



云安全联盟

GDPR合规 行为准则

隐私级别协议工作组，2020年9月

说明与感谢

云安全联盟（CSA）的通用数据保护条例（GDPR）合规行为准则（CoC）是在CSA内部由Paolo Balboni教授（ICT法律咨询公司的创始合伙人；马斯特里赫特大学法学院中的欧洲隐私和网络安全中心的隐私、网络安全和IT合同法教授；欧洲隐私协会主席）和Françoise Gilbert（Greenberg Traurig合伙人；《全球隐私和安全法》作者和编辑；PLI隐私和安全法研究所联合主席）主持的一个专家工作组（WG）开发完成。Paolo Balboni教授也是隐私级别协议（PLA）的主要作者。Daniele Catteddu、Eleftherios Skoutaris、John Di Maria和Martim Taborda Barata对本准则的创作也做出了很大贡献。

隐私级别协议（PLA）工作组由云服务提供商（CSP）、地方监管机构和独立的安全与隐私专业人士的代表组成。¹

我们还要感谢CSA工作人员Hillary Baron、Damir Savanovic和Kendall Scoboria的支持。

我们的赞助商Gemalto和Shellman也为本准则的出版做出了巨大贡献。

¹ 本文件的第三部分，即PLA CoC治理部分，是在欧盟委员会资助的欧洲安全认证框架（EU-SEC）项目的帮助下制定的。

版权声明

© 2013-2020 CSA—版权所有

云安全联盟（CSA）欧洲通用数据保护条例（GDPR）合规行为准则（CoC）及其附件，例如：附件1：隐私级别协议（PLA）模板，附件2：遵守声明模板（统称为“CSA GDPR合规行为准则”）由CSA根据知识共享署名-非商业性使用-禁止演绎4.0国际许可协议（CC-BY-NC-ND 4.0）授权。

分享

您可以通过任何媒介或任何形式分享和分发CSA GDPR合规行为准则。

署名

您必须提及CSA，并链接到位于<https://gdpr.cloudsecurityalliance.org/>的CSA GDPR网页。您不得暗示CSA认可您或您的使用。

非商业性使用

您不得使用、共享或重新分发PLA CoC以获得商业收益或金钱补偿。

禁止演绎

如果你对CSA GDPR合规行为准则本创作进行了重混、转换、依据本创作进行再创作等行为，你不得再次公开传播经过修改的创作。

不得增加额外限制

您不得运用法律条款或技术措施，来限制他人实施本许可证允许的任何行为。

商业许可

如果您出于商业营收的目的，希望调整、转换、构建或分发CSA GDPR合规行为准则的副本，您必须首先获得相应的CSA的许可。请联系我们info@cloudsecurityalliance.org。

声明

所有在CSA GDPR合规行为准则上出现的商标、版权或其他声明必须同时被复制，不得删除。

中文版说明

云安全联盟（CSA）GDPR合规行为准则（CoC）于2020年发布了更新的4.0版本，与上一版相比，从体量和内容上均有较大改动。鉴于数据安全与隐私合规成为普遍关注的话题，CSA大中华区（CSA GCR）数据安全工作组牵头进行了新版本的翻译工作，隐私法律工作组支持并进行审校。

翻译组长：

高巍

翻译组专家成员（按姓氏拼音排序，排名不分先后）：

仇蓉蓉、付艳艳、李安伦、李芊晔、王安宇、王彪、王永霞、姚凯、张淼、张明敏

审校组长：

原浩

审校组专家成员（按姓氏拼音排序，排名不分先后）：

江澎、邢海韬、魏晓刚、张元恺、赵晔、曾令平

注：

本准则正文中有较多缩写，为便于读者的阅读，正文中第一次出现缩写时使用：中文全称（英文缩写）的格式，例如：云安全联盟（CSA），该术语再次出现时使用英文缩写表述。

翻译过程中难免有一些不当之处，敬请读者联系CSA GCR数据安全工作组给与修正。联系邮箱：research@c-csa.cn。

序言

2018 年 5 月 25 日，欧洲议会通过的《通用数据保护条例》(GDPR)法案正式生效实施。这意味着欧盟对个人信息保护及其监管达到了前所未有的高度，堪称史上最严格的数据保护法案。

云安全联盟 CSA 发布的 CoC for GDPR Compliance (CSA GDPR 合规行为准则)，旨在为云服务提供商(CSP)、云消费者、及相关企业提供 GDPR 合规解决方案，并提供涉及云服务提供商应提交的关于数据保护级别的透明性准则。这个准则为各种规模的客户提供工具来评估其个人数据保护水平从而支持决策。它也指导任何规模和地点的云服务提供商，遵守欧盟 (EU)个人数据保护法规，并以结构化的方式披露其提供给客户的个人数据保护级别。

GDPR 对于中国业务范围涉及欧盟成员国领土及其公民的企业进行合规运营、避免高昂处罚，以及对中国与数据相关的法学研究都具有重要意义。CSA 发布的 GDPR 合规行动准则在德国、法国等欧盟国家受到首席隐私保护官的认可，在国际和国内即将推出 GDPR 合规自检和第三方认证。CSA 大中华区组织专家进行翻译为中文版本，对中国今后借鉴它把《数据安全法》和《个人信息保护法》进行落地实施也会有很大帮助，相信一定会有助中国企业对 GDPR 的认知并帮助它们在欧洲的业务避免隐私风险。



李雨航
云安全联盟大中华区主席

目录

I. 简介.....	1
II. 背景信息.....	3
III. CSA GDPR 合规行为准则的结构.....	6
第一部分 CSA CoC 的目标、范围、方法、假设和注释说明.....	7
1. CSA CoC 的目标.....	8
2. 范围和方法.....	10
3. 假设.....	14
3.1 云客户的内部尽职调查.....	15
3.2 云客户的外部尽职调查.....	15
4. 说明性注释.....	16
5. 词汇表.....	17
6. 参考文献列表.....	21
第二部分 CSA 行为准则控制指南：隐私级别协议.....	27
1. CSP 的合规和职责声明.....	28
2. CSP 相关联系人及其角色.....	32
3. 数据处理方式.....	34
3.1 指令.....	34
3.2 服务变更.....	35
3.3 个人数据位置.....	36
3.4 子处理者.....	37
3.5 在云客户系统上安装软件.....	39
3.6 数据处理协议（或其他具有约束力的法律行为）.....	40
3.7 通过设计和默认的设置保护数据.....	42
4. 记录保存.....	44
5. 数据传输.....	45
6. 数据安全措施.....	48
7. 监督.....	52
8. 个人数据违规.....	52
9. 数据转移、迁移和回传.....	55
10. 对处理的限制.....	56
11. 数据留存、归还和删除.....	57
11.1 数据留存、归还和删除策略.....	57
11.2 数据留存.....	57
11.3 为遵守特定部门的法律要求而留存数据.....	58

11.4	数据归还和/或删除.....	58
12.	与云客户的合作.....	59
13.	法律要求的披露.....	60
14.	云客户的补救措施.....	60
15.	CSP 保险策略.....	62
第三部分 CSA 行为准则治理和遵守机制.....		63
1.	技术构建.....	65
1.1	控制指南：PLA.....	68
1.2	CoC 遵守机制.....	68
1.3	道德准则.....	74
1.4	隐私级别协议（PLA）工作组及开放认证框架（OCF）工作组章程.....	74
2.	治理工作组、角色和职责.....	74
2.1	PLA 工作组.....	74
2.2	OCF 工作组.....	74
2.3	云安全联盟（CSA）.....	75
2.4	针对监管机构的协作和支持行动.....	76
2.5	监督机构.....	76
3.	治理过程和相关活动.....	86
3.1	控制指南：PLA 的评审过程.....	86
3.2	CoC 遵守机制的评审过程.....	87
3.3	CoC 认证标识的颁发和遵守声明的发布.....	87
3.4	投诉管理过程.....	88
3.5	持续监督过程.....	88
3.6	道德准则评审过程.....	89
3.7	PLA 和开放认证框架工作组章程文件评审过程.....	90
附录 1：隐私级别协议[v4]模板.....		1
附录 2：遵守声明模板.....		1
附录 3：CSA STAR 计划和开放认证框架（OCF）.....		1
附录 4：道德准则.....		1
附录 5：隐私级别协议工作组章程.....		1
附录 6：开放认证框架工作组章程.....		1
附录 7：投诉管理过程.....		1
附录 8：监督/审计过程.....		1
附录 9：ENISA 技术指南：安全目标.....		1

I. 简介

考虑到EDPB的行为准则（CoC）指南¹，CoC的第1部分以及提交CoC时的封面，包含了详细说明CoC目的、CoC范围以及它将如何促进GDPR有效应用的“解释性声明”。

数据保护合规越来越以风险为基础²。数据控制者和处理者有职责在其组织中确定并实施对所处理个人数据的适当保护级别。在这样的决定中，他们必须考虑到各种因素，如技术级别，实施成本，处理的性质、范围、背景和目的，以及对自然人³权利和自由产生不同可能性和严重程度的风险。因此，云服务提供商（CSP）将负责确定所处理个人数据所需的保护级别。

正是在这种情况下，CSA创建了CoC。

CoC的目标是为CSP和云客户提供GDPR合规的解决方案，以及关于CSP所能提供的数据保护级别的透明性指南。

CoC主要是为了提供：

- 任何规模的云客户都可以使用的一个工具，来评估不同CSP所提供服务的个人数据保护级别（从而支持知情决策）⁴
- 任何规模和地点的CSP都可以使用的一个指南，可以用来遵守欧盟个人数据保护法规，并以结构化方式披露他们向客户所提供服务的个人数据保护级别。

尽管CoC的直接目标受众是CSP（而不是云客户），因为只有CSP才会实际提供其遵守CoC的服务。然而，CoC通过隐私级别协议（PLA）控制措施（控制指南：PLA），最终使CSP和云客户（以及数据主体和整个云社区）都受益。

CoC的合规基于两个主要的技术部分，即“控制指南：PLA”（这是一个技术

¹ 下文第一部分第6节中包含一个词汇表，它包括本准则中使用的定义和缩写，以及那些与立法和其他参考资料有关的词汇。

² 例如序言部分83条，和GDPR第25，32，33，34和35条款。

³ 例如GDPR第24，25，32，35和39条款。

⁴ WP29云计算指南，第2页：“所有在欧洲经济区（EEA）提供服务的云供应商应向云客户提供所有必要的信息，以正确评估采用此类服务的利弊。安全性、透明度和客户的法律确定性应该是提供云计算服务的主要驱动力。”，第4页：“（……）依赖云计算安排的前提条件是控制者[云客户]进行充分的风险评估工作，包括处理数据的服务器位置以及从数据保护角度考虑风险和利益。”

标准），规定了GDPR中包含的要求；以及与CoC相关的遵守机制。

由于CoC主要侧重于法律要求，CSA建议将该CoC与CSA的其他最佳实践和认证⁵结合起来采用，如云控制矩阵（CCM）和安全，信任，保证和风险（STAR）认证（或STAR证明，或STAR自评估），它们围绕信息安全的技术控制和目标提供额外指导。

在这种情况下，采用信息安全技术标准，如云控制矩阵或其等同物（如ISO 27001，由ISO 27017或ISO 27018支持，或AICPA可信服务标准），及其相关的认证体系（如STAR认证、STAR证明、STAR自评估、ISO 27001或SOC2）将证明CSP已经实施了安全项目或信息安全管理体系（ISMS），充分保护消费者数据免受风险评估和数据保护影响评估（DPIA）中概述的威胁的证据。

为了避免疑问：

- 上述体系下的认证（或证明）（如ISO 27001、STAR认证、SOC2证明）并不意味着自动遵守CoC。CSP仍需通过所提供的遵守机制来提交他们的服务，以实现遵从性：自评估（第三部分，第1.2.1节和第3.3.1节）或第三方评估（第三部分，第1.2.2节和第3.3.2节）。
- 同样，遵守CoC也不意味着自动获得上述任何一种认证。

CoC反映了与云计算相关的GDPR要求，是CSA STAR的组成部分。

如下文第3部分第1.2节所述，提交其一项或多项服务以遵守CoC的CSP将受“控制指南：PLA”（第二部分）中的控制措施约束，并且必须遵守所有适用于他们的规定。否则，在监督机构对投诉进行调查（下文第3部分，第2.5.7节，以及附件7）或持续的CoC合规监测活动（下文第3部分，第2.5.12节，以及附件8）中，可能会导致CSP被监督机构处罚。

最后，需要注意的是，对CoC的任何遵守行为都不会降低CSP和云客户遵守GDPR的职责，且不影响国家监管机构的任务和权力。

⁵ 为避免疑问，这里提到的认证体系不是第42条规定的“认证机制”，而是与信息安全和/或云安全有关的认证体系。这些其他体系下的认证不是CoC的先决条件；相反，CSP可能也想考虑将其作为加强其信息安全实践的一种手段（这将有助于满足CoC的安全相关控制措施—见第2部分，第6项控制措施）

II. 背景信息

作为CoC的所有者，CSA是世界领先的组织，致力于定义和提高对最佳实践的认识，以帮助确保安全的云计算环境。CSA是一个非营利性组织，其成员包括全球CSP和云安全供应商的很大一部分（超过350名成员），以及一些云客户。此外，CSA在全球范围内拥有超过9万名个人会员和85个国家和地区分会。

自2013年以来，CSA一直致力于为云环境制定隐私和数据保护指南和最佳实践。本准则由CSA内部的专家工作组（WG）制定，该工作组由CSP、当地监管机构和独立的安全和隐私专业人士的代表组成（“PLA工作组”，或“PLA WG”）。它于2017年11月21日发布，最后一次更新于2019年5月，以反映欧洲数据保护委员会（EDPB，原第29条数据保护工作组）的最新指南，并包含对法国国家信息与自由委员会（CNIL）安全指南的参考。

欧盟云服务销售隐私级别协议大纲（PLA [v1]）于2013年2月发布，作为一种自律协调工具，提供了一种结构化的方式来向当前和潜在客户传达CSP提供的个人数据保护级别。PLA [v1]不仅基于欧盟个人数据保护的强制性法律要求，而且还基于最佳实践和建议。

PLA [v1]得到了一些监管机构⁶的认可，并收到了积极的反馈。它曾被用来制定欧盟关于云计算相关的个人数据保护事项的进一步研究、最佳实践和CoC。

然而，在PLA [v1]发布后，PLA工作组意识到，CSP、云客户和潜在客户仍在努力识别整个欧盟个人数据保护合规的必要基线。

因此，PLA工作组将这些指南更新为PLA [v2]，以便为云计算市场上的各种参与者提供合规工具，而不仅仅是一种透明机制。

PLA [v2]是基于实际的、强制性的欧盟个人数据保护法律要求（95/46/EC指令及其在欧盟成员国的实施方式）。

2016年5月，GDPR开始生效，并从2018年5月25日起直接适用于所有欧盟成员国。随着GDPR的引入，PLA工作组立即发现，CSP、云客户和潜在的云客户需要在云环境中遵守新的法律的指导。因此，PLA工作组开发了PLA [v3]，这是一个反映GDPR所规定的新义务的合规工具⁷。

⁶ 特别是，PLA [v1]得到了CNIL本身以及爱尔兰监管机构的认可。英国ICO和意大利Garante，以及希腊、斯洛文尼亚和加泰罗尼亚的监管机构也提供了积极的反馈。

⁷ 相关要求已被添加到PLA [v2]中，以反映GDPR中规定的新职责和义务。

PLA应被视为隐私和数据保护透明度、保障和合规的实践准则。

PLA的当前版本，即[v4]，将随着相关立法、意见、指南和主管当局的发展，按要求进行更新。

因此，PLA [v4]通过利用PLA [v2]的结构，在数据保护指令中规定的欧盟个人数据保护法律要求及其在欧盟成员国的实施方式，以及GDPR的要求之间建立连续性。

PLA [v4]的结构用于帮助CSP、云客户和潜在的云客户管理从旧的欧盟数据保护制度到新的欧盟数据保护制度的过渡，并有助于将GDPR正确应用于云行业。

PLA [v4]规定了GDPR在云环境中的应用，主要涉及到以下几类要求：

- 个人数据的公平和透明处理。
- 向公众和数据主体提供的信息（根据GDPR第4（1）条的定义）。
- 行使数据主体的权利。
- GDPR第24条和第25条提及的措施和规程以及GDPR第32条提及的确保安全处理的措施。
- 向监管机构（根据GDPR第4（21）条的定义）通报个人数据违规情况，并向数据主体通报此类个人数据违规情况；及
- 将个人数据转移到第三国。

PLA [v4]进一步寻求解决云计算领域在隐私和数据保护方面的几个关键特点，包括面临的具体问题，如⁸：

- **资源共享问题**，由于使用共享系统和基础设施来处理与多个不同的云客户和数据主体类型相关的个人数据，可能出现潜在的冲突。
- **共享职责模式**，云引入了一种新的模式，在CSP和云客户之间分配和分派信息安全职责。有时这会在各方之间造成混淆，特别是在“将某些安全措施实施的职责转嫁给CSP”和“保持云客户自身的职责与义务”之间的区别。
- **执法要求**，位于多个司法管辖区的CSP可能会发现自己被法律要求向公共

⁸ 见WP29云计算意见，其中强调了许多这样的问题。

机构披露与云客户有关的个人数据，这可能会违反欧盟数据保护法。

- **复杂的外包链**，CSP可能会雇用位于全球不同地区的众多子处理者，从而形成难以管理的合同安排，并且通常不会为云客户提供足够的手段来反对以这种方式使用其数据（包括不向这些云客户提供足够的透明度）。
- **处理数据主体请求的障碍**，在这种情况下，云服务可能没有得到适当的配置来，例如：允许删除请求、允许限制处理或满足及时和适当的转移请求。
- **对提供云服务的条款进行修改**，这可能会影响到在提供服务期间处理云客户数据的条件。
- **缺乏隔离**，CSP（由于他们对其代为处理的多个云客户的数据的控制）有可能决定将其代为处理的不同云客户的数据关联起来，用于可能未经这些云客户授权的其他目的。
- **CSP对数据进行进一步未经授权的处理**，例如使用云客户数据来进一步开发分析/定制算法或用于程序化广告目的。
- **向云客户和CSP分配数据保护角色的复杂度**，考虑到CSP可能开展的各种类型的活动（其中一些可能是作为处理者，另一些可能是作为控制者）以及欧盟委员会最近关于联合控制者的判例。
- **供应商锁定**，云客户可能会发现自己在CSP之间切换的能力受到限制，原因是（例如）缺乏确保个人数据在CSP服务之间转移的手段。

此外，PLA [v4]包含一些机制，使GDPR第41（1）条提及的机构能够对承诺应用该协议的CSP遵守其规定的情况进行强制性监督，但不影响GDPR第55或56条规定的主管监管机构的任务和权力。

正如下文第三部分第2.1节所述，PLA工作组现在和以往都负责定义、批准和更新PLA [v3]的变更，它代表CoC的基本技术部分，确定相关的欧盟数据保护合规要求并定义条款/控制，以管理CSP对这些要求的合规（见下文第三部分第1.1节）。

PLA工作组由CSP，当地监管机构以及独立的安全和隐私专业人士的代表组成，他们都是云计算界的重要利益相关者，因此能够对CoC中技术部分的结构和内容进行评判。

此外，按照CSA开发的任何研究成果的惯例，CoC在CSA的网站上为期30天公开征求反馈和意见，在此期间，任何感兴趣的个人都可以提供被认为相关的意见或

见解。CoC的公开同行评审过程已向整个CSA社区宣布（CSA的LinkedIn小组、CSA的分会网络、CSA公司成员和相关CSA委员会）。

由于这些原因，PLA [v4]（CoC第2部分），连同本准则的其余部分，包括其治理和遵守机制（CoC第3部分），符合GDPR第40条规定的CoC“草案”。

III. CSA GDPR 合规行为准则的结构

CoC分为三个部分：

- CoC的第一部分描述了其目标、范围、方法和假设，并提供了解释性说明。
- CoC的第二部分包含“控制指南：PLA”及其实质性条款，由PLA工作组制定。
- CoC的第三部分概述了CoC的治理结构和遵守机制。



第一部分

CSA CoC 的目标、
范围、方法、假设和
注释说明

1. CSA CoC 的目标

1. 本准则可被CSP遵守来提供一个或多个服务，也可被遵守此规范的CSP作为云服务协议的附录引用或使用，以描述CSP将提供的隐私保护级别。虽然服务级别协议（SLAs）通常用于提供有关服务性能的度量和其他信息，但CoC将提供信息隐私和个人数据⁹保护的实践。
2. 遵守CoC，CSP必须实施和描述客观上足以满足CoC的每一项控制的技术和组织措施（第2部分）。这使得CSP能够描述其承诺维护的隐私和数据保护级别，涉及开展的个人数据处理相关活动，CSP向云客户提供的与CoC保持一致的服务¹⁰。
3. 在全球范围内采用CoC可以促进一个强大的全球行业标准，加强协调并促进对适用的欧盟数据保护法的遵守。事实上，CoC寻求建立一个基于GDPR的CSP合规标准，该标准可在国际上适用（包括欧盟境外，因为并不局限于欧盟的CSP遵守）。从这个意义上说，CoC的批准可能会使它成为全球CSP遵循的数据保护合规基准—就像它所依据的GDPR一样，通常被认为是数据保护合规的坚实国际基线—使欧盟境内外的云客户和数据主体受益。
4. 此外，CoC的批准将为云计算领域数据保护实践带来有意义的共同监管，市场（以隐私级别协议工作组及其参与者的形式）和欧盟监管机构（在批准过程中）都会提供意见。
5. 最终，CoC提供以下内容：
 - 任何规模的云客户和潜在云客户，都可以使用一个工具来评估不同CSP提供的与他们服务相关的个人数据保护级别（从而支持明智的决策）；¹¹和
 - 任何规模的CSP可以得到指导，来实现对欧盟个人数据保护立法的遵守，

⁹ “个人数据”指的是任何已识别或可识别的自然人（“数据主体”）相关的信息；一个可识别的自然人是一个能够被直接或间接识别的个体，特别是通过诸如姓名、身份编号、地址数据、网上标识或者自然人所特有的一项或多项的身体性、生理性、遗传性、精神性、经济性、文化性或社会性身份而识别个体。” GDPR第4（1）条。

¹⁰ 处理”是指任何一项或多项针对单一个人数据或系列个人数据所进行的操作行为，不论该操作行为是否采取收集、记录、组织、构造、存储、调整、变更、检索、咨询、使用、通过传输而公开、散布或以其他方式对他人公开、排列或组合、限制、删除或销毁而公开等自动化方式。GDPR第4（2）条。

¹¹ “所有在欧洲经济区提供服务的云提供商应向云客户提供所有必要的信息，以正确评估采用此类服务的利弊。客户的安全性、透明度和法律确定性应该是提供云计算服务背后的关键驱动因素。” WP29云计算意见，第2页；“依赖云计算安排的先决条件是控制者[云客户]进行充分的风险评估，包括处理数据的服务器的位置，以及从数据保护角度考虑的风险和收益。”。第4页同上。

并以结构化的方式披露其向云客户提供服务相关的个人数据保护级别。

6. CoC寻求通过以下方式为潜在和当前的云客户以及CSP、数据主体和整个云计算社区创造额外的价值：

- 以有机的、结构化的和系统化的方式确定CSP在处理个人数据时必须遵守的所有GDPR相关条款；
- 解释GDPR条款及其应用在计算环境中的实际相关性，也考虑到WP29/EDPB在这方面提供的澄清，以及欧盟监管机构就该主题提供的指导；
- 通过增加基于CSA、欧盟网络安全局（ENISA）、国际标准化组织（ISO）标准（如ISO 27001、ISO 27017、ISO 27018）制定的指南和其他最佳实践定义的控制措施，如CSP需要识别和提供其信息安全官员的联系方式（第2部分第2.5项控制措施），定义CSP将其意识到的个人数据违规事件通知云客户的时间表（第2部分第8项控制措施），在违反“控制指南：PLA”义务的情况下，为云客户提供有效和业务友好的补救措施（第2部分第14项控制措施），购买数据保护合规保险，涵盖子处理器造成的违规，以及网络保险，也涵盖可能发生的安全和个人数据违规（第2部分第15项控制措施）来提高云计算中数据保护和隐私的门槛；
- 通过制定披露策略，并要求遵守CoC要求的CSP在提交自评估/第三方评估时，提供最低限度的信息和证据，以证明其合规，从而强调透明度的必要性，并实现遵守问责制原则。此外，在要求此类披露时，与CSP相关的云客户获得必要信息，以遵守自身对数据主体的透明度和问责义务；
- 允许公众对遵守CoC的情况进行监督，要求合规的CSP在CSA STAR注册中心内披露其CoC的自评估/第三方评估报告（包括，例如，具体细节说明CSP如何理解其满足CoC的最低要求），通过CoC的投诉管理过程（最终如果发现投诉有效，可能导致暂停或撤销向被投诉CSP提供的合规标识）在实践中，对任何偏离这些提交文件情况进行检查。

通过这种方式，CoC超越了GDPR的要求，并为遵守规范的CSP的数据保护实践提供了更高的标准。

7. “控制指南：PLA”反映了云中相关的GDPR要求。它还重申并加强了GDPR的要求，特别是在涉及行使数据主体权利的情况下一例如，见第2部分第3.5.6项控制措施（关于CSP需要通过合同义务承诺协助云客户响应数据主体请求），第2部分第9项控制措施（关于CSP需要确保数据的可转移，包括以结构化、常

用的、机器可读的、和可互操作的格式的方式直接向数据主体传输个人数据的能力)和第2部分第10项控制措施(关于CSP需要向云客户解释它如何允许对个人数据处理的限制)。此外,通过增加基于CSA、ENISA、ISO标准和其他最佳实践制定的控制措施,提高云计算中数据保护和隐私的门槛—特别是在第2部分第6项控制措施中,CoC通过CSA云控制矩阵为CSP实施技术和组织安全措施提供了坚实的基础。该矩阵专门为指导CSP提供基本安全原则而设计,通过13个域的控制框架,可以详细了解关键的安全概念和原则,与其他行业认可的安全标准、法规和控制框架保持着定制关系。“控制指南:PLA”反映了GDPR的所有要求,并通过为符合规范的CSP的数据保护实践提供更高的标准而超越了GDPR。

8. CoC通过“控制指南:PLA”,不仅寻求提升遵守规范的CSP的合法行为,也寻求促进道德行为。CoC的要求包括CSP的义务,虽然适用的法律没有严格要求,但这些义务对于保证CSP和云客户之间关系的公正平衡是必要的,最终目的是确保数据主体的权利能够得到有效尊重。例如:要求CSP在云客户合同终止时向云客户提供过渡期(由于反对变更个人数据处理位置或子处理者),在此期间CSP将继续向其提供服务,因为云客户在寻找替代解决方案。本要求为了防止因云客户行使异议/终止权而突然被CSP终止提供服务时可能产生对云客户以及相关数据主体的损害(见第2部分第3.2.3项控制措施和第3.3.5项控制措施)。另一个例子是第2部分第14项控制措施,它要求CSP在自身违反“控制指南:PLA”规定的义务时向云客户提供补救措施,从而确保对云客户的赔偿,防止纠纷的发生和升级。
9. 值得一提的是,术语PLA的使用意义在于,遵守CoC的隐私和数据保护方法不是“一刀切”;相反,在合规方面有不同程度的保证(例如针对不同的安全措施,或不同的技术手段来协助处理数据主体的请求),这些保证可能由遵守规范的CSP提供,这些提供商仍然满足CoC的要求。因此,通过与术语“服务级别协议”的类比,“隐私级别”被认为是适当的。

2. 范围和方法

CoC只处理企业对企业(B2B)场景,将云客户视为公司而不是个人(与企业对消费者,或B2C的场景相反)。CoC针对CSP在B2B环境中提供的具体服务—CSP可能提供多种服务,其中一些符合CoC的条款,而另一些则不符合。CSP提供的服务通常属于以下三个类别中的一个或多个:

- 软件即服务(SaaS): SaaS CSP通过互联网提供软件应用。SaaS的例子包

括电子邮件服务、人力资源和客户关系管理应用（HRM/HRIS、CRM）、在线备份服务等。

- 平台即服务（PaaS）：PaaS CSP通过互联网提供开发工具。例如，通过PaaS提供的工具可以用来开发SaaS、电子商务平台等。
- 基础设施即服务（IaaS）：IaaS CSP按需通过互联网提供存储、网络 and 计算服务。

CoC涵盖的与服务相关的处理活动是由CSP执行的，CSP代表云客户作为处理者。这通常反映两种主要情形之一：

- 云客户作为控制者，CSP代表他们作为处理者；
- 云客户作为处理者（代表另一方），CSP代表他们作为子处理者。

无论CSP是作为处理者还是子处理者，它都必须遵守CoC中规定的控制措施，以便让云客户（作为控制者或处理者本身）在设计任何可能包括CSP服务的产品时考虑这些控制措施。

作为本准则的发起者，PLA工作组认识到，可能存在更为复杂/混合的情况（例如，对于单一服务，CSP作为某些活动的控制者），这些情况目前不在CoC的范围内。

CoC考虑了欧盟监管机构和其他有关（欧盟和非欧盟）机构发布的各种相关意见和指南（见下文第6节）。因此，本准则不仅基于适用的欧盟个人数据保护框架的强制性法律条款，还反映了欧盟监管当局的相关解释以及相关机构和其他团体制定的相关最佳实践。CoC旨在成为一个横向工具，用于横跨不同部门和领域实现/评估遵守欧盟个人数据保护立法的情况。PLA工作组了解欧盟成员国在GDPR¹²基础上提供豁免或减损、更具体的规则和附加要求的可能性，以及适用于特定服务的欧盟个人数据保护条款的存在（例如，电子隐私指令、电子隐私法规和NIS指令）。因此，PLA工作组建议CoC的用户识别可能的成员国和/或特定领域的附加要求。CoC的编写还考虑了云计算筛选产业组在CoC¹³上的工作、欧洲云基础设施服务提供商（CISPE）¹⁴和云计算问责项目¹⁵的工作。

CoC反映了与云领域相关的GDPR要求，并且遵循GDPR的“地域范围”，“控

¹² 见GDPR第37（4）条和第九章“与具体处理情况有关的规定”。

¹³ 更多信息请访问：<https://ec.europa.eu/digital-single-market/en/cloud-select-industry-group-code-conduct>。

¹⁴ 更多信息请访问：<https://cispe.cloud/>。

¹⁵ 更多信息请访问：<http://www.a4cloud.eu/>。另请参见：<http://cloudaccountability.eu/>。

制指南：PLA”超出了欧盟范围¹⁶。此外，CoC还对每个定义的控制措施重要性提供了实际解释（第2部分），强调了实施每个控制措施背后的实际意义（通过适当的例子），超出了对强制性要求的遵守（特别是没有法律要求的控制措施）。

