CLOUD SECURITY ALLIANCE

CODE OF CONDUCT FOR GDPR COMPLIANCE

PRIVACY LEVEL AGREEMENT WORKING GROUP, JUNE 2018

cloud security alliance®

ABOUT & ACKNOWLEDGMENTS

The Cloud Security Alliance (CSA) Code of Conduct (CoC) for GDPR Compliance has been developed within CSA by an expert Working Group (WG) chaired by Prof. Dr. Paolo Balboni (Founding Partner of ICT Legal Consulting; Professor of Privacy, Cybersecurity, and IT Contract Law at the European Centre on Privacy and Cybersecurity within the Maastricht University Faculty of Law; President of the European Privacy Association) and Francoise Gilbert (Partner, Greenberg Traurig; co-chair PLI Privacy and Security Law Institute; author and editor of Global Privacy and Security Law). Prof. Dr. Paolo Balboni is also the main author of the PLA. Daniele Catteddu and Eleftherios Skoutaris greatly contributed to the document creation.

The PLA WG is composed of representatives of cloud service providers, local supervisory authorities and independent security and privacy professionals.[1]

We would also like to thank CSA staff, Hillary Baron, Daniele Catteddu, Damir Savanovic, Kendall Scoboria Cline, and Eleftherios Skoutaris for their support and contribtion.

Our sponsors Gemalto and Shellman have also greatly contributed to the publication of this document.

[1] Part 3 of this document, i.e. PLA CoC Governance, has been developed thanks to the contribution of the European Commission-funded project European Security Certification Framework (EU-SEC).

COPYRIGHT NOTICE

The Cloud Security Alliance (CSA) Code of Conduct (CoC) for European General Data Protection Regulation (GDPR) Compliance and its Annexes (e.g. Annex 1: PLA Template, Annex 2: Statement of Adherence Template (collectively, "CSA Code of Conduct for GDPR Compliance") is licensed by the Cloud Security Alliance under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License (CC-BY-NC-ND 4.0).

Sharing
You may share and redistribute the CSA Code of Conduct for GDPR Compliance in any medium or any format.

Attribution
You must give credit to the Cloud Security Alliance, and link to the CSA GDPR webpage located at https://gdpr.cloudsecurityalliance.org/. You may not suggest that the Cloud Security Alliance endorsed you or your use.

Non-Commercial
You may not use, share or redistribute the CSA Code of Conduct for GDPR Compliance for commercial gain or monetary compensation.

No Derivatives
If you remix, transform, or build upon the CSA Code of Conduct for GDPR Compliance, you may not publish, share or distribute the modified material.

No additional restrictions
You may not apply legal terms or technological measures that restrict others from doing anything that this license permits.

Commercial Licenses
If you wish to adapt, transform build upon, or distribute copies of the CSA Code of Conduct for GDPR Compliance for revenue generating purposes, you must first obtain an appropriate license from the Cloud Security Alliance. Please contact us at info@cloudsecurityalliance.org.

Notices
All trademark, copyright or other notices affixed onto the CSA Code of Conduct for GDPR Compliance must be reproduced and may not be removed.

TABLE OF CONTENTS

I. INTRODUCTION 6
II. BACKGROUND INFORMATION 7
III. STRUCTURE OF THE CSA CoC FOR GDPR COMPLIANCE 9

PART 1: CSA CoC OBJECTIVES, SCOPE, METHODOLOGY, ASSUMPTIONS & EXPLANATORY NOTES 10
1. OBJECTIVES OF THE CSA COC 11
2. SCOPE AND METHODOLOGY 11
3. ASSUMPTIONS 13
3.1 Cloud Customer Internal Due Diligence 13
3.2 Cloud Customer External Due Diligence 14
4. EXPLANATORY NOTES 14
PART 2: PRIVACY LEVEL AGREEMENT CODE OF PRACTISE 16
1. CSP DECLARATION OF COMPLIANCE AND ACCOUNTABILITY 16
2. CSP RELEVANT CONTACTS AND ITS ROLE 17
3. WAYS IN WHICH DATA WILL BE PROCESSED 18
3.1 General information 18
3.2 Personal data location 19
3.3 Subcontractors 19
3.4 Installation of software on cloud customer's system 20
3.5 Data processing contract (or other binding legal act) 20
4. RECORDKEEPING 21
4.1 Recordkeeping for CSP-controller 21
4.2 Recordkeeping for CSP-processor 22
5. DATA TRANSFER 22
6. DATA SECURITY MEASURES 23
7. MONITORING 25
8. PERSONAL DATA BREACH 25
9. DATA PORTABILITY, MIGRATION, AND TRANSFER BACK 26
10. RESTRICTION OF PROCESSING 27
11. DATA RETENTION, RESTITUTION, AND DELETION 27
11.1 Data retention, restitution, and deletion policies 27
11.2 Data retention 27
11.3 Data retention for compliance with sector-specific legal requirements 28
11.4 Data restitution and/or deletion 28
12. COOPERATION WITH THE CLOUD CUSTOMERS 28
13. LEGALLY REQUIRED DISCLOSURE 28
14. REMEDIES FOR CLOUD CUSTOMERS 29
15. CSP INSURANCE POLICY 29
PART 3: CSA CODE OF CONDUCT GOVERNANCE AND ADHERENCE MECHANISMS 30

