency and to allow review by customers (see, e.g., Control no. MON-1.1, below);*	Applicable	Applicable
			SEC-1.2.v	*(v) isolation (purpose limitation) - How the CSP provides appropriate isolation to personal data (e.g., adequate governance of the rights and roles for accessing personal data (reviewed on a regular basis), access management based on the "least privilege" principle; hardening of hypervisors; and proper management of shared resources wherever virtual machines are used to share physical resources among cloud customers);*	Applicable	Applicable
			SEC-1.2.vi	*(vi) intervenability - methods by which the CSP enables data subjects' rights of access, rectification, erasure ('right to be forgotten'), blocking, objection, restriction of processing (see Control no. ROP-1.1, below), portability (see Controls no. PMT-1.1 to 1.2, below) in order to demonstrate the absence of technical and organisational obstacles to these requirements, including cases when data are further processed by subcontractors (this is also relevant for Section 9, 'Data portability, migration and transfer back');*	Applicable	Applicable
			SEC-1.2.vii	*(vii) portability - refer to Controls no. PMT-1.1 to 1.2., below;*	Applicable	Applicable
			SEC-1.2.viii	*(viii) accountability: refer to Controls no. DCA-1.1 to 1.4, above.*	Applicable	Applicable
			SEC-1.3	*3. As a minimum acceptable baseline, this CoC requires CSPs to comply with the controls set out in ENISA's Technical Guidelines for the implementation of minimum security measures for Digital Service Providers; for each control, the tables on sophistication levels within security measures provided in the ENISA's Technical Guidelines will apply, and the CSP must indicate the appropriate sophistication level complied with per each control (1 to 3), taking into account the state of the art, costs*	Applicable	Applicable

Requirement	Requirement ID	Control	Control ID	Specification	CSP is Data Controller	CSP is Data Processor
				of implementation and the nature, scope, context and purposes of processing, as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons. *It shall be noted that not all the minimum security measures listed in the ENISA's Technical Guidelines are directly applicable to all the CSPs. For instance, the requirements SO08 or SO09 cannot be directly implemented by a PaaS or SaaS provider. In any case, if some of the below mentioned security measures cannot be directly implemented by a CSP, the CSP in question shall nonetheless guarantee their implementation through their providers.*		
			SEC-1.3.i	*i. (SO 01) – Information security policy: The CSP establishes and maintains an information security policy. The document details information on main assets and processes, strategic security objectives.*	Applicable	Applicable
			SEC-1.3.ii	*ii. (SO 02) – Risk Management: The CSP establishes and maintains an appropriate governance and risk management framework, to identify and address risks for the security of the offered services. Risks management procedures can include (but are not limited to), maintaining a list of risks and assets, using Governance Risk management and Compliance (GRC) tools and Risk Assessment (RA) tools etc.*	Applicable	Applicable
			SEC-1.3.iii	*iii. (SO 03) – Security Roles: The CSP assigns appropriate security roles and security responsibilities to designated personnel. (i.e. CSO, CISO, CTO etc.).*	Applicable	Applicable
			SEC-1.3.iv	*iv. (SO 04) – Third party management: The CSP establishes and maintains a policy with security requirements for contracts with suppliers and customers. SLAs, security requirements in contracts, outsourcing agreements etc., are established to ensure that the dependencies on suppliers and residual risks do not negatively affect security of the offered services.*	Applicable	Applicable
			SEC-1.3.v	*v. (SO 05) – Background checks: The CSP performs appropriate background checks on personnel (employees, contractors and third party users) before hiring, if required, for their duties and responsibilities provided that this is allowed by the local regulatory framework. Background checks may include checking past jobs, checking professional references, etc.*	Applicable	Applicable
			SEC-1.3.vi	*vi. (SO 06) – Security knowledge and training: The CSP verifies and ensures that personnel have sufficient security knowledge and that they are provided with regular security training. This is achieved through for example, security awareness raising,*	Applicable	Applicable

Requirement	Requirement ID	Control	Control ID	Specification	CSP is Data Controller	CSP is Data Processor
				security education, security training etc.		
			SEC-1.3.vii	*vii. (SO 07) – Personnel changes: The CSP establishes and maintains an appropriate process for managing changes in personnel or changes in their roles and responsibilities.*	Applicable	Applicable
			SEC-1.3.viii	*viii. (SO 08) – Physical and environmental security: The CSP establishes and maintains policies and measures for physical and environmental security of datacentres such as physical access controls, alarm systems, environmental controls and automated fire extinguishers etc.*	Applicable	Applicable
			SEC-1.3.ix	*ix. (SO 09) – Security of supporting utilities: The CSP establishes and maintains appropriate security measures to ensure the security of supporting utilities such as electricity, fuel, HVAC etc. For example, this may be through the protection of power grid connections, diesel generators, fuel supplies, etc.*	Applicable	Applicable
			SEC-1.3.x	*x. (SO 10) – Access control to network and information systems: The CSP established and maintains appropriate policies and measures for access to business resources. For example, zero trust model, ID management, authentication of users, access control systems, firewall and network security etc.*	Applicable	Applicable
			SEC-1.3.xi	*xi. (SO 11) – Integrity of network components and information systems: The CSP establishes, protects, and maintains the integrity of its own network, platforms and services by taking steps to prevent successful security incidents. The goal is the protection from viruses, code injections and other malware that can alter the functionality of the systems or integrity or accessibility of information.*	Applicable	Applicable
			SEC-1.3.xii	*xii. (SO 12) – Operating procedures: The CSP establishes and maintains procedures for the operation of key network and information systems by personnel. (i.e. operating procedures, user manual, administration procedures for critical systems etc.).*	Applicable	Applicable
			SEC-1.3.xiii	*xiii. (SO 13) – Change management: The CSP establishes and maintains change management procedures for key network and information systems. These may include for example, change and configuration procedures and processes, change procedures and tools, procedures for applying patches etc.*	Applicable	Applicable
			SEC-1.3.xiv	*xiv. (SO 14) – Asset management: The CSP establishes and maintains change management procedures for key network and information systems. These may include for example, change and configuration procedures and processes, change procedures and tools, procedures for applying patches etc.*	Applicable	Applicable