CoC的目标受众是CSP（因为只有CSP可以提交其服务以遵守CoC），但CoC也可以作为云计算和欧盟个人数据保护立法领域其他利益相关者的有用工具，如云客户和潜在的云客户，云审计人员和云代理商。CoC是与一个由相关参与方组成的跨职能的工作组合作编写的，并向云计算社区广泛发布寻求意见。这个过程确保了CoC在它的每个控制中都考虑到了云计算领域的细微差别。

此外，CoC还考虑到中小型企业的数据保护领域的需求——特别是需要清楚了解GDPR如何适用于他们，以便他们能够有效地分配资源以实现合规。从这个意义上说，CoC进一步规定了控制措施，以防止GDPR合规（考虑到GDPR的所有内在职责和义务，合规需要大量的时间、金钱和精力投入）成为这些企业的竞争劣势：第2部分第6项控制措施中有一个例子，它依赖于CSA云控制矩阵中制定的详细控制措施，使中小企业能够清楚地了解他们应实施的不同类型和级别的安全措施。所期望的最终结果是CoC为中小企业提供易于理解的指南，使他们能够有效地遵守适用的数据保护要求，并与更大的CSP公平竞争——简而言之，CoC寻求在云计算领域为所有规模的CSP开发出一致的数据保护方法。

目前，CoC并不是为了满足GDPR第46（2）（e）条款的要求——即作为适当的保障措施，在获得批准后可以作为将个人数据从欧盟境内转移到欧盟境外的法律依据（如果接收国不在充分性认定的范围内）。然而CSA目前正在审议用于满足这些要求的CoC附录。

CNIL被确定为CoC的主管监管机构（CompSA）。这是根据以下因素决定的：

- **该倡议由CNIL制定。**CNIL已经制定了与CoC范围相关的若干准则和举措，包括CNIL云建议和CNIL安全指南。此外，最重要的是，CNIL从PLA的第一个版本开始就一直关注CoC的进展，并在CSA发起的非正式协商过程中对CoC提供了广泛的反馈。结果表明，CNIL是CompSA的自然选择，有权决定CoC的批准。也是因为CompSA的另一个潜在候选人——ICO（考虑到在苏格兰CSA附属机构的存在）——可能会因英国退出欧盟而受到损害。
- **处理活动/部门最为密集的地点。**法国是欧洲许多CSP的所在地，其中包

¹⁶ 见GDPR第3条：“2.本条例适用于如下相关活动中的个人数据处理，即使数据控制者或处理者不在欧盟设立：（a）为欧盟境内的数据主体提供商品或服务，无论此项商品或服务是否要求数据主体支付对价；或（b）对发生在欧盟境内的数据主体的活动进行持续监视。”

括约10家CSA企业会员的总部或子公司落户法国。

- **受影响的数据主体的最为密集的地点。**考虑到对可能通过CSP提供的服务处理其个人数据的数据主体类别没有限制，且法国是欧盟人口最多的国家之一，因此法国再次被视为符合这一标准。

鉴于CoC寻求适用于任何位置的，希望遵守其要求的所有类型的CSP，它的范围是跨越国界的，以下所有其他欧盟监管机构都可能被视为相关的监管机构：

- 奥地利数据保护局；
- 比利时数据保护局；
- 保加利亚个人数据保护委员会；
- 克罗地亚个人数据保护局；
- 塞浦路斯个人数据保护专员；
- 捷克个人数据保护办公室；
- 丹麦数据网；
- 爱沙尼亚数据保护监察局；（安第斯监察局）
- 芬兰数据保护监察办公室；
- 德国联邦数据保护和信息自由委员会（以及组成德国的几个州的监管机构¹⁷）；
- 希腊数据保护局；
- 匈牙利国家数据保护和信息自由局；
- 爱尔兰数据保护委员会；
- 意大利数据保护监管机构；
- 拉脱维亚国家数据检查局；

¹⁷ 这些机构的名单可在以下网站上找到：

https://www.datenschutzwiki.de/Aufsichtsbeh%C3%B6rden_und_Landesdatenschutzbeauftragte

- 立陶宛国家数据保护监察局；
- 卢森堡国家数据保护委员会；
- 马耳他信息和数据保护专员办公室；
- 荷兰个人数据管理局；
- 波兰个人数据保护办公室；
- 葡萄牙国家数据保护委员会；
- 罗马尼亚个人数据处理国家监督局；
- 斯洛伐克个人数据保护办公室；
- 斯洛文尼亚信息委员会；
- 西班牙数据保护局；
- 瑞典的数据检查机构。

3. 假设

在签订提供云服务的合同之前，或当此类合同需要根据GDPR要求进行评审时，建议当前和潜在的云客户分别进行内部和外部尽职调查评估。例如：

- 可以利用内部尽职调查来识别可能伴随或阻止使用云服务的限制和约束（例如，对于实体希望在云中处理的数据类型，云是事实上可行的解决方案吗？）。
- 外部尽职调查确定提议的云提供商的产品/服务是否满足潜在云客户的需求和合规义务。它可以帮助评估CSP提供的个人数据保护级别。例如，提议的CSP提供的服务是否提供了公司所需的隐私和数据保护级别以及适用的欧盟法律的合规级别（无论该级别是由公司自己决定，还是因为适用法律要求）？¹⁸

¹⁸ 有关此问题的更多信息，请参阅CSA安全指南。

3.1 云客户的内部尽职调查

作为内部尽职调查的一部分，打算将个人数据移动到云端的实体可能会考虑以下事项：

1. 定义其安全性、数据保护和合规要求。
2. 识别哪些数据/过程/服务需要移动到云端。
3. 评审其内部安全和隐私/数据保护策略以及对其使用个人数据的其他限制，如原有合同、适用的法律法规、指南和最佳实践。
4. 分析和评估风险（例如，在GDPR第35条要求的范围内执行数据保护影响分析¹⁹）。
5. 识别哪些安全控制措施和认证是必要的或有用的，以便充分保护其员工或云客户在云上处理的个人数据。
6. 定义实施安全控制措施的职责和任务（即，了解哪些安全控制措施由组织直接管理，哪些安全控制措施由CSP负责）。
7. 确定实体应监视其服务提供商的哪些活动以及如何监视（例如，是否需要现场访问，或者依赖第三方的认证或证明是否足够？）。

3.2 云客户的外部尽职调查

云客户还可以考虑对提议的CSP的实际工作进行尽职调查评估²⁰。这应包括：

1. 使用“控制指南：PLA”评估CSP提供的服务—包括参与的（分）包商/子处理者，是否满足云客户关于隐私和数据保护的要求。

¹⁹ 有关实用指南，请参阅WP29数据保护影响评估指南。

²⁰ 请注意，根据GDPR的职责原则，始终建议对CSP进行尽职调查，无论他们的服务是否遵守CoCCoC—云客户在任何情况下都对将个人数据委托给CSP承担最终职责。这意味着云客户必须确保具体的CSP适合开展云客户希望委托给他们的处理活动（在安全性、个人数据传输、分包商参与等方面）。为CSP提供评估方案的相关机构也采用了这种方法—例如加拿大网络安全中心的CSP IT安全评估计划（说明见：https://www.cyber.gc.ca/sites/default/files/publications/ITSE.50.060_0.pdf）：“注意，当我们评审CSP的过程和现有控制措施时，您的组织负责确定您的安全要求，并确保您选择的CSP能够满足这些要求。您可以使用我们的评估结果（例如总结报告）来帮助您做出决策”。

2. 根据独立的第三方评估确定CSP是否持有任何相关的认证或证明²¹。
3. 了解是否以及如何知晓和监视CSP实施的安全控制措施和实践。

4. 说明性注释

一个CSP可以为云客户提供多种服务。该规范并不适用于CSP本身（作为一个实体），而适用于它提供的一项或多项服务。因此，CSP有可能在其提供的多项服务中满足本准则的要求，但仍提供本指南未涵盖的其它服务。

此外，此规范可能会留有空间，或指向其它文件，以便进一步澄清将要提供的云服务的特定主题和时间框架，以及CSP处理个人数据的范围、方式和目的，以及将要处理的个人数据的类型。应收集此类信息并与云客户达成一致。²²

尽管CSP基于本指南所承担的义务独立于其对云客户承担的义务（例如，在与这些云客户签署的数据处理协议中），但CSP可以选择将本指南纳入其提供给云客户的合同文件中。在这种情况下，为了避免重复，也可以在主服务协议、服务级别协议（SLA）或云服务合同的其他文件中的适当条款中对其进行引用。例如，服务级别协议通常包含有关数据安全性的信息。文档之间交叉引用的使用旨在简化云客户和CSP的工作（而不是误导云客户）。清晰化和透明度至关重要。

CoC第二部分中的控制措施要求CSP证明它向潜在的云客户提供特定类型的信息，并遵守那些为云客户利益考虑的要求。这不会改变这样一个事实，即基于CoC创建的关系是在CSA（作为CoC的所有者）和CSP（作为CoC成员）之间—CoC不会在CSP和云客户²³之间创建关系。然而，从这个意义上看，CoC第二部分中的控制措施是以类似于B2B领域的第三方受益人合同的方式建立的，根据该合同，CSP向CSA承诺遵守为云客户和最终数据主体（第三方受益人）的利益而设计的义务。

必须强调的是，这一结构旨在确保云领域的数据主体得到更大的保护，符合GDPR和欧盟数据保护法律框架。CSP对实际和潜在云客户的透明性和职责义务的承诺越大，CSP呈现给云客户的合规姿态的意识就越强，而这反过来又会创造必要的条件，使云客户能够对其负责的个人数据提供更高级别的保护（从而确保对这些个人数据相关的数据主体亦提供保护）。

²¹ 见GDPR第40条及以下。

²² WP29云计算意见，第3.4.2节，第13页。

²³ 除非CSP决定将CoC纳入与云客户的合同关系中，如前段所述。

5. 词汇表

有关本准则（CoC）中使用的法律和其他参考资料的定义，请参考下文第6节。

有关本准则中技术部分和管理小组的定义，请参考下文第3部分第1节。

“**遵守标识**”是指符合CoC的标识，因其寻求符合的特定目标而授予CSP。正如第3部分进一步说明的那样，遵守标识有一定的有效期，过期之后必须更新。根据CSP使用的遵守机制，遵守标识可以有两种类型：自评估遵守标识，或第三方评估遵守标识。

“**自动化决策**”是指完全基于自动处理的决策，包括通过画像的方式，对相关数据主体产生法律效力或类似的重大影响。

“**CJEU**”指欧盟法院。

“**云客户**”指由CSP提供服务的B2B客户（即：公司、组织或法人，而非消费者）。

“**CNIL**”指法国国家信息与自由委员会，为法国监管机构。

“**CompSA**”指CoC的主要监管机构，CNIL，拥有GDPR第55条规定的权限。

“**相关监管机构**”是指关注个人数据处理的监管机构，因为（a）控制者或处理者设立在该监管机构的成员国内，（b）居住在该监管机构的成员国的数据主体受到或可能受到处理的重大影响，或（c）该监管机构已收到投诉。

“**同意**”（Consent）是指数据主体自主给予的、具体的、知情的和明确的意思表示，他或她通过声明或明确的肯定行动，表示同意处理与他或她有关的个人数据。

“**控制者**”（Controller）是指决定个人数据处理的的目的和方式的自然人或法人、公共机关、机构或其他机构。如果此类处理的的目的和方式由欧盟或成员国法律决定，则控制者或该名称的具体标准可由欧盟或成员国法律规定。

“**CSA**”指CSA，CoC的所有者。

“**CSP**”指基于云的服务（SaaS、IaaS或PaaS）的提供商，寻求使一项或多项服务满足CSA CoC标准。

“**数据主体**”指已识别或可识别的自然人。而“可识别的自然人”是指可直接

或间接识别的人，特别是通过指向诸如姓名、识别号码、位置数据、在线标识符等标识符而识别或与该自然人的身体、生理、遗传、精神、经济、文化或社会身份有关的一个或多个因素而识别。

“**DPA**”或“数据处理协议”是指控制者和处理者之间签订的协议，以规范处理者代表控制者进行的个人数据处理，参考GDPR第28条的定义。

“**DPIA**”或“数据保护影响评估”是指根据GDPR第35条的规定，旨在描述预定的处理活动，评估其必要性和相称性，并帮助管理因处理个人数据而对自然人的权利和自由造成的风险，评估这些风险并确定处理措施。

“**DPO**”或“数据保护官”是指具有数据保护法律和实践的专业知识的人，受聘协助控制者或处理者监测内部对GDPR的遵守情况，并以独立的方式履行GDPR第37至39条规定的所有任务和职责。

“**EDPB**”是指欧洲数据保护委员会，是独立的欧洲机构，有助于在整个欧盟范围内统一应用数据保护规则，并促进欧盟数据保护机构之间的合作。EDPB由各国数据保护机构和EDPS的代表组成。

“**EDPS**”是指欧洲数据保护监督员，是欧盟的独立数据保护机构，负责监督和确保欧盟机构和团体在处理个人数据时对个人数据和隐私的保护，并处理其他相关任务。

“**EEA**”是指欧洲经济区。

“**ENISA**”是指欧盟网络安全局，该欧盟机构的任务是在整个欧盟实现高度的共同网络安全，包括积极支持成员国、欧盟机构、机关、办事处和机构改善网络安全，并作为欧盟机构、机关、办事处和机构以及其他相关欧盟利益攸关方的网络安全咨询和专业知识的参考。

“**欧盟**”（EU）是指欧洲联盟。

“**Garante**”是指意大利的监督机构。

“**ICO**”是指信息专员办公室，英国的监督机构。

“**ISO**”是指国际标准化组织。它是一个独立的非政府组织，作为国际标准制定机构，由各国家标准组织的代表组成。

“**联合控制者**”是指与其他控制者（一个或多个）共同决定处理个人数据的目的。

的和方式的控制者。

“**监督机构**”是指由CSA设立的内部委员会，其任务是积极有效地监督CSP遵守数据保护做法。

“**个人数据**”是指与数据主体有关的任何信息。

“**个人数据违规**”是指违反安全规定，导致意外或非法破坏、丢失、变更、未经授权披露或访问传输、存储或以其他方式处理的个人数据。²⁴

“**处理**”（以及与个人数据有关的变体，如“在处理”和“被处理”）是指对个人数据进行的任何操作，无论是否通过自动化手段，如收集、记录、组织、结构化、存储、改编或变更、检索、咨询、使用、通过传输、传播或以其他方式提供披露、调整或组合、限制、删除或销毁。

“**处理者**”（Processor）是指代表控制者处理个人数据的自然人或法人、公共当局、机构或其他组织。

“**画像**”是指任何形式的个人数据自动处理，包括使用个人数据评估与自然人有关的某些方面，特别是分析或预测与该自然人的工作表现、经济状况、健康状况、个人喜好、兴趣、可靠性、行为、位置或运动有关的方面。

“**假名化**”是指以这样的方式处理个人数据，即在不使用额外信息的情况下，个人数据不能再归属于特定的数据主体。这种额外信息应单独保存，并采取技术和组织措施，以确保个人数据不归属于一个已识别或可识别的自然人。

“**接收方**”是指接受个人数据的自然人或法人、公共当局、机构或其他机构，无论是否为第三方。然而，根据欧盟或成员国法律，在特定调查框架内可能接收个人数据的公共机构不被视为“接收方”；这些公共机构对这些数据的处理应根据处理目的遵守适用的数据保护规则。

“**限制处理**”是指对已存储的个人数据进行标识，以便在将来限制其处理。

“**特殊类别的个人数据**”是指揭示种族或民族血统、政治观点、宗教或哲学信仰或工会会员资格的个人数据、遗传数据、生物识别数据（当为唯一识别自然人的目的而处理时）、有关健康的数据或有关自然人性生活或性取向的数据。

“**重大变更**”是指对CSP处理与服务有关的个人数据的方式产生重大影响的变

²⁴ GDPR第4（12）条。

更, 该变更影响STAR注册中心上公布的该CSP服务的报告, 进而影响云客户对CSP的数据保护状况进行准确评估。

“子处理者” (Sub-processor) 是指自然人或法人、公共机关、机构或其他机构, 由处理者聘用, 代表控制者协助处理个人数据。

“监管机构” 是指欧盟成员国根据GDPR第51条设立的独立公共机构。

“第三国” 是指欧盟或欧洲经济区以外的国家。

“WP29” 是指“第29条数据保护工作组”, 该工作组是独立的欧洲工作组, 在2018年5月25日 (GDPR的生效) 之前一直处理与保护隐私和个人数据有关的问题, 此后被EDPB取代。



6. 参考文献列表

欧盟立法（和立法文件）

- 2016年4月27日欧洲议会和理事会第（EU）2016/679号条例，关于个人数据处理和自由流动方面的自然人保护，并废除了第95/46/EC号指令（GDPR或通用数据保护条例）²⁵；
- 1995年10月24日欧洲议会和理事会第95/46/EC号指令，关于在个人数据处理和自由流动方面的个人保护（数据保护指令）²⁶；
- 2002年7月12日欧洲议会和理事会第2002/58/EC号指令，关于电子通信领域个人数据处理和隐私保护（电子隐私指令）²⁷；
- 欧洲议会和理事会关于尊重私人生活和保护电子通信中的个人数据并废除第2002/58/EC号指令（电子隐私指令）的提案²⁸；
- 2016年7月6日欧洲议会和理事会第（EU）2016/1148号指令，涉及整个欧盟的网络和信息系统的核心共同安全的措施（NIS指令）²⁹。

欧盟法院（CJEU）

- 案件C-362/14，法院（大法庭）判决书（2015年10月6日）（Schrems I案）³⁰；
- 案件C-210/16，法院（大法庭）判决书（2018年6月5日）（Facebook洞察案）³¹；
- 案件C-40/17，法院（大法庭）判决书（2019年7月29日）（Fashion ID案）³²；

²⁵ 访问：<https://eur-lex.europa.eu/eli/reg/2016/679/oj>。

²⁶ 废除前的最新合并版本，可从以下网址获取：<https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=CELEX:01995L0046-20031120>。

²⁷ 最新版本，由欧洲议会和理事会2009年11月25日的2009/136/EC指令修订，修订指令2002/22/EC与电子通信网络和服务相关的普遍服务和用户权利，指令2002/58/EC关于处理个人数据和电子通信领域的隐私保护以及关于负责执行消费者保护法的国家当局之间合作的第2006/2004号条例（EC），可在以下网址获取：<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02002L0058-20091219>。

²⁸ 访问：<https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2017:0010:FIN>。

²⁹ 访问：<https://eur-lex.europa.eu/eli/dir/2016/1148/oj>。

³⁰ 访问：<http://curia.europa.eu/juris/liste.jsf?num=C-362/14>。

³¹ 访问：<http://curia.europa.eu/juris/liste.jsf?num=C-210/16>。

³² 访问：<http://curia.europa.eu/juris/liste.jsf?num=C-40/17>。

- 案件C-311/18，法院（大法庭）判决书（2020年7月16日）（Schrems II案）³³。

云问责项目

- D38.2证据框架（终版）（CAP证据框架）³⁴。

CNIL

- 2014-298号决定（2014年8月7日）（CNIL橙色决定）³⁵；
- 对计划使用云计算服务的公司的建议（CNIL云建议）³⁶；
- 个人数据的安全（2018年版）（CNIL安全指南）³⁷；
- 第2020-050号审议意见：通过负责监督行为准则遵守情况的机构协议的参考框架（2020年4月30日）（CNIL认证要求）³⁸。

CSA

- 云计算关键领域的安全指南v4.0（CSA安全指南）³⁹；
- 云控制矩阵v.3.0.1（CSA云控制矩阵）⁴⁰。

EDPB

- 关于2016/679号法规第49条的减损的准则2/2018（2018年5月25日）（EDPB转移减损准则）⁴¹；
- 关于2016/679条例下的行为守则和监督机构的准则1/2019（2019年2月12日）

³³ 访问：<http://curia.europa.eu/juris/liste.jsf?num=C-311/18>。

³⁴ 访问：<http://cloudaccountability.eu/sites/default/files/D38.2%20Framework%20of%20evidence%20%28final%29.pdf>

³⁵ 访问：<https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000029406662&fastReqId=1788142702&fastPos=1>

³⁶ https://www.cnil.fr/sites/default/files/typo/document/Recommendations_for_companies_planning_to_use_Cloud_computing_services.pdf

³⁷ https://www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle_gb_web.pdf

³⁸ https://www.cnil.fr/sites/default/files/atoms/files/referentiel-agrement_code-de-conduite_0.pdf

³⁹ <https://cloudsecurityalliance.org/research/guidance/>

⁴⁰ <https://cloudsecurityalliance.org/research/working-groups/cloud-controls-matrix/>

⁴¹ https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf

（EDPB CoC准则）⁴²；

- 关于欧盟法院对C-311/18号案件—数据保护专员诉Facebook爱尔兰有限公司和Maximilian Schrems的判决的常见问题（2020年7月23日）（EDPB Schrems II FAQ）⁴³。

EDPS

- 欧盟机构和机关的个人数据违规通知指南（2018年11月21日）（EDPS数据违规指南）⁴⁴；
- 数据保护词汇（EDPS词汇）⁴⁵。

ENISA

- 关于个人数据违规严重性评估方法的建议（2013年12月20日）（ENISA违规严重性评估建议）⁴⁶；
- 数字服务供应商最低安全措施实施技术指南（2017年2月16日）（ENISA技术指南）⁴⁷。

欧盟委员会

- 云服务级别协议标准化指南（2014年6月26日）（EC云SLAS指南）⁴⁸；
- 2016年7月12日，根据欧洲议会和理事会关于欧盟-美国隐私盾保护充分性的95/46/EC指令，欧盟委员会实施决定（EU）2016/1250，（隐私盾充分性决定）⁴⁹。

Garante

- 云计算—保护云端数据安全（2012）（Garante云计算指南）⁵⁰。

ICO

⁴² https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201901_v2.0_codesofconduct_en.pdf

⁴³ https://edpb.europa.eu/sites/edpb/files/files/file1/20200724_edpb_faqoncjeuc31118_en.pdf

⁴⁴ https://edps.europa.eu/sites/edp/files/publication/18-12-14_edps_guidelines_data_breach_en.pdf

⁴⁵ https://edps.europa.eu/data-protection/data-protection/glossary_en

⁴⁶ <https://www.enisa.europa.eu/publications/dbn-severity>

⁴⁷ <https://www.enisa.europa.eu/publications/minimum-security-measures-for-digital-service-providers>

⁴⁸ <https://ec.europa.eu/digital-single-market/news/cloud-service-level-agreement-standardisationguidelines>

⁴⁹ https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.207.01.0001.01.ENG

⁵⁰ <https://www.garanteprivacy.it/web/guest/home/docweb/docwebdisplay/docweb/1895296&DOWNLOAD=true>

- 关于使用云计算的指南（2012年10月2日）（ICO云计算指南）⁵¹。

电信数据保护国际工作组

- 关于云计算-隐私和数据保护问题的工作文件（2012年4月24日）（索波特备忘录）⁵²。

国际标准化组织（ISO）

- ISO/IEC 17021, 遵守评估—对提供管理体系审计和认证的机构的要求（ISO 17021）⁵³;
- ISO/IEC 17065: 2012, 遵守评估—对产品、过程和服务认证机构的要求（ISO 17065）⁵⁴;
- ISO/IEC 27001: 2013, 信息技术—安全技术—信息安全管理体系—要求（ISO 27001）⁵⁵;
- ISO/IEC 27017: 2015, 信息技术—安全技术—基于ISO/IEC 27002的云服务信息安全控制措施实施准则（ISO 27017）⁵⁶;
- ISO/IEC 27018: 2014, 信息技术—安全技术—作为PII处理者的公共云中个人身份信息（PII）的保护规范（ISO 27018）⁵⁷。

国家网络安全中心（英国）

- 云安全指南—实施云安全原则（NCSC指南）⁵⁸。

WP29

- 关于“控制者”和“处理者”概念的第1/2010号意见（2010年2月16日）（WP29控制者/处理者意见）⁵⁹;

⁵¹ https://ico.org.uk/media/fororganisations/documents/1540/cloud_computing_guidance_for_organisations.pdf

⁵² <http://germanitlaw.com/wp-content/uploads/2012/04/Sopot-Memorandum1.pdf>

⁵³ 第一部分：<https://www.iso.org/standard/61651.html>。其余部分（2到12）：<https://www.iso.org/standards-catalogue/browse-by-ics.html>

⁵⁴ <https://www.iso.org/standard/46568.html>

⁵⁵ <https://www.iso.org/standard/54534.html>

⁵⁶ <https://www.iso.org/standard/43757.html>

⁵⁷ <https://www.iso.org/standard/61498.html>

⁵⁸

<https://www.ncsc.gov.uk/collection/cloud-security?curPage=/collection/cloudsecurity/implementing-the-cloud-security-principles>

⁵⁹ https://ec.europa.eu/justice/article-29/documentation/opinionrecommendation/files/2010/wp169_en.pdf

- 关于在线行为广告的第2/2010号意见（2010年6月22日）（WP29在线行为广告意见）⁶⁰；
- 关于云计算的第05/2012号意见（2012年7月1日）（WP29云计算意见）⁶¹；
- 关于为情报和国家安全目而监视电子通信的第04/2014号意见（2014年4月10日）（WP29电子通信监视意见）⁶²；
- 关于数据转移权利的指南（2017年4月5日）（WP29转移指南）⁶³；
- 数据保护官（DPO）指南（2017年4月5日）（WP29 DPO指南）⁶⁴；
- 确定控制者或处理者的主要监管机构的指南（2017年4月5日）（WP29主要监管机构指南）⁶⁵；
- 为2016/679号条例的目的应用和设定行政罚款的指南（2017年10月3日）（WP29行政罚款指南）⁶⁶；
- 关于数据保护影响评估（DPIA）和为2016/679号条例的目的确定数据处理是否“可能导致高风险”的指南（2017年10月4日）（WP29 DPIA指南）⁶⁷；
- 2016/679条例下的个人数据违规通知指南（2018年2月6日）（WP29数据违规指南）⁶⁸；
- 2016/679条例下的个人自动化决策和画像指南（2018年2月6日）（WP29自动化决策指南）⁶⁹；
- 关于2016/679号条例下的透明度指南（2018年4月11日）（WP29透明度指南）⁷⁰；
- 关于根据GDPR第30(5)条保持处理活动记录的义务而减损的立场文件(2018

⁶⁰ https://ec.europa.eu/justice/article-29/documentation/opinionrecommendation/files/2010/wp171_en.pdf

⁶¹ https://ec.europa.eu/justice/article-29/documentation/opinionrecommendation/files/2012/wp196_en.pdf

⁶² https://ec.europa.eu/justice/article-29/documentation/opinionrecommendation/files/2014/wp215_en.pdf

⁶³ https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233

⁶⁴ https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048

⁶⁵ https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611235

⁶⁶ https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237

⁶⁷ https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

⁶⁸ https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052

⁶⁹ https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053

⁷⁰ https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612227

年4月19日）（WP29记录立场文件）⁷¹。



⁷¹ https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=624045



第二部分

CSA 行为准则控制
指南：隐私级别协议

本准则第2部分（控制指南：PLA）应与附件1：PLA [v4]模板配合使用。

“控制指南：PLA”可分解为称为“控制措施”的不同要求。本指南共有15项控制措施，并分解为子控制措施。可通过控制措施的编号（1到15）以及相关子控制措施的编号（如适用）引用这些控制措施，例如：

- 第1.1项控制措施（可在第30-31页找到）；
- 第6.3.iii项控制措施（可在第69页找到）；
- 第15项控制措施（可在第84-85页找到）。

第2部分的一些控制措施是“透明度控制措施”，要求CSP向云客户描述、指出或解释其处理活动的特定方面。这些控制措施必须在与CSP正式约定之前满足（而不仅仅是在签署服务协议之后提供），以便潜在云客户能够基于CSP提供的必要信息进行适当评估。一般而言，可通过如下方式实现：

- 通过公开的文档（如公开的隐私策略、数据处理协议或服务协议范本、常见问题解答等）；或
- 通过在谈判/合同谈判阶段向潜在云客户提供的文件（可以签署保密协议为前提）。

1. CSP 的合规和职责声明

CSP向云客户声明并确保：

1. 遵守适用的欧盟数据保护法，并具体说明直接适用于CSP并需要遵守的任何特定部门或地方立法/要求、本准则的条款、技术和组织安全措施，并保障数据主体的权利。如果适用的欧盟数据保护法发生重大变更，可能意味着产生与本准则条款相关的新义务或有冲突的义务，CSP承诺遵守适用的欧盟数据保护法条款。

相关信息：通过提供这一声明，CSP以额外承诺遵守本准则的条款的方式扩展了既有法律义务的内容，如遵守欧盟数据保护法，包括适用的特定部门法规。如果

欧盟数据保护法的变更意味着与本准则发生冲突，**CSP**承诺遵守欧盟数据保护法（尽管本准则将按照后续第3部分描述的过程及时修订以符合新的法律标准）。本准则独立存在，并与遵守本准则的**CSP**可能与其云客户签订的任何数据处理协议并行不悖。遵守本准则使**CSP**有义务遵守其条款，否则本准则下的遵守标识将会被移除或暂停。

该控制措施要求**CSP**向云客户声明其遵守以下两项要求：

- 适用的欧盟数据保护法，包括适用的特定部门法规；和
- 本准则的条款

作为遵守本准则条款的声明（而不是遵守适用的欧盟数据保护法的声明）的替代方案，**CSP**可以向云客户承诺，在遵守本准则被认可后做出此类声明。

某些司法管辖区可能会对适用于（或仅适用于）云服务商的个人数据（或特定类型的个人数据）的合法处理提出额外要求⁷²。本准则要求**CSP**向云客户透明地描述**CSP**的服务满足此类特定部门或地方要求，以便云客户可以评估相关条款，从而可以合法采购该**CSP**的服务。

2. 能够证明遵守适用的欧盟数据保护法和本准则的条款（问责制），以及第1.1项控制措施指明的具体部门或地方立法/要求⁷³。

相关信息：通过这种方式，**CSP**保证任何时候都能证明其遵守法律义务，以及本准则中的额外义务。基于云客户和数据主体的利益，云客户和数据主体有权要求使用的**CSP**提供合规的切实证据（另见下文控制措施，以及第3.5.9项、4项、7项和第12.2项控制项措施中的细则）。

本控制措施要求**CSP**向云客户声明，他们不仅能够遵守，而且能够证明他们遵守了：

- 适用的欧盟数据保护法；
- 本准则的条款；以及
- **CSP**声明其服务符合的特定部门或地方要求（如上述第1.1项控制措施的规定）。

⁷² 包括地方立法对**CSP**合法处理特定类型的个人数据提出的要求，如法国公共卫生法规定的HDS（Hébergeur de Données de Santé）认证要求。

