ABOUT & ACKNOWLEDGMENTS

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

The PLA WG is composed of representatives of cloud service providers, local Supervisory Authorities and independent security and privacy professionals.1

We would also like to thank CSA staff, Hillary Baron, Damir Savanovic, and Kendall Scoboria, for their support.

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

1 Part 3 of this document, i.e., PLA CoC Governance, has been developed thanks to the contribution of the European Commission-funded project European Security Certification Framework (EU-SEC).
COPYRIGHT NOTICE
© 2013-2020 Cloud Security Alliance – All Rights Reserved.

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

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

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

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

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

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

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

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

**I. INTRODUCTION** .......................................................................................................................... 1  
**II. BACKGROUND INFORMATION** ................................................................................................. 3  
**III. STRUCTURE OF THE CSA CoC FOR GDPR COMPLIANCE** .................................................. 7  

**PART 1 CSA CoC OBJECTIVES, SCOPE, METHODOLOGY, ASSUMPTIONS & EXPLANATORY NOTES** .................................................................................................................................................................................. 8  
   1. **OBJECTIVES OF THE CSA CoC** ................................................................................................. 9  
   2. **SCOPE AND METHODOLOGY** ............................................................................................... 12  
   3. **ASSUMPTIONS** .......................................................................................................................... 17  
      3.1 Cloud Customer Internal Due Diligence ............................................................................... 17  
      3.2 Cloud Customer External Due Diligence ............................................................................ 18  
   4. **EXPLANATORY NOTES** ............................................................................................................ 19  
   5. **GLOSSARY** ............................................................................................................................... 20  
   6. **LIST OF REFERENCES** ............................................................................................................ 24  

**PART 2 CSA CoC CONTROL SPECIFICATIONS: PRIVACY LEVEL AGREEMENT** ...................... 30  
   1. **CSP DECLARATION OF COMPLIANCE AND ACCOUNTABILITY** ........................................ 31  
   2. **CSP RELEVANT CONTACTS AND ITS ROLE** ........................................................................ 36  
   3. **WAYS IN WHICH DATA WILL BE PROCESSED** .................................................................... 40  
      3.1 Instructions .............................................................................................................................. 40  
      3.2 Changes to the service ............................................................................................................ 41  
      3.3 Personal Data location ............................................................................................................ 42  
      3.4 Sub-processors ......................................................................................................................... 44  
      3.5 Installation of software on Cloud Customer’s system ............................................................ 46  
      3.6 Data Processing Agreement (or other binding legal act) ....................................................... 48  
      3.7 Data protection by design and by default .............................................................................. 51  
   4. **RECORDKEEPING** .................................................................................................................... 54  
   5. **DATA TRANSFER** .................................................................................................................. 55  
   6. **DATA SECURITY MEASURES** ................................................................................................ 59  
   7. **MONITORING** ......................................................................................................................... 66  
   8. **PERSONAL DATA BREACH** .................................................................................................... 66  
   9. **DATA PORTABILITY, MIGRATION AND TRANSFER BACK** .............................................. 70  
  10. **RESTRICTION OF PROCESSING** ............................................................................................ 72  
  11. **DATA RETENTION, RESTITUTION AND DELETION** ........................................................... 73  
      11.1 Data retention, restitution and deletion policies ................................................................. 73  
      11.2 Data retention ........................................................................................................................ 73
## 11.3 Data retention for compliance with sector-specific legal requirements

## 11.4 Data restitution and/or deletion

## 12. COOPERATION WITH THE CLOUD CUSTOMERS

## 13. LEGALLY REQUIRED DISCLOSURE

## 14. REMEDIES FOR CLOUD CUSTOMERS

## 15. CSP INSURANCE POLICY

### PART 3 CSA CODE OF CONDUCT GOVERNANCE AND ADHERENCE MECHANISMS

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>Control Specifications: PLA</td>
<td>87</td>
</tr>
<tr>
<td>1.2</td>
<td>Adherence Mechanisms to the CoC</td>
<td>87</td>
</tr>
<tr>
<td>1.2.1</td>
<td>CoC Self-attestation</td>
<td>88</td>
</tr>
<tr>
<td>1.2.2</td>
<td>CoC Third-party Assessment</td>
<td>90</td>
</tr>
<tr>
<td>1.3</td>
<td>Code of Ethics</td>
<td>94</td>
</tr>
<tr>
<td>1.4</td>
<td>PLA WG and OCF WG Charters</td>
<td>94</td>
</tr>
<tr>
<td>2.1</td>
<td>PLA WG</td>
<td>94</td>
</tr>
<tr>
<td>2.2</td>
<td>OCF WG</td>
<td>94</td>
</tr>
<tr>
<td>2.3</td>
<td>Cloud Security Alliance (CSA)</td>
<td>95</td>
</tr>
<tr>
<td>2.4</td>
<td>Collaboration and supporting actions toward Supervisory Authorities</td>
<td>95</td>
</tr>
<tr>
<td>2.5</td>
<td>Monitoring Body</td>
<td>96</td>
</tr>
<tr>
<td>2.5.1</td>
<td>Independence</td>
<td>97</td>
</tr>
<tr>
<td>2.5.2</td>
<td>Absence of a conflict of interests</td>
<td>98</td>
</tr>
<tr>
<td>2.5.3</td>
<td>Expertise</td>
<td>99</td>
</tr>
<tr>
<td>2.5.4</td>
<td>Resources and staffing</td>
<td>101</td>
</tr>
<tr>
<td>2.5.5</td>
<td>Established procedures and structures</td>
<td>101</td>
</tr>
<tr>
<td>2.5.6</td>
<td>Eligibility assessment</td>
<td>102</td>
</tr>
<tr>
<td>2.5.7</td>
<td>Transparent complaints handling</td>
<td>103</td>
</tr>
<tr>
<td>2.5.8</td>
<td>Communication with the competent Supervisory Authority</td>
<td>104</td>
</tr>
<tr>
<td>2.5.9</td>
<td>Review mechanisms</td>
<td>104</td>
</tr>
<tr>
<td>2.5.10</td>
<td>Legal status</td>
<td>105</td>
</tr>
<tr>
<td>2.5.11</td>
<td>Continuous improvement</td>
<td>105</td>
</tr>
<tr>
<td>2.5.12</td>
<td>Monitoring</td>
<td>106</td>
</tr>
<tr>
<td>3.1</td>
<td>Control Specifications: PLA review process</td>
<td>107</td>
</tr>
<tr>
<td>3.2</td>
<td>CoC Adherence Mechanism review process</td>
<td>108</td>
</tr>
</tbody>
</table>
3.3 CoC Adherence Seal issuing and Statement of Adherence publication ................................................................. 109
  3.3.1 CoC Self-attestation ................................................................................................................................. 109
  3.3.2 CoC Third-party assessment ..................................................................................................................... 109
3.4 Complaint management process .................................................................................................................... 110
3.5 Ongoing monitoring processes .................................................................................................................... 110
  3.5.1 Qualified CoC Auditing Partner monitoring process ............................................................................. 110
3.6 Code of Ethics review process ..................................................................................................................... 111
3.7 PLA and OCF WG charter documents review process ................................................................................. 111

ANNEX 1: PLA [V3] TEMPLATE ............................................................................................................................ 1
ANNEX 2: STATEMENT OF ADHERENCE TEMPLATE .......................................................................................... 1
ANNEX 3: THE CSA STAR PROGRAM AND OPEN CERTIFICATION FRAMEWORK (OCF) ..................... 1
ANNEX 4: CODE OF ETHICS ................................................................................................................................. 1
ANNEX 5: PRIVACY LEVEL AGREEMENT WORKING GROUP CHARTER ..................................................... 1
ANNEX 6: OPEN CERTIFICATION FRAMEWORK WORKING GROUP CHARTER ......................................... 1
ANNEX 7: COMPLAINT MANAGEMENT PROCESS ............................................................................................ 1
ANNEX 8: MONITORING/AUDIT PROCESS ........................................................................................................ 1
ANNEX 9: ENISA TECHNICAL GUIDELINES: SECURITY OBJECTIVES ......................................................... 6
I. INTRODUCTION

In consideration of the EDPB CoC Guidelines, Part 1 of the CoC, as well as the cover letter included with the submission of the CoC, contains the “explanatory statement” providing details as to the purpose of the CoC, the scope of the CoC and how it will facilitate the effective application of the GDPR.

Data protection compliance is becoming increasingly risk-based. Controllers and Processors are accountable for determining and implementing in their organisations appropriate levels of protection of the Personal Data they Process. In such decision, they have to take into account factors such as state of the art of technology; costs of implementation; and the nature, scope, context and purposes of Processing; as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. As a result, CSPs will be responsible for self-determining the level of protection required for the Personal Data they Process.

It is in this context that CSA has created the CoC.

The CoC aims to provide CSPs and Cloud Customers a solution for GDPR compliance and to provide transparency guidelines regarding the level of data protection offered by the CSP.

The CoC is essentially intended to provide:

- Cloud Customers of any size with a tool to evaluate the level of Personal Data protection offered in connection with services provided by different CSPs (and thus to support informed decisions)
- CSPs of any size and geographic location with a guidance to comply with EU Personal Data protection legislation and to disclose, in a structured way, the level of Personal Data protection they offer to customers, in connection with their services.

---

1 A glossary including definitions and acronyms used in this CoC, including those relating to legislative and other references, is included in Part 1, Section 6, below.
2 See, e.g., Preamble 83 and Articles 25, 32, 33, 34 and 35 GDPR.
3 See, e.g., Articles 24, 25, 32, 35 and 39 GDPR.
4 WP29 Cloud Computing Guidelines, p. 2: “All cloud providers offering services in the European Economic Area (EEA) should provide the cloud client with all the information necessary to rightly assess the pros and cons of adopting such services. Security, transparency, and legal certainty for the clients should be key drivers behind the offer of cloud computing services.”, p. 4: “(...) a precondition for relying on cloud computing arrangements is for the controller [cloud client] to perform an adequate risk assessment exercise, including the locations of the servers where the data are processed and the consideration of risks and benefits from a data protection perspective.”.
The above notwithstanding, the direct target audience for the CoC are CSPs (and not Cloud Customers), as only CSPs can actually submit their services for adherence to the CoC. However, the CoC is nonetheless designed in a way that, ultimately, seeks to benefit both CSPs and Cloud Customers (as well as Data Subjects and, in general, the cloud community), by means of the controls imposed through the Privacy Level Agreement Controls (“Control Specifications: PLA”).

CoC compliance is based on two major Technical Components, the Control Specifications: PLA – which is a technical standard that specifies the requirements included in the GDPR – and the adherence mechanisms associated with the CoC.

Since the CoC mainly focuses on legal requirements, CSA proposes the combined adoption of this CoC with other CSA best practices and certifications\(^5\), such as the Cloud Control Matrix (CCM) and the STAR Certification (or STAR Attestation or STAR Self-Assessment), which provide additional guidance around technical controls and objectives for information security.

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

**For the avoidance of doubt:**

- Certification (or Attestation) under the schemes mentioned above (e.g., ISO 27001, STAR Certification, SOC2 Attestation) will not imply an automatic adherence to the CoC. CSPs will be required to submit their service(s) for adherence by means of the Adherence Mechanisms provided: Self-Attestation (Part 3, Sections 1.2.1. and 3.3.1., below) or Third-party Assessment (Part 3, Sections 1.2.2. and 3.3.2., below).

- Adherence to the CoC will, likewise, not imply an automatic certification under any of the abovementioned certification schemes.

---

\(^5\) For the avoidance of doubt, the certification schemes mentioned here are not “certification mechanisms” under Art. 42 GDPR, but rather certification schemes related to information security and/or cloud security. Certification under these other schemes is not a prerequisite to the CoC; rather, CSPs might also want to consider this as a means to fortify their information security practices (which would help meet the CoC’s security-related controls – see Part 2, Control no. 6.).
The CoC reflects the GDPR requirements that are relevant in the cloud and is a component of the CSA Security, Transparency and Assurance Registry (STAR).

As noted further in Part 3, Section 1.2., below, CSPs which submit one or more of their services for adherence to the CoC become bound by the controls within the Control Specifications: PLA (Part 2), and must comply with all of those applicable to them. Failure to do so may result in sanctions imposed by the Monitoring Body, as the result of an investigation of a complaint (Part 3, Section 2.5.7., below, as well as Annex 7) or the ongoing CoC compliance monitoring activities performed by the Monitoring Body (Part 3, Section 2.5.12., below, as well as Annex 8).

Finally, it is important to note that any adherence to the CoC does not reduce CSPs’ and Cloud Customers’ responsibility for compliance with the GDPR and is without prejudice to the tasks and powers of the national Supervisory Authorities.

II. BACKGROUND INFORMATION

CSA, the owner of the CoC, is the world’s leading organization dedicated to defining and raising awareness of best practices to help ensure a secure cloud computing environment. CSA is a not-for-profit organisation that includes in its membership base a significant portion (over 350 members) of worldwide CSPs and cloud security vendors, as well as several Cloud Customers. Moreover, CSA has over 90,000 individual members and 85 National and Regional Chapters on a global scale.

CSA has been working on the development of privacy and data protection guidelines and best practices for the cloud environment since 2013. This CoC has been developed within CSA by an expert Working Group (WG) composed of representatives of cloud service providers, local Supervisory Authorities and independent security and privacy professionals (the “PLA Working Group”, or “PLA WG”). It was published on 21 November 2017, and last updated on May 2019, to reflect the most recent Guidelines of the EDPB (former Article 29 Data Protection Working Party) and also to incorporate by reference the CNIL Security Guide.

The Privacy Level Agreement Outline for the Sale of Cloud Services in the European Union (PLA [V1]), was released in February 2013 as a self-regulatory harmonization tool that offers a structured way to communicate the level of Personal Data protection offered by a CSP to current and potential customers. PLA [V1] was based not only on EU Personal Data protection mandatory legal requirements, but also on best practices and recommendations.
PLA [V1] was endorsed by, and received positive feedback from, a number of Supervisory Authorities\(^6\). It was used to develop further EU studies, best practices and codes of conduct on Personal Data protection matters related to cloud computing.

However, after the release of PLA [V1], the PLA WG realized that CSPs, Cloud Customers and potential customers still struggled to identify the necessary baseline for Personal Data protection compliance across the EU.

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

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

In May 2016, the GDPR entered into force, and became directly applicable in all EU Member States from 25 May 2018 onwards. With the introduction of the GDPR, it was immediately evident to the PLA WG that CSPs, Cloud Customers and potential Cloud Customers needed guidance in order to comply with the new law in the cloud environment. Therefore, the PLA WG developed PLA [V3], a compliance tool that reflects the new obligations set forth by the GDPR.\(^7\)

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

This current version of the PLA, i.e. [V4] will be updated as required on the basis of the development of relevant legislation, opinions, guidelines and recommendations from competent authorities.

PLA [V4] is thus designed to create continuity between the EU legal Personal Data protection requirements set forth in the Data Protection Directive and its implementations in the EU Member States, by leveraging the PLA [V2] structure, and the requirements of the GDPR.

PLA [V4] is structured to help CSPs, Cloud Customers and potential Cloud Customers manage the transition from the old to the new EU data protection regime, and contributes to the proper application of the GDPR into the cloud sector.

\(^6\) In particular, PLA [V1] was endorsed by the CNIL itself, as well as by the Irish Supervisory Authority. Positive feedback was received from the ICO and the Garante, as well as the Supervisory Authorities of Greece, Slovenia, and Catalonia.

\(^7\) Relevant requirements have been added to the PLA [V2] in order reflect the new duties and obligations set forth in the GDPR.
PLA [V4] specifies the application of the GDPR in the cloud environment, primarily with regard to the following categories of requirements:

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

PLA [V4] further seeks to address several key particularities of the cloud domain regarding privacy and data protection, including specific issues faced, such as:

- **Resource sharing issues**, where potential conflicts may arise due to the use of shared systems and infrastructures to Process Personal Data related to multiple different Cloud Customers and types of Data Subjects;

- **Shared-responsibility model**, where the cloud introduced a new model for the allocation and distribution of the information security responsibility between CSP and Cloud Customers. That sometimes creates confusion between the parties, especially on the difference between transferring of the responsibilities for certain security controls implementation to the CPS and maintaining the accountability and duty of care on the shoulder of the Cloud Customers;

- **Law enforcement requests**, where CSPs located in multiple jurisdictions may find themselves legally required to disclose Personal Data related to Cloud Customers to public authorities, potentially in breach of EU data protection law;

- **Complex outsourcing chains**, where CSPs may engage a multitude of Sub-processors located in various different territories worldwide, creating contracting arrangements which may be difficult to manage and often not providing Cloud Customers with sufficient means to oppose use of their data in this way (including by not affording sufficient transparency to those Cloud Customers);

---

8 See the WP29 Cloud Computing Opinion, which highlights many of these issues.
• **Obstacles to the addressing of Data Subject requests**, where cloud services may not have been properly configured to allow, e.g., requests for erasure, restriction of Processing or portability to be promptly and properly complied with;

• **Changes to the terms under which a cloud service is provided**, which may affect the conditions under which a Cloud Customer's data is Processed during the provision of the service;

• **Lack of isolation**, whereby CSPs (due to their control over data handled on behalf of multiple Cloud Customers) could potentially decide to connect data handled on behalf of different Cloud Customers, for secondary purposes which may not have been authorised by those Cloud Customers;

• **Further unauthorised Processing of data by CSPs in general**, such as use of Cloud Customer data to further develop analytics/Profiling algorithms or for programmatic advertising purposes;

• **Complexities in the allocation of data protection roles to Cloud Customers and CSPs**, considering the various types of activities which a CSP may carry out (some of which may be as a Processor, and others as a Controller) and recent CJEU jurisprudence on Joint Controllers.

• **Vendor lock-in**, whereby Cloud Customers may find themselves restricted in their ability to switch between CSPs, due to (e.g.) a lack of means to ensure portability of Personal Data between CSP services.

Additionally, PLA [V4] contains mechanisms that enable the body referred to in Article 41(1) GDPR to carry out the mandatory monitoring of compliance with its provisions by the CSPs that undertake to apply it, without prejudice to the tasks and powers of competent Supervisory Authorities pursuant to Article 55 or 56 GDPR.

As noted in **Part 3, Section 2.1.**, below, the PLA WG is and was responsible for defining, approving and updating changes to PLA [V3], which represents the fundamental Technical Component of the CoC, identifying the relevant EU data protection compliance requirements and defining clauses / controls to manage CSPs’ compliance with those requirements (see **Part 3, Section 1.1.** below).

The PLA WG is composed of representatives of CSPs, local Supervisory Authorities and independent security and privacy professionals – all of which are important stakeholders within the cloud computing community, and which were thus able to weigh in on the structure and contents of the Technical Components within the CoC.
Additionally, the CoC was left open for feedback and consultation on CSA’s website, for a period of 30 days, as customary for any research artefacts developed by CSA, during which any interested individuals could provide input or insights deemed relevant. The public peer review process for the CoC was announced to the overall CSA community (CSA’s LinkedIn groups, CSA’s network of chapters, CSA corporate members and relevant CSA committees).

For these reasons, PLA [V4] (Part 2 of the CoC), together with the remainder of this document, including its Governance and Adherence Mechanisms (Part 3 of the CoC), qualifies as a “draft” Code of Conduct pursuant to Article 40 GDPR.

III. STRUCTURE OF THE CSA CoC FOR GDPR COMPLIANCE

The CoC is structured in three parts:

- **Part 1** of the CoC describes its objectives, scope, methodology and assumptions, and provides explanatory notes.
- **Part 2** of the CoC contains the Control Specifications: PLA and its substantial provisions, developed by the PLA WG.
- **Part 3** of the CoC outlines the governance structure and the mechanisms of adherence to the CoC.
PART 1
CSA CoC OBJECTIVES, SCOPE, METHODOLOGY, ASSUMPTIONS & EXPLANATORY NOTES
1. **OBJECTIVES OF THE CSA COC**

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

2. In order to adhere to the CoC, the CSP must implement and describe technical and organisational measures which are objectively sufficient to meet every single one of the CoC’s controls (Part 2). This allows the CSP to describe the level of privacy and data protection that it undertakes to maintain with respect to relevant Personal Data Processing activities performed, regarding the service(s) it provides to Cloud Customers which the CSP has aligned with this CoC.

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

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

---

9 "‘[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.

10 "‘[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.
5. Ultimately, the CoC is intended to provide the following:

- Cloud Customers and potential Cloud Customers, of any size, with a tool to evaluate the level of Personal Data protection offered by different CSPs, in connection with the service(s) provided (and thus to support informed decisions);\(^{11}\) 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 Cloud Customers, in connection with their service(s).

6. The CoC seeks to create additional value for potential and current Cloud Customers, as well as for CSPs, Data Subjects and the cloud computing community at large by:

- Identifying – in an organic, structured and systematic manner – all relevant GDPR provisions which CSPs must comply with when handling Personal Data;
- Explaining the GDPR provisions and their practical relevance, when applied to the computing environment, considering also the clarifications provided in this respect by the WP29 / EDPB, as well as by EU Supervisory Authorities which have provided guidance on the subject;
- Raising the bar for data protection and privacy in cloud computing, by adding controls defined on the basis of guidelines produced by CSA, ENISA, ISO standards (e.g., ISO 27001, ISO 27017, ISO 27018) and additional best practices developed (including controls such as the need for CSPs to identify and provide contact details for their Information Security Officer – Part 2, Control no. 2.5. –, defining a timeframe for CSPs to notify Cloud Customers regarding Personal Data Breaches of which they become aware – Part 2, Control no. 8. –, to offer effective and business-friendly remedies to Cloud Customers in the event of breaches of obligations under the Control Specifications: PLA – Part 2, Control no. 14. – and to procure data protection compliance insurance, with coverage over breaches caused by Sub-processors, and cyber-insurance, covering also security and Personal Data Breaches which may occur – Part 2, Control no. 15.);
- Emphasising the need for transparency and enabling compliance with the principle of accountability for CSPs, by establishing a disclosure policy and requiring CSPs adhering to the CoC’s requirements to provide minimum information and evidence to demonstrate their compliance, in the context of their Self-attestation/Third-party

\(^{11}\) “All cloud providers offering services in the EEA should provide the cloud client with all the information necessary to rightly assess the pros and cons of adopting such services. Security, transparency, and legal certainty for the clients should be key drivers behind the offer of cloud computing services.” WP29 Cloud Computing Opinion, 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.
Assessment submissions. Additionally, in requiring this disclosure, the information necessary for Cloud Customers engaging those CSPs to comply with their own transparency and accountability obligations towards Data Subjects, around the engagement of CSPs to Process Personal Data, will be made available to them;

- Allowing for **public scrutiny of compliance with the CoC**, by requiring adhering CSPs to disclose their CoC Self-attestation/Third-party Assessment submissions within the CSA STAR Registry (including, e.g., specific details on how those CSPs understand that they meet the minimum requirements set by the CoC), with any deviations from those submissions in practice kept in check by means of the CoC’s Complaint Management Process (which may, ultimately, lead to suspension or revocation of Adherence Seals provided to adherent CSPs, where a complaint is found to be valid).

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

7. The Control Specifications: PLA reflect the GDPR requirements that are relevant in the cloud. It also restates and reinforces the requirements of the GDPR, particularly where the exercise of Data Subjects’ rights are concerned – see, for example, **Part 2, Control no. 3.5.6.** (on the need for a CSP to commit, via contractual obligations, to assisting Cloud Customers in responding to Data Subject requests), **Part 2, Control no. 9.** (on the need for a CSP to assure the portability of data, including the capability to transmit Personal Data in a structured, commonly used, machine-readable and interoperable format directly to Data Subjects) and **Part 2, Control no. 10.** (on the need for a CSP to explain to Cloud Customers how it allows for the restriction of Processing of Personal Data). Moreover, it raises the bar for data protection and privacy in cloud computing, by adding controls defined on the basis of guidelines produced by CSA, ENISA, ISO standards and additional best practices developed – in particular, in **Part 2, Control no. 6.**, the CoC provides a solid baseline for technical and organisational security measures to be implemented by CSPs, through the CSA Cloud Controls Matrix, which is specifically designed to provide fundamental security principles to guide CSPs, by means of a 13-domain controls framework allowing for a detailed understanding of key security concepts and principles, resting on a customized relationship to other industry-accepted security standards, regulations and controls frameworks. The Control Specifications: PLA reflect all of the GDPR requirements and goes beyond, by providing a higher standard for adhering CSPs’ data protection practices.