1. TECHNICAL COMPONENTS 31
1.1 PLA Code of Practise 31
1.2 Certification scheme / adherence mechanisms to the Code 31
1.2.1 CoC Self-Attestation 32
1.2.2 CoC Third-Party Certification 33
1.3 Code of Ethics 34
1.4 PLA and OCF Working Group Charters 34
2. GOVERNANCE BODIES, ROLES AND RESPONSIBILITIES 34
2.1 PLA Working Group 34
2.2 OCF Working Group 35
2.3 Cloud Security Alliance (CSA) 35
2.4 Collaboration and supporting actions toward data protection supervisory authorities 36
3. GOVERNANCE PROCESS AND RELATED ACTIVITIES 36
3.1 PLA Code of Practise review process 36
3.2 CoC certification review process 37
3.3 CoC marks issuing, Statement of Adherence publication and complaints management 37
3.4 Code of Ethics review process 38
3.5 PLA and OCF WG charters documents review process 38
ANNEX 1: PLA [3] TEMPLATE 39
ANNEX 2: STATEMENT OF ADHERENCE TEMPLATE 45
ANNEX 3: THE CSA STAR PROGRAM AND OPEN CERTIFICATION FRAMEWORK (OCF) 51
ANNEX 4: CODE OF ETHICS 53
1. Scope 53
2. Definitions 53
3. Ethics Principles 53
4. Review and Acknowledgment of Statement of Ethics 53
5. Entry into Force and Implementation 54
6. Oversight 54
7. Review and Changes 54
ANNEX 5: PRIVACY LEVEL AGREEMENT WORKING GROUP CHARTER 55
ANNEX 6: OPEN CERTIFICATION FRAMEWORK WORKING GROUP CHARTER 63

I. INTRODUCTION

Data protection compliance is becoming increasingly risk-based.[1] 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 a 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.[2] 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 by different CSPs (and thus to support informed decisions)[3]
- 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.

The CSA CoC for GDPR compliance is based on two major components, the Privacy Level Agreement Code of Practise (PLA CoP), which is a technical standard that specifies the requirements included in the GDPR, as well as the certification scheme and 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 practises 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

---

1 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)

2 See, e.g., Articles 24, 25, 32, 35 and 39 of the GDPR.

3 "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).

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 domain 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 certification against 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).

II. 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 practises and recommendations.

PLA [V1] received the endorsement of a number of EU supervisory authorities and was used to develop further EU studies, best practises 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 struggle 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)[4] entered into force, and is directly applicable in all EU

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

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 need 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.[5]

The PLA shall be considered as a Code of Practise (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.

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 Practise [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").

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

III. STRUCTURE OF THE CSA CoC FOR GDPR COMPLIANCE

The CSA CoC for GDPR Compliance (also referred to as the "CSA Code of Conduct", the "CoC" or "the Code" in this document) is structured in three parts:

- Part 1 describes scope, objectives, scope, methodology and assumptions; and provides explanatory notes.
- Part 2 describes the PLA Code of Practise [V3] and its substantial provisions, developed by the CSA PLA Working Group.
- Part 3 outlines the governance structure and the mechanisms of adherence to the CSA Code of Conduct.

PART 1

CSA CoC OBJECTIVES, SCOPE, METHODOLOGY, ASSUMPTIONS & EXPLANATORY NOTES

1. OBJECTIVES OF THE CSA COC

1. The CSA CoC may be reference or used as an appendix to a Cloud Services Agreement and 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[6] protection practises.

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.[7]

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.

4. 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 (and thus to support informed decisions);[8] 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.

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 two types of customer situations:

- the cloud customer is the data "controller"[9] and the CSP is a data "processor"[10]
- both the cloud customer and the CSP are data controllers[11]

As originators of this document, the PLA Working Group recognizes that there may be more complex/ hybrid situations (e.g., a CSP that is a joint data controller or a situation in which both the cloud

---

6 "'[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 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.

7 "'[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.

8 "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.

9 "'[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.

10 "'[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.

11 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."

customer and the CSP are data processors) which fall outside the scope of this Code and recommends 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.[12] In complex/hybrid situations, the PLA Code of Practise (CoP) (i.e., the technical standard underlining this Code) may still serve as a useful 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.[13]

The CoC takes into consideration Article 29 Data Protection Working Party Guidelines on the Right to Data Portability[14] (A.29WP242/16-rev.01), Guidelines on Data Protection Officers[15] (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[16] (A.29WP248/17-rev.01), Guidelines on the Lead Supervisory Authority[17] (A.29WP244/16-rev.01), Guidelines on the application and setting of administrative fines[18] (A.29WP253/17), Guidelines on Personal data breach notification under Regulation 2016/679[19] (A.29WP250/17-rev.01), Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679[20] (A.29WP251/17-rev.01), Guidelines on Transparency under Regulation 2016/679[21] (A.29WP260/17-rev.01), Opinion 05/2012 on Cloud Computing[22] (A.29WP05/2012) and ENISA Technical Guidelines for the implementation of minimum security measures for Digital Service Providers[23] (ENISA Guidelines February 16, 2017). 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 practises 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

---

12 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).

13 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.

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

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

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

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

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

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

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

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

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

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

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

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]

The Code 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]

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.

3. 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?[33]

3.1 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.

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/.

[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."

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

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 practises.
4. Analysing and assessing risks (e.g., performing a Data Protection Impact Assessment to the extent required by Article 35 GDPR[34]).
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 activities of its service providers the entity should monitor and how (e.g., are onsite visits required, or is it sufficient to rely on a certification or attestation from a third party?).

