企业采购云服务合规要旨

作者：潘永建 | 邓梓珊 | 胡鑫超

随着互联网产业的迅猛发展和全球云计算领域的活跃创新，越来越多企业采用云计算模式部署信息系统，以加快企业的数字化、网络化、智能化转型。2020 年全球范围内的云计算市场规模达到 1435 亿美元，全球使用云计算的企业比例也由 2016 年的 33%上升至 2020 年的 53%。[1]根据工业和信息化部《推动企业上云实施指南(2018-2020 年)》提出的企业上云的工作目标，到 2020 年，云计算在企业生产、经营、管理中的应用将广泛普及，全国新增上云企业 100 万家，我国的云计算也进入了高速发展时期。随着各行各业深度拥抱云计算，云端数据安全的重要性不言而喻。

本文旨在探讨企业上云的优势和风险，并从用户角度就云服务采购协议提供合规建议，以帮助用户尽可能从源头控制上云风险。

一. 企业上云已成大势所趋

企业纷纷选择上云，主要原因在于云计算具有更强的资源能力和成熟完备的运维体系，企业能够借助云上的软件应用和数据服务，降低成本、提高生产管理效率、优化业务流程。

一方面，企业运营过程中，基础设施架构是成本投入的重要组成部分，企业通过选择公平台服务，在应用设计、生产、营销、办公、财务等环节，租用存储、计算、网络等基础设施资源，极大地减少了对于建设机房、购买服务器等硬件设备的成本开支。另一方面，与传统的 IT 方案相比，企业采购云服务可以满足企业弹性、快速地根据业务需要调整设施的能力，实现便捷、灵活管理，推动业务创新和技术创新。

如您需要了解我们的出版物，
请联系:

Publication@llinkslaw.com

[1] 智研咨询: 《2017-2022 年中国云计算市场行情动态与发展前景预测报告》。

国家政策鼓励企业上云。《国务院关于促进云计算创新发展培育信息产业新业态的意见》《推动企业上云实施指南(2018-2020)》《关于推进“上云用数赋智”行动 培育新经济发展实施方案》均要求各地政府相关部门优化企业上云环境，推进企业上云工作。▶▷例如，《推动企业上云实施指南(2018-2020)》提出“利用保险模式对上云企业给予保障”；《关于推进“上云用数赋智”行动 培育新经济发展实施方案》进一步强化数字化转型金融供给，要求“对于获得国家政策支持的试点平台、服务机构、示范项目等，原则上应面向中小微企业提供至少一年期的减免费服务”。这些政策的出台在一定程度上消减了企业上云的后顾之忧，促使企业加快上云步伐。

疫情促使企业上云。疫情期间远程办公、视频会议、员工培训、协同研发、电子商务等巨大需求要求企业在短时间内部署云服务，以实现降本增效，业务持续创新发展。实践表明，云计算等信息技术的采用对疫情防控和企业复工复产发挥了关键作用。

二. 云上风险

在云环境下，企业的业务运行，数据存储、处理、传输等都与云服务商所提供的服务质量密切相关。一旦云服务商出现软硬件问题或是管理上的失误，都将引发云上企业的数据安全问题，进而对业务造成不同程度的影响。

云服务相关的网络安全事件在国内外层出不穷，不少云服务头部企业也不免“翻车”。▶▷例如，2018 年 8 月国内某头部云服务商即发生了客户数据丢失事件，根据该服务商官方声明，由于硬盘静默错误及数据迁移过程中的不规范操作，用户使用其服务器八个月期间的用户数据和内容数据全部丢失。[2]再如，2019 年 7 月美国第一资本金融公司(Capital One)被曝一名软件工程师利用 Capital One 系统防火墙的漏洞，侵入了其保存处理客户数据的亚马逊云服务平台(AWS S3)的服务器并窃取了数百万信用卡申请资料，包括 14 万个社会安全号和近 8 万个银行账号，Capital One 因此面临集体诉讼。

云服务商导致的网络安全事件频发，▶▷例如埃森哲曾因 AWS 服务器配置不当导致约 15 万患者的姓名、地址、医生、病历记录及血液检查结果等隐私信息暴露在网上；**也可能因企业用户自身疏漏导致，**▶▷如联邦快递曾因其 AWS 存储服务器没有设定密码保护致使关键数据泄露。在此前引起广泛热议的微盟删库事件中，由于云服务商微盟的运维人员恶意删库，大量用户蒙受了难以估量的经济损失。一系列网络安全事件在企业争先恐后上云的过程中拉响了风险警报，据 SANS Institute 发布的《2019 年云安全报告》统计分析，当前云环境所面临的安全风险最显著的是黑客攻击，其次是错误配置问题，除此以外还包括系统漏洞和安全缺陷、账户劫持、内部恶意行为等问题。

