Guidance for submitting the CSA Code of Conduct (CoC) for GDPR Compliance Self-Assessment

The CSA CoC for GDPR Compliance Self-Assessment is the voluntary publication of a CSP's self-assessment results based on the requirements specified in the PLA Code of Practice (CoP).

The publication on the CSA STAR Registry requires the submission of the CoC Statement of Adherence (Annex 2 of the Code) and PLA CoP Template (Annex 1 of the Code) to the Cloud Security Alliance.

Note: A CSP must take into consideration all the PLA CoP requirements – CSPs cannot declare adherence only to a chosen subset of those requirements.

Why Submit to the Registry?

The General Data Protection Regulation emphasizes transparency, security, and accountability within an organization. Each of those areas affects security in different ways – from action and prevention to mitigation, governance, awareness, and more. It is critical that organizations emphasize the seriousness of security and can show evidence of a formal program and its effectiveness.

How it Works

1. Submit the PLA Template and the CoC Statement of Adherence. CSPs are responsible for filling out the PLA Template and the CoC Statement of Adherence in good faith, and must ensure that all answers they provide are accurate and truthful.
2. Pay the submission fee of EUR 1,495.00. This is required prior to any submission being accepted into the evaluation process (Reference Figure 1 Submission Process Flow).
3. Our experts will verify the submission has been completed in all its sections and ensure that the PLA CoP requirements are properly addressed in the answers given. (In other words, the experts will perform a “plausibility check” on the answers given, without performing a material or substantive audit as to the accuracy and veracity of those answers).
4. To avoid violating impartiality policy and to keep pricing down, multiple submissions of the same assessment is discouraged. Upon the third submission of the same self-assessment a surcharge of 50% of the original base fee will be charged upon resubmission.

CSA will also verify the submitter has provided a public notice of compliance to the CoC on its website.

5. Once verified that all the necessary conditions are satisfied, CSA will provide the CSP with a self-assessment seal, with a validity of 12 months.
Submitting a Self-Assessment

If you have multiple cloud services
If a CSP offers several cloud services, and wishes to demonstrate its adherence to the Code of Conduct requirements for all of them, that CSP will be required to submit several Self-Assessments, one for each service.

Submission Forms and Instructions
The submission forms and instructions for the CSA Code of Conduct for GDPR Compliance can be found here: https://gdpr.cloudsecurityalliance.org/public-registry/

Read the Entire CoC First
It is critical to carefully read through the entire CSA Code of Conduct, and all of its controls, prior proceeding to the completion of the PLA Template. Part 1 and Part 2 of the CSA Code of Conduct contain relevant details that help to clarify the type and level of accuracy of the information which a CSP must provide in their Self-Assessment, in order to justify how each PLA CoP requirement is satisfied.

Find Additional Criteria & Guidance in CoC Part 2
In particular, in Part 2 of the CSA Code of Conduct, the CSA has outlined additional criteria and guidance to further explain the scope and objectives of each requirement – in other words, its “relevance.”

CSPs should use each “relevance” section as a guide and carefully analyze each one before addressing the corresponding control in the PLA CoP Template.

Satisfy All Controls
CSPs are required to satisfy all controls applicable to its processing role or roles, regarding the services under assessment (Controller/Processor). No applicable controls may be considered as out of scope. Exclusions do not apply, especially as the nature of the GDPR is about demonstrating compliance.

What if I don’t process a data category?
If, for instance, you do not process any special categories of data, then you obviously do not need to meet any requirements related to the processing of those types of data. In this case, you must represent that you comply with them due to the fact that you do not process special categories of personal data.

Prove compliance for vendors & third-parties
Controllers and processors are always responsible for complying with each of the controls applicable to them, even when they have outsourced activities under the scope of a control to third-parties. Even if certain aspects are outsourced or the responsibility of a vendor or third party, you are still responsible for having a process in place proving you have an effective system that ensures you know that vendor is in compliance.

Failing to address even a single control will prevent the acceptance of the submission and the award of a Self-Assessment Seal.

