EUSEC
EU SECURITY CERTIFICATION

EUROPEAN SECURITY CERTIFICATION FRAMEWORK

D2.3 PRIVACY CODE OF CONDUCT DRAFT

VERSION

PROJECT NUMBER: 731845

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

PROJECT TITLE: EU-SEC

AUTHOR:
ELEFTHERIOS SKOUTARIS, CSA
DAMIR SAVANOVIC, CSA
DANIELE CATTEDDU, CSA

PARTNERS CONTRIBUTED:
PWC GERMANY

EXECUTIVE SUMMARY

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

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

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

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

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

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

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

DISCLAIMER

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

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

ABBREVIATIONS

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

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

TABLE OF CONTENTS

1 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 for the personal data they process. In such decision, they have to take into account factors such as the state of the art of technology; costs of implementation; the nature, scope, context and purposes of processing; as well as the risks of varying likelihood and severity to 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 Privacy Level Agreement Code of Practice is of fundamental importance, as it 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.

[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 customer with all the information necessary to rightly assess the pros and cons of adopting such services. Security, transparency, and legal certainty for the customers 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).

In May 2016, the regulation (EU) 2016/679 (GDPR)[4] entered into force, which will be directly applicable in all EU Member States from 25 May 2018. With the introduction of GDPR, it was immediately evident that CSPs, cloud customers and potential customers would need guidance in order to comply with the new law in the cloud environment.

In this context, the EU-SEC project focuses on addressing issues related to security and privacy governance, risk management and compliance in the cloud. The objective is to improve the effectiveness and efficiency of existing security certification processes by bridging the requirement gaps between them and minimizing the lack of transparency toward cloud services customers. Furthermore, it aims at providing support to the European industry through the development and introduction of a governance structure and compliance framework that enhances its trans-European adoption and extensibility to privacy requirements, deployment of underlying tools, architectures and governing bodies.

More specifically, the current work aims at addressing the evolving landscape of privacy and data protection requirements EU-wide, and guaranteeing compliance by defining the governance of the Privacy Code of Conduct (CoC) based on Cloud Security Alliance’s Privacy Level Agreement (PLA) Code of Practice (CoP), version 3.

The PLA CoC constitutes an extension of the framework in order to ensure compliance with the relevant data protection requirements. It is of fundamental importance as it provides the necessary transparency on the level of data protection offered by the Cloud Service Provider, as presented in “Privacy Level Agreement [V3] Code of Conduct - A Compliance Tool for Providing Cloud Services in the European Union”).

1.1 SCOPE AND METHODOLOGY

The PLA CoC 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) and addresses two types of customer situations:

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

- the cloud customer is the data 'controller'[5] and the CSP is a data 'processor'[6]
- both the cloud customer and the CSP are data controllers[7]

It should be noted that there may be more complex/hybrid situations (e.g., a CSP that is a joint data controller), which fall outside the scope of the PLA. Therefore, it is recommended to the users of PLA that they carefully evaluate the respective privacy roles of the parties involved on a case-by-case basis to clearly identify related obligations.[8] In complex/hybrid situations, PLA 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 table in Appendix A.[9]

PLA takes into consideration Article 29 Data Protection Working Party Guidelines on the Right to Data Portability[10] (A.29WP242/16), Guidelines on Data Protection Officers[11] (A.29WP243/16), Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a

[5] "'[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.

[6] "'[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.

[7] 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."

[8] 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).

[9] 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."

[10] http://ec.europa.eu/newsroom/document.cfm?doc_id=44099 .

[11] http://ec.europa.eu/newsroom/document.cfm?doc_id=44100.

high risk" for the purposes of Regulation 2016/679[12] (A.29WP248/17), Opinion 05/2012 on Cloud Computing[13] (A.29WP05/2012) and ENISA Technical Guidelines for the implementation of minimum security measures for Digital Service Providers[14] (ENISA Guidelines February 16, 2017). Therefore, PLA is not only based on the mandatory legal provisions of the applicable EU personal data protection framework, but also reflects the relevant interpretation by the European supervisory authorities and related best practices developed by relevant Agencies. PLA aims to be a "horizontal" tool that can be used to assess and achieve compliance with the EU personal data protection legislation horizontally across different sectors and domains. It is based on awareness of the existing EU personal data protection provisions applicable to specific services (e.g., Directive on privacy and electronic communications,[15] and the network and information systems Directive[16]). Users of the PLA are recommended to identify possible sector-specific additional requirements.

The PLA is also written taking into account ISO/IEC 27018,[17] the "Cloud Service Level Agreement Standardisation Guidelines,"[18] the works developed by the Cloud Select Industry Group on Code of Conduct[19], by the Cloud Infrastructure Service Providers in Europe (CISPE),[20] and the Cloud

[12] http://ec.europa.eu/newsroom/document.cfm?doc_id=44137.

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

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

[15] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, as subsequently amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws. See also the Proposal for a Regulation on Privacy and Electronic Communications, https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications.

[16] 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.

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

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

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

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

Accountability Project.[21] It reflects the GDPR requirements that are relevant to the cloud domain and, following the "territorial scope" of the GDPR, extends beyond the EU.[22]

The target audience for the PLA CoC and CoP 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.