3.2 Cloud Customer External Due Diligence

The cloud customer may also consider conducting a due diligence evaluation of the practises 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 CoP.
2. Determining whether the CSP holds any relevant certification or attestation based on an independent third-party assessment.[35]
3. Understanding whether and how to have visibility of, and the ability to monitor, the security controls and practises implemented by the CSP.

4. EXPLANATORY NOTES

A CSP may offer a variety of Codes depending on the type of service provided, different offerings, or different practises and markets covered.

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.[36]

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.

[34] See, for practical guidelines, A.29WP248/17-rev.01.
[35] See Articles 40 ff. GDPR.
[36] A.29WP05/2012, Section 3.4.2, p. 13.

PART 2

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.

PRIVACY LEVEL AGREEMENT CODE OF PRACTISE

1. CSP DECLARATION OF COMPLIANCE AND ACCOUNTABILITY

The CSP declares to the cloud customers:

1. to comply with the applicable EU data protection law, also in terms of technical and organisational security measures, and to safeguard the protection of the rights of the data subject; **[C & P]**
2. to be able to demonstrate compliance with the applicable EU data protection law (accountability).[37] **[C & P]**

The CSP describes 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 Section 3.3, "Subcontractors", below) or business associates. **[C & P]**

The CSP identifies:

4. the elements that can be produced as evidence to demonstrate such compliance.[38, 39] Evidence elements can take different forms, such as self-certification/attestation, third-party audits[40]

---

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

38 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.

39 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".

40 "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.

(e.g., certifications,[41] attestations,[42] 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,[43] 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.[44] **[C & P]**

2. CSP RELEVANT CONTACTS AND ITS ROLE

The CSP specifies to the cloud customers:

1. CSP identity and contact details (e.g., name, address, email address, telephone number and place of establishment); **[C & P]**
2. identity and contact details (e.g., name, address, email address, telephone number and place of establishment) of CSP local representative(s) (e.g., a local representative in the EU);[45] **[C & P]**
3. its data protection role in the relevant processing (i.e., controller, joint-controller, processor or subprocessor);[46] **[C & P]**

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

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

[43] 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 fulfillment 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.

[44] 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. According 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."

[45] 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."

[46] 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. 4 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_services.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

4. contact details of the Data Protection Officer (DPO)[47] 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]**
5. contact details of the 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]**

3. WAYS IN WHICH DATA WILL BE PROCESSED

3.1 General information

CSPs that are **controllers** provide details to cloud customers regarding the following[48]:

1. categorie 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;[49] **[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[50] (as defined in Article 4 (21) GDPR); **[C]**
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,[51] and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject; **[C]**

---

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 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.garanteprivacy.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.

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

48 See A.29WP260/17-rev.01.

49 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.

50 For the list of supervisory authorities, please see: http://ec.europa.eu/justice/data-protection/article-29/structure/data-protection-authorities/index_en.htm.

51 See Article 22 (1), (4) GDPR and A.29WP251/17-rev.01.

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;[52] **[C]**
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]**

CSPs that are **processors** 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.[53] **[P]**

The CSP specifies 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.[54] **[C & P]**

3.2 Personal data location

The CSP specifies to cloud customers:

1. the location(s) of all data centres or other data processing locations (by country) where personal data may be processed,[55] 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]**

3.3 Subcontractors

The CSP identifies:

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

---

52 See Articles 13 and 14 GDPR.

53 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."

54 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').

55 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 subjects 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?"

fulfilled.[56] **[C & P]**

The CSP declares to cloud customers that:

2. the CSP will not engage another processor without prior specific or general written authorisation of the cloud customer.[57] **[P]**

The CSP declares to cloud customers 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 Identifies:

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.[58] **[C & P]**

3.4 Installation of software on cloud customer's system

The CSP indicates to could 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.[59] **[C & P]**

3.5 Data processing contract (or other binding legal act)

The CSP shares 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 stipulates, 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

[56] See the concept of "layered services" in ICO Guidance, pp. 6-8.
[57] See Article 28.2. GDPR.
[58] 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.
[59] A.29WP05/2012, Section 3.4.1.1, p. 11.

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 instructions from the cloud customer, unless otherwise required by Union or Member State law;[60] **[P]**
4. take all measures required by applicable EU law;[61] **[P]**
5. respect the conditions for engaging another processor;[62] (see Section 3.3, "Subcontractors", above) **[P]**
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;[63] **[P]**
7. assist the cloud customer in ensuring compliance with obligations related to security of processing,[64] notification of a personal data breach to the supervisory authority;[65] communication of a personal data breach to the data subject,[66] and data protection impact assessment;[67] 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 Section 11, "Data retention, restitution, and deletion", 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]**

4. RECORDKEEPING

4.1 Recordkeeping for CSP-controller

A CSP-controller confirms to the cloud customers:

1. to maintain a record of processing activities under CSP responsibility and make it available to the supervisory authority on request. **[C]**

60 See Article 32.4. GDPR.
61 See Article 32 GDPR.
62 See Article 28.2 and 28.4.
63 See Chapter III GDPR.
64 See Article 32 GDPR.
65 See Article 33 GDPR.
66 See Article 34 GDPR.
67 See Article 35 GDPR.

