联合国 A/CN.9/WG.IV/WP.148

大 会

Distr.: Limited
30 January 2018
Chinese
Original: English

联合国国际贸易法委员会
第四工作组（电子商务）
第五十六届会议
2018 年 4 月 16 日至 20 日，纽约

云计算所涉合同方面

秘书处的说明

目录

V.18-00388 (C) 080318 080318

一. 导言

1. 工作组似可查阅 A/CN.9/WG.IV/WP.142 号文件第 1 至 6 段了解工作组第五十五届会议（2017 年 4 月 24 日至 28 日，纽约）之前与云计算工作有关的背景情况。关于工作组第五十五届会议和委员会第五十届会议工作的有关进展情况概要，可参见本届会议临时议程（见 A/CN.9/WG.IV/WP.147 号文件，第 7、8 段）。

2. 根据工作组关于今后可能开展云计算方面工作的建议（A/CN.9/902，第 23 段）以及委员会第五十届会议就同一事项所表达的看法，[1]秘书处向工作组提交了一份云计算合同主要问题清单草稿，供其审议。清单草稿由秘书处在专家参与下编写，反映了工作组对清单范围和内容以及对清单起草办法进行的初步审议（A/CN.9/902，第 11-28 段）。

3. 预期工作组将就云计算方面工作进展情况向委员会第五十一届会议（2018 年 6 月 25 日至 7 月 13 日，纽约）提出报告。[2]鉴于清单所针对的用户以及预期使用清单的交易，工作组似宜考虑是否作为一种在线参考工具编制清单。如果这样做，工作组似宜向委员会建议行动方针，特别是建议，秘书处应编制的在线参考工具将反映经工作组第五十六届会议和委员会第五十一届会议修订的清单草稿实质内容。

二. 云计算合同主要问题清单草稿

[清单末尾术语表对清单全文中的黑体字作了说明．在线参考工具以更方便用户的方式对这些黑体字做了解释。]

导言

1. 清单述及商业实体之间云计算合同的主要问题，其中一方（提供商）向另一方（客户）提供终端使用的一种或多种**云计算服务**。**云计算服务**转售合同或其他形式的进一步分销不在清单范围之内。与**云计算服务伙伴**以及与可能参与向客户提供云计算服务的其他第三方的合同（例如，与分包商和互联网服务提供商的合同）也不包括在清单范围之内。

2. 云计算合同可以根据适用法律成为合格的服务合同、租赁合同、外包合同、许可合同、混合合同或者其他类型合同。因此，关于云计算合同的形式和内容，可能有不同的法定要求。在一些法域，如果法律未就这一问题做出规定或者规定含糊不清，订约方本人可在其合同中将合同定性为某一类型的合同；在对合同条款做出解释时，法院将考虑到这种定性，除非这样做会违反法律、法院实践、订约方实际意图、实际情况或者商业习惯或惯例。

3. 本清单所涉及的问题可能产生于云计算合同，而不考虑**云计算服务**的类型（如**基础设施即服务（IaaS）、平台即服务（PaaS）、软件即服务（SaaS）**）、**部署模式**（如公共、**社区、私人或混合**）和付费条款（有无报酬）。清单主要侧重点是提供**公共 SaaS** 类型付酬云计算服务的合同。

[1] 《大会正式记录，第七十二届会议，补编第 17 号》（A/72/17），第 116-127 段。

[2] 同上，第 116 和 127 段。

4. 谈判云计算合同条款的能力取决于多种因素，特别是合同涉及**标准化商用型多订户云解决方案**还是单个定制解决方案，是否存在选择相竞提议的可能性，而且还取决于潜在订约方的议价地位。在有选择的情况下，谈判合同条款的能力，特别是关于提供商单方面暂停、终止或修改合同的条款以及责任条款，是选择提供商的一项重要因素[交叉链接]。清单主要为云计算合同谈判方编写，但对于客户研究提供商所提供的标准条款以确定其是否充分考虑到客户需要也不误益处。

5. 各方不应将清单视为起草云计算合同方面详尽无遗的资料来源，也不应以此取代从有关专业顾问获得任何法律和技术咨询和服务。清单提出供潜在各方在起草合同之前和期间应当考虑的问题，但本意并非表示所有这些问题都必须加以考虑。就清单所讨论问题提出的各种解决方案将不会管辖各方之间的关系，除非各方明确同意这种解决方案，或者除非解决方案产生于适用法律的规定。清单中所使用的标题和小标题及其序列不应视为必须使用的，或者暗示云计算合同的任何首选结构或风格。云计算合同的形式、内容、风格和结构可能大相径庭，反映出各种不同的法律传统、起草风格、法律要求以及各方的需要和偏好。

6. [清单并非意在表示贸易法委员会对于订立云计算服务合同的可取性的立场。]

7. 清单由两个部分和术语表组成：第一部分述及潜在订约方——主要是客户——在订立云计算合同之前似宜考虑的订约前主要问题；第二部分述及谈判各方起草云计算合同时可能面对的主要合同问题；术语表对清单中使用的一些技术用语作出说明，以便于理解。

第一部分 订约前的主要方面

A. 核对强制性法律及其他要求

8. 适用于客户、供应商或两者的法律框架可以规定订立云计算合同的条件。此类条件还可能产生于合同承诺，其中包括**知识产权许可证**。客户和供应商尤其应当了解可能对其本人和其未来合同适用的与**个人数据**、网络安全、出口管制、海关、税务、商业秘密、知识产权和**特定部门条例**有关的法律和条例。不遵守强制性要求会造成重大负面影响，包括合同或其中部分无效或无法执行、行政罚款和刑事责任等。

9. 订立云计算合同的条件可以因部门和法域而不同。这些条件可包括要求采取特别措施保护**数据主体**的权利、部署特定模式（例如，**私人云**而不是**公共云**）、对放入云中的数据加密，以及向国家机关登记交易或者在**个人数据**处理中使用的软件。它们还可包括**数据本地化**要求以及对提供商的要求。

- *数据本地化*

10. **数据本地化**要求尤其可能产生于适用于**个人数据**、财会数据和公共部门数据的法律，以及可能限制对特定国家**转移**某些信息或软件的出口管制法律和条例。**数据本地化**要求还可能产生于合同承诺，例如，知识产权许可能要求将**特许内容**存储于用户个人的保密服务器。**数据本地化**之所以可取，可能纯粹出于实际原因，例如，增加**时延**，这对于股票交易所交易之类的实时操作可能特别重要。

11. 提供商的标准条款可能明确保留提供商在其任何营业所在国或其分包商的任何营业所在国存储客户数据的权利。这是最有可能采取的做法，即使没有明确规定的合同权利也是如此，因其暗含于**云计算服务**的安排中，即：作为一般规则，可以从不止一个地点提供**云计算服务**（例如，备份和防病毒保护可能是远程的，并可按照“**跟着太阳走**”全球模式提供支持）。顾客在必须遵守**数据本地化**要求时将需要获得这些要求可以得到满足的保证。在有可能谈判云计算合同的情况下，可将合同保障条款包括在内，例如，禁止移出规定地点，或者要求提供商事先征求客户核准此类移出[交叉链接]。

- *对提供商的要求*

12. 除市场条件外，客户选择合适提供商可能受到法定要求的限制。法律可能禁止与外国供应商、某些法域的供应商或者未取得国家主管机关认可/核证的提供商订立云计算合同。可能要求外国提供商为在某一法域提供**云计算服务**与本国供应商组建合营企业或取得当地执照和许可证，包括出口管制许可。**数据本地化**要求[交叉链接]也会影响到提供商的选择。在选择合适的提供商时，客户可能还关心对供应商规定的向外国国家机关透露客户数据及其他内容或提供其访问权限的任何法定义务。

B. 订约前风险评估

13. 适用的强制性法律可能要求将风险评估作为订立云计算合同一项先决条件。即使没有法定要求，云计算合同潜在订约方亦可决定进行风险评估，这可能有助于他们确定适当的减少风险战略，包括谈判适当的合同条款。

14. 并非所有产生于云计算合同的风险都与云具体相关。有些风险将需要在未来云计算合同以外加以处理（例如，网上连接中断所引发的风险），并不是所有风险都能够以可接受的费用减轻（例如，名誉损失）。此外，风险评估并不是订立合同前的一次性活动。风险评估可能会持续到合同进行期间，风险评估结果出来后可能要求修正或终止合同。

- 核实关于所选提供商的信息

15. 以下信息可使客户了解与特定提供商打交道可能面临的风险：

(a) 提供商的隐私、保密和安全政策，特别是关于防止在处理、中转、移入移出提供商系统期间擅自获取、使用、更改或破坏客户数据；

(b) 对客户持续获取**元数据**、审计记录以及显示安全措施的其他记录的保证；

(c) 发生泄密或系统故障时的现有灾难恢复计划和通知义务；

(d) 提供商提供的云迁移和服务终了援助，以及提供商给予的**互操作性**和**可移植性**方面的援助；

(e) 对雇员、分包商和参与提供云计算服务的第三方进行背景审查和培训的现有措施；

(f) 安全事件统计数字，以及关于灾难恢复程序以往运行情况的资料；

(g) 独立第三方对遵守技术标准的核证；

(h) 关于独立机构审计定期安排和范围的证据；

(i) 财务状况；

(j) 保险单；

(k) 可能的利益冲突；以及

(l) 分包和**分层云计算服务**的范围。

- 渗透测试、审计和实地考察

16. 强制适用于客户的法律和条例可能要求对参与提供云计算服务的数据中心进行**审计**、渗透测试和实地检查，目的主要是确定其所在地符合**数据本地化**法定要求。客户和供应商需要商定开展这些活动的条件，其中包括时间安排、费用分担以及对由于这些活动可能给提供商造成的任何损失的补偿。

- 知识产权侵权风险

17. 可能发生知识产权侵权风险，例如，提供商不是向其客户提供的资源的所有人或开发人，而是根据与第三方的**知识产权许可**安排使用这些资源。如果为执行合同而要求客户准予提供商一项使用客户打算放入云中内容的许可，也有可能出现知识产权侵权风险。在有些法域，即使为备份目的存储内容可能也会定性为复制，需要事先取得知识产权所有人的授权。

18. 为了双方的利益，应事先确保云计算服务的使用不会构成侵犯知识产权并成为撤销授予其中任何一方的知识产权许可的理由。知识产权侵权的代价可能非常高。

可能需要就分包权做出安排，或者与有关的第三方许可人订立直接许可安排，以根据这种安排准予对第三方许可的管理权。开源软件或其他内容的使用可能必须事先取得第三方的同意，并披露源代码和对开源软件或其他内容做出的任何修改。