8. The CoC, through the Control Specifications: PLA, does not only seek to promote lawful behaviour on the part of adhering CSPs, but also ethical behaviour. The CoC’s requirements include obligations upon CSPs which, while not strictly required by the applicable law, are necessary to guarantee a fair balance in the relationship between CSPs and Cloud Customers, eventually aiming to ensure that Data Subject rights can
effectively be respected. For example: the requirement for a CSP to provide a transitional period to Cloud Customers upon Cloud Customer termination (as a result of an objection to a change of Personal Data Processing locations or of Sub-processors), during which services will continue to be provided to Cloud Customers as they seek an alternative solution. This requirement seeks to prevent harm which might arise for Cloud Customers, as well as for the Data Subjects whose data are Processed by those Cloud Customers, if the services provided by a CSP were abruptly ended, as a result of the Cloud Customer’s exercise of their right of objection/termination (see Part 2, Control no. 3.2.3. and Control no. 3.3.5.). One further example is Part 2, Control no. 14., which requires CSPs to offer remediation to Cloud Customers in the event that a CSP breaches its obligations under the Control Specifications: PLA, thereby ensuring compensation to the Cloud Customer and preventing the occurrence and escalation of disputes.

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

2. SCOPE AND METHODOLOGY

The 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). The CoC addresses specific services provided by a CSP in a B2B context – CSPs may offer a variety of services, some of which comply with the terms of the CoC, and others which do not. Services provided by CSPs will typically fall under one or more of the below three categories:

- **Software as a Service (“SaaS”):** SaaS CSPs provide software applications over the Internet. Examples of SaaS include e-mail services, human resource and customer relationship management applications (“HRM”/“HRIS”, “CRM”), online backup services, etc.

- **Platform as a Service (“PaaS”):** PaaS CSPs provide development tools over the Internet. Tools offered via PaaS could be used, for instance, to develop SaaS, e-commerce platforms, etc.
• Infrastructure as a Service (“IaaS”): IaaS CSPs provide storage, networking and computing services over the Internet, on demand.

The Processing activities related to services which are covered by the CoC are those which are performed by a CSP which acts as a Processor on behalf of a Cloud Customer. This will typically reflect one of two main types of situations:

• The Cloud Customer acts as a Controller, and the CSP acts as a Processor on their behalf;
• The Cloud Customer acts as a Processor (on behalf of another party), and the CSP acts as a Sub-processor on their behalf.

Regardless of whether the CSP acts as a Processor or Sub-processor, it must comply with the controls laid out in this CoC, so as to allow the Cloud Customer (acting as a Controller or Processor itself) to take those controls into consideration when crafting any offerings which may include the CSP’s services.

As originators of this document, the PLA WG recognizes that there may be more complex/hybrid situations (e.g., such as the situation where, for a single service, a CSP acts as a Controller for some activities) which are not, at present, covered by the CoC.

The CoC takes into consideration various relevant opinions and guidelines, issued by EU Supervisory authorities and other relevant (EU and non-EU) bodies (as listed in Section 6., below). Therefore, this CoC is not only based on the mandatory legal provisions of the applicable EU Personal Data protection framework, but also reflects the relevant interpretation by the EU Supervisory Authorities and related best practices developed by relevant agencies and other bodies. The CoC aims to be a horizontal tool that can be used to achieve/assess compliance with the EU Personal Data protection legislation horizontally across different sectors and domains. The PLA WG is aware of the possibility for EU Member States to provide for exemptions or derogations, more specific rules and additional requirements on top of the GDPR\(^\text{12}\), as well as of the existence of EU Personal Data protection provisions applicable to specific services (e.g., ePrivacy Directive, ePrivacy Regulation, and the NIS Directive). Hence, the PLA WG recommends that users of the CoC identify possible Member States’ and/or sector-specific additional requirements. The CoC is also written taking into account the works

\(^{12}\) See, e.g., Article 37 (4) and CHAPTER IX ’Provisions relating to specific processing situations’ GDPR.
developed by the Cloud Select Industry Group on Code of Conduct\(^{13}\), by the Cloud Infrastructure Service Providers in Europe (CISPE),\(^{14}\) and the Cloud Accountability Project.\(^{15}\)

The CoC reflects the GDPR requirements that are relevant in the cloud domain and, following the “territorial scope” of the GDPR, the Control Specifications: PLA extend beyond the EU.\(^{16}\) Additionally, the CoC provides also practical explanations of the importance of each defined control (in Part 2), emphasizing the practical relevance (by means of examples, where appropriate) behind implementing each control, beyond compliance with mandatory requirements (particularly regarding controls which are not legally required).

The target audience for this CoC are CSPs (as only CSPs can submit their services for adherence to the CoC), but the CoC may serve as a useful tool also for other interested stakeholders in the area of cloud computing and EU Personal Data protection legislation, such as Cloud Customers and potential Cloud Customers, cloud auditors and cloud brokers. The CoC has been prepared in collaboration with a cross-functional working group of relevant players as well as posted for comment to a wider range of the cloud computing community. This process ensured that the CoC considers the nuances of the cloud computing sector in each of its controls.

Additionally, the CoC takes into consideration the needs of small and medium enterprises in the realm of data protection – particularly, the need to clearly understand how the GDPR may apply to them, so that they may allocate their resources for compliance in an effective manner. In this sense, the CoC further specifies controls to prevent GDPR compliance (considering all of the GDPR’s inherent duties and obligations, compliance with which requires a significant investment of time, money and effort) from becoming a competitive disadvantage for those enterprises: an example can be found in Part 2, Control no. 6, which relies on the detailed controls developed within the CSA Cloud Controls Matrix to allow SMEs to clearly understand the different types and levels of security measures which they are to implement. The desired end-result is for the CoC to provide easily understandable guidelines for SMEs, which may allow them to efficiently comply with applicable data protection requirements and level the playing


\(^{14}\) More information is available at: [https://cispe.cloud/](https://cispe.cloud/).

\(^{15}\) More information is available at: [http://www.a4cloud.eu/](http://www.a4cloud.eu/). See also: [http://cloudaccountability.eu/](http://cloudaccountability.eu/).

\(^{16}\) 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.”
field with larger CSPs – in short, the CoC seeks to develop a consistent approach to data protection in the cloud computing sector, for CSPs of all sizes.

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

The CompSA which has been identified for the CoC is the CNIL. This has been decided on the basis of the following factors:

- **Initiatives developed by the CNIL.** The CNIL has developed several guidelines and initiatives of relevance to the scope of the CoC, including the CNIL Cloud Recommendations and the CNIL Security Guide. Furthermore, and most importantly, the CNIL has followed the work developed on the CoC from the first versions of the PLA which were produced, and has to date provided extensive feedback on the CoC in the context of an informal consultation process initiated by the CSA. It results that the CNIL is the natural choice for the CompSA, competent to decide on the approval of the CoC. This is compounded by the fact that the other potential candidate for CompSA – the ICO (given the existence of a CSA subsidiary in Scotland) – may be compromised due to the impending possibility of the United Kingdom leaving the EU.

- **Location of the largest density of the Processing activity/sector.** France is home to a significant number of CSPs within Europe, including around 10 CSA corporate members with either their headquarters or a subsidiary settled in France.

- **Location of the largest density of Data Subjects affected.** Considering that there are no limitations as to the categories of Data Subjects which may have their Personal Data Processed via services provided by a CSP, France may again be considered as meeting this criterion, given that it is one of the most populated EU countries.

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

- The Austrian Österreichische Datenschutzbehörde;
- The Belgian Autorité de la Protection des Données;
- The Bulgarian Commission for Personal Data Protection;
• The Croatian *Personal Data Protection Agency*;
• The Cypriot *Commissioner for Personal Data Protection*;
• The Czech *Office for Personal Data Protection*;
• The Danish *Datatilsynet*;
• The Estonian *Data Protection Inspectorate (Andmekaitse Inspektsioon)*;
• The Finnish *Office of the Data Protection Ombudsman*;
• The German *Bundesbeauftragte für den Datenschutz und die Informationsfreiheit* (as well as the Supervisory Authorities of the several Länder which make up Germany\(^\text{17}\));
• The Greek *Hellenic Data Protection Authority*;
• The Hungarian *National Authority for Data Protection and Freedom of Information*;
• The Irish *Data Protection Commission*;
• The Garante;
• The Latvian *Data State Inspectorate*;
• The Lithuanian *State Data Protection Inspectorate*;
• The Luxembourg *Commission Nationale pour la Protection des Données*;
• The Maltese *Office of the Information and Data Protection Commissioner*;
• The Dutch * Autoriteit Persoonsgegevens*;
• The Polish *Urząd Ochrony Danych Osobowych*;
• The Portuguese *Comissão Nacional de Protecção de Dados*;
• The Romanian *National Supervisory Authority for Personal Data Processing*;

\(^{17}\) A list of these authorities is available at: [https://www.datenschutz-wiki.de/Aufsichtsbeh%C3%B6rdend_landesdatenschutzbeauftragte](https://www.datenschutz-wiki.de/Aufsichtsbeh%C3%B6rdend_landesdatenschutzbeauftragte).
• The Slovakian Office for Personal Data Protection;
• The Slovenian Information Commissioner;
• The Spanish Agencia Española de Protección de Datos; and
• The Swedish Datainspektionen.

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/services meet the potential Cloud Customer’s needs and compliance obligations. It could help to evaluate the level of Personal Data protection that a CSP would provide. For example, do the services provided by 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?18

3.1 Cloud Customer Internal Due Diligence

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

1. Defining its security, data protection and compliance requirements.
2. Identifying what data/processes/services it will want to move to the cloud.

18 For more on this issue, see the CSA Security Guidance.
3. Reviewing its own internal security and privacy/data protection policies and other restrictions on its use of Personal Data, such as pre-existing contracts, applicable laws and regulations, guide- lines and best practices.

4. Analysing and assessing risks (e.g., performing a DPIA to the extent required by Article 35 GDPR\(^\text{19}\)).

5. Identifying which security controls and certifications are required or useful to achieve adequate protection of its employees or Cloud Customers’ Personal Data while Processed in the cloud.

6. Defining responsibilities and tasks for security controls implementation (i.e., understand which security controls are under the direct governance of the organisation and which security controls are under the responsibility of the CSP).

7. Determining which activities of its service providers the entity should monitor and how (e.g., are onsite visits required, or is it sufficient to rely on a certification or attestation from a third party?).

### 3.2 Cloud Customer External Due Diligence

The Cloud Customer **may** also consider conducting a due diligence evaluation of the practices of the proposed CSP\(^\text{20}\). This may include, among other things:

1. Evaluating whether the services provided by the CSP - including the (sub)contractors/Sub-processors engaged - fulfil the Cloud Customer’s requirements with respect to privacy and data protection, using the Control Specifications: PLA.

\(^{19}\) See, for practical guidelines, the WP29 DPIA Guidelines.

\(^{20}\) Note that performing due diligence on CSPs, regardless of the adherence of their services to the CoC, is always recommended, under the GDPR’s principle of accountability – Cloud Customers remain ultimately responsible for entrusting a CSP with personal data, in any case. This means that Cloud Customers must make sure that a given CSP is appropriate for the processing activities which the Cloud Customers want to entrust to them (in terms of security, transfers of personal data, engagement of sub-contractors, etc.). This approach is taken also by relevant authorities providing assessment programs for CSPs – see, for example, the Canadian Centre for Cyber Security’s CSP IT Security Assessment Program (description available at: https://www.cyber.gc.ca/sites/default/files/publications/ITSE_50.060_0.pdf): “Note that while we review the CSP’s processes and existing controls, your organisation is responsible for determining your security requirements and ensuring that the CSP you choose to work with is capable of meeting those requirements. You can use the outputs of our assessment (e.g. summary reports) to help you make your decision.”
2. Determining whether the CSP holds any relevant certification or attestation based on an independent third-party assessment.\textsuperscript{21}

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

\textbf{4. EXPLANATORY NOTES}

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

Moreover, this Code may leave room, or point to other documents, for further clarification of specific subject and time frame of the cloud service to be provided, and the extent, manner and purpose of the Processing of Personal Data by the CSP, as well as the types of Personal Data that will be Processed. Such information should be gathered and agreed upon with the Cloud Customer.\textsuperscript{22}

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

The controls within Part 2 of the CoC require a CSP to demonstrate that it provides certain types of information to potential Cloud Customers and to comply with requirements set out for Cloud Customers’ benefit. This does not change the fact that the relationship created by this CoC is between CSA (as the CoC owner) and CSP (as the CoC member) – the CoC does not create a relationship between CSP and Cloud Customer\textsuperscript{23}. However, in this sense, the controls within Part 2 of the CoC are set up in a manner akin to a third-party beneficiary contract for the

\textsuperscript{21} See Articles 40 et seq. GDPR.
\textsuperscript{22} WP29 Cloud Computing Opinion, Section 3.4.2, p. 13.
\textsuperscript{23} Unless the CSP decides to incorporate the CoC into a contractual relationship with a Cloud Customer, as noted in the preceding paragraph.
B2B domain, whereby CSPs commit, towards CSA, to complying with obligations which are designed for the benefit of Cloud Customers and, ultimately, Data Subjects (the third-party beneficiaries).

It must be stressed that this construction is aimed at ensuring greater protection of Data Subjects in the cloud domain, in line with the GDPR and EU data protection legal framework. The greater the commitment made by CSPs to transparency and accountability towards actual and potential Cloud Customers, the greater the awareness of CSPs’ compliance posture for Cloud Customers – which, in turn, creates the conditions necessary for Cloud Customers to be able to afford a greater level of protection to the Personal Data for which they are responsible (thereby ensuring also protection to the Data Subjects to whom those Personal Data relate).

5. **GLOSSARY**

For definitions pertaining to legislative and other references used in this CoC, please refer to **Section 6.**, below.

For definitions pertaining to the CoC Technical Components and Governance Groups, please refer to **Part 3, Section 1.**, below.

“**Adherence Seal**” means a seal of conformity to the CoC, awarded to CSPs regarding a specific purpose for which they have sought adherence. As further clarified in **Part 3**, Adherence Seals have a limited validity, after which they must be renewed. Adherence Seals can be of two types, depending on the adherence mechanism used by the CSP: Self-attestation Adherence Seal, or Third-party Assessment Adherence Seal.

“**Automated Decision-making**” means the taking of decisions based solely on automated Processing, including by means of Profiling, which produce legal effects concerning a Data Subject or similarly significantly affect a Data Subject.

“**CJEU**” means the Court of Justice of the EU.

“**Cloud Customer**” means a B2B customer of the services provided by a CSP (i.e., a company, organisation or legal person, as opposed to a consumer).

“**CNIL**” means the Commission Nationale de l’Informatique et des Libertés, the Supervisory Authority for France.

“**CompSA**” means the lead Supervisory Authority for the CoC – the CNIL – with the competence laid out in Article 55 GDPR.

“**Concerned SA**” means a Supervisory Authority which is concerned by the Processing of Personal Data because (a) the Controller or Processor is established on the territory of the
Member State of that Supervisory Authority, (b) Data Subjects residing in the Member State of that Supervisory Authority are substantially affected or likely to be substantially affected by the Processing, or (c) a complaint has been lodged with that Supervisory Authority.

“Consent” means a freely given, specific, informed and unambiguous indication of a Data Subject’s wishes by which he or she, by a statement or a clear affirmative action, signifies agreement to the Processing of Personal Data related to him or her.

“Controller” means a natural or legal person, public authority, agency or other body which determines the purposes and means of the Processing of Personal Data. Where the purposes and means of such Processing are determined by EU or Member State law, the Controller or the specific criteria for its nomination may be provided for by EU or Member State law.

“CSA” means Cloud Security Alliance, the owner of the CoC.

“CSP” means a provider of cloud-based services (SaaS, IaaS or PaaS) which seeks to align one or more of those services with the criteria of the CSA CoC.

“Data Subject” means an identified or identifiable natural person. In turn, 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.

“DPA” or “Data Processing Agreement” means an agreement entered into between a Controller and a Processor, in order to regulate the Processing of Personal Data to be performed by the Processor on behalf of the Controller, as defined under Art. 28 GDPR.

“DPIA” or “Data Protection Impact Assessment” means a process designed to describe an intended Processing activity, assess its necessity and proportionality and help manage the risks to the rights and freedoms of natural persons resulting from the Processing of Personal Data, by assessing them and determining measures to address them, under Art. 35 GDPR.

“DPO” or “Data Protection Officer” means a person with expert knowledge of data protection law and practices, engaged to assist a Controller or Processor to monitor internal compliance with the GDPR and to perform all other tasks and duties set out in Arts. 37 to 39 GDPR, in an independent manner.

“EDPB” means the European Data Protection Board, the independent European body which contributes to the consistent application of data protection rules throughout the EU and promotes cooperation between the EU’s data protection authorities. The EDPB is composed of representatives of the national data protection authorities and of the EDPS.
“EDPS” means the European Data Protection Supervisor, the EU’s independent data protection authority, tasked with monitoring and ensuring the protection of Personal Data and privacy when EU institutions and bodies Process Personal Data, and other related tasks.

“EEA” means the European Economic Area.

“ENISA” means the European Union Agency for Cybersecurity, the EU body with a mandate to achieve a high common level of cybersecurity across the EU, including by actively supporting Member States, EU institutions, bodies, offices and agencies in improving cybersecurity, and which acts as a reference point for advice and expertise on cybersecurity for EU institutions, bodies, offices and agencies, as well as for other relevant EU stakeholders.

“EU” means the European Union.

“Garante” means the Garante per la Protezione dei Dati Personali, the Supervisory Authority for Italy.

“ICO” means the Information Commissioner’s Office, the Supervisory Authority for the United Kingdom.

“ISO” means the International Organisation for Standardization, an independent, non-governmental organization acting as an international standard-setting body, composed of representatives from various national standards organizations.

“Joint Controller” means a Controller which determines the purposes and means of the Processing of Personal Data jointly with other Controllers (one or more).

“Monitoring Body” refers to the internal committee established by CSA, which is tasked with the active and effective monitoring of adhering CSPs’ data protection practices.

“Personal Data” means any information related to a Data Subject.

“Personal Data Breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed.  

“Processing” (and variations, such as “Process” and “Processed”, when related to Personal Data) 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,

---

24 Article 4(12) GDPR.
disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

“Processor” means a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller.

“Profiling” means any form of automated Processing of Personal Data consisting of the use of Personal Data to evaluate certain aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

“Pseudonymisation” means the Processing of Personal Data in such a manner that the Personal Data can no longer be attributed to a specific Data Subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the Personal Data are not attributed to an identified or identifiable natural person.

“Recipient” means a natural or legal person, public authority, agency or other body, to which Personal Data are disclosed, whether a third party or not. However, public authorities which may receive Personal Data in the framework of a particular inquiry in accordance with EU or Member State law are not considered as “recipients”; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the Processing.

“Restriction of Processing” means the marking of stored Personal Data with the aim of limiting their Processing in the future.

“Special Categories of Personal Data” means Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data (when Processed for the purpose of uniquely identifying a natural person), data concerning health or data concerning a natural person’s sex life or sexual orientation.

"Substantial Change" means a change which materially affects the manner in which the CSP Processes Personal Data in connection with the service, such that the documents published on the STAR Registry for that CSP’s service no longer provide all relevant information needed for a Cloud Customer to make an accurate assessment of the CSP’s data protection posture.

“Sub-processors” means a natural or legal person, public authority, agency or other body which is engaged by a Processor to assist in the Processing of Personal Data on behalf of a Controller.

“Supervisory Authority” means an independent public authority which is established by an EU Member State pursuant to Article 51 GDPR.

“Third Country” means a country outside of the EU or European Economic Area.
“WP29” means the Article 29 Data Protection Working Party, the independent European working party that dealt with issues relating to the protection of privacy and Personal Data until 25 May 2018 (entry into application of the GDPR), at which point it was replaced by the EDPB.

6. LIST OF REFERENCES

EU Legislation (and legislative documents)

- 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 ("GDPR" or “General Data Protection Regulation”)\(^{25}\);
- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (“Data Protection Directive”)\(^{26}\);

CJEU

- Case C-362/14, Judgment of the Court (Grand Chamber) (6 October 2015) (“Schrems I Case”)\(^{30}\).

\(^{25}\) Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj.


\(^{28}\) Available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2017:0010:FIN.

\(^{29}\) Available at: https://eur-lex.europa.eu/eli/dir/2016/1148/oj.

• Case C-210/16, Judgment of the Court (Grand Chamber) (5 June 2018) ("Facebook Insights Case")\textsuperscript{31};
• Case C-40/17, Judgment of the Court (Grand Chamber) (29 July 2019) ("Fashion ID Case")\textsuperscript{32};
• Case C-311/18, Judgment of the Court (Grand Chamber) (16 July 2020) ("Schrems II Case")\textsuperscript{33}.

Cloud Accountability Project
• D38.2 Framework of evidence (final) ("CAP Framework of Evidence")\textsuperscript{34}.

CNIL
• Decision 2014-298 (7 August 2014) ("CNIL Orange Decision")\textsuperscript{35};
• Recommendations for companies planning to use Cloud computing services ("CNIL Cloud Recommendations")\textsuperscript{36};
• Délibération n° 2020-050 portant adoption d’un référentiel relatif à l’agrément des organismes chargés de contrôler le respect des codes de conduit (30 April 2020) ("CNIL Accreditation Requirements")\textsuperscript{38}.

CSA
• Security Guidance for Critical Areas of Focus in Cloud Computing v4.0 ("CSA Security Guidance")\textsuperscript{39};
• Cloud Controls Matrix v.3.0.1 ("CSA Cloud Controls Matrix")\textsuperscript{40}.

EDPB

\textsuperscript{31} Available at: http://curia.europa.eu/juris/liste.jsf?num=C-210/16.
\textsuperscript{32} Available at: http://curia.europa.eu/juris/liste.jsf?num=C-40/17.
\textsuperscript{33} Available at: http://curia.europa.eu/juris/liste.jsf?num=C-311/18.
\textsuperscript{34} Available at: http://cloudaccountability.eu/sites/default/files/D38.2%20Framework%20of%20Evidence%20%28final%29.pdf.
\textsuperscript{35} Available at: https://www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000029406662&fastReqId=1788142702&fastPos=1.
\textsuperscript{36} Available at: https://www.cnil.fr/sites/default/files/typo/document/Recommendations_for_companies_planning_to_use_Cloud_computing_services.pdf.
\textsuperscript{37} Available at: https://www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle_gb_web.pdf.
\textsuperscript{38} Available at: https://www.cnil.fr/sites/default/files/atoms/files/referentiel-agrement_-code-de-conduite_0.pdf.
\textsuperscript{39} Available at: https://cloudsecurityalliance.org/research/guidance/.
\textsuperscript{40} Available at: https://cloudsecurityalliance.org/research/working-groups/cloud-controls-matrix/.
• Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679 (25 May 2018) (“EDPB Transfer Derogation Guidelines”)41;
• Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679 (12 February 2019) (“EDPB CoC Guidelines”)42;
• Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 – Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems (23 July 2020) (“EDPB Schrems II FAQ”)43.

EDPS
• Guidelines on personal data breach notification for the European Union Institutions and Bodies (21 November 2018)” (“EDPS Data Breach Guidelines”)44;
• Data Protection Glossary (“EDPS Glossary”)45.

ENISA
• Recommendations for a methodology of the assessment of severity of personal data breaches (20 December 2013) (“ENISA Breach Severity Assessment Recommendations”)46;
• Technical Guidelines for the implementation of minimum security measures for Digital Service Providers (16 February 2017) (“ENISA Technical Guidelines”)47.

European Commission
• Cloud Service Level Agreement Standardisation Guidelines (26 June 2014) (“EC Cloud SLAS Guidelines”)48;

Garante

42 Available at: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201901_v2_0_codesofconduct_en.pdf.
44 Available at: https://edps.europa.eu/sites/edp/files/publication/18-12-14_edps_guidelines_data_breach_en.pdf.
46 Available at: https://www.enisa.europa.eu/publications/dbn-severity.
47 Available at: https://www.enisa.europa.eu/publications/minimum-security-measures-for-digital-service-providers.
49 Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L__2016.207.01.0001.01.ENG.