The record contains 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; **[C]**
8. where possible, a general description of technical and organisational security measures.[68, 69] **[C]**

4.2 Recordkeeping for CSP-processor

A CSP-processor confirms to the cloud customers:

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 contains 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. where possible, a general description of technical and organisational security measures.[70,71] **[P]**

5. DATA TRANSFER

The CSP indicates:

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]**

---

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

[69] 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."

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

[71] 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."

If such transfer is restricted under applicable EU law, identify:

2. the legal ground for the transfer (including onward transfers through several layers of subcontractors),[72] e.g., European Commission adequacy decision, model contracts/standard data protection clauses,[73] approved codes of conduct[74] or certification mechanisms,[75] binding corporate rules (BCRs),[76] and Privacy Shield.[77] **[C & P]**

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."*[78] In completing this section, which is based on A.29WP05/2012, CSPs are invited to consider and possibly follow the ENISA Guidelines of February 16, 2017.[79] Moreover, evidence of data security compliance may also be provided to cloud customers by way of adherence to relevant codes of conduct, and certification mechanisms.[80]

Taking into account the state of the art, costs of implementation and the nature, scope, context and purposes of processing, as well and the risk of varying likelihood and severity for the rights and freedoms of natural persons, the CSP:[81]

1. specifies 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;[82] **[C & P]**

---

72 See ICO Guidance p. 18.
73 See Article 44 ff. GDPR. See A29WP05/2012, Section 3.5.3, p. 18.
74 Pursuant to Article 40 GDPR.
75 Pursuant to Article 42 GDPR.
76 See A29WP05/2012, Section 3.5.4, p. 19.
77 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).
78 See ENISA Guidelines, February 16, 2017, p. 6.
79 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).
80 See Articles 32.3, 40 and 42 GDPR.
81 See Article 32 GDPR.
82 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."

2. describes to cloud customers the concrete technical, physical, and organisational measures (protective, detective and corrective) to ensure the following safeguards:[83] **[C & P]**
    i. **availability**[84] - 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;[85] **[C & P]**
    ii. **integrity**[86] - methods by which the CSP ensures integrity[87] (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.);[88] **[C & P]**
    iii. **confidentiality**[89] - 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[90] "in transit" and "at rest",[91] authorisation mechanism and strong authentication;[92] 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., Section 7, "Monitoring", below);[93] **[C & P]**

---

83 A.29WP05/2012, Section 3.4.2, p. 13. See also ICO Guidance, pp. 13-14.

84 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?"

85 A.29WP05/2012, Section 3.4.3.1, p.14.

86 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?"

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

88 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."

89 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.

90 See Article 32.1 (a) GDPR.

91 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.

92 A.29WP05/2012, Section 3.4.3.3, p. 15.

93 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 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

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;[94] and proper management of shared resources wherever virtual machines are used to share physical resources among cloud customers);[95] **[C & P]**

vi. **intervenability** - methods by which the CSP enables data subjects' rights of access, rectification, erasure ("right to be forgotten"),[96] blocking, objection, restriction of processing[97] (see Section 10, "Restriction of processing", below), portability[98] (see Section 9, "Data portability, migration, and transfer back", below) in order to demonstrate the absence of technical and organisational obstacles to these requirements, including cases when data are further processed by subcontractors[99] (this is also relevant for Section 9, "Data portability, migration, and transfer back"); **[C & P]**

vii. **portability** - see Section 9, "Data portability, migration, and transfer back", below; **[C & P]**

viii. **accountability** - see Section 1, "CSP declaration of compliance and accountability", above. **[C & P]**

7. MONITORING

The CSP Indicates to cloud customers:

1. the options that the customer has to monitor and/or audit in order to ensure appropriate privacy and security measures described in PLA are met on an on-going basis (e.g., logging, reporting, first- and/or third-party auditing[100] of relevant processing operations performed by the CSP or subcontractors).[101] **[C & P]**

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,[102] in connection with the provision of a service provided by a CSP.[103]

---

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.

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

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

96 Article 17 GDPR.

97 Article 18 GDPR.

98 Article 20 GDPR.

99 A.29WP05/2012, Section 3.4.3.5, p. 16.

100 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

101 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.

102 Article 4.(12) GDPR.

103 See A.29WP250/17-rev.01.

The CSP specifies to the could 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 and within what timeframe.[104] **[C & P]**

In this respect, the information will at least and to the maximum extent possible:

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 propose to be taken) to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.[105] **[C & P]**

The CSP also specifies:

6. 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]**
7. 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.[106] **[C]**

9. DATA PORTABILITY, MIGRATION, AND TRANSFER BACK

The CSP specifies 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:[107] **[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).[108] **[C & P]**

[104] 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.

[105] See Article 33 GDPR.

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

[107] See Recital 68 GDPR.

[108] 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

The CSP describes 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.[109] **[C & P]**

10. RESTRICTION OF PROCESSING

The CSP explains 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 reasons of important public interest of the Union or of a Member State.[110] **[C & P]**

11. DATA RETENTION, RESTITUTION, AND DELETION

11.1 Data retention, restitution, and deletion policies

The CSP describes 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]**

11.2 Data retention

The CSP indicates:

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.[111] **[C & P]**

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.
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."

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

[110] 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 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.