- 锁定风险

19. 避免或减少**锁定**风险是客户的最重要考虑之一。缺乏**互操作性**和**可移植性**尤其会引起**锁定**风险。法律可能不要求提供商确保**互操作性**和**可移植性**。建立兼容导出程序可能完全是客户的义务，除非合同另有规定。

20. 合同可能特别载明提供商对**互操作性**和**可移植性**的保证。合同可能要求使用广泛使用的共同标准化或可互操作的数据和其他内容导出格式，或者给予客户在现有格式中做出选择的权利。合同可能还需要涉及客户对于联合产品和提供商应用程序或软件的权利，没有这些权利可能无法在另一云主机或者在内部使用客户数据和其他内容[交叉链接]。合同还可包括提供商在合同终止时协助将客户数据导回内部或导入另一个提供商的义务[交叉链接]。客户还需要认真考虑合同期限的影响：长期合同以及自动延期的中短期合同可能导致锁定风险升高[交叉链接]。

21. 客户似宜考虑事先测试数据和其他内容是否能够导入另一云提供商或者导回内部并使其可在内部使用。客户可能还需要确保云平台与内部平台同步以及他地复制其数据。与不止一个提供商进行交易并选择组合各种类型的**云计算服务**及其**部署模式**（即多方外包），即使会给客户造成费用及其他影响，可能不失为一种重要的减轻**锁定**风险的战略。

- 业务连续性风险

22. 客户将会担心业务连续性风险，不仅预期合同按预定时间终止存在这种风险，而且合同可能提前终止——包括其中一方不再经营—也有这种风险。业务连续性风险还可能产生于提供商暂停提供云计算服务。法律可能要求客户提前准备好适当战略，以确保业务连续性，避免因终止或暂停云计算服务而给终端用户造成不利影响。合同条款可有助于客户减轻业务连续性风险，特别是在提供商破产[交叉链接]并单方面暂停或终止云计算服务的情况下[交叉链接]。

- 撤出战略

23. 客户需要提前考虑必须撤出的内容（例如，只撤出客户输入云中的数据，还是也撤出**云服务衍生数据**）。客户还需要就及时获取提供商或第三方保管的任何解密钥匙寻求保证。客户还需要考虑为了在提供商系统之外使用数据和其他内容而要求对**知识产权许可**作出的任何修改。如果客户已经开发了与提供商的应用程序接口（API）直接互动的程序，可能需要重写这些程序以考虑到新供应商的应用程序接口。**软件即服务（SaaS）**客户如果拥有庞大用户基础，迁入另一 **SaaS** 提供商涉及的费用可能特别高，因为需要提供终端用户重新培训。

24. 所有这些因素，以及将所有客户数据和其他内容导回内部或者导入另一供应商系统所需要的时间框架，都需要在谈判服务终了合同条款时加以考虑[交叉链接]。

C. 其他订约前问题

- 披露信息

25. 适用法律可能要求潜在订约方相互提供信息，以便其就订立合同作出知情选择。在有些法域，如果订立合同之前没有向对方明确传达使义务对象得以确定或者可以确定的任何信息，或者缺乏此种传达，将使合同或其中的部分归于无效，或者使受侵害方有权提出损害赔偿。

26. 有些法域会将订约前提供的信息视为合同不可分割的组成部分。在这种情况下，双方需要确保将这类信息适当记录在案，并确保避免该信息与合同有任何不匹配之处。双方还需要处理对订约前披露信息给合同执行阶段灵活性和创所带来影响的问题。

- 保密

27. 订约前阶段所披露的信息可能被视为机密信息（例如，客户所要求或者提供商所提供的安全、身份识别和认证，关于分包商的信息，以及关于数据中心所在地和类型的信息，这种信息又可确定存储于该地点的数据类型以及国家机关（包括外国国家机关）对数据的访问权。潜在订约方可能需要就订约前阶段可予披露信息的保密达成协定。可能还需由参与订约前尽职调查的第三方（如审计师）提供书面保密承诺或签订不披露协议。

- 云迁移

28. 在迁入云中之前，通常要求客户对将要迁入云中的数据分类，并根据其敏感度和关键度对其进行安全处理，然后告知提供商每一类数据所需要的保护级别。客户可能还需要为提供某些服务（如客户数据留存和处分时间表、用户身份和访问管理机制以及必要时获取密钥程序）而向提供商提供所需要的其他信息。

29. 除了将数据和其他内容从客户或客户先前的提供商转移到提供商的云中，云迁移还可能涉及安装、配置、加密、测试以及客户工作人员及其他终端用户的培训。提供商可以作为与客户合同的一部分或者根据与客户或者与代表客户行事的第三方（如**系统集成商**）的单独协议，帮助客户处理这些问题，另外收费或采取其他方式。参与迁移各方需要就其在以下方面的作用和责任达成一致：安装和配置、拟迁入云中数据或其他内容的格式、迁移时间、确定迁移按协议实施的接收程序，以及迁移计划的其他细节。

第二部分 起草合同

A. 一般考虑

- 合同自由

30. 普遍承认的商业交易合同自由原则允许订约方订立一项合同并确定其内容。对合同自由的限制产生于就某些类型合同所适用的不可谈判条款制定的立法，或者产生于惩罚滥用权利行为和损害公共秩序和道德等方面行为的规则。不遵守这些限制所造成的后果包括合同或其中的部分不可执行以及承担民事、行政或刑事责任。不是通过自由谈判达成的合同，特别是那些对处于较弱谈判地位订约方[交叉链接]规定了滥权条款的合同，其可执行性尤其可能在预期订约方将遵守诚信和公平交易原则的法域产生问题。

- 合同的成立

31. 要约和承诺概念一向用来确定订约方是否以及何时就各自法律权利和义务达成了在合同存续期间对其具有约束力的协议。适用法律可能规定了为使一项订立合同的提议构成有约束力的最终邀约而必须满足的某些条件（例如，该提议应就所涵盖的云计算服务和付费条款具有足够确定性）。

32. 接受邀约生效，即为订立合同。可能有不同的接受机制（例如，对客户来说，点击网页上的选择框，在线登记云计算服务，开始使用云计算服务或者支付服务费；对提供商来说，开始或者继续提供服务；对双方来说，在线或者书面签署合同）。对邀约的重大修改（例如，关于赔偿责任、云计算服务质量和数量或者付费条款的修改）可以构成反要约，需由对方接受，方为订立合同。

33. **标准化商用型多订户云解决方案**一般通过交互式应用程序（如“点击完成”协定）提供。标准要约可能没有谈判和调整余地，或者余地极少。点击“我接受”、“好的”或者“我同意”，是订立合同预期采取的唯一步骤。在涉及合同谈判时，合同的成立可能包含一系列步骤，其中包括初步交换信息、谈判、发出和接受要约以及合同制备。

- 合同的形式

34. 云计算合同一般是在网上订立的。云计算合同可能有不同称谓（云计算服务协议、主服务协议或服务条款），可能包含一项或多项文件，如**可接受的使用政策（AUP)、服务级别协议（SLA）**、数据处理协议，或者数据保护政策、安全政策和许可协议等。

35. 适用于云计算合同的法律规则可能规定合同必须为**书面形式**，特别是如果涉及**个人数据处理**；所有以提及方式纳入的文件都必须附于主合同附件。即使不要求**书面**形式，为便于参考以及合同的明确性、完整性、可执行性和有效性，订约方依然可能决定以**书面方式**订立合同并将所有附属协议纳入其中。

36. 适用法律可能要求在纸张上签署合同，例如，一些法域出于税收考虑可能有此要求。

- 定义和术语

37. 鉴于云计算服务的性质，云计算合同必然包含许多技术术语。合同可能列入术语表以及合同全文所使用的主要术语定义，以避免出现模棱两可的解释。为确保一致性和法律明确性，订约方不妨考虑采用国际公认术语。

- 最低限合同内容

38. 合同通常包括以下内容：(a)确定订约方；(b)界定合同范围和标的；(c)具体规定订约方的权利和义务，包括付费条款；(d)确定合同期以及合同终止和展延条件；(e)确定违约救济和免责。合同通常还载有争议解决条款以及法律选择和诉讼地选择条款。

B. 订约方身份识别

39. 正确识别订约方的身份会对合同的成立和可执行性产生直接影响。法人名称及其法律形式、商业登记号（适用的）、注册办事处或营业地址，连同该法人的法定文件，通常提供了确定企业实体（无论公司或个人）法律人格及其订立有约束力合同的能力的充分依据。法律可能要求通过其他信息，例如，为税收目的的身份号码或者委托书，以确定自然人是否拥有代表法律实体签署和承诺的权力。

40. 法人身份的验证可以不同方式进行，或是直接由订约方直接进行，或是依赖第三方进行。订约方通常可以自由决定身份识别方法，除非适用法律禁止这样做。可能要求经授权的法人代表亲自到场，或者，如果使用可为各方接受的电子身份识别手段远程出席可能足矣。如果订约方可以选择，其选择通常由若干因素决定，其中包括特定合同交易所涉风险。有些法规可能要求或者仅承认某些身份识别方法，尤其是在签发委托书的情况下。法规还可能要求提供商依照适用标准向国家主管机关验明其客户身份。

C. 界定合同范围和标的

41. 鉴于**云计算服务**的范围，云计算合同标的在类型和复杂性上差别极大。在单项合同期内，标的可能发生变化：有些**云计算服务**可能被取消，同时也可能添加其他服务。合同标的可以包括提供核心服务、辅助服务和任选服务。

42. 合同标的说明将包括对云计算服务类型（**软件即服务（SaaS）、平台即服务（PaaS）、基础设施即服务（IaaS**）或其组合）及其**部署模式**（**公共、社区、私人或混合**）、其技术特点、质量特点和性能特点以及任何适用的标准作出说明。组成合同的若干文件可能与确定合同标的有关[交叉链接]。

- 服务级别协议

43. **服务级别协议**载明**绩效参数**，将据此衡量提供商交付的云计算服务。因此，这是确定合同义务范围以及提供商可能违约的一个重要工具。提供商的标准**服务级别协议**可能不就结果规定任何具体义务，而是载列不可执行的意图声明（例如，“提供商将作出最佳[或合理]努力，以确保高服务获取率”，“提供商将力求每周 7 天每天 24 小时提供服务[或达到 99%的正常运行时间]（但不保证）”）。客户可能在这些合同中缺乏救济，因为何为违反最佳专业努力条款可能难以确定。为避免这种