1.2 OBJECTIVES

(i) A Privacy Level Agreement (PLA) is intended to be used as an appendix to a Cloud Services Agreement and to describe the level of privacy protection that the Cloud Service Provider (CSP) will provide. While Service Level Agreements (SLAs) are generally used to provide metrics and other information on the performance of the services, PLAs will address information privacy and personal data[23] protection practices.

(ii) In a PLA, the CSP would clearly describe the level of privacy and data protection that it undertakes to maintain with respect to relevant data processing.[24]

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

(iv) Ultimately, PLAs are intended to provide the following:

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

[22] 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."

[23] "'[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.

[24] "'[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.

- 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);[25] 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.

1.3 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?[26]

[25] "All cloud providers offering services in the EEA should provide the cloud customer with all the information necessary to rightly assess the pros and cons of adopting such services. Security, transparency, and legal certainty for the customers 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.

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

1.3.1 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:

(i) Defining its security, data protection and compliance requirements.

(ii) Identifying what data/processes/services it will want to move to the cloud.

(iii) Reviewing its own internal security and privacy/data protection policies and other restrictions on its use of personal data, such as pre-existing contracts, applicable laws and regulations, guidelines and best practices.

(iv) Analysing and assessing risks (e.g., performing a Data Protection Impact Assessment to the extent required by Article 35 GDPR[27]).

(v) 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.

(vi) 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).

(vii) Determining which CSP activities the entity should monitor (e.g., are onsite visits required, or is it sufficient to rely on a certification or attestation from a third party?).

1.3.2 CLOUD CUSTOMER EXTERNAL DUE DILIGENCE

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

(i) 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.

(ii) Determining whether the CSP holds any relevant certification or attestation based on an independent third-party assessment.[28]

(iii) Understanding whether and how to have visibility of, and the ability to monitor, the security controls and practices implemented by the CSP.

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

[28] See Articles 40 ff. GDPR.

1.4 EXPLANATORY NOTES

A CSP may offer a variety of PLAs depending on the type of service provided, different offerings, or different practices and markets covered. Moreover, a PLA 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.[29]

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 customer and CSPs (as opposed to disorient customers). Clarity and transparency are critical.

1.5 STRUCTURE OF THE DOCUMENT

The rest of this document is organized as follows:

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

2 PLA PRIVACY REQUIREMENTS

This section constitutes a collection of data protection requirements formalized as follows:

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

- Section 2 of this document shall be used in conjunction with Appendix A: PLA Table
- *Next to each requirement it is specified:*
    - *[C & P] if the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;*
    - *[C] if the requirement is applicable only to the situation in which the CSP is a controller;*
    - *[P] if the requirement is applicable only to the situation in which the CSP is a processor.*

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

2.1 CSP DECLARATION OF COMPLIANCE AND ACCOUNTABILITY

The CSP declares to the cloud customers:

A. 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; **[C & P]**
B. to be able to demonstrate compliance with the applicable EU data protection law (accountability).[30] **[C & P]**

The CSP describes to the cloud customers:

C. what policies and procedures the CSP has in place to ensure and demonstrate compliance by the CSP itself and its subcontractors (see also Section 2.3.3 – 'Subcontractors', below) or business associates. **[C & P]**

The CSP identifies:

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

D. the elements that can be produced as evidence to demonstrate such compliance.[31, 32] Evidence elements can take different forms, such as self-certification/attestation, third-party audits[33] (e.g. certifications,[34] attestations,[35] 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,[36] 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.[37] **[C & P]**

[31] 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, http://www.edps.europa.eu/EDPSWEB/edps/site/mySite/pid/71#accountability.

[32] 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".

[33] "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.

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

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

[36] 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.

[37] 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."

2.2 CSP RELEVANT CONTACTS AND ITS ROLE

The CSP specifies to the cloud customers:

A. CSP identity and contact details (e.g., name, address, email address, telephone number and place of establishment); **[C & P]**
B. 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);[38] **[C & P]**
C. its data protection role in the relevant processing (i.e., controller, joint-controller, processor or subprocessor);[39] **[C & P]**

[38] 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."

[39] 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 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.

D. contact details of the Data Protection Officer (DPO)[40] 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]**
E. 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]**

2.3 WAYS IN WHICH DATA WILL BE PROCESSED

2.3.1 GENERAL INFORMATION

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

A. categories of personal data concerned in the processing; **[C]**
B. purposes of the processing for which data are intended and the necessary legal basis to carry out such processing in a lawful way;[41] **[C]**
C. recipients or categories of recipients of the data; **[C]**
D. 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]**
E. 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]**
F. the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period; **[C]**
G. 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]**
H. the right to lodge a complaint with a supervisory authority[42] (as defined in Article 4 (21) GDPR); **[C]**

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

[41] 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.