ICO

International Working Group on Data Protection in Telecommunications

ISO
• ISSO/IEC 17021, Conformity assessment — Requirements for bodies providing audit and certification of management systems (“ISSO 17021”)53;
• ISSO/IEC 17065:2012, Conformity assessment — Requirements for bodies certifying products, processes and services (“ISSO 17065”)54;
• ISSO/IEC 27001:2013, Information technology — Security techniques — Information security management systems — Requirements (“ISSO 27001”)55;

National Cyber Security Centre (UK)

50 Available at: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1895296&DOWNLOAD=true.
51 Available at: https://ico.org.uk/media/for-organisations/documents/1540/cloud_computing_guidance_for_organisations.pdf.
53 Part 1 available at: https://www.iso.org/standard/61651.html. The remaining parts (2 to 12) can be found at: https://www.iso.org/standards-catalogue/browse-by-ics.html.
54 Available at: https://www.iso.org/standard/46568.html.
55 Available at: https://www.iso.org/standard/54534.html.
56 Available at: https://www.iso.org/standard/43757.html.
57 Available at: https://www.iso.org/standard/61498.html.
58 Available at: https://www.ncsc.gov.uk/collection/cloud-security/implementing-the-cloud-security-principles.
WP29

• Opinion 1/2010 on the concepts of “controller” and “processor” (16 February 2010) ("WP29 Controller/Processor Opinion")59;
• Opinion 2/2010 on online behavioural advertising (22 June 2010) (“WP29 Online Behavioural Advertising Opinion”)60;
• Opinion 05/2012 on Cloud Computing (1 July 2012) (“WP29 Cloud Computing Opinion”)61;
• Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes (10 April 2014) (“WP29 Electronic Communications Surveillance Opinion”)62;
• Guidelines on the right to data portability (5 April 2017) (“WP29 Portability Guidelines”)63;
• Guidelines on Data Protection Officers (‘DPOs’) (5 April 2017) (“WP29 DPO Guidelines”)64;
• Guidelines for identifying a controller or processor’s lead supervisory authority (5 April 2017) (“WP29 Lead Supervisory Authority Guidelines”)65;
• Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679 (3 October 2017) (“WP29 Administrative Fine Guidelines”)66;
• Guidelines on Data Protection Impact Assessments (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679 (4 October 2017) (“WP29 DPIA Guidelines”)67;
• Guidelines on personal data breach notification under Regulation 2016/679 (6 February 2018) (“WP29 Data Breach Guidelines”)68;
• Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (6 February 2018) (“WP29 Automated Decision-making Guidelines”)69;

62 Available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237.
63 Available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233.
64 Available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048.
65 Available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612035.
66 Available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237.
67 Available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.
68 Available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052.
69 Available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053.
• Guidelines on transparency under Regulation 2016/679 (11 April 2018) ("WP29 Transparency Guidelines")\(^70\);
• Position Paper on the derogations from the obligation to maintain records of processing activities pursuant to Article 30(5) GDPR (19 April 2018) ("WP29 Records Position Paper")\(^71\).

\(^70\) Available at: [https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227](https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227).

\(^71\) Available at: [https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=624045](https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=624045).
PART 2
CSA CoC CONTROL
SPECIFICATIONS: PRIVACY LEVEL AGREEMENT
The CSP declares to the Cloud Customers and ensures:

1. To comply with the applicable EU data protection law, specifying any sector-specific or local legislation/requirements directly applicable to the CSP with which they are compliant, and with the terms of this CoC, also with respect to technical and organisational security measures, and to safeguard the protection of the rights of the Data Subject. Where there is a material change in applicable EU data protection law which may imply new or conflicting obligations regarding the terms of this CoC, the CSP commits to complying with the terms of the applicable EU data protection law.

**Relevance:** By providing such a declaration, CSPs extend what is already a legal obligation – i.e., to comply with EU data protection law, including applicable sector-specific or local legislation/requirements.
specific legislation – by means of an additional commitment to complying with the terms of this CoC. If changes in EU data protection law imply a conflict with the CoC, the CSP commits to complying with EU data protection law (regardless of the fact that the CoC will be promptly revised to meet the new legal standards, following the processes described further in Part 3). The CoC exists independently and alongside any Data Processing Agreements which an adhering CSP may have entered into with its Cloud Customers. Adhering to the CoC creates an obligation for the CSP to comply with its terms, lest its Adherence Seal under the CoC be removed or suspended.

This control requires CSPs to have made a declaration to Cloud Customers of their compliance with both:

- The applicable EU data protection law, including applicable sector-specific legislation; and

- The terms of this CoC.

As an alternative regarding the declaration of compliance with the terms of this CoC (and NOT the declaration of compliance with applicable EU data protection law), CSPs may provide a commitment to make such a declaration to Cloud Customers after adherence to the CoC has been approved.

Certain jurisdictions may impose additional requirements for the lawful Processing of Personal Data (or of certain types of Personal Data) applicable (also, or exclusively) to CSPs. The CoC requires CSPs to transparently describe to Cloud Customers any such sector-specific or local requirements which the CSP’s service meets, so that the Cloud Customer can assess the terms under which it can lawfully procure that CSP’s service.

2. To be able to demonstrate compliance with the applicable EU data protection law and with the terms of this CoC (accountability), as well as with the sector-specific or local legislation/requirements indicated under Control no. 1.1.

**Relevance:** In this manner, CSPs guarantee that they will be able, at any time, to prove that they comply with their legal obligations, as well as their additional obligations under this CoC, for the benefit of Cloud Customers and Data Subjects, which are thus

---

72 This includes local legislation imposing requirements on CSPs in order to be able to lawfully Process certain types of Personal Data, such as the requirement for HDS (Hébergeur de Données de Santé) certification imposed by the French Public Health Code.

73 See, in this respect, the fundamental principle of “accountability” reflected in Article 28(3)(h) GDPR.
empowered to ask for tangible evidence of compliance from the CSPs they engage (see also below controls, as well as Control no. 3.5.9., Control no. 4., Control no. 7. and Control no. 12.2., below, for specifications of this).

This control requires CSPs to have made a declaration to Cloud Customers that they are able to not only comply, but also **demonstrate** their compliance with:

- The applicable EU data protection law;
- The terms of this CoC; and
- The sector-specific or local requirements with which the CSP declares its service is compliant (as required by Control no. 1.1., above).

As an alternative regarding the declaration of the ability to demonstrate compliance with the terms of this CoC (and NOT the same declaration regarding compliance with applicable EU data protection law, or the sector-specific/local requirements mentioned), CSPs may instead provide a commitment to make such a declaration to their Cloud Customers after adherence to the CoC has been approved.

The CSP must have in place, and describe to the Cloud Customers:

3. The elements that can be produced as evidence to demonstrate such compliance.\(^{74,75}\)

Elements to meet each of the following levels must be clearly indicated:

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

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

iii. **Operations level**, to demonstrate that systems are behaving (or not) as planned.

---

\(^{74}\) See definition of accountability in the EDPS Glossary: “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.”

\(^{75}\) The WP29 Cloud Computing Opinion, 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”.
Relevance: This control further specifies Control no. 1.2., above, by establishing specific forms in which CSPs may produce evidence of their compliance to Cloud Customers. It covers also the subject-areas which must be addressed by this evidence, to provide a complete and clear picture to Data Subjects – i.e., compliance regarding the CSP’s organizational policies, IT controls and practical operations.

For clarity:

- Evidence at **Organisational policies level** can be defined as documentation and procedures showing that policies, aligned with relevant legal and regulatory obligations and standards, have been established, documented, approved, communicated and/or implemented by the CSP, and are enforced and maintained in relation to the service in question.

- Evidence at **IT controls level** can be defined as documentation showing that policies, procedures and/or tools associated with technical controls designed to reduce the security risks associated with IT system use have been implemented by the CSP, and are enforced and maintained in relation to the service in question.

- Evidence at **Operations level** can be defined as “collection of data, metadata, routine information and formal operations performed on data and metadata which provide attributable and verifiable account of the fulfilment of relevant obligations with respect to the service and that can be used to support an argument shown to a third party about the validity of claims about the appropriate and effective functioning (or not) of an observable system”.

Evidence elements can take different forms, such as self-certification/attestation, third-party audits (e.g., certifications, attestations, and seals), logs, audit trails, system maintenance records, or more general system reports and documentary evidence of all Processing operations under its responsibility. Examples of evidence elements

---

76 See the CAP Framework of Evidence, p. 2.
77 See the WP29 Cloud Computing Opinion, Section 4.2, p. 22: “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.”.
78 E.g., CSA STAR certification, ISO 27001 certification (possibly augmented with the controls from ISO 27018),
79 E.g., CSA STAR Attestation, SOC 2 attestation.
pertaining to different levels also include data protection certifications, seals and marks.\textsuperscript{80}

In particular, concerning the **Organisational policies level**, CSPs must clearly describe to Cloud Customers what policies and procedures the CSP has in place to ensure and demonstrate compliance by the CSP itself and its Sub-processors (see also **Control no. 3.3.**, below) or business associates, with the applicable EU data protection law and with the terms of this CoC. Providing Cloud Customers with the CSP’s internal policies and procedures on the protection of Personal Data is a fundamental step in empowering Cloud Customers to selecting a CSP which they consider will handle the Personal Data for which they are responsible in an appropriate manner, thereby complying with the internationally recognized data protection principle of transparency. Furthermore, these policies and procedures should accurately describe to Cloud Customers how compliance will be demonstrated, both with respect to the CSP, as well as its subcontractors and business associates engaged to provide services (thereby offering reassurance over the entire Processing chain used).

Examples of policies and procedures which CSPs should consider implementing (and describing to Cloud Customers) include policies and procedures on:

- Retention of Personal Data;
- Compliance with GDPR/EU data protection principles (including legal basis for Processing Personal Data);
- Data protection by design and by default;

\textsuperscript{80} 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 the WP29 Cloud Computing Opinion, Section 3.4.2, p. 14. See also Article 17(2) of the Data Protection Directive and the WP29 Cloud Computing Opinion, Section 3.4.3, p. 14 and Section 3.4.4.7. See also, e.g., the CNIL Cloud Recommendations, p. 12: “\textit{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.”
• Management of Personal Data Breaches (including a procedure to assess Personal Data Breach severity);
• Engagement of Sub-processors;
• Management of persons authorised by a CSP to handle Personal Data on its behalf;
• Data Subject requests;
• Acceptable use of IT tools;
• Information security;
• Transfers of Personal Data;
• DPIAs;
• The appointment, tasks and duties of the DPO (where relevant);
• Cooperation with Supervisory Authorities;
• Privacy risk assessments (to gauge the impact that a Processing activity may have upon the rights, freedoms and legitimate interests of Data Subjects).

2. **CSP RELEVANT CONTACTS AND ITS ROLE**

The CSP must specify to the Cloud Customers:

1. The CSP’s identity and contact details (e.g., name, address, email address, telephone number and place of establishment);

**Relevance:** This control requires CSPs to correctly identify the legal entity which will be responsible not only for providing the services, but for ensuring that the services provided are and remain compliant with applicable data protection legislation. CSPs must also provide contact details which Cloud Customers can use to reach them.
2. The identity and contact details (e.g., name, address, email address, telephone number and place of establishment) of the CSP’s local representative(s) (e.g., a local representative in the EU);\(^{81}\)

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

CSPs must either identify an EU-based affiliate which is tasked with handling any data protection-related issues or inquiries for the EU, or otherwise identify a representative appointed for the CSP under Article 27 GDPR (where applicable).

3. The CSP’s data protection role for each of the relevant Processing activities inherent to the services and under the scope of the CoC (i.e., Processor or Sub-processor);\(^{82}\)

---

\(^{81}\) 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.”

\(^{82}\) The WP29 Cloud Computing Opinion 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 the CSA’s opinion, the respective roles need to be carefully assessed on a case-by-case basis, as also confirmed by the ICO Cloud Computing Guidance, p. 7. In this respect, see the 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.”; see also the WP29 Cloud Computing Opinion, 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”; see also the CNIL Cloud Recommendations, pp. 5-6: “When a customer uses a
Relevance: It is fundamental, in practice, for both parties to understand and agree upon the roles that they perform in the Personal Data Processing relationship inherent to the provision of the services, given the significantly different practical implications and legal obligations for a party depending on the role it plays. Therefore, CSPs are required to perform their own assessments in light of the services they provide and communicate the roles which they understand as applicable to them to Cloud Customers, in order to allow these Cloud Customers to understand what to expect and what they can demand from CSPs (noting that, in the cases covered by this CoC, CSPs will act as Processors/Sub-processors on behalf of their B2B Cloud Customers).

Further guidance on different activities which may, generally, fall under the role of Processor or Sub-processor, is provided in the WP29 Controller/Processor Opinion, and below:

- **Processor**: if a CSP does not determine the purpose for which a Personal Data Processing Activity is carried out, and instead only executes an activity in accordance with instructions given by the Cloud Customer (in a service agreement, a Data Processing Agreement, in ad hoc instructions given during the course of service provision, or otherwise), the CSP will typically act as a Processor for that activity. Typical examples include the use of Cloud Customer data which is strictly necessary to provide the service to the Cloud Customer, or to address a data-related request made by a Cloud Customer (such as restricting the Processing of certain data, erasing or rectifying certain data, etc.).

- **Sub-processor**: CSPs which qualify as Processors may also be called Sub-processors, if the Cloud Customer in question does not act as a Controller for a given Processing activity. In this sense, if a CSP’s Cloud Customer is not a Controller for an activity (and instead acts as a Processor, performing that activity on behalf of one of its own Cloud Customers, for example), the CSP will be a “Processor of a Processor” (or 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, as noted in the Garante Cloud Computing Guide, pp. 14-15. See also the ICO Cloud Computing Guidance, pp. 7-9, on the privacy roles in different cloud service deployment models.
Sub-processor) for the activity in question. For the purposes of the CoC, it makes no difference whether a CSP is a Processor or a Sub-processor – all controls apply without distinction to both. One example of this is where an IaaS/PaaS CSP Processes Personal Data in connection with the offering to other CSPs of the possibility to host services on their infrastructure/platform, which in turn will be used to Process Personal Data on behalf of those CSPs’ B2B end-customers.

4. The contact details of the CSP’s DPO or, if there is no DPO, the contact details of the individual in charge of privacy matters to whom the Cloud Customer may address requests;

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

CSPs must provide this information by means of public-facing documentation (e.g., publicly-available privacy policy, proposed Data Processing Agreement or service agreement, FAQs, etc.).

5. The contact details of the CSP’s Information Security Officer (ISO) or, if there is no ISO, the contact details of the individual in charge of security matters to whom the Cloud Customer may address requests.

Relevance: Given that CSPs may segregate internal roles related to privacy and information security (e.g., by having separate individuals acting as DPO / privacy contact and ISO / security contact), and that more technical security matters raised by Cloud Customers might be better handled by the CSP’s ISO (or equivalent function – “security contact”), the CoC requires CSPs to disclose their contact details for this individual, in order to ensure a correct and swift resolution of any concerns related more precisely to technical and organisational security measures raised by Cloud Customers.

CSPs must provide this information by means of public-facing documentation (e.g., publicly-available privacy policy, proposed Data Processing Agreement or service agreement, FAQs, etc.).

---

83 See Article 13(1)(b) GDPR and Articles 37 et seq. GDPR. Moreover, see the WP29 DPO Guidelines.
3. **WAYS IN WHICH DATA WILL BE PROCESSED**

3.1 **Instructions**

CSPs must provide to Cloud Customers details on:

1. The extent and modalities in which the Cloud Customer can issue its binding instructions to the CSP.\(^{84}\)

**Relevance:** This control addresses the important matter of how Cloud Customers can issue instructions to CSPs. Given that, in the cloud computing domain, it is typical for terms of service and associated contractual documentation to be defined unilaterally by the CSP, it is important that this specific point is clearly addressed in the information given to Cloud Customers, so that Cloud Customers will be in a position to confirm upfront whether the terms offered by the CSP are aligned with Art. 28 GDPR. This requirement goes beyond what is strictly needed under the GDPR, in that it obliges CSPs to detail how and to what extent Cloud Customers will be able to instruct the CSP regarding the use of the Personal Data provided, and ties in to the declarations and commitments made under **Control no. 1.1.**, above – given that CSPs are legally obliged to comply with Cloud Customers’ instructions regarding Personal Data Processing, this control requires CSPs to delve deeper into the details of how this obligation will be performed, by clearly informing Cloud Customers of how they will be able to exercise this right.

If Cloud Customers are limited to the instructions set out in contractual arrangements with the CSP, in that they cannot issue further instructions than those set out in the

---

\(^{84}\) See Articles 28 and 29 GDPR. See also the WP29 Cloud Computing Opinion, 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,”, as well as the Sopot Memorandum, p. 4. See also the ICO Cloud Computing 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.”
service agreement, Data Processing Agreement, privacy policy or other documents, then this should be clearly indicated to Cloud Customers.

### 3.2 Changes to the service

The CSP must specify to Cloud Customers:

1. How the Cloud Customers will be informed, in written form, about relevant changes concerning relevant cloud service(s), such as the implementation or removal of functions.\(^{85}\)

**Relevance:** This control arguably exceeds the requirements of the GDPR, born out of the WP29’s recommendations in the WP29 Cloud Computing Opinion\(^ {86}\). There, WP29 stresses that, to ensure legal certainty, CSPs must provide certain safeguards in the contracts they sign with Cloud Customers, among which is the obligation to inform Cloud Customers where relevant changes are to be implemented in the services provided, such as the addition of functions to those services. This control goes beyond WP29’s recommendations, by expressly identifying also the removal of functions as a relevant change to be communicated to Cloud Customers.

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

Examples of means by which these communications can be made to Cloud Customers (which should be stipulated in the service agreement entered into between CSP and Cloud Customer) include e-mail, publishing a message/notification on a dashboard provided to the Cloud Customer within the service, updating a service changelog, etc.

---

\(^{85}\) WP29 Cloud Computing Opinion, Section 3.4.2, p. 13. See also the ‘Legal’ Section of ICO Cloud Computing Guidance’s checklist, p. 22: “How will the cloud provider communicate changes to the cloud service which may impact on your agreement?” Note that CSPs may need to have changes approved by customers, and failure to do so may result in the CSP acting as controllers (see the WP29 Controller/Processor Opinion).

3.3 Personal Data location

The CSP must specify to Cloud Customers:

1. The location(s) of all data centres or other Personal Data Processing locations (by country) where Personal Data may be Processed, and in particular, where and how data may be stored, mirrored, backed up, and recovered (this may include both digital and non-digital means).

The CSP must also:

2. Notify Cloud Customers of any intended changes to these locations once a contract has been entered into, in order to allow the Cloud Customer to acknowledge or object.

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

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

Cloud Customers should also be informed when changes of location are to take place after the performance of services has begun, and allowed to acknowledge or object to these changes. In the event that an objection cannot be resolved, the Cloud Customer

---

87 WP29 Cloud Computing Opinion, Section 3.4.1.1, p. 11 and Section 3.4.2, p. 13. See also the principle of ‘location transparency,’ in the Sopot Memorandum, p. 4 and the CNIL Cloud Recommendations, p. 14. See also the ‘Legal’ Section of the ICO Cloud Computing Guidance’s 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?”
must be entitled to terminate the contract. In this case, the Cloud Customer and CSP must agree on a transitional period during which the CSP will continue to provide a set level of services to the Cloud Customer, while the Cloud Customer procures a suitable alternative to the services offered by the CSP, in order to prevent damages which may occur from an abrupt end to the provision of services for the Cloud Customer (e.g., sudden lack of availability of Personal Data).

When notifying an intended change of Processing location to a Cloud Customer, CSPs must ensure that they provide the following information:

- Intended new Processing location(s) – the specific country(ies) must be identified;
- Reasons for the change of Processing location;
- Whether or not this involves a change of Sub-processors (if so, the requirements of Control no. 3.3., below, must also be considered);
- The foreseen timing for the change to be completed;
- The possibility for the Cloud Customer to object, with reference to the service agreement, Data Processing Agreement or other agreement in which this is regulated, explaining also the terms under which objection can be carried out and the possible consequences for objection.

CSPs remain free to determine the means by which they will provide these notifications to Cloud Customers, within the service agreement, Data Processing Agreement or other agreement in which this is regulated. However, they must ensure that such means effectively allow the Cloud Customer to become aware of notifications and object to proposed changes of location in a timely manner – in other words, the means chosen cannot compromise the objectives aimed at by this Control.
3.4 Sub-processors

The CSP must identify, for Cloud Customers:

1. Sub-processors that participate in the Personal Data Processing, along with the chain of accountabilities and responsibilities used to ensure that data protection requirements are fulfilled.\(^8^8\)

The CSP declares to Cloud Customers, and further ensures, that:

2. The CSP will not engage any Sub-processor without prior specific or general written authorization of the Cloud Customer.\(^8^9\)

The CSP declares to Cloud Customers, and further ensures, that the CSP:

3. Imposes on Sub-processors the same (or, at least, substantially equivalent) data protection obligations stipulated between the CSP and the Cloud Customer, by way of a contract (or other binding legal act), and will only engage Sub-processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the Processing will meet the requirements of applicable EU law.

4. Will, upon request, disclose to the Cloud Customer the contracts (or other binding legal acts) entered into between the CSP and its Sub-processors (in full, or in part), in order to demonstrate that the requirements of Control no. 3.4.3., above, have been met.

5. Remains fully liable to the Cloud Customer for the performance of Sub-processors’ obligations, in case the Sub-processors fail to fulfil their data protection obligations.

The CSP must have in place, and describe to Cloud Customers:

6. the procedures used to inform the Cloud Customer of any intended changes concerning the addition or replacement of Sub-processors, with Cloud Customers retaining at all times the possibility to object to such changes or

---

\(^8^8\) See the concept of “layered services” in the ICO Cloud Computing Guidance, pp. 6-8.

\(^8^9\) See Article 28(2) GDPR.
terminate the contract.\textsuperscript{90} In the event of termination by the Cloud Customer, the Cloud Customer must be afforded sufficient time to procure an alternative CSP or solution (by establishing a transition period during which an agreed-upon level of services will continue to be provided to the Cloud Customer, under the contract).

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

CSPs wishing to engage Sub-processors should either obtain from Cloud Customers a specific authorisation for this (in which specifically identified Sub-processors are approved by the Cloud Customer, with future engagements being subjected to Cloud Customer approval) or a general authorisation for this (in which Cloud Customers generally accept the use of Sub-processors, subject to prior notification to the Cloud Customer before any future engagement, so that they may object if willing).

Given the practical difficulties that may arise in enforcing the exact same data protection obligations between a CSP and its Sub-processors as exist between a CSP and its Cloud Customers, a general practice in the cloud domain is for the CSP to commit, at least, to imposing substantially equivalent data protection obligations upon those Sub-processors (remaining, naturally, fully liable for any breach of its own obligations towards the Cloud Customer that may be caused by a disparity between those obligations, and those by which the CSP’s Sub-processors have been bound). This approach is bolstered by the CoC’s emphasis on the need for CSPs to only engage Sub-processors which the CSP deems as providing sufficient guarantees of having implemented appropriate technical and organisational measures, in such a manner that their Processing of Personal Data will be compliant with applicable EU data protection law.

\textsuperscript{90} WP29 Cloud Computing Opinion, Section 3.3.2, p. 10: “There should also be clear obligation of the cloud provider to name all the subcontractors commissioned (e.g., in a public digital register).”, Section 3.4.2, p. 13, and also Section 3.4.1.1, pp. 10-11. See further the ICO Cloud Computing Guidance, p.11, and Article 10 of the Data Protection Directive.
Furthermore, the CoC imposes upon CSPs obligations related to the “cascade of liability” (i.e., to assume full liability to the Cloud Customer for the performance of their Sub-processors), and to notify the Cloud Customer of any intended addition or replacement of Sub-processors, allowing Cloud Customers to object (in line with the general authorisation given) or refuse to authorise this change – ultimately, a stalemate here (where the Cloud Customer and CSP cannot agree on how to resolve an objection) must allow the Cloud Customer (and not the CSP) to terminate the agreement, providing the Cloud Customer sufficient time to adjust to the changes required.

When notifying an intended change, concerning the addition or replacement of Sub-processors, to a Cloud Customer, CSPs must ensure that they provide the following information:

- Legal name of the intended new Sub-processor(s);
- The specific country(ies) where the new Sub-processor(s) will Process Personal Data on behalf of the CSP;
- The role which each new Sub-processor will play in the Processing of the Cloud Customer’s Personal Data;
- The possibility for the Cloud Customer to object, with reference to the service agreement, Data Processing Agreement or other agreement in which this is regulated, explaining also the terms under which objection can be carried out and the possible consequences for objection.

While this control seeks to ensure that Cloud Customers are afforded with enough information to fully understand the chain of Sub-processors which a CSP may rely on to provide a service, it will not apply if no such Sub-processors are, or will be engaged by a CSP. In this case, it should nonetheless be made clear to Cloud Customers that no such Sub-processors are, or will be engaged.

