关于云计算合同所涉主要问题的说明

（联合国国际贸易法委员会秘书处编拟，2019年）

联合国

可向贸易法委员会秘书处索取进一步资料：

UNCITRAL secretariat, Vienna International Centre
P.O. Box 500, 1400 Vienna, Austria

电话：(+43-1) 26060-4060　　传真：(+43-1) 26060-5813
网址：uncitral.un.org　　电子邮件：uncitral@un.org

联合国国际贸易法委员会

关于云计算合同所涉主要问题的说明

（联合国国际贸易法委员会秘书处编拟，2019年）

联合国
2019年，纽约

前言

根据加拿大的建议(A/CN.9/823、A/CN.9/856)、第四工作组(电子商务)进度报告和秘书处的口头报告,[1]贸易法委员会在2014年至2017年分别举行的第四十七届至第五十届会议上审议了关于云计算所涉合同方面的专题。在这些会议上,贸易法委员会请秘书处和工作组就这一专题开展准备工作。[2]

在工作组第五十五届会议(2017年4月24日至28日,纽约)上根据秘书处的说明(A/CN.9/WG.IV/WP.142),并在工作组第五十六届会议(2018年4月16日至20日,纽约)上根据由专家提供投入——包括在秘书处于2017年11月20日和21日在维也纳召开专家组会议期间由专家提供的投入——编写的云计算所涉合同方面清单草案(A/CN.9/WG.IV/WP.148),工作组详细审议了这一专题。继委员会第五十一届会议决定在出版前审查秘书处编写的关于云计算合同所涉主要问题的说明草案之后,[3]贸易法委员会在2019年第五十二届会议上核准作为秘书处的说明,以在线参考工具以及纸质和电子小册子的形式,以联合国六种正式语文出版经该届会议修订的说明。[4]

本出版物转载贸易法委员会核准于2019年出版的《关于云计算合同所涉主要问题的说明》。

[1]《大会正式记录,第六十九届会议,补编第*17*号》(A/69/17),第150段;同上,《第七十届会议,补编第*17*号》(A/70/17),第358段;同上,《第七十一届会议,补编第*17*号》(A/71/17),第229段。

[2]同上,《第七十一届会议,补编第*17*号》(A/71/17),第235、353段;同上,《第七十二届会议,补编第*17*号》(A/72/17),第127段。

[3]同上,《第七十三届会议,补编第*17*号》(A/73/17),第150段。

[4]同上,《第七十四届会议,补编第*17*号》(A/74/17),第151段。

目录

导言

1. 本《说明》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《说明》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《说明》范围之内。

2. 云计算合同可根据适用法律定性为服务合同、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作出规定或者规定含糊不清，订约方本人可将合同定性为某一类型的合同；在对合同条款作出解释时，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《说明》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**公共云**、**社区云**、**私人云**或**混合云**）和付费条款（有无报酬）。《说明》主要侧重点是提供**软件即服务(SaaS)**类型公共付酬云计算服务的合同。

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。尽管《说明》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无益处。

5. 各方不应将《说明》视为起草云计算合同方面详尽无遗的资料来源，也不应以此替代专业顾问的任何法律和技术咨询和服务。《说明》提出供潜在订约方在起草合同之前和期间应当考虑的问题，包括对安全问题的共同责任，但本意并非表示所有这些问题都必须加以考虑。《说明》中所讨论的各种解决方案将不会管辖订约方之间的关系，除非订约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。《说明》中使用的标题和小标题及其序列不应视为硬性要求，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、风格和结构可能迥异，反映出各种不同的法律传统、起草风格、法律要求以及订约各方的需要和偏好。

6. 最后，《说明》并非意在表示联合国国际贸易法委员会（贸易法委员会）或其秘书处对于订立云计算服务合同可取性的立场。

7. 《说明》由两个部分和术语表组成：第一部分述及潜在订约方在订立云计算合同之前似宜考虑的订约前主要方面；第二部分述及谈判各方起草云计算合同时可能面临的主要合同问题；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、提供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**。订约方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**、消费者保护、网络安全、出口管制、海关、税务、商业秘密、特定知识产权和**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内容无效或无法执行、行政罚款和刑事责任等。

9.　订立云计算合同的条件可能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。它们还可能包括**数据本地化存储要求**以及对提供商的要求。

数据本地化存储

10.　**数据本地化存储要求**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，以及可能限制对某些信息或软件移入移出特定国家或区域的出口管制法律和条例。遵守适用法律中规定的**数据本地化存储要求**对于订约各方至关重要。合同不能推翻这些要求。

11.　**数据本地化存储要求**还可能产生于合同承诺（例如，要求将特许内容存储于用户个人的保密服务器的**知识产权许可**）。可能纯粹出于

实际原因而倾向于**数据本地化存储**，例如，减少**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。(关于合约要求的数据本地化存储保障措施，见第二部分，第74–75、78段。)

订约方的选择

12. 除市场条件外，订约方的选择可能受到法定要求的限制。法律可能禁止与外籍人员、某些法域人员或未取得国家主管机关认可/核证的人员订立云计算合同。可能要求外籍人员为在某一法域提供**云计算服务**与本国实体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。**数据本地化存储要求**（见上文第10–11段）以及每一方向外国国家机关披露数据及其他内容或提供其访问权的法定义务也会影响到订约方的选择。

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的一项先决条件。即使没有法定要求，订约双方亦可决定进行风险评估，这可能有助于他们确定减少风险战略，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是云业务特有的。有些风险将在云计算合同以外加以处理（例如，网络连接中断所引发的风险），而且并非所有风险都能够以可接受的费用减轻（例如，名誉损失）。此外，风险评估不是订约前的一次性活动。风险评估可能会在整个合同期间持续进行，风险评估结果出来后可能要求修正或终止合同。

核实关于特定云计算服务和所选订约方的信息

15. 当订约方考虑采用某项**云计算服务**和选择订约方时，以下信息可能与订约方相关：

(a) 使用特定云计算服务所需要的**知识产权许可证**；

(b) 所确立的隐私、保密和安全政策，特别是关于防止在使用云计算基础设施进行处理、中转或转移期间擅自获取、使用、翻改或销毁数据的政策；

(c) 所建立的确保持续获取**元数据**、审计记录以及显示安全措施的其他记录的措施；

(d) 发生泄密或系统故障时的现有灾难恢复计划和通知义务；

(e) 所确立的关于云迁移和服务终了援助以及**互操作性**和**可移植性**的政策；

(f) 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；

(g) **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；

(h) 独立第三方进行技术标准合规情况核证；

(i) 表明独立机构审计经常性和范围的信息；

(j) 财务可行性；

(k) 保险合同；

(l) 可能的利益冲突；

(m) 分包和**分层云计算服务**的范围；

(n) 数据及其他内容在云计算基础设施中的隔离程度；以及

(o) 订约双方对采取安全措施的预期分工和共同职责。

知识产权侵权风险

16. 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，即使为备份目的而在云上存储内容可能也会定性为复制，要求事先取得知识产权所有人的授权。

17. 为了双方的利益，应在订立合同之前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极高。可能需要就次级许可做出安排，或者可能需要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。

数据安全、完整性、保密和隐私方面的风险

18. 数据全部或部分迁移到云中会导致客户失去对该数据的专属控制，无法部署必要措施来保证数据的完整性和机密性，也无法验证数据处理和留存是否得到充分处置。失控程度将取决于**云计算服务**的类型。

19. 诸如**广泛网络接入**、**多租户安排**和**资源集合**等**云计算服务**的固有特性可能要求各方采取更多防范措施，以防止拦截通信和其他网络攻击，这可能导致云计算服务访问证书丧失或受损、数据丢失以及其他安全漏洞。在云计算等共享环境中，充分隔绝资源和隔离数据以及强大的安全程序尤为重要。

20. 无论采用何种云计算服务，安全措施都将是云计算环境中双方的共同责任。订约前风险评估为双方提供了良好机会，可籍此消除在界定双方与数据安全、完整性、保密和隐私相关的作用和职责方面的任何模糊之处。合同条款将发挥的重要作用是，反映双方就提供云计算服务的这些方面及其他方面彼此分担风险和责任达成的协议（见第二部分，第125–137段）。这些条款不能凌驾于强制性法律条款之上。