[42] For the list of supervisory authorities, please see: http://ec.europa.eu/justice/data-protection/article-29/structure/data-

I. 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]**

J. the existence of automated decision-making, including profiling,[43] and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject; **[C]**

K. 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]**

L. 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;[44] **[C]**

M. 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:

N. the extent and modalities in which the customer-data controller can issue its binding instructions to the CSP-data processor.[45] **[P]**

The CSP specifies to cloud customers:

protection-authorities/index_en.htm.

[43] See Article 22 (1) and (4) GDPR.

[44] See Articles 13 and 14 GDPR.

[45] 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."

O. how the cloud customers will be informed about relevant changes concerning relevant cloud service(s), such as the implementation or removal of functions.[46] **[C & P]**

2.3.2 PERSONAL DATA LOCATION

The CSP specifies to cloud customers:

A. the location(s) of all data centres or other data processing locations (by country) where personal data may be processed,[47] 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]**

2.3.3 SUBCONTRACTORS

The CSP identifies:

A. 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.[48] **[C & P]**

The CSP declares to cloud customers that:

B. the CSP will not engage another processor without prior specific or general written authorisation of the cloud customer.[49] **[P]**

[46] 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').

[47] 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?"

[48] See the concept of "layered services" in ICO Guidance, pp. 6-8.

[49] See Article 28.2. GDPR.

The CSP declares to cloud customers that the CSP:

C. 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]**
D. 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:

E. 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.[50] **[C & P]**

2.3.4 INSTALLATION OF SOFTWARE ON CLOUD CUSTOMER'S SYSTEM

The CSP indicates to could customers:

A. whether the provision of the service requires the installation of software on the cloud customer's system (e.g., browser plug-ins) **[C & P]**
B. the software's implications from a data protection and data security point of view.[51] **[C & P]**

2.3.5 DATA PROCESSING CONTRACT (OR OTHER BINDING LEGAL ACT)

The CSP shares with the cloud customers:

A. 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

[50] 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.
[51] A.29WP05/2012, Section 3.4.1.1, p. 11.

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:

B. process personal data only upon documented instructions from the cloud customer, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the CSP is subject; in such a case, the CSP will inform the cloud customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest; **[P]**
C. 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;[52] **[P]**
D. take all measures required by applicable EU law;[53] **[P]**
E. respect the conditions for engaging another processor;[54] (see Section 2.3.3 'Subcontractors', above) **[P]**
F. 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;[55] **[P]**
G. assist the cloud customer in ensuring compliance with obligations related to security of processing,[56] notification of a personal data breach to the supervisory authority;[57] communication of a personal data breach to the data subject,[58] and data protection impact assessment;[59] taking into account the nature of processing and the information available to the processor; **[P]**
H. 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

[52] See Article 32.4. GDPR.
[53] See Article 32 GDPR.
[54] See Article 28.2 and 28.4.
[55] See Chapter III GDPR.
[56] See Article 32 GDPR.
[57] See Article 33 GDPR.
[58] See Article 34 GDPR.
[59] See Article 35 GDPR.

Union or Member State law requires storage of the personal data; (see Section 2.11 'Data retention, restitution, and deletion', below) **[P]**

I. 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]**

2.4 RECORDKEEPING

2.4.1 RECORDKEEPING FOR CSP-CONTROLLER

A CSP-controller confirms to the cloud customers:

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

The record contains the following information:

B. name and contact details of controller and, where applicable, the joint controller, the controller's representative and the data protection officer; **[C]**
C. the purposes of the processing; **[C]**
D. a description of the categories of data subjects and of the categories of personal data; **[C]**
E. categories of recipients to whom the personal data have been or will be disclosed, including recipients in third countries or international organisations; **[C]**
F. 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]**
G. where possible, the envisaged time limits for erasure of different categories of data; **[C]**
H. where possible, a general description of technical and organisational security measures.[60, 61] **[C]**

[60] See Section 2.6 'Data security measures', below; and Article 35 GDPR.

[61] 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."

2.4.2 RECORDKEEPING FOR CSP-PROCESSOR

A CSP-processor confirms to the cloud customers:

A. 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:

B. 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]**
C. categories of processing carried out on behalf of each controller; **[P]**
D. 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]**
E. where possible, a general description of technical and organisational security measures.[62,63] **[P]**

2.5 DATA TRANSFER

The CSP indicates:

A. 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]**

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

B. the legal ground for the transfer (including onward transfers through several layers of subcontractors),[64] e.g., European Commission adequacy decision, model

[62] See Section 2.6 'Data security measures', below; and Article 35 GDPR.
[63] 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."
[64] See ICO Guidance p. 18.

contracts/standard data protection clauses,[65] approved codes of conduct[66] or certification mechanisms,[67] binding corporate rules (BCRs),[68] and Privacy Shield.[69] **[C & P]**

2.6 DATA SECURITY MEASURES

Preliminarily, the CSP should note that: "... [C]loud computing services are considered as Digital Service Providers (DSPs) in the context of the recently adopted Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union."[70] 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.[71] 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.[72]

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:[73]

A. specifies to cloud customers the technical, physical and organisational measures that are in place to protect personal data against accidental or unlawful destruction; or

[65] See Article 44 ff. GDPR. See A29WP05/2012, Section 3.5.3, p. 18.

