

---

# EU-SEC The European Security Certification Framework

Privacy Code of Conduct



# Contents

---

- Objectives
- Scope
- PLA CoC Components
- PLA CoP Assessment Tool
- PLA CoC Governance
- Conclusions

# Objectives

---

The Privacy Level Agreement (PLA) Code of Conduct (CoC) is to be used:

- As an appendix to a Cloud Services Agreement and describe the level of privacy protection of the CSP
- By cloud customers and potential customers as a tool to evaluate the level of personal data protection offered by different CSPs
- By CSPs as guidance to:
  - achieve compliance with EU personal data protection legislation and
  - describe the level of privacy and data protection towards data processing

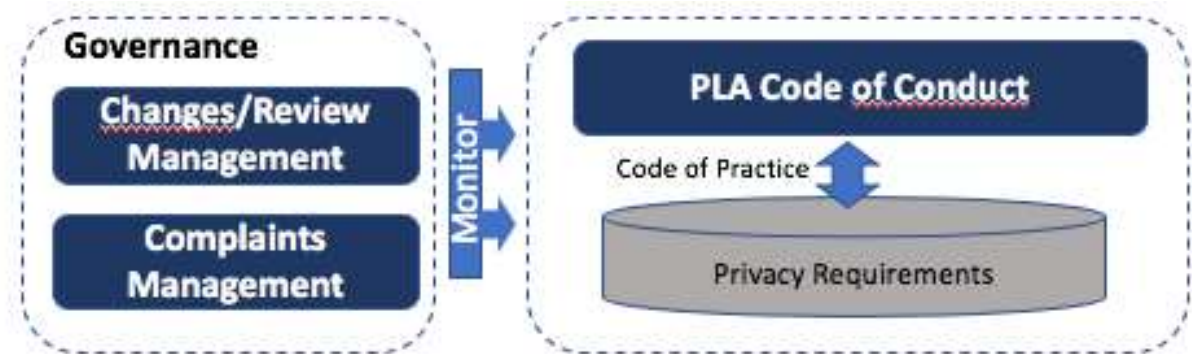
# Scope

---

- PLA CoC deals only with the Business-to-Business (B2B) scenario
  - the cloud customer is the data “controller” and the CSP is a data “processor”
  - both the cloud customer and the CSP are data controllers
- Reflects the GDPR requirements that are relevant to the cloud domain and extends beyond the EU
- Can assess and achieve compliance with the EU personal data protection legislation horizontally across different sectors and domains


# PLA Code of Conduct (CoC) Components

- PLA Code of Practice (CoP)
  - Is the “technical standard” and includes a set of privacy controls that a CSP should implement in order to establish adherence to the GDPR requirements
  - 15 domains / 94 controls
- PLA Governance
  - PLA CoC Self Attestation
  - PLA CoC 3<sup>rd</sup> party Certification



# PLA Code of Practice – Assessment Tool

- 15 domains/areas and 94 privacy controls

1			<p>© 2017 Cloud Security Alliance – All Rights Reserved.                  The Cloud Security Alliance PLA Code of Conduct and its Annexes (e.g. Annex 1: PLA Template, Annex 2: Statement of Adherence Template (collectively, "PLA Code of Conduct") is licensed by the Cloud Security Alliance under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License (CC-BY-NC-ND 4.0).  <b>Sharing:</b> You may share and redistribute the PLA Code of Conduct in any medium or any format.  <b>Attribution:</b> You must give credit to the Cloud Security Alliance, and link to the Cloud Security Alliance PLA Code of Conduct webpage located at <a href="https://cloudsecurityalliance.org/download/">https://cloudsecurityalliance.org/download/</a>. You may not suggest that the Cloud Security Alliance endorsed you or your use.</p>			<p><b>No Derivatives:</b> If you remix, transform, or build upon the PLA Code of Conduct, you may not publish, share or distribute the modified material.  <b>No additional restrictions:</b> You may not apply legal terms or technological measures that restrict others from doing anything that this license permits.  <b>Commercial Licenses:</b> If you wish to adapt, transform build upon, or distribute copies of the Cloud Security Alliance PLA Code of Conduct for revenue generating purposes, you must first obtain an appropriate license from the Cloud Security Alliance.</p>			
2	<b>Requirement</b>	<b>Requirement ID</b>	<b>Control</b>	<b>Control ID</b>	<b>Specification</b>	<b>CSP is Data Controller</b>	<b>CSP is Data Processor</b>	<b>Additional sector specific requirements</b>	<b>Additional specification on national level</b>
3	<b>1. CSP DECLARATION OF COMPLIANCE AND ACCOUNTABILITY.</b>	<b>DCA</b>	<b>1. Declaration of compliance and accountability</b>	<b>DCA-1.1</b>	<i>1. Declare to comply with the applicable EU data protection law, also in terms of technical and organisational security measures, and to ensure the protection of the rights of the data subject;</i>	Applicable	Applicable		
4				<b>DCA-1.2</b>	<i>2. Declare to be able to demonstrate compliance with the applicable EU data protection law (accountability).</i>	Applicable	Applicable		
5				<b>DCA-1.3</b>	<i>3. Describe what policies and procedures the CSP has in place to ensure and demonstrate compliance by the CSP itself and its subcontractors (see also Section 3.3 – 'Subcontractors', below) or business associates.</i>	Applicable	Applicable		
6				<b>DCA-1.4</b>	<i>4. Identify the elements that can be produced as evidence to demonstrate such compliance., Evidence elements can take different forms, such as self-certification/attestation, third-party audits (e.g. certifications, attestations, and seals), logs, audit trails, system</i>	Applicable	Applicable		
7									
8									
9									
10									
11									
12									
13									
14									

# PLA CoC Governance

---

- Governance Bodies, Roles and Responsibilities
- Governance Processes
  - Change management process for EU-SEC privacy requirements repository
  - Complaints management process
  - PLA CoP, PLA CoC Certification and Code of Ethics review processes
- PLA CoC marks issuing, statement of adherence publication

# Conclusions

---

- PLA CoC aims at increasing the level of transparency and accountability from the privacy and security point of view
  - CSPs offers a tool for assessing their level of adherence to GDPR requirements as well as a mechanism of compliance
  - Cloud Customers have a tool to evaluate the level of personal data protection offered by the different CSPs
  
- PLA CoC governance structure and its management processes assist the maintenance and constant alignment of the tool to EU regulatory landscape