渗透测试、审计和实地考察

21. 可在订约前阶段采取步骤，对资源隔绝和数据隔离、身份识别程序以及其他安全措施是否充分进行核证。这些步骤应当着眼于查

明各方可能还需采取哪些可能的补充措施，以防向客户提供云计算服务出现数据安全漏洞及其他故障。

22. 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法定的**数据本地化存储要求**（见上文第10–11段）。双方需商定开展这些活动的条件，其中包括时间安排、费用分担以及对这些活动可能造成的任何损失的补偿。

锁定风险

23. **锁定**风险通常由于缺乏**互操作性**和**可移植性**而产生，避免或减少这种风险是双方的最重要考虑之一。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。

24. **软件即服务(SaaS)**和**平台即服务(PaaS)**中的应用程序和数据锁定风险尤其高。数据可能以某一云系统特有的格式存在，而这种格式不能在其他系统中使用。此外，组织数据所使用的专有应用程序或系统可能要求调整许可条款才能在另一不同网络中操作。与应用程序编程接口(API)交互的程序可能需要重写，以考虑到新系统的API。还可能由于需要重新培训终端用户而产生很高的转换成本。

25. **平台即服务(PaaS)**中还可能存在运行时锁定，因为运行时（即为支持执行用特定编程语言编写的计算机程序而设计的软件）通常是高定制的（如记忆分配或释放、调试等方面）。**基础设施即服务(IaaS)**中的锁定因所使用的特定基础设施服务而不同。同平台即服务一样，一些基础设施服务如果依赖于某一政策特征（如访问控制）有可能导致应用程序锁定。如果有更多数据移入云中存储，一些基础设施服务也可能导致数据锁定。

26. 在订约前阶段，可以为验证数据及其他内容是否能够被导入另一系统并可在该系统上使用而进行测试。云平台与内部平台之间可能需要同步，还可能需要异地复制数据。与不止一方进行交易并选择组合各类型的**云计算服务**及其**部署模式**（即多来源），即使可能会

造成费用及其他影响，可能不失为防范**锁定**风险的缓减战略的一个重要部分。合同条款也可有助于减轻锁定风险（见第二部分，特别是第84–86段和144段）。

业务连续性风险

27. 双方可能担心业务连续性风险，不仅预期合同按预定时间终止，而且预期合同可能单方面暂停或提前终止，包括其中一方可能不再经营。法律可能要求提前确立一种确保业务连续性的适当战略，主要是为了避免终止或暂停云计算服务给终端用户造成不利影响。合同条款也可有助于减轻业务连续性风险（见第二部分，第109–111、114–115、153、173、182段）。

撤出战略

28. 为确保撤出战略成功，双方可能需要从一开始就明确以下几点：*(a)*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**）；*(b)*为能够在另一系统使用该内容而要求对**知识产权许可**作出的任何修改；*(c)*对解密钥匙及其使用权的控制；*(d)*完成撤出所需时间。服务终了合同条款通常反映双方就这些问题达成的协议（见第二部分，第157–167段）。

C. 其他订约前问题

披露信息

29. 适用法律可能要求订约双方相互提供信息，使对方能够就订立合同作出知情选择。如果订立合同之前没有向对方明确传达使义务对象被确定或可以被确定所必需的信息，或此种传达不充分，将使合同或其中的部分内容归于无效，或使受侵害方有权提出损害赔偿。

30. 有些法域可能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本身有任何不匹配之处。双方还需处理的关切是，订约前披露信息给合同执行阶段的灵活性和创新带来的影响。

保密

31. 订约前阶段披露的信息可能被视为机密信息，特别是关于安全、身份识别和认证措施、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本国或外国国家机关对数据的访问权）。双方可以商定，订约前阶段披露的某些信息应作为机密信息对待。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

32. 在云迁移之前，通常预期客户会对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。还可能预期客户为所提供的服务（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）而向提供商提供其他必要信息。

33. 除了将数据及其他内容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。这些方面可以是客户与提供商合同的一部分，或是客户与提供商或第三方（如**云计算服务伙伴**）单独协议的事项。可能会产生额外费用。参与迁移各方通常商定各自在迁移期间的作用和职责、参与条件、数据或其他内容迁入云中拟使用的格式、迁移时间、确认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

34. 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。对合同自由的限制可能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，或者产生于制裁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内容不可执行以及承担民事、行政或刑事责任。

合同的成立

35. 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要约而必须满足的某些条件（例如，该提议应在所涵盖的云计算服务和付费条款方面具有足够确定性）。

36. 接受要约的承诺生效，即为订立合同。可能有不同的承诺机制（例如，对客户来说，点击网页上的选择框，网上登记云计算服务，开始使用云计算服务或支付服务费；对提供商来说，开始或继续提供服务；对双方来说，网上[1]或书面签署合同）。对要约的重大修改（例如，

[1] 关于贸易法委员会有关电子签名的法规，见《联合国关于在国际合同中使用电子通信的公约》（2005年，纽约）、《贸易法委员会电子商务示范法》（1996年）和《贸易法委员会电子签名示范法》（2001年）。另见贸易法委员会秘书处编写的解释性案文，标题为“增进对电子商务的信心：国际使用电子认证和签名方法的法律问题（2007年）”，查阅网址：https://uncitral.un.org/en/texts/ecommerce。

关于赔偿责任、云计算服务质量和数量或付费条款的修改）可构成反要约，需由对方接受方为订立合同。

37. **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，或余地极少。点击“我接受”、“好的”或“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

38. 云计算合同一般在网上订立。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)**、数据处理协议或数据保护政策、安全政策和许可协议等。

39. 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，为便于参考并为合同的明确性、完整性、可执行性和有效性起见，订约方仍然可能决定以**书面**方式订立合同并将所有附属协议纳入其中。

40. 适用法律可能为特定目的（如税收目的）而要求在纸张上签署合同，不过在日趋无纸化的环境中鲜有此类要求。

定义和术语

41. 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。合同可以列入术语表，也可以列入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。

合同基本内容

42. 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续订条件；*(e)*确定违约补救办法和免责情形；及*(f)*指明终止合同的效力。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。合同内容、风格和结构可能迥异，反映出各种不同的法律传统、起草风格、法律要求以及订约方的需要和偏好。

B. 订约方身份识别

43. 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。适用法律会就确定企业实体法律人格及其订立合同的能力所需要的信息作出具体规定。法律可能要求为特定目的提供其他信息，例如，为税收目的提供身份识别号码或委托书，以确定自然人是否拥有代表法律实体进行签署和作出承诺的权力。

C. 界定合同范围和合同标的

44. 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。单项合同期内的标的可能发生变化：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。

45. 合同标的说明通常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)**或这些服务的组合）及其**部署模式**（**公共云**、**社区云**、**私人云**或**混合云**）、技术特点、质量特点和绩效特点以及任何适用标准的说明。组成合同的若干文件可能与确定合同标的有关（见上文第38段）。

服务级别协议

46. **服务级别协议(SLA)**载明**绩效参数**，将据此衡量云计算服务交付情况、合同义务范围以及提供商的可能违约。信息技术专家通常参与制定**绩效参数**。

47. 数量方面的绩效参数通常与载量（可供运行程序使用的规定数据存储量或规定记忆量）、**宕机时间**或**中断时间**、**时延**、**数据存储持久性**、**正常运行时间**、支持服务（例如，在客户营业时间内或每周7天每天24小时）以及事件和灾难管理和恢复计划有关。后面一项可包括解决事件的最长时间、最长**第一反应时间**、**恢复点目标**和**恢复时间目标**。

48. 质量方面的绩效参数可能与**数据删除**、**数据本地化存储要求**、**可移植性**、安全以及数据保护/隐私有关。某些服务方面可根据质量和数量方面的绩效参数衡量。例如，**弹性**和**伸缩性**可参照规定最短期限内可用资源最大量以及措施的质量和安全性加以界定，就后者而言，可能需调整措施使之适合所存储客户数据的不同敏感度。加密可表述为闲置、中转和使用时的一定位值。除了用数量参数衡量之外，或者如果不用数量参数衡量，还可以参照质量参数衡量加密情况（例如，提供商应确保，任何时候客户数据经由公开通信网络传输，以及任何时候客户数据在提供商所使用的数据中心处于闲置状态，这些数据都是加密的）。