[66] Pursuant to Article 40 GDPR.

[67] Pursuant to Article 42 GDPR.

[68] See A29WP05/2012, Section 3.5.4, p. 19.

[69] 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).

[70] See ENISA Guidelines, February 16, 2017, p. 6.

[71] See also National Cyber Security Centre: Guidance Implementing the Cloud Security Principles (https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles).

[72] See Articles 32.3, 40 and 42 GDPR.

[73] See Article 32 GDPR.

accidental loss, alteration, unauthorized use, unauthorised modification, disclosure or access; and against all other unlawful forms of processing;[74] **[C & P]**

B. describes to cloud customers the concrete technical, physical, and organisational measures (protective, detective and corrective) to ensure the following safeguards:[75] **[C & P]**

(i) availability[76] - 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;[77] **[C & P]**

(ii) integrity:[78] - methods by which the CSP ensures integrity[79](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.);[80] **[C & P]**

(iii) confidentiality[81] - methods by which the CSP ensures confidentiality from a technical point of view in order to assure that only authorised persons have access

[74] 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."

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

[76] 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?"

[77] A.29WP05/2012, Section 3.4.3.1, p.14.

[78] 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?"

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

[80] 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."

[81] 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 practice 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

to data; including, inter alia as appropriate, pseudonymisation and encryption of personal data[82] 'in transit' and 'at rest,'[83] authorisation mechanism and strong authentication;[84] 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 2.7 'Monitoring', below);[85] **[C & P]**

(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;[86] and proper management of shared resources wherever virtual machines are used to share physical resources among cloud customers);[87] **[C & P]**

(vi) intervenability - methods by which the CSP enables data subjects' rights of access, rectification, erasure ('right to be forgotten'),[88] blocking, objection, restriction of

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.

[82] See Article 32.1 (a) GDPR.

[83] 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.

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

[85] 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 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 practice 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.

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

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

[88] Article 17 GDPR.

processing[89] (see Section 2.10, 'Restriction of processing', below), portability[90] (see to Section 2.9, '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[91] (this is also relevant for Section 2.9, 'Data portability, migration, and transfer back'); **[C & P]**

(vii) portability - refer to Section 2.9, 'Data portability, migration, and transfer back' below; **[C & P]**

(viii) accountability: refer to Section 2.1, 'CSP declaration of compliance and accountability', above. **[C & P]**

2.7 MONITORING

The CSP Indicates to cloud customers:

A. 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[92] of relevant processing operations performed by the CSP or subcontractors).[93] **[C & P]**

2.8 PERSONAL DATA BREACH

"Personal data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted,

[89] Article 18 GDPR.

[90] Article 20 GDPR.

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

[92] 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

[93] 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.

stored or otherwise processed,[94] in connection with the provision of a service provided by a CSP.

The CSP specifies to the could customers:

A. 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.[95] **[C & P]**

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

B. describe the nature of the personal data breach including, where possible, the categories and approximate number of personal data records concerned; **[C & P]**
C. communicate the name and contact details of the data protection officer or other contact point where more information can be obtained (see Section 2.2 'CSP relevant contacts and its role', above); **[C & P]**
D. describe the likely consequences of the personal data breach; **[C & P]**
E. 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.[96] **[C & P]**

The CSP also specifies:

F. 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]**
G. 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.[97] **[C]**

[94] Article 4.(12) GDPR.
[95] 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.
[96] See Article 33 GDPR.
[97] See Article 33 GDPR. See also Article 34 GDPR.

2.9 DATA PORTABILITY, MIGRATION, AND TRANSFER BACK

The CSP specifies to cloud customers:

A. 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:[98] **[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).[99] **[C & P]**

[98] See Recital 68 GDPR.

[99] 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 for practical guidelines, best practices and tools that support compliance with the right to data portability. The right to data portability is a new right introduced by the GDPR. However, even before the GDPR will be directly applicable in the EU Member States (25 May 2018), there seems to be enough ground for considering data portability as a mandatory requirement pursuant to general EU personal data protection principles, such as "data accuracy" (Article 6.1.d of Directive 95/46/EC), "data availability" and possibility to grant data subjects' rights per Sections 11.1.c and 12 of Directive 95/46/EC. See also A29WP05/2012, Section 3.4.3.6, p.16 and ICO Guidance, p. 22: "Make sure that the cloud provider allows you to get a copy of your data, at your request, in a usable format. Moreover, see Section 5.4 of the Data Portability of the Cloud Service Level Agreement Standardisation Guidelines: "5.4. Data Portability

Description of the context or of the requirement

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

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

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

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.

The CSP describes to cloud customers:

B. 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.[100] **[C & P]**

2.10 RESTRICTION OF PROCESSING

The CSP explains to cloud customers:

A. 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.[101] **[C & P]**

2.11 DATA RETENTION, RESTITUTION, AND DELETION

2.11.1 DATA RETENTION, RESTITUTION, AND DELETION POLICIES

The CSP describes to the cloud customers:

A. the CSP's data retention policies, timelines and conditions for returning personal data or deleting data once the service is terminated, **[C & P]**
B. as well as these policies, timelines and conditions for their subcontractors. **[C & P]**

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."