Requirement	Requirement ID	Control	Control ID	Specification	CSP is Data Controller	CSP is Data Processor
			SEC-1.3.xv	*xv. (SO 15) – Security incident detection & Response: The CSP establishes and maintains procedures for detecting and responding to security incidents appropriately. These should consider detection, response, mitigation, recovery and remediation from a security incident. Lessons learned should also be adopted by the service provider.*	Applicable	Applicable
			SEC-1.3.xvi	*xvi. (SO 16) – Security incident reporting: The CSP establishes and maintains appropriate procedures for reporting and communicating about security incidents.*	Applicable	Applicable
			SEC-1.3.xvii	*xvii. (SO 17) – Business continuity: The CSP establishes and maintains contingency plans and a continuity strategy for ensuring continuity of the services offered.*	Applicable	Applicable
			SEC-1.3.xviii	*xviii. (SO 18) – Disaster recovery capabilities: The CSP establishes and maintains an appropriate disaster recovery capability for restoring the offered services in case of natural and/or major disasters.*	Applicable	Applicable
			SEC-1.3.xix	*xix. (SO 19) – Monitoring and logging: The CSP establishes and maintains procedures and systems for monitoring and logging of the offered services (logs of user actions, system transactions/performance monitors, automated monitoring tools etc.).*	Applicable	Applicable
			SEC-1.3.xx	*xx. (SO 20) – System test: The CSP establishes and maintains appropriate procedures for testing key network and information systems underpinning the offered services.*	Applicable	Applicable
			SEC-1.3.xxi	*xxi. (SO 21) – Security assessments: The CSP establishes and maintains appropriate procedures for performing security assessments of critical assets.*	Applicable	Applicable
			SEC-1.3.xxii	*xxii. (SO 22) – Compliance: The CSP establishes and maintains a policy for checking and enforcing the compliance of internal policies against the national and EU legal requirements and industry best practices and standards. These policies are reviewed on a regular basis.*	Applicable	Applicable
			SEC-1.3.xxiii	*xxiii. (SO 23) – Security of data at rest: The CSP establishes and maintains appropriate mechanisms for the protection of the data at rest.*	Applicable	Applicable
			SEC-1.3.xxiv	*xxiv. (SO 24) – Interface security: The CSP should establish and maintain an appropriate policy for keeping secure the interfaces of services which use personal data.*	Applicable	Applicable
			SEC-1.3.xxv	*xxv. (SO 25) – Software security: The CSP establishes and maintains a policy which ensures that the software is developed in a manner which respects security.*	Applicable	Applicable

Requirement	Requirement ID	Control	Control ID	Specification	CSP is Data Controller	CSP is Data Processor
			SEC-1.3.xxvi	*xxvi. (SO 26) – Interoperability and portability: The CSP uses standards which allow customers to interface with other digital services and/or if needed to migrate to other providers offering similar services.*	Applicable	Applicable
			SEC-1.3.xxvii	*xxvii. (SO 27) – Customer Monitoring and log access: The CSP grants customers access to relevant transaction and performance logs so customers can investigate issues or security incidents when needed.*	Applicable	Applicable
7. MONITORING.	**MON**	**1. Monitoring**	**MON-1.1**	*1. Indicate to cloud customers the options that the CSP has in place to allow the customer to monitor and/or audit in order to ensure appropriate privacy and security measures described in the PLA are met on an on-going basis (e.g., logging, reporting, first- and/or third-party auditing of relevant processing operations performed by the CSP or subcontractors). Any audits carried out which imply that an auditor will have access to personal data stored on the systems used by the CSP to provide the services will require that auditor to accept a confidentiality agreement.*	Applicable	Applicable
8. PERSONAL DATA BREACH.	**PDB**	**1. Personal Data Breach**	**PDB-1.1**	*Specify to cloud customers: 1. How the customer will be informed of personal data breaches affecting the customer's data processed by the CSP and/or its subcontractors, without undue delay and, where feasible, no later than 72 hours from the moment on which the CSP is made aware of the personal data breach in question. A CSP will be considered as "aware" of a personal data breach on the moment that it detects (e.g., directly, or due to a notification received from a subcontractor/sub-processor) an incident which qualifies as a personal data breach and establishes that that incident has affected data processed by the CSP and/or its subcontractors on behalf of a given customer. Should it not be feasible to inform a given customer of a personal data breach within the 72-hour deadline, the CSP will inform that customer of the personal data breach as soon as possible and accompany this communication to the customer with reasons for the delay.*	Applicable	Applicable
			PDB-1.2	*Explain to cloud customers the procedures in place to collect and disclose the following information:*	Applicable	Applicable
				2. the nature of the personal data breach including, where possible, the categories and approximate number of personal data records concerned;	Applicable	Applicable
			PDB-1.3	*3. the name and contact details of the data protection officer or other contact point where more information can be obtained*	Applicable	Applicable

Requirement	Requirement ID	Control	Control ID	Specification	CSP is Data Controller	CSP is Data Processor
				(see Section 2 'CSP relevant contacts and its role', above);		
			PDB-1.4	*4. the likely consequences of the personal data breach;*	Applicable	Applicable
			PDB-1.5	*5. the measures taken (or propose to be taken) to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.*	Applicable	Applicable
			PDB-1.6	*6. Where it is not feasible to provide all of the above information in an initial notification, the CSP must provide as much information to the customer as possible on the reported incident, and provide any further details needed to meet the above requirement as soon as possible (i.e., provision of information in phases).*	Applicable	Applicable
			PDB-1.7	*Specify to cloud customers:* *7. How the competent supervisory authority/ies will be informed of personal data security breaches, in less than 72 hours of becoming aware of a personal data breach);*	Applicable	Not Applicable
			PDB-1.8	*Specify to cloud customers:* *8. How data subjects will be informed, without undue delay, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.*	Applicable	Not Applicable
9. DATA PORTABILITY, MIGRATION AND TRANSFER BACK.	**PMT**	**1. Data portability, migration and transfer back**	**PMT-1.1**	*Specify to cloud customers:* *1.hHow the CSP assures data portability, in terms of the capability to transmit personal data in a structured, commonly used, machine-readable and interoperable format:*	Applicable	Applicable
			PMT-1.1.i	*(i) to the cloud customer ('transfer back', e.g., to an in-house IT environment);*	Applicable	Applicable
			PMT-1.1.ii	*(ii) directly to the data subjects;*	Applicable	Applicable
			PMT-1.1.iii	*(iii) to another service provider ('migration'), e.g., by means of download tools or Application Programming Interfaces, or APIs).*	Applicable	Applicable
			PMT-1.2	*2. how and at what cost the CSP will assist customers in the possible migration of data to another provider or back to an in-house IT environment. Whatever the procedure implemented, the CSP must cooperate in good faith with cloud customers, by providing a reasonable solution.*	Applicable	Applicable
10. RESTRICTION OF PROCESSING.	**ROP**	**1. Restriction of processing**	**ROP-1.1**	*1. Explain to cloud customers how the possibility of restricting the processing of personal data is granted; considering that where processing has been restricted, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims, or for the*	Applicable	Applicable

Requirement	Requirement ID	Control	Control ID	Specification	CSP is Data Controller	CSP is Data Processor
				protection of the rights of another natural or legal person, or for reasons of important public interest of the Union or of a Member State.		