[111] 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, p. 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

11.3 Data retention for compliance with sector-specific legal requirements

The CSP indicates to the cloud customers:

1. whether and how the cloud customer can request the CSP to comply with specific sector laws and regulations.[112] **[C & P]**

11.4 Data restitution and/or deletion

The CSP indicates to the cloud customers:

1. the procedure for returning to the cloud customers the personal data in a format allowing data portability (see also Section 9, "Data portability, migration, and transfer back", above); **[C & P]**
2. the methods available or used to delete data; **[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]**

12. COOPERATION WITH THE CLOUD CUSTOMERS

The CSP specifies:

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), to manage incidents including forensic analysis in case of security/data breach.[113] See also Section 6, "Data security measures: Intervenability"; and Section 8, "Personal data breach", 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 Section 1, "CSP declaration of compliance and accountability", above).[114] **[C & P]**

13. LEGALLY REQUIRED DISCLOSURE

The CSP describes to cloud customers:

1. the process in place to manage and respond to requests for disclosure of personal data by Law Enforcement Authorities, with special attention to the notification procedure to interested customers, unless otherwise prohibited, such as a prohibition under criminal law to preserve

---

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.

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

[113] 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.

[114] Articles 5.2. and 28.3 (h) GDPR.

confidentiality of a law enforcement investigation.[115] **[C & P]**

14. REMEDIES FOR CLOUD CUSTOMERS

The CSP indicates to cloud customers:

1. what remedies are available to the cloud customer in the event the CSP – and/or the CSP's subcontractors (see Section 3, "Ways in which data will be processed", above; and, more specifically, 3.3, "Subcontractors") – breach contractual obligations under PLA. Remedies could include service credits for the cloud customer and/or contractual penalties for the CSP.[116] **[C & P]**

15. CSP INSURANCE POLICY

The CSP describes to cloud customers:

1. the scope of the CSP's relevant insurance policy/ies (e.g., data protection compliance-insurance,[117] including coverage for sub-processors that fail to fulfil their data protection obligations[118] and cyber-insurance, including insurance regarding security/data breaches). **[C & P]**

[115] 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.
[116] A.29WP05/2012, Section 3.4.2 p. 12.
[117] See Articles 58, 77 ff. GDPR.
[118] See Article 28.4. GDPR.

PART 3

CSA CODE OF CONDUCT
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 accurately the "if," "when," "how" and by "whom" such changes should be applied to this CoC and related documents.

Pertaining to the governance structure of this 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 processes and relevant activities as related to the definition, revision and implementation of the Code's component.

1. TECHNICAL COMPONENTS

Components of the CoC governance structure:

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

1.1 PLA Code of Practise

The PLA Code of Practise (CoP) presented Part 2 of this document is the 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. PLA Code of Practise constitutes the fundamental technical component of this CoC.

1.2 Certification scheme / adherence mechanisms to the Code

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 certification 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 certification.

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 CoC certification 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 certification;
(b) auditing rules and mechanism;
(c) the auditor qualification process;
(d) the condition for revocation and complaint mechanism;
(e) certification fees.

The CoC certification scheme is a component of the CSA certification framework, i.e., STAR Program/ Open Certification Framework (OCF; see Annex 3 below). The scheme is based on two levels of assurance:

1. CoC self-attestation;
2. Coc third-party certification.

We report below the contribution that the CSA PLA Working Group will submit to the attention of the CSA OCF Working as input for the creation of the CoC certification scheme.

1.2.1 CoC Self-Attestation

The CoC self-attestation is voluntarily published by a CSP or cloud customer on the CSA STAR Registry (see Annex 3), indicating that the company has adopted the Code. The publication on the CSA STAR Registry entails the submission of the CoC Statement of Adherence (Annex 2) and PLA Template (Annex 1) to the Cloud Security Alliance for its upload on the STAR Registry. In the self-attestation process, the Code is not reviewed by an independent and qualified third party. 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 and 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 provide the adherent to the Code a self-attestation compliance mark.

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

The condition for revoking the mark and the mechanism of complain are described in section 3.3, "CoC marks issuing, Statement of Adherence publication and complaints management".

It shall be noted that the publication on CSA STAR Registry and issuing of the certification mark might be subject to an administrative fee.

1.2.2 CoC Third-Party Certification

The CoC third-party certification is obtained via the validation by a qualified CoC auditing partner (described in more detail below) of the adherence to the PLA CoP requirements. 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?).

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).

Once verified that all the necessary conditions are satisfied, CSA will provide the adherent to the CoC third-party certification mark.

The CoC third-party certification mark will have a validity of 12 months from the day of its issuance and it should be renewed after this period. Moreover, the CoC third-party certification mark must be revised every time there's a change in the company relevant policies or practises.

The condition for revoking the mark and the mechanism of complain are described in section 3.3, "CoC Marks issuing, Statement of Adherence publication and complaints management".

It shall be noted that the publication on CSA STAR Registry and issuing of the certification mark might be subject to an administrative fee.

1.3 Code of Ethics

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

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.

2. GOVERNANCE BODIES, ROLES AND RESPONSIBILITIES

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

2.1 PLA Working Group

The PLA Working Group (WG) is responsible for defining, approving and updating changes to the technical standard/code of practise i.e., the PLA Code of Practise (currently in its third version, i.e., PLA [V3]). This body also provides expert opinion to CSA when complaints about CoC Self-Attestation or Certification 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.

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 (e.g., the CoC certification 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.