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

[101] 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.

2.11.2 DATA RETENTION POLICY

The CSP Indicates:

A. 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.[102] **[C & P]**

2.11.3 DATA RETENTION FOR COMPLIANCE WITH SECTOR-SPECIFIC LEGAL REQUIREMENTS

The CSP Indicates to the cloud customers:

A. whether and how the cloud customer can request the CSP to comply with specific sector laws and regulations.[103] **[C & P]**

2.11.4 DATA RESTITUTION AND/OR DELETION

The CSP indicates to the cloud customers:

A. the procedure for returning to the cloud customers the personal data in a format allowing data portability (see also Section 2.9 'Data portability, migration, and transfer back', above); **[C & P]**
B. the methods available or used to delete data; **[C & P]**
C. 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]**
D. the specific reason for retaining the data; **[C & P]**
E. the period during which the CSP will retain the data. **[C & P]**

[102] 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 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.

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

2.12 COOPERATION WITH THE CLOUD CUSTOMER(S)

The CSP specifies:

A. 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.[104] See also Section 2.6, 'Data security measures': Intervenability; and Section 2.8: 'Personal data breach', above]. **[C & P]**

The CSP undertakes towards cloud customers:

B. to make available to the cloud customer and the competent supervisory authorities the information necessary to demonstrate compliance (see also Section 2.1, 'CSP declaration of compliance and accountability', above).[105] **[C & P]**

2.13 LEGALLY REQUIRED DISCLOSURE

The CSP describes to cloud customers:

A. 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.[106] **[C & P]**

[104] 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.

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

[106] 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.

2.14 REMEDIES FOR CLOUD CUSTOMER(S)

The CSP indicates to cloud customers:

A. what remedies are available to the cloud customer in the event the CSP – and/or the CSP's subcontractors (see Section 2.3 'Ways in which data will be processed', above; and, more specifically, 2.3.3 'Subcontractors') – breach contractual obligations under PLA. Remedies could include service credits for the cloud customer and/or contractual penalties for the CSP.[107] **[C & P]**

2.15 CSP INSURANCE POLICY

The CSP describes to cloud customers:

A. the scope of the CSP's relevant insurance policy/ies (e.g., data protection compliance-insurance,[108] including coverage for sub-processors that fail to fulfil their data protection obligations[109] and cyber-insurance, including insurance regarding security/data breaches). **[C & P]**

[107] A.29WP05/2012, Section 3.4.2 p. 12.

[108] See Articles 58, 77 ff. GDPR.

[109] See Article 28.4. GDPR.

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

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

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

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

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

3.1 TECHNICAL COMPONENTS

Components of the PLA CoC governance structure include:

1. PLA Code of Practice
2. PLA certification scheme and mechanism of adherence;
3. Code of Ethics;
4. PLA and OCF Working Group charters documentation.

3.1.1 PLA CODE OF PRACTICE

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

3.1.2 PLA CERTIFICATION SCHEME / ADHERENCE MECHANISMS

CSPs and Cloud Customers that are willing to adhere to the requirements of the CSA PLA Code of Practice (CoP) shall submit a Statement of Adherence (See Appendix A) to the Cloud Security Alliance in accordance to the principles, policies and guidelines established in this document and in subsequent updates of the PLA Certification scheme developed by the CSA Open Certification Framework 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 CoC Adherence Template (see Appendix A) either in the form of a PLA Self Attestation or in the form of PLA Third Party Certification.

The PLA CoC 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.

PLA CoC Certification scheme defines the objective, policy, mechanisms, scope, rules, requirements and processes for adhering to PLA CoC, and includes the following:

(i) scope and objective of certification;
(ii) auditing rules and mechanism;
(iii) the auditor qualification process;
(iv) the condition for revocation and complaint mechanism;
(v) certification fees.

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

(i) PLA CoC Self Attestation;

(ii) PLA 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 PLA CoC Certification scheme.

(i) PLA CoC Self Attestation

PLA Self Attestation is the voluntary publication by a CSP or Cloud Customer on the CSA STAR Registry (see Appendix B), indicating that the company has adopted PLA.

The publication on the CSA STAR Registry entails the submission of the PLA Statement of Adherence and Template (Appendix A) to the Cloud Security Alliance for its upload on the STAR Registry.

In the Self Attestation process, PLA is not reviewed by an independent and qualified third party.

The PLA Adherence Template is submitted to CSA to verify that the PLA has been completed in all its sections and to make sure that a “good faith” effort to completely address PLA requirements was made. CSA will also verify the submitter has provided a public notice of compliance to PLA on its website.

Once verified that all the necessary conditions are satisfied, CSA will provide the adherent to the PLA CoC a Self-Attestation Compliance Mark.

The PLA 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 PLA CoC Self Attestation must be revised every time there’s a change in the company relevant policies or practices.

The condition for revoking the Mark and the mechanism of complain are described in paragraph “3.3 PLA CoC Marks issuing, Statement of Adherence publication and complaints management”.