### 3.5 Installation of software on Cloud Customer’s system

The CSP must indicate to Cloud Customers:

1. Whether the provision of the service requires the installation of software on the Cloud Customer’s system (e.g., browser plug-ins).
2. The software’s implications from a data protection and data security point of view.\textsuperscript{91}

\textbf{Relevance:} This control is supported by a similar justification to Control no. 3.1.15., above, in that requiring software to be installed on Cloud Customers’ systems for services to be provided can have an impact on the Cloud Customers’ data governance (e.g., where this may imply an additional collection or transfer of data), and is also born out of the WP29 Cloud Computing Opinion\textsuperscript{92}. Note that, although WP29 states that Cloud Customers should raise this matter ex ante (where not sufficiently addressed by the CSP), the CoC eliminates the need for this by requiring all CSPs to disclose implications for any software to be installed, from a data protection and data security point of view (such as whether any additional data will be collected, transferred or retained by the CSP via this software, and what security measures the software is subjected to, in as much detail as needed for Cloud Customers to understand how relevant this installation may be from a compliance perspective).

The information provided should cover any additional Personal Data Processing activities which may take place due to that software needing to be installed (e.g., if third-party software is needed, a link to that third party’s privacy policy or privacy-related public documents should be provided), as well as meaningful information about the security measures which this additional software is subjected to. Cloud Customers should be able to understand what consequences installing such additional software may have for them and their Data Subjects, from these two perspectives.

If the installation of software is optional (not necessary for the service to be provided, as there are functional alternatives which do not require installation of software, such as browser-based solutions), the above information does not necessarily need to be made available to Cloud Customers prior to the engagement of the CSP (though this is still a recommended best practice for CSPs). However, the CSP should still ensure that Cloud Customers wishing to install such software are able to access all of this information before installation takes place.

\textsuperscript{91} WP29 Cloud Computing Opinion, Section 3.4.1.1, p. 11.
\textsuperscript{92} WP29 Cloud Computing Opinion, p. 11.
3.6 Data Processing Agreement (or other binding legal act)

The CSP must share and execute with the Cloud Customers:

1. A proposed Data Processing Agreement (or other binding legal act) to govern the Processing carried out by the CSP on behalf of the Cloud Customer and set out the subject matter and duration of the Processing, the type of Personal Data and categories of Data Subjects and the obligations and rights of the Cloud Customer. The Data Processing Agreement or other legal act must stipulate, in particular, that the CSP will do the following:

2. Process Personal Data only upon documented instructions from the Cloud Customer, including with regard to transfers of Personal Data to a third country or an international organisation, unless required to do so by EU 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;

3. Ensure that persons authorised to Process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality, and that they do not Process Personal Data except upon instructions from the Cloud Customer, unless otherwise required by EU or Member State law;93

4. Undertake that all persons authorised to Process the Personal Data have received appropriate training, at least on an annual basis, on privacy, data protection and data security matters, in particular related to the specific risks arising from the Processing inherent to the provision of the service;

5. Implement all technical and organizational security measures which the CSP deems adequate, in light of the available technology, the state of the art, the costs in implementing those measures and the Processing activities inherent to the services provided, to ensure that the CSP’s services are covered by a level of security which is appropriate, considering the potential risks to the interests, rights and freedoms of Data Subjects;94

93 See Article 32(4) GDPR.
94 See Article 32 GDPR.
6. Respect the conditions laid down in this CoC for engaging Sub-processors95 (see Control no. 3.3., above);

7. Taking into account the nature of the Processing, assist the Cloud Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Cloud Customer’s obligation to respond to requests for exercising the Data Subject’s rights;96

8. Assist the Cloud Customer in ensuring compliance with obligations related to security of Processing,97 notification of a Personal Data Breach to the Supervisory Authority,98 communication of a Personal Data Breach to the Data Subject,99 and DPIA;100 taking into account the nature of Processing and the information available to the CSP;

9. At the choice of the Cloud Customer, delete or return all Personal Data to the Cloud Customer after the end of the provision of services relating to Processing; and delete existing copies unless EU or Member State law requires storage of the Personal Data; (see Control no. 11., below);

10. 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 Cloud Customer.

Relevance: This control is a formal requirement, seeking, as a first goal, to reproduce the formal obligations contained within Art. 28 GDPR, in order to ensure that all contracts entered into by CSPs with Cloud Customers will meet the minimum legal requirements. However, the CoC goes beyond this, by not only reaffirming these requirements but also further specifying them – as seen, e.g., in the commitment to respect the conditions required in order to engage Sub-processors (wherein the CoC, under Control no. 3.3., above, imposes upon CSPs the obligation to provide clear and transparent information on their entire Processing chain – both initially and regarding any subsequent intended changes – and to offer Cloud Customers the ability to

---

95 See Article 28(2) and 28(4) GDPR.
96 See Chapter III GDPR.
97 See Article 32 GDPR.
98 See Article 33 GDPR.
99 See Article 34 GDPR.
100 See Article 35 GDPR.
terminate the agreement in the event that their objection to a change in Sub-processors cannot be resolved) and in the requirement to delete or return all Personal Data to Cloud Customers after services have ended (which, under Control no. 11.4., below, also obliges CSPs to offer information as to the methods in place to delete or return the data).

CSPs are required to propose their Data Processing Agreement to Cloud Customers. Such Data Processing Agreement is, effectively, an agreement which can be proposed by one party (the CSP) and might be accepted by the other (Cloud Customer). Its acceptance and/or modification will be a matter for negotiation between the parties; considering that the CoC applies only to B2B scenarios, this should allow CSPs and Cloud Customers to reach a mutually satisfactory (or, at least, acceptable) agreement in this regard. By proposing its own Data Processing Agreement, the CSP also informs Cloud Customers of terms which it deems commercially acceptable upfront – Cloud Customers may more readily enter into agreements with CSPs if they also find those terms acceptable.

While it is true that a CSP will not be able to determine the purposes of Processing, and therefore cannot propose a complete Data Processing Agreement to Cloud Customers (as it may not always be aware of the categories of Personal Data / Data Subjects which will be concerned by the Cloud Customer’s use of the CSP’s service), it may still provide the core terms regulating a Personal Data Processing relationship with Cloud Customers (including and expanding on the obligations of Art. 28(3) GDPR’s subparagraphs), in particular the duration of Processing and obligations/rights of the Cloud Customer and CSP. More specific terms which must be determined by the Cloud Customer (as Controller, or main Processor), such as the types of Personal Data and Data Subjects concerned, may be specifically inserted into an annex to the proposed Data Processing Agreement for each Cloud Customer, to be filled out by the Cloud Customer itself. This is, in any case, a typical approach followed by several CSPs at present.

The engagement of Sub-processors should be regulated even if the CSP does not require this engagement in order to provide the service (e.g., by including a commitment to the effect that no such Sub-processors will be engaged by the CSP).

Concerning CSPs’ contractual obligations to make available all information necessary to demonstrate data protection compliance, as well as allow for and contribute to audits/inspections, it is standard practice within the cloud domain to allow Cloud Customers to have access to reports of audits carried out by independent and qualified third parties, rather than providing direct access to the CSPs’ systems, equipment or facilities used to Process Personal Data. These third-party audits must be regularly carried out by CSPs, with a frequency which is adequate to their nature and purpose.
The best practice in this regard, which is also the generally-recognised rule for certification and attestation audits, is to set at least an annual frequency for these audits, and to carry out additional *ad hoc* audits in the event of a substantial or relevant change to the target of the audit.

### 3.7 Data protection by design and by default

1. CSPs must have in place, and describe to Cloud Customers, available evidence of technical and organisational measures (including, where relevant, data protection enhancing techniques) **incorporated into the design of the service**, which include specific training sessions for persons authorised to Process Personal Data, at least annually, to address and implement each of the below principles:

   **i. Lawfulness**: The Processing of Personal Data must be done for a legitimate purpose (or purposes), and a suitable legal basis for each Processing purpose under applicable EU data protection law must be identified. Where special categories of Personal Data and/or Personal Data relating to criminal convictions/offences are Processed, an exception to the prohibitions for Processing these Personal Data under applicable EU data protection law must also be identified;

   **ii. Fairness**: The Processing of Personal Data must be done in a manner which does not unjustifiably or excessively intrude upon the privacy of Data Subjects, affect their rights, freedoms and legitimate interests negatively in a disproportionate manner, or result in a Processing of Personal Data which would run counter to Data Subjects’ legitimate expectations;

   **iii. Transparency**: Data Subjects must be provided with all information deemed necessary under applicable EU data protection law to ensure that they are fully aware of the circumstances under which the Processing of their Personal Data takes place, and their possibilities to react to this, save for where any relevant exception under applicable EU data protection law applies;

   **iv. Purpose Limitation**: The Processing of Personal Data must be done for specified, explicit and legitimate purposes. Any further Processing of Personal Data must be compatible, under applicable EU data protection law, with the purposes for which Personal Data were initially collected/Processed;

   **v. Data Minimisation**: Any Personal Data Processed must be adequate, relevant and limited to what is strictly necessary in order for the purposes for which the
Processing is carried out to be met. Where a purpose can be met with fewer, or no Personal Data (e.g., aggregated data), this should be done;

vi. **Accuracy:** Any Personal Data Processed must be accurate, complete and kept updated, with all reasonable steps taken to ensure that inaccurate, incomplete or outdated Personal Data are erased, completed or rectified without delay;

vii. **Storage Limitation:** Any Personal Data Processed must only be kept in a form which allows identification of the corresponding Data Subjects for the strictly minimum period of time needed in order for the purposes for which the Personal Data are Processed to be met. This requires the identification of retention periods for each category of Personal Data, after which those Personal Data must be erased, anonymised or (at least) restricted from further Processing;

viii. **Integrity and Confidentiality (Security):** Technical and organisational security measures must be implemented in order to ensure that Personal Data are Processed in a manner which ensures their confidentiality, integrity and availability, including protection against unauthorised or unlawful Processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures;

**Relevance:** CSA regards data protection by design and by default not as independent principles, but as means to achieve compliance with the principles set forth in Article 5 GDPR. Therefore, the aim of this control is to make sure that there are technical and organisational measures in place to ensure that the CSP complies with all such principles.

Through this control, CSPs are required to provide evidence that each of the data protection principles reflected in EU data protection law have been addressed, in connection with the service under assessment, and to explain how this has been achieved in practice (through specific technical and organisational measures). This should be done concerning the Processing activities which are inherent to the service, by demonstrating that data protection principles have been considered from the outset/design stage of the service, and continue to be seen as a core element of the service throughout its provision and development (i.e., not unnecessarily compromised in favour of service effectiveness or profitability, or tacked-on as a compliance-oriented afterthought).

Although the GDPR only requires Controllers to ensure that all data protection principles are complied with, this CoC extends this obligation to CSPs acting as Processors, to
ensure that these controls can effectively raise the bar on data protection compliance for CSPs. CSPs must be able to demonstrate that the service which is to adhere to the CoC is supported by technical and/or organisational measures which may assist the relevant Controllers in complying with the aforementioned data protection principles. It should be demonstrated not only that the service does not pose any obstacle to full compliance with these principles, but also that the service actively promotes this compliance, by offering tools with which the use of Personal Data through the service can be managed in a manner which is perfectly aligned with data protection requirements.

For example – CSPs must be able to show that their service allows Cloud Customers to control retention periods applicable to Personal Data, so that they can ensure that the principle of storage limitation is met. Where a CSP develops and designs cloud services that will typically be used to Process Personal Data, it should take into account the duties and obligations under the GDPR and other applicable data protection laws when developing and designing such services and, with due regard to the state of the art, make sure that its Cloud Customers are able to fulfil their data protection obligations, under the principle of lawfulness\(^\text{101}\). An example could be that where a CSP foresees that its Cloud Customers will rely on Consent as a legal basis to Process Personal Data via the service, the CSP may consider providing means for this Consent to be collected by or on behalf of the Cloud Customer in a valid and lawful manner. Providing Cloud Customers with enough information on the service, and the inherent Processing of Personal Data, to allow those Cloud Customers to properly inform their Data Subjects would align the CSP with the principle of transparency (note that this is covered also in other sections of this CoC).

2. The CSP must have in place, and describe to Cloud Customers the evidence that, upon request, can be produced to demonstrate that the service, by default, only Processes Personal Data which are strictly necessary for each of the Processing purposes identified by the Controller (in relation to the amount of Personal Data collected, the extent of their Processing, retention periods and accessibility of Personal Data). In particular, the CSP must demonstrate that, by default, Personal Data are not made accessible to the public at large, or an indefinite number of natural persons, or further Processed, without the Data Subject’s intervention.

**Relevance:** This Control covers the principle of privacy/data protection by default, requiring CSPs to show that Personal Data is automatically protected in the systems

\(^{101}\) See Recital 78 GDPR.
used and Processing activities performed in connection with the assessed service, so that individuals do not need to take any specific actions in order to protect their privacy. CSPs should offer strong default privacy settings within their services, with user-friendly options and controls to respect preferences which may be set by users (e.g., allowing users to choose whether or not to receive communications from an online CSP’s platform by e-mail or push notifications).

In general, any Processing of Personal Data which is additional to (not strictly necessary for) the provision of the service should be left in the hands of the Data Subjects concerned.

4. **RECORDKEEPING**

CSPs must confirm to the Cloud Customers and commit:

1. To maintain a record of all categories of Processing activities carried out on behalf of a Controller and make it available to the Supervisory Authority upon request.

The record must contain the following information:

2. Name and contact details of the CSP and its Sub-processors, and of each Controller on behalf of which the CSP is acting, and, where applicable, of the Controller’s or the CSP’s representative, and the DPO;

3. Categories of Processing carried out on behalf of each Controller;

4. Where applicable, transfers of Personal Data to a third country or an international organisation, including the identification of that third country or international organisation and the documentation of suitable safeguards;

5. A description of technical and organisational security measures in place (see also Control no. 6., below).\(^{102,103}\)

---

\(^{102}\) See Article 32 GDPR.

\(^{103}\) See Article 30(2) GDPR and Article 30(5) GDPR, which set forth the following limitation: “The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9 (1) or personal data relating to criminal convictions and offences referred to in Article 10.” However, see also the clarification provided by the WP29 in the WP29 Records Position Paper, in which the applicability of this limitation is restricted.
**Relevance:** This control seeks to extend recordkeeping obligations, by requiring all CSPs to keep detailed records containing the above information, regardless of whether the exception laid down in Art. 30(5) GDPR might apply to a CSP or not (considering also WP29’s latest position on this exception, in the WP29 Records Position Paper, which dramatically reduced its scope of application). This is required of all CSPs due to the keeping of complete records being a fundamental tool in ensuring transparency and increasing controls on the CSPs compliance, as well as being a primary means of allowing the CSP to demonstrate compliance under the principle of accountability.

In designing their records of Processing activities, CSPs should take into consideration templates developed by Supervisory Authorities – notably, by the CNIL\(^{104}\). However, these templates should be seen as examples or illustrations of best practice, and not as mandatory models to be followed: in line with the principle of accountability and the risk-based approach inherent to the GDPR (as well as to this CoC), CSPs remain responsible for configuring their records in the manner which is deemed most appropriate to ensure compliance with their obligations – and, in particular, to meet the requirements of these CoC controls.

Whenever feasible, Recipients (see Control 4.1.5., above) should be identified individually, rather than by categories.

### 5. DATA TRANSFER

The CSP must clearly indicate to Cloud Customers:

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

**Relevance:** The purpose of this control, in practice, is to allow Cloud Customers to clearly understand the flows of data inherent to the provision of a CSP’s services. The CoC sees this control as important in order to shed light on practices which, in the cloud computing domain, are generally unclear to Data Subjects. CoC adherents remain free to comply with this control in the manner that they see as most adequate, provided that the end result is a clear and complete indication to Cloud Customers of how Personal Data will flow across borders in connection with the services – for instance, the use of

\(^{104}\) See the model record of Processing activities developed by the CNIL, which can be used by CSPs to record their Processing activities as a Processor, available at: [https://www.cnil.fr/en/record-processing-activities](https://www.cnil.fr/en/record-processing-activities).
pictures and data flow diagrams, accompanying a verbal explanation, may help to make the provision of this information transparent to Cloud Customers.

It is important for CSPs to understand that a transfer of Personal Data, for the purposes of this CoC, will take place whenever Personal Data Processed in one country is subsequently Processed in another country. This can happen when the CSP actively sends Personal Data from country A to a Recipient located in country B, but also when the CSP allows a Recipient, established in country B, to gain remote access to Personal Data stored in country A\textsuperscript{105}.

The information provided on transfers of Personal Data to Cloud Customers must cover the following:

• The types of transfers which will take place, in connection with the service;

• The purpose for each type of transfer identified (e.g., storage purposes, back-up purposes)

• The specific country(ies) to which Personal Data will be transferred, for each type of transfer identified.

Note that the purposes and specific receiving countries must be linked to each type of transfer identified. It will not suffice for a CSP to merely list all types, purposes and data destinations – the Cloud Customer must be able to understand the specific purpose(s) for which Personal Data will be transferred to each specific receiving country.

If such transfers are restricted under applicable EU law, the CSP must clearly indicate to Cloud Customers, and take all steps reasonably needed to put in place:

2. A lawful transfer mechanism for each transfer (including onward transfers through several layers of subcontractors),\textsuperscript{106} e.g., European Commission adequacy decision, model contracts/standard data protection clauses,\textsuperscript{107}

\textsuperscript{105} This last case is specifically addressed in the EDPB Transfer Derogation Guidelines, p. 4: “a transfer will for example generally be considered to be non-occasional or repetitive when the data importer is granted direct access to a database (e.g. via an interface to an IT-application) on a general basis.”

\textsuperscript{106} See the ICO Cloud Computing Guidance, p. 18.

\textsuperscript{107} See Articles 44 et seq. GDPR. See also the WP29 Cloud Computing Opinion, Section 3.5.3, p. 18.
approved codes of conduct\textsuperscript{108} or certification mechanisms\textsuperscript{109} and binding corporate rules (BCRs).\textsuperscript{110}

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

These mechanisms should be drawn from Articles 44 to 49 GDPR (e.g., adequacy decisions\textsuperscript{111}, BCRs, standard contractual clauses\textsuperscript{112}).

With specific reference to standard contractual clauses, whether or not a Controller may rely on them as a lawful transfer mechanism under the GDPR will depend on the results of an assessment carried out by the Controller (data exporter), alongside the data importer in the recipient country, as to whether the recipient country allows for the level of personal data protection offered by the standard contractual clauses (in other words, an essentially equivalent level of protection to that guaranteed in the EU) to be respected. This assessment must take into account all relevant circumstances of the intended transfer, including any supplementary measures which the exporter and importer may put in place to address identified risks or shortcomings concerning the

\textsuperscript{108} Pursuant to Article 40 GDPR.
\textsuperscript{109} Pursuant to Article 42 GDPR.
\textsuperscript{110} See the WP20 Cloud Computing Opinion, Section 3.5.4, p. 19.
\textsuperscript{111} The CJEU’s recent decision in the Schrems II Case caused the invalidation of the Privacy Shield Adequacy Decision, rendering the EU-U.S. Privacy Shield Framework as an unsuitable mechanism to ensure the lawful transfer of Personal Data from within the EEA to the United States of America, under the GDPR.
\textsuperscript{112} In contrast with its impact upon the Privacy Shield Adequacy Decision, the Schrems II Case did not cause the absolute invalidation of the standard contractual clauses as a lawful transfer mechanism under the GDPR. These remain in force, for the time being, and are a \textit{prima facie} legitimate means of transferring Personal Data to countries which have not received an adequacy decision from the European Commission. However, in light of the Schrems II Case and the EDPB Schrems II FAQ, caution must be exercised when choosing to rely on standard contractual clauses as a lawful transfer mechanism. In particular, both the data exporter (located within the EEA) and importer (located in a given recipient country, outsider of the EEA) must verify – before transferring any Personal Data based on the standard contractual clauses – whether an essentially equivalent level of protection to that guaranteed within the EU, by the GDPR, is provided and respected in the recipient country.
level of protection offered by the standard contractual clauses in the recipient country (as a result of local legislation).

With respect to supplementary measures, CSPs should take into consideration possible legal (e.g., obligations placed upon recipients within agreements, such as DPAs, joint controllership agreements or data management agreements\(^\text{113}\), to provide advance notice to the data exporter of any local authority requests for access to the Personal Data in question), organisational (e.g., procedural measures to ensure that as little Personal Data is made accessible, sent or Processed outside of the EU/EEA, while still allowing for the provision of services) and/or technical measures\(^\text{114}\) (e.g., implementing end-to-end encryption for all Personal Data transferred to the recipient country). The CSP should refer to recommendations which may, from time to time, be made available by the EDPB and EEA Supervisory Authorities.

The standard contractual clauses and supplementary measures combined would need to suffice to ensure that the laws applicable in the recipient country do not impinge on the adequate level of protection guaranteed by the clauses themselves. Should this not be possible, then the Controller must either (A) suspend or end the transfer of Personal Data based on standard contractual clauses, or (B) notify its competent Supervisory Authority of its intention to proceed with such a transfer, regardless of the insufficiency of the standard contractual clauses and supplementary measures to ensure an adequate level of protection for the Personal Data in question.

During the course of any relationship involving a transfer of Personal Data from within the EEA to outside the EEA based on standard contractual clauses, the data importer (located outside of the EEA) is also required by the standard contractual clauses themselves to notify the data exporter (i.e., the Controller) of any inability to comply with standard contractual clause requirements (or any supplementary measures agreed between the parties), following which the data importer is required to suspend the transfer of Personal Data in question and/or to terminate the relationship with the data importer.

\(^{113}\) A “data management agreement” is a written agreement entered into between two or more organisations which are involved in a relationship involving the Processing of Personal Data, in order to comprehensively regulate their respective data protection compliance responsibilities. These agreements may incorporate DPA terms, joint controllership terms and or additional terms to regulate relationships between independent Controllers.

\(^{114}\) When implementing technical measures, the recipient must ensure that doing so does not cause them to breach any of their obligations under the applicable local law.
Regarding **standard contractual clauses**, CSPs should note that there are currently no approved Processor-to-Processor standard contractual clauses. Therefore, in order to address onward transfers of Personal Data to non-EEA Sub-processors, CSPs will need to consider the following:

- **If the CSP is located in the EU/EEA**: The Controller must enter into standard contractual clauses with any non-EEA Recipients which may receive their EEA-originating Personal Data in connection with the service. The CSP must identify how this will be ensured – generally, either by having the Controller enter into standard contractual clauses with the Recipients directly, or by receiving a mandate from the Controller to do so on their behalf;

- **If the CSP is located outside of the EU/EEA**: The CSP can consider leveraging Clause 11 (“Subcontracting”) of the Controller-to-Processor standard contractual clauses entered into with the Cloud Customer, in order to enter into written agreements with its non-EEA Sub-processors, without the need for the Cloud Customer’s direct intervention (note that the requirements of **Control no. 3.3.**, above, must still be met in this case).

6. **DATA SECURITY MEASURES**

Preliminarily, the CSP should note that: “... **Cloud 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.**”\(^\text{115}\) In completing this section, which is based on the WP29 Cloud Computing Opinion, CSPs are required to follow the ENISA Technical Guidelines\(^\text{116}\) as a minimum acceptable baseline (controls provided below). 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.\(^\text{117}\)

\(^{115}\) See the ENISA Technical Guidelines, p. 6.

\(^{116}\) See also the NCSC Guidance and the CNIL Security GuidePersonal Data.

\(^{117}\) See Articles 32(3), 40 and 42 GDPR.
Taking into account the state of the art, costs of implementation and the nature, scope, context and purposes of Processing, as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the CSP must:118

1. Specify and justify to Cloud Customers the technical, physical and organisational (including specific training sessions on data security for persons authorised to Process Personal Data, at least annually) measures that are in place to protect Personal Data against accidental or unlawful destruction; or accidental loss, alteration, unauthorised use, unauthorised modification, disclosure or access; and against all other unlawful forms of Processing;119

Relevance: Evidence of data security compliance may also be provided to Cloud Customers by way of adherence to relevant codes of conduct, and certification mechanisms.120 Additionally, CSPs may also point to controls pertaining to other security certifications that CSPs may have (e.g., ISO 27001, SOC2, etc.). However, this does not relieve CSPs of the requirement to identify specific security measures in place to address each of the controls within the CSA Cloud Controls Matrix (see Control no. 6.3., below).

2. Have in place, describe and justify to Cloud Customers, concrete technical, physical, and organisational measures (protective, detective and corrective) to ensure the following safeguards:121

118 See Article 32 GDPR.
119 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.”
120 See Articles 32(3), 40 and 42 GDPR.
i. **Availability**\(^{122}\) - 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, whether such incidents are accidental or the result of malicious events,\(^{123}\)

ii. **Integrity**\(^{124}\) - methods by which the CSP ensures integrity\(^{125}\) (e.g., detecting unauthorised alterations to Personal Data, whether accidental or malicious, 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.);\(^{126}\)

iii. **Confidentiality**\(^{127}\) - methods by which the CSP ensures confidentiality from a technical point of view in order to assure that only authorised persons have access to data; Including, inter alia as appropriate, Pseudonymisation and

---

\(^{122}\) See the ‘Availability’ Section of the ICO Cloud Computing Guidance’s 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?”