⁷³ 参见GDPR 28（3）（h）条款中问责制的基本原则。

作为遵守本准则条款的声明（而不是遵守适用的欧盟数据保护法的声明或遵守上述特定部门/地方要求的声明）的替代方案，CSP可以向云客户承诺，在遵守本准则被认可后做出此类声明。

CSP必须制定并向云客户说明：

3. 能够生成可用作证明合规证据的元素⁷⁴、⁷⁵。必须明确指出能够满足以下各层面要求的元素：
 - i. 组织策略层面，证明策略的正确性和适当性。
 - ii. IT控制层面，证明已经部署了适当的控制措施；以及
 - iii. 操作层面，证明系统正按计划运行（或不运行）。

相关信息：本控制措施进一步细化了上述第1.2项控制措施，明确了CSP向云客户提供其合规证据的具体形式。该措施还包括证据必须涉及的主题领域，以便向数据主体提供完整和清晰的信息，即CSP的组织策略、IT控制和实际操作的合规。

更明确地：

- 组织策略层面的证据可以定义为文件和规程，表明CSP已经建立、记录、批准、传达和/或实施了一系列符合相关法律和监管义务以及标准的策略，而且这些策略在有关服务中得到执行和维护。
- IT控制层面的证据可定义为文件，这些文件表明CSP已采用了与技术控制措施相关的策略、规程和/或工具，这些策略、规程和/或工具旨在减少与IT系统使用相关的安全风险，并在有关服务中得到执行和维护。
- 操作层面的证据可定义为“数据、元数据和常规信息集以及对数据和元数据进行的正式操作，这些数据和元数据对云服务的相关义务的履行情况提供了可归属和可核查的记录，并可用于支持向第三方证明被观测系统适当和有效（或不）运作的声明的有效性”⁷⁶。

证据要素可以有不同的形式，如自评估/鉴证、第三方审计⁷⁷（如认证⁷⁸、鉴证⁷⁹和

⁷⁴ 参见《EDPS词汇表》中关于问责制的定义：“问责制要求控制者建立内部机制和控制系统以确保合规，并向包括监督机构在内的外部利益相关者提供证据（如审计报告）以证明合规。”

⁷⁵ WP29云计算意见书第16页第3.4.4.7节引入了（文件）证据的概念，支持所称的遵守数据保护原则，“[...]云供应商应提供文件证据，证明采取了适当和有效的措施落实数据保护原则的成果。”

⁷⁶ 参见CAP证据框架（the CAP Framework of Evidence）第2页。

⁷⁷ 参见WP29云计算意见书第22页第4.2节“由信誉良好的第三方进行的独立验证或认证可以成为云提供商证明

标识)、日志、审计跟踪、系统维护记录,或更一般的系统报告

和负责的所有处理操作的文件证据。与不同层面要求相关的证据要素的例子还包括数据保护认证、标识⁸⁰。

特别是,在组织策略层面,CSP必须向云客户明确说明CSP制定了哪些策略和规程,以确保并证明服务提供商本身及其子处理者(另见下文控制措施3.3)或业务伙伴遵守适用的欧盟数据保护法和本准则的条款。向云客户提供CSP关于保护个人数据的内部策略和规程,是让云客户选择他们认为将以适当方式处理其负责的个人数据的CSP的基本步骤,从而遵守了国际公认的数据保护透明原则。此外,这些策略和规程应向云客户准确描述如何证明CSP及其分包商和参与提供服务的业务伙伴的合规(从而为整个处理链提供证明)。

CSP应考虑实施(并向云客户说明)的策略和规程包括但不限于:

- 个人数据的留存;
- 遵守GDPR/EU数据保护原则(包括处理个人数据的合法依据);
- 通过设计和默认方式保护数据;
- 对个人数据违规的管理(包括评估个人数据违规严重性的规程)。
- 子处理者的参与;
- 对经授权代表CSP处理个人数据的人员进行管理;
- 数据主体请求;
- 可接受的IT工具使用;

其遵守本意见所规定义务的可靠手段。这种认证至少可以表明,数据保护控制措施已经过审计或评审,符合信誉良好的第三方组织的公认标准,符合本意见规定的要求。在云计算环境中,潜在客户应该查看CSP是否能够提供这种第三方审计证书的副本,或者提供审计报告的实际副本,以验证该认证,包括与本意见书中规定的要求有关的认证。”

⁷⁸ 如CSA STAR认证、ISO 27001认证(可以用ISO27018中的控制项增强要求)

⁷⁹ 如CSA STAR鉴证、SOC2鉴证。

⁸⁰ 参见GDPR第42条。此外请注意,根据WP29云计算意见第14页第3.4.2节,CSP可能要求承担一般义务,保证其内部组织和数据处理安排(以及其子处理者的安排,如有的话)符合适用的国家和国际法律要求和标准。另见《数据保护指令》第17(2)条和WP29云计算意见第14页第3.4.3节和第3.4.4.7节。另见,如CNIL云建议第12页:“a)遵守法国保护个人数据的原则。[当服务提供商是数据处理者时,可使用以下示范条款]双方承诺在收集和所有个人数据时遵守适用于这些数据处理的任何现行法规,特别是遵守1978年1月6日修订的第78-17号法律。根据该法律,客户是根据合同进行处理的数据控制者。[当服务提供商是联合数据控制者时,可使用以下示范条款]。双方承诺在收集和所有个人数据时遵守适用于这些数据处理的任何现行法规,特别是1978年1月6日修订的第78-17号法律。根据这项法律,双方是根据合同进行处理的联合数据控制者”。

- 信息安全；
- 个人数据转移；
- 数据保护影响评估（DPIAs）；
- DPO的任命、任务和职责（如相关）；
- 与监管部门合作；
- 隐私风险评估（衡量一项处理活动可能对数据主体的权利、自由和合法利益产生的影响）；

2. CSP 相关联系人及其角色

CSP必须向云客户说明：

1. CSP的身份和详细联系方式（如名字、地址、电子邮件地址、电话号码和机构所在地）

相关信息：本控制项要求CSP正确标识其法律实体，该实体不仅负责提供服务，还负责确保所提供的服务符合并始终符合适用的数据保护法律。CSP还必须向云客户提供可以联系的详细联系方式。

2. CSP本地代表（如欧盟的本地代表）的身份和联系方式（如名字、地址、电子邮件地址、电话号码和机构所在地）⁸¹

相关信息：为了向云客户和数据主体提供有效手段，要求CSP处理服务或服务中附带的个人数据处理有关事项，以及遵守GDPR第27条（适用时）的要求，CSP应指定本地代表代替上述控制措施2.1中确定的实体（非欧盟CSP则应包括欧盟的当地代表）处理这些云客户和数据主体的问题。

CSP必须确定一个位于欧盟的分支机构，负责处理欧盟任何数据保护相关问题

⁸¹ 参见GDPR第27条：“未在欧盟中设立控制者或处理者代表。1. 在第3条第（2）款适用的情况下，控制者或处理者应书面指定一名在欧盟的代表。2. 本条第1款规定的义务不适用于：（a）临时处理，不包括大批量地处理第9条第（1）款所述特殊类别数据或第10条所述的与刑事案件相关的个人资料、不太可能对自然人的权利和自由造成危险、考虑到处理的性质、背景、范围和目的；或（b）公共机关或机构。3. 代表应设立在数据主体所在的成员国之一，数据主体的个人数据因向数据主体提供商品或服务而被处理，或其行为受到监测。4. 该代表应由控制者或处理者授权，除了控制者或处理者之外，或代替控制者或处理者，处理与处理相关的所有问题，特别是应对监管机构和数据主体，以确保遵守本条例。5. 控制者或处理者指定代表不应妨碍对控制者或处理者本身提起的法律诉讼。”

或调查，或以其他方式确定一位CSP的代表以符合GDPR第27条要求（如适用）。

3. 在服务固有的和在本准则范围内的每项相关处理活动中，CSP的数据保护角色（即，处理者或子处理者）⁸²

相关信息：鉴于每一方所扮演的角色不同，其实际影响和法律义务也大不相同。在实践中，双方必须了解并同意他们在提供服务所附带的个人数据处理关系中所扮演的角色。因此，CSP应根据其提供的服务进行自评，并将其所理解的自身适用角色传达给云客户，使这些云客户了解对CSP的期望和要求（注意，在本准则的范围内，CSP将代表B2B云客户充当处理者/子处理者）。

关于通常属于处理者或子处理者角色的不同活动的进一步指导，见WP29控制者/处理者意见及下文：

- **处理者：**如果CSP不确定开展个人数据处理活动的目的，而只是根据云客户的指示（在服务协议、数据处理协议中，在提供服务过程中或其他情况下给出的特别指示）执行活动，则CSP通常将作为该活动的处理者。典型的例子包括：在向云客户提供服务所必须的情况下使用云客户的数据，或者为了满足云客户提出的与数据有关的要求而使用云客户的数据（如限制对特定数据的处理，或删除或纠正特定数据等）。
- **子处理者：**如果相关云客户不作为特定处理活动的控制者，则有资格作为处理者的CSP也可被称为子处理者。在此意义上，如果CSP的云客户不是某项活动的控制者（如作为处理者，代表其一个云客户执行该活动），该CSP将是“处理者的处理者”（或子处理者）。就本准则而言，CSP是处理者还是子处理者并无区别，所有控制措施均适用于两者。例如，IaaS/PaaS CSP向其他CSP提供在其基础设施/平台上的托管服务并处理个人数据，而这又将被用于代表这些其他云服务商的B2B终端客户处理个人数据。

⁸² WP29云计算意见书的撰写考虑了客户是控制者、CSP是处理者的情况，见第4页第1节和第3.4节。CSA认为，需要在个案的基础上仔细评估各自的角色，这一点也得到了ICO云计算指南第7页的确认。这方面内容见Sopot备忘录第8页：“一个普遍认可的数据保护原则是，处理者处理个人数据的程度不得超过控制者的明确指示。对于CC[云计算]，这意味着CSP不能单方面做出决定或安排个人数据（及其处理）或多或少地自动传输到未知的云数据中心。无论CSP是否以降低运营成本、管理峰值负载（溢出）、负载平衡、复制到备份等方式证明这种传输的合理性，都是如此。CSP也不得为自己的目的使用个人数据。”；另见WP29云计算意见书第23页：“提案草案澄清，未能遵守控制者指示的处理者有符合成为控制者的资格，并受特定的联合控制规则约束”；另见CNIL云建议第5-6页：“当客户使用服务提供商时，人们普遍认为前者是数据控制者，后者是数据处理者。然而，CNIL发现，在某些公共PaaS和SaaS的情况下，客户虽然负责选择他们的服务提供商，但不能真正给他们指示，也不能监督服务提供商所提供的安全和保密保障的有效性。这种缺乏指示和监测设施的情况，主要源于客户不能修改标准报价、以及没有谈判可能性的标准合同。在这种情况下，根据第95/46/EC号指令第2条对“数据控制者”的定义，服务提供商原则上可被视为联合控制者，对个人数据处理的目的和方式的定义做出了贡献。在有联合控制者的情况下，应明确界定每一方的职责”。根据意大利数据保护局的指示，CSP是一个处理者，正如Garante云计算指南第14-15页指出的。另见ICO《云计算指南》第7-9页，不同云服务部署模式中的隐私角色。

4. CSP的DPO的详细联系信息⁸³，或者，如果没有DPO，则隐私事务负责人的详细联系信息，以便云客户可解决问题。

相关信息：要求CSP提供有关其任命的DPO的信息，或者在没有任命DPO的情况下，提供每个CSP“隐私联系人”的信息，以确保云客户能够快速有效地联系到CSP的正确联系人，从而解决可能出现的隐私和数据保护问题。

CSP必须在面向公众的文件（如公开的隐私策略、拟议的数据处理协议或服务协议、FAQ等）中提供这些信息。

5. 信息安全官（ISO）联系方式或，如果没有信息安全官，处理客户安全相关事宜的负责人的联系方式，以便云客户可解决问题。

相关信息：鉴于CSP可能会将与隐私和信息安全相关的内部角色分开（如由不同的人担任DPO/隐私联系人和ISO/安全联系人），并且云客户提出的更多技术性安全问题可能由CSP的ISO（或同等职能的“安全联系人”）处理更好，因此本准则要求CSP公开该名人员的详细联系方式，以确保正确、迅速地解决云客户提出的与技术 and 组织安全措施有关的任何问题。

CSP必须在面向公众的文件（如公开的隐私策略、拟议的数据处理协议或服务协议、FAQ等）中提供这些信息。

3. 数据处理方式

3.1 指令

CSP应给云客户提供如下细节：

1. 云客户可以向CSP发出具有约束力指令的范围和方式⁸⁴。

⁸³ 参见GDPR第13（1）（b）条和第37条。此外，参见WP29的DPO指南（WP29 DPO Guidelines）。

⁸⁴ 请参阅GDPR第28、29条。另请参阅WP29《云计算意见》的第3.4.2节，见第12页：“协议应明确规定CSP不能将控制者的数据用于实现CSP自己的目的”以及索波特备忘录（Sopot Memorandum）的第4页。另外，请参阅ICO《云计算指南》第12页：“DPA要求数据控制员与数据处理员签订书面合同（附表1第二部分第12（a）（ii）段），要求“数据处理者仅根据数据控制者的指令行事”和“数据处理者要遵守的安全义务与强加给数据控制者的安全义务一致”。书面合同的存在意味着在云客户不知情或不同意的情况下，CSP将无法在合同有效期内变更数据处理操作的条款。如果CSP在没有机会进行协商的情况下提出‘接受或离开’的条款和条件，那么云客户就应该引起注意了。此类合同可能不允许云客户保留对数据的充分控制，而该控制权可以使云客户履行其数据保护义务。因此，云客户必须检查CSP提供的服务条款，以确保他们充分解决本指南中讨论的风险。”以及第17页提到的：“云客户应确保CSP仅在指定目的下处理个人数据。出于任何其他目的进行处理都可能违反数据保护的首要原则。如果CSP决定将数据用于其自身目的，则可能就属于这种情况，合同安排应防范这种情况的发生。”

相关性：该控制措施解决了云客户如何向CSP（CSP）发出指令的重要问题。鉴于在云计算领域服务条款和相关合同文件通常由CSP单方面定义，因此在提供给云客户的信息中明确说明这一点十分重要，以便云客户能够预先确认CSP提供的条款是否与GDPR第28条要求一致。此要求超出了GDPR的严格程度，因其要求CSP详细说明云客户将如何并在多大程度上指导CSP使用其所提供的个人数据，同时也与上文控制项1.1所提到的声明与承诺相关，鉴于CSP在法律上有义务遵守云客户对个人数据处理的指示，该控制措施要求CSP明确告知云客户如何行使此权利，以深入探讨如何履行此项义务的细节。

如果云客户受限于CSP合同安排中规定的指示，即除了服务协议、数据处理协议、隐私策略或其他文件中规定的指令外，云客户不能发布进一步的指令，这点也应向云客户明确指出。

3.2 服务变更

CSP应向云客户声明：

1. 如何以书面形式通知云客户与云服务相关的变更，如功能的实现或删除⁸⁵

相关性：该控制措施可以说超出了GDPR的要求，它源于WP29《云计算意见》⁸⁶中的建议。WP29强调，为了保障法律确定性，CSP必须在与云客户签订的合同中应提供一定保障，其中包括有义务告知云客户向其提供的云服务即将实施相关变更的地方，例如为这些服务添加功能。该控制项超出了WP29的建议，明确指出删除功能仍需要向云客户告知相关变更。

不断变更的特性可能会对云客户的数据治理产生相关影响。GDPR并未对这一问题进行明确处理，而WP29《云计算意见》早于GDPR提出该建议，因此CoC试图将这一最佳实践重新纳入当前的法律框架中。

与云客户进行此类交流的方式（应在CSP和云客户之间签订的服务协议中规定）包括电子邮件、在服务内提供给云客户的仪表板上发布消息/通知、更新服务变更日志等。

⁸⁵ WP29《云计算意见》，第3.4.2节，第13页。也可以参阅ICO《云计算指南》列表中的‘法律’部分，见第22页：“云提供商将如何传达可能影响您协议的云服务变更？”请注意，CSP可能需要客户批准变更，否则可能导致CSP充当控制者（请参阅WP29控制者/处理者意见）。

⁸⁶ WP29《云计算意见》，第12至13页。

3.3 个人数据位置

CSP应向云客户声明：

1. 可能处理个人数据的所有数据中心或其他个人数据处理地点（按照国家）的位置⁸⁷，特别是数据可能被存储、镜像、备份和恢复的位置和方式（这可能包括数字和非数字方式）。

CSP还应声明：

2. 一旦签订合同，需要将这些位置的任何预计变更通知云客户，以便云客户确认或反对。
3. 如果CSP和云客户之间的异议无法圆满解决，允许云客户终止合同，并为云客户提供足够时间购买替代的CSP（服务）或解决方案（通过建立一个过渡期，在该过渡期内，依据合同继续为云客户提供约定级别的服务）。

相关性：鉴于法律和物质环境的差异可能对各国间个人数据安全造成影响，特别是，如果这些国家在欧盟之外并且未被欧盟委员会做出的充分性决定所覆盖时，无论是在最初还是在服务提供过程中，CSP务必明确告知云客户其个人数据可能被处理的地点。如果没有这些信息，云客户将无法全面、清晰地了解所雇用CSP的影响，这就是为什么CoC要求CSP披露此类信息的原因。

开始执行服务后，若位置发生变更，也应通知给云客户，并允许他们确认或反对这些变更。如果异议无法解决，云客户必须有权终止合同。在这种情况下，云客户和CSP必须商定一个过渡期，在此期间，CSP将继续向云客户提供一定级别的服务，而云客户则需采购CSP所提供服务的适当替代方案，以防止因突然终止向云客户提供服务而可能造成的损害（例如，个人数据突然缺乏可用性）。

在向云客户通知处理地点的预期变更时，CSP必须确保提供以下信息：

- 预期的新处理地点—必须确定具体的国家；
- 处理地点变更的原因；

⁸⁷ WP29《云计算意见》，第3.4.1.1节（见第11页）和第3.4.2节（见第13页）。另可参阅索波特备忘录中的“地点透明”原则，见第14页。也可参阅ICO《云计算指南》列表的“法律”部分，见第22页：“您的云提供商将在哪些国家处理您的数据，以及与这些地点提供哪些与安全措施相关的信息？您能否确保相关主题数据的权利和自由得到保护？您应该向云提供商询问您的数据可能被传输到其他国家/地区的情况。您的云提供商能否限制将您的数据传输到您认为合适的国家？”

- 是否涉及子处理者的变更（如果涉及，则必须考虑下文控制项3.3的要求）
- 预计完成变更的时间
- 参考服务协议、数据处理协议或其他对此作出规定的协议，云客户提出异议的可能性，同时解释提出异议的条件以及异议可能产生的后果。

CSP仍然可在服务协议、数据处理协议或其他受监管协议范围内自由决定向云客户提供这些通知的方式。但是，必须确保这些方式应能够使云客户及时、有效地了解通知并对提及的位置变更提出反对—换句话说，所选择的方式不能损害该控制措施的目标。

3.4 子处理者

CSP应为云客户识别：

1. 参与个人数据处理的子处理者，以及用于确保满足数据保护要求的问责制和职责链。⁸⁸

CSP向云客户声明，并进一步确保：

2. 未经云客户事先特别或一般的书面授权，CSP不会聘用任何子处理者。⁸⁹

CSP向云客户声明，并进一步确保：

3. 通过合同（或其他有约束力的法律行为）向子处理者施加CSP和云客户之间规定的相同（或至少是基本相同）的数据保护义务。并且将仅聘用提供充分保证的子处理者来采用适当的技术和组织措施使前述处理符合欧盟适用法律的要求。
4. 根据要求，将向云客户披露CSP与其子处理者（全部或部分）之间签订的合同（或其他有约束力的法律行为），以证明第3.4.3项控制措施的要求已得到满足。
5. 如果子处理者未能履行其数据保护义务，则CSP仍然对云客户承担子处理者所需承担的全部职责。

CSP应具备并向云客户说明：

6. 设计规程用于向云客户通知有关添加或更换子处理者的任何预期变更，同时要

⁸⁸ 参阅ICO《云计算指南》中“分层服务”的概念，见6-8页。

⁸⁹ 参见GDPR第28条第二款。

始终为云客户保留反对此类变更或终止合同的可能性⁹⁰。如果云客户终止合同，云客户必须有足够的时间购买代替的CSP或解决方案（通过建立一个过渡期，在此期间，CSP继续根据合同向云客户提供约定的服务级别）。

相关性：通过这些控制措施，CoC要求CSP承担不可避免的义务，即向云客户披露CSP为提供服务而可能参与的处理链上的明确信息，同时以云客户的授权（特别授权或一般授权）为前提。尽管GDPR负有这样做的法律义务，但考虑到在云计算领域不披露此类信息的一般做法，这点被认为至关重要。CoC力求确保这些信息以清晰且真正便于访问的方式传递给云客户。

希望聘用子处理者的CSP应从云客户处获得这方面的特别授权（其中特定的子处理者要由云客户批准，未来的业务也须经云客户批准），或获得一般授权（其中云客户通常接受使用子处理者，但在任何未来业务开展之前应事先通知云客户，以便他们可以在愿意的情况下提出反对意见）。

基于CSP与其子处理者之间和CSP与其云客户之间执行完全相同的数据保护义务可能存在实际困难，在云领域中的一般做法是：**CSP至少承诺，对这些子处理者施加基本等效的数据保护义务（当然，由于前述义务与CSP的子处理者所受的义务之间存在差异而导致的CSP对云客户义务的任何违反，CSP仍应承担全部职责）。**这种方法得到了CoC的支持，因为CoC强调CSP只需聘用CSP认为能够充分保证实施适当技术和组织措施子处理者，以使其对个人数据的处理符合适用的欧盟数据保护法。

此外，CoC规定CSP承担与“连带职责”相关的义务（即就其子处理者的性能向云客户承担全部职责），并将任何打算增加或更换的子处理者告知给云客户以允许云客户提出反对意见（根据一般授权）或最终拒绝授权这一变更，这种僵局情况下（云客户和CSP无法就如何解决反对意见达成一致），必须允许云客户（而非CSP）终止协议，为云客户提供足够的时间来适应所需的变更。

当向云客户通知关于增加或更换子处理者的预期变更时，CSP必须确保其提供以下信息：

- 拟用的新子处理者的法定名称；
- 将代表CSP处理个人数据的新子处理者所在的具体国家；

⁹⁰ WP29《云计算意见》，第3.3.2节，第10页：“云提供商还应有指定所有受委托的分包商的明确义务（例如，在公共数字登记册中）。”第3.4.2节第13页，以及第3.4.1.1节第10-11页。另外还可以参阅ICO《云计算指南》的第11页，以及《数据保护指令》第10条。

- 每个新的子处理者在处理云客户个人数据过程中将扮演的角色；
- 云客户提出反对意见的可能性，参照服务协议、数据处理协议或其他协议中的规定，同时解释可以提出反对意见的条款以及反对可能产生的后果。

虽然此控制措施旨在确保云客户能够获得足够的信息，以充分了解CSP在提供服务时可能依赖的子处理者链，但如果CSP没有或不会聘用此类子处理者，则此控制措施将不适用。在这种情况下，CSP仍然应该向云客户明确说明CSP现在且将来都不会聘用此类子处理者。

3.5 在云客户系统上安装软件

CSP应向云客户表明：

1. 服务提供是否需要在云客户系统上安装软件（如，浏览器插件）。
2. 从数据保护和数据安全的角度看软件的含义⁹¹。

相关性：本控制措施的支持理由与上述第3.1.15项控制措施类似，因为要求在云客户系统上安装软件以提供服务可能会对云客户的数据治理产生影响（例如，这可能意味着额外的数据收集或转移），这也源于WP29《云计算意见》⁹²。需要注意的是，尽管WP29声明云客户应事先提出此问题（如果CSP未充分解决），但CoC要求所有的CSP从数据保护和数据安全的角度披露任何将要安装的软件的影响（如，CSP是否会通过此软件收集、传输或保留任何其他数据，以及该软件将采取何种安全措施，并尽可能详细地让云客户从合规的角度了解该软件安装的相关程度）。

所提供的信息应涵盖因需要安装该软件而可能发生的任何其他个人数据处理活动（例如，如果需要第三方软件，则应提供指向该第三方的隐私策略或与隐私相关的公共文件的链接），以及有关该附加软件须遵守的安全措施的有意义的信息。云客户应能够从这两个角度了解安装此类附加软件可能会对其自身及其数据主体可能产生的后果。

如果软件安全是可选的（对于提供服务不是必需的，因为有不需安装软件的功能替代方案，例如基于浏览器的解决方案），则上述信息不一定需要在CSP参与之前向云客户提供（尽管这仍然是推荐给CSP的最佳做法）。但是，CSP仍应该确保希望安装此类软件的云客户能够在安装之前访问所有这些信息。

⁹¹ WP29《云计算意见》，第3.4.1.1节，第11页。

⁹² WP29《云计算意见》，第11页

3.6 数据处理协议（或其他具有约束力的法律行为）

CSP应与云客户共享并执行：

1. 拟定的数据处理协议（或其他具有约束力的法律行为）管理代表云客户的CSP所进行的处理，同时也规定处理的主题和持续的时间、个人数据的类型和数据主体的类别，以及云客户的义务和权利。

数据处理协议或其他法律行为应特别规定CSP将执行以下操作：

2. 仅根据云客户的书面指示处理个人数据，包括将个人数据传输到第三国或国际组织，除非CSP遵守的欧盟或成员国法律要求这样做；在这种情况下，CSP将在处理前告知云客户该法律要求，除非该法律以重要的公共利益为由禁止此类信息；
3. 确保被授权处理个人数据的人员承诺保密或承担适当的法定保密义务，并且除非欧盟或成员国法律另有规定，否则未经云客户指示，他们不会处理个人数据⁹³；
4. 保证所有被授权处理个人数据的人员都接受过适当的培训，至少每年一次，内容涉及隐私、数据保护和数据安全问题，尤其是与提供数据处理所固有的特定风险相关的培训服务；
5. 根据现有技术、技术级别、实施这些措施的成本以及所提供服务的固有处理活动，实施CSP认为足够的所有技术和组织安全措施，以确保CSP的服务具有适当的安全级别的保护，并考虑到数据主体的利益、权利和自由的潜在风险时，确保CSP的服务具有适当的安全级别的保护⁹⁴；
6. 尊重本准则中规定的聘用的子处理者⁹⁵的条件（参阅上文第3.3项控制措施）；
7. 考虑到处理的性质，采取适当的技术和组织措施协助云客户，尽可能满足云客户行使数据主体权利的请求⁹⁶；
8. 协助云客户确保其遵守与处理安全有关的义务⁹⁷；向监管机构通报个人数据违规事件⁹⁸；向数据主体⁹⁹和DPIA¹⁰⁰通报个人数据违规事件；考虑处理性质和CSP

⁹³ 参见GDPR第32（4）条。

⁹⁴ 参见GDPR第32条。

⁹⁵ 参见GDPR第28（2）条和第28（4）条。

⁹⁶ 参见GDPR第三章。

⁹⁷ 参见GDPR第32条。

⁹⁸ 参见GDPR第33条。

可用的信息；

9. 根据云客户的选择，在与处理相关的服务结束后，删除或返还所有个人数据给云客户；并且删除现有副本除非欧盟或成员国法律要求存储个人数据；（参阅下文第11项控制措施）；
10. 向云客户提供所有必要的信息，以证明遵守相关的数据保护义务；允许并协助云客户或由云客户授权的其他审计师进行的审计，包括检查。

相关性：此控制措施是一项正式要求，作为首要目标，要求复制GDPR第28条中包含的正式义务，以确保CSP与云客户签订的所有合同都符合最低法律要求。然而，CoC超越了这一点，不仅重申了这些要求，还进一步明确了这些要求，例如，在承诺聘用的子处理者所需遵守的条件中就可以看出（其中，依据上文第3.3项控制措施，CoC规定，CSP有义务提供关于其整个处理链的清晰、透明的信息-包括最初的信息和任何后续的预期变更-并且子处理者变更的异议无法解决时，允许云客户终止协议），以及在服务结束后删除或返还所有个人数据给云客户的要求（根据下文的第11.4项控制措施，CSP也有义务提供关于删除或返还数据的方法的信息）。

CSP需要向云客户提出他们的个人数据处理协议。这种数据处理协议实际上是一个可以由一方（CSP）提出并可能被另一方（云客户）接受的协议。该协议的接受和/或修改将由双方协商决定；考虑到CoC仅适用于B2B场景，这应允许CSP和云客户就此达成双方都满意（或至少是可接受）的协议。通过提出自己的数据处理协议，CSP还将其认为在商业上可以接受的条款预先告知云客户—如果云客户也认为这些条款可以接受，他们可能更愿意与CSP签订协议。

CSP无法确定处理的目的，因此无法向云客户提出完整的数据处理协议（是因为它可能并不总是了解云客户使用的CSP服务的个人数据/数据对象的类别），但它可能仍然提供核心条款来规范与云客户的个人数据处理关系（包括并扩展GDPR第28条第3款的义务），特别是处理期限以及云客户和CSP的义务/权利。必须由云客户（作为控制者或主要处理者）确定更多的具体条款，如个人数据的类型和相关的数据主体，可以专门插入每个云客户的拟议数据处理协议的附件中，由云客户自己填写。在任何情况下，这都是目前几个CSP采用的典型方法。

即使CSP不需要子处理者参与提供服务，也应对子处理者的参与进行规范（例如，包括承诺CSP将不聘用此类子处理者）。

⁹⁹ 参见GDPR第34条。

¹⁰⁰ 参见GDPR第35条。

关于CSP提供所有必要信息以证明数据保护合规的合同义务、以及允许和协助审计/检查，云计算领域的标准做法是允许云客户访问由独立且合格的第三方进行的审计报告，而不是提供对CSP用于处理个人数据的系统、设备或设施的直接访问。这种第三方审计必须由CSP定期执行，其频率应符合其性质和目的。这方面的最佳做法，这也是普遍认可的认证和鉴证审计的规则，至少每年进行一次审核，并在审核目标发生重大或相关变更时进行额外的临时审核。