(ii) PLA CoC Third Party Certification

The PLA Third Party Certification is obtained via the validation by a Qualified PLA 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 PLA (e.g., did the Data Controller/Data Processor complete all Sections in PLA? Does the content included in every Section provide the necessary information on data handling and processing?);
- the accuracy of information included in PLA (e.g., is the information included in the PLA truthful? Are statements supported by evidence?).

As mentioned above the validation must be performed by a Qualified PLA Auditing Partners, which is an organisation that meets the following requirements:

- the organisation is a CSA Corporate Member[110] in good standing or a CSA Affiliate Member;[111]
- it has signed the "Qualified PLA Auditing Partnership Agreement" with CSA;
- it employs at least one Qualified PLA Auditor.

Qualified PLA Auditors are professionals that comply with requirements 1. and 2. listed below:

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 PLA training and certification).

2.a minimum 1 year experience on cloud security compliance or the possession of a relevant professional certification (e.g., CSA CCSK, ISC(2) CCSP). This requirement applies in cases where the auditee already has a relevant information security certification[112] (e.g., CSA STAR Certification/Attestation, ISO 27001);

2.b 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). This requirement applies as alternative to 2.a: that is, when the auditee does not already have a relevant information security certification.

Once verified that all the necessary conditions are satisfied, CSA will provide the adherent to the PLA CoC Third Party Certification Mark.

[110] http://www.businessdictionary.com/definition/member.html

[111] http://www.investopedia.com/terms/a/affiliate.asp

[112] Note that information security certification must cover a scope relevant to the scope of processing.

The PLA 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 PLA CoC Third Party Certification must be revised every time there's a change in the company relevant policies or practices.

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

3.1.3 1.3 CODE OF ETHICS

See Appendix C below for a description of the Code of Ethics.

3.1.4 1.4 PLA AND OCF WORKING GROUP CHARTERS

Please consult CSA's relative documentation of "Privacy Level Agreement Working Group Charter, 2017"[113] and "Open Certification Framework Working Group Charter, 2017"[114].

3.2 BODIES, ROLES AND RESPONSIBILITIES

The governance of PLA CoC and its components (PLA Code of Practice, Certification scheme and code of ethics) is a shared responsibility between the PLA and the Open Certification Framework Working Groups, and CSA.

3.2.1 PLA WORKING GROUP (WG)

This body is responsible for defining, approving and updating changes to the legal-technical standard/code of practise (i.e., PLA). The group also provides expert opinion to CSA when complaints about PLA Self Attestation or Certification are submitted.

[113] https://docs.google.com/document/d/1HWklskzaDvl6sN-bh-4Rxh1pWCYA2Em5xMpagmGjCdE

[114] https://docs.google.com/document/d/1xadjhcPZv30VDMTTrLLsb2r1_BUTX4OIn3aFh57ZDZs

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 PLA standard.

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

3.2.2 OCF WORKING GROUP

This body is responsible for the definition of the certification scheme(s) adopted within the CSA STAR Program. The OCF WG defines, reviews and approves changes in certification schemes already existing within the CSA OCF/STAR Program; and defines, reviews and approves any new certification scheme (e.g., the PLA CoC Certification scheme).

The OCF WG Charter documentation 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.

3.2.3 CLOUD SECURITY ALLIANCE (CSA)

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

- maintaining a public registry of issued PLA Certificates. Each entry includes as minimum the following information:
  (i) name and description of organisation,
  (ii) name and description of service for which the PLA is relevant,
  (iii) PLA entry,
  (iv) version of PLA standard used (currently V3),
  (v) validity of certificate,
  (vi) name of auditing organisation/auditor;
- maintaining a public registry of Qualified PLA Auditors;

- maintaining a web site where information and guidelines about the PLA concept, approach and technical standards are provided, together with the requirements, process and cost of the certification scheme;
- reviewing PLA Self Attestations and verifying minimum requirements are met;
- maintaining a mechanism for filing complaints;
- verifying complaints and taking appropriate actions (e.g., removing a PLA Entry and Certificate from the Registry; removing a Qualified PLA 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 PLA 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 PLA Qualified Auditor training partners;
- providing a public accounting of all fees and other revenues collected and their disposition in the management of this program.

3.2.4 COLLABORATION AND SUPPORTING ACTIONS TOWARD DATA PROTECTION SUPERVISORY AUTHORITIES

The PLA CoC governance bodies agree to collaborate and support national data protection supervisory authorities (SAs) 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 SA, the Article 29 Data Protection Working Party (A.29WP), or the European Data Protection Board, PLA 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 SA toward the relevant national parliament and/or public authorities).

With respect to supporting actions, and upon request by a national SA, A.29 WP, or the European Data Protection Board, the PLA CoC Governance Bodies also may do the following:

- promote awareness between the PLA Self-Attested and Certified companies about measures issued by national SAs (general provisions, as well as specific provisions - when issued towards a PLA Self-Attested or Certified company);
- if a national SA carries out an inspection of a PLA-Certified company, provide SA with all information and evidence available in CSA about the PLA-Certified company. In these cases, CoC Governance Bodies will act as the CSA point of reference.
- review and, if necessary, withdraw the PLA certification of a company subject to penalties issued by a national SA.