\(^{123}\) WP29 Cloud Computing Opinion, Section 3.4.3.1, p. 14.

\(^{124}\) See the ‘Integrity’ Section of the ICO Cloud Computing Guidance’s 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?”

\(^{125}\) The description should concern all data layers within the CSP, from the customer’s information context, through to physical data components and software codes.

\(^{126}\) WP29 Cloud Computing Opinion, Section 3.4.3.2, p. 15. See also the ICO Cloud Computing 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.”

\(^{127}\) See the ‘Confidentiality’ Section of the ICO Cloud Computing Guidance’s checklist, p. 22: “Can your cloud provider provide an appropriate third-party security assessment? Does this comply with an appropriate industry code of practise or other quality standard? How quickly will the cloud provider react if a security vulnerability is identified in their product? What are the timescales and costs for creating, suspending and deleting accounts? Is all communication in transit encrypted? Is it appropriate to encrypt your data at rest? What key management is in place? What are the data deletion and retention timescales? Does this include end-of-life destruction? Will the cloud provider delete all of your data securely if you decide to withdraw from the cloud in the future? Find out if your data, or data about your cloud users will be shared with third parties or shared across other services the cloud provider may offer.”
encryption of Personal Data\textsuperscript{128} “in transit” and “at rest,”\textsuperscript{129} authorisation mechanism and strong authentication;\textsuperscript{130} 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 Sub-processors (or other subcontractors) who may be able to access data;

iv. Transparency – technical, physical and organisational measures the CSP has in place to support transparency and to allow review by Cloud Customers (see, e.g., \textbf{Control no. 7.}, below);\textsuperscript{131}

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, including delegation of access, revocation of access, logging of access, access conflict detection/resolution and reviewing of access rights on a regular basis; access management based on the “least privilege” principle; hardening of hypervisors;\textsuperscript{132} and proper management of shared resources.

\textsuperscript{128} See Article 32(1)(a) GDPR.

\textsuperscript{129} 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.” WP29 Cloud Computing Opinion, Section 3.4.3.3, p. 15. See also the ICO Cloud Computing Guidance, pp. 14-15.

\textsuperscript{130} WP29 Cloud Computing Opinion, Section 3.4.3.3, p. 15.

\textsuperscript{131} WP29 Cloud Computing Opinion, 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 practise inform the client about this circumstance and in particular about its implications from a data protection and data security point of view. Vice versa, the cloud client should raise this matter \textit{ex ante}, if it is not addressed sufficiently by the cloud provider.” WP29 Cloud Computing Opinion, Section 3.4.1.1, pp. 10-11.

\textsuperscript{132} “[H]ardening of hypervisors” is also relevant to ‘Integrity’. 
wherever virtual machines are used to share physical resources among Cloud Customers).\textsuperscript{133}

vi. Intervenability – methods and tools by which the CSP enables and facilitates Data Subjects’ rights of access, rectification, erasure ("right to be forgotten"),\textsuperscript{134} blocking, objection, Restriction of Processing\textsuperscript{135} (see Control no. 10., below), portability\textsuperscript{136} (see Control no. 9., below) in order to demonstrate the absence of technical and organisational obstacles to these requirements, including cases when data are further Processed by Sub-processors\textsuperscript{137} (this is also relevant for Control no. 9., below);

vii. Portability – see Control no. 9., below;

viii. Accountability – see Control no. 1., above.

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

It is understood that providing specific, “one-size-fits-all” security measures to be implemented, regardless of the risks to the rights and freedoms of the Data Subjects and technological developments, would run counter to the idea behind Art. 32 GDPR. However, the CoC establishes a minimum baseline of security controls and measures that CSPs must adopt, regardless of any factors which might be deemed as mitigating (e.g., level of risk inherent to the CSP’s Processing activities, maturity of the CSP’s security program, cost and budget, and so on). These baseline security measures – identified in Control no. 6.3., below – should be used as a foundation upon which CSPs must build, in order to offer an additional level of assurance and protection to Cloud Customers, depending on the state of the art, costs of implementation and the nature,

\textsuperscript{133} WP29 Cloud Computing Opinion, Section 3.4.3.5, p. 16. See also the ICO Cloud Computing Guidance, p. 20.

\textsuperscript{134} Article 17 GDPR.

\textsuperscript{135} Article 18 GDPR.

\textsuperscript{136} Article 20 GDPR.

\textsuperscript{137} WP29 Cloud Computing Opinion, Section 3.4.3.5, p. 16.
scope, context and purposes of Processing, as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons.

This security baseline is expressed as a set of requirements and control objectives, in line with the best practices and standards commonly adopted in the information security domain. The rationale behind defining requirements and control objectives, as opposed to mandating prescriptive technical specification/controls/measures, is that the latter would need to vary depending on a number of factors, such as the type of cloud deployment and delivery models, type of internal architecture, type of the technology platform adopted, technology developments, etc. This would prevent the CoC from achieving the much required level of flexibility, necessary for its efficient and adequate implementation by CSPs.

It must be noted, though, that all adherents to the CoC will have access to the CSA’s knowledge and resources (e.g., CSA Security Guidance\textsuperscript{138} and Cloud Control Matrix\textsuperscript{139}, Consensus Assessment Initiative Questionnaire\textsuperscript{140}, etc) on data and information security, which will allow those CSPs to become aware of, and to implement, the most relevant measures.

Thus, CSPs will be required, under Art. 32 GDPR, to take responsibility for establishing the most appropriate security measures to be implemented given the resources made available to them, and to disclose information on the measures chosen and put in place following the structure within this control – this will allow a more coherent and clear provision of information to Cloud Customers, which will more easily understand exactly what is offered by each CSP in terms of security.

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

Concerning Control 6.2.iv., above (Transparency), this Control refers specifically to security measures which the CSP has implemented to allow Cloud Customers to understand what is done with Personal Data they entrust to a CSP in connection with a

\textsuperscript{138} Available at: https://cloudsecurityalliance.org/research/guidance/.

\textsuperscript{139} Available at: https://cloudsecurityalliance.org/research/cloud-controls-matrix/.

\textsuperscript{140} Available at: https://cloudsecurityalliance.org/artifacts/consensus-assessments-initiative-questionnaire-v3-1/.
service. This is tied in to Control 7., below, which requires an identification of options put in place to allow a Cloud Customer to monitor and audit the use of their data.

Concerning Control 6.2.vi., above (Intervenability), CSPs should, in particular, provide details to Cloud Customers to show that their service does not create any obstacles to the response to Data Subject or other intervenability-related requests, and explain specific measures put in place to ensure that these requests can be addressed by the CSP (and, consequently and where applicable, also by Cloud Customers) in a timely and effective manner.

3. As a minimum acceptable baseline, this CoC requires CSPs to comply with the controls set out in the CSA Cloud Controls Matrix\textsuperscript{141}. The CSP must indicate and justify how each of the relevant controls is met, taking into account the state of the art, costs of implementation and the nature, scope, context and purposes of Processing, as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons\textsuperscript{142}:

**Relevance:** To meet the minimum acceptable baseline for this control, CSPs must demonstrate that they have at least met the requirements of CSA STAR Self Assessment (LEVEL 1)\textsuperscript{143}, by pointing to a relevant entry on the CSA STAR Registry\textsuperscript{144} submitted by the CSP based on the CSA Cloud Controls Matrix.

For the latest version of the CSA Cloud Controls Matrix controls, please see the CSA’s website\textsuperscript{145}, or otherwise refer to the attached file (CoC GDPR_Annex 1_Compliance_Assessment_Template).

Evidence of data security compliance may also be provided to Cloud Customers by way of adherence to relevant codes of conduct, and certification mechanisms.\textsuperscript{146} Additionally, CSPs may also point to controls pertaining to other security certifications that CSPs may have (e.g., ISO 27001, SOC2, etc.). However, this does not relieve CSPs of the requirement to identify specific security measures in place to address each of the controls within the CSA Cloud Controls Matrix.

\textsuperscript{141} Available at: https://cloudsecurityalliance.org/research/working-groups/cloud-controls-matrix/.

\textsuperscript{142} CSPs may also take into consideration the CNIL Security Guide.

\textsuperscript{143} More information available at: https://cloudsecurityalliance.org/artifacts/star-level-and-scheme-requirements.

\textsuperscript{144} Available at: https://cloudsecurityalliance.org/star/registry/.

\textsuperscript{145} Available at: https://cloudsecurityalliance.org/research/cloud-controls-matrix/.

\textsuperscript{146} See Articles 32(3), 40 and 42 GDPR.
7. MONITORING

The CSP must have in place, and indicate to Cloud Customers:

1. Options to allow the Cloud Customer to monitor and audit in order to ensure appropriate privacy and security measures described in the Control Specifications: PLA are met on an ongoing basis (e.g., logging, reporting, first- and/or third-party auditing\footnote{See the CNIL Orange Decision, which evokes the lack of a security audit.} of relevant Processing operations performed by the CSP or subcontractors).\footnote{See Article 28(3)(h) GDPR and Control no. 1., above. See also the WP29 Cloud Computing Opinion, Section 3.4.2, p. 13 and Section 3.4.1.2, p. 11. See also the ICO Cloud Computing Guidance, pp. 13.14.} Any audits carried out which imply that an auditor will have access to Personal Data stored on the systems used by the CSP to provide the services will require that auditor to accept a confidentiality agreement.

**Relevance:** This control further specifies Art. 28(3)(h) GDPR, by imposing upon CSPs the obligation to inform Cloud Customers as to their specific options for effectively monitoring CSPs’ compliance and to audit the privacy and security measures they have implemented regarding the Processing activities inherent to the services. CSPs are given options as to how this can be done – such as maintaining logs which Cloud Customers can monitor, periodic reporting to Cloud Customers or relying upon first-party or third-party audits performed upon their operations, and those of Sub-processors engaged.

As noted in Control 3.5., above, it is standard practice within the cloud domain to allow Cloud Customers to have access to reports of audits carried out by independent and qualified third parties, rather than providing direct access to the CSPs’ systems, equipment or facilities used to Process Personal Data. These third-party audits must be regularly carried out by CSPs, with a frequency which is adequate to their nature and purpose. The best practice in this regard, which is also the generally-recognised rule for certification and attestation audits, is to set at least an annual frequency for these audits, and to carry out additional *ad hoc* audits in the event of a substantial or relevant change to the target of the audit.

8. PERSONAL DATA BREACH

The CSP must confirm:

1. That it will notify Cloud Customers of Personal Data Breaches affecting the Cloud Customer’s data Processed by the CSP and/or its Sub-processors, without undue delay
and, where feasible\textsuperscript{149}, no later than 72 hours from the moment on which the CSP becomes aware of the incident in question\textsuperscript{150}.

2. That, should it not be feasible to inform a given Cloud Customer of a Personal Data Breach within the 72-hour deadline, the CSP will inform that Cloud Customer of the Personal Data Breach as soon as possible and accompany this communication to the Cloud Customer with reasons for the delay.

3. That each notification made to Cloud Customers will, at least and to the maximum extent possible, include the below information:

i. Description of the nature of the Personal Data Breach, including the categories and approximate number of Personal Data records concerned;

ii. Name and contact details of the DPO or other contact point where more information can be obtained (see Control no. 2., above);

iii. Likely consequences of the Personal Data Breach, in terms of potential impact for the relevant Data Subjects\textsuperscript{151};

iv. Description of measures taken (or proposed to be taken) to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects (which have been, or can be, taken by the CSP, Cloud Customer and/or the Data Subjects themselves).\textsuperscript{152}

4. That, where it is not feasible to provide all of the above information in an initial notification, the CSP must provide as much information to the Cloud Customer as

\textsuperscript{149} As further detailed in the ‘Relevance’ section of this control, the investigation of a potential Personal Data Breach by a CSP may take some time, particularly in terms of correcting identifying the scope of the Personal Data Breach. Aside from practical and technical complications in the identification and assessment of Personal Data Breaches, there may also be similar complications in the notification of those Personal Data Breaches, particularly where a large number of Cloud Customers may have been affected. In order to avoid premature, unnecessary and incomplete notifications to the greatest extent possible, and to make this Control practically implementable for CSPs, it was considered reasonable to set for CSPs the same notification deadline to Cloud Customers as the GDPR sets for Controllers to notify Supervisory Authorities – i.e., 72 hours from the moment on which a CSP becomes aware of a Personal Data Breach, where feasible.

\textsuperscript{150} See Articles 33 and 34 GDPR, as well as see the EDPS Data Breach Guidelines, p. 15 and the WP29 Data Breach Guidelines, pp. 11-12.

\textsuperscript{151} To help with this, CSPs can refer to the ENISA Breach Severity Assessment Recommendations.

\textsuperscript{152} See Article 33 GDPR.
possible on the reported incident, and provide any further details needed to meet the above requirement as soon as possible (i.e., provision of information in phases).\textsuperscript{153}

The CSP must inform Cloud Customers as to:

5. The obligations upon the CSP for Personal Data Breach reporting under the above Controls, as well as how notifications will be made to the Cloud Customer.

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

A CSP will be considered as “aware” of a Personal Data Breach on the moment that it detects (e.g., directly, or due to a notification received from a Sub-processor) an incident which qualifies as a Personal Data Breach and establishes that that incident has affected data processed by the CSP and/or its Sub-processors on behalf of a given Cloud Customer.

A timeframe for CSPs to notify affected Cloud Customers of a detected Personal Data Breach has been defined as a baseline, which must be met whenever feasible. There are several practical circumstances which may lead to delays in the CSP’s ability to properly identify, assess and communicate a Personal Data Breach to Cloud Customers. Given that CSPs are required to notify actual Personal Data Breaches, rather than all incidents which might potentially qualify as a Personal Data Breach, CSPs will be required to investigate security incidents occurred and correctly identify their scope. This work may

\textsuperscript{153} See the WP29 Data Breach Guidelines, pp. 13-14: “The GDPR does not provide an explicit time limit within which the processor must alert the controller, except that it must do so “without undue delay”. Therefore, WP29 recommends the processor promptly notifies the controller, with further information about the breach provided in phases as more details become available. This is important in order to help the controller to meet the requirement of notification to the supervisory authority within 72 hours”.

CSA Code of Conduct for GDPR Compliance © Copyright 2013-2020, Cloud Security Alliance. All rights reserved. 68
be more arduous and time-consuming for smaller CSPs, which may not have the staff or processes in place to allow an immediate identification or assessment of a potential Personal Data Breach (including where incident handling may have been outsourced to third parties). Finally, there are also technical circumstances to be considered regarding the actual notification, as where an actual Personal Data Breach affects a large number of Cloud Customers for a CSP, the process of setting up and issuing the notifications to be sent out may take time (in particular due to the need to avoid spamming filters, or other mechanisms designed to stop mass emails). Furthermore, large-scale Personal Data Breach notifications may also have relevant effects with respect to the application of other legislation – e.g., accidental notification to certain Cloud Customers may put them at risk of insider trading; certain local laws may require CSPs to notify law enforcement authorities directly in the event of Personal Data Breaches of criminal relevance (possibly without notifying the Cloud Customer) – which therefore requires a series of prior legal checks to be carried out before such external communications are completed.

These and other examples are considered as supporting the argument that CSPs should be subjected, regarding their obligation to report Personal Data Breaches to Cloud Customers, to the same timeframe that the GDPR affords to Controllers vis-à-vis Supervisory Authorities: i.e., 72 hours from the moment on which the CSP becomes ‘aware’ of the Personal Data Breach (i.e., where it has identified that a Personal Data Breach has taken place and has affected a given Cloud Customer), whenever feasible. In any case where the 72-hour deadline cannot feasibly be met, the CSP should nonetheless inform the Cloud Customer as soon as possible, and provide reasons for this delay. Naturally, CSPs may also wish to provide shorter deadlines for incident response in their agreements with Cloud Customers, particularly where their Cloud Customers belong to specific sectors (including EU institutions and agencies\textsuperscript{154}) which may be subjected to tighter notification requirements.

The potential impact which must be considered by CSPs includes any form of relevant harm which Data Subjects will, or may, suffer as a result of a Personal Data Breach. To help in assessing such an impact, CSPs are strongly recommended to refer to the methodology described in the ENISA Breach Severity Assessment Recommendations, which lays out objective criteria allowing for the calculation of a “severity level”, based on the characteristics of the Personal Data Breach in question. CSPs are also

\textsuperscript{154} Entities that are subject to compliance with Regulation (EU) 2018/1725 of the European Parliament and of the Council, of 23 October 2018.
recommended to refer to the examples provided in the WP29 Data Breach Guidelines, which illustrate scenarios of varying risks to the Data Subjects concerned.

CSPs may also inform Cloud Customers that they rely on expert third parties, such as privacy consultants, to manage any Personal Data Breaches which take place.

9. **DATA PORTABILITY, MIGRATION AND TRANSFER BACK**

The CSP must have in place, and specify to Cloud Customers:

1. A procedure or process to assure data portability, in terms of the capability to transmit Personal Data in a structured, commonly used, machine-readable and interoperable format.\(^{155}\)
   
   i. To the Cloud Customer (“transfer back”, e.g., to an in-house IT environment);
   
   ii. Directly to the Data Subjects;
   
   iii. To another service provider (“migration”), e.g., by means of download tools or Application Programming Interfaces, or APIs.\(^ {156}\)

---

\(^{155}\) See Recital 68 GDPR.

\(^{156}\) 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 WP29 Portability Guidelines for practical guidelines, best practises and tools that support compliance with the right to data portability. The right to data portability is a new right introduced by the GDPR. However, even before the GDPR will be directly applicable in the EU Member States (25 May 2018), there seems to be enough ground for considering data portability as a mandatory requirement pursuant to general EU Personal Data protection principles, such as “data accuracy” (Article 6(1)(d) of the Data Protection Directive), “data availability” and possibility to grant Data Subjects’ rights per Articles 11(1)(c) and 12 of the Data Protection Directive. See also the WP29 Cloud Computing Opinion, Section 3.4.3.6, p. 16 and the ICO Cloud Computing 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 EC Cloud SLAS Guidelines: “5.4. Data Portability.
The CSP must describe to Cloud Customers:

2. **How and at what cost the CSP will assist Cloud Customers in the possible migration of data to another service provider or back to an in-house IT environment.**\(^{157}\) Whatever the procedure implemented, the CSP must cooperate in good faith with Cloud Customers, by providing a reasonable solution.

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

The above this applies not only to portability, per se, but also to the migration of data to other service providers and the “transfer-back” of data to the Cloud Customer’s in-house IT environment.

---

**Description of the context or of the requirement**

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

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

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

**Description of relevant SLOs**

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

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

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

\(^{157}\) See the WP29 Cloud Computing Opinion, Section 3.4.3.6, p. 16.
10. **RESTRICTION OF PROCESSING**

The CSP must have in place, and explain to Cloud Customers:

1. A procedure or process for Restriction of Processing of Personal Data when needed; 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 EU or of a Member State.\(^{158}\)

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

Examples of how CSPs may seek to address this right could include measures to isolate restricted data from general processing systems used by the CSP, block or otherwise make restricted data unavailable to the CSP’s end-users, remove restricted data from websites, mark personal data so that it cannot be changed or further processed, clearly flag restricted data, etc. Any such measures would need to be temporary and reversible, so that they can be undone upon lifting of the restriction.

---

\(^{158}\) 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.
11. DATA RETENTION, RESTITUTION AND DELETION

11.1 Data retention, restitution and deletion policies

The CSP must have in place, and describe to the Cloud Customers:

1. The CSP’s data retention policies, timelines and conditions for returning Personal Data or deleting data once the service is terminated.

The CSP must have in place, and describe to the Cloud Customers:

2. Data retention policies, timelines and conditions for returning Personal Data or deleting data once the service is terminated, applicable to the CSP’s Sub-processors.

11.2 Data retention

The CSP must define, indicate to Cloud Customers and commit to comply with:

1. The time period for which the Personal Data will or may be retained, or if that is not possible, the criteria used to determine such a period. ¹⁵⁹

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

2. Necessity – Personal Data is retained for as long as necessary in order to achieve the purpose for which it was collected, so long as it remains necessary to achieve that purpose (e.g., to perform the services); Legal Obligation – Personal Data is retained for as long as necessary in order to comply with an applicable legal obligation of retention (e.g., as defined in applicable labour or tax law), for the period of time defined by that obligation; Opportunity – Personal Data is retained for as long as permitted by the applicable law (e.g., Processing based on Consent, Processing for the purpose of establishing, exercising or defending

¹⁵⁹ Note that “[P]ersonal data must be erased [or anonymised] as soon as their retention is not necessary anymore.” WP29 Cloud Computing Opinion, 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, p. 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).” Section 3.4.1.4, p. 12. See Article 6 of the Data Protection Directive, as well as Articles 5, 13(2)(a) and 14(2)(a) GDPR. See also the WP29 Cloud Computing Opinion, Section 3.4.2, p. 13.
against legal claims – based on applicable statutes of limitations regarding legal claims related to the performance of the services).

11.3 Data retention for compliance with sector-specific legal requirements

The CSP must have in place, and indicate to the Cloud Customers:

1. A procedure for the Cloud Customer to request the CSP to comply with specific sector laws and regulations, requiring specific retention periods for Personal Data.\(^{160}\)

11.4 Data restitution and/or deletion

The CSP must have in place, and indicate to the Cloud Customers:

1. A procedure for returning to the Cloud Customers the Personal Data in a format allowing data portability, after termination of the contract/service (see also Control no. 9., above);

2. Methods which may be used by the CSP and its Sub-processors to delete data, whether at the request of the Cloud Customer or upon a valid request for erasure from a Data Subject.

CSPs must clearly explain to Cloud Customers:

3. Whether data may be retained after the Cloud Customer has deleted (or requested deletion of) the data, or after the termination of the contract/service;

4. The specific reason for retaining the data;

5. The period during which the CSP will retain the data.

Relevance: In requiring CSPs to provide all information above, this control seeks to provide transparency to Cloud Customers as to the retention periods for which CSPs may hold onto their data. Furthermore, in specifying the methods available or used to delete data, CSPs must also clarify how they will provide evidence of this, such as by

\(^{160}\) See the ICO Cloud Computing Guidance, pp. 16-17.
providing a certified statement that no further copies of the Cloud Customers’ data have been retained in the CSPs systems, or those of its Sub-processors.

In particular, CSPs must inform Cloud Customers as to the means by which they will allow Personal Data stored on their systems to be deleted, either where this is done at the initiative of the Cloud Customer (for example, as a result of the termination of services) or a Data Subject (validly exercising his/her right to erasure, under Art. 17 GDPR). In this manner, Cloud Customers will be made aware of how a CSP will allow them to comply with their obligation, as a Controller, to address valid Data Subject requests for erasure, by also ensuring the deletion of Personal Data related to those Data Subjects which may be further stored on the CSP’s systems.

Examples of measures for data deletion in the cloud include: the initial delegation from databases, storage and back-up systems followed by data overwrite or crypto-shredding (i.e., the practice of encryption of data and the destruction of the encryption keys), in order to ensure the complete deletion of the subject data. After the implementation of such a practice, evidence of deletion can be provided via extensive controls documentation of how the data is handled and deleted, and then the associated logs of the activities.

As a caveat, it should be noted that providing 100% assurance that data has been deleted is very difficult to achieve. For instance, to ensure this, a Cloud Customer would need to encrypt the data with a strong key before they store it in cloud, never lose the key, and delete the key when they are done. This would bring the likelihood of full deletion close to 100% (depending on the crypto-algorithm) since the CSP has never had access to both the key and the data at once.

12. COOPERATION WITH THE CLOUD CUSTOMERS

The CSP must have in place, and specify to Cloud Customers:

1. Procedures or processes for cooperation with the Cloud Customers in order to ensure compliance with applicable data protection provisions, e.g., to enable the Cloud Customer to effectively guarantee the exercise of Data Subjects’ rights (rights of access, rectification, erasure (“right to be forgotten”), Restriction of Processing, portability and rights concerning Automated Decision-making), to carry out DPIAs and requests for prior consultation with Supervisory Authorities, and to manage incidents including forensic
The CSP undertakes towards Cloud Customers:

2. To make available to the Cloud Customer and the competent Supervisory Authorities the information necessary to demonstrate compliance (see also Control no. 1., above).\(^{162}\)

**Relevance:** The obligation for a CSP to cooperate with its Cloud Customers is not directly spelled out in the GDPR (other than the references in Art. 28 GDPR), but it is nonetheless fundamental for Cloud Customers to properly comply with their obligations regarding Personal Data Breaches, responding to Data Subject rights and, in general, ensuring that they can demonstrate that the CSPs they engage to Process Personal Data maintain compliant practices. CSPs also commit to make available not only to Cloud Customers, but also to inquiring Supervisory Authorities, the information which may be required in order to demonstrate their compliance with applicable legal obligations and with the terms of the CoC. It should be noted also that cooperating with Cloud Customers in this manner may be the only way for those Cloud Customers to have access to all information needed to complete a DPIA concerning their use of the CSP’s services.