3.7 通过设计和默认的设置保护数据

1. CSP必须具备并向云客户说明纳入服务设计的技术和组织措施（包括相关的数据保护增强技术）的可用证据，其中包括针对授权处理个人数据人员举办的培训课程（该培训课程至少每年一次），以处理并实施以下每项原则：
 - i. **合法性**：必须出于合法目的（或多个目的）处理个人数据，并且必须根据适用的欧盟数据保护法为每个处理目的确定适当的法律依据。在处理特殊类别的个人数据和/或与刑事定罪/犯罪相关的个人数据时，还必须确定适用的欧盟数据保护法禁止处理这些个人数据的例外情况；
 - ii. **公平性**：处理个人数据的方式不得无理或过度侵犯数据主体的隐私，不得以不当的方式对其权利、自由和合法利益产生负面影响，或导致对个人数据的处理与数据主体的合法期望背道而驰；
 - iii. **透明度**：必须向数据主体提供可适用的欧盟数据保护法认为必要的信息，以确保他们完全了解其个人数据的处理情况以及他们对此做出反应的可能性，可适用的欧盟数据保护法的任何相关例外情况除外；
 - iv. **目的限制**：必须出于特定、明确和合法的目的处理个人数据。根据可适用的欧盟数据保护法，任何对个人数据的进一步处理都必须与最初收集/处理个人数据的目的兼容；
 - v. **数据最小化**：处理的任何个人数据必须适当、相关，并且仅限于为实现处理目的且绝对必要的数据。如果可以使用较少的个人数据或没有个人数据就能满足某个目的，那就应该这样做；
 - vi. **准确性**：处理的任何个人数据必须准确、完整并保持更新，同时应采取一切合理措施确保不准确、不完整或过时的个人数据被及时删除、完成或纠正；
 - vii. **存储限制**：任何处理过的个人数据必须以一种允许识别相应数据主体的形

式保存，保存时间严格限制为满足处理个人数据的目的所需的最短时间。这需要确定每类个人数据的保留期，之后这些个人数据必须被删除、匿名化或（至少）限制进一步处理；

- viii. **完整性和保密性（安全）**：必须实施技术和组织安全措施，以确保个人数据在处理过程中的机密性、完整性和可用性，包括使用适当的技术或组织措施防止未经授权或非法处理以及意外损失、破坏或损坏；

相关性：CSA未将设计和默认的数据保护视为独立原则，而将其作为实现GDPR第5条规定的原则的方式。因此，这种控制的目的是确保有技术和组织措施到位，以保证CSP符合所有此类原则。

通过这种控制，CSP需要提供证据证明欧盟数据保护法中反映的每项数据保护原则都已在被评估的服务中得到了遵循，并且说明在实践中是如何实现这一目标的（通过具体的技术和组织措施）。应就服务的固有处理活动来完成这项工作，证明数据保护原则从服务的开始/设计阶段就已被考虑到，并在整个服务的提供和开发过程中继续被视为服务的核心要素（即，不会为了服务的有效性或盈利性而做出不必要的妥协，也不要将其作为合规的事后补救措施）。

尽管GDPR只要求控制者确保遵守所有的数据保护原则，但本CoC将此义务扩展到充当处理者的CSP，以确保这些控制措施能够有效提高CSP的数据保护合规标准。CSP必须能够证明遵循CoC的服务得到了技术和/或组织措施的支持，这些控制措施可以帮助相关控制者遵守上述数据保护原则。不仅应证明该服务不会对完全遵守这些原则构成任何障碍，而且该服务还积极促进遵循这些合规要求，通过提供工具，可以以完全符合数据保护要求的方式管理使用该服务的个人数据。

例如—CSP应能够展示其服务允许云客户控制适用于个人数据的保留期，以便他们能够确保满足存储限制原则。如果CSP开发和设计的云服务被特别用于处理个人数据，则应在开发和设计此类服务时考虑GDPR和其他适用的数据保护法律规定的职责和义务，采取最先进的技术，确保云客户能够在合法原则下履行其数据保护义务¹⁰¹。例如，如果CSP预知其云客户将依赖授权作为通过服务处理个人数据的法律依据，那么CSP可以考虑提供授权的方式，由云客户或代表云客户以有效和合法的方式收集该授权。向云客户提供足够的服务信息和个人数据固有的处理信息，使这些云客户能够正确通知他们的数据主体，这将使CSP符合透明度原则（需要注意的是，本准则的其他部分也涉及这一点）。

2. CSP必须具备并向云客户说明可应要求提供的证据，以证明该服务在默认情况

¹⁰¹ 参见GDPR陈述第78条

下仅对控制者确定的每个处理目的所严格需要的个人数据进行处理（与收集的个人信息量、处理程度、保留期限和个人数据的可访问性有关）。特别是，CSP必须证明，默认情况下，个人数据不会被广大公众或不确定数量的自然人访问，也不会未经数据主体干预的情况下被进一步处理。

相关性：本控制涵盖默认的隐私/数据保护原则，要求CSP表明个人数据在评估服务相关的使用系统和处理活动中得到自动保护，因此个人无需采用任何具体行动来保护其隐私。CSP应在其服务中提供强大的默认隐私设置，并提供方便用户的选项和控制措施以尊重用户设置的偏好（例如，允许用户选择是否通过电子邮件或推送通知接收来自在线CSP平台的通信）。

一般来说，任何在提供服务之外（并非严格要求）的个人数据处理，都应由相关数据主体自行决定。

4. 记录保存

CSP必须向云客户确认并承诺：

1. 保存代表控制者进行的所有类别的处理活动的记录，并应要求提供给监管机构。

该记录必须包含以下信息：

2. CSP及其子处理者、CSP所代表的控制者的姓名和联系方式，以及（如适用）控制者或CSP的代表以及数据保护官的姓名和联系方式；
3. 代表每个控制者进行的处理类别；
4. 在适用的情况下，将个人数据传输到第三国或国际组织，包括该第三国或国际组织的身份以及适当保护措施的文件；
5. 对现有技术和组织安全措施的描述已具备（另见下文第6号控制措施）。¹⁰² ¹⁰³

相关性：无论GDPR第30（5）条规定的例外情况能否适用于CSP（也考虑到WP29在WP29记录立场文件中对此例外的最新立场大大缩小了其适用范围），该控制措施旨在扩大记录保存义务，要求所有CSP保存包含上述信息的详细记录。这是

¹⁰² 参见GDPR第32条。

¹⁰³ 参见GDPR第30（2）条和GDPR第30（5）条，其中规定了以下限制：“第1款和第2款所指的义务不适用于雇佣少于250人的企业或组织，除非其进行的处理可能会对数据主体的权利和自由造成风险，处理不是偶然性的，或者不适用于处理包括第9条第1款所述的特殊类别的数据或第10条所指与刑事定罪和犯罪有关的个人数据。”但是，另请参见WP29在WP29记录立场文件中提供的澄清，限制了这一限制的适用性。

所有CSP都需要的，因为保留完整的记录是确保透明度和加强对CSP合规控制措施的基本工具，也是允许CSP根据问责制原则证明合规的主要手段。

在设计处理活动记录时，CSP应考虑监管机构开发的模板——尤其是CNIL¹⁰⁴。但是，这些模板应被视为最佳实践的示例或说明，而不是要遵循的强制性模型：尽管符合GDPR（以及本准则）固有的问责制原则和基于风险的方法，CSP仍然负责以最合适的方式配置他们的记录，确保遵守其义务——尤其是满足这些CoC控制措施的要求。

只要可行，接收者（见上文第4.1.5项控制措施）应单独识别，而不是按类别识别。

5. 数据传输

CSP必须向云客户明确指出：

1. 无论是在正常运营过程中还是在紧急情况下，是否存在跨境传输、备份和/或恢复数据。

相关性：在实践中，此控制措施的目的是让云客户能够清楚了解提供CSP服务固有的数据流。CoC认为这种控制措施很重要，以便阐明在云计算领域中数据主体通常不清楚的实践。CoC拥护者仍然可以自由地以他们认为最合适的方式遵守此控制措施，前提是提供的最终结果清楚、完整地向云客户表明与服务相关时个人数据将如何跨境流动——例如，使用图片和数据流图，并附带口头解释，可能有助于使这些信息的提供对云客户保持透明。

CSP必须了解，就本准则而言，只要在一个国家/地区处理的个人数据随后在另一个国家/地区进行处理，就会发生个人数据的传输。当CSP主动将个人数据从A国发送到位于B国的接收方时，以及当CSP允许在B国设立的接收方远程访问存储在A国的个人数据时，就会发生这种情况。¹⁰⁵

向云客户提供的有关传输个人数据的信息必须涵盖以下内容：

- 与服务相关的传输类型；

¹⁰⁴ 参见CNIL开发的处理活动的记录模版，CSP可以使用它记录作为处理者的处理活动，记录模版可在以下网址获取：<https://www.cnil.fr/en/record-processing-activities>。

¹⁰⁵ 这最后一种情况在《EDPB转移减损指南》第4页中得到了具体阐述：“例如，当数据输入者被允许直接访问数据库（例如通过IT应用的接口）时，一般情况下，转移将被视为非偶然性或重复性的。”

- 确定每种传输类型的目的（例如，存储目的、备份目的）
- 对于确定的每种传输类型，个人数据将传输到的特定国家/地区。

请注意，目的和特定接收国必须与确定的传输类型关联。**CSP**仅列出所有类型、目的和数据目的地是不够的—云客户必须能够了解将个人数据传输到每个特定接收国家的具体目的。

如果此类传输受到适用欧盟法律的限制，**CSP**必须向云客户明确说明，并采取所有合理必要的步骤实施。

2. 每次传输的合法传输机制（包括通过多层分包商的传输），¹⁰⁶例如，欧盟委员会的充分性决定、合同范本/标准数据保护条款，¹⁰⁷批准的CoC¹⁰⁸或认证机制¹⁰⁹和具有约束力的公司规则（BCR）。¹¹⁰

相关性：对于**CSP**而言，根据**GDPR**第45至49条明确确定从欧盟内部向欧盟外部传输个人数据（以及在欧盟外部继续传输）所依赖的合法传输机制也很重要，以便云客户能够正确评估此类机制是否足够并且是否符合云客户希望实现的参与**CSP**的目的。某些云客户可能希望依赖于使用某些传输机制（例如，合同范本/标准数据保护条款或BCR）与**CSP**合作。底线是**CSP**必须向云客户提供支持所披露传输的法律机制相关的所有信息，以便云客户能够就这些信息是否合适做出明智的决定。

这些机制应来自**GDPR**第44至49条（例如，充分性认定¹¹¹、BCR、标准合同条款¹¹²）。

具体参考标准合同条款，控制者是否可以依赖它们作为**GDPR**下的合法传输机制取决于控制者（数据出口者）以及接收国家的数据进口者进行的评估结果，即接收国是否允许遵守标准合同条款提供的个人数据保护级别（换句话说，与欧盟保证的保护级别基本相同）。该评估必须考虑预期转移的所有相关情况，包括出口者和

¹⁰⁶ 参见《ICO云计算指南》，第18页。

¹⁰⁷ 见第44条及以下。**GDPR**。另见WP29云计算意见，第3.5.3节，第18页。

¹⁰⁸ 根据**GDPR**第40条的规定。

¹⁰⁹ 根据**GDPR**第42条的规定。

¹¹⁰ 见WP20云计算意见，第3.5.4节，第19页。

¹¹¹ 欧盟法院最近在Schrems II案中的决定导致隐私盾充分性决定无效，使确保根据**GDPR**将个人数据从欧洲经济区合法传输到美国的欧盟—美国隐私保护框架成为一种不合适的机制。

¹¹² 与Schrems II案对隐私盾充分性决定的影响相反，该案并未导致标准合同条款作为**GDPR**下的合法转移机制绝对无效。这些措施暂时仍然有效，并且是将个人数据传输到尚未收到欧盟委员会充分性决定的国家的表面上合法的手段。但是，根据Schrems II案和EDPB Schrems II常见问题解答，在选择依赖标准合同条款作为合法传输机制时必须谨慎行事。特别是，数据出口者（位于EEA境内）和进口者（位于欧洲经济区境外的特定接收国）都必须在根据标准合同条款传输任何个人数据之前验证与根据**GDPR**在欧盟范围内所保证的基本相同的保护级别内容在接收国是否提供和得到尊重。

进口者可能采取的任何补充措施，解决与接收国标准合同条款所提供的保护级别相关的已识别风险或缺陷（由于地方立法的原因）。

关于补充措施，CSP应考虑可能的法律（如在协议中接收方应履行的义务，如DPA、联合控制协议或数据管理协议¹¹³，将任何地方当局访问相关个人数据的要求提前通知数据出口者）、组织（例如，采取规程性措施以确保在欧盟/欧洲经济区以外的地方尽可能少地访问、发送或处理个人数据，同时仍允许提供服务）和/或技术措施¹¹⁴（如对传输到接收国的所有个人数据实施端到端加密）。CSP应参考EDPB和EEA监管机构可能不时提供的建议。

标准合同条款和补充措施结合起来需要足以确保接收国适用的法律不会影响条款本身所保证的充分保护级别。如果这是不可能的，则控制者必须（A）根据标准合同条款暂停或结束个人数据传输，或（B）通知其主管监管机构进行此类传输的意图，无论标准合同条款和补充措施是否不足以确保对相关个人数据提供足够的保护。

在涉及根据标准合同条款将个人数据从欧洲经济区（EEA）内部传输到EEA外部的过程中，标准合同条款本身也要求数据进口者（位于EEA外部）通知数据出口者（即控制者）任何无法遵守标准合同条款要求的情况（或双方商定的任何补充措施），随后数据进口者必须暂停相关个人数据的传输和/或终止与数据出口者的关系。

关于标准合同条款，CSP应注意，目前没有经过批准的处理者到处理者标准合同条款。因此，为了解决向非EEA子处理者转移个人数据的问题，CSP需要考虑以下事项：

- 如果CSP位于欧盟/欧洲经济区：控制者必须与任何非欧洲经济区接收者签订标准合同条款，这些接收者可能会收到与服务相关的源自欧洲经济区的个人数据。CSP必须确定如何确保这一点——一般来说，要么让控制者直接与接收者签订标准合同条款，要么接受控制者代表他们这样做的授权；
- 如果CSP位于欧盟/欧洲经济区之外：CSP可以考虑利用与云客户签订的控制者到处理者标准合同条款的第11条（“分包”），以便与非EEA子处理者签订书面协议，无需云客户的直接干预（请注意，在这种情况下，仍必须满足上述第3.3项控制措施的要求）。

¹¹³ “数据管理协议”是涉及个人数据处理关系的两个或多个组织之间为全面规范各自数据保护合规职责而订立的书面协议。这些协议可能包含DPA条款、联合控制条款和/或附加条款，以规范独立控制者之间的关系。

¹¹⁴ 在实施技术措施时，接收者必须确保这样做不会导致他们违反适用的当地法律规定的任何义务。

6. 数据安全措施

初步而言，CSP应注意：“……在欧洲议会和理事会于2016年7月6日通过的关于欧盟网络和信息系统高通用安全措施的第（EU）2016/1148指令背景下，云计算服务被视为数字服务提供商（DSP）。”¹¹⁵在完成基于WP29云计算意见的本节时，CSP必须遵循ENISA技术指南¹¹⁶作为最低可接受基线（下面提供了控制措施）。此外还可以通过遵守相关CoC和认证机制的方式向云客户提供数据安全合规的证据。

117

考虑到最新技术、实施成本和处理的性质、范围、背景和目的，以及自然人权利和自由的风险的不同可能性和严重程度，CSP必须：¹¹⁸

1. 向云客户指定技术、物理和组织措施（包括至少每年为被授权处理个人数据的人员安排一次关于数据安全的特定培训课程），这是为了保护个人数据免遭意外或非法破坏；或意外丢失、变更、未经授权的使用、未经授权的修改、披露或访问；和抵制所有其他非法形式的处理。¹¹⁹

相关性：数据安全合规的证据也可以通过遵守相关CoC和认证机制的方式提供给云客户。¹²⁰此外，CSP还可以指出与CSP可能拥有的其他安全认证（如ISO27001、SOC2等）相关的控制措施。但是，这并不意味着CSP无需确定特定安全措施以应对CSA云控制措施矩阵中的每个控制措施的要求（参见下文第6.3项控制措施）。

2. 已具备、向云客户描述具体的技术、物理和组织措施（保护、检测和纠正），确保以下保护措施：¹²¹

- i. 可用性¹²²—管理中断风险和预防、检测和应对事件而制定过程和措施，例

¹¹⁵ 参见ENISA技术指南第6页。

¹¹⁶ 另参见NCSC指南和CNIL个人数据安全指南。

¹¹⁷ 参见GDPR第32（3）、40和42条

¹¹⁸ 参见GDPR第32条。

¹¹⁹ 参见GDPR第32条：“处理的安全性：1.考虑到最先进的技术、实施成本和处理的性质、范围、背景和目的，以及对自然人的权利和自由不同可能性和严重程度的风险，控制者和处理者应实施适当的技术和组织措施，以确保与风险相适应的安全级别，其中包括：（a）个人数据的假名化和加密；（b）确保处理系统和服务的持续机密性、完整性、可用性和弹性的能力；（c）在发生物理或技术事故时，能够及时恢复个人数据的可用性和访问权限；（d）定期测试、评估和评价技术和组织措施的有效性以确保处理过程的安全性。2.在评估适当的安全级别时，应特别考虑因意外或非法破坏、丢失、变更、未经授权披露或访问传输、存储或以其他方式处理个人数据而产生的风险。3.遵守第40条所述的经批准的CoC或第42条所述的经批准的认证机制可用作证明符合本条第1款规定的要求的要素。4.控制者和处理者应采取适当措施确保在控制者或处理者的授权下行事的任何自然人除非得到控制者的指示，否则不会进行处理，除非他或她被要求根据联盟或成员国法律执行。”

¹²⁰ 参见GDPR第32（3）、40和42条。

¹²¹ WP29云计算意见，第3页第3.4.2节，另见ICO云计算指南第13-14页。

¹²² 参见ICO云计算指南列表中的“可用性”部分第22页：“云提供商是否有足够的应对少数其他云客户的高需

如备份互联网网络链接、冗余存储和有效的数据备份、恢复机制和补丁管理，无论此类事件是意外还是恶意事件的结果；¹²³

- ii. **完整性**¹²⁴—CSP确保完整性的方法¹²⁵（例如，通过消息验证代码或签名、纠错、散列、硬件辐射/电离保护、物理访问/妥协/破坏、软件错误、设计缺陷和人为错误等来检测对个人数据的未经授权的改动，无论是意外还是恶意的）；¹²⁶
- iii. **机密性**¹²⁷—CSP从技术角度确保机密性的方法，确保只有授权人员才能访问数据；包括除其他方法外，酌情对“传输中”和“静止”¹²⁸个人数据进行匿名化和加密，¹²⁹授权机制和强身份验证；¹³⁰以及从合同的角度，对CSP及其任何员工（全职、兼职和合同工）以及可能能够访问数据的子处理者（或其他分包商）采取保密协议、保密条款、公司策略和相关规程；
- iv. **透明度**—CSP为支持透明度并允许云客户进行评审而采取的技术、物理和组织措施（见下文第7项控制措施）；¹³¹

求？其他云客户或其云用户的行为如何影响服务质量？您能否保证在需要时能够访问数据或服务？您将如何支付云用户在离开办公室时访问云服务的硬件和连接成本？如果云提供商发生重大中断，这会对您的业务产生什么影响？”

¹²³ WP29云计算意见第14页第3.4.3.1节。

¹²⁴ 参见ICO云计算指南列表中“完整性”部分第22页：“有哪些审计跟踪，以便您可以监视谁在访问哪些数据？确保云提供商允许您根据您的要求以可用格式获取数据副本。如果发生重大数据丢失，云提供商可以多快从备份中恢复您的数据（无需变更）？”

¹²⁵ 描述应涉及CSP内的所有数据层，从客户的信息上下文到物理数据组件和软件代码。

¹²⁶ WP29云计算意见第15页第3.4.3.2节。另见ICO云计算指南第22页：“确保云提供商允许您根据您的要求以可用格式获取数据副本。”

¹²⁷ 参见ICO云计算指南列表“机密性”部分第22页：“您的云提供商能否提供适当的第三方安全评估？这是否符合适当的行业CoC或其他质量标准？如果在其产品中发现安全漏洞，云提供商多快做出反应？创建、暂停和删除帐户的时间表和成本是多少？传输中的所有通信是否加密？加密您的静态数据是否合适？什么密钥管理措施？什么是数据删除和保留时间尺度？这包括报废销毁吗？如果您决定将来退出云，云提供商会安全地删除您的所有数据吗？了解您的数据或有关云用户的数据是否会与第三方共享或在云提供商可能提供的其他服务之间共享。”

¹²⁸ 参见GDPR第32（1）（a）条。

¹²⁹ 注意：“在‘传输中’和‘静止’数据可用的所有情况下，都应使用个人数据加密。……云提供商和客户以及数据中心之间的通信应该加密。”WP29云计算意见第15页第3.4.3.3节。另见ICO云计算指南，第14-15页。

¹³⁰ WP29云计算意见第15页第3.4.3.3节

¹³¹ WP29云计算意见第15页第3.4.3.4节。此外，“透明度对于公平合法地处理个人数据至关重要。95/46/EC指令要求云客户向数据主体提供有关其身份和处理目的的信息。云客户还应提供任何进一步的信息，例如有关数据接收者或接收者类别的信息，其中还可以包括处理者和子处理者，只要此类进一步信息是保证对数据主体进行公平处理所必需的（参见指令第10条）还必须确保云客户、云提供商和分包商（如果有）之间关系的透明度。如果提供商将所有相关问题告知客户，则云客户就能评估在云中处理个人数据的合法性。考虑聘请云提供商的控制者应仔细检查云提供商的条款和条件，从数据保护的角度对其进行评估。云中的透明度意味着云客户有必要了解所有参与提供相应云服务的分包商以及所有数据中心个人数据可能被处理的位置。如果服务的提供需要在云客户的系统上安装软件（如浏览器插件），作为良好实践，云提供商应将这种情况，特别是从数据保护和数据安全的角度对数据的含义通知客户，反之亦然。如果云提供商没有充分解决这个问题，则云客户应该事先提出这个问题。”WP29云计算意见第10-11页第3.4.1.1节。

- v. 隔离（目的限制）—CSP如何为个人数据提供适当的隔离（例如，对访问个人数据的权利和角色进行充分治理，包括访问授权、访问撤销、访问记录、访问冲突检测/解决和定期评审访问权限；基于“最小特权”原则的访问管理；强化虚拟机管理程序；¹³²以及在使用虚拟机在云客户之间共享物理资源的任何地方正确管理共享资源）；¹³³
- vi. 可干预性—CSP启用和促进数据主体访问、纠正、删除权利（被遗忘权）、¹³⁴阻止、反对、限制处理¹³⁵（参见下文第10项控制措施）的方法和工具，转移¹³⁶（参见下文第9项控制措施），以证明这些要求不存在技术和组织障碍，包括数据由子处理器进一步处理的情况¹³⁷（这也与下文第9项控制措施相关）；
- vii. 转移—见下文第9项控制措施；
- viii. 问责制—见上文第1项控制措施。

相关性：由于GDPR没有就具体安全措施的实施提供明确的结构或规范性规则，CoC会利用多个主管当局和相关机构/团体的指南—例如WP29/EDPB、CNIL、ICO、ENISA和ISO—为了对CSP施加结构化的方式，以披露有关技术和组织措施的信息，确保其服务内在的处理安全性。

无视数据主体的权利和自由面临的风险以及技术发展，提供要实施的特定的、“一刀切”的安全措施与GDPR第32条背后的理念背道而驰。然而，CoC建立了CSP必须采用的最低限度的安全控制基线，不管任何可能被视为减轻风险的因素（例如，CSP处理活动固有的风险级别、CSP安全计划的成熟度、成本和预算等）。这些基线安全措施在6.3的控制措施中确定，应用作CSP必须建立的基础，以便为云客户提供额外级别的保证和保护，具体取决于最新技术、实施成本和性质，处理的范围、背景和目的，以及对自然人权利和自由的不同可能性和严重性的风险。

该安全基线表示为一组要求和控制措施目标，符合信息安全领域普遍采用的最佳实践和标准。定义需求和控制措施目标背后的理由，而不是强制规定规范的技术规范/控制措施/措施，后者需要随许多因素而变，例如云部署和交付模型的类型、内部架构类型、采用的技术平台类型、技术发展等。这将阻止CoC实现所需的灵活

¹³² “虚拟机管理程序的加固”也与“完整性”有关。

¹³³ WP29云计算意见第16页第3.4.3.5节。另见ICO云计算指南第20页。

¹³⁴ GDPR第17条。

¹³⁵ GDPR第18条。

¹³⁶ GDPR第20条。

¹³⁷ WP29云计算意见第16页第3.4.3.5节。

性级别，而这对于CSP是有效和充分实施的必要条件。

但是必须指出，CoC的所有拥护者都可以访问CSA的数据和信息安全方面的知识和资源（例如CSA安全指南¹³⁸和云控制措施矩阵¹³⁹、共识评估倡议问卷¹⁴⁰等），这将允许CSP了解并实施最相关的措施。

因此，根据GDPR第32条，CSP将被要求负责制定要实施的最合适的安全措施，并在此控制结构中披露所选择和实施的措施的信息。—这将允许向云客户提供更加一致和清楚的信息，也更容易准确地了解每个CSP在安全方面提供的措施。

在任何情况下，为了建立数据保护的最佳实践，CoC在范围里会提供尽可能多的指导。因此，以下控制措施为所有CSP必须采取的最低可接受的安全措施提供指导，并参照CSA云控制措施矩阵对该事项进行了说明。

关于上述第6.2.iv项控制措施（透明度），此控制措施特指CSP已实施的安全措施，以允许云客户了解他们委托给CSP的与服务相关的个人数据的处理方式。这与下文第7项控制措施关联，后者需要确定已实施的选项，允许云客户监视和审计其数据的使用。

关于上述第6.2.vi项控制措施（可干预性），CSP尤其应向云客户提供详细信息，表明其服务不会对响应数据主体或其他与干预性相关的请求造成障碍，并解释具体措施以确保这些请求可以由CSP（因此，在适用的情况下，也可以由云客户）及时有效地解决。

3. 作为最低可接受的基线，此CoC要求CSP符合CSA云控制措施矩阵¹⁴¹中规定的控制措施。CSP必须说明和证明如何满足每个相关控制措施，同时考虑到技术级别、实施成本和处理的性质、范围、背景和目的，以及对自然人的权利和自由具有不同可能性和严重性的风险¹⁴²：

相关性：为了满足此控制措施的最低可接受基线，CSP须证明其至少已达到CSA STAR注册中心（一级）¹⁴³上的要求，具体方法是指出CSP根据CSA Cloud Controls Matrix提交的CSA STAR注册中心¹⁴⁴上的相关条目。

¹³⁸ 可在<https://cloudsecurityalliance.org/research/guidance/>获得。

¹³⁹ 可在<https://cloudsecurityalliance.org/research/cloud-controls-matrix/>获得。

¹⁴⁰ 可在<https://cloudsecurityalliance.org/research/cloud-controls-matrix/>获得。

¹⁴¹ 可在<https://cloudsecurityalliance.org/research/working-groups/cloud-controls-matrix/>获得。

¹⁴² CSP还可以考虑CNIL安全指南。

¹⁴³ 可在<https://cloudsecurityalliance.org/star/registry/>获得。

¹⁴⁴ 更多信息，请访问：<https://cloudsecurityalliance.org/artifacts/star-level-and-scheme-requirements>。

有关CSA Cloud Controls Matrix控制措施的最新版本，参阅CSA网站¹⁴⁵，或以其他方式参阅附件（CoC GDPR_Annex 1_Compliance_Assessment_Template）。

数据安全合规的证据也可以通过遵守相关CoC和认证机制的方式提供给云客户。¹⁴⁶此外，CSP还可以指出与CSP可能拥有的其他安全认证有关的控制措施（如ISO 27001、SOC2等）。但是，这并不能免除CSP确定特定安全措施以应对CSA云控制措施矩阵中的每个控制措施的要求。

7. 监督

CSP必须实施，并向云客户表明：

1. 允许云客户进行监督和审计的选项，该选项是为了确保控制规范中描述的适当隐私和“控制指南：PLA”持续得到满足（例如，对CSP或子处理者执行的相关处理操作进行记录、报告、第一和/或第三方审计¹⁴⁷）¹⁴⁸。任何审计工作都意味着审计人员可以访问存储在CSP提供服务的系统中的个人数据，则该审计人员须接受保密协议。

相关性：该控制措施进一步明确了GDPR第28（3）（h）条的要求，规定CSP有义务告知云客户，他们有效监督CSP合规的具体选择，并审核他们就服务中固有的处理活动所实施的隐私和安全措施。CSP可选择如何实现这一目标，例如维护云客户可以监督的日志，定期向云客户报告，或依靠第一方或第三方对其业务和所聘用的子处理者进行审计。

如上文第3.5项控制措施所述，云领域的标准做法是允许云客户访问由合格的独立第三方进行的审计报告，而不是提供对CSP用于处理个人数据的系统、设备或设施的直接访问。这些第三方审计必须由CSP定期进行，其频率应符合其性质和目的。这方面的最佳做法是至少每年一次审计，并在审计对象发生重大或相关变更时进行额外的临时审计，这也是普遍认可的认证和验证审计规则。

8. 个人数据违规

CSP必须确认：

¹⁴⁵ 可在<https://cloudsecurityalliance.org/research/cloud-controls-matrix/>获得。

¹⁴⁶ 参见GDPR第32（3）、40和42条。

¹⁴⁷ 见《CNIL橙色决定》，该决定引起了安全审计的缺乏。

¹⁴⁸ 见GDPR第28（3）（h）条和上文第1项控制措施。另见WP29《云计算意见》，第13页第3.4.2节，和第11页第3.4.1.2节。另见《ICO云计算指南》，第13.14页。

1. 由CSP和/或其子处理者处理的影响云客户数据的个人数据违规，应告知云客户，而不得无故延迟。并在可行的情况下，¹⁴⁹不晚于CSP意识到有关事件后的72小时。¹⁵⁰
2. 如果无法在72小时期限内将个人数据违规事件通知特定的云客户，则CSP将尽快通知该云客户有关个人数据违规的信息，并在与云客户的沟通中说明延迟原因。
3. 向云客户发出的每份通知将至少并在最大程度上包括以下信息：
 - i. 说明个人数据违规的性质，包括有关个人数据记录的类别和大致数量。
 - ii. DPO的名称和联系方式或其他可以获得更多信息的联络方式（见上文第2项控制措施）。
 - iii. 个人数据违规的可能后果，即对相关数据主体的潜在影响¹⁵¹。
 - iv. 描述为处理个人数据违规问题而采取（或拟采取）的措施，包括（在适当情况下）为减轻其可能的不利影响而采取的措施（CSP、云客户和/或数据主体自身已经或可以采取的措施）。¹⁵²
4. 如果在初始通知中不能提供上述所有信息，则CSP必须向云客户提供尽可能多的关于所报告事件的信息，并尽快提供满足上述要求所需的任何进一步细节（即分阶段提供信息）。¹⁵³