情况，客户将会愿意在**服务级别协议**中列明数量和质量方面的绩效参数，以及具体的衡量标准、质量保证和绩效测量方法。

数量方面绩效参数实例

能力	- X 数据存储能力 - X 程序运行可用记忆量
提供率	- 正常**运行时间**量或比例（如 99.9%） - 计算正常**运行时间**的具体公式 - 当服务提供率至关重要时（100%）的具体日期或天数和时间 - 特定应用程序的提供率（100%）
停机或中断	- 10 次 6 分钟中断 - 1 次 1 小时中断 - 服务中断后恢复数据的时间
弹性和伸缩性	- 服务伸缩量多大、速度多快，例如，最短期限内可用资源的最大量
时延	- 小于 X 毫秒
加密	- 闲置、中转和使用时的 **X 位值**
配套服务	- 24/7 - 客户的典型运行时间
事件和灾难管理恢复计划	- 解决事件的最长时间 - 最长**第一反应时间** - **恢复点目标（RPO）** - **恢复时间目标（RTO）** - 当在 X 时限内实现恢复至关重要时的具体日期或天数和时间
数据存储持久性	- 完好数据/（X 时限（如一个日历月）内完好数据+丢失数据）。需要确定数据类型（例如，文档、数据库、代码、应用）和衡量单位（文档数、位长）。

质量方面绩效参数实例

数据可移植性	- 可通过单一下载链接或者通过记载型应用程序接口（API）检索客户数据 - 数据格式的结构和记录方式足以让客户重新使用数据格式或者将其重构为所需要的不同数据格式
数据本地化要求	- 存储客户数据（包括任何复制件、**元数据**和其备份）的数据中心只能是实际位于合同所指明的法域并且由设

	在这些法域中的实体拥有并运行的数据中心——永远不得将数据转移出 X 国，必须在 Y 国及他地复制数据，但绝不能在 Z 国复制数据
安全	- 根据合同提供的服务至少每年由独立审计师根据合同中确定的安全标准进行核证
加密	- 提供商将确保，凡是经由公共通信网络（如互联网）在客户与提供商之间以及在提供商所使用的数据中心之间传输客户数据的，凡是客户数据在提供商所使用的数据中心处于闲置状态的，将对客户数据加密 - 提供商已实行了符合合同所确定的国际标准的密钥管理政策
数据保护/隐私	- 根据合同提供的服务至少每年由独立审计师根据合同中确定的数据保护/隐私标准进行核证
数据删除	- 提供商将确保，只要客户在合同确定的某一时限内提出请求，在符合合同所确定标准或方法的情况下，即应有效、不可逆转地、永久性删除客户数据

44. 合同可能需要列入便利更改客户需求的执行机制。否则，每次客户需求发生变化，可能都要进行耗费时日的谈判进程。

绩效测量

45. 合同可能需要规定所选择的测量方法和程序，特别是具体指明测量服务的参照期（每日、每周、每月）、服务交付报告机制（频度和形式）、订约方作用和职责，以及测量点。订约方可以商定独立测量绩效和分担相关费用的办法。

46. 客户将有意测量高峰时段——即最需要服务时段——的服务情况。客户或许有能力进行测量，也可以核实提供商或第三方提供的测量数据，这些计量数据是基于消费点绩效，而不是基于服务提供点的系统绩效。客户或许有能力评估提供商或第三方所提供报告中的测量数据。提供商可能同意根据客户要求提供绩效报告，定期提供（每日、每周、每月等），或者在某一特定事件之后提供。或者，提供商可能同意准予客户审查提供商服务水平测量相关记录的权利。有些提供商让顾客实时检查服务绩效数据。

47. 合同可能要求双方在一定时期内保持关于提供和消费服务的记录。这类资料可有助于谈判合同的任何修正和处理争议。

- 可接受的使用政策（AUP）

48. **AUP 政策**载明客户和其终端用户使用合同所涵盖的云计算服务的条件。其目的是保护提供商不因客户和其终端用户的行为而承担赔偿责任。预期任何潜在客户都会接受这种政策，而这种政策将成为与提供商合同的一部分。对于提供商认为属于不当或非法使用**云计算服务**的一贯性系列活动，绝大多数标准 AUP 政策都予以禁止。在有些情况下，可以根据客户具体需要取消某些禁止规定。

49. 常见做法是，提供商的标准条款要求客户的终端用户也遵守 **AUP 政策**，并要求客户必须尽其最大努力或者作出商业上合理的努力确保这种遵守。有些提供商可能要求客户积极防止第三方未经授权或不适当使用合同下所提供的云计算服务。客户除了向提供商通知客户所了解的所有未经授权或不适当的使用之外，可能倾向于将其 **AUP 政策**的告知义务限于已知终端用户，而不是授权或者**特意**允许此种使用。

- 安全政策

50. 系统安全，包括客户数据安全，涉及提供商和客户的共同责任。合同需要具体指明双方对于安全措施的对等作用和职责，以反映强制性法律对其中一方或双方规定的义务。

51. 提供商依循自己的安全政策乃是通常做法。在有些情况下，也有可能就提供商依循客户的安全政策进行谈判，不过这不包括**标准化商用型多订户解决方案**。合同可以具体规定安全措施（例如，受损媒介数据杀毒或删除要求，在不同地点分开存储成套数据要求，在客户独有的规定硬件上存储客户数据要求）。不过，双方需要评估合同过度披露安全信息的风险。

52. 一些安全措施并不预先假定对方提供投入，而完全依赖于相关方的例行活动，例如，提供商对存储数据并运行服务的硬件的检查，以及为确保控制下访问而采取的有效措施。在其他情况下，如果允许一方履行其相应义务或者评价和监测所执行安全措施的质量，就会预先假定对方提供投入。例如，将预期客户更新用户证书及其访问权清单并向提供商及时告知变更情况，从而确保适当的身份和访问管理机制。还将预期客户向提供商确认将分配给每一类数据的安全级别。

53. 一些安全威胁可能超出客户与供应商之间的合同框架，并可能要求调整云计算合同条款，使之与提供商和客户的其他合同（例如，与互联网服务提供商的合同）协调一致。

- 数据完整性

54. 提供商的标准合同可能载有一般免责声明，即保全客户数据完整性的最终责任在于客户。提供商可能仅提供其将尽最大努力保障客户数据这种不具约束力的保证。

55. 有些提供商可能愿意作出数据完整性承诺（例如，定期备份），可能是为了收取额外费用。不论与提供商的合同安排如何，客户似宜考虑是否有必要在提供商及其分包商的控制、触角或影响范围之外，在没有其参与的情况下获取客户数据至少一份可用复制件的访问权。

- 保密条款

56. 在有些情况下，提供商不提供保密或不披露条款，或者这些条款不足以保证尊重客户数据保密性。一些提供商可能甚至明确放弃对客户数据的任何保密义务，通过加密等方式，将数据保密的全部责任转移给客户。提供商可能仅同意对客户在合同谈判期间所披露的数据承担保密责任，但不对提供服务期间所处理的数据承担保密责任。提供商是否愿意承诺为客户数据保密，取决于根据合同向客户提供服务的性质，特别是是否要求提供商为提供这些服务而取得对数据的不加密访问权。

57. 在大多数情况下，客户希望提供商确保放入云中的所有客户数据的保密性，并对某些敏感数据作出更高级别的保密承诺（此类数据泄密适用单独赔偿责任制度）。客户可能特别担心其商业秘密、专门知识以及根据法律或者对第三方承诺必须保密的信息。

58. 如果需要额外保护层，适当做法或许是限制客户数据访问权，只允许小范围的提供商工作人员接触客户数据，同时要求提供商取得工作人员、特别是那些承担高风险职责的人员（例如，系统管理员，审计师以及处理侵入侦测报告和事件对策的人员）的个人保密承诺。将由客户向提供商准确无误地指明保密信息、所要求的保护级别、任何适用法律或合同要求，以及影响此类信息的任何变化，包括适用立法的任何修改。

59. 在有些情况下可能需为履行合同而披露客户数据。在其他情况下，法律可能要求必须披露数据，例如，根据向国家主管机关提供信息的义务[交叉链接]。因此，保密条款是可以有适当例外情形的。

60. 反之，提供商可能也希望规定客户有义务不披露关于提供商安全安排的信息以及根据合同或法律向客户提供服务的其他细节。

- *数据保护/隐私政策或者数据处理协议*

61. **个人数据**在许多法域受到法律特殊保护。适用于此类数据**处理**的法律可能不同于合同的适用法律，并将优先于任何不合规的合同条款。

62. 合同可能包括一个数据保护或隐私条款、数据处理协议或者类似协议，不过一些提供商可能仅同意遵守适用数据保护法律的一般义务。在一些法域，这类一般承诺可能是不够的：合同需要至少规定所涉事项、期限、**处理**的性质和目的、**个人数据**类型和**数据主体**种类，以及**数据控制人和数据处理人**的义务和权利。如果不存在谈判一项合同中的数据保护条款的可能性，客户可能起码需要审查标准条款，以确定相关规定在合法的**个人数据处理**以及损害的适当救济方面给予客户充分保障。

63. 客户可能就是**数据控制人**，在云中收集和处理的**个人数据**方面，将承担遵守数据保护法律的责任。客户可能需要寻求以合同条款要求提供商为客户遵守适用的数据保护条例——包括与**数据主体权利**有关的请求——提供支持。一旦提供商违反这一义务，可以谈判单独救济办法，其中包括客户单方面解约以及提供商赔偿损失的可能性。

64. 提供商的标准合同通常规定提供商不承担**数据控制人**的任何职责。提供商完全为提供云计算服务目的而依照客户指示处理客户数据，有可能只是作为**数据处理人**行事。但是，不论合同条款如何规定，如果提供商为自身目的或者按照国家机关的指示进一步处理数据，就有可能被视为**数据控制人**[交叉链接]。提供商将在这种进一步**处理**方面承担对于**个人数据**保护的全部责任。

- *数据泄密及其他安全事件所产生的义务*

65. 双方立即通知对方影响到合同的安全事件或其得知的任何这种疑似事件，这可能是法律或者合同要求的，也可能是两者同时都要求的。可以在法律规定的安全事件一般通知义务之外规定这项义务，要求通知所有利益攸关方，包括**数据主体**、保险公司和国家机关，以防止或尽量减少安全事件的影响。

66. 双方可以商定通知期（例如，一方得知事件或威胁后一天内）以及**安全事件通知和事件发生后步骤**的形式和内容，它们可能各不相同，取决于云中存储数据的种类。任何通知要求都应确认有必要不披露任何可能导致受影响方的系统、业务或网络受损的敏感资料。

67. 客户可能希望保留在发生严重安全事件造成客户数据**丢失**等情况时终止合同的权利。

D. 对客户数据及其他内容的权利

- *提供商为提供服务而对客户数据享有的权利*

68. 提供商通常保留根据“需要知道”原则访问客户数据权利。这种安排将允许提供商的雇员、分包商和其他第三方（如审计师）在为提供云计算服务（包括为维护、支持和安全目的）以及在为监测 **AUP 政策**、**服务级别协议**、**知识产权许可证**和其他合同文件合规情况而需要时访问客户数据。客户可能有意缩窄允许访问的情形，并坚持采取将确保客户数据保密性和完整性的措施。