49. 可以商定不同承诺（即保证结果的义务或保证最佳努力的义务），这主要取决于付费条款以及是否提供**标准化商用型多订户云解决方案**。承诺的类型将产生影响，包括对发生争议时的举证责任产生影响。

绩效测量

50. 订约方可在合同中列明测量方法和程序，特别是具体指明服务测量的参照期（每日、每周、每月）、服务交付报告机制（即此种报告的频度和形式）、订约方的作用和职责，以及所使用的计量数据（即服务提供点的计量数据或服务消费点的计量数据）。订约方可商定独立测量绩效的方法以及如何分担相关费用。

51. 客户通常希望测量高峰时段——即最需要服务时段——的服务情况。客户一般有能力进行测量（或核实提供商或第三方提供的测量

数据），但仅限于那些基于消费点绩效的计量数据，而不是那些基于服务提供点系统绩效的计量数据。客户或许有能力根据提供商或第三方提供的报告评估服务提供点的绩效。提供商可能同意根据客户要求为其提供绩效报告，或定期提供（每日、每周、每月等），或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级别测量相关记录的权利。有些提供商支持顾客实时监测服务绩效数据。

52. 合同可以要求双方在一定时间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

53. **可接受的使用政策(AUP)**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，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**的一系列一贯性活动，绝大多数标准的**可接受的使用政策(AUP)**都予以禁止。**可接受的使用政策(AUP)**不仅可限制允许放入云中的内容种类，还可限制客户准许第三方（即某些国家的国民或列入制裁名单的个人）访问云中数据及其他内容的权利。订约方可同意取消某些禁令以顾及客户的特定业务需要，但以法律允许取消此种禁令为限。

54. 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**可接受的使用政策(AUP)**，并要求客户必须尽其最大努力或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使用或不当使用合同下所提供的云计算服务。订约方可以约定一些有限的义务，例如，客户向已知终端用户传达**可接受的使用政策(AUP)**，不授权或者不故意允许此种使用，并向提供商通知客户所了解的一切未经授权的使用或不当使用。

55. 在一些法域，法律可能就提供商在其云计算基础设施上托管的内容对其规定一些义务，例如，向公共当局报告非法材料的义务。此等义务不可通过**可接受的使用政策(AUP)**或其他方式转移给客户或终端用户。这些义务可能涉及隐私及其他影响，将是选择适当提供商时所考虑的因素之一（见第一部分，第12段）。

安全政策

56. 系统安全，包括客户数据安全，涉及订约双方的共同责任。合同需要具体指明订约双方对安全措施的分工和职责，以反映强制性法律对其中一方或双方规定的义务。

57. 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达成协议，不过这不包括**标准化商用型多订户云解决方案**。合同可以具体规定安全措施（例如，对受损媒介数据杀毒或删除的要求、在不同地点存储单独成套数据的要求、在客户独有的规定硬件上存储客户数据的要求）。不过，在合同中过度披露安全信息可能会有风险。

58. 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义务或评估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通知变更情况，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告知将分配给每一类数据的安全级别。

59. 一些安全威胁可能超出客户与提供商之间的合同框架，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

60. 提供商的标准合同可载有一般免责声明，即保全客户数据完整性的最终责任在于客户。

61. 有些提供商可能愿意作出数据完整性承诺（例如，定期备份），这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获取其数据至少一份可用复制件的访问权，此种访问权是在提供商及其分包商的控制、触及或影响范围之外，且独立于提供商及其分包商的参与。

保密条款

62. 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。有些提供商可能没有能力提供保密或不披露条款，并可能明确放弃对客户数据的任何保密义务。有些提供商可能愿意对客户在合同谈判期间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责任。提供商的一些标准保密条款可能不足以确保遵守适用法律。

63. 在没有关于提供商保守机密的合同承诺和法定义务的情况下，客户可能要对数据保密（例如，通过加密）承担全部责任。如果不可能谈判一项适用于放入云中所有客户数据的一般保密条款，订约双方可以就某些敏感数据商定保密承诺（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对第三方承诺必须保密的信息。订约双方可以商定限制此种数据的访问权，只允许有限人员接触此种数据，同时要求这些人员作出个人保密承诺，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）。在这些情况下，客户通常向提供商具体指明此种信息、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，包括适用法律的任何变化。

64. 在有些情况下，披露客户数据可能是履行合同所必需的。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（见下文第82段）。因此，保密条款是可以有适当例外情形的。

65. 反之，提供商可能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/隐私政策或数据处理协议

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

67. 合同可以包括一个数据保护或隐私条款、数据处理协议或类似协议，不过一些提供商可能仅同意对所适用的数据保护法律的一般遵守义务。在一些法域，这种一般承诺可能还不够：合同需要至少规定所涉事项和期限、**个人数据处理**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。如果不可能在合同中谈判一项数据保护条款，客户似宜审查标准条款，以确定相关规定是否给予客户对合法**个人数据处理**的充分保障以及适当的损害补救办法。

68. 客户很有可能就是**数据控制人**，将对云中收集和处理的**个人数据**承担遵守数据保护法律的责任。订约双方可以商定旨在遵守适用的数据保护条例——包括与**数据主体的权利**有关的请求——的合同条款。双方还可以商定一旦违反这些条款时的单独补救办法，其中包括单方面解约以及赔偿损失。

69. 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。只有当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时，提供商才有可能作为**数据处理人**行事。但是，在有些

法域，不论合同条款如何规定，如果提供商为自身目的或按照国家机关的指示进一步处理数据，就可被视为**数据控制人**，并可能因此而在这种进一步的**个人数据处理**方面对保护**个人数据**承担全部责任(见下文第125段)。

数据泄密及其他安全事件所产生的义务

70. 订约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，这可能是法律或合同要求的，(也可能是两者同时都要求的)。可在法律可能规定的**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或公共大众)，以防止或尽量减轻安全事件的影响。

71. 法律可能载明具体的安全事件通知要求，包括通知时间，并确定负责遵守这些要求的人。在不违反这些强制性规定的前提下，双方可在合同中具体规定通知期 (例如，一方得知事件或威胁后一天内)以及安全事件通知的形式和内容。后者通常包括各种情形和事件原因、受影响数据类型、解决事件拟采取的步骤、预期事件得到解决的时间，以及解决事件期间拟采用的任何应急计划。这方面还可包括关于未成功泄密行动、针对特定目标 (特定客户用户、特定应用程序、特定物理机) 的攻击、趋势和统计数据的信息。任何通知要求通常都考虑到不披露任何可能导致受影响方系统、业务或网络受损的敏感信息的必要性。

72. 法律或合同可能要求提供商或客户或者要求这两者，包括在有第三方参与的情况下，在安全事件后采取措施 (所谓“事件后步骤”)，其中包括隔绝或隔离受影响区域、进行根源分析并出具事件分析报告。事件分析报告可由受影响方或由受影响方会同另一方出具，也可由独立第三方出具。事件后步骤可能因云中存储的数据种类以及其他因素而不同。

73. 严重安全事件如造成客户数据丢失等情况可能导致终止合同。

数据本地化存储要求

74. 提供商的标准条款可能明确保留提供商在其运营地或其分包商运营地的任何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以是远程的，并可按照“**跟着太阳走**”的全球模式提供支持）。这种做法可能不符合适用于一方或双方的**数据本地化存储要求**（见第一部分，第10–11段）。

75. 可在合同中包括确保遵守**数据本地化存储要求**的保障措施，例如，禁止将数据及其他内容移出规定地点，或要求事先取得另一方对此种转移的批准。举例来说，可以列入**服务级别协议(SLA)**的质量绩效参数，以确保唯一存储客户数据（包括其任何复件、**元数据**和备份）的数据中心实际位于合同中指明的法域并且由在这些法域建立的实体拥有和运营。还比如说，参数可以具体规定，永远不得将数据移出某国或某区域，但可在一特定第三国或其他地方复制，但永远不得在某国复制。