[2] 关于客户“前沿数控”数据完整性受损的技术复盘: https://cloud.tencent.com/developer/article/1180156

三. 采购协议重点条款

企业决定上云多出于商业需求考量，即需要某种特定产品、云服务的价格因素、服务商的相应速度、或倚赖服务厂商的声望，往往忽视云服务采购协议中对于数据保护和责任划分的约定。当发生网络安全事件时，企业无法依赖合同条款保障自身权益，诉诸争议解决机构往往也无济于事，这对企业而言是生死攸关的。

为尽可能降低云上风险，企业除根据安全需求和云计算服务的安全能力进行服务商的选择外，还需与云服务商就协议条款进行磋商，以保障自身权益。根据当前实践，我们为上云企业在采购云服务时应当重点关注的协议条款做出如下提示。

(1) 明确法律地位以划分权责

由于部署模式和云计算环境的复杂性，云服务模式中的业务运维主体和数据安全责任主体并非全然一致。从责任分配的角度而言，遵循权责一致的原则，在数据收集、处理和利用的过程中，数据控制者承担着首要的数据安全管理责任和风险。根据《个人信息保护法(草案)》中“个人信息处理者”的定义，和《信息安全技术 个人信息安全规范》中“个人信息控制者”的定义，数据控制者应被理解为“有能力决定数据处理目的、方式等处理事项的组织或个人”。因此，实践中企业通常被认定为数据控制者，而云服务商是否具有数据控制者的地位应视情况而定。

若在某项云服务中，云服务商能够完全控制并有权决定云服务平台中部分数据的处理事项，则其实质上已具有数据控制者的地位。▶▷例如，通过互联网登录和使用 SaaS 提供者的软件，且该种软件安装于完全由 SaaS 提供者建立并运维的数据中心，数据中心亦由云服务商的技术人员进行运维。该种情况下，上云企业可在协议中明确云服务商与其构成“共同数据控制者”，以加强云服务商的数据安全责任。若无法将云服务商列为共同数据控制者，则应根据云服务商在数据处理、存储活动中实际具有的权限，列明其能够自行决定的数据处理活动的范围和程度，如明确数据的访问条件、访问标准等。

(2) 数据安全性、完整性和可用性

企业在采购云服务时应重点关注数据在服务器中的安全性、完整性和可用性。但事实上，无论是 IaaS、PaaS，还是 SaaS 服务，数据的安全性、完整性和可用性均依赖于云服务商的安全保护能力以及其所采取的安全措施，但不同服务模式下安全措施所针对的客体不同。云服务商通常把其实施的安全措施及安全状态视为知识产权和商业秘密，企业用户在无法(或客观没有能力)行使知情权的情况下，难以对这些安全措施进行有效监督和管理，增加了企业数据安全风险。▶▷根据我们的观察，目前多数云服务商在协议中设计了“最大努力”条款，以表示其在履行数据安全保护义务方面的竭诚努力，例如亚马逊在服务合同条款中声明“将会尽最大的努力来保护数

据安全”，阿里云在服务合同中承诺“不断提升服务质量及服务水平”。这类条款看似服务商给企业用户的一颗“定心丸”，但其本质上为免责条款，无法充分有效保障用户利益。

因此，企业应首先明确自身的数据及业务系统的安全管理需求，在协议中针对不同重要程度的业务数据约定不同级别的安全措施，尤其关注是否与其他企业共享云计算平台、对相关技术人员技能的要求、业务持续性和可扩展性、数据可移植性和互操作性等问题，并且要求云服务商在系统开发与供应链安全、系统与通信保护、访问控制、配置管理、维护、应急响应与灾备、审计、风险评估与持续监管、安全组织与人员、物理与环境保护等方面均达到相应的国家标准和行业标准。相关服务水平协议应参照《信息安全技术 云计算 云服务级别协议基本要求》的规定，同时宜将该基本要求作为采购协议的附件由双方共同签署确认。

(3) 数据查询、访问、使用权限

现行实践中，云服务商多保留了自由处理用户数据的权利，其能够视情况拒绝提供服务、关闭账户或改变存储内容，且许多企业用户可能并没有相应的意识或做好应对措施。▶▷例如，苹果的云存储服务规定，其具有“无须预先通知而在任何时间由其自行决定预先筛选、移动、拒绝、修改或移除内容”的权利；又如阿里云的服务合同包含类似的自由访问数据条款，“您一旦开通服务即意味着您授权阿里云对您开通服务应用的用户的访问行为数据进行收集及分析计算”。此外，虽然多数云服务商明确其无权审查企业数据，但其仍能够通过对客户的资源消耗、通讯流量、缴费等数据的收集分析，获取企业的大量运营数据。