2.3 Cloud Security Alliance (CSA)

CSA supports and oversees implementation of the CoC certification 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 certificates. 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 certificate, (vi) name of auditing organisation/auditor;
- 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 certification scheme;
- reviewing CoC self-attestations and verifying minimum requirements are met;
- maintaining a mechanism for filing complaints;
- verifying complaints and taking appropriate actions (e.g., removing a CoC entry and certificate from the Registry; removing a qualified CoC auditing partner from the Registry, etc.);
- providing guidance on handling conflicts;
- creating an advisory body (i.e., composed of organisations, such as the European Privacy Association, or EPA) to support CSA in its implementation and oversight of the scheme (e.g., performing periodic audits of the requirements of CoC audits; performing periodic checks of audit results; managing complaints);
- assuring transparency and integrity throughout the development of standards, certification implementation and management;

- approving the OCF charter revision and extension;
- approving the PLA charter revision and extensions;
- setting and reviewing certification 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.

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, the Article 29 Data Protection Working Party (A.29WP), 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, A.29 WP, or the European Data Protection Board, the CoC governance bodies also may do the following:

- promote awareness between the CoC self-attested and certified companies about measures issued by national DPAs (general provisions, as well as specific provisions - when issued towards a CoC self-attested or certified company);
- if a national DPA carries out an inspection of a CoC-certified company, provide DPA with all information and evidence available in CSA about the CoC-certified company. In these cases, CoC governance bodies will act as the CSA point of reference.
- review and, if necessary, withdraw the CoC certification of a company subject to penalties issued by a national DPA.

3. GOVERNANCE PROCESS 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.

3.1 PLA Code of Practise 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 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.

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.

3.2 CoC certification 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 CoC marks issuing, Statement of Adherence publication and complaints management

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:

(i) CoC self-attestation
CSA is responsible for reviewing any CoC self-attestation and relevant complaints submitted by any third party. 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 CoC self-attestation, or b) remove the self-attestation from the CSA Registry and revoke the mark.

(ii) CoC certification
CSA is responsible for publishing the CoC certification in 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 CoC auditor that issued a certification if a related complaint is filed. In that case, the qualified CoC 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 mark.

3.4 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.

3.5 PLA and OCF WG charters documents review process

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

ANNEX 1: PLA [3] TEMPLATE

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 to comply with the applicable EU data protection law, also in terms of technical and organisational security measures, and to ensure the protection of the rights of the data subject;*	Applicable	Applicable
			DCA-1.2	*2. Declare to be able to demonstrate compliance with the applicable EU data protection law (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 Section 3.3 – 'Subcontractors', below) or business associates.*	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 identity and contact details (e.g., name, address, email address, telephone number and place of establishment);*	Applicable	Applicable
			CAR-1.2	*2. Specify identity and contact details (e.g., name, address, email address, telephone number and place of establishment) of CSP local representative(s) (e.g. a local representative in the EU);*	Applicable	Applicable
			CAR-1.3	*3. Specify its data protection role in the relevant processing (i.e., controller, joint-controller, processor or subprocessor);*	Applicable	Applicable
			CAR-1.4	*4. Specify contact details of the 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 contact details of the 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** 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-1.10	*10. the existence of automated decision-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	Not 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** 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).*		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
		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 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 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. 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.*	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 other binding legal act)	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 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.*	Not Applicable	Applicable
			WWP-5.2	*The contract or other legal act stipulates, 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. take all measures required by applicable EU law;*	Not Applicable	Applicable
			WWP-5.5	*5. Respect the conditions for engaging another processor; (see Section 3.3 'Subcontractors', 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 Union or Member State law requires storage of the personal data; (see Section 11 'Data retention, restitution, and deletion', below).*	Not Applicable	Applicable
			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. RECORDKEEPING.	**REC**	**1.Recordkeeping for CSP-controller**	**REC-1.1**	*1. CSP controller confirms to cloud customers: 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;*	Applicable	Not Applicable
			REC-1.8	*8. where possible, a general description of technical and organisational security measures.*	Applicable	Not Applicable
		2 Recordkeeping for CSP-processor	**REC-2.1**	*1. CSP processor confirms to cloud customers that he/she maintains 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
			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. where possible, a general description of technical and organisational security measures.*	Not Applicable	Applicable
5. DATA TRANSFER.	**DTR**	**1. Data transfer**	**DTR-1-1**	*1. 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. identifythe 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) 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
			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., Section 7 'Monitoring', 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 Section 10, 'Restriction of processing', below), portability (see to Section 9, 'Data portability, migration, and transfer back' 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 Section 9, 'Data portability, migration, and transfer back' below;*	Applicable	Applicable
			SEC-1.2.viii	*(viii) accountability: refer to Section 1, 'CSP declaration of compliance and accountability', above.*	Applicable	Applicable
7. MONITORING.	**MON**	**1. Monitoring**	**MON-1.1**	*1. Indicate to cloud customers the options that the customer has to monitor and/or audit in order to ensure appropriate privacy and security measures described in PLA [V3] 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).*	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 and within what timeframe.*	Applicable	Applicable
			PDB-1.2	*2. describe 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. 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);*	Applicable	Applicable
			PDB-1.4	*4. describe the likely consequences of the personal data breach;*	Applicable	Applicable
			PDB-1.5	*5. describe 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. 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-1.7	*7. 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. 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:*	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.*	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 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.*	Applicable	Applicable
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**	*3. Indicate 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
		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 Section 9 'Data portability, migration, and transfer back', 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
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 Section 6, 'Data security measures': Intervenability; and Section 8: 'Personal data breach', 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 Section 1, 'CSP declaration of compliance and accountability', above).*	Applicable	Applicable
13. LEGALLY REQUIRED DISCLOSURE.	**LRD**	**1. Legally required disclousure**	**LRD-1.1**	*1. Describe the process in place to manage and respond to requests for disclosure of personal data by Law Enforcement Authorities, 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 are available to the cloud customer in the event the CSP – and/or the CSP's subcontractors (see Section 3 'Ways in which data will be processed', above; and, more specifically, 3.3 'Subcontractors') – breach contractual obligations under PLA [V3]. 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