11. DATA RETENTION, RESTITUTION AND DELETION.	**RRD**	**1. Data Retention, Restitution and Deletion policies.**	**RRD-1.1**	*1. Describe to cloud customers the CSP's data retention policies, timelines and conditions for returning personal data or deleting data once the service is terminated.*	Applicable	Applicable
			RRD-1.2	*2. Describe to cloud customers CSP's subcontractors' data retention policies, timelines and conditions for returning personal data or deleting data once the service is terminated.*	Applicable	Applicable
		2. Data Retention	**RRD-2.1**	*1. Indicate and commit to complying with the time period for which the personal data will or may be retained, or if that is not possible, the criteria used to determine such a period.*	Applicable	Applicable
			RRD-2.2	*2. Take into consideration the following criteria, when defining retention periods:* *Necessity – Personal data is retained for as long as necessary in order to achieve the purpose for which it was collected, so long as it remains necessary to achieve that purpose (e.g., to perform the services);* *Legal Obligation – Personal data is retained for as long as necessary in order to comply with an applicable legal obligation of retention (e.g., as defined in applicable labour or tax law), for the period of time defined by that obligation;* *Opportunity – Personal data is retained for as long as permitted by the applicable law (e.g., processing based on consent, processing for the purpose of establishing, exercising or defending against legal claims – based on applicable statutes of limitations regarding legal claims related to the performance of the services).*	Applicable	Applicable
		3. Data retention for compliance with sector-specific legal requirements	**RRD-3.1**	*1. Indicate whether and how the cloud customer can request the CSP to comply with specific sector laws and regulations.*	Applicable	Applicable
		4. Data restitution and/or deletion	**RRD-4.1**	*1. indicate the procedure for returning to the cloud customers the personal data in a format allowing data portability (see also Controls no. PMT-1.1 to 1.2, above);*	Applicable	Applicable
			RRD-4.2	*2. the methods available or used to delete data;*	Applicable	Applicable
			RRD-4.3	*3. whether data may be retained after the cloud customer has deleted (or requested deletion of) the data, or after the termination of the contract;*	Applicable	Applicable
			RRD-4.4	*4. the specific reason for retaining the data;*	Applicable	Applicable
			RRD-4.5	*5. the period during which the CSP will retain the data.*	Applicable	Applicable

Requirement	Requirement ID	Control	Control ID	Specification	CSP is Data Controller	CSP is Data Processor
12. COOPERATION WITH THE CLOUD CUSTOMERS.	**CPC**	**1. Cooperation with the cloud customers**	**CPC-1.1**	*1. Specify how the CSP will cooperate with the cloud customers in order to ensure compliance with applicable data protection provisions, e.g., to enable the customer to effectively guarantee the exercise of data subjects' rights: rights of access, rectification, erasure ('right to be forgotten'), restriction of processing, portability), to manage incidents including forensic analysis in case of security/data breach. See also Controls no. SEC-1.1 to 1.3.xxvii and PDB-1.1 to 1.8, above.*	Applicable	Applicable
			CPC-1.2	*2. Make available to the cloud customer and the competent supervisory authorities the information necessary to demonstrate compliance (see also Controls no. DCA-1.1 to 1.4, above).*	Applicable	Applicable
13. LEGALLY REQUIRED DISCLOSURE.	**LRD**	**1. Legally required disclosure**	**LRD-1.1**	*1. Describe the process in place to manage and respond to requests for disclosure of personal data by Law Enforcement Authorities, including to verify the legal grounds upon which such requests are based prior to responding to them, with special attention to the notification procedure to interested customers, unless otherwise prohibited, such as a prohibition under criminal law to preserve confidentiality of a law enforcement investigation.*	Applicable	Applicable
14. REMEDIES FOR CLOUD CUSTOMERS.	**RMD**	**1. Remedies for customer**	**RMD-1.1**	*1. Indicate what remedies the CSP makes available to the cloud customer in the event the CSP – and/or the CSP's subcontractors (see Controls no. WWP-1.1 to 5.9, above and, more specifically, Controls no. WWP-3.1 to 3.5, above) – breach the obligations under the PLA. Remedies could include service credits for the cloud customer and/or contractual penalties for the CSP.*	Applicable	Applicable
15. CSP INSURANCE POLICY.	**INS**	**1. CSP insurance policy**	**INS-1.1**	*1. Describe the scope of the CSP's relevant insurance policy/ies (e.g., data protection compliance-insurance, including coverage for sub-processors that fail to fulfil their data protection obligations and cyber-insurance, including insurance regarding security/data breaches).*	Applicable	Applicable

APPENDIX B – PLA COC STATEMENT OF ADHERENCE

CSA Code of Conduct (CoC):
Statement of Adherence
Self-Assessment

3. Name and URL/Address

Name	
URL/Address	

4. Services covered by the PLA Code of Practice (CoP)

Please provide a list with the name(s) of the service(s) covered by the PLA CoP will be provided in the table below.

Service 1 name	
Service 2 name	
…	
Service *n* name	

5. Means of Adherence

Self-Assessment	

6. Scope of Adherence

Please provide a description of the assessment scope for each of the services listed in (2) with regards to the PLA Code of Practice.

Description	

7. PLA Code of Practice version used

Version ID	(e.g., v. 3.0)

8. Issue/Expiry Date

Issue Date	
Expiry Date	

9. Legal representative/DPO signed by

By signing this statement of adherence, the organization/company confirms that:

a. As of this date, the services listed in (2) adhere to the CSA CoC requirements (see CSA CoC section 3.3, "CSA CoC Marks issuing, Statement of Adherence publication and complaints management").

b. The CSA CoC self-attestation mark will have a validity of 12 months from the day of their issuance and should be renewed after this period. Moreover, the CSA CoC self-attestation must be revised every time there's a change in the company's relevant policies or practices.

Name	
Title	
Date	

CSA Code of Conduct (CoC):
Statement of Adherence
3rd Party Assessment

1. Name and URL/Address

Name	
URL/Address	

2. Services covered by the PLA Code of Practice (CoP)

Please provide a list with the name(s) of the service(s) covered by the PLA CoP will be provided in the table below.