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

76. 提供商通常在“需要知道”的基础上保留访问客户数据的权利。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**可接受的使用政策(AUP)**、**知识产权许可**、**服务级别协议(SLA)**和其他合同文件合规情况而需要时访问客户数据。订约双方可以商定准予提供商对客户数据访问权的情形以及确保客户数据保密性和完整性的措施。

77. 通过要求提供某项服务或性能，可以认为客户默示准予提供商对客户数据的某些访问权：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，如果分包商想要处理客户数据，提供商必须能够向其转移数据。

78. 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的权利的地域范围和时间范围。当数据根据法律不能离开某国或某区域时，地域限制可能特别重要（见第一部分，第10–11段）。合同一般规定客户是否能够撤销被准予的权利或暗含的权利以及在何种条件下可以撤销。由于按规定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是修正或终止合同。

提供商为其他目的使用客户数据

79. 大多数法域并不自动准予提供商为其自身目的而使用客户数据的权利。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。这方面要考虑的问题可包括：*(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)*是否会与其他组织、公司或个人共享这些信息，如果是，这样做的理由，以及这样做是否将取得客户同意；*(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**，双方通常还要仔细评估所适用的数据保护法律对其规定的监管合规义务。

80. 如果合同准予提供商为其自身目的使用客户数据的权利，合同还可列出此种使用的理由，载明对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，并规定对复制内容和对外公开的限制。通常，在合同存续期间或之后准许提供商为自身目的使用客户数据，但仅限于匿名化开放数据或采用汇总和去身份化形式。

提供商使用客户名称、标志和商标

81. 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。双方可以就删除或修改这些规定达成协议，包括将允许使用范围限于客户名称，并要求事先取得客户对使用其名称、标志和商标的批准。

提供商根据国家命令或为监管合规而就客户数据采取行动

82. 提供商的标准条款可能为提供商保留酌情向国家机关披露客户数据或提供客户数据访问权的权利（例如，列入“如果这样做将最有利于提供商”这样的措辞）。这些条款通常还规定，在提供商得知或了解非法内容后，或者当提供商必须执行**数据主体被遗忘权**时，提供商有权立即去除或封锁客户数据，以避免法律规定的赔偿责任（“通知后下架”程序（见下文第128段））。订约双方可以就缩窄提供商能够采取这些行动的情形达成协议，例如，限于法院或其他国家机关责令提供商提供数据访问权或删改数据的情形。

83. 订约双方可以商定，作为最低限，将立即向客户通知国家命令或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。如果预先通知和客户参与都不可行，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。双方还可以就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的规定达成协议。

对云服务衍生数据的权利

84. 订约双方可以就客户对**云服务衍生数据**的权利以及如何在合同关系存续期间并在合同终止时行使这类权利达成协议。

知识产权保护条款

85. 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共同产生这种客体（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，其中将确定合同哪一方拥有对云中部署或开发的各种客体的知识产权以及双方可对这类权利作何使用。如果不存在谈判可能，客户似宜审查可能拟订的知识产权条款，以确定提供商提供足够保障，同时允许客户利用适当工具保护、享有其知识产权并避免**锁定**风险（见第一部分，第23–26段）。

互操作性和可移植性

86. 在确保**互操作性**和**可移植性**方面可能没有法定要求。除非合同另有规定，例如，就互操作性和可移植性以及在合同终止时协助导出数据列入合同承诺，否则，创设兼容导出程序的义务可能完全在客户方面（见下文第161段）。合同可以要求为数据及其他内容使用普通、广泛使用的标准化或互通导出格式，或者在可用格式当中提供选择。还可以列入关于联合产品和应用程序或软件的权利的合同条款，没有这些权利，可能无法在另一系统中使用数据及其他内容（见上文第85段）。

为法律目的检索数据

87. 客户可能需具备以原件形式搜索和查找放在云中的数据的能力，以便（在调查等方面）满足法律要求。电子记录可能需满足审计和取证方面的标准。有些提供商可能有能力协助客户按法律要求的格式检索数据。合同可能需界定这种援助的形式和条件。

数据删除

88. **数据删除**方面的考虑可能在合同期内适用，但在合同终止时尤其如此（见下文第162段）。例如，可能需要根据客户的留存计划删除某些数据。敏感数据可能需在其寿命周期某一规定时间销毁（例如，在存有此类数据的设备寿命终止时销毁硬盘）。还可能需为遵守执法

机构的删除请求或在知识产权侵权案件得到确认后删除数据（见上文第82段）。

89. 提供商的标准条款可以仅载列定期删除客户数据的声明。订约双方可以就按照数据留存和处置计划或按照客户发给提供商的其他形式授权或请求立即、有效、不可逆转地永久性删除数据及其备份和**元数据**达成协议。合同可以涉及数据删除的时间期限和其他条件，其中包括在删除完成后确认数据删除并提供删除活动审计记录访问权的义务。

90. 可以根据数据的性质和敏感性指明删除数据所使用的具体标准或方法。可以要求提供商从不同地点和媒介删除数据，包括从分包商和其他第三方的系统中删除数据，分不同级别删除数据，例如，数据杀毒以在彻底删除数据或销毁硬件之前确保数据的保密性。涉及销毁设备而不是重新部署设备的删除虽然更安全，但成本可能更高，而且不一定总是可行（例如，如果同一硬件上存有他人数据的话）。这些问题可能导致在合同中要求使用被隔绝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

91. 订约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，客户及其终端用户遵守**可接受的使用政策(AUP)**和**知识产权许可**的情况，提供商遵守**服务级别协议(SLA)** 和数据保护政策的情况）。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。

92. 合同可以确定定期或经常性监测活动，并确定负责执行这些活动的一方和对方为监测提供方便的义务。合同还可预期任何例外监测活动，并提供处理这些活动的选项。合同也可规定对另一方的报告要求以及与这种监测活动有关的任何保密承诺。

93. 过度监测会影响服务的履行，增加服务费用。合同可以规定在某些情况下必须暂停监测，例如，在监测实质上不利于履行服务的情况下。要求近实时履行的服务尤其可能存在这种担忧。

审计和安全测试

94. 审计和安全测试经常进行，特别是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）。

95. 双方可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。双方可在事件发生后，根据事件严重性和类型，商定对审计或安全测试的特别安排（例如，事件责任方可能必须部分或全部赔偿费用）。

F. 付费条款

随用随付

96. 价格是一项必不可少的合同条款，合同中不列明价格或没有一种定价机制，可能致使合同无法执行。

97. 云计算服务的**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（例如，规定用户数、使用次数或使用时间）的单位价格。可以设计价格表或其他价格调整办法，包括批量折扣，以此作为对任何一方的奖惩办法。免费试用很常见。还经常有个别服务不收费的做法。尽管价格计算会有多种变式，但制定可为双方理解的清晰、透明的价格条款可避免争议和诉讼。

许可证费用

98. 订约双方似应在合同中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。

99. 许可证可以按机器台数计费，也可以按开机次数计费，费用可能取决于用户类型（例如，相对于非专业用户，专业用户可能属于付费最高的类别之一）。不同付款结构会产生不同影响。例如，如果按开机次数收取软件费用，每次连接一台新机器，即使客户在同一时段内使用同样的开机次数，客户的许可证费用也可能显著增加。

100. 合同可以确定许可安排所涵盖软件的潜在用户数目、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。合同还可以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及其终端用户的访问和使用情形。

额外费用

101. 价格可能还包括一次性费用（例如，配置和云迁移费用）（见第一部分，第32–33段）。还可能有一些额外服务是提供商单独收费提供的（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）。

102. 在某些法域，**云计算服务**可能属于课税服务或货物类别。订约双方似宜在合同中处理税收对付费条款影响问题。

其他付费条款

103. 付费条款可涵盖发票开具方式（如电子发票）以及发票形式和内容，这对于税务合规可能很重要。一些法域的税务机关可能不接受电子发票（不过这在日趋无纸化环境中越来越少见），也可能要求使用一种特殊格式，其中包括，凡与云计算服务有关的税项可能需单独列明。