ANNEX 2: STATEMENT OF ADHERENCE TEMPLATE

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

Self-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. Issue/Expiry date

Issue Date	
Expiry Date	

7. 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 Certification

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 Certification	

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. Certification Body

Name	

7. Country of issuing

Name	

8. Certificate number

Name	

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

Name	
Title	
Date	

ANNEX 3: 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.

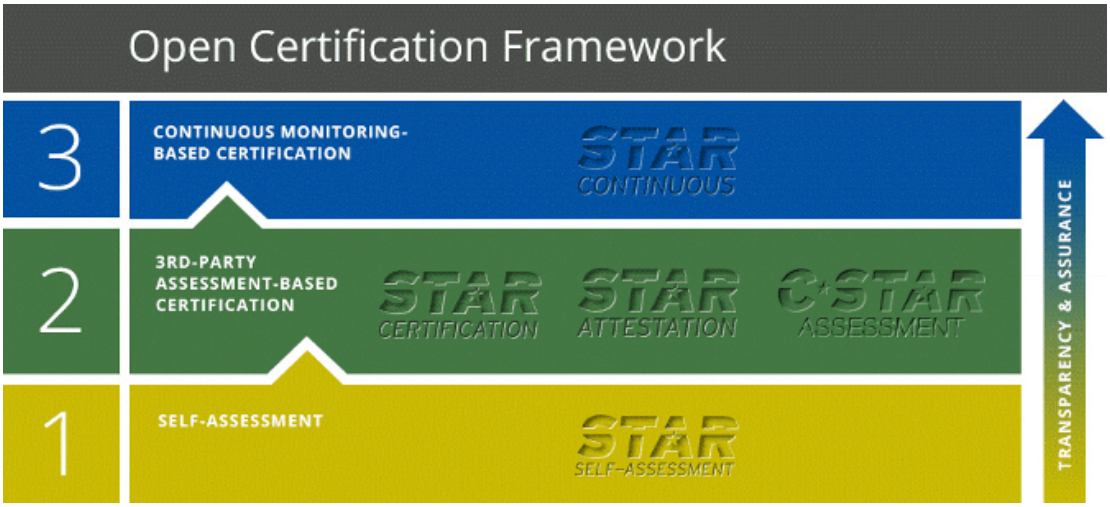
The CSA STAR provides cloud stakeholders, e.g., Cloud Service Customers (CSC), Cloud Service Providers (CSPs), Cloud Auditors, and others with a public repository in which CSPs can publish information related to their internal due diligence results based on CSA best practises: the Cloud Control Matrix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



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

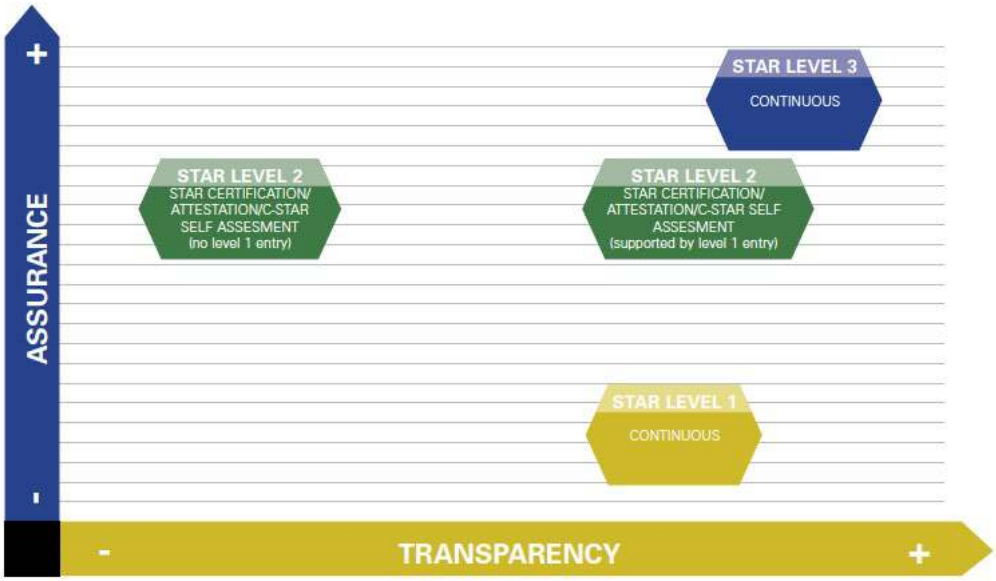
Currently the STAR Program offers the Self-Assessment (Level 1) and Third-Party Assessment-based Certification/Attestation (Level 2).

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.



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.

ANNEX 4: 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.