Service 1 name	
Service 2 name	
…	
Service *n* name	

3. Means of Adherence

3rd Party Assessment	

4. Scope of Adherence

Please provide a description of the assessment scope for each of the services listed in (2) with regards to the PLA Code of Practice.

Description	

5. PLA Code of Practice version used

Version ID	(e.g., v. 3.0)

6. Assessing Body

Name	

7. Country of Issuing

Name	

8. Seal Number

Number	

9. Issue/Expiry Date

Issue Date	
Expiry Date	

10. Legal representative/DPO signed by

By signing this statement of adherence, the organization/company confirms that:

a. As of this date, the services listed in (2) adhere to the CSA CoC requirements (see CSA CoC section 3.3, "CSA CoC Marks issuing, Statement of Adherence publication and complaints management").

b. The third-party assessment seals will have a validity of 12 months from the day of their issuance and should be renewed after this period. Moreover, third-party assessment must be revised every time there's a change in the company's relevant policies or practices.

Name	
Title	
Date	

APPENDIX C - THE CSA STAR PROGRAM AND OPEN CERTIFICATION FRAMEWORK (OCF)

CSA launched the CSA Security Trust and Assurance Registry (STAR) in 2011 with the objective of improving trust in the cloud market by offering increased transparency and information security assurance.

The CSA STAR provides cloud stakeholders, e.g., Cloud Service Customers (CSC), Cloud Service Providers (CSPs), Cloud Auditors, and others with a public repository in which CSPs can publish information related to their internal due diligence results based on CSA best practices: the Cloud Control Matrix (CCM) and Consensus Assessment Initiative (CAI).

The CSA Open Certification Framework (OCF) Working Group (WG) was launched in 2012 with the objective to develop the technical capabilities necessary to support CSA STAR.

The OCF WG was tasked with defining the CSA security certification framework as well as the certification schemes included in the framework.

The WG defined the Open Certification Framework as a multilayer structure based on three levels of trust:

- Level 1, Self-Assessment: STAR Self-Assessment
- Level 2, Third-Party Assessment: STAR Certification, STAR Attestation and C-STAR Assessment
- Level 3, Continuous Monitoring/Auditing: STAR Continuous

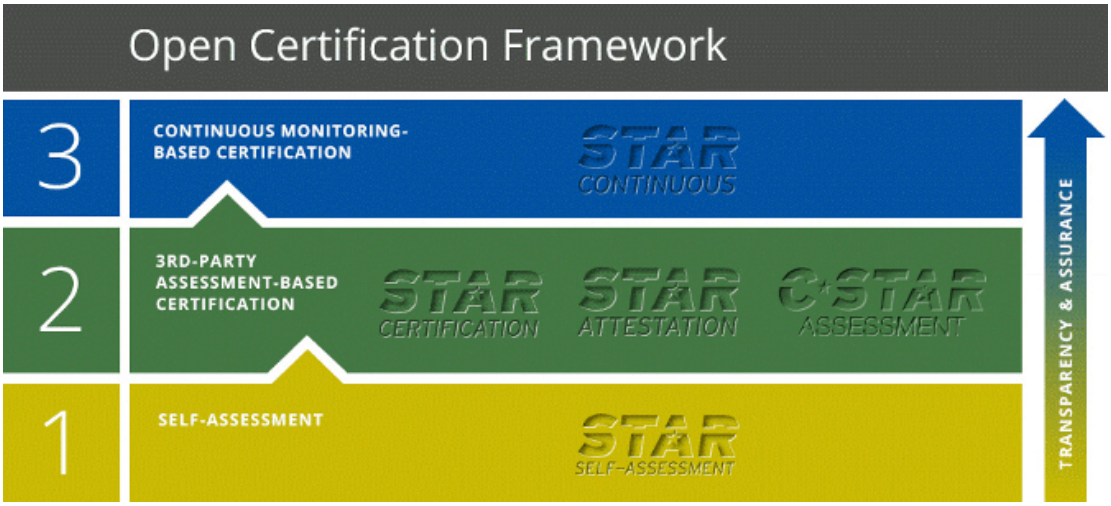


Figure 2: Open Certification Levels Diagram

In 2012, the CSA STAR Program was launched as a means of supporting the CSA STAR effort and managing the implementation of the OCF.

Currently the STAR Program offers the Self-Assessment (Level 1) and Third-Party Assessment-based Certification/Attestation (Level 2).

The continuous monitoring/auditing-based certification is under development.

The relationship between OCF Levels is the following.

From the "assurance" perspective, OCF Level 1 provides good-to-moderate assurance, OCF Level 2 provides high assurance, and OCF Level 3 provides very high assurance.

From a "transparency" perspective, OCF Level 1 provides good transparency, OCF Level 2 provides low to high transparency, and OCF Level 3 provides very high transparency.

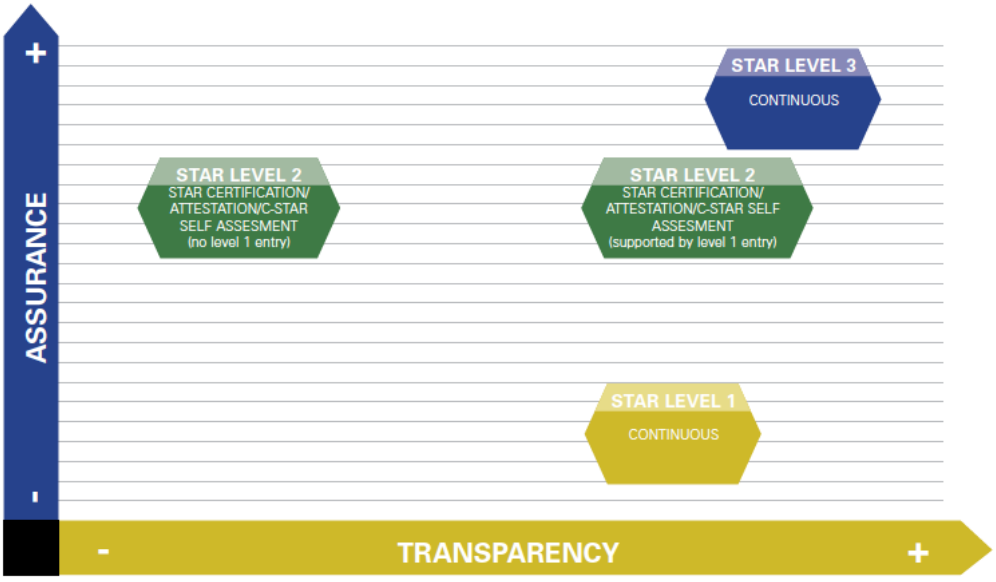


Figure 3: Levels of Transparency offered by the three OCF levels

Notice that degrees of transparency offered by the three OCF levels do not necessarily correspond to the three levels of assurance. For instance, OCF Level 1 could provide better transparency than OCF Level 2, since neither the STAR Certification nor STAR Attestation schemes require the organisation to make its security controls publicly available.