CSP必须告知云客户：

5. 根据上述控制措施，CSP有义务报告个人数据违规情况，以及如何向云客户发出通知。

相关性： CSP需要说明，如何以及何时将通知云客户所发生的个人数据违规，

¹⁴⁹ 正如本控制措施的“相关性”部分所进一步详述的，CSP对潜在的个人数据违规事件的调查可能需要一些时间，特别是在确认个人数据违规的范围方面。除了识别和评估个人数据违规的实际和技术问题外，在通知这些个人数据违规方面也可能存在类似的问题，特别是在大量云客户可能受到影响的情况下。为了最大限度地避免过早、不必要和不完整的通知，并使这一控制措施对CSP来说切实可行，我们认为CSP设定的通知云客户的期限与GDPR为控制者规定的通知监管机构的期限应相同，即在可行的情况下，从CSP意识到个人数据违规的时点起，最迟不超过72小时。

¹⁵⁰ 见GDPR第33和34条，以及《EDPS数据违规指南》的第15页和《WP29数据违规指南》的第11-12页。

¹⁵¹ 为了对此有所帮助，CSP可以参考ENISA漏洞严重程度评估建议。

¹⁵² 见GDPR第33条。

¹⁵³ 见WP29《数据违规指南》，第13-14页。“GDPR没有规定处理者必须提醒控制者的明确时限，但它必须在“无不当延迟”的情况下提醒。因此WP29建议处理者迅速通知控制者，并在获得更多细节时分阶段提供有关违规的进一步信息。这一点很重要，可以帮助控制者满足在72小时内通知监管机构的要求”。

并向云客户提供清楚透明的规程（特别是因为云客户通常作为控制者，可能依靠CSP向其提供必要的信息，以便云客户遵守其自身与个人数据违规有关的通知、沟通和记录的义务）。CSP不仅必须确定发生的个人数据违规事件，还必须在最大程度上提供欧盟监管机构在通知个人数据违规事件时要求的信息，如果无法一次性提供所有必要的信息，CSP仍应在第一次通知云客户时提供尽可能多的信息，并在可能的情况下尽快补充所缺的细节。

如果CSP发现（例如，直接发现或收到子处理者的通知）符合个人数据违规条件的事件，并确定该事件影响到CSP和/或其子处理者代表特定云客户所处理的数据，则将被视为意识到个人数据违规事件。

CSP向受影响的云客户通知所发现的个人数据违规事件的时间框架已被定义为一个基线，在可行的情况下必须满足该基线。有几种实际情况可能会导致CSP在正确识别、评估和向云客户通报个人数据违规事件的能力方面出现延误。鉴于CSP被要求通知实际的个人数据违规事件，而不是所有可能符合个人数据违规条件的事件，CSP将被要求调查所发生的安全事件并正确识别其范围。这项工作可能对于规模较小的CSP来说更加困难和费时，因为它们可能没有足够的人员或过程来立即识别或评估潜在的个人数据违规（包括事件处理可能已外包给第三方）。最后，实际通知方面还需要考虑技术情况，因为如果实际的个人数据违规影响到CSP的大量云客户，设置和发布通知的过程可能需要时间（特别是由于需要避免垃圾邮件过滤器，或其他旨在阻止大量电子邮件的机制）。此外，大规模的个人数据违规通知还可能对其他法律的应用产生相关影响。例如，意外通知某些云客户可能使其面临内幕交易的风险；某些当地法律可能要求CSP在发生与刑事有关的个人数据违规时直接通知执法机关（可能不通知云客户）—因此在完成此类外部沟通之前，需要事先进行一系列法律检索。

这些例子和其他例子被认为支持这样的论点，即CSP在向云客户报告个人数据违规的义务方面，应遵守GDPR赋予控制者对监督机构的相同时间框架：即在可行的情况下，从CSP“意识到”个人数据违规（即，确定个人数据违规事件已经发生并影响到特定云客户）的72小时内。在任何无法满足72小时期限的情况下，CSP仍应尽快通知云客户，并提供延迟的原因。当然，CSP也可能希望在与云客户的协议中约定更短的事件响应期限，特别是在其云客户属于特定部门（包括欧盟机构和机关¹⁵⁴）的情况下，可能会受到更严格的通知要求。

CSP必须考虑的潜在影响包括数据主体因个人数据违规将或可能遭受的任何形式的伤害。为了帮助评估这种影响，强烈建议CSP参考ENISA违规严重性评估建议

¹⁵⁴ 须遵守2018年10月23日欧洲议会和理事会第2018/1725号条例（欧盟）的实体。

中描述的方法，该建议列出了客观标准，允许根据有关个人数据违规的特点计算“严重程度”。也建议CSP参考WP29《数据违规指南》中提供的例子，这些例子说明了相关数据主体具有不同风险的情况。

CSP还可能告知云客户，他们依靠专业的第三方（如隐私顾问）来管理所发生的任何个人数据违规事件。

9. 数据转移、迁移和回传

CSP必须具备，并向云客户说明。

1. 确保数据转移的规程或过程，即以结构化、通用、机器可读和可互操作的格式传输个人数据的能力：¹⁵⁵
 - i. 给云客户（回传，例如，传到内部IT环境）
 - ii. 直接向数据主体提供
 - iii. 传给另一个服务提供商（迁移），例如，通过下载工具或应用程序编程接口，或API）。¹⁵⁶

¹⁵⁵ 见GDPR第68号叙文。

¹⁵⁶ 数据转移的权利被授予数据主体，在大多数情况下，他们是云客户的客户。更确切地说，根据GDPR第20条，“数据主体应有权以结构化的、常用的和机器可读的格式接收他或她提供给控制者的关于他或她的个人数据，并有权将这些数据传送给另一个控制者，而不受向其提供个人数据的控制者的阻挠，其中：（a）根据第6（1）条（a）点或第9（2）条（a）点，处理是基于同意，或根据第6（1）条（b）点，处理是基于合同；以及（b）处理是通过自动化手段进行的。2.在根据第1款行使其数据转移权利时，如果技术上可行，数据主体应有权将个人数据从一个控制者直接传送到另一个控制者。”这意味着云客户必须确保代表控制者（云客户）处理个人数据的CSP确保数据转移。显然，当CSP作为数据控制者处理数据时，它们必须保证数据的转移。请参阅WP29转移指南，了解支持遵守数据转移权利的实用指南、最佳做法和工具。数据转移权利是GDPR引入的一项新权利。然而，即使在GDPR直接适用于欧盟成员国之前（2018年5月25日），似乎也有足够的理由将数据转移视为欧盟个人数据保护的一般原则，如“数据准确性”（《数据保护指令》第6（1）（d）条）、“数据可用性”以及根据《数据保护指令》第11（1）（c）和12条授予数据主体权利的可能性，将数据可携性视为一项强制性要求。另见WP29云计算意见，第3.4.3.6节，第16页和ICO云计算指南，第22页：“确保云供应商允许你根据你的要求，以可用的格式获得你的数据副本。”此外，见《欧盟云计算SLAS指南》第5.4节，数据转移。

对背景或要求的描述

以下的服务等级目标列表与CSP输出数据的能力有关，所以客户仍然可以使用，例如在终止合同的情况。

说明对服务等级目标的需求，除了通过认证可获得的信息之外

在相关的安全控制框架和认证中，数据转移控制的实施通常侧重于适用的CSP策略的规范，这使得云服务客户很难（有时甚至不可能）提取与可用格式、接口和传输速率相关的具体指标。以下服务等级目标列表集中在CSP数据转移特征的这三个基本方面，客户可以使用这些特征，例如，与供应商的终止过程相关的技术特征进行谈判。

相关服务等级目标的描述

数据转移格式：云服务客户数据可转移到/或从云服务访问到的电子格式。

数据转移接口：可使用各种机制将云服务客户数据传输到云服务中或从云服务中传输出来。该规范可能包括传

CSP必须向云客户表明：

2. CSP将如何协助云客户将数据迁移至另一服务提供商或迁移回内部IT环境，并为此支付多少费用。¹⁵⁷无论实施何种规程，CSP必须与云客户真诚合作，提供合理的解决方案。

相关性：这种控制不仅反映了GDPR中与数据转移权利有关的义务。它更进一步，将这一权利扩展到云客户本身（在B2B背景下，他们不会是数据主体）。CSP必须保证，即使没有数据主体的请求，云客户也可以触发转移权利，这反映了GDPR中数据转移权利条款的巨大扩展。云客户的关键是，在与遵守CoC的CSP开展业务时，他们将控制自己的数据。

上述内容不仅适用于转移本身，还适用于将数据迁移到其他服务提供商以及将数据“回传”到云客户的内部IT环境。

10. 对处理的限制

CSP必须制定并向云客户解释：

1. 必要时限制处理个人数据的规程或过程；考虑到在处理受到限制的情况下，除存储外，这些个人数据只应在征得数据主体同意后处理，或为确立、行使或辩护法律主张，或为保护另一自然人或法人的权利，或为欧盟或某成员国的重要公共利益而处理。¹⁵⁸

相关性：要求CSP明确解释如何在实践中落实限制处理个人数据的权利。云客户不仅应能够了解何时可能触发该权利（参考GDPR第18条），而且应了解CSP将如何阻止使用超出存储或GDPR规定的其他例外情况的受限数据（例如，行使和辩护法律主张），以及如何在CSP的系统内将数据标识为受限数据。

CSP可能寻求解决这一权利的例子包括：采取措施将受限数据与CSP使用的一般处理系统隔离、阻止或以其他方式使CSP的最终用户无法使用受限数据、从网站上删除受限数据、标识个人数据使其不能被改变或进一步处理、明确标识受限数据

输协议的规范和API的规范或任何其它机制的规范。

数据传输率：使用数据接口中所述的机制将云服务客户数据传输入/传出云服务的最低速率。”

¹⁵⁷ 见WP29云计算意见，第3.4.3.6节，第16页。

¹⁵⁸ 见GDPR第18条：“限制个人数据处理的方法可以包括，除其他外，将选定的数据暂时转移到另一个处理系统，使用户无法获得选定的个人数据，或暂时从网站上删除已发布的数据。在自动归档系统中，原则上应通过技术手段确保对处理的限制，其方式是使个人数据不受进一步处理操作的影响，并且不能被改变。个人数据的处理受到限制的事实应在系统中明确指出。”GDPR序言67。

等等。任何此类措施都需要是临时性的和可逆的，以便在取消限制时可以撤销。

11. 数据留存、归还和删除

11.1 数据留存、归还和删除策略

CSP必须具备，并向云客户说明：

1. CSP的数据留存策略，时限和服务终止后归还个人数据或删除数据的条件。

CSP必须具备，并向云客户说明：

2. 适用于CSP的子处理者的数据留存策略、时限和服务终止后归还个人数据或删除数据的条件

11.2 数据留存

CSP必须定义、向云客户表明并承诺遵守：

1. 个人数据将被保存或可能被保存的时间段，或者如果不可能，则确定该时间段的标准。¹⁵⁹

在确定留存期时，CSP必须考虑以下标准：

2. 必要性—为了达到收集个人数据的目的，个人数据留存的时间要尽可能长，只要仍有必要实现这一目的（例如，执行服务）；法律义务—为了遵守适用的保留数据的法律义务，在该义务规定的期限内个人数据留存的时间要尽可能长（例如，根据适用的劳动法或税法的定义）；机会—在适用法律允许的范围内保留个人数据（例如，基于同意的处理，为建立、行使或抗辩法律索赔而进行的处理—基于与履行服务性能有关的法律索赔的适用时效法规）。

¹⁵⁹ 注意：“一旦不再需要留存个人数据，就必须将其删除[或匿名化]。”WP29云计算意见，第3.4.1节，第10页，以及“如果由于法律上的保留规则（例如税收法规），这些数据不能被删除，对这些个人数据的访问应该被阻止。”第3.4.1.3节，第11页，以及“由于个人数据可能被冗余地保存在不同地点的不同服务器上，因此必须确保它们的每个实例都被不可逆转地删除（即以前的版本、临时甚至文件碎片也要被删除）。”3.4.1.4节，第12页。参见《数据保护指令》第6条，以及GDPR第5、13（2）（a）和14（2）（a）条。另见WP29《云计算意见》，第3.4.2节，第13页。

11.3 为遵守特定部门的法律要求而留存数据

CSP必须具备，并向云客户声明：

1. 云客户要求CSP遵守特定部门法律法规的规程，要求个人数据的特定留存期限。

160

11.4 数据归还和/或删除

CSP必须具备，并向云客户表明：

1. 在合同/服务终止后，将个人数据以允许数据移植的格式向云客户返还的规程（另见上文第9项控制措施）；
2. 不论是应云客户的要求，还是应数据主体的有效删除请求，CSP及其子处理者可能使用的数据删除方法。

CSP必须向云客户明确解释：

3. 在云客户删除（或要求删除）数据后，或在合同/服务终止后，是否可以保留数据；
4. 保留数据的具体原因；
5. CSP的数据留存期限。

相关性：通过要求CSP提供上述所有信息，本控制措施旨在为云客户提供透明性，使其了解CSP可能留存其数据的期限。此外，在规定可用的或用于删除数据的方法时，CSP还必须明确他们将如何提供相关证据，例如提供一份经认证的声明，说明云客户数据的额外副本不再留存在CSP或其子处理者的系统中。

特别是，CSP必须告知云客户，他们将通过何种方式允许删除存储在其系统中的个人数据，无论是否由云客户（例如，由于服务的终止）或数据主体（根据GDPR第17条有效行使其删除权）主动提出。通过这种方式，云客户将了解到，作为控制者，CSP将如何履行其义务，处理数据主体的有效删除请求，同时确保删除可能进一步存储在CSP系统中的与这些数据主体有关的个人数据。

¹⁶⁰ 参见《ICO云计算指南》，见第16-17页。

在云中删除数据的措施的例子包括：从数据库、存储和备份系统中初始授权，然后进行数据覆写或加密粉碎（即对数据进行加密并销毁加密密钥的做法），以确保完全删除数据。在实施这种做法后，可以通过广泛的控制文件来提供删除的证据，说明数据是如何处理和删除的，然后是相关的处理日志。

应该注意的是，提供100%的保证，确保数据已被删除是很难实现的。例如，为了确保这一点，云客户需要在将数据存储于云端之前用一个强大的密钥对其进行加密，永不丢失密钥，并在完成后删除密钥。这将使完全删除的可能性接近100%（取决于加密算法），因为CSP从未同时访问过密钥和数据。

12. 与云客户的合作

CSP必须履行，且向云客户说明：

1. 与云客户合作的规程或过程，以确保遵守适用的数据保护规定，例如，使云客户能够有效地保证数据主体行使其权利（访问权、更正权、删除权或“被遗忘权”、限制处理权、转移权和与自动化决策相关的权利）、执行DPIA和要求事先咨询监管机构，以及当出现安全/个人数据违规事件¹⁶¹时进行包括取证分析在内的事件管理。另见上文第6项和第8项控制措施。

CSP向云客户承诺：

2. 向云客户和主管监管机构披露必要的信息，以证明其遵守规定（另见上文第1项控制措施）。¹⁶²

相关性：在GDPR中没有直接规定CSP与其云客户合作的义务（GDPR第28条中提到的除外），但这对于云客户必须恰当遵守其关于个人数据违规的义务，响应数据主体的权利，并在整体上确保他们能够证明其参与处理个人数据的做法合规是至关重要的。

CSP还需要承诺不但向云客户，而且向问询的监管机构提供可能需要的信息，以证明他们遵守适用的法律义务和CoC的条款。

还应该注意的，由于使用CSP的服务，这种方式的合作可能是云客户仅有的途径以获得全部必要信息用于完成所使用服务的DPIA。

¹⁶¹ WP29云计算意见，第3.4.2节，第13页。请注意，CSP有义务支持客户促进数据主体权利的行使，并确保任何分包商也是如此。WP29云计算意见，第3.4.3.5节，第16页

¹⁶² GDPR第5条第（2）款和第28条第（3）款（h）项。

CSP必须特别关注他们向云客户提供明确和具体的信息，说明他们将如何协助云客户处理存储在CSP的系统上的个人数据（或由CSP以其他方式处理）有关的数据主体请求，包括数据转移权（上文第9项控制措施）、限制处理的权利（上文第10项控制措施）、删除权（上文第11.4.2项控制措施）和数据主体在自动化决策方面的权利，其形式是CSP对这些自动化决策实施的保障措施（上文第3.1.10项控制措施）。

这应该包括确保数据主体权利得到保护的具体过程信息，以及在提供这种协助时是否涉及云客户的任何费用。

请注意，如果云客户将个人数据违规事件告知CSP，CSP对云客户的义务变成合作义务，而不是通知义务（在上文第8项控制措施中提及），因为云客户已经意识到个人数据违规。在此条款下，CSP应向云客户介绍他们将如何协助客户管理个人数据违规事件（例如共享信息、讨论和实施缓解/预防措施等）。

13. 法律要求的披露

CSP必须履行，且向云客户说明：

1. 管理和回应执法机构关于披露个人数据请求的规程，包括在回应任何此类请求之前核实其法律依据，特别注意向有关云客户发出通知的规程，除非另有禁止，例如刑法作出的为执法调查保密的禁止性规定。¹⁶³

相关性：CoC强调对云客户的透明度，这意味着他们必须清楚地了解CSP将在何种情况下根据监管机构的要求向其披露个人数据处理方法，从而允许云客户不仅能够事先评估这一规程，而且在适用法律允许的范围内为云客户提供干预的可能性（例如，为了限制披露或对请求提出异议）。此规程必须说明CSP将如何评估这些请求本身的合法性，在什么情况下云客户可能不会被通知此类请求和披露（必须严格基于防止这种情况的适用法律），并承诺只披露合法处理此类请求所需的严格意义上的最小数量个人数据。

14. 云客户的补救措施

CSP必须履行，且向云客户表明：

¹⁶³ WP29云计算意见，第3.4.2节，第13-14页。另见WP29电子通信监视意见和ICO云计算指南，第19-20页。另见GDPR序言115。

1. 在CSP和/或CSP的子处理者（参见上文第3项控制措施，以及更具体的第3.3项控制措施）在违反“控制指南：PLA”中的义务情况下，云客户可采取的补救措施。

CSP还必须清楚地向云客户表明：

2. 根据CoC的规定，云客户可以针对这类违规行为向CSP提出投诉的可能性和方式。

相关性：只要CSP或子处理者在实践中未能或不再遵守CSP为遵守CoC而提交的公开自评/第三方评估中的声明/承诺，就存在违反“控制指南：PLA”义务的行为，而根据该声明/承诺，已就指定服务授予遵守标识。

为了进一步强调CSP对遵守适用法律和CoC条款的承诺，CSP需要在发生违规事件时为云客户提供补救措施。可能的补救措施包括云客户终止与CSP的协议，以及更复杂和结构化的补救形式（包括例如：服务信用和/或合同罚款¹⁶⁴）

作为最佳实践，提供的补救措施最好是业务友好的（从而在可行的情况下保持云客户和CSP之间的服务关系），并为违规事件中的云客户提供适当补偿。

提供此类补救措施不得妨碍云客户对CSP采取法律行动的权利，以及云客户向CoC监管机构提交投诉CSP的可能性。

云客户必须具有自由选择是否追求法律行动或提交投诉的权利，无论是否向他们提供了补救措施

但是，当云客户接受了CSP提供的补救措施（不仅仅是终止与CSP的合约，而是为云客户提供某种补偿），CSP可以要求云客户承诺在适用法律允许的情况下，不对CSP的相同违规行为提起法律诉讼或提交投诉。

如CoC第三部分所述（并在附件7中进一步阐述），云客户有权向违反“控制指南：PLA”的CSP提交投诉。

CSP需要明确告知云客户提供CoC¹⁶⁵的链接和用于提交CoC投诉的CSA线上表单的可能性，以及如何操作。¹⁶⁶

¹⁶⁴ WP29云计算意见，第3.4.2节，第2页。

¹⁶⁵ 参见<https://cloudsecurityalliance.org/artifacts/cloud-security-alliance-code-of-actor-for-gdpr-control/>。

¹⁶⁶ 参见<https://cloudsecurityalliance.org/star/feedback/>。

15. CSP 保险策略

CSP必须履行，且向云客户说明：

1. 相关保险策略的范围（例如，数据保护合规保险，¹⁶⁷涵盖未能履行其数据保护义务¹⁶⁸的子处理者的保险（脚注168）和网络保险，有关安全/个人数据违规的保险）。

相关性： 这项条款用于向云客户保证，如果CSP因自身或子处理者的违规行为或个人数据违规而遭受损失，CSP将得到充分保障（但不包括随之而来的行政罚款或制裁，因为在欧洲这通常是不在保险范围内的）。

CSP必须向云客户披露他们的保险范围，以便使他们可以了解该保险如何作为业务连续性的保证（避免由于破产或控制权的突然变更导致无法履行）。

在向云客户提供其保险范围的信息时，CSP应明确指出：

- 保险策略的范围；
- 保险范围（根据保额计算）；
- 任何相关的例外条款。

CSP必须确保向云客户提供有意义的信息，说明CSP在发生违反数据保护相关义务，个人数据违规或其他相关事件时能触发保险的程度。

¹⁶⁷ GDPR第58条、第77条及其后各条。

¹⁶⁸ GDPR第28条第（4）款。



第三部分

CSA 行为准则治理
和遵守机制

云的范围不是一成不变的而是应时而变的。**CSP**和云客户必须及时满足有关个人数据保护的所有新法律法规的合规要求。相关方和现有合规工具必须进行调整，以确保现有的安全和隐私措施不断发展，并不断满足任何新的监管要求。

CoC覆盖的范围处于不断变更的过程。在这种情况下，需要一个治理结构以确保变更的一致性，可控制性和可实施性，并准确定义“是否”、“何时”、“如何”以及由“谁”将此类变更应用于**CoC**和相关文件。

关于**CoC**的治理结构，应重点考虑以下因素：

1. 技术部分：随着时间的推移，将受到法律、监管和技术环境变更或**CSA**内部变更所影响的组件；
2. 治理过程：与**CoC**技术部分的定义、修订和实施相关的治理过程和相关活动；
3. 治理小组：主要的治理机构及他们的角色和职责；

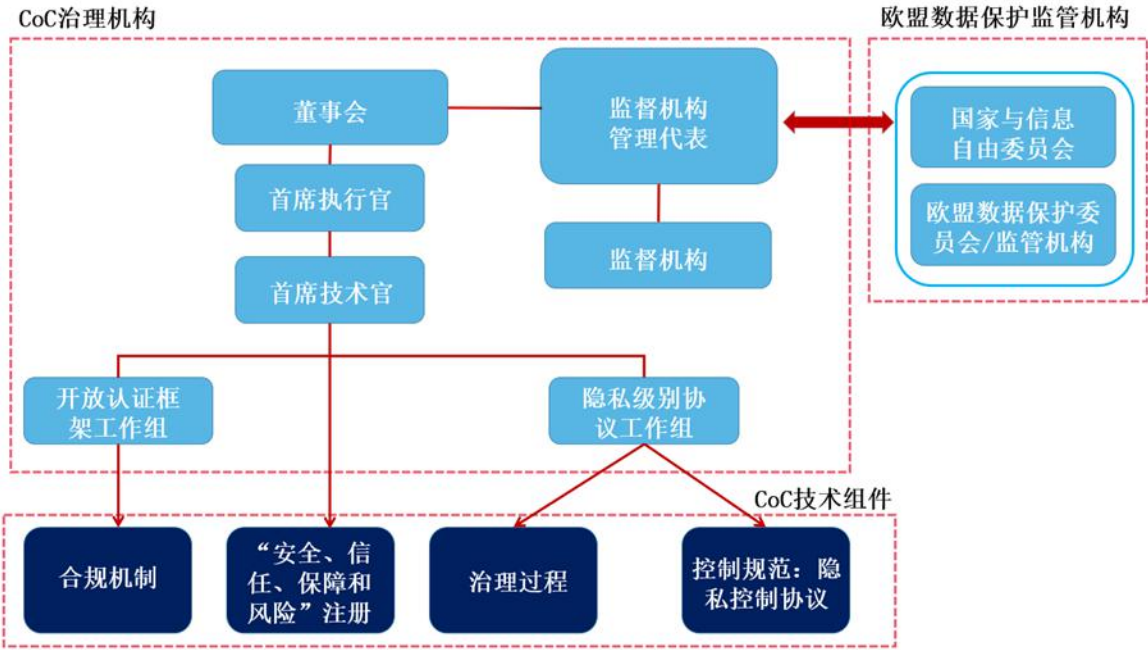
1. 技术构建

为了便于参考，请参阅下表

技术构成	描述
CoC	CoC是指CSA GDPR合规行为准则（即本文）
控制指南：PLA	“控制指南：PLA”是体现在CoC第2部分中，描述CoC数据保护控制措施的技术标准
治理过程	所有在第3节中提及的7个过程： <ul style="list-style-type: none">• 第3.1节“控制指南：PLA”评审过程；• 第3.2节CoC遵守机制评审过程；• 第3.3节颁发CoC认证标识和遵守声明的发布；• 第3.4节投诉管理过程；• 第3.5节持续监督过程；• 第3.6节道德准则评审过程；• 第3.7节PLA和OCF工作组章程文件审核过程。
遵守机制	第1.2节中定义的CoC遵守机制，如下所示： <ul style="list-style-type: none">• 第1.2.1节CoC自评估；• 第1.2.2节CoC第三方评估
STAR注册中心	将提交给监督机构并经其批准的自评估和第三方评估申请，以及随后授予的关于遵守规定的CSP的具体服务的遵守标识归档。

治理组织	角色和职责
CSA董事会	<p>董事会是CSA中的主要治理委员会。除其他任务外，董事会还负责批准首席执行官提出的CSA年度计划和预算。</p> <p>董事会包括一个审计委员会，该委员会是董事会内部的一个小组，由至少两2名董事会成员组成，任务是：</p> <ul style="list-style-type: none"> • 作为CSA的STAR计划的一部分，支持和监督CSP实施CoC遵守机制； • 在与云上个人数据保护相关的事项上与监督机构合作并提供支持（例如，提供有关遵守CoC的CSP的信息/证据）
监管机构	<p>提供与欧盟数据保护法（例如GDPR）相关的指导，建议和最佳实践。</p>
开放认证框架工作组	<ul style="list-style-type: none"> • 定义、评审和批准CSA OCF/STAR计划内新的或现有的认证方案和一致性方法的变更。； • 管理遵守评估方法/遵守机制，以及监督相关活动； • 维护STAR注册中心； • 向董事会汇报。
PLA工作组（PLA WG）	<ul style="list-style-type: none"> • 定义，批准和更新“控制指南：PLA”的变更； • “控制指南：PLA”和其他隐私标准的对比（即映射和差距分析）； • 管理“控制指南：PLA”并确保过程的维护； • 向董事会汇报，并将结果传达给OCF工作组

治理组织	角色和职责
监督机构	<ul style="list-style-type: none"> • 评估云服务商申请者的资质是否符合“控制指南：PLA”要求； • 监督并核实CSP持续遵守控制指南的情况； • 管理投诉并向不合规的云服务商提出纠正措施； • 与监督机构合作并报告关于CoC的执行情况（例如，投诉管理活动，执行的审计）。 <p>监督机构包括一名监督机构管理代表（MBMR），他是监督机构的成员，任务是代表监督机构执行关键任务，在下文第2.5节中进一步阐述。</p>



1.1 控制指南：PLA

在该CoC的第2部分提供的“控制指南：PLA”是识别欧盟相关的个人数据保护合规要求的技术标准，并定义了管理这些要求合规的条款和控制措施。

“控制指南：PLA”构成该CoC的基本技术组成部分。

1.2 CoC 遵守机制

对于愿意遵循“控制指南：PLA”要求的云服务供应商，其需要提交遵守声明（见附件2）至CSA，表明其符合本文档中提及的原则、策略和指南、及持续更新的CoC要求，该遵守机制由开放认证框架（OCF）工作组制定，并由CSA颁布。

遵守声明应由公司或组织的法定代表人签署，且应遵守PLA第三版模板（见附件1）格式、并以自评估或第三方评估的形式呈现。

CSA GDPR合规CoC遵守模板以表格结构总结了“控制指南：PLA”中包含的要求。

需要明确的是云服务供应商必须考虑所有“控制指南：PLA”，而不仅是声明遵守其中的某一部分。

CSA GDPR合规遵循CoC是CSA认证框架的组成部分，即STAR计划/开放认证框架（OCF，见附录3）。CoC预设了两种遵守机制，对应两（2）种保证级别。

1. CoC自评估；
2. CoC第三方评估。

下文中第1.2.1章节确定了实现CSA CoC自评估的过程。

CoC遵守机制定义了遵守该准则的目标、策略、机制、范围、规则、要求及过程。

- a) 遵循范围和目标；
- b) 审计规则和机制；
- c) 审核员认可过程；

- d) 撤销条件和申诉机制；
- e) 遵循费用。

1.2.1 CoC 自评

CoC自评是云服务供应商在CSA STAR注册中心（见附录3）自愿发布如下2（两）份关键文件的行为：

- CoC遵守声明（见附录2），及
- PLA模板（见附录1）

PLA模板及CoC遵守声明将被提交至监督机构以便对如下内容进行验证：

- CoC中的所有章节都被包含；
- 提供的细节足够有效支持对现有或潜在云客户的非正式评估；并且
- 确定一个“诚信者”努力以完全满足“控制指南：PLA”制定的要求。

监督机构将同时验证提交者已在其网站上发布的CoC公开符合声明。一旦验证所有必要条件已经达成，监督机构将公布（提交者）对应于CSA STAR注册中心资质的自评结果，并在其上加盖CoC自评遵从性的标识。