How to fill out a self-assessment
Describe the measures/actions/contractual clauses a CSP has in place to satisfy the requirements specified in the PLA Template - Annex 1, for the cloud service being assessed.
How to Fill Out the PLA Template (Annex 1)

In order to address the controls within the PLA Template (Annex 1) it is recommended that the CSP covers each control individually for each service, starting from the top and working its way down to the final control. Each control should be answered with as much detail as possible. CSPs should be aware that controls will progressively go from higher-level to lower-level requirements, and that the same data protection aspects may be questioned in different controls with different degrees of detail/specificity.

Provide Self-Contained Answers

It is strongly recommended to provide self-contained answers per control. References to answers given in the submission regarding other controls should not be used – it should be possible to understand the full contents of each answer without needing to read other answers given in the submission, even if this means repeating information in different answers. While some controls are related, it is important to understand that the scope of each control is different and must be addressed individually, although there may be some overlap between answers.

Example of a Poorly Addressed Control

Below is an example of a poorly-addressed control. It is not enough, to address controls, to provide a high-level description of the information, meeting the controls' requirements, which is provided in contracts entered into with cloud customers.

| WWP-1.15 | 15. Specify to cloud customers how the cloud customers will be informed about relevant changes concerning relevant cloud service(s), such as the implementation or removal of functions (General Information - applicable to both CSPs that are controllers and CSPs that are processors) | Applicable | Applicable | Will be notified as per contractual obligations with them. Through mail to their designated contact. |

It is important that CSA is able to assess all information required to validate a Self-Assessment submission from the answers given in the submission alone. Therefore, when referring to clauses or sections within a contract, privacy policy, terms of service or other documentation, the CSP must include a reference to the clause/section/document in question and quote the relevant wording, as well as (whenever feasible) add a link to the document in question.

Answers which refer to contracts or other documents should be framed so as to contain the following:

- Short summary of the action that you put in place (i.e. “Cloud customers will be notified as per contractual obligations with them, through e-mail, to their designated contact.”);
- Reference to the contractual clause or any other evidence that satisfies the control, including a quote of the relevant wording which addresses the control;
- Link(s) to the document in question.
## Example of a Properly Addressed Control

<table>
<thead>
<tr>
<th>WWP-1.15</th>
<th>Applicable</th>
<th>Applicable</th>
</tr>
</thead>
<tbody>
<tr>
<td>15. Specify to cloud customers how the cloud customers will be informed about relevant changes concerning relevant cloud service(s), such as the implementation or removal of functions (General Information - applicable to both CSPs that are controllers and CSPs that are processors)</td>
<td>Cloud customers will be notified as per contractual obligations with them, through e-mail, to their designated contact. As per Section 9.8 of our DPA, available at xyz.com/dpa: “In the event of planned substantial changes or further updates to the Service, which may be relevant to the Customer from the security or data protection perspective, the Customer will be notified by e-mail, with 30 days’ advance notice, through the contact details specified in Clause 10.4 below.”</td>
<td></td>
</tr>
</tbody>
</table>

### What happens after I submit a self-assessment?

Once completed, CSA estimates a period of 10 working days to review a Self-Assessment submission. Approval of the Self-Assessment submission will be completed within this period if the submission addresses all of the controls appropriately; otherwise, CSA may ask that the CSP clarify or supplement some or all of the answers given. Any further information or clarifications provided by the CSP will be subject to a new review.

After publication, the company will receive authorized use of a Compliance Mark (Seal), valid for 1 year from the day of its issuance and it should be renewed after this period. Moreover, the Self-Assessment must be revised every time there is a change to the company policies or practices related to the service under assessment.
CSA GDPR COC Self Assessment Flow V3

Submission of GDPR Self-Attestation

CSP submits:
- Self-Attestation Statement of Adherence and
- Self-Attestation results based on the PLA V3 Template

CSP pays submission fee

Monitoring Body performs eligibility assessment

Approved?

No

Yes

Credit Card Payment required prior to review process

CSP addresses comments and sends revision

Gaps identified; CSP to address questions and comments raised by Monitoring Body

Adherence Seal is granted and Self-attestation is published on STAR Registry

Adherence Seal is valid for a period of 12 months (renewable)

Recurring 50% surcharge (from base fee) upon 3rd resubmission in approval process