CSA encourages organisations aiming to certify at OCF Level 2 to first self-assess at OCF Level 1.

APPENDIX D - CODE OF ETHICS

1. Scope

This Statement of Ethics applies to all Board Members, officers, full-time and part-time employees, contractors, or volunteers of the Cloud Security Alliance ("CSA Parties").

2. Definitions

Board Member: a member of the Board of Directors of the Cloud Security Alliance in office.

CSA Party: a Board Member, officer, full-time or part-time employee, contractor, or volunteer of the Cloud Security Alliance.

Volunteer: an individual who spends significant time advancing the mission of the Cloud Security Alliance as a member of its Board of Directors or through service on an advisory committee to the Board of Directors.

3. Ethics principles

The CSA Parties, by virtue of their roles and responsibilities within the Cloud Security Alliance, represent the Cloud Security Alliance to the larger society. They have a special duty to observe the highest standards of personal and professional conduct.

The Cloud Security Alliance requires all CSA Parties to comply with the following Ethics Principles:

- Our words and actions embody respect for truth, fairness, free inquiry, and the opinions of others;
- We respect all individuals without regard to race, colour, sex, sexual orientation, marital status, creed, ethnic or national identity, handicap, or age;
- We uphold the professional reputation of others and give credit for ideas, words, or images originated by others;
- We safeguard privacy rights and confidential information;
- We do not grant or accept favours for personal gain;
- We do not solicit or accept favours where a higher public interest would be violated;
- We avoid actual or apparent conflicts of interest and, if in doubt, seek guidance from appropriate authorities;

- We follow the letter and spirit of the laws and regulations affecting the Cloud Security Alliance;
- We actively encourage colleagues to join us in supporting these laws and regulations and the standards of conduct in these Ethics Principles.

4. Review and Acknowledgment of Statement of Ethics

Upon the entry into force of this Statement of Ethics, and thereafter for each calendar year before the last day of January, each CSA Party shall be provided with and asked to review a copy of this Statement of Ethics and to acknowledge in writing that he/she has read, understood and agreed to abide by this Statement of Ethics.

5. Entry into Force and Implementation

This Statement of Ethics is approved by the Board of Directors of the Cloud Security Alliance. This Statement of Ethics will enter into force as of January 1, 2012. The Board of Directors directs the Cloud Security Alliance Executive Director to ensure that this Statement of Ethics is given to and acknowledged by all CSA Parties.

6. Oversight

The Board shall have direct responsibility for the oversight of this Statement of Ethics and for the establishment of procedures to support this Statement of Ethics.

7. Review and Changes

This Statement of Ethics shall be reviewed and updated as necessary, annually by the Board of Directors. Any changes to the Statement of Ethics shall be communicated to all CSA Parties.

APPENDIX E – PRIVACY LEVEL AGREEMENT WORKING GROUP CHARTER

EXECUTIVE OVERVIEW

Data protection compliance is becoming increasingly risk-based.[144] Data controllers and processors are accountable for determining and implementing in their organisations appropriate levels of protection of the personal data they process. In such decision, they have to take into account factors such as state of the art of technology; 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.[145] As a result, Cloud Service Providers (CSPs) will be responsible for self-determining the level of protection required for the personal data they process.

In this scenario, the PLA Code of Conduct gives guidance for legal compliance and the necessary transparency on the level of data protection offered by the CSP.

Privacy Level Agreements (PLAs) are essentially intended to provide:

- Cloud customers of any size with a tool to evaluate the level of personal data protection offered by different CSPs (and thus to support informed decisions)146
- CSPs of any size and geographic location with a guidance to comply with European Union (EU) personal data protection legislation and to disclose, in a structured way, the level of personal data protection they offer to customers.

PLA Code of Conduct is designed to meet both actual, mandatory EU legal personal data protection requirements (i.e., Directive 95/46/EC and its implementations in the EU Member States), by leveraging the PLA [V2] structure, and the forthcoming requirements of the GDPR. This specific feature makes PLA [V3] a unique tool that helps CSPs, cloud customers and potential customers manage the transition from the old to the new EU data protection regime, and contributes to the proper application of the GDPR into the cloud sector. PLA [V3] specifies the application of the GDPR in the cloud environment, primarily with regard to the following categories of requirements:

[144] See, e.g., Preamble 83 and Articles 25, 32, 33, 34 and 35 of the 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 - GDPR)

[145] See, e.g., Articles 24, 25, 32, 35 and 39 of the GDPR.

[146] "All cloud providers offering services in the European Economic Area (EEA) should provide the cloud client with all the information necessary to rightly assess the pros and cons of adopting such services. Security, transparency, and legal certainty for the clients should be key drivers behind the offer of cloud computing services." Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing ("A.29WP05/2012"), p. 2; "A precondition for relying on cloud computing arrangements is for the controller [cloud client] to perform an adequate risk assessment exercise, including the locations of the servers where the data are processed and the consideration of risks and benefits from a data protection perspective." p. 4 id. (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf).

- Fair and transparent processing of personal data;
- The information provided to the public and to data subjects (as defined in Article 4 (1) GDPR);
- The exercise of the rights of the data subjects;
- The measures and procedures referred to in Articles 24 and 25 GDPR and the measures to ensure security of processing referred to in Article 32 GDPR;
- The notification of personal data breaches to Supervisory Authorities (as defined in Article 4 (21) GDPR) and the communication of such personal data breaches to data subjects; and
- The transfer of personal data to third countries.

Additionally, PLA [V3] contains mechanisms that enable the body referred to in Article 41 (1) GDPR to carry out the mandatory monitoring of compliance with its provisions by the controllers or processors that undertake to apply it, without prejudice to the tasks and powers of competent Supervisory Authorities pursuant to Article 55 or 56 GDPR.