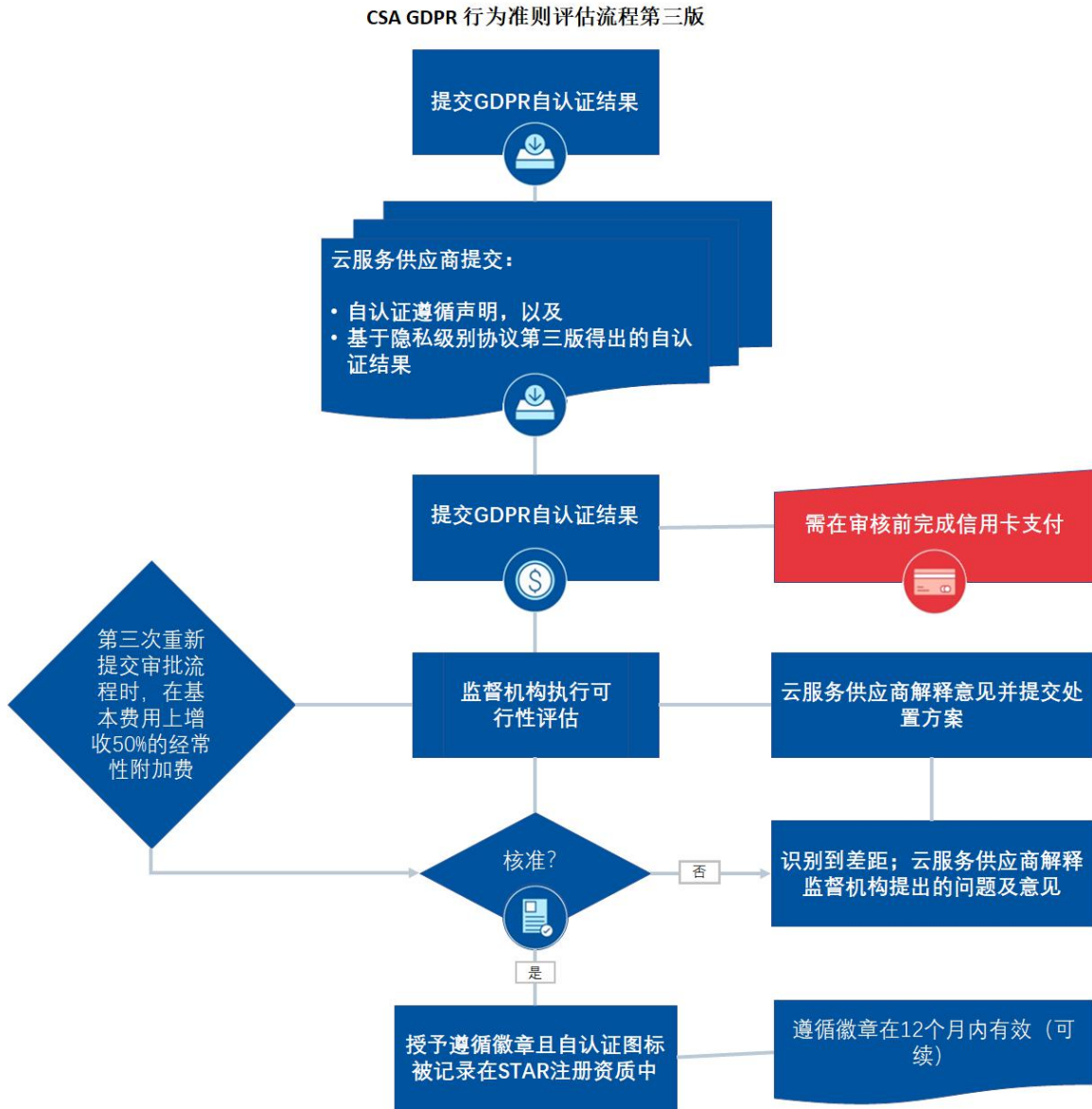
CoC自评符合资格有效期为自颁发之日起的12个月内，且应在此有效期后进行续证。每次续证需要重新提交经过更新的CoC遵守声明（附录2）和PLA模板（附录1）。同时，应在CSP相关策略及实践发生变动时，对CoC自评内容进行修正，并提交新的证明。

基于CSA STAR注册中心资质自评结果的发布—如附录4所示，其内容应可在公开网站上被任何人自由访问到，这种方式确保了CoC自评受到必要的公众监督，并提供了相较于云服务供应商所提供服务的隐私程度而言更高的透明度。对公布自评结果的公众监督是监督CoC遵从性实施情况的有效机制。

自评的撤销条件和投诉机制在下文3.3节“CoC符合资质签发及遵守声明的发布”和3.4节“投诉管理过程”中进行说明。

应指出的是CSA STAR注册资质的发布和遵守标识的颁发可能受限于管理费的缴纳情况（而有所区分）。

下图简要总结了评估和申请自评估遵守审批的过程：



1.2.2 CoC 第三方评估

CoC第三方评估是由经授权的CoC审计合作伙伴（详见下文描述）对CSP的PLA控制指南的遵从性情况实施的验证（活动）。其验证过程包含如下内容：

- 对CoC的正确使用（例如：是否CSP完成了PLA控制指南中的全部内容？是否每个章节所包含的内容提供了有关数据处理和处置的必要信息？）

- CoC中包含信息的准确性（例如：提交的信息是否真实可信？声明内容是否有相关证据支持？）

第三方审核应基于一系列过程分析的纸质记录和人工评审来完成。

如上所述，验证必须由与CSA签订了“合格CoC审计合作协议”的授权CoC审计伙伴来执行。合作伙伴协议中的重要要求如下：

- 合作伙伴应具有ISO17021及ISO17065资质；
- 作伙伴应至少雇佣一名符合CoC执业要求的CoC授权审核员；
- 合作伙伴应至少雇佣一名CoC授权安全专家全职或兼职承担审计工作中对应部分工作（这名人员也可以是CoC认证审核员）。

应注意的是，成为授权的CoC审计伙伴的CSA企业会员名单将被免费公布在CSA网站上¹⁶⁹。

授权的CoC审核员应是满足以下要求的专业人士：

1. 具备至少两年有关数据保护法律合规的经验或持有相关专业证书（如IAPP CIPP/E¹⁷⁰，ECPC-B DPO认证¹⁷¹，CSA CoC培训及认证¹⁷²）。

授权的CoC安全专家应是满足如下要求的专业人士（请注意，根据被审核公司的信息安全认证状态，要求会有所不同）：

1. 被审核公司已具备相关信息安全资质（如CSA STAR认证/评估¹⁷³，ISO27001）：具备至少1年的云安全合规经验或持有相关专业证书（如CSA CCSK¹⁷⁴，ISC2 CCSP¹⁷⁵）。
2. 被审核公司不具备相关信息安全资质（如CSA STAR认证/评估，ISO27001）。具备至少3年相关信息安全认证对应技术、物理及组织合规的经验，或持有相关

¹⁶⁹ 任何满足相关要求成为授权的CoC审计合作伙伴的公司中，仅有那些也同时具备CSA企业会员资质的公司会被免费公布在CSA网站上。成为授权CoC审计伙伴的非CSA企业会员仍需缴纳注册费以将其信息公布在CSA网站上。

¹⁷⁰ 更多信息参见：<https://iapp.org/certify/cippe/>。

¹⁷¹ 更多信息参见：<https://www.maastrichtuniversity.nl/research/institutes/ecpc/professional-certification-education>。

¹⁷² 更多信息参见：<https://gdpr.cloudsecurityalliance.org/>。

¹⁷³ 更多信息参见：<https://cloudsecurityalliance.org/star/levels/>。

¹⁷⁴ 更多信息参见：<https://cloudsecurityalliance.org/education/ccsk/>

¹⁷⁵ 更多信息参见：<https://www.isc2.org/Certifications/CCSP>。

专业证书（如ISACA CISA¹⁷⁶，CSA STAR认证审核员¹⁷⁷，ISO27001主任审核员）。

审计顺利完成后，如经验证满足所有条件，授权CoC审计合作伙伴将以提问形式向CSP出具评估结果。同时，授权CoC审计合作伙伴将通知CSA和监管机构审计过程顺利完成，并代CSP向监管机构提交CoC遵守声明（附录2）和PLA模板（附录1）。

监管机构在发现了违反CoC遵守声明和（或）PLA模板内容的情况下，将向代提交材料的授权CoC审计合作伙伴进行反馈。授权CoC审计合作伙伴应基于监管机构的反馈随后审阅所提交的材料，并在必要时联系CSP。

如未发现违反情形或者之前发现的违反情形并已完成改进，CSA将继续基于CSA STAR注册资质进行CoC遵守声明（附录2）和PLA模板（附录1）的发布，且监管机构将向其授予CoC第三方评估符合资格。

CoC第三方评估符合资格有效期为自颁发之日起的12个月内，且应在此有效期之后进行续证。每次续证需要重新提交经过更新的CoC遵守声明（附录2）和PLA模板（附录1）。同时，应在CSP相关策略及实践发生变动时，对CoC第三方评估内容进行修正。

自评估符合资质的撤销和投诉机制在下文3.3节“CoC符合资质签发及遵守声明的发布”和3.4节“投诉管理过程”中进行说明。

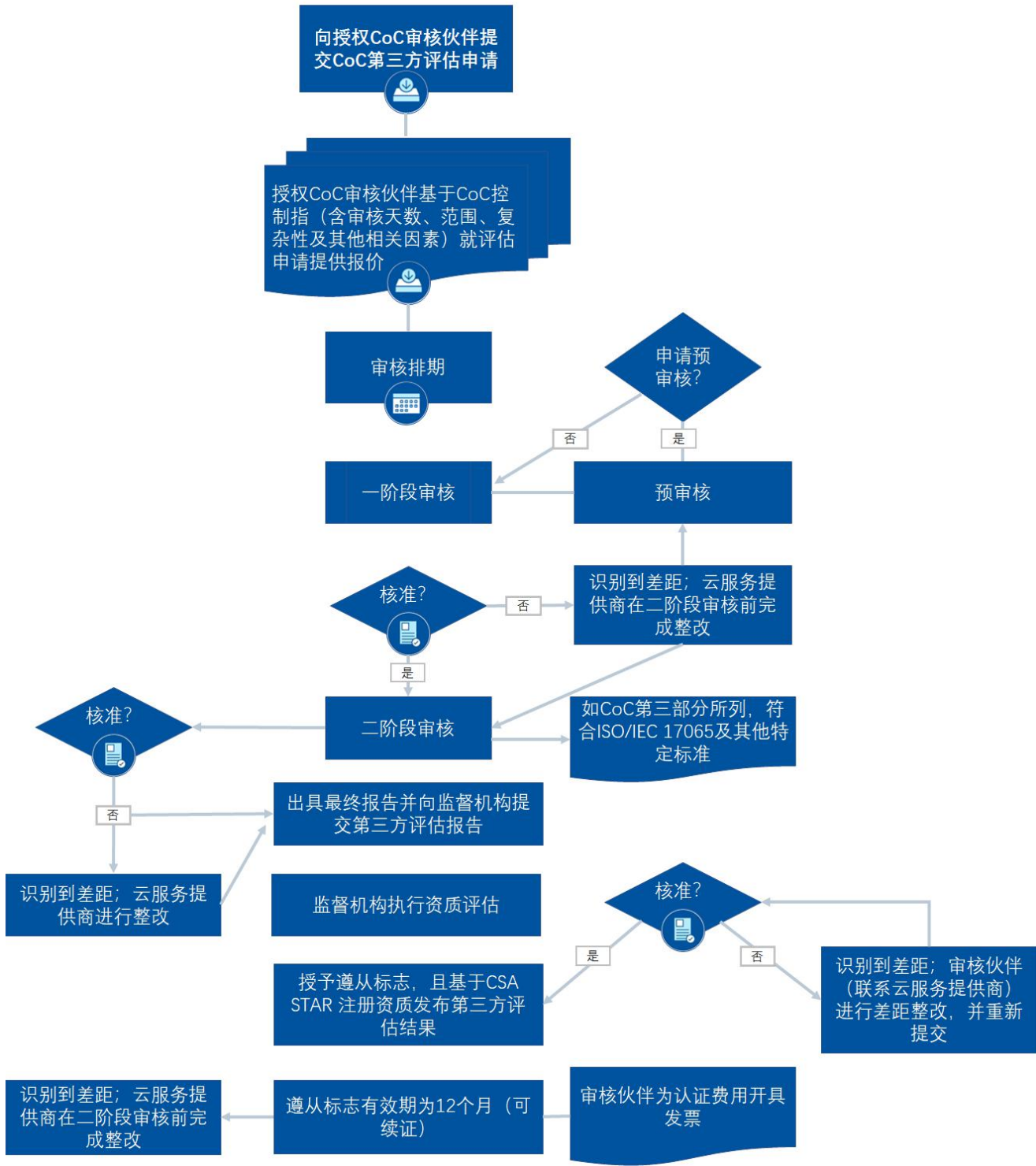
应指出的是CSA STAR注册中心资质的发布和遵守标识的颁发可能受限于管理费的缴纳情况（而有所区分）。

下图简要总结了评估和申请第三方遵守审批的过程：

¹⁷⁶ 参见：<http://www.isaca.org/Certification/CISA-Certified-Information-Systems-Auditor/Pages/default.aspx>。

¹⁷⁷ 更多信息参见：<https://cloudsecurityalliance.org/star/auditors-and-consultants/>。

CSA GDPR 行为准则评估流程第三版



1.3 道德准则

参见下文附录4中有关道德准则内容的描述。

1.4 隐私级别协议（PLA）工作组及开放认证框架（OCF）工作组章程

参见下文附录5、附录6中，分别对应于PLA（PLA）工作组、开放认证框架（OCF）工作组的描述。

2. 治理工作组、角色和职责

CoC及其技术部分（控制指南：PLA、遵守机制和道德准则）的管理是PLA工作组、OCF工作组和CSA的共同职责。

2.1 PLA 工作组

PLA工作组负责定义、批准和更新技术标准/操作规范的变更，例如“控制指南：PLA”（当前第3版，例如，PLA [v4]）。当发生关于CoC自评或第三方评估的投诉时，该工作组也以专家身份向监督机构提供意见。PLA工作组章程定义了工作组的目标和范围、成员、结构和职责；与其他相关CSA工作组的关系；以及相关的对外活动、业务、沟通方式、决策过程、活动、交付成果、期限和知识产权策略。每个成员都有权对CoC提出修改建议。

任何隐私、数据保护和/或数据安全方面的专家，无论其从属关系如何，都可以自愿参加PLA工作组。

2.2 OCF 工作组

该工作组负责定义CSA STAR计划内采用的认证方案。OCF工作组定义、评审和批准CSA OCF/STAR计划中现有认证方案的变更；并定义、评审和批准任何新的认证方案。同时负责定义、评审和批准CoC遵守机制中的变更。

OCF工作组的章程（见下文，附件6）规定了工作组的目标、范围、成员、结构

和职责；与其他相关CSA工作组的关系；以及相关的外部活动、业务、沟通方法、决策过程、活动、交付成果、期限和知识产权策略。每个成员都有权对CSA STAR计划下包含的认证方案以及CoC遵守机制提出修改建议。

2.3 云安全联盟（CSA）

作为STAR计划的一部分，CSA支持并监督CoC遵守机制的实施。这些活动包括但不限于以下内容：

- 维护已签发的CoC合规证书的公共注册表（STAR注册）。每个条目至少包括以下信息：（i）组织的名称和描述，（ii）与CoC相关的服务的名称和描述，（iii）CoC条目，（iv）使用的CoC的版本（目前为V4），（v）标识的有效性，（vi）审计组织/审核员名称（如果适用）；
- 维护授权的CoC优质审计合作伙伴的公共注册表；
- 维护一个提供关于CoC概念、方法和技术标准的信息和指南，以及遵守机制的要求、过程和成本介绍的网站；
- 开发和维护CoC：
 - 定义如何提交和评审CoC自评估的指导方针；
 - 审核CoC自评估并验证是否满足最低要求；
 - 维持投诉机制；
 - 提供处理冲突的指导；
 - 设立一个咨询机构，负责支撑CSA实施和监督STAR计划；
- 在标准制定、标识实施和管理过程中确保透明度和完整性；
- 批准OCF章程修订和延期；
- 批准PLA的修订和延期；
- 制定并审核遵守费用；
- 授权CoC合格的审核员培训合作伙伴；

- 公开所有收取的费用和其他收入及在本项目管理中使用的情况

2.4 针对监管机构的协作和支持行动

CoC治理工作组同意根据以下条款，在云中的个人数据保护相关事宜上要支持国家数据保护部门（监管机构）。

关于协作，根据监管机构或EDPB的要求，CoC治理小组将合理地遵守要求，并提供以下内容：

- 针对云计算服务的公司和个人用户的指导方针和宣传倡议；
- 对应发布的有关数据保护法的意见提供建议（例如，监管机构依法应向相关国家议会和/或公共当局提出的意见）。

关于支持行动，在监管机构或EDPB的要求下，CoC治理小组还将合理地遵守要求，并执行以下操作：

- 提高CoC自评和第三方评估公司对监管机构发布的措施的认识（向CoC自评或第三方评估公司发布的一般规定及特殊规定）；
- 如果监管机构对遵守CoC的公司进行检查，应向监管机构提供CSA中关于遵守CoC的公司的所有可用信息和证据。在这些情况下，CoC治理小组将充当CSA的参考点。
- 评审并在必要时撤回受监管机构处罚的公司的CoC合规证书。
- 如果CoC自评和/或第三方评估遵守标识被撤销，请通知EDPB和/或相关监管机构。

2.5 监督机构

为了确保和核实CSP持续遵守CoC要求的情况，CSA成立了一个内部委员会，负责积极有效地监督遵守CSP的数据保护做法。

监督机构采用CoC中规定的纠正措施和制裁规定。

本节介绍了内部委员会（监督机构）如何根据GDPR第41条、EDPB CoC指南和CNIL认证要求满足CompSA认证的要求。

采用分包的方式并不会导致职责下放：无论如何，监督机构仍对监管机构履行其任务负责，包括监督遵守CoC的情况。

CoC的CompSA（CNIL）已根据GDPR第41条的目的对监督机构进行了认证。

2.5.1 独立性

监督机构是CSA设立的内部机构，在职责上与CSA其他职能或部门分开。监督机构，包括其承包商，适当地独立于任何CSP（无论是否为CoC成员）、CSA和云计算部门内的其他职能或部门，以确保其监督职责在其认证期间的连续性。

独立性是通过以下方式实现的：

- 监督机构有自己的工作人员，并自主管理；
- 监督机构工作人员不得在CSA内承担其他职责或职能，这可能会与其在监督机构内执行的任务产生利益冲突；
- 监督机构有自己单独的¹⁷⁸个和充足的预算；
- 监督机构管理代表（MBMR）的任命、薪酬和免职须经董事会批准；
- 监督机构的成员不得因履行其任务而受到任何形式的解雇或处罚；
- MBMR直接（在职能上）向董事会报告并与董事会互动；
- 监督机构的活动不受CSA内部或外部的干扰。监督机构可以自由执行其任务，而不接受CSA的指示或在履行其任务时受到CSA的任何形式的制裁或干预（例如，监督机构可以自由决定投诉的管理、审计的执行及其范围、其工作规程和结果的传达，以及对CoC成员实施制裁）。

为了实现组织独立性，MBMR的职能是向董事会报告（如上所述）。董事会参与的工作包括：

- 批准有关监督机构的规则和规程及其任何修正案；
- 批准监督机构基于风险的年度（监督）计划；

¹⁷⁸ CSA有不同的收入来源，这些收入来源构成了其资金。为了确保MB的持续独立性和公正性，CSA承诺为MB分配适当的预算（由董事会根据年度预算和资源计划批准）。该预算与这些来自于CoC成员提交和交付的续签费等收入来源保持适当的独立。

- 核准监督机构的预算和资源计划；
- 接收MBMR关于实现其（监督）计划所述目标和活动的信息；
- 批准监督机构关于MBMR的任命、报酬、更换和/或解聘的决定。

监督机构在履行其任务和行使其权力时也独立于CoC成员。

监督机构负责持续评估其作为独立机构的地位，以便查明其在执行任务时独立性面临的任何潜在风险。如果发现其独立性面临的风险，且监督机构本身无法消除或驳回该风险，MBMR将向董事会报告该风险，并提出如何消除或将该风险降至最低的建议。MBMR应至少每年向董事会确认监督机构的组织独立性。

在CompSA要求或其他情况下，监督机构将提供其持续评估的结果，并将展示如何消除或最大限度地减少它可能发现的任何此类风险，以维护监督机构的独立性。

2.5.2 消除利益冲突

监督机构通过实施评审制度，以确保其活动不会导致利益冲突，并确保其不受外部或内部影响，无论是直接影响还是间接影响。

这些系统还用于记录和展示监督机构在防止任何与其任务和职责不相符的行为（例如，在对CoC成员违反CoC条款的行为实施制裁时给予CoC成员以不适当的宽大处理），并减轻监督机构内部产生的或与监督机构任何成员有关的利益冲突的风险。

如果发现监督机构的公正性面临风险，MBMR将向董事会报告该风险，并提及监督机构如何消除或降低此类风险。MBMR应至少每年向董事会确认监督机构的公正性。

监督机构及其成员必须保证，他们与CSP没有任何利害关系或地位，因为这可能会损害他们的判断或与他们的监督作用产生利益冲突。此外，监督机构及其成员不得采取任何与其任务和职责不符的行动。在执行任务和职责时，他们不得寻求或接受任何个人、组织或协会（包括CSA或任何CSP）的指示。

监督机构成员可以执行分配给监督机构的与他们以前曾向其提供咨询或其他服务的CSP有关的任务，只要这些服务的性质不损害其执行分配给监督机构的任务客观性。

在指派成员执行特定任务时，监督机构成员的个人客观性由MBMR管理。

监督机构成员必须避免评估或评审其以前负责的具体行动。如果该成员在上一年内负有此类职责，则推定其客观性降低。

在CompSA或董事会要求的情况下，监督机构需要出示其持续评估的结果，并展示如何消除或降低其可能已识别的此类风险，以保障监督机构的公正性。

监督机构的每个成员和为监督机构工作的每个第三方都签署了本策略声明。任何违反本策略的行为都将受到适当的纪律处分，或可能会负合同职责。

2.5.3 专业知识

CSA负责监督和保留与监督机构成员和代表监督机构开展（次要）活动的第三方和人员的培训和能力有关的记录。这是为了表明监督机构具备有效履行其职责所需的专门知识级别。MBMR执行这些保证活动，并向董事会报告其调查结果。

MBMR应至少每年向董事会确认监督机构所需的专门知识。

监督机构的成员和由监督机构签约代表其执行任务的任何第三方必须具备足够的知识和技能，以便能够适当地执行各自分配的任务。

监督机构在执行其任务时，总体上要求满足以下的最低标准：

- 对数据保护问题有深入的了解；
- 以CoC为主题的云计算行业和其他相关活动的专业知识；
- 在开展合规监测活动（如审计）方面有适当的业务经验和培训，该类经验和培训最好是在隐私和数据治理领域；
- 顺利完成CSA GDPR认证-主任审计员培训课程；
- 以合理审慎和尽职的方式执行任务所需的谨慎和技能；
- 人员应在最近三年内至少参加过两次从准备到最终结论的全面审计工作；
- 任何有法律背景的人员都必须：
 - 至少拥有法律领域的一年级硕士学位或同等法律学位；

- 在个人数据保护领域拥有至少两年的专业经验（如咨询、诉讼等）；
- 任何拥有技术背景的人员必须：
 - 至少拥有计算机科学、信息系统或网络安全领域的学士学位或同等学历；
 - 至少接受了为期两天的信息系统安全管理相关标准（如条例、标准、方法、最佳做法、风险管理）的培训课程；
 - 在信息系统安全领域有至少两年的工作经验。

当监督机构成员被指派处理特定投诉或监督过程或其部分管理时，必须同时满足上述要求。如果由于监督机构成员不足而无法做到这一点，MBMR有职责获得称职和足够的外部建议和/或支持，以满足这些要求。在没有这些要求的情况下，监督机构必须推迟这些活动，直到有可能遵守这些要求。

监督机构及其成员必须在履行任务和职责中表现出应有的专业谨慎，考虑到：

- 要执行的活动所需的工作范围；
- 主体的相对复杂性、重要性；
- 治理、风险管理和控制过程的充分性和有效性；
- 出现重大错误、欺诈或违规的可能性；
- 与潜在利益相关的担保成本。

监督机构成员必须经常努力不断提高其知识、技能和其他能力（例如，通过培训课程、会议和认证），以确保维持上述专门知识要求。监督机构的预算应足以满足这一要求。

组成监督机构的初始成员是由CSA根据他们的专业知识和以及缺乏与CSP相关利益或地位而选出的，这可能被认为与这一角色不相容。在此之后，监督机构将完全自主决定自己的组成，条件是没有任何成员在数据保护/信息安全问题上不具备必要的专门知识或可能处于利益冲突的地位上。但是，有关MBMR的任命、薪酬、更换和/或解聘的决定由监督机构作出，并需要得到董事会的批准。董事会的这些决定应记录在案，并予以证实。

2.5.4 资源和人员配置

必须向监督机构提供足够的资源和人员，使其能够以适当的方式履行其任务。这些资源必须与监督机构监督的CoC成员的预期数量和规模，以及这些CoC成员可能进行的个人数据处理活动的复杂性和风险程度相匹配。监督机构在与分包商签订的任何合同中都必须包括一项特定条款，以确保个人数据的机密性，在适用的情况下，可在监督任务期间向分包商披露这些个人数据。董事会负责确保这一点，并保存文件以证明上述规定得到遵守。

为了能够进行评估，MBMR向董事会提供所有必要的信息，包括基于风险的年度（监督）计划。

2.5.5 既定的规程和结构

已经建立了适当的治理结构和规程，充分评估CSP签署和遵守CoC的资格。还有适当的治理结构和规程，以确保CoC成员能够遵守CoC的规定，并监督其对规定的遵守情况。资格评估（第2.5.6节）、投诉处理（第2.5.7节）中概述了这些规程，以及下面的监控部分（第2.5.12节）。

在执行任何任务时，监督机构必须确保CSP提供的所有相关文件（包括审计证据）和监督机构出具的所有相关文件（例如，审计计划、审计结果和报告）都处于严格保密的条件——监督机构不应在其任务范围之外披露此类文件或其中的信息，除非这是履行其在本准则下的义务所必需的，或者是履行监督机构或CSA的适用法律义务所必需的。

一旦执行其任务或出于任何其他合法目的不再需要此类文件（包括可能需要进一步保留以履行对监督机构或CSA的法律义务，或为允许CSA建立、行使或抗辩与监督机构任务相关的任何法律索赔或监督机构的调查所必需的情况），这些文件应被明确和安全地销毁。

2.5.6 资格评估

根据GDPR第41条第（2）款（b）项的要求，监督机构通过制定适用CoC的规程，允许对有关CSP进行强制性资格评估。适用以下工作过程：

- 监督机构将收到CSP提交的关于特定服务的CoC遵守申请。如上所述，这些可

能是自评估申请（上文1.2.1.节）或第三方评估申请（上文1.2.2.节）。

- 自评估：监督机构将检查CSP在其申请中做出的所有声明，以确保声明充分涉及CoC的控制，并决定是否批准。如果获得批准，监督机构将为CSP的服务颁发自评估合规证书（之后CSP将有权声明该服务遵守CoC）。在这样做时，监督机构可以利用外部律师；无论如何，监督机构将保留最终决定是否批准加入的职责。
- 第三方评估：监督机构将依靠合格的CoC审计伙伴对申请人CSP的服务进行的评估和描述的结论-监督机构将只执行正式检查，以确保结论充分涉及CoC的所有控制措施，如果是，则授予CSP服务的第三方评估合规证书（之后CSP将有权宣布该服务符合CoC）；因为监督机构最终将保留决定是否遵守CoC的职责。应该强调的是，监督机构将通过准则委员会正在进行的监督机制，以及通过投诉管理规程，在准予遵守准则委员会之后，对准则委员会的做法进行更实质性的评估。

在任何一种情况下，如下文进一步说明的那样，监督机构将根据CoC投诉管理（下文第2.5.7节和附件7）和持续监督规程（下文第2.5.12节和附件8）中规定的标准，对遵守CSP进行有针对性的审计。

为免生疑问，CSP在监督机构授予该服务的遵守标识之前不得宣布服务遵守CoC（只有在监督机构成功进行资格评估后才能这样做）。

2.5.7 透明的投诉处理

如果CoC成员违反CoC条款，特别是维持与CoC成员在申请CoC合规证书时所陈述不一致的做法（无论是在自评估或第三方评估的框架下），监督机构将立即采取其认为适当的纠正措施来解决这种情况。如果出现与合格的CoC审计合作伙伴有关的任何相关问题，监督机构将对此进行调查，并针对每个案例采取认为适当的纠正措施。

尤其是，监督机构可能会因云用户、数据主体或其他CSP提交的投诉而发现侵权行为，同时对遵守CSP或合格的CoC审计合作伙伴采取行动。

如果收到此类投诉，监督机构将对其进行调查。如果对投诉的调查得出结论认为CoC成员违反了CoC的一项或多项规定，则监督机构将采取其认为适当的立即纠正措施来处理这种情况。所采取的措施应旨在制止侵权行为，并防止今后再次发生相同或类似的侵权行为。此类补救行动和制裁见附件7。

监管机构可公布这些措施，特别是在存在严重违反CoC规定的情况下。

如有需要，监管机构应将所采取的措施及其理由通知CSA、CoC成员、CompSA和所有其他相关SA，不得无故拖延。

监管机构将在MBMR的监督下定期生成报告，以记录投诉的调查结果，并至少生成一份年度报告，涵盖该年度开展的所有与投诉有关的活动。本年度报告将在相关情况下与董事会、CompSA和其他相关的SA共享，并将在CSA的网站上发布。

更多细节详见于CoC的附件7。

2.5.8 与主管监管机构的沟通

监管机构框架允许将监管机构采取的任何行动有效地传达给CompSA和其他有关CoC的监管机构。

监管机构每年至少向CompSA报告一次。其报告至少包括以下主题：

- 已开展的审计情况；
- 特定的重要评审或审计结果；
- 已开展的投诉管理活动；
- 关于CoC成员违反CoC的情况下采取的行动的决定的决定（包括采取行动的正当理由）；
- CoC成员的任何相关变更；
- 监管机构的未来议程以及有关其运作的任何其他相关信息；
- 可能与CoC的解释和/或运作相关的技术、法律或其他发展。

此外，监管机构应以书面形式迅速、直接地与CompSA进行沟通：

- 由于未能正确遵守CoC的要求（包括采取纠正措施的理由）而决定暂停或撤销授予CSP的合规证书的任何具体情况；
- 监管机构（特别是其结构和/或组织）的任何重大变动，可能使其独立性或专门知识受到质疑，或可能在监管机构或其任何成员内部造成利益冲突。

此外，监管机构应迅速与CompSA合作，并提供与CoC及其活动有关的任何必

要信息，以确保CompSA的作用不受损害或阻碍。

2.5.9 评审机制

应建立适当的评审机制，以确保CoC保持相关性，并继续为GDPR的正确实施做出贡献。PLA工作组设立并执行评审机制，以适应法律适用和解释方面的任何变更，或可能对委员会成员进行的个人数据处理产生影响的新技术发展的发生。