104. 除其他付费条款外，订约双方似应列明付费到期日、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

105. **云计算服务**本质上具有灵活性和波动性。**云计算服务**的**弹性**、**伸缩性**和**按需自助服务**特征通常是通过合同规定的多个选项来实现的，客户可利用这些选项根据其需要来调整服务的消费方式，从而可避免客户每次要求变更服务消费方式时重新谈判合同的必要性。

106. 反过来，提供商可保留酌情调整其服务组合的权利。可能适合采取不同的合同处理办法，需视变更涉及核心服务还是辅助服务及配套方面而定。如果变更有可能对服务产生不利影响，而不是改进服务，也可适用不同的合同处理办法（例如，从提供标准服务转换为提供安全级别更高、反应时间更短的加强型云计算服务提议）。提供商单方面更改合同条款和条件可能给客户造成严重后果，特别是导致向另一系统迁移的高昂成本。

价格变动

107. 提供商可保留单方面修改价格或价目表的权利。双方可以商定在合同中具体规定定价方法（例如，提供商可以提价的频度和幅度）。价格上限可定为某一消费价格指数、预先设定的百分比或提供商某一特定时刻的价目表。合同可以规定预先通知提价以及客户不接受提价的后果。

升级

108. 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，因为即使在每周7天每天24小时基础上提供服务，升级也有

可能变为正常工作时间内的较高**宕机时间**。双方可以商定提前通知客户即将进行的升级及其影响，并且升级一般都安排在对客户需求量低或没有需求的时段。合同还可规定报告和解决可能出现的问题的程序。

109. 升级还可能产生其他负面影响，例如，需要对客户应用程序或信息系统作出调整，或者要求对客户的用户进行再培训。合同可以规定升级所产生费用的分配办法。双方还可以商定，如果对旧版本作出重大修改，所提供服务的旧版本应当在商定期间与新版本并行保留，以确保客户业务的连续性。合同也可涉及提供商可协助对客户应用程序或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。

服务降级或中断

110. 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降级或中断。提供商可以在合同中保留对所提供的服务组合进行调整（例如，终止一部分服务）的权利。不过，提供商即使只是中断部分云计算服务，也可能使客户面临对其终端用户的赔偿责任。

111. 合同可以规定预先向客户通知这些变更，规定客户有权在变更令人无法接受时解约，并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**。有些合同禁止会对所提供服务的性质、范围或质量产生不利影响的修改，或者将可允许的变更限于“商业上合理的修改”。

变更通知

112. 提供商的标准条款可以载明提供商向客户通知服务条款变更的义务。若非如此，客户可能需定期查看合同有无任何变化。合同可以由多份文件构成（见上文第38段）。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，而这些其他文件可能又以提及方式纳

入补充条款和政策，所有这些文件都可能由提供商单方面修改。提供商网站上可能在不止一处托放这些不同文件。因此，可能不易注意到提供商对合同作出的改动。

113. 鉴于客户继续使用服务被视为接受经修改的条款，订约双方可以商定，在修改生效之前将服务条款变更事宜充分提前通知客户。双方还可以商定，客户有权访问服务变化过程的审计记录，所有商定条款以及参照某一版本或版次对服务作出的界定都将予以保存。

H. 暂停服务

114. 提供商的标准条款可以载明提供商随时酌情暂停服务的权利。“不可预见事件”是提供商单方面暂停服务的一个常见理由。此种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。

115. 订约双方可以商定，只可在合同确定的有限情况下暂停服务（例如，客户有重大违约情形，如不付款）。因不可预见事件而暂停服务的权利可能是以适当执行一项业务连续性和灾难恢复计划为条件。合同可以要求这类计划针对提供云计算服务方面的共同威胁包含防范措施并将计划提交另一方征求意见和批准。这些防范措施可以包括在另一地域分设一个能够无缝转移的灾难恢复站点，并使用不间断电源和备用发电机。

I. 分包商、分提供商和外包

确定分包链

116. 分包、**分层云计算服务**和外包是云计算环境下的常见运营模式。提供商的标准条款可以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，由于所提供服务的性质，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。

117. 法律可能要求订约双方在合同中确定参与提供云计算服务的任何第三方。此种确定还可能有利于客户实现核证目的，特别是核证第三方是否遵守合同或法律所规定的安全、保密、数据保护及其他要求，以及第三方不涉及利益冲突。

118. 此种信息还可用于减轻提供商由于第三方故障而无法履行合同的风险。例如，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。客户还可以尝试与关键第三方谈判其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。

119. 提供商或许能够指明那些发挥关键作用的第三方，但未必能够指明所有第三方。参与提供云计算服务第三方的组成情况有可能在合同期间发生变化（见下文第120–121段）。

分包链变更

120. 分包链常发生单方面变化。合同可以具体规定是否允许对分包链进行变更以及在哪些条件下允许变更（例如，客户可以保留在实施变更之前对参与向客户提供云计算服务的任何新的第三方进行背景审查并予以否决的权利）。另一种办法是，合同可以列入客户预先核准的第三方清单，提供商可在需要时从中选择。再有一个选择是先做变更尔后需取得客户批准，在未获此种批准的情况下，将由先前批准或其他预先批准的第三方继续提供服务，或由双方将商定的另一第三方继续提供服务；否则可以解约。

121. 强制性适用法律可能规定，在哪些情况下提供商分包链发生变更后可以要求解约。

合同条款与关联合同挂钩

122. 法律或合同可以要求订约双方使合同条款与现有或未来关联合同挂钩，以确保保密性并遵守**数据本地化存储**要求和数据保护要求。合同还可以要求双方为核证目的相互提供关联合同副本。

分包商、分提供商和其他第三方的责任

123. 虽然可在合同中列明有助于履行云计算合同的第三方，但其并非提供商与客户之间合同的当事方。他们将对各自在合同下与提供商的义务承担责任。在关联合同中为客户设定第三方受益人权利，或使客户成为关联合同的一方，将允许客户在第三方未根据关联合同履约的情况下对该第三方享有直接追索权。

124. 在适用法律或合同之下，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。

J. 赔偿责任

对合同自由的法定限制

125. 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限制或排除赔偿责任，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，某些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订约方受其管辖的法律制度。由于非法处理**个人数据**或任何不符合

国内数据保护条例的行为而遭受损失的**数据主体**可能有权直接从**数据控制人**获得赔偿。

126. 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（包括患病和死亡）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不遵守适用的监管要求的赔偿责任。某些类型的赔偿责任限制条款可能因被认为带有“滥用性”而无效，例如，在客户无法控制或无法实施安全措施的情况下提供商免除对**安全事件**的赔偿责任的条款。附和合同的条款通常不是谈判达成，而是由一方预先确定，因而可能会受到特别审查。此外，无限赔偿责任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）。

127. 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，或者禁止公共机构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。

128. 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（见上文第82段），如果提供商一得知在其云基础设施上有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。

129. 在某些法域，为了得以执行，必须在合同中纳入载有订约双方商定的免责声明和责任限制的条款。适用法律可能对这些条款的有效性和可执行性规定形式上的要求或其他要求。

起草赔偿责任条款方面的其他考虑

130. 在就风险和赔偿责任分配进行谈判时，将考虑到云计算服务的任何收费数额以及提供这些服务所涉及的风险。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、分包商作为或不作为）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赔偿责任，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赔偿责任是与受其控制部分成比例逐渐增加的。

131. 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出现故障的情况，提供商可能都要承担赔偿责任。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，对其控制下的数据加密或备份。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。

提供商的标准条款

132. 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而可能发生的违反事件（例如，不可预见的事件或泄露机密数据）的赔偿责任。

133. 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。如果一般接受赔偿责任或接受对某些具体指明情形的赔偿责任，提供商的标准条款往往（按每起事件、每批事件或每段时期）限制将赔付的损失金。此外，提供商往往对合同规定的赔偿责任设定一个总上限，与之有关的可能是合同下预期得到的收入、提供商营业额或保险范围。