BACKGROUND

The Cloud Security Alliance ("CSA") published in 2013 the "Privacy Level Agreement Outline for the Sale of Cloud Services in the European Union" (PLA [V1]) and in 2015 the "Privacy Level Agreement [V2]: A Compliance Tool for Providing Cloud Services in the European Union" (PLA [V2]).

Based on the work already created by the, i.e. PLA V1 and PLA V2, the CSA PLA WG will develop "Privacy Level Agreement [V3] Code of Conduct. A Compliance Tool for Providing Cloud Services in the European Union" (PLA [V3]) to address the upcoming change to the data protection laws of the European Union and Europe Economic Area Member States to the General Data Protection Regulation, Regulation (EU) 2016/679 also known at the GDPR.[147]

PRACTICAL USE

The PLA CoC is intended to be used as the structure for the creation of an appendix to a Cloud Services Agreement that would describe the level of privacy and data protection that the CSP undertakes to commit to provide and maintain with respect to the personal data that its customer will provide to the CSP and process through the CSP's service(s).

[147] http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=it.

The PLA Code of Conduct provides a structure for CSPs to register the completed Privacy Statement developed in accordance to the PLA Code of Practice [V3] with the CSA STAR Service that will be used as a custodian.

The adoption of the PLA CoC worldwide can promote a powerful global industry standard, enhance harmonization and facilitate compliance with applicable EU data protection law.

WORKING GROUP SCOPE AND OBJECTIVES

The working group is chartered to research in the area of privacy and data protection compliance for cloud computing services at global scale and will pursue the following three goals.

Objective 1: Define a Privacy Level Agreement Code of Practice that addresses the requirements set forth in the GDPR, based on the experience of PLA [V2].

Objective 2: Define a Governance Structure and mechanisms of adherence to the PLA CoC.

Objective 3: Participate in the implementation and management over time of the PLA CoC.

Objective 4: Monitor the legal and regularly landscape so to be able to update the PLA Code of Practice.

Objective 5: Provide expert opinion to CSA when complaints about PLA Self Attestation or Third-Party Assessment are submitted.

Objective 6: Provide expert opinion to CSA Open Certification Working Group on the PLA CoC third party assessment scheme.

WORKING GROUP STRUCTURE AND FUNCTIONING

Co-Chairs
The working group will be led by co-chairs in addition to the selected leadership. The co-chairs will assist with the leadership responsibility of the working group. The co-chairs may appoint others as necessary to assure the effective execution of the defined research.

Sub-Work Groups
Ad hoc sub-working groups comprised of subject matter experts may be formed to plan or execute any related outreach, awareness, or research opportunities. Such sub-working groups shall report directly to the PLA Working Group.

The Working Group may also choose to allow resource sharing between cloud communities and other CSA working groups to assist in the timely completion of projects, programs and other activities needed to support/enable the working group's defined body of work.

Membership

Any individual with the appropriate expertise can participate to the activities of the working group. The table below provides an example of the organizations that CSA encourages to join the PLA Working Group.

Community	Purpose	Example
International, Regional, National Regulatory Bodies, Agencies, Supervisory Authorities, and Institutions	Policy makers and Supervisory Authorities who can ensure appropriate alignment with legal and regulatory requirements	· European Commission · European Data Protection Board · EDPS · National Supervisory Authorities · ENISA · METI · IDB - IDA · USA FTC · etc.
CSA OCF Co-Chairs	To maintain the alignment with OCF and assess the feasibility of the introduction of a privacy module / seal in the OCF.	· OCF Co-chairs
CSA GRC Stack WG Co-Chair	Maintain alignment GRC Stack research initiatives	· Cloud Controls Matrix (CCM) · Consensus Assessment Initiative (CAI) · CloudAudit · Cloud Trust Protocol (CTP)
CSA International Standardization Council	Maintain alignment with ISC work	· ISC Co-chairs
Internal Auditors/Consultants	Lead representatives from organization who provides internal auditing services and consultancies.	· Big Four (PwC, E&Y, Deloitte, KPMG) · Representatives of smaller Auditing and consulting firms
Other research effort	Representatives from ongoing research project with similar scope to maintain alignment and consistency between projects	· A4Cloud · Internet2
CSA Corporate Members (Cloud Service Providers	Representatives from cloud service/solution providers to validate applicability of the PLA4EU Compliance and the feasibility of the introduction of privacy certification	·
Independent Subject Matter Expert	Independent Subject Matter Expert	· European Privacy Association (EPA) · International Association of Privacy Professionals (IAPP)
Cloud	Representatives from corporate	· EuroCio

Community	Purpose	Example
Users/Consumers	cloud provider and/or representatives of users/consumers organization to ensure alignment with user requirements and needs	· etc.

Alignments with Other Groups
The working group will share research and align with other CSA Working Groups, advisory groups, and industry partners such as SDO's.

Operations

Advisory
The PLA Working Group will be advised by the CSA Subject Matter Expert (SME) Advisory Council, International Standardization Council (ISC), and CSA Executive Team to ensure that the research under the working group is within the scope of the CSA and aligns with other industry partner research. The research will remain unique to industry and make reference to any redundant or replicated works.

Research Lifecycle
The PLA Working Group will follow the development of the CSA research lifecycle for all projects and initiatives.

Peer Review
The PLA Working Group will seek CSA's help in reaching out to peers for reviewing our charter, publications, and other documented activities of the working groups.

Communications Methods

Infrastructure & Resource Requirements
The PLA Working Group will be composed of CSA volunteers; it will have co-chairs and/or committee(s). The working group will require typical project management, online workspace and technical writing assistance.

Working Group Meetings
The PLA Working Group will hold periodic conference calls. Attendance or participation in the online workspace by the Principal or Alternate is required. The Alternate must have full authority to act on behalf of the Principal if the Principal is absent. In-person meetings will happen in a location to be determined.

Decision-making Procedure
Decision shall be made by simple majority of the PLA Working Group members (including the Co-Chairs).

Definition of a majority

1. A majority shall consist of more than half the members participating in person or by phone, and voting

2. In computing a majority, all members casting a vote for, against or abstention) shall be counted and taken into account.

3. In case of a tie, a proposal or amendment shall be deemed rejected.

4. For the purpose under this Charter, a "member present and voting" shall be a member voting for, against, or "no opinion" a proposal, including proxy representative. Proxy where authority is delegated through a written statement or non-repudiated email will be declared and inspected for validity by a co- chair before voting starts.

Abstentions of more than fifty per cent
When the number of abstentions exceeds half the total number of votes cast (for, against, abstentions), consideration of the matter under discussion shall be postponed to a later meeting, at which time the matter shall be further discussed, any documentation or decision reviewed and amended, and the revised proposal shall be submitted again to a vote by the Working Group.