此外，所有CSA服务和过程都采用了¹⁷⁹定期评审的过程，以确定可能的改进机会。

所有变更都将通过CSA管理委员会进行变更管理。

关于监督机构的规则和规程的改变可由MBMR向董事会提出的倡议发起。

对CoC的修订将考虑来自监督机构活动的反馈，包括对CSP和合格CoC审计合作伙伴进行的审计结果、从监管机构、云用户、CSP和数据主体收到的反馈、投诉和所有其他相关信息。

2.5.10 法律地位

作为一个内部机构，监督机构不具有独立的法律地位，根据GDPR第83条第（4）款，监督机构对其履行任务和职责负有职责。因此，CSA将对任何违反GDPR第41条（4）款规定的监督机构义务的行为承担全部职责。

在欧盟内部，CSA在芬兰和希腊设立了作为法人实体的办事处—因此，作为一个内部机构，该监督机构可以被认为是在欧盟内部建立。

2.5.11 持续改进

MBMR针对监督机构的所有任务制定并维护质量保证和改进计划。通过监督机构进行的定期评审，不断提高监督机构和监督过程的效力，评审范围包括投诉处理、监督和其他规程，以及监督机构的治理结构。这些评审在MBMR的监督下进行，将考虑对CSP和合格的CoC审计合作伙伴进行的审计结果、从监管机构、云用户、CSP和数据主体收到的反馈、投诉和所有其他相关信息。

¹⁷⁹ 每年至少一次，但根据法律和行业形势，可能会更频繁。

任何CoC利益相关者，包括CoC成员和工作人员，都可以向监督机构提交改进建议。且改进行动将作为这些定期审计的结果进行评估和记录。

这种评审必须每年至少举行一次；在MB认为有必要时可以触发特别评审。MBMR向董事会报告这些评审的结果。

2.5.12 监督

监督过程分为两个部分。一个是投诉管理（见上文2.5.7.节、3.4节和附件7），另一个是监督机构积极监督的职责。监督机构制定了一套过程，允许对CSP进行随机抽查，以便每年对CSP在遵守CoC时所证明的过程的遵从性和有效性进行审计。一旦发现违规行为，将遵循制裁过程。

此外，还有一个过程可以对合格的CoC审计合作伙伴提供的报告和第三方评估进行抽样，并确保其遵守CoC对其施加的要求。一旦发现违规行为，监督机构将采取任何认为适当的纠正措施。当监督机构根据CoC实施纠正措施或发布制裁时，监督机构应确保守则成员的权利得到尊重。

关键过程的评审是通过审计或特殊情况下进行的。该评审用于识别和消除潜在的不合格。

监督机构通过确保遵守CoC的规程来监督CoC成员，并通过确保遵守CoC的相关要求的规程来监督合格的CoC审计合作伙伴。如果发现CoC成员的行为违反CoC的规定，监督机构有权立即采取纠正措施，这甚至可能导致暂停CoC或将其排除在CoC之外（见上文第2.5.7节）。此外，监督机构有权向委员会报告任何调查结果，如果通过监督机构的评审发现合格的CoC审计合作伙伴不符合CoC对其资格的要求或相关的认证标准（即ISO 17065），委员会可采取行动暂停或排除合格的CoC审计伙伴进行第三方评估。

监督机构和董事会在正式会议上定期评审所有报告，并应评估采取行动防止未来不合格或进行变更的必要性。

更多详情见CoC附件8。

2.5.13 个人数据保护

为了确保整个组织和其运营的各个司法管辖区始终保持高级别的个人数据保护，

CSA实施了一套内部策略、规程、指南、模板和其他工具来规范其内部的个人数据处理活动-CSA组织数据保护合规框架（CSA G-DPCF）。

鉴于GDPR所确立的保护个人数据的标准是全球个人数据保护的最高标准之一，加上GDPR所确定的原则已获国际认可，委员会已选择将GSA G-DPCF的组成部分与GDPR的要求和义务协调一致，甚至扩大GDPR的适用范围。

作为CSA内的一个内部委员会，监督机构在处理与其活动相关的个人数据时，必须遵守CSA G-DPCF数据保护合规框架。这使得监督机构能够确保其在执行监督任务时以符合GDPR的方式处理个人数据。

特别是，正如CSA关于处理者参与的内部指南中所述，监督机构（或代表监督机构的CSA）必须与受雇协助执行监督机构任务的任何分包商签订书面协议，其内容与GDPR第28条保持一致。

3. 治理过程和相关活动

CoC的治理过程定义了治理工作组之间的关系以及他们需要遵守的一系列活动，以便为每个技术部分保持一致的管理过程。

3.1 控制指南：PLA 的评审过程

应定期对“控制指南：PLA”进行评审，因为它受到欧盟个人数据保护相关法律框架变更的影响。“控制指南：PLA”的评审过程属于PLA工作组的职责范围。CSA承诺，通过PLA工作组，在“控制指南：PLA”中及时反映任何相关的立法变更，并及时通知加入的云服务商遵守这些变更。

“控制指南：PLA”的评审过程可由CSA社区的任何成员（志愿者、企业会员、PLA工作组成员等）根据调整该规范的需要而启动以符合最新的相关立法。

任何更新PLA [v3]的请求都应由PLA工作组成员评估和决定（参考下文附件5的PLA章程）。

CSA和PLA工作组成员将确保及时更新“控制指南：PLA”，以降低组织遵守不完整要求的潜在风险。因此，尽管有立法变更或CSA社区成员要求启动的评审条款，CSA承诺评审“控制指南：PLA”。通过PLA工作组，从前一次评审开始，至少每十二（12）个月评审一次。

应将“控制指南：PLA”中的任何变更以及需要组织内部做出的必要调整通知采纳该规范的云服务商，以便其在实践中遵守这些规定。根据对“控制指南：PLA”所做修改的影响，云服务商被要求在此时间段内实施这些调整。PLA—微小的变更为三十（30）天，相关变更为六十（60）天，重大变更为九十（90）天。

对“控制指南：PLA”的修改可能会增加监督机构进行评审和监督CoC的履行所需的时间、精力、资源，可能会导致向云服务商收取的提交费用增加。

根据通用数据保护条例（GDPR）第40条将“控制指南：PLA”作为认可的CoC后所产生的任何变更，将通知主管监督机构。监督机构通过监督过程（附件8）监督PLA工作组决定的修改的应用情况。

目前版本的“控制指南：PLA”既关注之前（数据保护指令及其在欧盟成员国）的实施，也关注当下欧盟关于保护个人数据的相关立法（GDPR）。

PLA工作组的章程还包括扩展“控制指南：PLA”现有的地理范围。PLA工作组还预计开发一个CoC，解决全球层面的隐私/数据保护要求。

3.2 CoC 遵守机制的评审过程

开放认证框架（OCF）工作组负责启动CoC遵守机制的评审，以及评估和批准评审请求，实施提议的变更。

开放认证框架工作组成员有权对CSA“安全、信任、保障和风险（STAR）”项目中的认证方案以及CoC遵守机制提出修改建议。

3.3 CoC 认证标识的颁发和遵守声明的发布

监督机构负责评审、批准和管理基于CoC的自评材料 and 第三方认证标识的发放、遵守声明的提交过程以及相关投诉。具体如下：

3.3.1 CoC 的自评材料

监督机构负责评审任何第一方提交的证明材料和第三方提交的相关投诉。针对前者，监督机构应核实材料已满足最低要求。针对后者，监督机构应核实投诉的有效性，并根据PLA工作组的意见，采取相关行动。

在核实后，CSA应确保CoC自评估材料通过线上的CSA STAR注册中心发布。

如果不满足最低要求，或如果投诉被认为是有效的，监督机构将采取以下行动之一：a) 要求修正CoC的自评估，或b) 撤销CSA STAR注册中心的自评估并吊销认证标识。

3.3.2 CoC 第三方评估

CSA负责在收到监督机构（基于从有资质的CoC审计方收到的信息）被审计方通过审计的通知后，在STAR注册中心公布CoC第三方评估结果。

如果收到相关投诉，监督机构负责通知提交评估结果的审计方。在这种情况下，审计方应核实投诉的有效性并向监督机构提供反馈。

如果投诉被认为是有效的，监督机构应暂停或吊销标识的颁发。相应地，CSA应从其STAR注册中心撤销评估结果。

3.4 投诉管理过程

投诉管理过程规定了监督机构将如何接收、管理和处理收到的与CSA CoC自评估和第三方评估机制有关的投诉。

关于监督机构遵循的投诉管理过程的详细说明，请参考附件7。

3.5 持续监督过程

除处理投诉管理过程外（见上文第3.4节和附件7），监督机构还负责积极监督CoC的遵守情况。通过在年度审计期间对遵守CoC的云服务商进行抽查来实现，以评估其对提交的CoC条款的遵守情况，在此基础上颁发CoC遵守标识。任何被发现的违规行为将触发相应的处罚过程。

关于监督机构对成为CoC成员的云服务商的持续监督过程的详细描述，请参考附件8。

3.5.1 有资质的 CoC 审计方的持续监督过程

考虑到上述第1.2.2节中的要求和ISO 17065的条款，监督机构还必须每年对有资质的CoC审计方进行监督和评估。所有有资质的CoC审计方必须在三年内至少接受一次审计。

这些工作必须遵守以下条款：

- 审计可以在现场或远程进行，这取决于审计的范围。
- 审计将以随机抽样的方式对有资质的CoC审计方进行审计，其条件与上文所述相同（上文第2.5.12节），并进行必要的调整。
- 必须对有资质的CoC审计方进行持续监督，包括每两年至少进行一次现场或远程的更新认证检查，以及每两年进行一次见证审计或复核审计。
- 见证审计必须定期在一个有代表性的地点进行，以验证CoC和ISO 17065条款下的适当交付。
- 对于有资质的CoC审计方，只要至少有一次年度认证检查，评审以下文件，就可以在同一年内进行认证检查、见证审计或复核审计。
 - 该审计方的管理体系。
 - 该审计方负责协助云服务商提交第三方评估的人员专业知识和能力(如上文第1.2.2节所示)。
 - 该审计方对寻求申请第三方评估的云服务商进行评估的过程。
 - 该审计方用于跟踪和报告他们在CoC下评估云服务商的记录和规程。

这些审计的结果将报告给CSA。监督机构保留根据审计结果暂停、撤销或终止对合格CoC审计方的认证权利—特别是当这些实体未能适当实施监督机构对其要求的任何纠正措施时。

3.6 道德准则评审过程

道德准则每年由董事会评审和更新。对道德准则声明的任何修改都应通报给CSA所有相关方。

3.7 PLA 和开放认证框架工作组章程文件评审过程

CSA负责审批任何对开放认证框架工作组和PLA工作组章程进行修订和延期的请求。



附录 1：隐私级别协议[v4]模板

由于该模板内容较多，以Excel格式编写，不便于在Word/PDF中阅读，请参考文件CoC GDPR_Annex 1_Compliance_Assessment_Template

附录 2：遵守声明模板



CSA CoC (CoC) :

遵守声明

自评估

1. 名称和URL/地址

名称	
URL/地址	

2. PLA CoC (CoP) 所涵盖的服务

请提供一份列表，列出“控制指南：PLA”所涵盖的服务名称。

服务1名称	
服务2名称	
.....	
服务n名称	

3. 采取的机制

自评估	
-----	--

4. 适用范围

请提供（2）中所列每项服务的评估范围与“控制指南：PLA”的描述

说明	
----	--

5. 使用的“控制指南：PLA”版本

版本编号	（例如：v.3.2）
------	------------

6. 发证/到期日期

发证日期	
到期日期	

7. 法定代表人/DPO签署人

通过签署本遵守声明，该组织/公司确认：

- a) 截至当日，（2）中所列的服务遵守CSA CoC要求（见CSA CoC第3.3节，“CoC遵守标识的签发和遵守声明出版物”）。
- b) CSA CoC自评估遵守标识自签发之日起有效期为12个月，并应在此期限后进行更新。此外，每次在公司的相关策略或做法发生变更时，CSA CoC自评估必须进行修订。

姓名	
----	--

职务	
日期	



© 2013-2020 CSA—版权所有

云安全联盟（CSA）欧洲通用数据保护条例（GDPR）合规行为准则（CoC）及其附件，例如：附件1：PLA模板，附件2：遵守声明模板（统称为“CSA GDPR 合规行为准则”）由CSA根据知识共享署名-非商业性使用-禁止演绎4.0国际许可协议（CC-BY-NC-ND 4.0）授权。

分享

您可以通过任何媒介或任何形式分享和分发CSA GDPR合规行为准则。

署名

您必须提及CSA，并链接到位于<https://gdpr.cloudsecurityalliance.org/>的CSA GDPR网页。您不得暗示CSA认可您或您的使用。

非商业性使用

您不得使用、共享或重新分发PLA CoC以获得商业收益或金钱补偿。

禁止演绎

如果你对CSA GDPR合规行为准则本创作进行了重混、转换、依据本创作进行再创作等行为，你不得再次公开传播经过修改的创作。

不得增加额外限制

您不得运用法律条款或技术措施，来限制他人实施本许可证允许的任何行为。

商业许可

如果您出于商业营收的目的，希望调整、转换、构建或分发CSA GDPR合规行为准则的副本，您必须首先获得相应的CSA的许可。请联系我们info@cloudsecurityalliance.org。

声明

所有在CSA GDPR合规行为准则上出现的商标、版权或其他声明必须同时被复制，不得删除。



CSA CoC (CoC) :

遵守声明

第三方评估

1. 名称和URL/地址

名称	
URL/地址	

2. PLA CoC (CoP) 所涵盖的服务

请提供一份列表，列出“控制指南：PLA”所涵盖的服务名称。

服务1名称	
服务2名称	
.....	
服务n名称	

3. 采取的机制

第三方评估	
-------	--

4. 适用范围

请提供（2）中所列每项服务的评估范围与“控制指南：PLA”的描述

说明	
----	--

5. 使用的“控制指南：PLA”版本

版本编号	(例如: v.3.2)
------	-------------

6. 评估机构

名称	
----	--

7. 发证国家

名称	
----	--

8. 标识编号

编号	
----	--

9. 发证/到期日期

发证日期	
到期日期	

10. 法定代表人/DPO签署人

通过签署本遵守声明，该组织/公司确认：。

- a) 截至当日，(2)中所列的服务遵守CSA CoC要求（见CSA CoC第3.3节，“CoC遵守标识的签发和遵守声明出版物”）。
- b) 第三方评估遵从性标识自签发之日起有效期为12个月，并应在此期限后进行更新。此外，每次在公司的相关策略或做法发生变更时，第三方评估必须进行修订。

姓名	
职务	
日期	



© 2013-2020 CSA—版权所有

云安全联盟（CSA）欧洲通用数据保护条例（GDPR）合规行为准则（CoC）及其附件，例如：附件1：PLA模板，附件2：遵守声明模板（统称为“CSA GDPR 合规行为准则”）由CSA根据知识共享署名-非商业性使用-禁止演绎4.0国际许可协议（CC-BY-NC-ND 4.0）授权。

分享

您可以通过任何媒介或任何形式分享和分发CSA GDPR合规行为准则。

署名

您必须提及CSA，并链接到位于<https://gdpr.cloudsecurityalliance.org/>的CSA GDPR网页。您不得暗示CSA认可您或您的使用。

非商业性使用

您不得使用、共享或重新分发PLA CoC以获得商业收益或金钱补偿。

禁止演绎

如果你对CSA GDPR合规行为准则本创作进行了重混、转换、依据本创作进行再创作等行为，你不得再次公开传播经过修改的创作。

不得增加额外限制

您不得运用法律条款或技术措施，来限制他人实施本许可证允许的任何行为。

商业许可

如果您出于商业营收的目的，希望调整、转换、构建或分发CSA GDPR合规行为准则的副本，您必须首先获得相应的CSA的许可。请联系我们info@cloudsecurityalliance.org。

声明

所有在CSA GDPR合规行为准则上出现的商标、版权或其他声明必须同时被复制，不得删除。

附录 3：CSA STAR 计划和开放认证框架 (OCF)

CSA于2011年推出了“安全、信任、保障和风险 (STAR)”项目，目的是通过提供更高的透明度和信息安全保障来提高云市场的信任度。

CSA STAR为云计算利益相关者，如云服务客户 (CSC)、CSP (CSPs)、云服务审计者等提供了一个公共知识库，CSPs可以在公共知识库中发布基于CSA最佳实践，即云控制矩阵 (CCM) 和云安全共识评估标准 (CAI) 的内部尽职调查结果。

为了开发支持CSA STAR所需的技术能力，CSA开放式认证框架 (OCF) 工作组于2012年成立。

OCF工作组的任务是定义CSA安全认证框架及框架中包含的认证机制。

工作组将开放认证框架定义为三个信任等级：

- 一级，自评估：STAR自评估
- 二级，第三方评估：STAR认证、STAR证明和C-STAR评估
- 三级，持续监督/审计：STAR持续认证

开放认证框架

	审计频率	安全	隐私	
审计类型	●●●○	STAR三级	持续审计	-
	●●●○	STAR二级	二级+持续自评估	-
		STAR二级	第三方认证	GDPR CoC认证
	●○○○	STAR一级 持续监测	持续自评估	-
		STAR一级	自评估	GDPR CoC自评估

↑ 透明与保障

2012年，启动了CSA STAR项目，以支持CSA STAR的工作及管理OCF的实施。目前，STAR项目提供自评估（一级）和第三方评估认证/证明（二级）。持续监督/审计的认证正在开发之中。

OCF各等级之间的关系如下：

- 从“保障”的角度来看，OCF一级提供良好至中等级别的保障，OCF二级提供高级别保障，OCF三级提供更高级别保障。
- 从“透明度”的角度来看，OCF一级提供良好的透明度，OCF二级提供低至高的透明度，OCF三级提供更高的透明度。



注意，OCF三个等级所提供的透明度并非与三个保障级别对应。例如，OCF一级能提供比OCF二级更好的透明度，因为STAR认证和STAR证明都不要求组织公开其安全控制状况。

CSA鼓励想要获得OCF二级认证的组织首先进行OCF一级的自评估。

附录 4：道德准则

1. 范围

本道德准则适用于CSA（“CSA相关方”）的所有董事会成员、管理人员、全职和兼职员工、合作者或志愿者。

2. 定义

董事会成员：CSA董事会的在职人员。

CSA相关方：CSA的董事会成员、管理人员、全职或兼职员工、承包商或志愿者。

志愿者：花费大量时间以推进CSA董事会的使命或向董事会的咨询委员会提供服务的个人。

3. 道德原则

CSA成员，凭借其在CSA中的角色和职责，在更大的社会范围内代表CSA。他们有特别的义务遵守个人和职业行为的最高标准。

CSA要求所有CSA成员遵守以下道德原则：

- 我们的言行体现了对真理、公平、自由探索和他人意见的尊重。
- 我们尊重所有人，不分种族、肤色、性别、性取向、婚姻状况、信仰、种族或民族身份、残障或年龄。
- 我们维护他人的专业声誉，并为其提出的想法、文字或图像给予赞誉。
- 我们维护隐私权和机密信息。
- 我们不会为了私利给予或接受好处。
- 我们不会为了招揽或者接受利益而损害更高的公共利益。

- 我们避免实际或明显的利益冲突，如有疑问，应寻求有关当局的指导。
- 我们遵守CSA所要遵守的法律法规和精神。
- 我们积极鼓励各界同仁与我们一起支持这些法律法规和本道德声明中的行为标准。

4. 评审和确认道德准则声明

本道德准则生效后，以及此后每年的1月最后一天之前，应向每个CSA成员提供本准则的副本并要求复审，并书面确认其已阅读、理解并同意遵守本道德准则。

5. 生效和实施

本道德声明已获得CSA董事会的批准。本道德声明将于2012年1月1日生效。董事会指示CSA执行董事确保将本道德声明提供给所有CSA相关方并得到其认可。

6. 监督

董事会应直接负责监督本道德声明，并制定规程以支持本道德声明。

7. 评审和修改

本道德声明每年由董事会进行评审并在必要时进行更新。对道德声明的任何修改都应通知所有CSA成员。

附录 5：隐私级别协议工作组章程



隐私级别协议工作组
章程 2017

执行概览

数据保护合规正变得越来越基于风险¹。数据控制者和处理者有职责确定并在其组织中实施对所处理个人数据的适当保护级别。在作出这种决定时，他们必须考虑到各种因素，如技术发展，实施成本，数据处理的性质、范围、背景和目的，以及对自然人的权利和自由造成的不同可能性和严重性的风险²。因此，云服务供应商（CSPs）将负责确定他们所处理的个人数据所需的保护级别

在这种情况下，隐私级别协议（PLA）CoC为法律合规和CSP提供的数据保护级别透明度提供了指导。

隐私级别协议（PLAs）为了提供：

- 为任何规模的云客户提供工具，以评估不同CSP所提供的个人数据保护级别（从而支持知情决定）³。
- 指导任何规模和地理位置的云服务供应商遵守欧盟（EU）的个人数据保护立法，并以结构化的方式披露他们向客户提供的个人数据保护级别。

PLA CoC旨在通过利用PLA [v2]的结构，同时满足实际的、强制性的欧盟法律个人数据保护要求（即95/46/EC指令及其在欧盟成员国的实施），以及即将出台的GDPR的要求。这一具体特点使PLA [v3]成为一个独特的工具，帮助CSP、云客户和潜在客户实现新旧欧盟数据保护制度的过渡，并有助于将GDPR正确应用于云计算行业。PLA [v3]规定了GDPR在云环境中的应用，主要涉及到以下几类要求：

- 公平和透明地处理个人数据；
- 向公众和数据主体提供的信息（根据GDPR第4条第1款的定义）；
- 数据主体行使权利；

¹ 见GDPR的序言83和第25、32、33、34和35条。

² 见GDPR的第24、25、32、35和39条。

³ “所有在欧洲经济区（EEA）提供服务的云供应商应向云客户提供所有必要的信息，以便正确地评估采用这种服务的利弊。安全性、透明度和客户的法律确定性应该是提供云计算服务背后的主要驱动力”。WP29云计算意见，第2页；“依赖云计算安排的前提条件是控制者[云客户]进行充分的风险评估工作，包括处理数据的服务器位置以及从数据保护的角度考虑风险和利益。”第4页，同上。

- GDPR第24条和第25条所述的方法和规程以及GDPR第32条所述的确保安全处理的方法；
- 将个人数据违规情况通知给监管机构（GDPR第4条21款的规定）和数据主体；
- 向第三国传输个人数据。

此外，PLA [v3]包含一些机制，使GDPR第41条第1款中提到的监管机构能够对承诺采纳CoC的数据控制者或处理者遵守其规定的情况进行强制性监督，但不违背监管机构根据GDPR第55或56条规定的职责和权力。

背景

云安全联盟（CSA）于2013年发布了“欧盟云服务销售的PLA大纲”（PLA [第1版]），并于2015年发布了“PLA [v2]：欧盟云服务合规工具（PLA [v2]）”。

基于已有文件，即PLA [v1]和PLA [v2]，CSA PLA工作组将开发“PLA [v3] CoC：欧盟云服务合规工具”（PLA [v3]），以应对欧盟和欧洲经济区成员国的数据保护法即将对GDPR（欧盟条例2016/679，又称GDPR）做出的修改。⁴

实际使用

PLA CoC旨在作为创建云服务协议附录的结构，该附录将描述云服务商承诺提供和维护的隐私和数据保护级别，涉及其客户将提供给云服务商并通过云服务商服务处理的个人数据。

客户将向云服务商提供个人数据并通过云服务商的服务进行处理。

PLA CoC为云服务商提供了一个结构，使其能够将根据PLA CoC [v3]制定的完整的隐私声明在将作为保管人的CSA STAR服务机构登记。

在全球范围内采用PLA CoC可以促进一个强大的全球行业标准，加强协调性，并促进遵守适用的欧盟数据保护法。

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

工作小组的范围和目标

该工作组被授权在全球范围内研究云计算服务的隐私和数据保护合规，并将遵守以下目标：

目标1： 根据PLA [v2]的经验，定义一个PLA的实践准则，以满足GDPR的要求。

目标2： 定义治理结构和遵守PLA CoC的机制。

目标3： 参与PLA CoC的实施和长期管理。

目标4： 监视法律法规的发展，以便能够更新PLA实践准则。

目标5： 当有关于PLA自评估和第三方认证的投诉时，向CSA提供专家意见。

目标6： 向CSA开放认证工作组提供关于PLA CoC第三方认证方案的专业意见。

工作组的结构和职能

联合主席

除了选定的领导之外，工作组将由联合主席领导。联合主席将协助工作组的领导职责。联合主席可指定其他人，以确保有效地执行已定义的研究工作。

子项目组

由领域专家组成的特设工作组，可以计划或执行任何相关的外联、宣传或研究机会。这些工作组应直接向PLA工作组报告。

工作组允许云社区和其他CSA工作组之间的资源共享，以协助及时完成项目、计划和其他需要帮助的活动，支持工作组定义的工作主体。

会员

任何具有适当专业知识的个人都可以参与工作组的的活动。下表提供了CSA鼓励加入PLA工作组的组织的例子

社区	目的	示例
国际/区域/国家监管机构、机关、监管部门和协会	能够确保与法律法规要求一致的策略制定者和监管机构	<ul style="list-style-type: none"> • 欧盟委员会（EC） • 欧洲数据保护委员会（EDPB） • 欧洲数据保护监督署（EDPS） • 各国监管机构（SA） • 欧盟网络安全局（ENISA） • METI • IDB—IDA • 美国联邦贸易委员会 • 等其他机构
CSA开放认证框架联合主席	保持与开放认证框架的一致性，评估在开放认证框架中引入隐私模块/标识的可行性。	<ul style="list-style-type: none"> • 开放认证框架联合主席
CSAGRC Stack工作组联合主席	与GRC Stack研究举措保持一致	<ul style="list-style-type: none"> • 云控制矩阵（CCM） • 共识评估倡议（CAI） • 云审计 • 云信任协定（CTP）
CSA 国际标准化委员会	与ISC工作保持一致	<ul style="list-style-type: none"> • ISC联合主席
内审员/顾问	来自提供内部审计服务和咨询的组织代表	<ul style="list-style-type: none"> • 四大（普华永道，安永，德勤，毕马威） • 小型审计和咨询公司的代表

社区	目的	示例
其他研究工作	来自正在进行的具有相似范围研究项目的代表，以保持项目之间的协调和一致。	<ul style="list-style-type: none"> • A4Cloud • Internet2
CSA企业会员（云服务商）	来自云服务/解决方案提供商的代表，验证PLA4EU的适用性，合规和引入隐私认证的可行性	
独立领域专家	独立领域专家	<ul style="list-style-type: none"> • 欧洲隐私协会（EPA） • 国际隐私专业协会（IAPP）
云用户/消费者	来自企业云供应商的代表和/或用户/消费者组织的代表，以确保与用户要求和需求相一致	<ul style="list-style-type: none"> • 欧洲CIO协会（EuroCIO） • 等其他机构

与其他工作组的配合

本工作组将与CSA其他工作组、咨询小组和行业伙伴（如SDO）分享研究成果并保持一致。

业务

咨询

PLA工作组将接受CSA行业专家（SME）咨询委员会、国际标准化委员会（ISC）和CSA执行团队的建议，以确保工作组的研究在CSA的范围内，并与其他行业伙伴的研究相一致。该研究将保持行业的独特性，并引用任何冗余或重复的工作。

研究周期

PLA工作组将遵循CSA在所有项目和倡议中采用的研究周期。

同行评审

PLA工作组将寻求CSA的帮助，联系同行来评审我们的章程、出版物和工作组的其他文档化的活动。

沟通方法

基础设施和资源要求

PLA工作组将由CSA志愿者组成；设立联合主席和/或委员会。该工作组需要项目管理、在线工作空间和技术性写作协助。

工作组会议

PLA工作组将定期举行电话会议。负责人或其委托人必须出席或参与在线工作空间。如果负责人缺席，委托人必须有充分的授权代表负责人行事。线下会议将在选定的地点举行。

决策规程

决策应由PLA工作组中多数成员（包括联合主席）的意见决定。

多数的定义

1. 多数应包括一半以上的成员亲自或通过电话参与并投票。
2. 在计算多数时，所有投赞成票、反对票或弃权票的成员都应被计入。
3. 如果票数相同，提案或修正案应视为被否决。
4. 就本章程而言，“出席并参加表决的成员”是指对某项提案投赞成、反对或弃权的成员，包括委托人。委托人应通过书面或不可抵赖的电子邮件获得授权，并将在投票开始前由联合主席检验和宣布委托人授权的合法性。

过半数弃权

当弃权票数超过总投票数（赞成、反对、弃权）的一半时，对所讨论事项的审议应推迟到以后的会议，届时应进一步讨论该事项，评审和修正任何文件或决定，并将修正后的提案再次提交工作组进行表决。

表决规程

表决规程如下：

1. 通过向联合主席发送电子邮件，除非要求进行无记名投票。
2. 投票要求采用无记名方式（网上投票也适用），如果有超过20%出席且有权投票的成员参与，则通过邮寄给受信任的第三方进行无记名投票。