134. 提供商的标准条款通常对客户不遵守**可接受的使用政策(AUP)**规定赔偿责任。

标准条款的可能变式

135. 有些事件（例如，侵犯**个人数据**保护和侵犯知识产权）可能使其中一方对第三方承担潜在的高额赔偿责任，或导致监管罚款。当由于另一方的过失或疏忽而发生这些事件时，通常商定一种更严格的赔偿制度（无限赔偿责任或更高赔金）。

136. 合同或法律可以限制或排除订约双方对其无法控制的第三方行动的赔偿责任（例如，客户对终端用户行动的赔偿责任，或提供商对客户或其终端用户行动的赔偿责任）。

赔偿责任保险

137. 合同可以载明双方或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相互提供当前保险合同副本。

K. 违约的补救办法

补救种类

138. 订约双方可以在适用法律规定的限度内自由选择补救办法。补救办法可以包括实物补救——旨在为受害方提供预期从履约获得的同样或同等益处（如更换有缺陷硬件）、金钱补救（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补救办法。

暂停或终止服务

139. 暂停或终止向客户提供云计算服务是提供商针对客户违约或客户终端用户违反**可接受的使用政策(AUP)**通常采取的补救办法。合同可载明针对广泛暂停权或终止权的合同保障。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、对提供商的系统安全或完整性构成严重威胁的情形以及适用法律规定的情形。提供商的暂停权或终止权也可仅限于受违约影响的服务，而这种可能性是存在的。

服务积分

140. 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，即减费百分比可取决于提供商根据合同提供服务在多大程度上未达到**服务级别协议(SLA)**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，或在接下来的一定时期内提供增强服务包(例如,免费提供信息技术咨询)。如果存在一系列选项，提供商的标准条款可以规定由提供商选择对其不履约的任何补救办法。

141. 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补救办法可能会限制客户对于其他补救办法的权利，包括提起损害赔偿诉讼或解约。此外，如果合同即将终止，在接下来的一定时期内减费或提供增强服务包，这种形式的服务积分可能并无益处。如果从合同一开始就认为过高的服务积分是一种不合理的损害估算方法，则可能无法执行服务积分办法。诸如罚款（可接受情况下）或预定损失赔偿金等其他措施可为确保守约提供更适当的激励办法。

违约时应依循的程序

142. 合同可以载明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机会补救此种声称的违约。还可设定要求补救的时限。

L. 合同期和解约

合同开始生效的日期

143. 合同开始生效的日期可以不同于签字日期、接受要约日期或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的日期，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的日期，即使提供商为客户提供的服务尚未到位。出于这些原因，并为了避免不确定性，订约双方可以在合同中注明其开始生效的日期。

合同期

144. 合同期可分为短期、中期或长期。**标准化商用型多订户云解决方案**通常规定一个固定的初始期（短期或中期），然后自动展延，除非任何一方终止合同。提供商可能同意向客户发出合同即将期满的预先通知。各种考虑因素都会影响就展期作出决定，其中包括**锁定**风险和可能错过更好交易。

提前解约

145. 合同通常除合同固定期期满之外还涉及其他解约理由，如出于方便、违约或其他原因。合同可以规定提前解约的方式，包括对充分预先通知、**可逆性**以及其他服务终了承诺的要求（见下文第157–167段）。

为方便而解约

146. 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，通常为提供商保留任何时候无需客户违约即可解约的权利。双方可以商定限制行使此种权利的情形，并要求提供商向客户充分提前发出解约预先通知。

147. 客户为方便（即无需提供商违约）而解约的权利尤其多见于公共合同。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。

因违约而解约

148. 重大违约通常是解约理由。为避免含糊不清，订约双方可以在合同中界定构成重大违约的事件。提供商的重大违约可包括数据丢失或误用、违反**个人数据**保护规定、重复性**安全事件**（例如，任何一段衡量期内超过一定次数）、泄密以及某些时间点或某一时段未提供服务。客户不付费以及客户或其终端用户违反**可接受的使用政策(AUP)** 是提供商解约的最常见理由。该订约方的解约权可能有附加条件：发出事先通知、举行诚信协商并提供纠正状况的可能性。该订约方根据合同可能有义务在采取补救行动后一定天数内恢复履约。

149. 合同可以涉及提供商在发生客户重大违约后兑现服务终了承诺，包括客户数据及其他内容的**可逆性**（见下文第157–167段）。

因合同修改不可接受而解约

150. 一方对合同的修改可能不为另一方所接受并可成为解约理由。这些修改可以包括对**数据本地化存储要求**或分包条款的修改。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更换一些服务，则合同可以规定客户有权终止整个合同（见上文第105–124段，下文第155段）。

破产时解约

151. 对于破产风险，可以在风险评估期间确定（见第一部分，第15段*(j)*项），也可以在合同期间确定，例如，如果合同要求定期

报告双方的财务状况。允许在任何一方破产时终止合同的条款是常见的。破产法中的强制性条款可优先于这些条款。

152. 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。订约双方可以限制在客户没有合同规定的拖欠付款情形时援用破产作为唯一解约理由的权利。

153. 订约双方可以在合同中规定在提供商破产时检索客户数据的机制（例如，自动发放源代码或托管密钥以允许访问客户数据及其他内容），法律也可以作此种规定。否则，客户从破产提供商的基础设施检索其数据及其他内容可能面临困难和延误。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，破产提供商或**破产管理人**可以限制特定期间内可撤出内容（数据和应用代码）的数量，或者决定在“先来先得”的基础上兑现服务终了承诺。

控制权变更时解约

154. 控制权变更可能涉及一些变化，例如，所有权变更，或者直接或间接决定提供商经营和财务政策的能力发生变化，这又可能导致提供商服务组合的变化。控制权变更还可能涉及合同的转让或更新，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）可能需改为对第三方履行。

155. 如果由于控制权变更而无法满足强制性法律要求（例如，**数据本地化存储要求**，或者对与置于国际制裁制度下的某些实体打交道的禁令或由于国家安全考虑对与某些实体打交道的禁令），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。此外，在控制权发生变更的情况下，订约双方也可以商定终止合同，特别是如果提供商或合同由于此种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发生重大改变。通常做法是要求预先通知即将发生的控制权变更及其对合同的预期影响。

闲置账户条款

156. 合同规定的某一时期内无客户活动，可以是提供商单方面解约的一个理由。不过，在为取酬而订立的商对商云计算合同中，这种闲置账户条款并不多见。

M. 服务终了承诺

157. 服务终了承诺不仅会引起合同问题，还会引起监管问题。订约双方可能关注于实现客户利益和提供商利益之间的平衡，前者在于能够不间断地访问其数据及其他内容，包括在过渡期间，后者在于尽早结束对前客户的任何义务。

158. 服务终了承诺可以不论解约原因一概而论，也有可能根据解约是因为违约或其他原因而有所不同。以下各段论及双方似宜在合同中处理的问题。

导出的时限

159. 订约双方可以在合同中具体规定导出的时间范围，这个时间范围需要足够长方可确保客户将其数据及其他内容顺利导出至另一系统。

客户访问需导出的内容

160. 合同将指明需导出的数据及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第三方持有的任何解密钥匙（见第一部分，第28段）。为了便利在提供商最少参与的情况下导出客户数据，双方可以商定一项托管安排（即由第三方参与，授权其在发生某些事件——如终止合同——时自动向客户发放源代码、解密密钥或其他允许访问客户数据及其他内容的要件（另见上文第153段））。合同还

可以尽量列明导出选项，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

161. 提供商可能并不总是同意积极参与协助客户将其数据导出至另一系统，但根据法律可以要求确保这种导出是可能的和简单的。如果订约双方就提供商参与向另一系统导出客户数据达成协议，合同可指明具体细节，如协助导出的范围、程序和期限。提供商可以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在某一特定期间的价目表。另一种做法是，双方可以商定将这种协助计入合同价格，如果在提供商违约后解约不额外收费。

数据删除

162. 合同可能需要具体规定导出完成后或合同规定的导出期期满时提供商云基础设施的**数据删除**规则。数据删除可以由提供商自动完成，例如，某些事件发生之时双方商定的时间期限到期，或依从法律的要求。也可以仅根据客户的具体请求和指示删除数据。双方可以商定，将向客户通知即将进行的删除并提供删除数据——包括从第三方系统删除数据——的证明、报告或声明。