Voting procedures
The voting procedures are as follows:

1. By email sent to the co-chairs unless a secret ballot has been requested;

2. By a secret ballot, sent by mail to a trusted third party, if at least 20% of the members present and entitled to vote so request before the beginning of the vote (online voting is applicable)

Before commencing a vote, the Chair(s) shall review any request as to the manner in which the voting shall be conducted, and then shall formally announce the voting procedure to be applied and the issue to be submitted to the vote. The Chair(s) shall then declare the beginning of the vote and, when the vote has been taken, shall announce the results.

In the case of a secret ballot, the secretariat shall at once take steps to ensure the secrecy of the vote.

Deliverable approval and endorsement process
PLA Working Group deliverables are subject to the approval and endorsement of CSA. The decision is based on the advice of the SME Advisory Council.

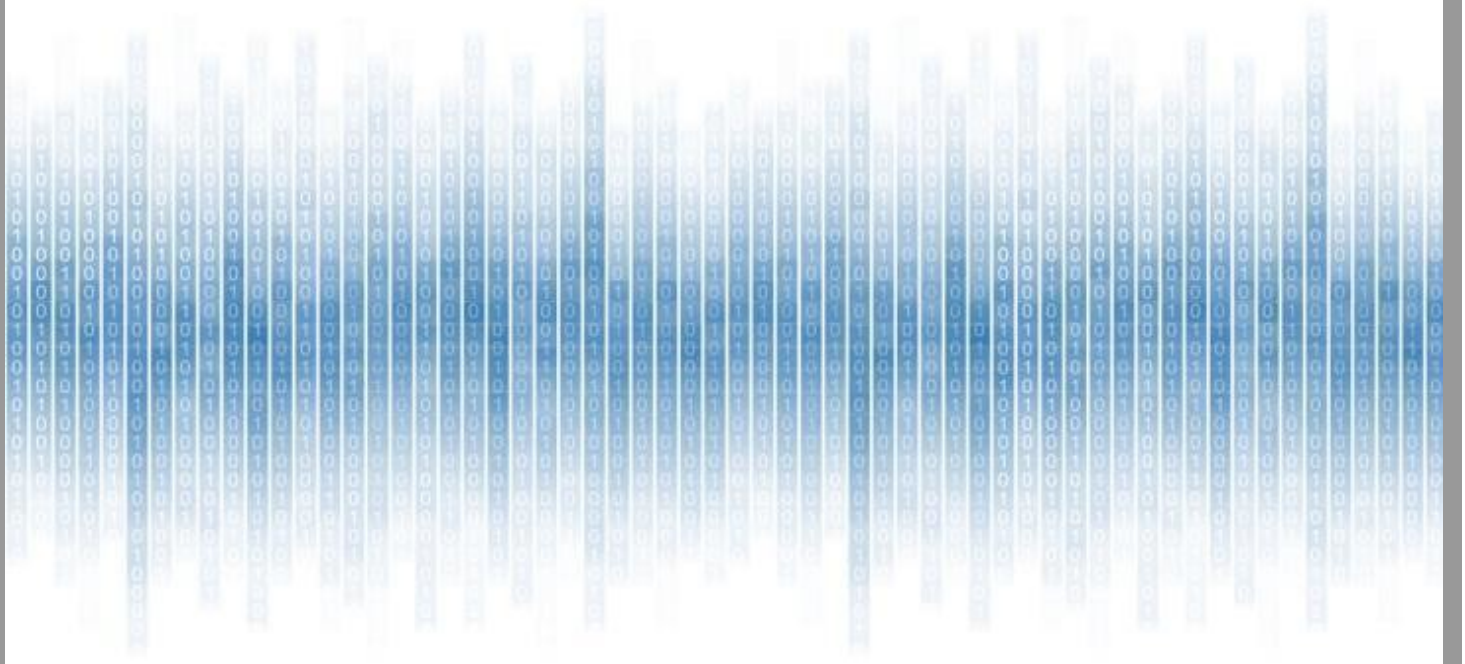
DELIVERABLES

1. PLA CoC objectives, scope, methodology, assumptions and explanatory notes
2. Privacy Level Agreement [V3] Code of Practice
3. PLA Code of Conduct (CoC) Governance and adherence mechanisms
4. The PLA Template
5. The PLA Statement of Adherence template
6. Presentations and other awareness material
7. Procedure for complain management
8. PLA Code of Practice change management process

DURATION

This charter will be valid until 31 March 2019

APPENDIX F – OPEN CERTIFICATION WORKING GROUP CHARTER



Open Certification Framework

Working Group

Charter

2017

WORKING GROUP EXECUTIVE OVERVIEW

Mission

The mission of the Open Certification Framework Working Group is to develop, maintain, review, update, support the implementation of all the certification schemes included in the CSA Security Transparency Assurance Registry (STAR) Program. The OCF WG focuses on information security and privacy certification schemes for processes and product in the areas of cloud computing and mobile.

Working Group Scope and Responsibilities

The Cloud Security Alliance has identified gaps within the IT ecosystem that are inhibiting market adoption of secure and reliable cloud services. Consumers do not have simple, cost effective ways to evaluate and compare their providers' resilience, data protection and privacy capabilities and service portability.

The CSA Open Certification Framework (OCF) is an industry initiative to allow global, trusted certification of cloud providers. It is a program for flexible, incremental and multi-layered cloud provider certification according to the Cloud Security Alliance's industry leading security guidance and control framework.

The objective of the program will be to harmonize with existing third-party certifications and audit standards to avoid duplication of effort and cost.

The CSA OCF is based upon the control capabilities achieving maturity through continuous assurance as defined within the CSA Governance, Risk and Compliance (GRC) Stack and Privacy Level Agreement research initiatives.

The CSA OCF will support several tiers, recognizing the varying assurance requirements and maturity levels of providers and consumers. These will range from the CSA Security, Trust and Assurance Registry (STAR) self- assessment to high-assurance specifications that are continuously monitored.

Discussions and decisions/changes proposed by the OCF and its working groups are considered privileged and confidential and are not to be made public until either the proposed changes have been finalized or a vote has been taken and so documented.