CSPs must pay particular attention to the need to provide clear and specific information to Cloud Customers as to how they will assist those Cloud Customers in addressing Data Subject requests which relate to Personal Data stored on the CSPs’ systems (or otherwise Processed by those CSPs), including the right to data portability (Control no. 9., above), the right to Restriction of Processing (Control no. 10., above), the right to erasure (Control no. 11.4.2., above) and the rights afforded to Data Subjects concerning Automated Decision-making, in the form of safeguards implemented by the CSP concerning those automated decisions (Control no. 3.1.10., above). This should include information on the specific processes in place to ensure that Data Subjects’ rights can be addressed, as well as whether any costs for Cloud Customers may be involved in the provision of this assistance.

\(^{161}\) WP29 Cloud Computing Opinion, 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. WP29 Cloud Computing Opinion, Section 3.4.3.5, p. 16.

\(^{162}\) Articles 5(2) and 28(3)(h) GDPR.
Note that where a Cloud Customer brings a Personal Data Breach to the attention of the CSP, the CSP’s obligations towards the Cloud Customer become cooperation obligations, rather than notification obligations (addressed in Control no. 8., above), as the Cloud Customer will already be aware of the Personal Data Breach. The CSP should, under this control, describe to Cloud Customers how they will assist them in the management of Personal Data Breaches (e.g., sharing of information, discussion and implementation of mitigation/preventive measures, etc.).

13. **LEGALLY REQUIRED DISCLOSURE**

The CSP must have in place, and describe to Cloud Customers:

1. A procedure to manage and respond to requests for disclosure of Personal Data by Law Enforcement Authorities, including to verify the legal grounds upon which any such requests are based prior to responding to them, with special attention to the notification procedure to interested Cloud Customers, unless otherwise prohibited, such as a prohibition under criminal law to preserve confidentiality of a law enforcement investigation.163

**Relevance:** The CoC’s emphasis on transparency towards Cloud Customers implies that they must have clear visibility on the circumstances under which a CSP will disclose Personal Data Processed to authorities upon request, thereby allowing a Cloud Customer not only to assess this procedure a priori, but also affording possibilities for the Cloud Customer to intervene (e.g., in order to limit the disclosure or contest the request), to the extent that the applicable law allows this. This procedure must include an explanation of how the CSP will assess the lawfulness of these requests itself, under what circumstances Cloud Customers may not be notified of such requests and disclosures (which must strictly be based on applicable laws preventing this), and a commitment to only disclosing the strict minimum amount of Personal Data needed to address such requests lawfully.

---

163 WP29 Cloud Computing Opinion, Section 3.4.2 pp. 13-14. See also, and extensively, the WP29 Electronic Communications Surveillance Opinion and the ICO Cloud Computing Guidance, pp. 19-20. See also Preamble 115 GDPR.
14. REMEDIES FOR CLOUD CUSTOMERS

The CSP must have in place, and indicate to Cloud Customers:

1. Remedies available to the Cloud Customer in the event the CSP – and/or the CSP’s Sub-processors (see Control no. 3., above and, more specifically, Control no. 3.3., above) – breach the obligations under the Control Specifications: PLA.

The CSP must also clearly indicate to Cloud Customers:

2. The possibility and means by which Cloud Customers can raise complaints against the CSP for such a breach, as provided by this CoC.

Relevance: A breach of obligations under the Control Specifications: PLA will exist whenever a CSP or a Sub-processor engaged by a CSP fails or ceases to comply, in practice, with the declarations / commitments made in the CSP’s public Self-attestation / Third-party Assessment submission for adherence to the CoC, under which an Adherence Seal was granted in relation to a given service.

To further stress CSPs’ commitment to maintaining their compliance with the applicable law and with the terms of this CoC, CSPs are required to offer remedies to Cloud Customers in the event that such a breach occurs. Remedies may range from the possibility for the Cloud Customer to terminate agreements entered into with the CSP, to more complex and structured forms of remediation (including, e.g., service credits and/or contractual penalties\textsuperscript{164}). As a matter of best practice, the remedies offered should, ideally, be business-friendly (thereby preserving the service relationship between Cloud Customer and CSP, whenever feasible) and suitable to provide compensation to the Cloud Customer for the breach occurred.

Such remedies must be offered without prejudice to the Cloud Customers’ rights to bring legal action against the CSP, as well as the possibility for the Cloud Customer to submit a complaint against the CSP to the CoC Monitoring Body. Cloud Customers must remain free to choose whether or not to pursue legal action or submit complaints, regardless of whether remedies are offered to them. However, where a Cloud Customer accepts remedies offered by the CSP (which go beyond the mere possibility for termination of the agreements entered into with the CSP, by providing some form of adequate compensation to the Cloud Customer), the CSP can require the Cloud

\textsuperscript{164} WP29 Cloud Computing Opinion, Section 3.4.2, p. 12.
Customer to undertake to refrain from bringing legal action or submitting a complaint against the CSP for the same breach, where this is allowed under the applicable law.

As described in Part 3 of this CoC (and further developed in Annex 7), Cloud Customers are entitled to submit complaints against a CSP which is responsible for a breach of obligations under the Control Specifications: PLA. CSPs are required to clearly and expressly inform Cloud Customers of this possibility, and of how it can be exercised – namely, by providing Cloud Customers with a link to the CoC165 and to CSA’s online form for CoC complaint submission.166

15. CSP INSURANCE POLICY

The CSP must have in place, and describe to Cloud Customers:

1. Relevant insurance policy(ies) (e.g., data protection compliance-insurance,167 including coverage for Sub-processors that fail to fulfil their data protection obligations168 and cyber-insurance, including insurance regarding security/Personal Data Breaches).

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

In providing information to Cloud Customers on their insurance coverage, CSPs should specifically identify:

- The scope of their insurance policies;
- The coverage (in terms of amounts insured);

165 Available at: https://cloudsecurityalliance.org/artifacts/cloud-security-alliance-code-of-conduct-for-gdpr-compliance/.
166 Available at: https://cloudsecurityalliance.org/star/feedback/.
167 See Articles 58, 77 et seq. GDPR.
168 See Article 28(4). GDPR.
• Any relevant exclusions.

CSPs must ensure that Cloud Customers are provided meaningful information about the extent to which the CSP is able to trigger insurance, in the event of a relevant breach of data-protection-related obligations, Personal Data Breach, or other relevant incidents.
PART 3
CSA CODE OF CONDUCT
GOVERNANCE AND
ADHERENCE MECHANISMS
The cloud landscape is not static and is likely to change rapidly. CSP and Cloud Customers must promptly address all new laws and regulatory compliance requirements with respect to Personal Data protection. Related parties and existing compliance tools must adapt to ensure the security and privacy measures in place evolve, and that any new regulatory requirements are continuously met.

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

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

1. **Technical Components**: components that over time will be affected by changes in the legal, regulatory and technological environment or by changes within CSA;

2. **Governance Processes**: the governance processes and relevant activities as related to the definition, revision and implementation of the CoC’s Technical Components;

3. **Governance Groups**: the key governing bodies, along with their roles and responsibilities.
1. TECHNICAL COMPONENTS

For ease of reference, please see the tables below:

<table>
<thead>
<tr>
<th>Technical Components</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CoC</td>
<td>“CoC” means this CSA Code of Conduct for GDPR Compliance.</td>
</tr>
<tr>
<td>Control Specifications: PLA</td>
<td>“Control Specifications: PLA” means the technical standard that specifies the CoC’s data protection controls, reflected in Part 2 of the CoC.</td>
</tr>
<tr>
<td>Governance Processes</td>
<td>All 7 processes referred to in Section 3., below:</td>
</tr>
<tr>
<td></td>
<td>• Section 3.1. Control Specifications: PLA review process;</td>
</tr>
<tr>
<td></td>
<td>• Section 3.2. CoC Adherence Mechanism review process;</td>
</tr>
<tr>
<td></td>
<td>• Section 3.3. CoC Adherence Seal issuing and Statement of Adherence publication;</td>
</tr>
<tr>
<td></td>
<td>• Section 3.4. Complaint management process;</td>
</tr>
<tr>
<td></td>
<td>• Section 3.5. Ongoing monitoring processes;</td>
</tr>
<tr>
<td></td>
<td>• Section 3.6. Code of Ethics review process;</td>
</tr>
<tr>
<td></td>
<td>• Section 3.7. PLA and OCF WG charter documents review process.</td>
</tr>
<tr>
<td>Adherence Mechanisms</td>
<td>The CoC adherence mechanisms defined in Section 1.2., below:</td>
</tr>
<tr>
<td></td>
<td>• Section 1.2.1. CoC Self-attestation;</td>
</tr>
<tr>
<td></td>
<td>• Section 1.2.2. CoC Third-party assessment.</td>
</tr>
<tr>
<td>STAR Registry</td>
<td>Archives the Self-attestation and Third-party Assessment applications submitted to and approved by the Monitoring Body, as well as the subsequent Adherence Seals granted regarding specific services of adherent CSPs.</td>
</tr>
<tr>
<td>Governance Groups</td>
<td>Roles and Responsibilities</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------------------------</td>
</tr>
</tbody>
</table>
| CSA Board of Directors ("Board") | The Board is the main governance committee within CSA. Among other tasks, the Board approves CSA’s annual plans and budget, as proposed by the CEO. The Board includes an Auditing Committee, which is a group within the Board made up of at least two (2) Board members, tasked with:  
  - Supporting and overseeing the implementation of the CoC Adherence Mechanisms by CSPs, as part of CSA’s STAR Program;  
  - Collaborating with and supporting Supervisory Authorities in matters related to Personal Data protection in the cloud (e.g., providing information/evidence about CoC-adherent CSPs). |
| Supervisory Authorities | Provide guidance, recommendations and best practices related to EU data protection laws (e.g., GDPR). |
| Open Certification Framework Working Group ("OCF WG") |  
  - Defines, reviews and approves changes in certification schemes and conformance methodologies, new or existing, within the CSA OCF/STAR Program;  
  - Manages the Conformity Assessment Methodologies / Adherence Mechanisms, and supervises related activities;  
  - Maintains the STAR Registry;  
  - Reports to the Board. |
| Privacy Level Agreement Working Group ("PLA WG") | • Defines, approves and updates changes to the Control Specifications: PLA;  
• Performs comparison activities between the Control Specifications: PLA and other privacy standards (i.e., mapping and gap analysis);  
• Manages Control Specifications: PLA governance and ensures process maintenance;  
• Reports back to the Board and communicates output results to the OCF WG. |
|---|---|
| Monitoring Body | • Assesses the eligibility of applicant CSPs to comply with the Control Specifications: PLA;  
• Monitors and verifies the ongoing compliance of adherent CSPs to the Control Specifications: PLA;  
• Manages complaints and issues corrective measures to non-compliant adherent CSPs;  
• Collaborates with Supervisory Authorities and reports any actions carried out with respect to the CoC (e.g., complaints management activities, audits performed...).  

The Monitoring Body includes a Monitoring Body Management Representative ("MBMR"), who is a member of the Monitoring Body tasked with carrying out key tasks on behalf of the Monitoring Body, further developed in Section 2.5., below. |
1.1 Control Specifications: PLA

The Control Specifications: PLA, presented in Part 2 of this CoC, is the technical standard that identifies the relevant Personal Data protection compliance requirements in the EU, and defines clauses and controls to manage compliance with those requirements. The Control Specifications: PLA constitute the fundamental Technical Component of this CoC.

1.2 Adherence Mechanisms to the CoC

CSPs who are willing to adhere to the requirements of the Control Specifications: PLA shall submit a Statement of Adherence (see Annex 2) to the CSA in accordance to the principles, policies and guidelines established in this document and in subsequent updates of the CoC Adherence Mechanisms developed by the OCF WG and issued by the CSA.

The Statement of Adherence shall be signed by the company/organisation legal representative and must be supported by the PLA [V3] Template (see Annex 1) either in the form of Self-attestation or in the form of Third-party Assessment.

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

It shall remain clear that a CSP must take into consideration all the Control Specifications: PLA, and it cannot declare adherence only to a chosen subset of them.

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

1. CoC Self-attestation;
2. CoC Third-party Assessment.

The process for achieving a CSA CoC Self-attestation is defined in Section 1.2.1., below.

The CoC Adherence Mechanisms define the objective, policy, mechanisms, scope, rules, requirements and processes for adhering to this CoC, and include the following:

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

The CoC Self-attestation is the voluntary publication by a CSP on the CSA STAR Registry (see Annex 3) of two (2) key documents:

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

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

- The CoC has been completed in all its sections,
- The details provided are sufficient to support an informed evaluation from a current or potential Cloud Customer; and
- To make sure that a “good faith” effort to completely address the Control Specifications: PLA was made.

The Monitoring Body will also verify the submitter has provided a public notice of compliance to the CoC on its website. Once verified that all the necessary conditions are satisfied, the Monitoring Body will publish the results of the Self-attestation on the CSA STAR Registry, and the Monitoring Body will provide a Self-attestation Adherence Seal to the adherent to the CoC.

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

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

The conditions for revoking an Adherence Seal and the mechanism of complaints are described in Section 3.3., “CoC Adherence Seals issuing and Statement of Adherence publication” and Section 3.4., “Complaints Management Process”, below.

It shall be noted that the publication on CSA STAR Registry and issuing of the Adherence Seal will be subject to an administrative fee.
A graphical summary of the process for assessment and approval of an application for adherence through Self-attestation is provided below:

**CSA GDPR COC Self Assessment Flow V3**

1. **Submission of GDPR Self-Attestation**
2. CSP submits:
   - Self-Attestation Statement of Adherence and
   - Self-Attestation results based on the PLA V3 Template
3. CSP pays submission fee
4. Credit Card Payment required prior to review process
5. Monitoring Body Performs eligibility assessment
6. CSP addresses comments and sends revision
7. Gaps identified; CSP to address questions and comments raised by Monitoring Body
8. Approved?
   - Yes: Adherence Seal is granted and Self-attestation is published on STAR Registry
   - No: Recurring 50% surcharge (from base fee) upon 3rd resubmission in approval process
1.2.2 CoC Third-party Assessment

A CoC Third-party Assessment is obtained via the validation of a CSP’s adherence to the Control Specifications: PLA by a Qualified CoC Auditing Partner (described in more detail below). The validation process aims to verify the following:

- The correct use of the CoC (e.g., did the CSP complete all sections in the Control Specifications: PLA? Does the content included in every section provide the necessary information on data handling and Processing?);
- The accuracy of information included in the CoC (e.g., is the information included in the submission truthful? Are statements supported by evidence?).

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

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

- Partner is accredited to ISO 17021 and ISO 17065;
- Partner employs at least one qualified CoC auditor that meets the competency requirements outlined in this CoC;
- Partner either employs or engages with at least one qualified CoC security expert for the relevant portions of the audit engagement (this person could also be the qualified CoC auditor).

Please note that CSA corporate members who are also Qualified CoC Auditing Partners will receive a complimentary listing on the CSA website.

---

169 Any company satisfying the relevant requirements can become a Qualified CoC Auditing Partner, but only those which are also CSA corporate members will automatically be listed as such on the CSA website as such. Those who are not CSA corporate members must pay a registration fee, in order to be listed on the CSA website as a Qualified CoC Auditing Partner.
Qualified CoC Auditors are professionals who comply with the following requirements:

1. Minimum 2 years’ experience on data protection legal compliance or the possession of a relevant professional certification (e.g., IAPP CIPP/E\textsuperscript{170}, ECPC-B DPO Certification\textsuperscript{171}, CSA CoC training and certification\textsuperscript{172}).

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

2. Audited company has a relevant information security certification (e.g., CSA STAR Certification/Attestation\textsuperscript{173}, ISO 27001):

Minimum 1-year experience in cloud security compliance or the possession of a relevant professional certification (e.g., CSA CCSK\textsuperscript{174}, ISC(2) CCSP\textsuperscript{175}).

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

Minimum 3 years’ experience on technical, physical and organisational compliance with respect to relevant information security certifications (e.g., CSA STAR Certification/Attestation, ISO27001) or the possession of a relevant certification (e.g., ISACA CISA\textsuperscript{176}, CSA STAR Certification Auditor\textsuperscript{177}, ISO 27001 Lead Auditor).

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

\textsuperscript{170} More information available at: https://iapp.org/certify/cippe/.
\textsuperscript{171} More information available at: https://www.maastrichtuniversity.nl/research/institutes/ecpc/professional-certification-education.
\textsuperscript{172} More information available at: https://gdpr.cloudsecurityalliance.org/.
\textsuperscript{173} More information available at: https://cloudsecurityalliance.org/star/levels/.
\textsuperscript{174} More information available at: https://cloudsecurityalliance.org/education/ccsk/.
\textsuperscript{175} More information available at: https://www.isc2.org/Certifications/CCSP.
\textsuperscript{177} More information available at: https://cloudsecurityalliance.org/star/auditors-and-consultants/.
Monitoring Body with the CoC Statement of Adherence (Annex 2) and PLA Template (Annex 1), on behalf of the adherent.

In case the Monitoring Body detects non-conformities in the CoC Statement of Adherence and/or PLA Template, feedback on this will be provided to the Qualified CoC Auditing Partner which arranged for the submission. The Qualified CoC Auditing Partner should then revise the submission in accordance with the feedback provided, liaising with the CSP as needed.

If no non-conformities are detected, or once the detected non-conformities are fully resolved, CSA will proceed with the publication of the CoC Statement of Adherence (Annex 2) and PLA Template (Annex 1) on the CSA STAR Registry, and the Monitoring Body will issue a CoC Third-party Assessment Adherence Seal to the adherent.

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

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

It shall be noted that the publication on CSA STAR Registry and issuing of the Adherence Seal will be subject to an administrative fee.
A graphical summary of the process for assessment and approval of an application for adherence through Third-party Assessment is provided below:

**GDPR COC Third-party Flow**

1. **Submission of CoC Third-party Assessment application to qualified CoC auditing partner**
   - Qualified CoC auditing partner submits quote for the assessment of the application under the CoC’s Control Specification (based on number of days, scope and complexity, among other relevant factors).

2. **Audit Scheduling**
   - Pre-assessment requested?
     - No
     - Yes

3. **Stage I Audit**
   - Approved?
     - No
     - Yes

4. **Stage II Audit**
   - Compliant with ISO/IEC 17065 and other specified standards, as outlined in Part 3 of the CoC

5. **Approved?**
   - No
     - Final Report issued and Third-party Assessment submitted to Monitoring Body
     - Gaps identified; CSP to corrects gaps
   - Yes
     - Monitoring Body performs eligibility assessment
     - Adherence Seal is granted and Third-party Assessment is published on STAR Registry
     - Gaps identified; CSP to correct gaps prior to Stage II Audit

6. **Approved?**
   - Yes
   - Audit partner is invoiced for certification fee
   - Gaps identified; Audit Partner to correct gaps (in liaison with the CSP) and re-submit
   - Gaps identified; CSP to correct gaps prior to Stage II Audit

- Adherence Seal is valid for a period of 12 months (renewable)
1.3 Code of Ethics

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

1.4 PLA WG and OCF WG Charters

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

2. GOVERNANCE GROUPS, ROLES AND RESPONSIBILITIES

The governance of the CoC and its Technical Components (Control Specifications: PLA, Adherence Mechanisms and code of ethics) is a shared responsibility between the PLA WG and the OCF WG, and CSA.

2.1 PLA WG

The PLA WG is responsible for defining, approving and updating changes to the technical standard/code of practice, i.e., the Control Specifications: PLA (currently in its third version, i.e., PLA [V4]). This body also provides expert opinions to the Monitoring Body when complaints about CoC Self-attestation or Third-Party Assessment are submitted. The PLA WG Charter defines the objectives and scope, membership, structure and responsibilities; the relations with other relevant CSA WGs; and relevant external activities, operations, communications methods, decision-making processes, activities, deliverables, duration and Intellectual Property Right (IPR) policy of the WG. Each member has the right to propose changes to the CoC.

Participation in the PLA WG is voluntary and open to any privacy, data protection and/or data security subject-matter experts, regardless of their affiliation.

2.2 OCF WG

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

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

2.3 Cloud Security Alliance (CSA)

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

- Maintaining a public registry of issued CoC Adherence Seals (STAR Registry). Each entry includes as minimum the following information: (i) name and description of organisation, (ii) name and description of service for which the CoC is relevant, (iii) CoC entry, (iv) version of the CoC used (currently V4), (v) validity of seals, (vi) name of auditing organisation/auditor (if applicable);
- Maintaining a public registry of Qualified CoC Auditing Partners;
- Maintaining a website where information and guidelines about the CoC concept, approach and technical standards are provided, together with the requirements, process and cost of the Adherence Mechanisms;
- Developing and maintaining the CoC:
  - Defining guidelines on how to submit and how to review the CoC Self Attestation;
  - Reviewing CoC Self-attestations and verifying minimum requirements are met;
  - Maintaining a mechanism for filing complaints;
  - Providing guidance on handling conflicts;
  - Creating an advisory body to support CSA in the implementation and oversight of the scheme;
- Assuring transparency and integrity throughout the development of standards, implementation of seals and management;
- Approving the OCF charter revision and extension;
- Approving the PLA charter revision and extensions;
- Setting and reviewing the adherence fee;
- Approving CoC qualified auditor training partners;
- Providing a public accounting of all fees and other revenues collected and their disposition in the management of this program.

2.4 Collaboration and supporting actions toward Supervisory Authorities

The CoC Governance Groups agree to collaborate and support national data protection authorities (Supervisory Authorities) in matters related to Personal Data protection in the cloud according to the terms below.
With respect to collaboration, and upon request by a Supervisory Authority or the EDPB, the CoC Governance Groups will reasonably comply with requests to 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 Supervisory Authority toward the relevant national parliament and/or public authorities).

With respect to supporting actions, and upon request by a Supervisory Authority or the EDPB, the CoC Governance Groups also will reasonably comply with requests to do the following:

- Promote awareness between the CoC self-attested and third-party-assessed companies about measures issued by Supervisory Authorities (general provisions, as well as specific provisions – when issued towards a CoC self-attested or third-party-assessed company);
- If a Supervisory Authority carries out an inspection of a CoC-adherent company, provide the Supervisory Authority with all information and evidence available in CSA about the CoC-adherent company. In these cases, CoC Governance Groups will act as the CSA point of reference.
- Review and, if necessary, withdraw the CoC Adherence Seal of a company subject to penalties issued by a Supervisory Authority.
- Inform the EDPB and/or relevant Supervisory Authorities in case a CoC Self-attestation and/or Third-party Assessment Adherence Seal is revoked.

2.5 Monitoring Body

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

The Monitoring Body applies the corrective measures and sanctions set out in the CoC.

This section describes how this committee – i.e., the Monitoring Body – meets the requirements for its accreditation by the CompSA, under the terms of Article 41 GDPR, the EDPB CoC Guidelines and the CNIL Accreditation Requirements.

Recourse to subcontracting does not result in the delegation of responsibilities: in any case, the Monitoring Body remains responsible to the Supervisory Authority for the performance of its tasks, including monitoring compliance with the CoC.

The CompSA for the CoC – the CNIL – has accredited the Monitoring Body for the purposes of Article 41 GDPR.
2.5.1 Independence

The Monitoring Body is an internal body established by CSA, which is functionally separated from other CSA functions or departments. The Monitoring Body, including any of its contractors, are is appropriately independent from any CSP (whether CoC members or not), other functions or departments within CSA and the cloud computing sector, ensuring the continuity of its monitoring duties for the duration of its accreditation.

Independence is achieved by the following means:

- The Monitoring Body has its own staff and is autonomous in its own management;
- Monitoring Body staff may not assume other accountabilities or functions within CSA which may create a conflict of interests with the tasks they perform within the Monitoring Body;
- The Monitoring Body has its own separate¹⁷⁸ and adequate budget;
- The appointment, remuneration and removal/dismissal of the Monitoring Body Management Representative (“MBMR”) is subject to approval of the Board;
- Members of the Monitoring Body cannot be dismissed or penalised in any way as a result of the performance of their tasks;
- The MBMR directly (functionally) reports to and interacts with the Board;
- The activities of the Monitoring Body are free from interference, whether internal or external to CSA. The Monitoring Body is free to perform its tasks without taking instructions from CSA or suffering any sort of sanctions or interference from CSA in the performance of its tasks (e.g., the Monitoring Body is free to decide on the management of complaints, the performance of audits and their scopes, its working procedure and the communication of its results, as well as on the imposition of sanctions against CoC members).