69. 客户数据的某些访问权可被认为通过要求提供某项服务或性能而由客户默示准予提供商：没有这些权利，提供商将无法履行服务。例如，如果要求提供商定期备份客户数据，完成这项任务就必须获得复制数据的权利。同样，如果分承包商想要处理客户数据，提供商必须能够向其转移数据。

70. 合同可以明确指明客户将履行合同所必需的哪些涉及数据的权利赋予提供商、提供商是否以及在何种程度上有权向第三方（例如，其分包商）转让这些权利，以及被准予的权利或暗示权利的地域和时间范围。如果客户希望防止数据离开某一国家或地区，则地域限制对于客户可能特别重要。合同一般还将规定客户是否能够撤销准予的权利或暗示权利以及在何种条件下撤销。由于按要求质量水平提供服务的能力可能取决于客户赋予的权利，撤销某些权利所带来的直接影响可能就是修正或终止合同。

- *提供商为其他目的使用客户数据*

71. 除了与根据合同提供云计算服务有关的目的之外，提供商还可为其他目的（例如，广告、生成统计数据、分析和预测报告、从事其他数据挖掘工作）请求使用客户数据。这方面客户要考虑的问题包括：(a)提供商将收集哪些关于客户和其终端用户的信息，以及收集和使用这些信息的原因和目的；(b)这些信息是否将与其他组织、公司或个人共享，如果是，这样做的理由，以及这样做将取得客户同意还是不取得客户同意；(c)如果提供商与第三方共享这一信息，如何确保遵守保密和安全政策。如果提供商使用客户数据将影响到**个人数据**，双方还需要进一步仔细评估适用的数据保护法律对其规定的监管方面的守规义务。

72. 一般而言，合同可能需要规定，提供商不能为其自身目的自动取得客户数据使用权。合同可以列出不是为提供服务目的而使用客户数据的可允许的理由。例如，合同可以允许提供商为自身目的，在合同期内或之后，作为匿名开放数据或者以汇总、去身份化方式使用数据。在这种情况下，合同可以包括对于客户数据去身份化和匿名化的义务，以确保遵守任何适用的数据保护条例和其他条例。合同还可以限制内容复制和对外公开。

- 提供商使用客户名称、标志和商标

73. 提供商的标准条款可能准予提供商为其宣传目的而使用客户名称、标志和商标的权利。客户可以就删除或修改这些规定进行谈判。例如，客户可以要求提供商事先征求客户对使用其名称、标志和商标的同意，或者可将允许使用范围限于客户名称。

- 提供商根据国家命令或者为遵守条例而就客户数据采取行动

74. 提供商的标准条款可能保留提供商在向国家机关披露客户数据或者提供客户数据访问权方面的广泛酌处权（例如，列入“如果这样做将最有利于提供商”这样的措辞）。在提供商面临法院或其他国家机关要求提供数据访问权或者删改数据的命令等情况下（例如，执行**数据主体**的被遗忘权），客户可能有意缩窄提供商可以这样做的情形。然而，在其他情况下，例如，在提供商得知或者了解到非法内容之后，为了避免法律规定的赔偿责任，不论国家命令如何，提供商可能坚持其有权立即去除或封锁客户数据（“通知后下架”程序[交叉链接]）。

75. 作为最低限，合同可以要求提供商立即向客户通知国家命令或者提供商自行就客户数据作出的决定并附带所涉数据说明，除非此种通知将违反法律。如果事先通知和客户参与都不可能，合同可以要求提供商立即向客户发出相同信息的事后通知。合同可以要求提供商保持关于客户数据的所有命令、请求和其他活动的记录并为客户提供这些记录的访问权。

- 对云服务衍生数据的权利

76. 合同可能需要处理客户对**云服务衍生数据**的权利以及如何可在合同关系期间并在合同终止时行使这类权利的问题。

- 知识产权保护条款

77. 某些类型的云计算合同可能导致产生知识产权客体，或者是由提供商与客户合作产生这种客体（例如，通过顾客建议改进服务），或者由客户单独产生这种客体（新的应用程序、软件和其他原创工作）。合同可以载列一项明确的知识产权条款，以此确定合同哪一方拥有对云部署或云开发的各种客体的知识产权以及各方对这类权利的使用权。如果不存在谈判可能，客户至少需要审查可能拟定的知识产权条款，以确定提供商提供足够保障，并且允许客户使用适当工具保护、享有其知识产权并避免**锁定**风险[交叉链接]。

- 为法律目的检索数据

78. 可能要求客户具有为法律目的（如法律程序）搜索和查找原件形式云中数据的能力。为得以满足审计和调查标准，可能特别要求使用电子记录。有些提供商可能有条件在为法律目的检索法定格式数据方面向客户提供援助。在这种情况下，合同可能需要准确界定客户为满足主管机关对用于法律目的数据检索的请求而需要从提供商得到哪些援助。

- 数据删除

79. 数据删除方面的考虑将在合同期内适用，但在合同终止时尤其如此。例如，可能需要根据客户的留存计划删除某些数据。敏感数据可能需要在其生命周期某一特

定时间销毁（例如，在此类数据存储设备寿命终止时销毁硬盘）。还可能需要为遵守执法机构的删除请求，或者在确认知识产权侵权案件之后删除数据[交叉链接]。

80. 提供商的标准条款可能仅载有定期删除客户数据的无约束力声明。客户可能希望要求提供商按照数据留存和处置计划，或者按照客户发给提供商的授权或请求，立即、有效、不可逆转地永久性删除数据及其备份和**元数据**。合同可以涉及数据删除的时间期限和其他条件，包括提供商有义务在删除完成后发给客户数据删除确认函，并为客户提供对删除活动审计记录的访问权。

81. 可以根据数据性质和敏感性指明删除所使用的具体标准或方法（例如，可以要求从不同地点和媒介删除数据，其中包括分包商和其他第三方的系统，分不同级别删除数据，例如，数据杀毒以确保彻底删除数据或者销毁硬件之前数据的保密性）。涉及销毁设备而不是重新部署设备的删除虽然更安全，但成本更高，而且并非总是可行（例如，如果提供商其他客户的数据存储在同一硬件上的话）。这些方面都需要在谈判合同时考虑到，例如，要求提供商使用孤立的基础设施存储客户的特别敏感数据。

E. 审计和监测

- *监测活动*

82. 双方可能需要监测彼此的活动，以确保遵守条例和合同（例如，客户和其终端用户遵守 **AUP 政策**和**知识产权许可**的情况，提供商遵守**安全级别协议**、数据保护政策等方面的情况）。一些监测活动可能是法律规定必须进行的，例如，涉及**个人数据处理**的活动。

83. 合同应确定定期或经常性监测活动和负责执行这些活动的一方以及对方为监测提供方便的义务。合同还可以预期任何例外监测活动，并提供处理这些活动的选项。合同还可以规定对另一方的报告要求以及这种监测活动所要求的任何保密承诺。

84. 过度监测会影响绩效，增加服务费用。对于需要近实时履行的服务，客户可能希望寻求有权要求提供商在监测实质上不利于履行服务时暂停或停止监测。

- *审计和安全测试*

85. 审计和安全测试是常见的，特别是提供商发起的检验安全措施效能的审计和安全测试。有些审计和安全测试可能是法律要求必须进行的。合同可以包括涉及双方审计权、审计范围、重复率、手续和费用的条款。合同还可以要求双方相互交换各自委托进行的审计或安全测试结果。对于审计和安全测试方面的合同权利或法定义务，可能需要在合同中以对方的相应义务加以补充，以方便行使此类权利或履行这些义务（例如，准予相关数据中心的访问权）。

86. 双方可以商定只能由专业组织进行审计或安全测试，或者商定提供商或客户可以选择由专业组织进行审计或安全测试。合同可以具体规定第三方需满足的资格要求以及第三方的聘用条件，包括费用分担办法。双方可以在事件发生后，根据事件的严重性和类型，商定对审计或安全测试的特别安排（例如，事件的责任方必须部分或全部赔偿费用）。

F. 付费条款

- 随用随付

87. 价格是一项必不可少的合同条款，不确定价格或者没有一种定价机制，可能使合同无法执行。

88. 云计算的**按需自助服务**特点通常从**随用随付**账单系统中反映出来。通常做法是，合同具体规定云计算服务商定供应量（如规定用户数、使用次数或使用时间）的单位价格。作为对任何一方的奖惩办法，可以设计价格表或其他价格调整办法，包括批量折扣。免费试用很常见，因为一些服务不收费。尽管价格计算会有多种变式，但制定可为双方理解的清楚而透明的价格条款可避免今后引起冲突和诉讼。

- 许可证费用

89. 合同应当明确规定，云计算服务付费是否涵盖提供商可能作为服务一部分准予客户的任何许可的许可证费用。特别是，**软件即服务（SaaS）**往往涉及客户使用提供商许可的软件。

90. 许可证可以按机器台数计费，也可以按开机次数计费，费用取决于用户类型（例如，相对于非专业用户，专业用户可能是费用最高的类别之一）。客户需要考虑各种付款结构的影响。例如，如果按开机次数收取软件费用，每次连接一台新机器，即使客户在同样时间内使用同样的开机次数，客户的许可证费也可能显著增加。对于客户来说还有一点很重要：不仅要在合同中确定许可安排所涵盖软件的潜在用户数目，而且还要确定每一类别（如雇员、独立承包商、供应商）的用户数目以及准予每一类别用户的权利。客户还需要在合同中确定将归入许可范围的访问权和使用权，以及可能导致许可范围扩大并因此造成许可证费用增加的客户和其终端用户访问和使用情形。

- 额外费用

91. 价格可能还包括一次性费用（例如，配置和云迁移费用）。还可能有一些额外服务不包括在基本云计算服务合同内，云计算服务提供商提供这些服务要单独收费（例如，营业时间以外提供的支持按次数收费，或者按固定价格提供）。双方还应说明税务影响，因为云计算服务可能属于也可能不属于应税服务或货物类别。

- 价格变动

92. 提供商的标准条款往往赋予提供商单方面修改价格或价格表的权利。客户可能倾向于限制这一权利。双方可以商定在合同中规定定价方法（例如，提供商可以提价的频度和幅度）。价格上限可以是某一消费价格指数、预先设定的百分比或者提供商某一特定时刻的目录价格。客户可以要求提供商提前通知提价，并在合同中规定客户不接受提价的后果。