Working Group Membership

Eligible members are of the OCF WG

- CSA enterprise customer corporate members (Enterprise Users)
- CSA solution provider corporate members (CSPs)

- International, Regional, National Regulatory Bodies, Agencies and Institutions (European Commission, European Data Protection Board, ENISA, METI, IDB – IDA, NIST, FedRAMP, USA DoD, USA FTC, etc.)
- SDOs and other organizations (e.g., ISO/IEC / JTC 1 / SC27, SC38, ITU-T, ETSI, W3C, ISACA, AICPA, JIPDEC, JASA, etc.)
- Representatives of relevant research project not directly run under the auspices of the CSA, but relevant to the activities of the OCF WG (e.g., Accountability for Cloud, CUMULUS, SLA Ready, SPECS, Internet2/NET+, Cloud for Europe, etc.)
- Representative of trade and users associations (e.g., EuroCIO, etc.)

Working Group Structure

Co-Chairs
The working group will be led by co-chairs in addition to the selected leadership. Co-chairs must be members of CSA, unless the CSA Executive Team has granted an exception. The co-chairs will assist with the leadership responsibility of the working group. The co-chairs may appoint others as necessary to assure the effective execution of the defined research. Responsibilities of the co-chair include:

- Define the work plan for each year (e.g., meetings and expected deliverables)
- Ensure progress of work according to the work plan
- Report to the CSA Executive Team on execution risks and suggest possible solutions
- Convene meetings when necessary and act as Chairperson of OCF.
- Lead the preparation of draft deliverables, or identify a suitable person within the OCF who will take the role of main editor/rapporteur of the deliverable
- Ensure that guidance provided in the current OCF charter is followed
- Ensure that relevant documents are circulated to OCF members

Committees
The working group may designate and organize subcommittees to aid in research with the initiatives pertaining to the subject matter of the working group.

Sub-Work Groups
Ad hoc sub-work groups comprised of subject matter experts may be formed to plan or execute any related outreach, awareness or research opportunities. Such sub-working groups shall report directly to the main working group.

Alignments with Other Groups
The OCF working group may also choose to allow resource sharing between cloud communities and other CSA working groups to assist in the timely completion of projects,

programs and other activities needed to support/enable the working group's defined body of work, on demand basis. The list other groups that the OCF working group will be working closely with includes, but is not limited to:

- CSA Cloud Trust Working Group:
  - Specifically collaborating on the implementation of the OCF Level 3.
- CSA GRC Stack Working Group:
  - Specifically collaborating on…
    - defining "OCF compliance profiles" (e.g., subsets and addendum of CCM relevant to a certain sector, service offering)
    - ensure the controls and measures relevant to accountability are specified and integrated
- CSA PLA Working Group:
  - Specifically collaborating on the development of a scheme to assess adhering organizations against the requirements included in the PLA Code of Conduct v3.
- CSA MAST Initiative Working Group:
  - Specifically collaborating on development of a scheme (tentatively named CSA STAR Mobile) to certify mobile applications against the requirements to be developed from the MAST whitepaper
- Additional groups:
  - CSA Cloud Audit Working Group
  - EC C-SIG
  - ENISA
  - ISO SC 27
  - NIST
  - AICPA
  - The German Federal Office for Information Security (BSI)
  - and other (e.g., ANSSI)

Operations

Advisory

- The CSA Working Group will be advised by the CSA Subject Matter Expert (SME) Advisory Council, International Standardization Council (ISC), and CSA Executive Team to ensure that the research under the working group is within the scope of the CSA and aligns with other industry partner research. The research will remain unique to industry and make reference to any redundant or replicated works.

Research Lifecycle
The CSA Working Group will follow the development of the CSA research lifecycle for all projects and initiatives:
https://downloads.cloudsecurityalliance.org/initiatives/general/CSA_Research_Lifecycle_FINAL.pdf

Peer Review
We will seek CSA's help in reaching out to peers for reviewing our charter, publications, and other documented activities of the working groups.

Communications Methods

Infrastructure & Resource Requirements
The working group will be composed of CSA volunteers; it will have co-chairs and/or committee(s). The working group will require typical project management, online workspace and technical writing assistance.

Work Group Conference Calls and In-person Meetings
The working group will hold conference calls no less than bi-monthly. Attendance or participation in the online workspace by the Principal or Alternate is required. The Alternate must have full authority to act on behalf of the Principal if the Principal is absent. In-person meetings will happen in a location to be determined.

Decision-Making Procedures

A. Definition of a majority

1. A majority shall consist of more than half of the members present and voting.
2. In computing a majority, members abstaining shall not be taken into account.
3. In case of a tie, a proposal or amendment shall be considered rejected.
4. For the purpose under this Charter, a "member present and voting" shall be a member voting "for" or "against" a proposal, including proxy representative.
5. Proxy where authority is delegated through a written statement or non-repudiated email should be declared and inspected for validity by the working group leadership before voting starts.

B. Abstentions of more than fifty percent

1. When the number of abstentions exceeds half the number of votes cast (for votes, plus against votes, plus abstention votes), consideration of the matter under discussion shall be postponed to a later meeting, at which time abstentions shall not be taken into further account.

C. Voting procedures

1. The voting procedures are as follows:

   a) By a show of hands as a general rule, unless a secret ballot has been requested; if at least two members, present and entitled to vote, so request before the beginning of the vote and if a secret ballot under b) has not been requested, or if the procedure under a) shows no clear majority

   b) By a secret ballot, if at least five of the members present and entitled to vote so request before the beginning of the vote (online voting is applicable)

2) The Chair(s) shall, before commencing a vote, observe any request as to the manner in which the voting shall be conducted, and then shall formally announce the voting procedure to be applied and the issue to be submitted to the vote. The Chair(s) shall then declare the beginning of the vote and, when the vote has been taken, shall announce the results.

3) In the case of a secret ballot, the working group leadership shall at once take steps to ensure the secrecy of the vote.

Deliverables/Activities

The tentative deliverables include:

- Alignment of OCF Level 2 (STAR Certification) with ISO/IEC 27017 and 27018.
- Amendment of the STAR Certification scheme to better align with ISO/IEC 27006 current version.
- Amendment of the STAR Attestation certification scheme (STAR Attestation Type 1 based on SOC 2 Type 1).
- Definition and implementation of the OCF Level 3 – STAR Continuous.
- Whitepaper outlining the benefits of CSA STAR Program.
- Definition and implementation of the PLA Code of Conduct adherence scheme based on the recommendation of the PLA WG.
- Definition and implementation of the STAR Mobile Certification scheme based on the input of the MAST WG.

Deliverables will be governed by CSA's intellectual property rights policy.

Duration

This charter will be valid until 31 March 2019

Charter Revision History

November 2015	March 2016	Sept 2017