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

- Approving the rules and procedures concerning the Monitoring Body and any amendments to them;
- Approving the annual risk-based (monitoring) plan of the Monitoring Body;
- Approving the budget and resource plan of the Monitoring Body;
- Receiving communications of the MBMR as to the achievement of the goals and activities as mentioned in its (monitoring) plan;

¹⁷⁸ CSA has different sources of revenue which make up its funding. In order to ensure the continued independence and impartiality of the MB, CSA undertakes to allocate an appropriate budget to the MB (approved by the Board on the basis of annual budget and resource plans) which is kept appropriately independent from the source of revenue represented by the CoC submission and renewal fees paid by CoC members.
• Approving decisions of the Monitoring Body with regard to the appointment, remuneration, replacement and/or dismissal of the MBMR.

The Monitoring Body also acts independently from CoC members in performing its tasks and exercising its powers.

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

Where required by the CompSA or otherwise, the Monitoring Body will produce the results of its continuous assessment and will demonstrate how any such risks it may have identified are removed or minimised, so as to safeguard the Monitoring Body’s independence.

2.5.2 Absence of a conflict of interests

The Monitoring Body has implemented review systems to ensure its activities do not result in a conflict of interest, and that the Monitoring Body will remain free from external or internal influence, whether direct or indirect.

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

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

The Monitoring Body and its members must warrant that they do not have any stake or standing related to CSP’s which could compromise their judgement or create a conflict of interest with their monitoring role. Furthermore, the Monitoring Body and its members must refrain from any action that is incompatible with their tasks and duties. They shall neither seek nor take instructions from any person, organisation or association (including CSA or any CSP) in the performance of their tasks and duties.
The members of the Monitoring Body may perform the tasks assigned to the Monitoring Body in relation to CSPs to which they have previously provided consulting or other services, insofar as the nature of those services does not impair their objectivity in the performance of the tasks assigned to the Monitoring Body.

The individual objectivity of Monitoring Body members is managed by the MBMR when assigning members to perform specific tasks.

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

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

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

2.5.3 Expertise

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

The MBMR shall – at least annually – confirm the required expertise of the Monitoring Body to the Board.

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

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

• In-depth understanding of data protection issues;
• Expert knowledge of the cloud computing industry and other related activities which are the subject-matter of the CoC;
• Appropriate operational experience and training in the carrying out of compliance monitoring activities (e.g. auditing), preferably in the domain of privacy and data governance;

• Successful completion of the CSA GDPR Certification – Lead Auditor Training course;

• Care and skills needed in order to perform their tasks in a reasonably prudent and competent manner;

• The personnel shall have taken part in at least two full audits, from their preparation to the final conclusions, in the last three years;

• Any personnel with a legal profile must:
  — Hold, at least, a first-year Master’s degree or an equivalent degree in the legal field;
  — Have at least two years’ professional experience in the field of personal data protection (e.g., consulting, litigation, etc.);

• Any personnel with a technical profile must:
  — Hold, at least, a bachelor’s degree or an equivalent degree in the field of computer sciences, information systems or cybersecurity;
  — Have undergone at least a two-day training course on relevant standards for information system security management (e.g., regulations, standards, methods, best practices, risk management);
  — Have at least two years’ experience in the field of information system security.

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

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

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

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

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

2.5.4 Resources and staffing

The Monitoring Body must be provided with sufficient resources and staffing, so that it can perform its tasks in an appropriate manner. These resources must be proportionate to the expected number and size of the CoC members which the Monitoring Body is to supervise, as well as the complexity and degree of risk of the Personal Data Processing activities which those CoC members may carry out. The Monitoring Body includes a specific clause in any contract signed with subcontractors to ensure the confidentiality of Personal Data that may, where applicable, be disclosed to the subcontractor during the monitoring tasks. The Board is responsible for ensuring this and keeping documentation to demonstrate that the above is complied with.

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

2.5.5 Established procedures and structures

Appropriate governance structures and procedures are in place which adequately assess the eligibility of CSPs to sign up to and comply with the CoC. There are also appropriate governance structures and procedures to ensure that the provisions of the CoC are capable of being met by the CoC members and compliance with its provisions is monitored. These procedures are outlined in the eligibility assessment (Section 2.5.6.), complaints handling (Section 2.5.7.) and monitoring sections (Section 2.5.12.) below.

Whenever it performs any of its tasks, the Monitoring Body must ensure that all relevant documentation provided by CSPs (including audit evidence), and produced by the Monitoring Body (e.g., audit plans, audit findings and reports) are kept under conditions of strict confidentiality – the Monitoring Body should not disclose such documentation, or information
therein, outside of the context of its tasks, unless this is necessary to comply with its obligations under the CoC, or with applicable legal obligations upon the Monitoring Body or CSA.

As soon as such documentation is no longer necessary for the performance of its tasks, or for any other legitimate purpose (including where further retention may be necessary to comply with legal obligations upon the Monitoring Body or CSA, or necessary to allow CSA to establish, exercise or defend against any legal claims or Supervisory Authority inquiries brought in connection with the Monitoring Body’s tasks), it shall be definitively and securely destroyed.

### 2.5.6 Eligibility assessment

As required by Article 41(2)(b) GDPR, the Monitoring Body has established procedures which allow the mandatory eligibility assessment of CSPs concerned to apply the CoC. The following workflow applies:

- **The Monitoring Body will receive CoC adherence applications submitted by CSPs, with reference to a given service. As noted above, these may be Self-attestation applications (Section 1.2.1., above) or Third-party Assessment applications (Section 1.2.2., above).**

- **Self-attestation:** The Monitoring Body will check all statements made by the CSP in their application, to ensure that the statements adequately address the CoC’s controls, and to decide whether or not to approve the adherence. If approved, the Monitoring Body will grant a Self-attestation Adherence Seal for the CSP’s service (after which the CSP will be entitled to declare that service as adherent to the CoC). In so doing, the Monitoring Body may avail itself of external counsel; in any case, the Monitoring Body will retain responsibility for, ultimately, deciding on whether or not to grant adherence.

- **Third-party Assessment:** The Monitoring Body will rely on the evaluation carried out and conclusions described by the Qualified CoC Auditing Partner in respect of the applicant CSP’s service – the Monitoring Body will only perform a formal check, to ensure that the conclusions adequately address all of the CoC’s controls and, if so, grant a Third-party Assessment Adherence Seal for the CSP’s service (after which the CSP will be entitled to declare that service as adherent to the CoC); given that the Monitoring Body will ultimately retain responsibility for deciding on whether or not to grant adherence. It should be stressed that the Monitoring Body will perform more substantial assessments of the CSP’s practices after CoC adherence is granted, through the CoC’s ongoing monitoring mechanisms, but also *ad hoc* through the complaints management procedure.

In either case, as noted further below, the Monitoring Body will, concerning adherent CSPs, carry out targeted audits on the basis of the criteria laid down in the CoC’s complaints management (Section 2.5.7., below, and Annex 7) and ongoing monitoring procedures (Section 2.5.12., below, and Annex 8).
For the avoidance of doubt, CSPs are not allowed to declare a service as adhering to the CoC before they have been granted an Adherence Seal for that service by the Monitoring Body (which can only be done after a successful eligibility assessment by the Monitoring Body).

2.5.7 Transparent complaints handling

If a CoC member infringes the terms of the CoC, in particular by maintaining practices which are incompatible with the statements made by the CoC member in the submissions made to apply for a CoC Adherence Seal (whether under the framework of Self-attestation or Third-party Assessment), the Monitoring Body will take immediate corrective measures, as deemed appropriate by the Monitoring Body, to address the situation. If any relevant issues arise regarding a qualified CoC Auditing Partner, the Monitoring Body will investigate the matter and take the corrective measures deemed appropriate to each case.

In particular, the Monitoring Body may act against an adhering CSP or a Qualified CoC Auditing Partner as a result of an infringement detected through a complaint submitted by, for example, a Cloud Customer, a Data Subject or another CSP.

If such a complaint is received, the Monitoring Body will investigate this complaint. If the investigation of the complaint leads to the conclusion that the CoC member violated one or more provisions of the CoC, the Monitoring Body will take such immediate corrective measures, as deemed appropriate by the Monitoring Body to address the situation. The measures to be taken should aim at stopping the infringement and preventing recurrence of the same or similar infringements in the future. Such remedial actions and sanctions are described in Annex 7.

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

Where required, the Monitoring Body shall inform CSA, the CoC member, the CompSA and all other Concerned SAs about the measures taken and their reasoning, without undue delay.

The Monitoring Body will generate periodic reports under the supervision of the MBMR to document the results of the investigation of complaints, and at least one annual report encompassing all complaint-related activities carried out during that year. This annual report will be shared with the Board, the CompSA and other Concerned SAs, where relevant, and will be published on CSA’s website.

Further detail is provided in Annex 7 to the CoC.
2.5.8 Communication with the competent Supervisory Authority

The monitoring body framework allows for the effective communication of any actions carried out by the Monitoring Body to the CompSA and other Concerned SAs in respect of the CoC.

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

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

Furthermore, the Monitoring Body will promptly and directly communicate to the CompSA, in writing:

- Any specific cases where it decides to suspend or revoke Adherence Seals granted to CSPs, as a result of a failure to properly comply with the requirements of the CoC (including the reasons justifying corrective measures taken);
- Any substantial changes to the Monitoring Body (in particular, to its structure and/or organisation), which may call into question its independence or expertise, or which may create a conflict of interests within the Monitoring Body or any of its members.

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

2.5.9 Review mechanisms

Appropriate review mechanisms shall be in place to ensure that the CoC remains relevant and continues to contribute to the proper application of the GDPR. The PLA WG establishes and performs review mechanisms to adapt to any changes in the application and interpretation of the law or the occurrence of new technological developments which may have an impact upon the Personal Data Processing carried out by CoC members.
In addition, a process of periodic\textsuperscript{179} review is applied to all CSA services and processes to identify possible improvement opportunities.

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

Changes to the rules and procedures concerning the Monitoring Body may be triggered by an initiative presented by the MBMR to the Board.

Revisions to the CoC will consider feedback from the Monitoring Body’s activities, including the results of audits carried out on CSPs and Qualified CoC Auditing Partners, feedback received from Supervisory Authorities, Cloud Customers, CSPs and Data Subjects, complaints and all other associated information.

\textbf{2.5.10 Legal status}

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

Within the EU, CSA has offices set up as legal entities in Finland and Greece – as an internal body, the Monitoring Body can therefore be considered as being established within the EU.

\textbf{2.5.11 Continuous improvement}

The MBMR develops and maintains a quality assurance and improvement program with respect to all tasks of the Monitoring Body. The effectiveness of the Monitoring Body and the monitoring process is continually improved through regular reviews carried out by the Monitoring Body, covering the complaints handling, monitoring and other procedures, as well as the very governance structure of the Monitoring Body. These reviews – carried out under the supervision of the MBMR – will consider the results of audits carried out on CSPs and Qualified CoC Auditing Partners, feedback received from Supervisory Authorities, Cloud Customers, CSPs and Data Subjects, complaints and all other associated information.

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

\textsuperscript{179}At least once a year, but could be more frequent depending on the legal and industry landscape.
Such reviews must be held at least once annually; ad hoc reviews can be triggered whenever the MB deems necessary. The MBMR reports the outcome of those reviews to the Board.

2.5.12 Monitoring

There are two parts to the monitoring process. One is complaints management (see Section 2.5.7., above, Section 3.4., below, and Annex 7), and the other is the duty upon the Monitoring Body to actively monitor. The Monitoring Body has a process in place that allows for random checking of CSPs, to annually audit their compliance and effectiveness of the process as attested to by the CSP upon their adherence to the CoC. Upon the detection of irregularities, the sanctioning process will be followed.

There is also a process in place to sample reports and third-party assessments provided by Qualified CoC Auditing Partners, along with their adherence to the requirements imposed upon them in the CoC. Upon the detection of irregularities, the Monitoring Body will take any corrective action deemed appropriate. When it enforces the application of corrective measures or issues sanctions in accordance with the code of conduct, the Monitoring Body shall ensure that the code member’s rights are respected.

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

The Monitoring Body monitors CoC members through procedures that will ensure compliance with the CoC, and monitors Qualified CoC Auditing Partners through procedures that will ensure compliance with the relevant requirements of the CoC which address them. The Monitoring Body has powers to take immediate corrective measures if a CoC member acts outside the terms of the CoC, which may even lead to suspension or exclusion from the CoC (see Section 2.5.7., above). Additionally, the Monitoring Body has the authority to report any findings to the Board, which may take action to suspend or exclude a Qualified CoC Auditing Partner from performing third-party assessments, if through the Monitoring Body’s review it is found that the Qualified CoC Auditing Partner does not comply with the requirements for its qualification as such under the CoC, or with associated accreditation standards (i.e., ISO 17065).

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

Further detail is provided in Annex 8 to the CoC.
2.5.13 Personal Data Protection

In order to ensure a consistently high level of Personal Data protection throughout its organisation and across the various jurisdictions in which it operates, CSA has implemented an internal set of policies, procedures, guidelines, templates and other tools to regulate its internal Personal Data Processing activities – the CSA Group Data Protection Compliance Framework (“CSA G-DPCF”).

Recognising the standard of protection established by the GDPR as one of the highest standards for personal data protection worldwide, as well as the fact that the principles enshrined in the GDPR are internationally acknowledged, CSA has chosen to align the CSA G-DPCF’s components on the GDPR’s requirements and obligations, even beyond the GDPR’s territorial scope of application.

As an internal committee within CSA, the Monitoring Body is required to abide by the CSA G-DPCF whenever Personal Data is Processed in connection with their activities. This allows the Monitoring Body to ensure that it handles Personal Data, when performing its monitoring tasks, in a manner compliant with the GDPR.

In particular, as laid out in CSA’s internal guidelines on the engagement of Processors, the Monitoring Body (or CSA, on the Monitoring Body’s behalf) must enter into written agreements, aligned with Art. 28 GDPR, with any subcontractors engaged to assist in the performance of the Monitoring Body’s tasks.

3. GOVERNANCE PROCESSES AND RELATED ACTIVITIES

The Governance Processes of the CoC defines the relationship between the Governance Groups and a set of activities with which they are required to comply, in order to maintain a consistent management process for every Technical Component.

3.1 Control Specifications: PLA review process

The Control Specifications: PLA will be subject to periodic reviews, since it is subject to changes in the EU Personal Data protection-related legal framework. The Control Specifications: PLA review process falls under the responsibilities of the PLA WG. The CSA undertakes, through the PLA WG, to timely reflect any relevant legislative changes in the Control Specifications: PLA, and to promptly notify adhering CSPs to comply with these changes.
The Control Specifications: 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 Control Specifications: PLA to the most current relevant legislations.

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

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

CSPs adhering to the Control Specifications: PLA will be promptly notified of any changes and requested to make the necessary internal adjustments in order to comply with them in practice. CSPs will be given a timeframe within which to apply these adjustments, depending on the impact of changes made to the Control Specifications: PLA – thirty (30) days for minor changes, sixty (60) days for relevant changes, and ninety (90) days for critical changes.

A change to the Control Specifications: PLA that might increase the time/effort/resources required by the Monitoring Body to perform a review and monitor the CoC might entail an increase of the submission fees charged to CSPs.

Any changes to the Control Specifications: PLA, after approval of the CoC as a Code of Conduct under Art. 40 GDPR, will be notified to the competent Supervisory Authority, under Art. 40(5) GDPR. The Monitoring Body monitors the application of the changes decided by the PLA WG through the monitoring process (Annex 8).

The current version of the Control Specifications: PLA focuses both on the prior (Data Protection Directive and its implementations in the EU Member States) and actual EU relevant legislation concerning the protection of Personal Data (GDPR).

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

3.2 CoC Adherence Mechanism review process

The OCF WG is responsible for triggering the review of the CoC Adherence Mechanisms, 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, as well as to the CoC Adherence Mechanisms.

3.3 CoC Adherence Seal issuing and Statement of Adherence publication

The Monitoring Body is responsible for reviewing, approving and managing CoC Self-attestation and Third-party Assessment Adherence Seals issuing, the Statement of Adherence submission processes and relevant complaints. More specifically:

3.3.1 CoC Self-attestation

The Monitoring Body is responsible for reviewing any CoC Self-attestation and relevant complaints submitted by any third party. In the former case, the Monitoring Body shall verify that minimum requirements have been satisfied. In the latter case, the Monitoring Body shall verify the validity of the complaint and based on the input of the PLA WG, shall take relevant actions.

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

If minimum requirements are not satisfied or if a complaint is deemed valid, the Monitoring Body will take one of the following actions: a) request an amendment to the CoC Self-attestation, or b) remove the Self-attestation from the CSA STAR Registry and revoke the Adherence Seal.

3.3.2 CoC Third-party assessment

CSA is responsible for publishing the CoC Third-party assessment in the STAR Registry, upon notification from the Monitoring Body (based on information received from a Qualified CoC Auditing Partner) that the auditee has passed the audit.

The Monitoring Body is responsible for notifying a Qualified CoC Auditing Partner that issued an assessment if a related complaint is filed. In that case, the Qualified CoC Auditing Partner shall verify the validity of the complaint and provide feedback to the Monitoring Body.

If the complaint is deemed valid, the Monitoring Body shall temporarily suspend the seal or revoke it. Accordingly, CSA shall remove the assessment from its STAR Registry.
3.4 Complaint management process

The complaint management process defines how the Monitoring Body will receive, manage and address complaints received which are related to the CSA CoC Self-attestation and Third-party assessment mechanisms.

Please refer to Annex 7 for a detailed description of the complaint management process followed by the Monitoring Body.

3.5 Ongoing monitoring processes

Other than handling the Complaint Management Process (see Section 3.4., above, and Annex 7), the Monitoring Body is also tasked with the duty to actively monitor compliance with the CoC. This is achieved through a process allowing for random checking of adhering CSPs during annual audits, in order to assess their compliance with the terms of their CoC submissions, on the basis of which their CoC Adherence Seal was issued. Any irregularities detected will trigger a corresponding sanctioning process.

Please refer to Annex 8 for a detailed description of the ongoing monitoring processes followed by the Monitoring Body, regarding CSPs which become CoC members.

3.5.1 Qualified CoC Auditing Partner monitoring process

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

These exercises must abide by the following terms:

- Audits may be carried out on-site or remotely, depending on the scope of the audit.
- Audits will take place by random sampling of Qualified CoC Auditing Partners, under the same terms as described above (Section 2.5.12., above), with the necessary adaptations;
- There must be continuous monitoring of Qualified CoC Auditing Partners, including via the performance of at least one updated accreditation visit every two years, on-site or remotely, and one witness or review audit every two years.
- Witness audits must be performed periodically at a representative site, in order to verify proper delivery under the terms of the CoC and ISO 17065;
- Accreditation visits, witness audits or review audits may be performed in the same year for a Qualified CoC Auditing Partner, as long as there is at least one annual accreditation visit to review the following documentation:
  - The management system of that Qualified CoC Auditing Partner;
- The expertise and competence of the personnel of that Qualified CoC Auditing Partner tasked with facilitating Third-Party Assessment submissions for CSPs (as indicated in Section 1.2.2., above);
- The process followed by that Qualified CoC Auditing Partner to assess CSPs seeking to apply for a Third-Party Assessment submission;
- The records and procedures used by that Qualified CoC Auditing Partner to track and report on CSPs they have assessed under the CoC.

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

### 3.6 Code of Ethics review process

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

### 3.7 PLA and OCF WG charter documents review process

CSA is responsible for approving any OCF WG and PLA WG charter revision and extension requests.
ANNEX 1: PLA [V4] TEMPLATE

Please refer to the attached file (CoC GDPR_Annex 1_Compliance_Assessment_Template).
ANNEX 2: STATEMENT OF ADHERENCE TEMPLATE

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

1. Name and URL/Address

<table>
<thead>
<tr>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL/Address</td>
</tr>
</tbody>
</table>

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

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

<table>
<thead>
<tr>
<th>Service 1 name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service 2 name</td>
</tr>
<tr>
<td>...</td>
</tr>
<tr>
<td>Service n name</td>
</tr>
</tbody>
</table>

3. Adherence Mechanism

Self-attestation

4. Scope of Adherence

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

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
</table>

5. Control Specifications: PLA version used

<table>
<thead>
<tr>
<th>Version ID</th>
<th>(e.g., v. 3.2)</th>
</tr>
</thead>
</table>
6. Issue/Expiry Date

<table>
<thead>
<tr>
<th>Issue Date</th>
<th>Expiry Date</th>
</tr>
</thead>
</table>

7. Legal representative/DPO signed by

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

a. As of this date, the services listed in (2) adhere to the CSA CoC requirements (see CSA CoC Section 3.3, “CoC Adherence Seal issuing and Statement of Adherence publication”).

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

<table>
<thead>
<tr>
<th>Name</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td></td>
</tr>
<tr>
<td>Date</td>
<td></td>
</tr>
</tbody>
</table>
© 2013-2020 Cloud Security Alliance – All Rights Reserved.

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

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

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

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

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

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

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

Notices
All trademark, copyright or other notices affixed onto the Cloud Security Alliance PLA Code of Conduct must be reproduced and may not be removed.
CSA Code of Conduct (CoC): Statement of Adherence
Third-party Assessment

1. Name and URL/Address

<table>
<thead>
<tr>
<th>Name</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>URL/Address</td>
<td></td>
</tr>
</tbody>
</table>

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

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

<table>
<thead>
<tr>
<th>Service 1 name</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Service 2 name</td>
<td></td>
</tr>
<tr>
<td>...</td>
<td></td>
</tr>
<tr>
<td>Service n name</td>
<td></td>
</tr>
</tbody>
</table>

3. Adherence Mechanism

3rd Party Assessment

4. Scope of Adherence

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

| Description |            |

5. Control Specifications: PLA version used

| Version ID (e.g., v. 3.2) |            |
6. Assessing Body

| Name |

7. Country of Issuing

| Name |

8. Seal Number

| Number |

9. Issue/Expiry Date

| Issue Date | Expiry Date |

10. Legal representative/DPO signed by

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

a. As of this date, the services listed in (2) adhere to the CSA CoC requirements (see CSA CoC Section 3.3., “CoC Adherence Seal issuing and Statement of Adherence publication”).

b. The Third-party Assessment Adherence Seal will have a validity of 12 months from the day of its issuance and should be renewed after this period. Moreover, third-party assessments must be revised every time there is a change in the company’s relevant policies or practices.

| Name |
| Title |
| Date |
The Cloud Security Alliance Code of Conduct for GDPR Compliance and its Annexes (e.g., Annex 1: PLA Template, Annex 2: Statement of Adherence Template (collectively, “CSA Code of Conduct for GDPR Compliance”) is licensed by the Cloud Security Alliance under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 International License (CC-BY-NC-ND 4.0).

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

**Attribution**
You must give credit to the Cloud Security Alliance, and link to the Cloud Security Alliance Code of Conduct webpage located at [https://gdpr.cloudsecurityalliance.org](https://gdpr.cloudsecurityalliance.org). You may not suggest that the Cloud Security Alliance endorsed you or your use.

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

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

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

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

**Notices**
All trademark, copyright or other notices affixed onto the Cloud Security Alliance Code of Conduct must be reproduced and may not be removed.
ANNEX 3: THE CSA STAR PROGRAM AND OPEN CERTIFICATION FRAMEWORK (OCF)

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

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

---

**Open Certification Framework**

<table>
<thead>
<tr>
<th>Type of Audit</th>
<th>Audit Frequency</th>
<th>Security</th>
<th>Privacy</th>
</tr>
</thead>
<tbody>
<tr>
<td>STAR Level 3</td>
<td>Continuous Auditing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>STAR Level 2</td>
<td>Level 2 + Continuous Self-Assessment</td>
<td></td>
<td></td>
</tr>
<tr>
<td>STAR Level 1</td>
<td>Continuous Self-Assessment</td>
<td></td>
<td></td>
</tr>
<tr>
<td>STAR Level 1</td>
<td>Self-Assessment</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

CSA Code of Conduct for GDPR Compliance © Copyright 2013-2020, Cloud Security Alliance. All rights reserved.
In 2012, the CSA STAR Program launched as a means of supporting the CSA STAR effort and managing the implementation of the OCF. Currently the STAR Program offers the Self-Assessment (Level 1) and Third Party Assessment-based Certification/Attestation (Level 2). The continuous monitoring/auditing-based certification is under development.