3.3 GOVERNANCE PROCESSES AND RELATED ACTIVITIES

The governance process of the PLA 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 PLA CoC component.

3.3.1 CHANGE PROCESS OF EU-SEC PRIVACY CONTROL REPOSITORY

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

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

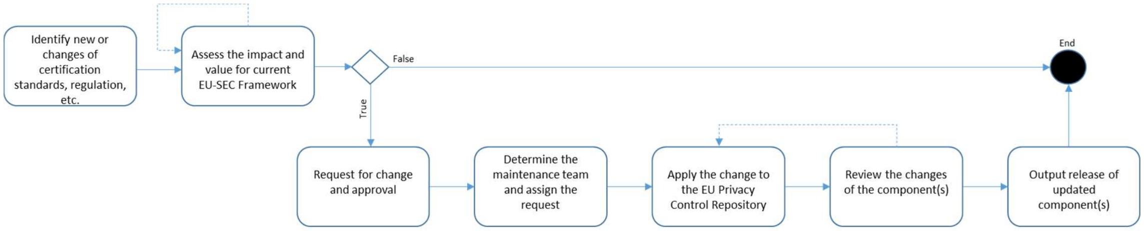
Identify new or changes of certification standards, regulation, etc.
Assess the impact and value for current EU-SEC Framework
False
End
True
Request for change and approval
Determine the maintenance team and assign the request
Apply the change to the EU Privacy Control Repository
Review the changes of the component(s)
Output release of updated component(s)

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

Change process includes following activities:

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

As Input for the change process, news and changes on privacy certification standards, regulation, etc. shall be continuously monitored. When there is new or changes of privacy certification standards or regulations in the market, they shall be reported to the governance office[115] and trigger the change management process. Both user and contributor of the PLA and the relevant stakeholders could identify and report the new and changes of privacy standards, or regulations. A change can also be identified from outcomes of reviews, meetings, updates, identified enhancements and/or inconsistencies of the contributors of the PLA or other stakeholders.

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

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

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

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

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

- Request for Change (RfC) and approval

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

- Determine the maintenance team and assign the request

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

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

- Apply the change to the EU privacy control repository

The maintenance team is responsible for the updates (addition, suppression, modification) of privacy control repository based on the change request and with respect to identified changes at the underlying privacy requirements. In addition, it will be ensured that the requested updates are done in a timely fashion in order to limit the possible risk of organizations adhering to an incomplete set of requirements.

- Review the change

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

- Output release of updated components

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

3.3.2 PLA CODE OF PRACTICE REVIEW PROCESS

The PLA will be subject to periodic reviews, since it is subject to changes in the European Union personal data protection-related legal framework. The PLA review process falls under the responsibilities of the PLA WG.

The PLA 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 requirements to the most current relevant legislations.

Any request to update the PLA shall be assessed and decided upon by PLA WG members (refer to the PLA Charter documentation).

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 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 PLA. PLA WG also foresees the development of a PLA that addresses Privacy/Data Protection requirements at the global level.

3.3.3 PLA COC CERTIFICATION REVIEW PROCESS

The OCF WG is responsible for triggering the review of the PLA 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 PLA CoC certification.

3.3.4 PLA COC MARKS ISSUING, STATEMENT OF ADHERENCE PUBLICATION AND COMPLAINTS MANAGEMENT

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

(i) **PLA CoC Self Attestation**

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

Upon validation, CSA shall ensure that the PLA Self Attestation is published at the online CSA Registry. If minimum requirements are not satisfied or if a complaint is deemed valid, CSA will take one of the following actions: a) request an amendment to the PLA Self Attestation, or b) Remove the Self Attestation from the CSA Registry and revoke the Mark.

(ii) **PLA CoC Certification**

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

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

If the complaint is deemed valid, the Qualified PLA Auditor shall temporarily suspend certification or revoke it. Accordingly, CSA shall remove the certification from its Registry and revoke the Mark.

3.3.5 CODE OF ETHICS REVIEW PROCESS

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

3.3.6 PLA AND OCF WG CHARTERS DOCUMENTS REVIEW PROCESS

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

4 CONCLUSIONS

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

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

Equally important, the presented PLA CoC governance structure and its integrated management processes will assist towards the maintenance and constant alignment of the tool in two ways. First, internally to the EU-SEC framework, it will provide consistency and updates with respect to any changes to the EU-SEC privacy control/requirements repository. Secondly, it will establish a trust and compliance transparency with the various external stakeholders within the cloud computing industry by employing coherent communication management and adherence mechanisms.