合同结束后留存数据

163. 法律特别是数据保护法律可能要求提供商留存客户数据，其中还可能涉及数据必须留存的期限。由于需要保留和存储数字签名证书，可能会产生具体问题和要求，尤其是在跨境情况下。订约双方可以商定由提供商在合同终止后留存客户数据。一些提供商可能为提供合同结束后留存期而另外收费。

164. 订约双方可以列明关于不退回或无法退回客户的数据以及无法删除的数据的特殊要求。例如，合同可以规定，所有个人信息必须

去身份化，数据应以加密格式留存或以可使用、可互操作的格式留存，以便于需要时检索。双方还可以商定各自对于合同结束后按规定格式留存数据的责任。

合同结束后保密条款

165. 双方可以商定一项合同结束后保密条款。保密义务可以在合同终止后某一规定年限内延续（如五年或七年），也可以无限期延续，取决于置于提供商云基础设施中客户数据及其他内容的性质。

合同结束后审计

166. 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。订约双方可以商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

167. 订约双方可以商定将提供商账上余款退还客户的条件或用这些余款抵消客户需付给提供商的任何额外费用的条件，其中包括服务终了活动的费用或补偿损失的费用。

N. 争议解决

争议解决方法

168. 订约双方可以商定合同争议的解决方法。争议解决方法包括谈判、调解、网上争议解决（网上解决）、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）有约束力的裁定，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。在小额索赔案中，借助网上解决机制的谈判或调解可为双方在网上达成合意性协议提供快速、有成本效益的方法。对于数额较高的索赔，特定云部门的网上解决机制可提供有管辖权的专门法庭并有助于司法程序。有些

法域的法律可能规定了某些非诉讼争议解决机制，双方需穷尽这些机制方可将争议诉诸法院。

仲裁程序

169. 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。然而，并非所有争议问题都可诉诸仲裁；有些问题可能需依法交由法院裁决。因此，各方不妨在选择仲裁之前核实其争议的可仲裁性。合同中的仲裁条款通常提及一套管辖仲裁程序的仲裁规则。合同可以列入一个标准争议解决条款，指明使用国际公认规则（如《贸易法委员会仲裁规则》）进行争议解决程序。在未作此种指明的情况下，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。

网上争议解决

170. 订约双方可选择网上解决机制来解决因其合同而产生的某些或所有类型争议，但须在法律规定的限度内。合同可具体规定诉诸网上解决机制的问题范围以及拟在程序中使用的网上解决平台和规则。在有些情况下，可在提供商提供的云服务包中嵌入网上解决办法和选择退出的可能性。

171. 网上解决程序通常包括：*(a)*双方通过网上解决平台进行谈判；*(b)*协助下调解，指定一名中立人，由其与双方沟通以设法达成和解；*(c)*最后阶段，网上解决的管理人或中立人将最后阶段的性质及其形式告知双方。网上解决的结果可能对双方不具约束力，除非合同或适用法律另有规定。

司法程序

172. 如果由于**云计算服务**的性质而需进行司法程序，可能会有若干国家声称拥有管辖权。可能的话，订约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（见下文第175–181段）。

数据留存

173. 在争议解决阶段，客户继续访问其数据——其中包括**元数据**和其他**云服务衍生数据**——除了对业务连续性至关重要外，对于客户参与争议解决程序（例如，提供索赔或反诉证据）可能也至关重要。合同可以具体规定，双方发生争议时，客户数据将由提供商留存，客户可在一段合理时间内访问其数据，而不论争议的性质如何。双方还可以商定一种托管安排（见上文第160段）。

投诉时效期

174. 订约双方可以在合同中规定提出索赔的时效期。法律规定的时效期可能适用，并将推翻不合规的合同条款。

O. 法律选择和诉讼地选择条款

175. 合同自由（见上文第34段）一般允许订约方选择其合同适用的法律并选择审理争议的管辖地或诉讼地。不过，强制性法律（如数据保护法）可能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，可能会有不止一项强制性法律（如数据保护法、破产法）适用于合同，包括不同法域的强制性法律。

选择适用法律和诉讼地所涉及的考虑

176. 法律选择条款和诉讼地选择条款相互关联。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另一裁决机构（如仲裁庭）提出法律选择条款。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对适用法律的选择。鉴于诉讼地法律关乎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。

177. 在选择诉讼地时，订约方通常考虑所选择的适用法律或其他适用法律的影响，以及在该诉讼地作出的司法裁定将在多大程度上在可能寻求执行所在国得到承认并可执行。保持执行选项灵活性可能是一项重要考虑，特别是在云计算环境下订约方在拟定法律选择条款和诉讼地选择条款时通常会考虑的许多因素可能都不确定，包括提供服务所涉资产的所在地以及提供商和客户的所在地。

强制性法律和诉讼地

178. 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，即可成为适用该国数据保护法的充分条件；

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

(c) 活动发端地（设备所在地）的法律或活动获利指向地的法律可导致适用该地法律。使用与某一地点关联的特定国家顶级域名、网站上使用当地语言、以当地货币定价以及当地联系点，这些都是作出此种判定时可能会考虑的因素。

提供商或客户本国的法律和诉讼地

179. **标准化商用型多订户云解决方案**的合同往往规定，合同由提供商主要营业地或主要机构所在地的法律管辖。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。客户可能倾向于首选本国的法律和管辖权。公共机构对其同意外国法律和管辖权的能力作出重大限制。在多个法域运营的提供商可能会对接受选择客户所在国的法律和诉讼地持灵活态度。

多选项

180. 订约双方还可以就合同的不同方面规定法律和诉讼地选择的各种选项。双方也可选择被告的管辖地，以消除本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

181. 订约双方可能倾向于不在合同中列入法律或诉讼地选择条款，而将这一问题留待日后需要时讨论。这或许可以看作是某些情况下唯一可行的解决办法。网上解决也可以是管辖权和适用法律问题解决办法的一部分（见第170–171段）。

P. 通知

182. 通知条款通常涉及通知的形式、语言、接收人和方式，以及通知何时生效（发出时、送达时或确认收讫时）。在没有任何强制性法律规定的情况下，订约双方可以商定通知手续，通知手续可以是统一的，也可以根据重要性、紧迫性和其他因素而有所不同。相较于例行通知，将对暂停或单方面解约等情形适用更严格的要求。双方可以商定最后期限，同时需考虑到**可逆性**以及业务连续性需要。合同可以提及法律规定的任何通知和期限。

183. 双方可以选择向合同中指明的联系人的物理地址或电子地址发出**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。

Q. 杂项条款

184. 订约双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——即允许从合同中去除失效

规定，或语文条款——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。其中一些条款可以由订约双方根据**云计算服务**的具体情况量身制定。

R. 修正合同

185. 任何一方均可提出修正合同。合同将涉及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。

186. 鉴于**云计算服务**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，客户使用一开始就在合同中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（见上文第105–106段）。另一方面，如果增加的特性未在最初商定的条款中涵盖并因此需要调整价格，则可能构成对合同的修正。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。

187. 允许对公共合同修改的程度可能受公共采购规则的限制，即对于必须经过公开招标程序的合同，通常限制订约双方重新谈判合同条款的自由。

188. 鉴于最初商定条款的频繁修改，每一方似应独立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的使用限度的部分。

审计: 审查合同要求和法定要求以及技术标准遵守情况的过程。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保证数据完整性而采取的适当措施，包括隔离。审计可以是内部审计或外部审议，也可以是提供商或客户分别指定或双方共同指定的独立第三方进行的审计。**服务级别协议(SLA)**可载明与审计有关的绩效参数，例如，至少每年由独立审计师参照合同中确定的安全标准对根据合同提供的服务进行核证。

云计算服务: 网络服务具有以下特点：

(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），在网络上利用服务；

(b) **计量化服务**，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**，指物理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服务，或为自动服务，或与提供商最低限互动；