- 其他付费条款

93. 付费条款可能需要涉及发票开具方式（如电子发票）以及发票形式和内容，这对于遵守税务条例可能很重要。一些法域的税务机关可能不接受电子发票，也可能规定特殊格式，其中包括，凡是适用于云计算服务的税务可能都需单独加以说明。

94. 合同可能还需要具体规定付费到期日、货币、适用汇率、付款方式、迟付制裁办法以及付费争议解决程序。

G. 服务变更

95. **云计算服务**呈现灵活性和波动性。合同可以载列多种选择，供客户用以调整服务使之适合客户不断变化的业务需要。此外，提供商可以保留酌情调整其服务组合的权利。根据变更涉及核心服务还是辅助服务及配套方面，适合采用不同合同制度。如果变更可能对服务产生不利影响，而不是改进服务，可能也有必要采用不同的合同制度（例如，从标准服务提议转换为安全级别更高、反应时间更短的加强型云计算服务提议）。

- 升级

96. 尽管升级可能符合客户利益，但也会对云计算服务的提供造成干扰，因为即使在 24/7 基础上提供服务，升级也有可能转化为正常工作时间内的较高**停机**时间。升级还有可能产生其他负面影响，例如，需要对客户的应用程序或者信息和电信系统作出修改，或者要求对客户的用户进行再培训。

97. 合同可以要求提供商提前通知客户即将进行的升级及其影响。可以要求提供商把升级安排在对客户需求量低或没有需求的期间。双方可以商定，对旧版作出重大修改的，旧版应当在商定期间与新版并行保留，以确保客户业务的连续性。可能需要商定报告和解决可能出现问题的程序。合同可能还需要涉及的是，提供商协助对客户应用程序和信息技术系统作出修改并根据请求对客户的终端用户进行再培训。双方可能还需要商定升级所产生费用的分担办法。

- 服务下降或中止

98. 不论是否以其他服务取而代之，技术发展、竞争压力或其他原因都可能导致一些云计算服务下降或中止。提供商可能在合同中保留调整所提供的服务组合的权利，例如，终止一部分服务。不过，提供商即使中止部分云计算服务也可能使客户面临对其终端用户的赔偿责任。

99. 在这种情况下，合同可能需要为客户建立充分保护，包括将这些更改预先通知给客户、客户有权在更改令人无法接受时解约，以及规定适当留存期以确保任何受影响客户数据或其他内容的及时**可逆性**。合同可以完全禁止会对所提供服务的性质、范围或者质量产生不利影响的修改，或者限制提供商的权利，只能引入“商业上合理的修改”。但是，客户不一定总能够判断修改对于所提供服务的合理性，因此可能需要在这方面依赖独立专家的意见。

- 提供商酌情暂停服务

100. 提供商的标准条款可能载有提供商可随时酌情暂停服务的权利。客户可能希望限制这种无附加条件的权利，除明确限定的情形外（例如，客户根本违反合同，如不付费），不允许暂停服务。“不可预见的事件”是提供商单方面暂停服务的一个常见理由。这些事件的定义范围通常很宽，涵盖任何超出提供商控制范围的障碍，包括分包商、分提供商和其他参与向客户提供云计算服务的第三方（如互联网提供商）发生的故障。

101. 客户可以考虑对由于不可预见的事件造成暂停的权利附加条件，要求提供商适当执行一项业务连续性和灾难恢复计划。合同可以要求这类计划包含防范对提供云计算服务共同威胁的措施并将计划提交客户征求意见和核准。这些防范措施可以包括在另一地域分设一个能够无缝转换的灾难恢复站点，并使用不间断电源和备用发电机。

- 变更通知

102. 提供商的标准条款可能不载列提供商向客户通知服务条款变更的义务。客户可能需定期查看提供商网站上公布的合同文件是否有任何实际变化。这些合同文件可能是多种多样的；有些文件可能以提及方式纳入载于其他文件的条款和政策，而这些文件可能以提及方式纳入补充条款和政策，所有这一切都可能由提供商单方面修改。因此，客户要想注意到提供商所作的改动可能并非易事。

103. 由于客户继续使用服务被视为接受经修改的条款，客户似宜在合同中列入一项义务，要求提供商在修改生效之前将服务条款变更事宜充分提前通知客户。合同还可以要求提供商为客户提供对服务变化过程审计记录的访问权。客户还似宜保存所有商定条款，并要求提供商以提及某一特定版本或版次的方式界定所提供的服务。

H. 分包商、分提供商和外包

- 确定分包链

104. 分包、**分层云计算服务**和外包是常见的**云计算**业务模式。提供商的标准条款可能明确保留提供商使用第三方向客户提供云计算服务的权利，或者因为所提供服务的性质，这项权利可能是默示性的。提供商可能有意尽可能多保留这方面的灵活性。

105. 在合同中确定参与向客户提供云计算服务的第三方，可能是法律要求的，也可能有利于客户实现核证目的。客户将特别希望就第三方遵守合同或者法律所规定的安全、保密、数据保护及其他要求，就不涉及利益冲突以及就提供商由于第三方故障无法履行合同的风险寻求保证。尽管提供商并非总能指明所有参与向客户提供云计算服务的第三方，但其应当能够指明那些发挥关键作用第三方。

- 分包链变化

106. 合同可以禁止未经客户同意进一步改变分包链。合同可以规定客户有权对任何参与向客户提供云计算服务的第三方进行背景审查并予以否决。另一种办法是，合同可以列入客户预先核准的第三方清单，提供商可以在有需要时从中选择。

107. 不过，提供商可以坚持其单方面改变分包链的权利，而不论是否通知客户。客户可能希望保留允许提供商先做改变尔后需取得客户批准的权利。在未获此种批准的情况下，可以商定将由先前批准或者其他预先批准的第三方继续提供服务，或者由双方将商定的另一第三方继续提供服务；否则，可以解约。强制性适用法律可能规定，在哪些情况下，提供商分包链的改变可能要求解约。

- 合同条款与关联合同匹配

108. 虽然可在合同中列明有助于履行云计算合同的第三方，但它们并不是提供商与客户之间合同的当事方。它们将对各自与提供商的合同下的义务承担责任。尽管如此，存在着各种可确保提供商与客户之间合同的条款对这些第三方具有约束力的机

制。特别是，合同可以要求提供商使合同条款与现有或今后的关联合同相匹配。合同还可以要求提供商为验证的向客户提供关联合同副本。

109. 客户可以选择与有助于履行云计算合同的第三方直接订立合同，特别是就诸如保密和**个人数据处理**之类敏感问题订立合同。客户可能还需要与关键第三方谈判在提供商未能根据合同履约的情况下——包括提供商破产——的介入义务。

- 分包商、分提供商和其他第三方的责任

110. 根据适用法律或合同，对于提供商让其参与履行合同的任何第三方的责任范围内的任何问题，可以要求提供商对客户承担责任。特别是，法律可以根据分包商参与数据处理的程度，规定提供商及其分包商对**个人数据处理**所引起的任何问题承担连带责任。

111. 合同可以要求提供商在关联合同中为客户设定第三方受益人的权利，或者使客户成为关联合同的一方。这两个选项都将允许客户在第三方未根据关联合同履约的情况下对第三方享有直接追索权。

I. 赔偿责任

- 风险和责任分配

112. 在企业对企业交易中，双方按其认为适当的方式自由分配风险和责任，只要不违反适用法律的任何强制性规定即可。在进行风险和责任分配方案的谈判时要考虑到各种因素，例如，提供云计算服务所涉及的种种风险，提供云计算服务是为了取酬还是另有安排，提供商就云计算服务收取费用数额，等等。尽管双方一般倾向于排除或限制对其无法控制或控制程度有限的因素（例如，终端用户行为、分包商行动或不作为）的赔偿责任，但控制程度并非总是一个决定性考虑因素。一方准备对不受其控制的要素承担风险和责任，可能是为了使其在市场上与众不同。但很有可能的是，该方所承担的风险和责任是与受其控制部分成比例地逐渐增加的。

113. 例如，在涉及使用标准办公软件的“**软件即服务**”（**SaaS**）模式下，提供商很可能对提供给客户的几乎所有资源负责，每次发生这些资源不到位或者出现故障的情况，提供商可能都要承担责任。尽管如此，即使在这些情况下，客户可能仍然要对服务的某些部分负责，例如，在其控制下的数据的加密或备份。如果不能确保适当备份，一旦数据丢失可能导致丧失对提供商的追索权。另一方面，在“**基础设施即服务**”（**IaaS**）和“**平台即服务**”（**PaaS**）模式下，提供商仅对所提供的基础设施和平台（如硬件资源、操作系统或中间设备）负责，而客户将对所有属于客户的部分承担责任，例如，使用所提供的基础设施或平台及其中所含数据运行的应用程序。

- 排除或者限制赔偿责任

114. 提供商的标准条款可能排除合同下的任何赔偿责任，并采取赔偿责任条款不容谈判的立场。或者，提供商可能愿意接受对提供商的可控性违反事件（例如，违反客户准予提供商的知识产权许可）的赔偿责任，包括无限赔偿责任，但不愿意接受对由于超出提供商控制范围的原因可能发生的违反事件（例如，安全事件、不可预见的事件或者泄露机密数据）的赔偿责任。提供商的标准条款一般都排除对间接损失或连带损失（例如，云计算服务不到位导致丧失商业机会）的赔偿责任。

115. 如果一般接受赔偿责任或者对某些具体指明的情形接受赔偿责任，提供商的标准条款往往限制（按每起事件、每批事件或每段时期）赔付的损失金。此外，提供商往往规定合同赔偿责任上限，与之有关的可能是合同下预期得到的收入、提供商营业额或者保险范围。

116. 客户可能有意谈判对提供商或其人员的行为或不作为造成特定类型损害的无限赔偿责任或较高赔偿责任。除其他因素外，这样做的能力可能取决于**部署模式**[交叉链接]。客户数据丢失或者被滥用、个人数据保护被侵犯以及知识产权侵权行为尤其会导致客户对第三方的潜在高额赔偿责任，或者导致监管罚款。对由于提供商过失或疏忽造成的这些情形，可能有必要规定一种更严格的赔偿责任制度。提供商的无限赔偿责任还可能产生于法律规定的某些类别的缺陷（例如，有缺陷的硬件或软件）。

117. 提供商的标准条款通常对客户规定不遵守 **AUP 政策**的赔偿责任。客户可能希望限制因违反 **AUP 政策**，特别是因其无法控制的终端用户行为而产生的赔偿责任。

118. 可能需要在合同正文载入免责声明和责任限制条款并以适当方式告知对方，以便于执行。

- 赔偿责任保险

119. 合同可以包含双方或者其中一方的保险义务，特别有关的是对保险公司的质量要求以及所寻求的最低保险额。合同还可以要求双方通知保险范围的变更情况或者相互提供当前保险单副本。