因此，我们建议企业在采购协议中与云服务商明确约定数据的相关权利归属，包括所有权、查询、访问和使用权限。例如，企业提供给云服务商的数据、设备等资源，云服务平台上企业业务系统运行过程中收集、产生、存储的数据和文档等都应归企业所有，企业对这些资源的访问、利用、支配、迁移等权利不受限制，而云服务商未经授权，不得访问、修改、披露、利用、转让、销毁企业数据。

(4) 跨境数据存储

企业在云环境中难以控制数据的实际存储位置，尤其是对于一些境外的云服务商，其可能将部分数据存储在境外的数据中心。目前我国法律明确规定特定种类的数据应本地化存储，例如人口健康信息、健康医疗大数据、关键信息基础设施所掌握的重要数据等。因此，涉及到这类特别监管的数据，企业在采购云存储服务时应特别关注数据的实际存储位置，要求云服务商将相关数据存储于中国境内，且不得依据其他国家的法律和司法要求将企业数据提供给其他国家的第三方。

此外，企业若在数据跨境传输或处理的过程中发生争议或法律适用冲突，难免因不熟悉适用法律或不同法院持有的不同法律适用态度而面临败诉风险。因此，企业还应特别关注云服务商提

供的协议中的域外管辖情况，若采购的云服务涉及其他司法管辖区，企业应与云服务商就争议解决条款进行协商，尤其是准据法和管辖地。

(5) 退出

服务到期或发生服务变更都可能导致企业退出云服务，或将数据和业务系统迁移到其他云计算平台上。没有云服务商的配合，企业很难独自将存放在云服务平台中的数据安全迁出，尤其是在双方发生纠纷、缺少事前约定的情况下，云服务商可能以删除或不归还数据为要挟，损害企业对数据的所有权和支配权。

因此，企业应在协议中与云服务商提前商议并约定退出条件，退出时双方的责任和义务，以及数据和业务系统迁移出云计算平台的接口和方案。当服务终止时，云服务商有义务安全完整地返还数据，配合企业将所有数据迁出，并通过相应条款规定数据迁出期间的数据保护义务和相关费用结算问题。当数据迁移完成后彻底删除平台上的企业数据，并继续承担企业退出服务后的保密义务。当然，若企业有数据留存需求，则应明确要求云服务商予以留存。

四. 结语

对于企业而言，上云并不意味着万事大吉，企业仍应注意自身网络安全义务，例如落实网络安全等级保护义务，聘请专业评测机构协助测评并备案；制定网络安全事件应急预案并根据预案及时处置安全风险；履行网络信息安全和个人信息保护责任；涉及数据出境时按照相关规定履行安全评估手续等。

此外，尽管法律法规对于企业和云服务商之间权责划分尚未有明确规定，但企业仍应根据项目实际情况与云服务商在协议中明确网络安全边界责任，例如通常在 IaaS 模式中，企业应负责其自行部署在云上的业务应用、数据库及中间件的安全管理，各类可控资源的安全配置，包括对虚拟网络资源安全防护，对云资源账户进行安全策略配置，对运维人员实施权限管理及职责分离，对云产品进行合理的安全策略配置。

如您希望就相关问题进一步交流，请联系：

潘永建
+86 21 3135 8701
david.pan@llinkslaw.com

如您希望就其他问题进一步交流或有其他业务咨询需求，请随时与我们联系：**master@llinkslaw.com**

上海	北京	深圳
上海市银城中路 68 号 时代金融中心 19 楼 T: +86 21 3135 8666 F: +86 21 3135 8600	北京市建国门北大街 8 号 华润大厦 4 楼 T: +86 10 8519 2266 F: +86 10 8519 2929	深圳市南山区科苑南路 2666 号 中国华润大厦 18 楼 T: +86 755 3391 7666 F: +86 755 3391 7668
香港	伦敦	
香港中环遮打道 18 号 历山大厦 32 楼 3201 室 T: +852 2592 1978 F: +852 2868 0883	1/F, 3 More London Riverside London SE1 2RE T: +44 (0)20 3283 4337 D: +44 (0)20 3283 4323	

www.llinkslaw.com

Wechat: LlinksLaw

本土化资源 国际化视野