ANNEX 5: PRIVACY LEVEL AGREEMENT WORKING GROUP CHARTER

Privacy Level Agreement Working Group

Charter 2017

EXECUTIVE OVERVIEW

Data protection compliance is becoming increasingly risk-based.[1] 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.[2] 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)[3]
- 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:

- 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;

[1] 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)

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

[3] "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).

- 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.[4]

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).

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.

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

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 Certification are submitted.

Objective 6: Provide expert opinion to CSA Open Certification Working Group on the PLA CoC third party certification 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 Users/Consumers	Representatives from corporate cloud provider and/or representatives of users/consumers organization to ensure alignment with user requirements and needs	· EuroCio · 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.

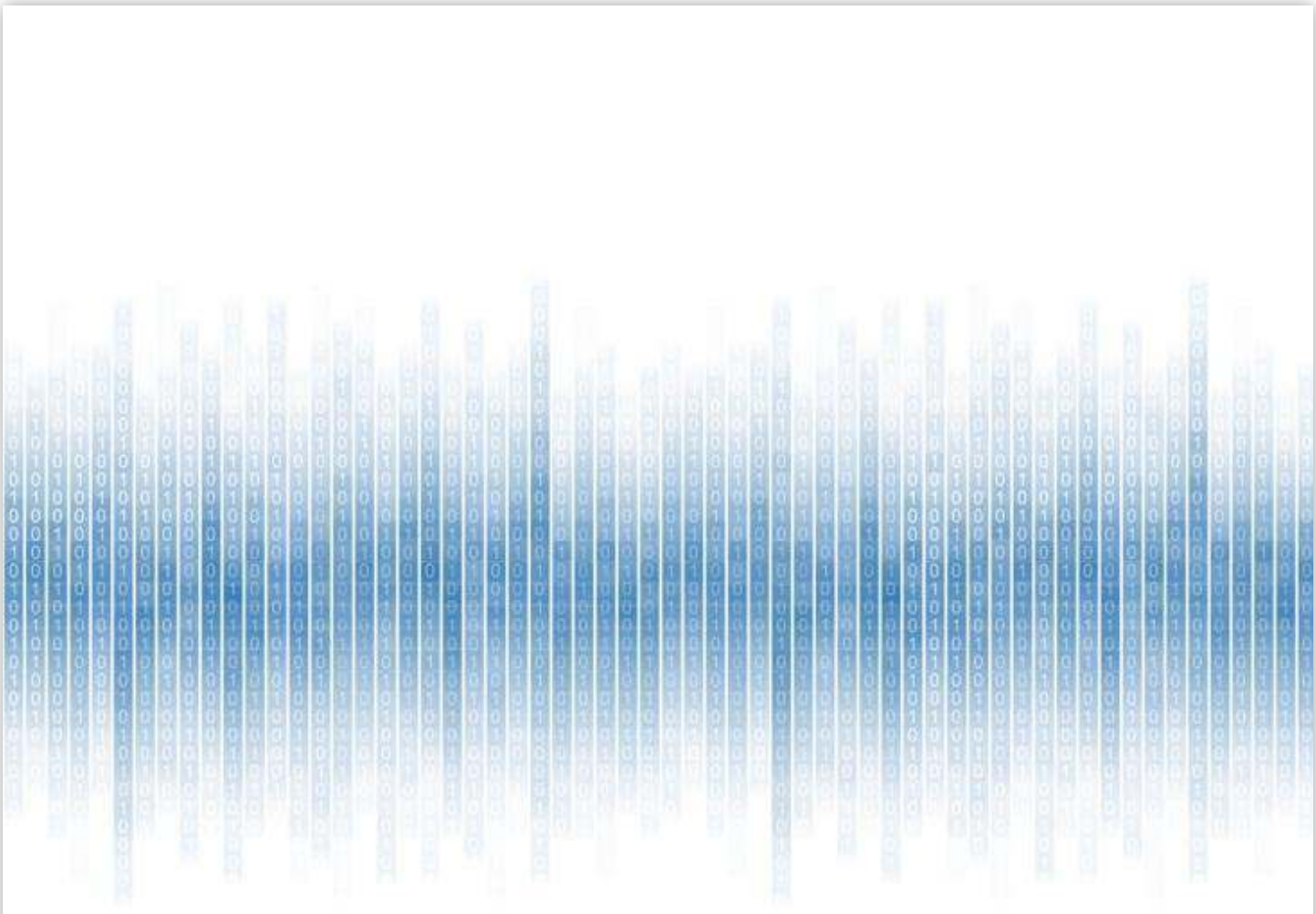
DELIVERABLES

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

ANNEX 6: OPEN CERTIFICATION FRAMEWORK WORKING GROUP CHARTER



Open Certification Framework Working Group

Charter

2017

TABLE OF CONTENTS

- WORKING GROUP EXECUTIVE OVERVIEW
  - Working Group Scope and Responsibilities
  - Relationship to Cloud
- Working Group Membership
  - Working Group Structure
    - Co-Chairs
    - Committees
    - Sub-Work Groups
- Alignments with Outside Groups
- Operations
  - Advisory
  - Research Lifecycle
  - Peer Review
- Communications Methods
  - Infrastructure & Resource Requirements
  - Work Group Conference Calls and In-person Meetings
- Decision-making Procedures
- IPR Policy
- Deliverables/Activities
- Duration
- Charter Revision History

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, Internt2/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 certify organization 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 Certification 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