(e) **弹性**和**伸缩性**，指根据客户需求——包括资源使用的大规模趋势（如季节性影响）——迅速调高或调低服务消费量的能力；

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

(g) **广泛服务**，所涵盖范围从提供和使用简单连接和基本计算服务（如存储、电子邮件和办公应用程序），到为客户建立自有信息技术平台或部署、管理和运行由客户创建或由客户获取的应用程序或软件而提供和使用所需要的全套信息技术物理基础设施（如服务器和数据中心）和虚拟资源。基础设施即服务**(IaaS)**、平台即服务**(PaaS)**或软件即服务**(SaaS)**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人）：参与支持或辅助提供商活动或客户活动或两者活动的人。云审计师对提供和使用**云计算服务**的情况进行**审计**。云服务经纪人或系统集成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数据，其中包含何人、何时使用服务以及涉及哪些功能和哪类数据的记录。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。

数据删除：旨在不可逆转地从云计算基础设施（物理设施和虚拟设施）清除数据（包括其备份和元数据）及其他内容的一系列操作。在某些情况下，数据删除可要求销毁存储数据的物理基础设施（如服务器）。**服务级别协议(SLA)** 可以包含与数据删除相关的具体绩效参数，例如，提供商确保在客户提出请求的任何情况下，在合同确定的某一期限内，按照合同确定的标准或方法，有效、不可撤销地永久删除数据。

数据本地化存储要求：与数据及其他内容所在地或与数据中心或提供商所在地有关的要求。这些规定可禁止某些数据（包括**元数据**和备份）在某个地区或法域驻留或移入移出，或要求事先就此取得国家主管机构的批准。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**驻留或移入不遵守某些**个人数据**保护标准的法域。

数据处理人：代表**数据控制人**处理数据的人。

数据主体：可通过数据直接或间接识别的自然人，包括参照诸如姓名、识别号码、所在地等标识以及与该人的身体、基因、心理、经济、文化或社会特质有关的任何因素进行识别。在一些法域，数据主体在数据保护或数据隐私条例下对能够识别他们的数据享有某些权利。这些条例可导致在**服务级别协议(SLA)** 中列入数据保护方面的绩效参数，例如，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。(另见**数据主体的权利**和**个人数据**)

数据主体的权利：与**数据主体的个人数据**相关联的权利。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)、限制其**个人数据处理**的权利，以及对其**个人数据可移植性**的权利。

部署模式：根据物理资源或虚拟资源的控制和共享情况对云计算服务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客户，资源由提供商控制；

(b) **社区云，云计算服务**专门向互相关联、有共同要求的特定客户群体提供支持，资源至少由该群体一名成员控制；

(c) **私人云：云计算服务**专供单一客户使用，资源由该客户控制；

(d) **混合云**，使用至少两种不同的云部署模式。

宕机时间或**中断时间：**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宕机时间。

可在**服务级别协议(SLA)** 中将其定义为特定时段内可允许的中断次数并指明中断时长，例如，每天不得中断一次以上，8点至17点之间不得中断。

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。这种模式的目的可以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，从而减少**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（数据转移速率(DTR)或吞吐量）。

基础设施即服务(IaaS)：客户用以获得并使用处理资源、存储资源或连网资源的各类**云计算服务**。客户并不管理或控制基础物理资源或虚拟资源，而是对使用物理资源或虚拟资源的操作系统、存储器或所部署的应用程序进行控制。客户也可享有控制某些连网部件（如主防火墙）的有限能力。

破产管理人：破产程序中被授权对破产债务人受破产程序管辖的资产的重整或清算进行管理的人或机构。

互操作性：两个或多个系统或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，软件和视像内容（设计、布局和图像）的许可证可限于特定用途，不允许复制、修改或增强，并且限于某一特定媒介。许可证可限于特定市场（如国家或（分）区域市场）、某一用户数量或某一设备数量，也可能有时限。可能不允许次级许可。许可人可要求每次使用知识产权必须报备知识产权所有权人。

时延：从用户提出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。**服务级别协议(SLA)**中通常以微秒表示时延。

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任何计算资源的所有人，但其本身是全部或部分**云计算服务**的客户。例如，**平台即服务(PaaS)** 或**软件即服务(SaaS)**类型服务的提供商可以利用另一实体拥有或提供的存储器和服务器基础设施（数据中心、数据服务器)。因此，可以有一个或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。

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，同时可能需要确保记录的真实性。客户或提供商均可生成元数据。

绩效参数：数量参数（数字指标或规格，或绩效范围)或质量参数（服务质量保证)。绩效参数可依据与适用标准的一致性，其中包括任何一致性核证的到期日（例如，提供商已按照合同中确定的国际标准执行一项关键的管理政策)。为求实效，绩效参数应允许客户以方便、可审计的方式衡量对客户具有重要意义的绩效。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、服务或应用程序的关键性，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**服务级别协议(SLA)** 条款。

数据存储持久性：云中存储的数据不会在合同期间丢失的概率。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（例如，某一确定时期（如一个日历月)内的完好数据/完好数据＋丢失数据)而采取的步骤。数据类型（如

文档、数据库、代码应用程序等）和衡量单位（文档数、位长），都需要在合同中确定。

个人数据：可用以识别自然人身份的与其相关的敏感数据和非敏感数据。在一些法域，**个人数据**定义可包含与身份已识别的个人或身份可识别的个人（见**数据主体**）直接或间接关联或相关的任何数据或信息。

个人数据处理：个人数据的收集、记录、整理、存储、改编或翻改、检索、咨询、使用、通过传输披露、传播或以其他方式提供、挂钩或组合、封锁、清除或销毁。

平台即服务(PaaS)：客户使用提供商支持的一种或数种现有编程语言和执行环境，用以在云中部署、管理和运行由客户创建或由客户获取的应用程序的各类**云计算服务**。

可移植性：从一系统向另一系统方便地（即低费、最少干扰且无需重新输入数据、重新设计流程或重编应用程序）转移数据、应用程序及其他内容的能力。如果能够以另一系统接受的格式检索数据，或者能够借助通用工具通过简单、直接的转换检索数据，即有可能实现可移植性。**服务级别协议(SLA)** 可载明与可移植性相关的参数，例如，客户可经由单一下载链接或已载入的应用程序编程接口(API)检索客户数据；数据格式的架构和载入方式足以允许客户再次使用客户数据或将其重构为另一种需要的格式。

恢复点目标(RPO)：容许在计划外中断服务之前因恢复而丢失数据更改内容的最长时间期限。如果合同将恢复点目标(RPO)定为服务中断前两小时，这就意味着可在恢复后以所有数据在中断发生前两小时这一时间点存在的形式调取所有数据。

恢复时间目标(RTO)：必须在计划外中断后恢复所有云计算服务和数据的时间期限。

可逆性：客户从云中检索其数据、应用程序及其他相关内容的过程，以及提供商在商定的期限后删除客户数据及其他相关内容的过程。

特定部门条例：金融、卫生、公共部门条例或其他具体部门或行业条例（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员访问的信息）。

安全事件：表明系统或数据已经受损的事件，或表明为保护系统或数据而建立的措施已经失灵的事件。安全事件的例子包括未经授权的来源试图进入系统或访问数据、计划外中断服务、服务被拒、擅自处理或存储数据，以及擅自更改系统的基础设施。

服务级别协议(SLA)：提供商与客户之间的云计算合同中确定合同所涵盖的云计算服务以及根据合同预期提供或应实现的服务级别的部分（见**绩效参数**）。

软件即服务(SaaS)：客户用以使用提供商的云中应用程序的各类**云计算服务**。

标准化商用型多订户云解决方案：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**。对于提供商的赔偿责任，这种解决方案普遍包含广泛免责声明和弃权条款。客户能够比较不同提供商及其合同并从市场现有提供商中选出最适合其需要者，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。可表示为数量或百分比、详细公式或具体日期或天数，以及提供某项应用服务的关键时段。

书面或**书面形式：**可调取以供日后查询时使用的信息。包含纸面信息和电子通信信息。“可调取”指计算机数据形式的信息应为可读和可释义，还指应保留使这种信息可读而可能需要的软件。“使用”涵盖人使用和计算机处理。

V.19-09102