- 法定要求

120. 虽然大多数法律制度一般都承认订约方有权通过合同条款分配风险和赔偿责任并且限制或者排除赔偿责任，但这种权利通常都附加各种限制和条件。例如，**个人数据处理**风险和赔偿责任分配方面的一个重要因素是，每一方对放入云中**个人数据**所承担的责任。在**个人数据**方面，许多法域的数据保护法律对**数据控制人**规定的赔偿责任比对**数据处理人**规定的赔偿责任更多。尽管有合同条款，但此类数据的实际处理方式一般将决定根据适用法律管辖订约方的法律制度。由于非法处理**个人数据**或者任何不符合国内数据保护条例的行为而遭受损失的**数据主体**或许有权直接从**数据控制人**获得赔偿。

121. 此外，在许多法域，完全排除对个人过失的赔偿责任是无法接受的，或者必须对此加以限制。也许不可能完全排除与人身伤害（包括生病和死亡）有关的赔偿责任，以及对于严重过失、故意伤害、缺陷、违反对于合同至关重要的核心义务或者不遵守适用的监管要求的赔偿责任。此外，如果合同条款不是自由谈判达成的，而是由其中一方规定或者预先确定的（“附合合同”），则某些类型的责任限制条款可能会被认为有“滥用性”并因此而归于无效[交叉链接]。

122. 公共机构承担某些赔偿责任的能力可能受到法律限制，或者公共机构需要事先征求国家主管机构同意才能这样做。还可能禁止公共机构接受完全排除或限制提供商的赔偿责任，或者禁止其接受排除或限制对于法律所定义的作为或不作为的赔偿责任。

123. 另一方面，适用法律可能规定，如果本来会面临赔偿责任风险的订约方满足了某些标准，可以免除责任。例如，根据某些法域的“通知后下架”程序，如果提供商一得知在其云基础设施上的非法内容即将其删除，提供商托管这些非法内容的责任将予以免除[交叉链接]。

J. 对违反合同的救济办法

- 救济种类

124. 在相关法律规定限度内，双方可以自由选择救济办法。救济办法可以包括旨在为受害方提供预期从履约获得的同样或者同等益处的实物救济（例如，更换有缺陷硬件）、金钱救济（例如，服务积分）和解约。合同可以对违约种类加以区分并规定相应救济。

- 暂停或终止服务

125. 暂停或终止向客户提供云计算服务是提供商对客户违约或者客户终端用户违反 **AUP 政策**的通常救济办法。客户将有意规定针对广泛暂停权或者终止权的合同保障。例如，提供商暂停或终止向客户提供云计算服务的权利可限于客户有重大违约行为的情形以及对提供商的系统安全或者完整性构成严重威胁的情形。提供商的暂停权或者终止权也可仅限于受违约影响的服务，这种可能性的确存在。

- 服务积分

126. 针对提供商不履约经常使用的客户赔偿机制是服务积分制度。这些积分采取的形式是，在接下来的一定时期内根据合同提供的服务减少收费。可以适用浮动费率，即减费百分比可能取决于提供商根据合同提供服务在多大程度上未达到**安全级别协议**或合同其他部分确定的绩效参数。还可以适用服务积分总上限。提供商可将给予服务积分的情形限制于某些情形，例如，由于提供商控制下事项引起故障，或者在一定时间内申领积分。有些提供商也可能愿意退还已付费用，或者在接下来的一定时期内增强服务包（例如，免费提供信息技术咨询）。如果存在一系列选项，提供商的标准条款通常规定由提供商选定对其不履约的任何救济办法。

127. 提供商需要在逐案基础上评估在合同中将服务积分定为对提供商未履行其合同承诺的唯一或全部救济办法是否合适。这样的规定可能会限制客户对其他救济办法的的权利，包括提起损害赔偿诉讼或者解约。客户可能有意在合同中规定减轻提供商不履约风险的其他措施，以及充分激励提供商认真履约并改进服务的措施。例如，罚款对提供商的财务影响可能比服务积分更大。此外，如果合同即将终止，在接下来的一定时期内减费或者增强服务包，这种形式的服务积分可能毫无用处。如果从合同一开始就认为过高服务积分是一种不合理的损害估算方法，则服务积分可能无法执行。

- 违反合同时应依循的程序

128. 合同可以包括违约情况下应依循的程序。例如，合同可以规定，一旦任何合同条款被视为违反，一方即应通知对方，并提供补救此种声称违约的机会。还可设定要求救济的时限。

K. 合同期和解约

- 合同开始生效日期

129. 合同开始生效日期必须在合同中明确规定。合同开始生效日期可能不同于签字日期、接受要约的日期，或者配置及客户云迁移所需采取的其他行动的验收日期。提供商向客户提供的云计算服务的到位日期可视为合同开始生效日期，即使客户还没有实际使用云计算服务。客户缴纳云计算服务第一笔费用的日期也可视为合同开始生效日期，即使提供商为客户提供的服务尚未到位。

- 合同期

130. 合同期可为短期、中期或长期。**标准化商用型多订户云解决方案**通常规定一个初始期（短期或中期），然后自动展延，除非任何一方终止合同。客户可以要求提供商通知客户合同即将期满和需要就展期作出决定。这一机制可能对客户努力避免锁定风险和错过更好交易有益。

- 提前解约

131. 合同将处理出于方便、违约或者其他原因而在合同固定期限期满之前解约的情形。合同可能需要规定提前解约的模式，包括关于充分提前通知、可逆性以及其他服务**终了**承诺的要求[交叉链接]。

为方便而解约

132. 提供商的标准条款，特别是**标准化商用型多订户云解决方案**的规定，通常保留提供商任何时候无需客户违约即可解约的权利。客户可能希望限制行使此种权利的情形，并要求提供商向客户发出充分提前解约通知。

133. 顾客为方便（即无需提供商违约）而解约的权利特别多见于公共合同。在这种情况下，提供商可以要求支付提前解约费。不过，公共实体支付提前解约费可能受到法律限制。在无限期合同中，提供商可能更倾向于接受客户仅为方便而解约，不要求赔偿，但也可能因此而导致合同提价。

因违反而解约

134. 重大违约通常是解约理由。为避免含糊不清，双方可在合同中界定双方视为重大违约的合同事件。对于客户来说，重大违约可以包括数据丢失或误用、个人数据保护侵权行为、重复性安全事件（例如，任何一段衡量期内发生的安全事件超过 X 倍）、泄密以及某一时间点或者某段时期未提供服务。客户不付费以及客户或其终端用户违反 **AUP 政策**是提供商解约的最常见理由。订约方的解约权可能有附加条件：发出事先通知、举行诚信协商、提供纠正状况的可能性，以及保证在采取补救行动后一定天数内恢复履行合同。

135. 合同可能需要涉及发生客户重大违约后如何兑现提供商作出的服务终了承诺。客户需要至少确保其数据及其他内容的**可逆性**[交叉链接]。

因合同修改不可接受而解约

136. 对合同不可接受、商业上不合理的修改或者对合同有实质性损害的单方面修改，都可以是解约理由。这些修改可能包括修改**数据本地化**要求或者分包条款。如果对合同的修改是因为重构提供商的服务组合并因此而导致终止或者更换一些服务，则合同可能特别需要保持客户终止整个合同的权利[交叉链接]。

破产时解约

137. 破产客户可能需要在解决其财务困难期间继续使用云计算服务。因此，客户可能有意限制提供商在客户没有合同规定的拖欠付款的情形时援用客户破产作为唯一解约理由的权利。

138. 提供商的破产风险可在风险评估期间加以确定。合同可以要求提供商向客户提交提供商财务状况定期报告，并规定，在提供商缺乏充分履行合同的财务能力时，客户有权解约而不承担进一步义务或责任。

139. 如果由于对提供商财务状况的信任危机而出现大规模撤出和撤离内容的情况，再也无法从破产提供商的云基础设施检索数据和其他内容的风险是很高的。破产提供商或**破产管理人**可以限制可在特定时间范围内撤出内容（数据和应用代码）的数量。还可以决定是否应在先来先得的基础上兑现服务终了承诺。因此，客户可能有意通过合同机制确保其能够从破产提供商检索其数据。客户可以请求提供源代码或托管密钥，提供商一旦破产即可自动发放，从而允许访问客户数据及其他内容。然而，破产法的强制性规定可以推翻合同承诺。

控制权变更时解约

140. 例如，控制权变更可能涉及所有权变更，或者涉及直接或间接决定提供商经营和财务政策的能力的变化，这又可能导致提供商服务组合的改变。控制权变更还可能涉及合同的转让或者更新，导致合同下的权利和义务或者只是合同下的权利转移给第三方。因此，合同原订约方可能发生变化，或者合同的某些方面（如付费）需要改为对第三方履行。

141. 合同可能需要要求提供商提前发出控制权即将变更及其对服务连续性预期影响的通知。如果提供商或者合同由于控制权变更而被客户的竞争对手接管，或者接管导致服务组合中断或者发生重大改变，客户可能希望保留其解约的合同权利，如果由于控制权变更而无法满足强制性法律要求（例如，**数据本地化**要求，或者禁止与置于国际制裁制度下的某些实体打交道，或者由于国家安全考虑禁止与某些实体打交道），适用法律可能要求终止合同。公共合同尤其可能受到控制权变更法定限制的影响。

闲置账户条款

142. 合同规定的某一时期内客户无活动，可以是提供商单方面解约的一个理由。不过，在为取酬而订立的企业对企业云计算合同中，即使存在这种闲置账户条款也极为罕见。

L. 服务终了承诺

143. 服务终了承诺不仅会引起合同问题，还会引起监管问题。合同需要兼顾客户利益和提供商利益，前者在于能够继续访问其数据和其他内容，包括在过渡期间，后者在于尽快结束对前客户的任何义务。

144. 服务终了承诺不论解约原因为何可能都是一样的，而根据解约是否因为违约或者其他原因则可能有所不同。双方可能需要在合同中处理的问题包括：

- 导出时限

145. 客户将希望有足够长的时间确保其能够将其数据和其他内容顺利转移到另一提供商或转回内部。

- 客户获取需导出内容

146. 合同需要指明需导出的数据和其他内容以及客户获取其访问权的方式，包括可能由提供商或者第三方持有的任何解密钥匙。双方可以商定托管办法，以确保客户自动获得导出所要求的所有属性。合同还可尽量列明导出选项，包括其格式和流程，同时需认识到它们可能随时间变化。

- 提供商协助导出

147. 可能需要在合同中具体规定云提供商参与将客户数据导出至客户或者客户所选择的另一提供商的程度、程序和时间期限。提供商可能要求为协助导出单独付费。在这种情况下，双方可以在合同中确定付费数额，或者商定参照提供商某一特定时间的定价表。另一种做法是，双方可以商定将这种协助计入合同价格，或者，提供商违约之后解约不额外收费。