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

APPENDIX A - PLA TEMPLATE AND STATEMENT OF ADHERENCE

Annex A_PLA V3 Template_04-10-2017.xlsx

APPENDIX B – PLA COC STATEMENT OF ADHERENCE

Annex B_Part 1_PLA CoC_Statement of Adherence_Certification_Template_04-10-17_Final.docx
Annex B_Part2_PLA CoC_Statement of Adherence_Self-Assessment_Template_04-10-17_Final.docx

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

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

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

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

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

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

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

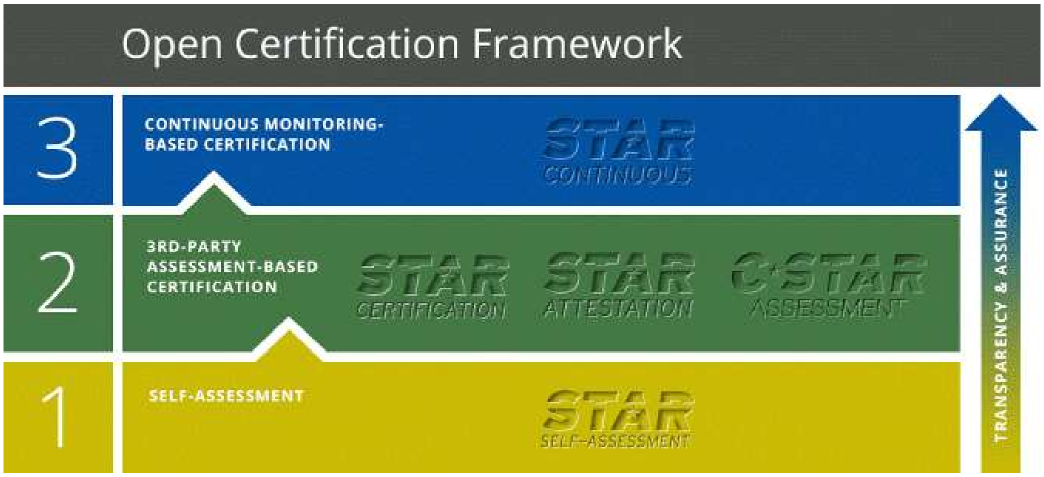

Figure 2: Open Certification Levels Diagram

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

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

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

The relationship between OCF Levels is the following.

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

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

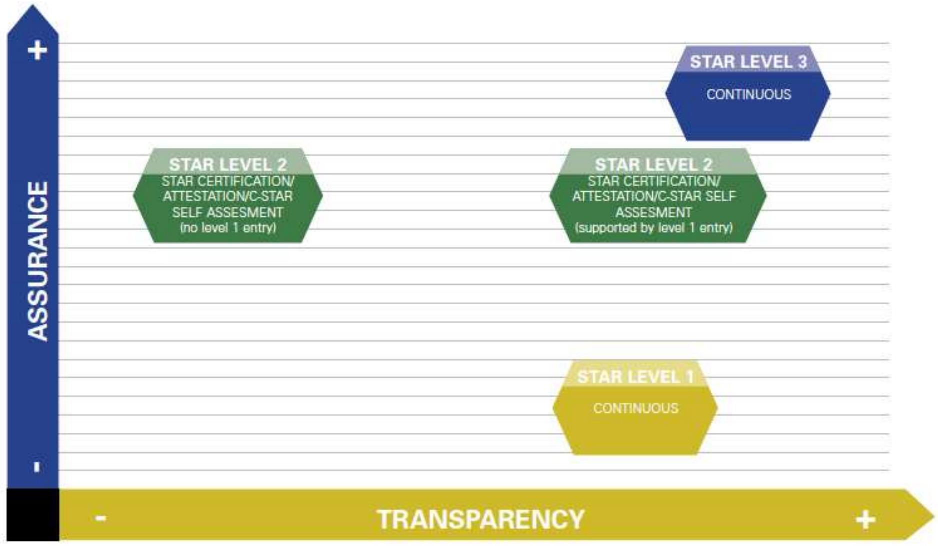

Figure 3: Levels of Transparency offered by the three OCF levels

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

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

APPENDIX D - CODE OF ETHICS

1. SCOPE

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

2. DEFINITIONS

Board Member: a member of the Board of Directors of the Cloud Security Alliance in office.
CSA Party: a Board Member, officer, full-time or part-time employee, contractor, or volunteer of the Cloud Security Alliance.
Volunteer: an individual who spends significant time advancing the mission of the Cloud Security Alliance as a member of its Board of Directors or through service on an advisory committee to the Board of Directors.

3. ETHICS PRINCIPLES

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

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

- our words and actions embody respect for truth, fairness, free inquiry, and the opinions of others;
- we respect all individuals without regard to race, colour, sex, sexual orientation, marital status, creed, ethnic or national identity, handicap, or age;
- we uphold the professional reputation of others and give credit for ideas, words, or images originated by others;
- we safeguard privacy rights and confidential information;
- we do not grant or accept favours for personal gain;
- we do not solicit or accept favours where a higher public interest would be violated;
- we avoid actual or apparent conflicts of interest and, if in doubt, seek guidance from appropriate authorities;
- we follow the letter and spirit of the laws and regulations affecting the Cloud Security Alliance;
- we actively encourage colleagues to join us in supporting these laws and regulations and the standards of conduct in these Ethics Principles.

4. REVIEW AND ACKNOWLEDGMENT OF STATEMENT OF ETHICS

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

5. ENTRY INTO FORCE AND IMPLEMENTATION

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

6. OVERSIGHT

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

7. REVIEW AND CHANGES

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