The relationship between OCF Levels is the following:

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

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

CSA encourages organisations aiming to certify at OCF Level 2 to first self-assess at OCF Level 1.
ANNEX 4: CODE OF ETHICS

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

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

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

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

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

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

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

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

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

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

7. Review and Changes
This Statement of Ethics shall be reviewed and updated as necessary, annually by the Board of Directors. Any changes to the Statement of Ethics shall be communicated to all CSA Parties.
Privacy Level Agreement Working Group

Charter 2017
EXECUTIVE OVERVIEW

Data protection compliance is becoming increasingly risk-based.\(^1\) Data controllers and processors are accountable for determining and implementing in their organisations appropriate levels of protection of the Personal Data they process. In such decision, they have to take into account factors such as state of the art of technology; costs of implementation; and the nature, scope, context and purposes of processing; as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.\(^2\) As a result, Cloud Service Providers (CSPs) will be responsible for self-determining the level of protection required for the Personal Data they process.

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

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

- Cloud customers of any size with a tool to evaluate the level of Personal Data protection offered by different CSPs (and thus to support informed decisions)\(^3\)
- CSPs of any size and geographic location with a guidance to comply with European Union (EU) Personal Data protection legislation and to disclose, in a structured way, the level of Personal Data protection they offer to customers.

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

- Fair and transparent processing of Personal Data;

---

\(^1\) See, e.g., Preamble 83 and Articles 25, 32, 33, 34 and 35 of the GDPR.

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

\(^3\) “All cloud providers offering services in the European Economic Area (EEA) should provide the cloud client with all the information necessary to rightly assess the pros and cons of adopting such services. Security, transparency, and legal certainty for the clients should be key drivers behind the offer of cloud computing services.” WP29 Cloud Computing Opinion, p. 2; “A precondition for relying on cloud computing arrangements is for the controller [cloud client] to perform an adequate risk assessment exercise, including the locations of the servers where the data are processed and the consideration of risks and benefits from a data protection perspective.” p. 4, id.
The information provided to the public and to data subjects (as defined in Article 4 (1) GDPR);

The exercise of the rights of the data subjects;

The measures and procedures referred to in Articles 24 and 25 GDPR and the measures to ensure security of processing referred to in Article 32 GDPR;

The notification of Personal Data breaches to Supervisory Authorities (as defined in Article 4 (21) GDPR) and the communication of such Personal Data breaches to data subjects; and

The transfer of Personal Data to third countries.

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

BACKGROUND

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

Based on the work already created by the, i.e. PLA V1 and PLA V2, the CSA PLA WG will develop “Privacy Level Agreement [V3] Code of Conduct. A Compliance Tool for Providing Cloud Services in the European Union” (PLA [V3]) to address the upcoming change to the data protection laws of the European Union and Europe Economic Area Member States to the General Data Protection Regulation, Regulation (EU) 2016/679 also known at the GDPR. 4

PRACTICAL USE

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

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

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

WORKING GROUP SCOPE AND OBJECTIVES

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

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

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

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

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

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

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

WORKING GROUP STRUCTURE AND FUNCTIONING

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

Sub-Work Groups
Ad hoc sub-working groups comprised of subject matter experts may be formed to plan or execute any related outreach, awareness, or research opportunities. Such sub-working groups shall report directly to the PLA Working Group.
The Working Group may also choose to allow resource sharing between cloud communities and other CSA working groups to assist in the timely completion of projects, programs and other activities needed to support/enable the working group’s defined body of work.

**Membership**

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

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

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

**Operations**

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

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

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

**Communications Methods**

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

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

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

**Definition of a majority**

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

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

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

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

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

**Voting procedures**
The voting procedures are as follows:

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

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

Before commencing a vote, the Chair(s) shall review any request as to the manner in which the voting shall be conducted, and then shall formally announce the voting procedure to be applied and the issue to be submitted to the vote. The Chair(s) shall then declare the beginning of the vote and, when the vote has been taken, shall announce the results.
In the case of a secret ballot, the secretariat shall at once take steps to ensure the secrecy of the vote.

**Deliverable approval and endorsement process**

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

**DELIVERABLES**

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

**DURATION**

This charter will be valid until 31 March 2019
Open Certification Framework Working Group

Charter

2019
Table of Contents

WORKING GROUP EXECUTIVE OVERVIEW
  Working Group Scope and Responsibilities
  Relationship to Cloud
WORKING GROUP MEMBERSHIP
  Working Group Structure
    Co-Chairs
    Committees
    Sub-Work Groups
ALIGNMENTS WITH OUTSIDE GROUPS
  Operations
    Advisory
    Research Lifecycle
    Peer Review
COMMUNICATIONS METHODS
  Infrastructure & Resource Requirements
  Work Group Conference Calls and In-person Meetings
DECISION-MAKING PROCEDURES
IPR POLICY
DELIVERABLES/ACTIVITIES
DURATION
CHARTER REVISION HISTORY
WORKING GROUP EXECUTIVE OVERVIEW

Mission

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

Working Group Scope and Responsibilities

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

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

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

The CSA OCF is based upon the technical best practices and control frameworks defined within relevant CSA’s Working Group, such as for instance the Cloud Control Matrix (CCM), the Consensus Assessment Initiative Questionnaire (CAIQ), the Level Agreement research initiatives, as well as the IoT Control Framework.

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

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

Eligible members are of the OCF WG

- CSA enterprise customer corporate members (Enterprise Users)
- CSA solution provider corporate members (CSPs)
- International, Regional, National Regulatory Bodies, Agencies and Institutions (European Commission, European Data Protection Board (EDPB) ENISA, BSI Germany, METI, IDB – IDA, NIST, FedRAMP, USA DoD, USA FTC, etc)
- SDOs and other organizations (e.g. ISO/IEC / JTC 1 / SC27, SC38, ITU-T, ETSI, W3C, ISACA, AICPA, JIPDEC, JASA, etc)
- Representatives of relevant research project not directly run under the auspices of the CSA, but relevant to the activities of the OCF WG (e.g. EU-SEC.)
- Representative of trade and users’ associations (e.g. EuroCIO, DigitalEurope, ECSO, etc.)

Working Group Structure

Co-Chairs

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

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

Committees

The working group may designate and organize subcommittees to aid in research with the initiatives pertaining to the subject matter of the working group.
Sub-Work Groups
Ad hoc sub-work groups comprised of subject matter experts may be formed to plan or execute any related outreach, awareness or research opportunities. Such sub-working groups shall report directly to the main working group.

Alignments with Other Groups

The OCF working group may also choose to allow resource sharing between cloud communities and other CSA working groups to assist in the timely completion of projects, programs and other activities needed to support/enable the working group’s defined body of work, on demand basis. The list other groups that the OCF working group will be working closely with includes, but is not limited to:

- CSA Cloud Control Matrix Working Group:
  - Specifically collaborating on the implementation of CCM related controls across the 3 levels of assurance and transparency of STAR
- EU-SEC Project:
  - Specifically collaborating on:
    - defining, testing and implementing the process for mutual recognition between STAR and other relevant certification and attestation.
    - defining, testing and implementing the process for Continuous Auditing based certification.
- CSA PLA Working Group:
  - Specifically collaborating on the development of a scheme to certify organization against the requirements included in the PLA Code of Practice v3.1.
- CSA MAST Initiative Working Group:
  - Specifically collaborating on development of a scheme (tentatively named CSA STAR Mobile) to certify mobile applications against the requirements to be developed from the MAST whitepaper
- IoT Matrix
  - Evaluate the extension of the STAR program to IoT (i.e. implementation of a certification for Edge Computing and IoT devices)
- International Standardization Council (ISC):
  - Specifically collaborating on the identification of international standardization opportunities for the STAR program components as well as relevant input from SDOs that could serve to improve the program.
• Additional groups:
  o EC Cloud Certification Group
  o ENISA
  o ISO SC 27
  o NIST
  o AICPA
  o The German Federal Office for Information Security (BSI)
and other (e.g. ANSSI)

Operations

Advisory
The CSA Working Group will be advised by various SMEs and councils including but not limited to the International Standardization Council (ISC) and CSA Executive Team to ensure that the research under the working group is within the scope of the CSA and aligns with other industry partner research. The research will remain unique to industry and make reference to any redundant or replicated works.

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

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

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

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

Decision-making Procedures

A. Definition of a majority

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

B. Abstentions of more than fifty percent

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

C. Voting procedures

1) The voting procedures are as follows:
   a) By a show of hands as a general rule, unless a secret ballot has been requested; if at least two members, present and entitled to vote, so request before the beginning of the vote and if a secret ballot under b) has not been requested, or if the procedure under a) shows no clear majority
   b) By a secret ballot, if at least five of the members present and entitled to vote so request before the beginning of the vote (online voting is applicable)
2) The Chair(s) shall, before commencing a vote, observe any request as to the manner in which the voting shall be conducted, and then shall formally announce the voting procedure to be applied and the issue to
be submitted to the vote. The Chair(s) shall then declare the beginning of the vote and, when the vote has been taken, shall announce the results.

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

Deliverables/Activities

The list of actions includes:

- Completion and implementation of the OCF Level 3 – STAR Continuous Certification.
- Implementation of the Mutual Recognition procedures into the STAR Program.
- Completion and implementation of the Privacy Certification and Self-Assessment (currently based on the GDPR Code of Conduct / PLA Code of Practice)
- Produce awareness and training material for the various STAR Program target audiences.
- Evaluate the feasibility of Edge Computing as an IoT extension of STAR.

Each of the above-mentioned actions will have one or more associated deliverables. The final list of deliverables will be included in the STAR Program annual work plan.

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

Duration

This charter will be valid until 30 April 2021 and it will be updated to reflect any changes in the OCF WG objectives and priorities.
## Charter Revision History

<table>
<thead>
<tr>
<th>November 2015</th>
<th>March 2016</th>
<th>Sept 2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>April 2019</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
ANNEX 7: COMPLAINT MANAGEMENT PROCESS

The main purpose of the complaint management process is to allow any Data Subject, CSP, Cloud Customer or individual (jointly referred to as “complainants” in this Annex) to report issues related to the CoC, such as (but not limited to) notifying:

- Inconsistencies between the information reported in a CoC Self-attestation submission and/or CoC Third-party Assessment submission made by a CSP, and the conditions/terms practically applied by that CSP in the provision of the relevant service(s);
- Misleading or inaccurate information reported in the CoC Self-attestation and/or CoC Third-party Assessment submission made by a CSP;
- Behavior which represents a breach of the CSA Code of Ethics;
- Cases of conflict of interest related to members of the CoC Governance Groups;
- Issues concerning a Qualified CoC Auditing Partner, or any Qualified CoC Auditors engaged by that Qualified CoC Auditing Partner.

Complaints:

Feedback is important in the development and management of the CoC and associated Adherence Seals. Feedback can be used to identify dissatisfaction as much as satisfaction. It may help to identify areas where changes could be made in the way the CoC operates in practice. Feedback can also ensure proper implementation, maintenance and monitoring of the CoC.

Dissatisfaction should be duly resolved and corrective action should be properly addressed.

The Monitoring Body has a transparent and easily accessible complaint procedure in order to ensure that:
- The Monitoring Body handles feedback in a positive manner;
- The performance in dealing with feedback is monitored;
- The Monitoring Body derives maximum benefit from any criticism, compliment or comment; and
- Corrective actions and improvement actions are implemented (if necessary).

Appeal:

During the process of complaint management or in relation to any decisions laid down by the Monitoring Body regarding a CoC member, conflicts sometimes occur that cannot be resolved via the normal line processes. These can range from disagreements on interpretation, to decisions related to the awarding, suspension or removal of Adherence Seals. The appeal process exists to enable such disputes to be settled in a formal and appropriate manner.
Process/Policy

Complaints fall into four categories:
1. Dissatisfaction comments;
2. Complaints;
3. Misuse of an Adherence Seal; and
4. Other comments that are obtained as a result of all feedback related to compliments, dissatisfaction comments, complaints, misuse of logo, centrally received through any platform at CSA or the Monitoring Body.

CSA and the Monitoring Body receiving appeals/complaints shall ensure that the members of the Monitoring Body engaged in the appeals/complaints-handling process are different from those who were involved in the management of the relevant complaint, carried out related CoC reviews or audits and made the decision under appeal.

Submission, investigation and decision on appeals/complaints shall not result in any discriminatory actions against the complainant or the appellant.

If a complaint is received that indicates a CoC member has broken the rules of the CoC, the Monitoring Body shall take immediate suitable measures. If the CoC member appeals any decision of the Monitoring Body, no action will be taken until the appeal process has been completed by means of a final decision.

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

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

The Monitoring Body may summarily dismiss a complaint if it is deemed, on a case-by-case basis, to be manifestly unfounded or excessive.

Complaints may be manifestly unfounded if the complainant has no clear intention to report an actual breach of CoC Control Specifications: PLA, or if the complaint is malicious in intent and is used to harass a CoC member with no real purposes other than to cause disruption. Factors that may indicate this include:

1. The individual having explicitly stated, in the complaint itself or elsewhere, that they intend to cause disruption;
• The complaint making unsubstantiated accusations against the CSP or specific CSP staff;
• The complaint targeting a particular member of CSP staff against whom they have some personal grudge; or
• The complainant systematically or frequently (e.g., once a week) filing different complaints against CSPs as part of a campaign with the intention of causing disruption.

Complaints may be excessive where they repeat the substance of previous requests (and a reasonable interval between them has not elapsed), or where they overlap with other requests.

Where a complaint is dismissed on these grounds, the Monitoring Body must inform the complainant of the dismissal, and provide a justification for this. The Monitoring Body must, in particular, clearly explain why such a complaint was found to be manifestly unfounded and/or excessive, based on specific circumstances applicable to the case at hand.

Complaints concerning CoC members

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

Where the CoC member is requested to undergo a third-party audit, this audit will be performed by an independent Qualified CoC Auditing Partner designated by the Monitoring Body, after it has been verified that no conflict of interests exists (the selected Qualified CoC Auditing Partner will be required to meet the requirements imposed upon the Monitoring Body, under Section 2.5.2 of the CoC). When performing this audit, the Qualified CoC Auditing Partner should comply with the CoC member’s security measures, to the extent that this is feasible and does not prevent the Qualified CoC Auditing Partner from performing its tasks.

Any dissatisfaction comments registered through a CSA or Monitoring Body portal with regard to CoC services will be forwarded to the Monitoring Body. The MBMR will assign the complaint to the member of the Monitoring Body responsible to communicate with the respective CoC member. This member of the Monitoring Body will investigate the claim under the supervision of the MBMR. The MBMR will report the outcome of important issues to the Board. The complaint and all related information will be documented in the complaint system, together with the resolution status details. When the complaint is settled, the record will be closed.
The Monitoring Body member that manages the complaint should ensure that the company being complained about is registered with CSA and that the complaint is within the scope of the CoC. It should also be checked whether the complainant has already lodged its complaint in writing to the relevant company. If not, this should be incentivized, as a manner to potentially allow for swift remediation of the complaint. Consent of the complainant is required for the disclosure of his/her name and other personal information that could lead to the identification of the complainant.

Any complaint received from a Supervisory Authority, including the CompSA, or other regulatory body, will be reported immediately to CSA.

In the event that the Monitoring Body accepts a complaint submitted regarding a CoC member (meaning that the complaint is considered valid and that a relevant infringement of the CoC has been detected), the Monitoring Body will take immediate suitable measures against the CoC member. The aim of these measures will be to stop the infringement and prevent its future recurrence. Measures taken may range from formal warnings requiring the implementation of corrective actions within a specified deadline, to temporary suspension or definitive revocation of the CSP’s CoC Adherence Seal:

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

- For minor issues, or where the CoC member does not respond adequately and in a timely manner to a formal warning issued by the Monitoring Body, the Monitoring Body will temporarily suspend the CoC member’s CoC Adherence Seal until the Monitoring Body is satisfied that the issue has been fully resolved;

- For major issues, the Monitoring Body will revoke the CoC member’s CoC Adherence Seal.

The Monitoring Body will also make public, through CSA’s website, any corrective measures imposed upon CoC members which result in a suspension or revocation of a CoC Adherence Seal.

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

In case a complaint received concerns inaccuracies, inconsistencies or any other issues related to the CoC third-party assessment mechanism, the Monitoring Body may request additional information from the CoC member in question (i.e., the CSP which is the subject of the
complaint) and will immediately notify the Qualified CoC Auditing Partner responsible for issuing the relevant third-party assessment. That Qualified CoC Auditing Partner will be tasked with investigating the complaint and producing a report with its findings. When performing this investigation, the Qualified CoC Auditing Partner should comply with the CoC member’s security measures, to the extent that this is feasible and does not prevent the Qualified CoC Auditing Partner from performing its tasks. Based on the complaint report produced by the Qualified CoC Auditing Partner, and on any further information at its disposal or which it may collect (e.g., from the complainant, the Qualified CoC Auditing Partner or the CoC member), the Monitoring Body will take immediate suitable measures against the CoC member, under the same terms as described above.

In case of suspension or revocation of Adherence Seals, the CompSA will be directly notified without undue delay, along with any other Concerned SAs (where legally required). The Monitoring Body may also decide to make public the actions or sanctions imposed upon an infringing CoC member, particularly where the issue is deemed “major”.

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

The Monitoring Body will generate periodic reports – under the supervision of the MBMR – to document the results of the investigation of complaints, and at least one annual report encompassing all complaint-related activities carried out during that year. This annual report will be shared with the Board, the CompSA and other Concerned SAs (where legally required).

All processed complaints will be reviewed during the Monitoring Body’s regular reviews.

Complaints concerning Qualified CoC Auditing Partners
The complaints management process concerning a complaint submitted regarding a Qualified CoC Auditing Partner – including complaints that a Qualified CoC Auditing Partner no longer meets the requirements imposed upon it by the CoC, or that an assessment produced by a Qualified CoC Auditing Partner has been fraudulently or inaccurately produced – will follow the same process as described for CoC members, with the below adaptations.

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

Appeal
Formal Communication
Where a CoC member wishes to dispute the conclusions and/or the sanctions or corrective actions imposed upon it, as notified upon conclusion of the investigation of a complaint, an appeal must be filed with the Monitoring Body within seven (7) calendar days of the notice. If an appeal is filed, no corrective actions will be enforced until the appeal process has been completed and a final decision has been handed down by the Monitoring Body.

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

**Establishing an Appeal Panel**

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

**Arranging a meeting of the Appeal Panel**

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

**Conduct of the hearing by the Appeal Panel**

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

- The Appeal Panel hears, in confidence, the evidence and opinion presented by the appellant;
- The Appeal Panel hears, in confidence, the evidence and opinion presented by the Monitoring Body and/or the complainant;
- The Appeal Panel evaluates the representations made by all parties and, after due consideration (and further questioning, if required), makes a final decision. The decision will be taken by majority of the Appeal Panel and is final and conclusive.
Involvement of CompSA and other regulatory bodies

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

The Appeal Panel Chairman records the proceedings and the final decision of the Appeal Panel. The Appeal Panel Chairman also notifies the Monitoring Body, CSA, the CompSA and other Concerned SAs (where legally required) of the final decision, in writing, within five (5) working days from the date of the Appeal Panel meeting.

Redress

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

Corrective Action

CSA will consider the findings of the Panel and take any additional appropriate corrective and preventive action as required.
ANNEX 8: MONITORING/AUDIT PROCESS

Monitoring CoC Member Submissions
The Monitoring Body will use generally recognized best practices for monitoring/auditing Self-attestation and third-party assessment CoC adherence submissions to provide a high-level of confidence that:

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

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

Monitoring methods used will be carried out in a graduating sampling format that is based on a sampling of a minimum of 5 samples or a sampling of 2% of the submissions, whichever is greater (Figure 1)

Sampling shall be increased based on factors deemed relevant by the Monitoring Body from the privacy and data protection-related perspective, including (but not limited to):

- The complexity and risks involved in the Processing activities performed by a given CoC member;
- The overall number of CoC members at any given time;
- The geographical scope of CoC members;
- The number of complaints received concerning a given CoC member; and
- The sensitivity of Personal Data which may be Processed by a given CoC member.

The Monitoring Body will document, for each sampling exercise performed with an increased sample size, a justification for the specific increase.
Each CoC member included within a sample will be assessed in terms of their compliance with the CoC’s controls, in order to verify the effectiveness of the implementation of those controls in practice. As a minimum, 10% of the CoC’s controls will be assessed randomly, based on the scope and complexity of the CoC members in question. If further questions arise regarding the compliance and effectiveness of the measures put in place by a CoC member to address some or all of the CoC’s controls, the Monitoring Body may increase the sample of assessed controls until there is sufficient evidence to determine the CoC member’s overall compliance or non-compliance with the CoC.

Numbers will be rounded based on standard mathematical rules. Samples will be pulled annually on a random basis. Reviews may be pulled more frequently depending on past reviews.
and the outcome of those reviews. Any CoC members that had non-conformities\(^1\) must submit written corrective action and be included in the next sampling plan to confirm implementation and effectiveness of the corrective action.

Members of the Monitoring Body which are assigned to perform a specific review must collectively meet the minimum competency requirements, as outlined in Part 3, Section 2.5.3. of the CoC (Expertise).

**Specific elements of the review**

**Announcement of the review and the information gathering process**

Reviews are carried out either on-site or virtually, depending on the scope of the review.

Reviews are announced by the Monitoring Body to the CoC member in writing and at least 3 months before. The announcement also entails the scope of the review and a list of all the information required.

The Monitoring Body will contact the CoC member to make an appointment for the on-site or virtual review at the time of earliest convenience for the CoC member and the Monitoring Body and other parties involved. The requested information should be sent in by the CoC member at least 6 weeks prior to the actual review.

If - after investigation of the received information - any additional information seems to be necessary according to the Monitoring Body, this will also be requested for in writing. Any additional information should be provided to the Monitoring Body by the CoC member within 2 weeks after the request.

In case of any undue delay or non-cooperation by the CoC member, the Monitoring Body has the power to impose appropriate sanctions.

**Language**

Reviews will be carried out in English.

**Basic elements of the review**

---

\(^1\)**Major Non-Conformity**: Based on objective evidence, the absence of, or a significant failure to implement and/or maintain conformance to the controls of the CoC (i.e., the absence of, or failure to implement, a CoC control); or a situation which would, on the basis of available objective evidence, raise significant doubts as to the capability of the measures implemented by the CoC member to achieve the stated policy and objectives of a control.

**Minor Non-Conformity**: Represents either a system weakness or minor issue that could lead to a major non-conformance if not addressed. Each minor non-conformity should be considered for potential improvement and to further investigate any system weaknesses, for possible inclusion in the corrective action program.
When carrying out an annual audit exercise, the Monitoring Body seeks to meet the following goals:

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

The Monitoring Body will, within the scope of the review:

a) Require the CoC member to demonstrate that the terms of its Self-attestation / third-party assessment submission are materially accurate and implemented in relation to the service(s) for which the assessment was submitted\(^2\), using the sampling process defined above (Monitoring CoC Member Submissions);

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

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

d) Ensure the integrity and traceability of evidence when collecting necessary information.

### Audit Reports

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

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

The report shall contain:

\(^2\) Typically virtually but the right for an on-site assessment is reserved and will be exercised at the discretion of the Monitoring Body in cases of continued non-conformance or high-risk environments.
a) The names of the members of the Monitoring Body that performed the review;
b) Significant audit trails followed and audit methodologies utilized;
c) Observations made, both positive (e.g. noteworthy features) and negative (e.g. potential nonconformities) regarding the requirements of the CoC and the effectiveness of its interpretation;
d) Opportunities for improvement of compliance (if appropriate);
e) Comments on the conformity of the CoC member’s practices with the requirements of the CoC. This should include a clear statement of conformity or nonconformity, referring to the applicable CoC controls and, where relevant, drawing comparisons with the results of previous audits carried out over that CSP;
f) A summary of the most important observations, positive as well as negative, regarding the implementation and effectiveness of the requirements of the CoC;
g) A recommendation as to whether the CoC member should be considered in full/partial compliance with the requirements of the CoC and, where relevant, corrective measures which should be enforced against that CoC member, along with supporting reasoning. Measures proposed, as well as timeframes to be afforded to the CoC member in order to correct detected irregularities (where relevant), must be adequate in light of the severity of the irregularities and the associated risks for Cloud Customers and Data Subjects; and
h) Any written or oral comments made by the CoC member upon receipt of the above observations, comments, summary and recommendation.

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

For minor-nonconformities, where the CoC member does not respond adequately and in a timely manner to a formal warning issued by the Monitoring Body, the Monitoring Body may temporarily suspend the CoC member’s CoC Adherence Seal until the Monitoring Body is satisfied that the issue has been fully resolved.

For major-nonconformities, the Monitoring Body may revoke the CoC member’s CoC Adherence Seal.

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

**Special reviews**
The activities necessary to perform special reviews shall be subject to special provision if a CoC member makes major modifications to its system or if other changes take place which could affect the basis of its data privacy process.