- 从提供商的云基础设施删除数据

148. 合同可能需要具体规定导出完成后或者合同规定的导出期期满时从提供商的云基础设施删除数据和其他内容的规则。数据可以由提供商自动删除，也可以根据客户具体要求和指示自动删除。合同可以列入一项提供商的义务，即在删除数据之前应当提醒客户并向客户确认数据、备份和**元数据**已经删除。提供商可能有义务签发一份删除证明、报告或声明，其中包括从第三方系统删除数据。

- 合同结束后保留数据

149. 法律可能要求提供商保留客户数据，特别是数据保护法律，其中还可能涉及数据必须予以保留的期限。此外，客户可能允许提供商保留特定数据，或者希望提供商以合同方式保证在为监管、诉讼原因以及其他影响客户的法律原因终止合同后保留数据。有些提供商可能另外收费，让客户选择合同结束后的保留期。

150. 对于不退回或者无法退回客户的数据以及无法删除的数据，可能需要载明特殊要求（例如，个人信息去身份化）。合同需要具体规定，合同终止后按照什么格式保留数据。可采用客户核准的格式（加密和不加密格式），也可在合同中一般申明将按照可使用和可互操作的格式保留数据，以便于需要时检索。合同需要具体规定双方对于合同终止后按照特定格式保留数据的责任。

- 合同结束后的保密条款

151. 双方还可商定合同结束后保密条款。保密义务可以延续到合同终止之后，例如，合同终止后延续五到七年或者无限期延续，取决于置于提供商云基础设施中客户数据和其他内容的性质。

- 合同结束后的审计

152. 合同结束后的审计可以是双方商定的，也可以是法律规定的。合同需要具体规定进行此类审计的条款，包括时间范围和费用分配。

- 账上余款

153. 双方可能需要商定将其账上余款退还客户的条件，或者用这些余款抵消客户需付给提供商的任何额外费用（包括服务终了活动的额外费用）或者补偿损失的条件。

M. 争议解决

- 争议解决方法

154. 可取做法是，双方商定未来产生于合同的争议的解决方法。争议解决方法包括谈判、调停、调解、仲裁和司法程序。不同类型争议可能需要采取不同争议解决程序。例如，财务和技术方面的争议可诉诸第三方专家（个人或机构）有约束力的决定，而其他一些类型的争议可通过双方直接谈判更有效地处理。有些法域的法律可能规定了某些非诉讼争议解决机制，双方需要穷尽这些机制方可将争议提交国内法院。

- 仲裁程序

155. 争议未能以友好方式解决的，可以诉诸仲裁程序，前提是双方做出这样的选择。双方应核实诉诸裁决问题的可仲裁性（即诉诸仲裁裁决的问题是否已为国家保留为国内法院裁决的问题）。双方选择仲裁的，似宜商定一套管辖仲裁程序的仲裁规则。合同可以列入一个标准的争议解决条款，指明使用国际公认的规则进行争议解决程序（例如，《贸易法委员会仲裁规则》）。在没有这种规定的情况下，通常由程序进行地所在国的程序法管辖仲裁程序，或者，如果双方选择某一仲裁机构，由该机构的规则管辖。双方可以选择有一套自己规则的网上争议解决机制。

- 司法程序

156. 如果由于**云计算服务**的性质而进行司法程序，可能会有若干国家声称拥有管辖权。可能的话，双方可以商定一个管辖权条款，双方必须根据这一条款将争议提交某一特定法院[交叉链接]。

- 数据留存

157. 不论争议为何性质，合同应解决在一段合理时间内保留客户数据和其他内容以及客户对其访问权的问题。这对于客户可能很重要，不仅是因为需要确保业务连续性，而且还因为获取数据——包括**元数据**和其他**云服务衍生数据**——可能对于争议解决程序本身至关重要（例如，佐证一项请求或反请求）。

- 投诉时效期

158. 双方可能需要商定提出索赔的时效期。提供商往往对客户就服务提出索赔规定较短的时效期。这些条款如果违反了适用法律规定的强制性时效期可能无法执行。

N. 法律选择和诉讼地选择条款

159. 合同自由一般允许订约方选择其合同适用的法律并选择审议争议的管辖地或诉讼地。不过，强制性法律（如数据保护法）可以优先于订约方拟定的法律选择和诉讼地选择条款，视争议事项而定。此外，不论法律选择和诉讼地选择如何，可能有不止一项强制性法律（例如，数据保护法、破产法）适用于合同。

- 选择适用法律和诉讼地所涉及的考虑

160. 法律选择和诉讼地选择互有关联。所选定和商定的法律最终是否适用，取决于在哪个诉讼地向法院或者另一裁决机构（如仲裁庭）**出示**法律选择条款。该诉讼地的法律将决定这一条款是否有效以及该诉讼地是否尊重订约方所选择的适用法律。由于诉讼地的法律决定了法律选择条款的命运，载有此种条款的合同通常还包括一个诉讼地选择条款。

161. 在选择诉讼地时，订约方通常考虑所选择的适用法律或者其他适用法律的影响，以及在该诉讼地作出的司法决定将在多大程度上在寻求执行所在国得到承认和执行。保持执行选项灵活性可能是一项重要考虑，尤其是在**云计算**环境下，因为提供服务所涉资产的地点、提供商和客户的地点以及订约方在拟定法律选择和诉讼地选择条款时通常会考虑的其他因素可能都是不确定的。

- 强制性法律和诉讼地

162. 由于各种原因，某一特定法域内的法律和诉讼地可能是强制性的，例如：

(a) 在某国境内开通云计算服务，足可适用该国的数据保护法律；

(b) 受影响的**数据主体**或者订约方（特别是**数据控制人**）的国籍或者居住地可导致适用该**数据主体**或者该订约方的法律；以及

(c) 活动发端地（设备地点）的法律或者活动获利指向地的法律可导致适用该地法律。使用与某一特定地点关联的地理域名、提供商在其网站上使用当地语言、以当地货币定价以及当地联系点，都是作出此种判定时可能会考虑的因素。

- 提供商或客户所在国的法律和诉讼地

163. **标准化商用型多订户云解决方案**合同往往规定，由云提供商主要营业地或者机构所在地的法律管辖此类合同。这些合同一般准予该国法院对合同引起的任何争议的专属管辖权。客户可能倾向于指定本国的法律和管辖权。公共机构一般对其同意外国法律和管辖权的能力作出重大限制。在多个法域运作的提供商可能会对选择客户所在国的法律和诉讼地持灵活态度。

- 多选项

164. 订约方还可对合同的不同方面规定不同选项。订约方也可选择被告的管辖地，以消除所在国诉讼地给原告带来的优势，从而鼓励以非正式方式解决争议。

- 不选择法律或诉讼地

165. 一些订约方可能倾向于不在合同中列入法律或者诉讼地选择条款，这一问题留待日后需要时辩论和解决。这或许可以看作是某些情况下唯一可行的解决办法。

O. 通知

166. 通知条款将涉及通知的形式、语言、接收人和方式，以及通知何时生效（发出时、送达时或者确认收讫时）。在没有任何强制性法律规定的情况下，双方可以商定通知手续，通知手续可以是统一的，也可以根据重要程度、紧迫性和其他因素而有所不同。相较于例行通知，对暂停或者单方面解约等情形规定更严格要求并无不可。这种情况下的最后期限应考虑到**可逆性**以及客户业务连续性。合同可以提及法律规定的任何通知和期限。

167. 双方可以选择向合同中指明的联系人的实际地址或者电子地址发出**书面**通知。合同可以规定不予通知以及对要求答复的通知不予答复的法律后果。

P. 杂项条款

168. 订约方通常把不属于合同其他部分的规定放在杂项条款下。其中一些条款可能包含载于各类商业合同中的标准案文（所谓“样板条款”）。这方面的例子包括分离条款——即允许从合同其余部分去除无效规定，以及语言条款——即确定在各种语文文本的解释发生冲突时以合同的某一语文文本作准。合同条款置于杂项条款中并不削弱其法律重要性。订约方可能需要根据云计算的具体情况认真研究其中一些条款。

Q. 修正合同

169. 任何一方均可提出修正合同。合同将处理提出修正并使之生效的程序。合同可能还需要涉及任何一方拒绝接受修正所造成的后果。

170. 鉴于**云计算**的性质，可能难以区分构成合同修正的修改和不构成合同修正的修改。例如，客户使用从合同一开始就提供的任何选项并不一定构成对初始合同的修正，而由于合同所涵盖的提供商例行维护及其他活动而发生的服务变化也是如此。另一方面，如果增加的任何特性未在最初商定的条款中涵盖并因此需要调整价格，则构成对合同的修正。任何导致先前商定条款和政策发生实质性变化的更新也可构成对合同的修正。如果对最初订立的合同的实质性条款作出重大修改（例如，中断某些云计算服务），可以实际导致新的合同。

171. 公共合同可允许修改程度可能受公共采购规则的限制，即合同必须经过公开招标程序的，订约方重新谈判合同条款的自由通常受到限制。

172. 鉴于最初商定条款的频繁修改，每一方不妨各自单独存放一套完整的最初商定条款及其修正。

术语表

可接受的使用政策（AUP）——提供商与客户之间云计算合同中界定客户及其终端用户对合同所涵盖云计算服务使用范围的部分，例如，客户及其终端用户不得将任何非法或者其他被禁止内容放入云中或者使用此种内容[交叉链接]。

审计——审查合同要求和法定要求遵守情况的过程。审计还包括技术方面，如硬件和软件质量和安全；任何适用的业界标准；以及为防止擅自进入和使用系统并确保数据完整性而采取的适当措施，包括隔离。审计可以是提供商进行的内部审计、客户进行的外部审议，也可以是提供商或者客户分别指定或者双方共同指定的独立第三方进行的审计。

云计算——通过公开或封闭网络提供和使用**云计算服务**。**云计算**可具有以下特点：

(a) **广泛网络接入**，指可从任何提供网络（如通过互联网）的地点，使用各种装置（如移动电话、平板电脑和膝上型计算机等），在网络上利用**云计算服务**；

(b) **计量化服务**，指**云计算服务**的可计量交付，如同公用事业部门（供气供电部门等），允许监测资源使用情况并按用量收费（**随用随付**制）；

(c) **多租户安排**，指实体资源和虚拟资源分配给多个用户，用户数据彼此隔绝，互不连通；

(d) **按需自助服务**，指客户根据需要使用**云计算服务**，为自动服务，或者与提供商进行最低限互动；

(e) **弹性和伸缩性**，指根据客户要求——包括资源使用的大规模趋势（如季节性影响）——迅速调高或调低**云计算服务**消费量。弹性和伸缩性不仅涵盖服务的数量方面，还涵盖可能需根据所存储客户数据的不同敏感度加以调整的措施的质量和安全性；