在开始投票之前，主席应评审任何关于投票方式的请求，然后正式宣布适用的投票规程和提交表决的问题。然后，主席应宣布投票开始，并在投票结束后宣布投票结果。

如果是无记名投票，秘书处应立即采取措施，确保投票的保密性。

可交付成果的批准和认可过程：

PLA工作组的交付物须经CSA批准和认可。审批和认可决定基于专家咨询委员会的建议。

交付物

1. PLA CoC的目标、范围、方法、假设和解释性说明
2. PLA [v3]实践准则
3. PLA CoC治理和遵守机制
4. PLA模板
5. PLA声明模板
6. 演示文稿和其他宣传材料

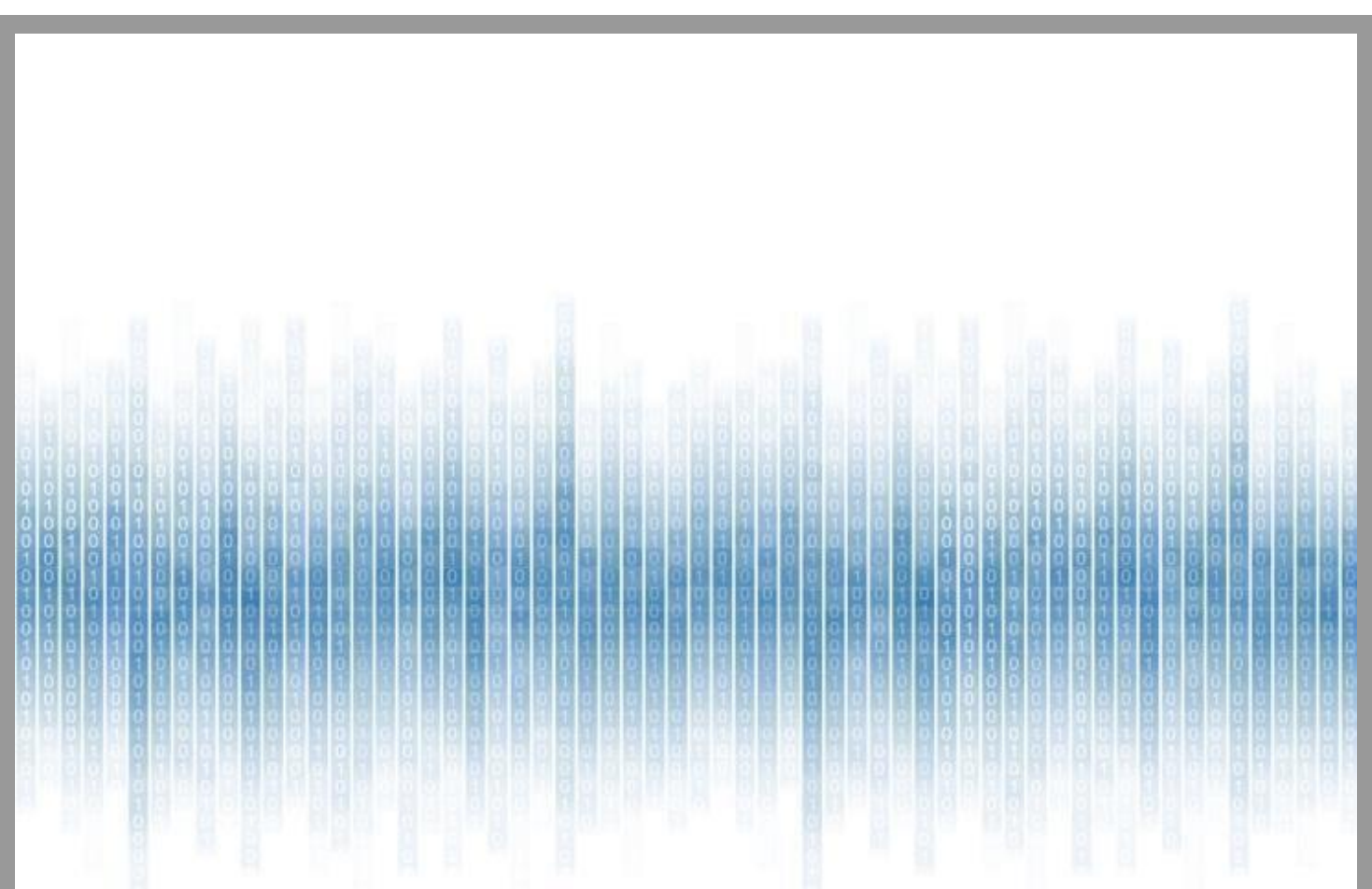
7. 投诉管理规程
8. PLA CoC变更过程

有效期限

本章程的有效有效期至2019年3月31日。



附录 6：开放认证框架工作组章程



开放式认证框架 工作组

章程

2019

目录

工作组执行概览.....	3
使命.....	3
工作组的范围和职责.....	3
工作组成员.....	3
工作组结构.....	4
联合主席.....	4
委员会.....	5
下属工作组.....	5
与其他工作组的配合.....	5
业务.....	6
咨询.....	6
研究周期.....	6
同行评审.....	6
沟通方法.....	7
基础设施和资源要求.....	7
工作组的电话会议和现场会议.....	7
决策规程.....	7
A. 多数的定义.....	7
B. 过半数弃权.....	7
C. 表决规程.....	7
交付物/活动.....	8
有效期限.....	8

工作组执行概览

使命

开放认证框架工作组的任务是开发、维护、评审、更新、支持CSA安全“安全、信任、保障和风险”项目（STAR）计划中包含的所有认证和证明计划的开发和部署。开放认证框架工作组专注于云计算和移动领域的过程和产品的信息安全和隐私认证方案。

工作组的范围和职责

CSA发现在IT生态系统中存在一些缺陷，阻碍着安全可靠的云服务在市场中的应用。消费者缺乏简单的、经济高效的方式来评估和比较供应商的恢复能力、数据保护和隐私能力以及服务转移。

CSA开放认证框架（OCF）是一项行业倡议，允许对云供应商进行全球性的、可信的独立评估。它是一个根据CSA行业领先的安全指导和控制框架，对云供应商提供灵活、渐进和多层次的认证和/或认证的计划。

该计划的目标是与现有的第三方认证和审计标准相协调，以避免重复工作和成本。

CSA开放认证框架基于CSA相关工作组定义的技术最佳实践和控制框架，例如，云控制矩阵（CCM）、共识评估倡议问卷（CAIQ）、等级协议研究倡议以及物联网控制框架。

CSA开放认证框架将支持几个层级，承认供应商和消费者的不同保证要求和成熟度级别。这将包括从CSA“安全、信任、保障和风险”项目（STAR）自评估到持续监督的高保障规格。

开放认证框架及其工作组提出的讨论和决定/变更被认为特权和秘密，在拟议的变更被最终确定或进行投票并记录在案之前，不会被公开。

工作组成员

以下为符合要求的开放认证框架工作组成员：

- CSA企业客户会员单位（企业用户）
- CSA解决方案提供商会员单位（云服务商）
- 国际、区域，国家立法机关、部门和机构（欧盟委员会、欧洲数据保护委员会/EDPB、ENISA、德国BSI、METI、IDB—IDA、NIST、FedRAMP、美国国防部、美国FTC等）。
- SDO和其他组织（如ISO/IEC/JTC 1/SC27, SC38, ITU-T, ETSI, W3C, ISACA, AICPA, JIPDEC, JASA等）
- 不直接由CSA主持，但与开放认证框架工作组活动有关的相关研究项目的代表（例如，EU-SEC）。
- 贸易和用户协会的代表（例如，EuroCIO、DigitalEurope、ECSO等）

工作组结构

联合主席

除选定的领导外，工作组将由联合主席领导。联合主席必须是CSA的成员，CSA执行小组批准例外。联合主席将协助工作小组的领导职责。联合主席可根据需要任命其他人，以确保有效地执行既定的研究工作。联合主席的职责包括：

- 确定每年的工作计划（例如，会议和预期交付成果）
- 确保按照工作计划进行
- 向CSA执行团队报告执行风险并提出可能的解决方案
- 必要时召开会议，并担任开放认证框架的主席
- 牵头准备可交付成果的草案，或在开放认证框架内确定一个合适的人，担任可交付成果的主要编辑/报告员的角色
- 确保遵循当前的开放认证框架章程中提供的指导
- 确保相关文件被分发给开放认证框架成员

委员会

工作组可以指定和组织下属委员会，以帮助研究与工作组主题有关的倡议。

下属工作组

可以成立由专家组成的下属工作组，可制定计划或执行任何相关的推广，意识宣传或研究机会。这些下属工作组应直接向隶属工作组汇报。

与其他工作组的配合

开放认证框架工作组也可以根据需要选择允许云社区和其他CSA工作组之间的资源共享，以协助及时完成项目、计划和其他活动，以支持/实现工作组所确定的工作内容。开放认证框架工作组会与包括但不限于以下的其他工作组紧密合作：

- **CSA云控制矩阵工作组**
 - 具体合作实施CCM相关的控制措施，包括STAR的三个保障级别和透明度。
- **EU-SEC项目**
 - 具体在以下方面进行合作：
 - 界定、测试和实施STAR与其他相关认证和证明之间的相互承认过程。
 - 定义、测试和实施基于持续审计的认证过程。
- **CSA PLA工作组**
 - 具体合作开发一个计划，根据PLA实践准则v3.1中的要求对组织进行认证。
- **CSA MAST倡议工作组**
 - 具体合作开发一项计划（暂定名为CSA STAR Mobile），根据MAST白皮书中的要求对移动应用程序进行认证。
- **物联网矩阵**
 - 评估STAR计划向物联网的延伸（即实施边缘计算和物联网设备的认证）。

- 国际标准化委员会（ISC）
 - 具体合作确定STAR计划组件的国际标准化机会，以及来自SDO的相关投入，这些投入可有助于改善该计划
- 其他小组：
 - 欧共体云计算认证小组
 - 欧盟网络安全局（ENISA）
 - ISO SC 27
 - 国家标准和技术研究所（NIST）
 - 国际注册专业会计师协会（AICPA）
 - 德国联邦信息安全局（BSI）和其他（如ANSSI）

业务

咨询

CSA工作组将接受各中小企业和理事会的咨询，包括但不限于国际标准化理事会（ISC）和CSA执行团队，以确保工作组的研究在CSA的范围内，并与其他行业合作伙伴的研究相一致。该研究将保持行业的独特性，并参考任何冗余或重复的工作。

研究周期

CSA工作组将对所有项目和倡议遵循CSA研究生命周期的发展
https://downloads.cloudsecurityalliance.org/initiatives/general/CSA_Research_Lifecycle_FINAL.pdf

同行评审

我们将寻求CSA的帮助，联系同行来评审我们的章程、出版物和其他工作小组的文档化活动。

沟通方法

基础设施和资源要求

该工作组将由CSA的志愿者组成；它将有联合主席和/或委员会。工作小组将需要项目管理、在线工作和技术写作协助。

工作组的电话会议和现场会议

工作组将至少每两个月召开一次电话会议。负责人或其委托人必须出席或参与在线工作。如果负责人缺席，委托人必须有充分的授权代表负责人行事。线下会议将在选定的地点举行。

决策规程

A. 多数的定义

1. 多数应包括超过一半的出席并投票的成员
2. 在计算多数时，弃权的成员不应考虑在内
3. 如果出现票数相同的情况，提案或修正案应视为被否决
4. 就本章程而言，“出席并参加表决的成员”是指对某项提案投“赞成”或“反对”票的成员，包括委托人。
5. 代理人应通过书面或不可抵赖的电子邮件获得授权，并将在投票开始前由联合主席检验和宣布代理人授权的合法性。

B. 过半数弃权

1. 当弃权票数超过所投票数的一半时（赞成票，加反对票，加弃权票），对所讨论事项的审议应推迟到以后的会议，届时弃权票将不再考虑。

C. 表决规程

1. 投票规程如下

- a) 一般采用举手表决方式，除非有人要求进行无记名投票；如果至少有两名出席并有权投票的成员在投票开始前提出要求，并且没有要求进行b)项下的无记名投票，或者a)项下的规程没有显示出明显的多数
 - b) 无记名方式，至少五名出席并有权投票的成员在投票开始前提出此要求（网上投票适用）
2. 在开始投票之前，主席应评审任何关于投票方式的要求，然后正式宣布适用的投票规程和提交表决的问题。然后，主席应宣布投票开始，并在投票结束后宣布投票结果。
 3. 如果是无记名投票，工作组负责人应立即采取措施，确保投票的保密性

交付物/活动

活动列表包括：

- 完成并实施开放认证框架三级STAR持续认证。
- 在STAR计划中实施相互承认的规程。
- 完成并实施隐私认证和自评估（目前基于GDPR CoC/PLA实践准则）。
- 为各种STAR计划的目标受众制作宣传和培训材料。
- 评估边缘计算作为STAR的物联网扩展的可行性

上述每项活动将有一个或多个相关的可交付成果。最终的可交付成果列表将包括在STAR计划的年度工作计划中。

可交付成果将受CSA的知识产权策略的约束。

有效期限

本章程的有效期至2021年4月30日，并将更新以反映开放认证框架工作组目标和优先事项的任何变更。

章程修订历史

2015年11月	2016年3月	2017年9月
2019年4月		



附录 7：投诉管理过程

投诉管理过程的主要目的是允许任何数据主体、云服务商、云客户或个人（在本附件中统称为“投诉方”）报告与CoC相关的问题，例如（但不限于）通知：

- 云服务商提交的CoC自评估和/或CoC第三方评估报告中报告的信息与该云服务商在提供相关服务时实际应用的条件/条款之间存在不一致。
- 云服务商在提交的CoC自评估和/或CoC第三方评估中报告了误导性或不准确的信息。
- 违反CSA道德准则的行为。
- 与CoC管理小组成员有关的利益冲突情况。
- 与有资质的CoC审计方或该有资质的CoC审计方聘用的任何有资质的CoC审计师有关的问题。

投诉：

反馈对于CoC的发展和管理以及相关的遵从性标识非常重要。反馈可以用来确定满意与否。它可以帮助识别在实践中可以改变CoC运作方式的领域。反馈还可以确保CoC的正确实施、维护和监督。

不满的方面应该得到相应的解决，纠正措施应该得到相应的处理。

监督机构有一个透明和易于使用的投诉规程，以确保：

- 监督机构以积极的方式处理反馈
- 反馈意见的处理受到监督
- 监督机构从任何批评、认可或评论中获得最大利益；以及
- 纠正行动和改进行动得到实施（如有必要）。

上诉

在投诉管理过程中，或在监督机构对CoC成员作出的任何决定方面，有时会出现无法通过正常过程解决的冲突。这些冲突的范围包括对解释的分歧，以及与授予、

暂停或取消遵从性标识有关的决定。上诉过程的存在是为了使这些争议能够以正式和适当的方式得到解决。

过程/策略

投诉可分为四类：

- 不满的意见
- 投诉
- 滥用遵从性标识；以及
- 通过CSA或监督机构的任何平台集中收到的与认可、不满意度、投诉、滥用标识有关的所有反馈，而获得的其他意见。

CSA和接受上诉/投诉的监督机构应确保：参与上诉/投诉处理过程的监督机构成员与参与管理相关投诉、基于上诉进行的相关CoC评审或审计以及决定的成员不同。

上诉/投诉的提交、调查和决定不应导致对投诉方或被投诉方的任何歧视性行为。

如果收到的投诉表明CoC成员违反了CoC的规则，监督机构应立即采取适当措施。如果CoC成员对监督机构的任何决定提出上诉，在上诉过程的最终决定完成之前，将不会采取任何行动。

收到的反馈和投诉

提出的任何投诉将在2（两）个工作日内向投诉方确认。一旦提出投诉，监督机构将在5（五）个工作日内开始处理该投诉。根据投诉的性质，相关机构（例如PLA工作组）将参与其中。在可行的情况下，将尽一切努力在投诉提出后的60（六十）天内完成。

在处理投诉时，监督机构可要求投诉方提供补充信息，以便更好地评估该事项。

就任何个案，如认为投诉明显没有根据或过度，监督机构可立即驳回投诉。

如果投诉方没有明确的意图来报告实际违反CoC“控制指南：PLA”的行为，那么投诉可能是明显的毫无根据，或者除了造成混乱外没有任何实际目的，那么投诉可能是恶意或用来骚扰CoC成员的。可能表明这种情况的因素包括：

- 个人在投诉中或其他场合明确表示他们打算造成破坏。
- 对云服务商或特定的云服务商工作人员提出毫无根据的指责。
- 投诉针对的是他们有个人恩怨的某位云服务商工作人员；或
- 作为一项持续活动的一部分，投诉方系统地或频繁地（例如，每周一次）对云服务商提出不同的投诉，目的是造成干扰。

如果投诉重复以前请求的内容（且两次请求之间没有经过合理的间隔），或其他请求重叠，则可能认为是过度投诉。

如果投诉因这些原因被驳回，监督机构必须将驳回的情况告知投诉方，并提供相关理由。监督机构必须特别清楚地解释，为什么根据适用于本案的具体情况，认定这种投诉是明显没有根据和/或过度的。

关于 CoC 成员的投诉

如果收到的投诉涉及CoC第一方证明机制的不准确、不一致或任何其他问题，监督机构可要求有关CoC成员（即被投诉的云服务商）提供补充信息。如果CoC成员向监督机构提供的信息不足以对投诉作出最终决定，或者如果投诉的性质涉及重大问题，CoC成员可能被要求接受第三方审计，以便能够保持其遵从性标识。

如果CoC成员被要求接受第三方审计，该审计将由监督机构指定的，并经核实不存在利益冲突后（所选的合格CoC审计方将被要求满足CoC第2.5.2条对监督机构提出的要求）独立的合格CoC审计方进行。在执行该审计时，有资质的CoC审计方应遵守CoC成员的任何可行的安全措施，但不应妨碍有资质的CoC审计方执行其任务。

任何通过CSA或监督机构门户网站登记的关于CoC服务的不满意意见都将被转交给监督机构。监督机构会将投诉分配给负责与各CoC成员沟通的监督机构成员。监督机构的该对应成员将在MBMR的监督下调查该投诉。MBMR向监督机构报告重要问题的结果。投诉和所有相关信息，以及解决状态的细节将记录在投诉系统中，并在投诉得到解决时关闭。

管理投诉的监督机构成员应确保被投诉的公司在CSA注册，且投诉属于CoC的范围。还应检查投诉方是否以书面形式向相关公司提出了投诉。如果没有，应将此作为一种可能允许迅速补救投诉的方式予以鼓励。披露投诉方的姓名和其他可能导致识别投诉方的个人信息需要得到投诉方的同意。

从监督机构（包括CompSA）或其他监管机构收到的任何投诉，将立即报告给CSA。

如果监督机构接受了提交的有关CoC成员的投诉（接受意味着投诉被认为是有效的，并且发现了违反CoC的相关行为），监督机构将立即对该CoC成员采取适当的措施。这些措施的目的是为了阻止违规行为，并防止其今后再次发生。采取的措施可以是正式警告，要求在规定的期限内采取纠正措施，也可以是暂时中止或最终撤销云服务商的CoC遵守标识：

- 对于非常轻微的问题，监督机构将向CoC成员发出正式警告，并提供一个时间期限，在此期间必须纠正所发现的不合规行为。
- 对于轻微的问题，或者CoC成员没有对监督机构发出的正式警告作出充分和及时的反应，监督机构将暂时停止该CoC成员的CoC遵守标识，直到监督机构确信问题已经完全解决。
- 对于重大问题，监督机构将撤销该CoC成员的CoC遵守标识。

监督机构还将通过CSA的网站，公布对CoC成员采取的导致CoC从标识被暂停或撤销的任何纠正措施。

PLA工作组将发布指导方针，以界定“非常小”、“小”和“大”的类别问题。

如果收到的投诉涉及CoC第三方评估机制的不准确、不一致或任何其他问题，监督机构可要求有关CoC成员（即被投诉的云服务商）提供补充信息，并立即通知负责发布相关第三方评估的有资质的CoC审计方。该有资质的CoC审计方将负责调查该投诉，并提交一份报告说明其调查结果。在进行调查时，有资质的CoC审计方应遵守CoC成员的任何可行的安全措施，但不应妨碍有资质的CoC审计方执行其任务。根据有资质的CoC审计方编制的投诉报告，以及其掌握的或可能收集到的任何进一步信息（例如，来自投诉方、有资质的CoC审计方或CoC成员），监督机构将立即对该CoC成员采取适当措施，条件与上述情形相同。

在暂停或撤销遵守标识的情况下，将无不当延迟的直接通知CompSA，同时也会通知任何其他相关的SA（如果法律要求）。监督机构也可以决定公布对违规的CoC成员采取的行动或制裁，特别是在问题被认为是“重大”的情况下。

CoC成员和投诉方将被告知投诉的调查结果，且不会有不当的延迟。

监督机构将在MBMR的监督下制定定期报告，以记录投诉调查的结果，并至少

形成一份年度报告，其中包括该年度开展的所有与投诉有关的活动。这份年度报告将与董事会、CompSA和其他相关的监管机构（在法律要求的情况下）共享。

所有经过处理的投诉将在监督机构的定期评审中进行评审。

有关有资质的 CoC 审计方的投诉

对有资质的Coc审计方的投诉管理过程—包括对有资质的Coc审计方不再符合Coc对其提出的要求的投诉，或对有资质的Coc审计方所做的评估有欺诈或不准确的投诉—将遵循对Coc成员所述的相同过程，但有以下调整。

监督机构在完成对合格Coc审计方的调查过程后，保留根据这些调查的结果暂停、撤销或终止合格Coc审计方的认证权利—特别是在这些实体未能适当执行监督机构对其包括违反合同的情况而施加的任何纠正措施。

上诉

正式沟通

如果Coc成员对投诉调查结束后通知的结论和/或对其实施的制裁或纠正措施提出异议，必须在收到通知后七（7）个自然日内向监督机构提出上诉。如果提出上诉，在上诉过程结束和监督机构作出最终决定之前，将不会执行任何纠正行动。

监督机构将与所有相关方协商以确定事实，并在商定的时间内获得所有支持信息。与上诉方的任何沟通都将以书面形式进行，并送达上诉方提供的联络地址，或上诉方指明的任何其他地址。

成立上诉委员会

MBMR将为每个上诉案件任命一个上诉委员会。上诉委员会将由三（3）名监督机构成员组成，其中一名成员将担任主席。这些成员必须没有参与作为上诉对象的具体投诉管理过程，并且必须与任何有关各方（即，上诉方和投诉方）没有关联。

安排上诉委员会的会议

上诉委员会将在上诉方、被上诉方和其他相关方最合适的时候安排会议。应至少七（7）个自然日提前通知上诉人会议日期、时间和地点，以及上诉委员会成员

的姓名。上诉方可以根据合理的理由，以书面形式反对任命一名或多名上诉委员会成员。任何此类反对意见将由MBMR评估；如果认为有效，被反对的上诉委员会成员将由符合上述独立性和公正性相同要求的其他监督机构成员取代。MBMR必须以书面形式说明就这种反对意见作出的任何决定，并在没有不当延迟的情况下通知上诉方。

举行上诉委员会听证

上诉委员会主席的任务是确保上诉委员会的会议以有序和适当的方式进行。特别是必须确保：

- 上诉委员会以保密方式听取上诉方提出的证据和意见。
- 上诉委员会以保密方式听取监督机构和/或被上诉方提出的证据和意见。
- 上诉委员会评估所有各方的陈述，并在适当考虑后（如有必要，可进一步询问），做出最终决定。该决定为由上诉委员会的多数成员作出的最终的和结论性的决定。

CompSA 和其他监管机构的参与

CompSA以及其他监管机构、实体可以介入上诉委员会会议或常规的上诉过程，就争议事项提交书面意见。

上诉委员会主席记录上诉委员会的议程和最终决定。上诉委员会主席也将在上诉委员会会议召开后的五（5）个工作日内，将最终决定以书面形式通知监督机构、CSA、CompSA和其他相关的监管机构（如法律要求）。

补救措施

如果上诉委员会决定改变监督机构的决定，上诉方的补救措施将限于由监督机构宣布的改变后的决定，其方式与宣布原决定的方式相同。对于上诉方因原决定而遭受的任何损失或损害，将不承担职责。

纠正行动

CSA将考虑委员会的调查结果，并根据需要采取任何其他适当的纠正和预防行动。

附录 8：监督/审计过程

监督 CoC 成员提交的材料

监督机构将采用公认的最佳实践做法来监督/审核第一方证明和第三方评估 CoC 遵守情况的提交材料，以提供高级别的信心：

- 1、CoC 成员申请加入 CoC 的服务相关的过程，符合 CoC 的要求，如提交给 STAR 注册处的第一方证明遵守声明/第三方评估遵守声明和 PLA 业务守则（CoP）模板—附件 1 所述；以及
- 2、CoC 成员持续更新所提交材料，以保持与 PLA 业务守则（CoP）模板—附件 1 的任何更新和修订同步。

使用的监测方法将以分级抽样的形式进行，该抽样是基于至少 5 个样本或 2% 的提交物的抽样，以较多者为准（图 1）。

应根据监督机构从隐私和数据保护角度认为相关的因素增加抽样，包括（但不限于）：

- 某一 CoC 成员进行的处理活动的复杂性和风险。
- 在任何特定时间，CoC 成员的总数量。
- CoC 成员的地理范围。
- 收到的有关某个 CoC 成员的投诉数量；以及
- 某一 CoC 成员可能处理的个人数据的敏感性。

监督机构将为每一次增加样本量的抽样工作提供文档，说明具体增加的理由。

人数	样本量	修正后的样本量
10	0.2	最少样本数量必须为 5
20	0.4	最少样本数量必须为 5
30	0.6	最少样本数量必须为 5
50	1	最少样本数量必须为 5
75	1.5	最少样本数量必须为 5
100	2.0	最少样本数量必须为 5
150	3.0	最少样本数量必须为 5
200	4.0	最少样本数量必须为 5
250	5.0	最少样本数量必须为 5
300	6.0	6
400	8.0	8
500	10.0	10
600	12.0	12
700	14.0	14
800	16.0	16
900	18.0	18
1, 000	20.0	20
1, 200	24.0	24
1, 500	30.0	30
2, 000	40.0	40
2, 500	50.0	50
3, 500	70.0	70
5, 000	100.0	100
7, 500	150.0	150
10, 000	200.0	200
25, 000	500.0	500
50, 000	1000.0	1000
75, 000	1500.0	1500
100, 000	2000.0	2000
250, 000	5000.0	5000
500, 000	10000.0	10000
1, 000, 000	20000.0	20000
2, 500, 000	50000.0	50000
10, 000, 000	200000.0	200000
100, 000, 000	2000000.0	2000000
264, 000, 000	5280000.0	5280000

图1 样本量

每个被纳入样本的CoC成员将被评估其对CoC控制措施的遵守情况，以核实这些控制措施的实际实施效果。根据有关CoC成员的范围和复杂性，至少有10%的CoC控制措施将被随机评估。如果对CoC成员部分或全部CoC控制措施的遵守和有效性产生进一步的疑问，监督机构可以增加评估控制的样本，直到有足够的证据来确定CoC成员对CoC的整体合规与否。

数字将根据标准数学规则进行四舍五入。样本将每年随机抽取一次。根据以往的评审和评审结果，评审可能会更频繁。任何有不符合项的CoC成员¹必须提交书面纠正措施，并被纳入下一次抽样计划，以确认纠正措施的实施和有效性。

被指派进行特定评审的监督机构成员必须满足最低能力的整体要求，如CoC（专业知识）第3部分第2.5.3节所述。

评审的具体内容

评审的公告和信息收集过程

根据评审范围，评审以现场或远程进行。

监督机构至少提前3个月以书面形式向CoC成员通知评审。该通知还包括评审的范围和所有需要的信息列表。

监督机构将与CoC成员联系，在CoC成员和监督机构及其他相关方最合适的时候预约现场或远程评审。要求的信息应由CoC成员在实际评审前最少提前6周送达。

如果在对收到的信息进行调查后，监督机构认为有必要提供任何额外的信息，也将书面要求补充提供。任何补充信息应在请求后2周内由CoC成员提供给监督机构。

如果CoC成员有任何不当延迟或不配合，监督机构有权实施相应的处罚。

¹ **严重不符合项：**根据客观证据，没有实施和/或保持与CoC控制的一致性，或存在重大失误（即没有实施CoC控制，或未能实施CoC控制）；或根据现有客观证据，对CoC成员实施的措施能否实现既定策略和控制目标产生重大怀疑的情况。

轻微不符合项：代表一个系统的弱点或小问题，如果不加以解决，可能会导致重大不符合项。每一个轻微的不符合项都应该被考虑以进行潜在的改进，并进一步调查任何系统的弱点，以便可能纳入纠正行动方案。

语言

评审将以英语进行

评审的基本内容

在开展年度审计工作时，监督机构力求达到以下目标：

- 从CoC成员处获得证据，证明其已经正确地解释和执行了CoC的要求。
- 确认CoC成员执行CoC要求的方式与这些成员提交的已公布的自评估/第三方评估的内容相一致。

监督机构将在评审的范围内：

- a) 要求CoC成员证明其提交的自评估/第三方评估的条款在实质上的准确性，并在提交评估的服务方面得到了执行²，并使用了上文定义的抽样过程（监测CoC成员提交的文件）；
- b) 确定CoC成员用于识别、检查和评估CoC下的隐私要求及其相关风险的规程，以及其实施结果是否符合CoC和成员的策略、目标和指标；
- c) 确定CoC成员采用的和评审范围内的任何和所有规程是否健全并得到适当执行；以及
- d) 在收集必要信息时，确保证据的完整性和可追溯性。

审计报告

对CoC成员进行的所有审计工作将要求形成一份审计报告草案。该报告必须足够详细，以辅助和支持监督机构对该CoC成员作出的任何决定。

监督机构的报告草案应接受至少一名其他监督机构成员（未参与实际评审）的评审。于完成后，该报告草案将发送给CoC成员，并给予至少7天的时间做出正式反应。监督机构在报告定稿前会评审CoC成员提出的任何意见。最终报告由MBMR

² 通常情况下是远程进行，但保留现场评估的权利，在持续不符合要求或高风险环境的情况下，监督机构将酌情行使。

负责发布。如果最终报告包含重大错误或遗漏，MBMR需要以书面形式通知所有相关方进行纠正。

该报告应包含：

- a) 进行评审的监督机构成员的姓名；
- b) 遵循的重要审计线索和使用的审计方法；
- c) 对CoC的要求及其解释的有效性提出的意见，包括正面的（如值得注意的特点）和负面的（如潜在的不符合项）；
- d) 改善遵守的机会（如果合适）；
- e) 对CoC成员的做法是否符合CoC的要求的意见。应包括对符合或不符合项的明确声明，提及适用的CoC控制，并在相关情况下，与此前对该云服务商进行的审计结果进行比较；
- f) 关于CoC要求的实施和有效性的最重要的意见总结，包括正面和负面的意见；
- g) 关于该CoC成员是否应被视为完全/部分遵守CoC的建议，以及对该CoC成员应采取的相应纠正措施，并说明理由。根据违规行为的严重程度以及对云客户和数据对象的相关风险，所建议的措施以及向CoC成员提供的纠正时限（如相关）必须是适当的；以及
- h) CoC成员在收到上述意见、建议、总结和建议后提出的任何书面或口头反馈。

对于轻微不符合项，监督机构可向CoC成员发出正式警告，并提供一个时间期限，在此期限内必须纠正所发现的不符合项。

对于轻微不符合的情况，如果CoC成员没有及时对监督机构发出的正式警告做出充分的反应，监督机构可以暂时中止该CoC成员的CoC遵守标识，直到监督机构认为问题已经完全解决。

对于严重不符合的情况，监督机构可以撤销该CoC成员的CoC认证遵从性标识。

监督机构有权要求对CoC成员进行全面的第三方现场评估，如果1.) 发现重大不符合项，或2.) 发现一些轻微不符合项，并提出充分证据表明CoC成员的数据隐私体系出现故障。第三方评估的费用将完全由CoC成员承担。

特别评审

如果CoC成员对其系统进行了重大修改，或发生了可能影响其数据隐私过程基础的其他变更，则应当按照特别规定执行特别评审。



附录 9：ENISA 技术指南：安全目标

译者注：CSA GDPR 合规行为准则的文件目录中有列出附件 9：ENISA 技术指南：安全目标。该文件已被 CSA 云控制矩阵（CCM v4）所替代。请访问 CSA GCR 官网（c-csa.cn）获取云控制矩阵最新中英文版本。