(f) **资源集合**，指提供商能够在客户不控制或者不了解所涉过程的情况下为服务一个或多个客户而集聚实体资源或虚拟资源。

云计算服务——通过**云计算**提供的服务。云计算服务各有不同，不断演变。可包括提供和使用简单连接和基本计算服务（如存储、电子邮件和办公室应用程序等）。还可包括提供和使用所需要的全套信息技术实体基础设施（如服务器和数据中心）和虚拟资源，用以建立自己的信息技术平台或者部署、管理和运行由客户创建或者由客户获取的应用程序或软件。**基础设施即服务（IaaS）、软件即服务（SaaS）和平台即服务（PaaS）**是云计算服务的各种类型。

云计算服务伙伴（如云审计师、云服务经纪人或系统集成商）——参与支持或辅助提供商活动或客户活动或者两者活动的人。云审计师对提供和使用**云计算服务**的情况进行**审计**。云服务经纪人协助各方处理广泛问题，例如，找出正确的云解决办法，谈判可接受的条款，以及进行客户云迁移。

云服务衍生数据——客户使用提供商的云计算服务所产生的、处于该提供商控制之下的数据。包括**元数据**以及提供商所生成的其他任何记录，其中载有何人、何时使用服务以及所涉及功能和数据类型的记录。还可包括关于获授权用户及其身份标识、任何配置、定制和修改的信息。

数据控制人——确定**个人数据**处理目的和手段的人。

数据本地化要求——与数据和其他内容所在地或者数据中心或提供商所在地有关的要求。这些规定可能禁止某些数据（包括**元数据**和备份）在某个地区或法域**驻留**或者移入移出，或者要求事先就此取得国家主管机构批准。这些规定通常见诸于数据保护法律和条例，其中可能特别禁止**个人数据**在不遵守某些**个人数据**保护标准的法域驻留或者**中转**。

数据处理人——代表**数据控制人**处理数据的人。

数据主体的权利——与数据主体的**个人数据**关联的权利。法律规定的数据主体可享有对与其个人数据相关的所有重要事实——包括数据所在地、第三方使用情况以及数据泄露或其他数据泄密行为——的知情权。数据主体还可享有随时访问其个人数据的权利、清除其个人数据的权利（根据“被遗忘权”）、限制**处理**其个人数据的权利，以及对其个人数据**可移植性**的权利。

部署模式——根据实体资源或者虚拟资源的控制和共享情况对云计算采用的各种组织方式：

(a) **公共云**——**云计算服务**有可能提供给任何感兴趣的云服务客户，资源由提供商控制；

(b) **社区云**——**云计算服务**专门向某一有关联、有共同要求的客户群体提供支持，资源至少由该群体一名成员控制；

(c) **私人云**——专供单一客户使用的**云计算服务**，资源由该客户控制；

(d) **混合云**——使用至少两种不同云部署模式。

停机或中断——无法向客户提供云计算服务的时间。这段时间不计入**正常运行时间**或提供率。维护和升级时间通常计入停机时间。

第一反应时间——从客户报告事件到提供商初次作出反应的时间。

跟着太阳走——为更有效平衡资源与需求而将工作量分布在不同地域。这种模式的目的可能是提供昼夜服务并最大限度减少服务器与终端用户之间的平均距离，以减少**时延**，并最大限度提高数据从一台设备传输到另一台设备的速度（数据转移速度（DTR）或吞吐量）。

基础设施即服务（IaaS）——客户用以获得和使用加工、存储或网络资源的各类云计算服务。客户并不管理或控制基础实体资源和虚拟资源，而是对使用实体资源和虚拟资源的操作系统、存储或部署的应用程序进行控制。客户也可享有控制某些网络部件（如主防火墙）的有限能力。

破产代表——在破产程序中被授权管理受破产程序管辖的破产提供商资产的重整或清算的人或机构。

互操作性——两个或多个系统或者应用程序交换信息并相互使用所交换信息的能力。

知识产权许可证——知识产权所有人（许可人）与获授权使用这些知识产权的人（被许可人）之间的协议。这些许可证通常对被许可人或者第三方使用获许可财产的程度和方式规定各种限制和义务。例如，软件和虚拟内容（设计、布局和图像）的许可可能限于特定用途，不允许复制、修改或增强，并且限于某一特定媒介。许可证可能限于特定市场（如国家或（分）区域市场）和一定用户数量，也可能有时限。

可能不允许次级许可。许可人可能要求每次使用知识产权必须获得知识产权所有权人的授权。

时延——从客户角度看，从用户请求到提供商回应请求迟滞的时间。时延影响到**云计算服务**有多大实际功用。

分层云计算服务——提供商不是其用以向客户提供云计算服务的全部或者任何计算资源的所有人，但本身是全部或者部分**云计算服务**的客户。例如，**平台即服务（PaaS）**或者**软件即服务（SaaS）**类服务的提供商可以利用另一实体拥有或者提供的存储和服务器基础设施（数据中心、数据服务器）。因此，可能有一个或者多个分提供商参与向客户提供云计算服务。客户可能并不知道在特定时间提供的服务涉及哪一层面，这就使得难以确定和管理风险。**分层云计算服务在软件即服务（SaaS）**中特别普遍。

锁定——客户因切换到另一提供商的费用颇巨而依赖于单一提供商。这方面的费用应作最广义理解，不仅包括金钱方面的费用，还包括花费的努力和时间以及相关方面。在**软件即服务（SaaS）**和**平台即服务（PaaS）**中，应用程序和数据的锁定风险可能很高。数据可能以提供商云系统特有的格式存在，无法在其他系统上使用。此外，提供商可能在客户数据的组织方式上使用有专利的应用程序或系统，因此需要调整许可证条款才能在该提供商网络之外运作。**平台即服务（PaaS）**还可能有运行期锁定，因为运行期（即为了支持用特定编程语言编写的计算机程序的执行而设计的软件）往往定制程度极高（例如，分配或者释放记忆、调试等方面）。**基础设施即服务（IaaS）**的锁定各不相同，取决于基础设施服务的具体消费情况，但是，如果依赖于具体政策特征（如访问控制），还有可能导致应用程序锁定，或者，如果有更多数据迁移到云中存储，可能导致数据锁定。

元数据——关于数据的基本信息（如作者、何时创建数据、何时修改数据以及文件大小）。元数据使得数据寻找和使用更加容易，随着时间推移可能需要元数据确保记录真实性。客户或者提供商均可生成元数据。

平台即服务（PaaS）——客户用以在云中部署、管理和运行客户创建的或者客户获取的应用程序的各类**云计算服务**，应用程序使用一种或数种现有编程语言和提供商支持的执行环境。

绩效参数——数量方面参数（数字指标或度量，或者绩效范围）或者质量方面参数（服务质量保证）。绩效参数可以参照与适用标准的符合度，包括任何符合度核证到期日。为求实效，绩效参数着眼于衡量对客户具有重要意义的绩效，并应以方便和可审计的方式进行衡量。绩效参数可能各不相同，取决于所涉风险和业务需要（例如，某些数据、服务和应用程序的关键性，以及恢复的相应优先性）。例如，旨在为存档目而使用云的非任务型关键系统，将不需要与任务型关键操作或实时操作相同的**正常运行时间**或其他**服务级别协定**条款。

数据存储持久性——云中存储的的数据不会在合同期间丢失的可能性。可在合同中将数据存储持久性表述为一种可衡量的指标，客户将据此衡量提供商为确保数据存储持久性所采取的步骤。

个人数据——可用来确定此种数据所涉自然人身份的数据。在一些法域，个人数据定义可能包含与身份已识别或者身份可识别个人（**数据主体**）直接或者间接关联或者相关的任何数据或者信息。

[个人数据]处理——数据收集、记录、整理、存储、改编或者改变、检索、咨询、使用、披露（通过传输、传播或者以其他方式提供）、匹配或者组合、封锁、清除或者销毁。

可移植性——从一个系统向另一个系统方便地（即低费、最少干扰、无需重新输入数据、重新设计流程或者重编应用程序）转移数据、应用程序和其他内容。如果能够以另一系统接受的格式检索数据，或者能够使用通用工具通过简单、直接转换检索数据，即有可能实现可移植性。

事件发生后的步骤——提供商或者客户或者双方在发生安全事件后采取的措施，包括让第三方参与。这些步骤可以包括隔绝或者隔离受影响区域、进行事件根源分析，以及由受影响方或者协同另一方、或者由独立第三方编写事件分析报告。

恢复点目标（RPO）——容许由于恢复而丢失数据更改的服务意外中断之前的时间极限。如果合同将**恢复点目标（RPO**）定为服务中断前两小时，这就意味着可以在恢复后以中断发生前两小时这个时间点存在的形式检索所有数据。

恢复时间目标（RTO）——意外中断后必须恢复所有云计算服务和数据的时间框架。

可逆性——客户从云中检索其数据、应用程序和其他相关内容的过程和提供商在商定期限后删除客户数据和其他相关内容的过程。

软件即服务（SaaS）——客户用以在云中使用提供商应用程序的各类**云计算服务**。

特定部门条例——金融、卫生、公共部门条例或者其他具体部门或者行业条例（例如，律师－委托人特权、医疗专业保密）以及机密信息处理规则（广义理解为法规条例规定限于特定类别人士访问的信息）。

安全事件通知——发给受影响方、国家机关或者广大公众的安全事件通知。可包括事件的情况和原因、受影响数据类型、解决事件所采取的步骤、事件预期得到解决的时间，以及解决事件期间采用的任何应急计划。还可包括关于未遂泄密行动、针对特定目标（每一客户用户、每一具体应用程序、每一具体实体机器）的袭击、趋势和统计数据的信息。

服务级别协议（SLA）——提供商与客户之间云计算合同中确定合同所涵盖的云计算服务和应当如何交付云计算服务（**绩效参数**）的部分[交叉链接]。

标准化商用型多用户云解决方案——按不可谈判的提供商标准条款作为海量产品或商品提供给无限数量客户的**云计算服务**。关于提供商的赔偿责任，这种解决方案普遍包含广泛的免责声明放弃条款。客户能够比较不同提供商及其合同并从市场上现有提供商中选出最适合自己需要者，但客户不能谈判合同。

正常运行时间——云计算服务可访问和可使用时间。

书面或者书面形式——信息必须可访问以便日后查询时可使用。包含纸面信息和电子通信信息。“可访问”指计算机数据形式的信息应为可读和可解释的，还指使这种信息可读所必需的软件应加以保留。“可使用”涵盖人的使用和计算机处理。