

云服务合同重点法律问题与责任初探(上)

作者：潘永建 | 左嘉玮 | 吴若衡

随着互联网与实体经济的深度融合，企业数字化转型成为必然趋势，而云服务也成为其中不可或缺的一环。2021 年，中国整体云服务市场规模已经达到 3280.2 亿元，而其中非公有云市场规模接近 1000 亿元¹。目前，云服务在提升资源质量、优化技术能力、升级伙伴能力、升级生态能力、为传统行业引入解决方案等领域发挥了重要作用。

与此同时，在企业使用云服务的过程中，也产生了许多新的法律问题。本文探讨云服务合同的重点法律问题及法律责任分配，以期为企业使用云服务提供合规建议。本文上篇从规范性文件和市场实践两方面分析云服务商与云用户之间在数据处理环节下的角色与责任分配，下篇结合相关案例，从用户角度探讨云服务合同的主要风险及注意要点。

一. 云服务简介

云服务，是基于互联网相关服务的增加、使用和交互模式，通常涉及通过互联网来提供动态易扩展且通常呈现为虚拟形态的资源。

根据部署方式的不同，云服务系统可分为传统部署型(包括本地部署 On-premise 和 IaaS)、PaaS 型和 SaaS 型。

- (1) 传统部署型是最早诞生的形态，为买断型，但企业需购买物理服务器(本地部署)或租用云服务器等(IaaS)自行搭建 IT 基础架构，前期投入成本占比较大。
- (2) SaaS 型则属于租用型，企业无需自备服务器，只需按期订阅，因此交付周期较短、部署门槛较低，但在数据安全和灵活性方面有所不足。
- (3) PaaS 型同样属于租用型，但在集成度和扩展性方面更胜一筹，可以扩展 CRM 功能模块。

.....
如您需要了解我们的出版物，
请联系：

Publication@llinkslaw.com

¹ 《2022 年基础云服务行业发展洞察》，<https://mp.weixin.qq.com/s/svKFqL3LdqtI9BNEHai3Q>

二. 云服务商与云用户之争：以 IaaS 部署模式为例

如上所述，云服务商的云服务模式可主要分为 SaaS 型、PaaS 型、IaaS 型三类(除纯本地化部署的 On-premise 类型之外)。而针对每一种云服务模式，由于其负责管理运行的主体、数据安全的责任主体不同，相互之间的法律责任如何界定和分配也相应地需要区分情形加以讨论。

由此，我们拟以云用户常用的 IaaS 型部署模式为例，从引发法律责任的两种情形出发，即发生因违法处理个人信息而侵害个人信息权益的事件(个人信息侵权责任)，或发生数据泄露、丢失等安全事故(数据安全风险)，梳理并探讨理论及实践中云服务商与云用户两者之间的法律关系及法律责任。

(一) 个人信息处理与侵权责任

企业用户在使用云服务期间，或因用户的投诉、举报企业违法处理个人信息而引发个人信息侵权责任，如侵害个人信息主体享有的知情同意权、限制处理权、访问复制权等。因此在发生该类个人信息侵权事件时，应首先厘清云服务商和企业之间的法律关系，从而明确其责任分配。

在个人信息处理方面，两者之间的法律关系可参考欧盟 WP29 的指南。企业可被认定为属于 GDPR 中的“数据控制者”，决定和控制收集和处理个人数据的目的；云服务商属于“数据处理者”，代表数据控制者行事，并且仅按照数据控制者的指示行事。我国《个人信息保护法》对于“个人信息处理者”的定义实则与 GDPR 下“数据控制者”相似，指“在个人信息处理活动中自主决定处理目的、处理方式的组织、个人”。通常情况下，云服务商不会访问企业上传于云服务系统中的数据，更无法自主决定数据的“处理目的、处理方式”，因此，在《个人信息保护法》定义下，也可以认为两者在个人信息处理方面构成了委托处理关系，即企业属于“个人信息处理者”，而云服务商属于“受托处理者”。

实践中，云服务商也会强调自身受托者的身份，如在《隐私政策》中强调其相关政策仅适用于使用云服务的企业，而不适用于终端用户。示例如下：

百度智能云 APP 隐私政策(2022 年 9 月 8 日)

本隐私政策适用于您通过【百度智能云】的【APP 端】来访问和使用我们的产品和服务。

本隐私政策不适用于我们作为受托人，根据委托人的委托要求处理您的个人信息、用户数据或业务数据。我们将与委托人签订协议，在确保不低于委托人要求的个人信息保护水准的前提下为委托人提供数据处理服务。

阿里云 APP 隐私权政策 (2022 年 9 月 23 日)

一、本协议的适用范围

- 1.1. 本政策适用于阿里云 APP 所有服务。服务包括向您提供内容浏览、APP 登录服务，以及通过阿里云 APP 向您提供的技术服务。
- 1.2. 本政策不适用于其他第三方向您提供的服务，该服务适用其向您另行说明的隐私权政策等个人信息收集适用规则。例如，阿里云云市场上的服务商依托云市场向您提供服务时，您向服务商提供的信息不适用本政策。
- 1.3. 需要特别说明的是，作为阿里云的用户，若您利用阿里云的技术服务，为您的用户再行提供服务，**因您的业务数据属于您所有，您应当另行与您的用户约定隐私权政策。**

因此，一般而言，在发生个人信息侵权事件时，应由企业作为个人信息处理者承担责任，而云服务商作为受托方无需担责。

(二) 数据安全责任

1. 规范性文件

在数据安全责任方面，由于涉及不同安全层级、而每一层级的安全责任分配各有不同，其情形较个人信息的侵权责任更为复杂。以工信部于 2022 年 4 月发布的《云计算安全责任共担模型》(YD/T 4060-2022)²，以及云计算开源产业联盟于 2020 年发布的《云计算安全责任共担白皮书》的责任分配模型为参考依据，从底层物理数据中心到上层数据可共分为七类，即包括物理基础设施、资源抽象和管理、操作系统、网络控制、应用、数据、身份识别和访问管理。

其中，底层安全责任一般由云服务商承担，上层安全责任则由云用户负责，除两者独立承担的责任外，中间部分安全责任由两者共同承担。以 IaaS 模式为例，概括如下：

IaaS 型	物理基础设施安全		云服务商
	资源抽象和管理安全		云服务商
	操作系统安全		云用户/云服务商
	网络控制安全		云用户/云服务商
	应用安全		云用户/云服务商
	数据安全	数据存储安全	云服务商
		数据传输安全	云服务商
		数据访问安全	云服务商

² 《云计算安全责任共担模型》(YD/T 4060-2022), <https://hbba.sacinfo.org.cn/attachment/onlineRead/65f9104378e423d06560c25356042b4fc77511c93dab912c655aa8f9f1d65e62>; 《云计算安全责任共担白皮书》, <https://v3.opensourcecloud.cn/static-file/media/72/f4/8219a38e2aceb64294a828fa428e1476.pdf>

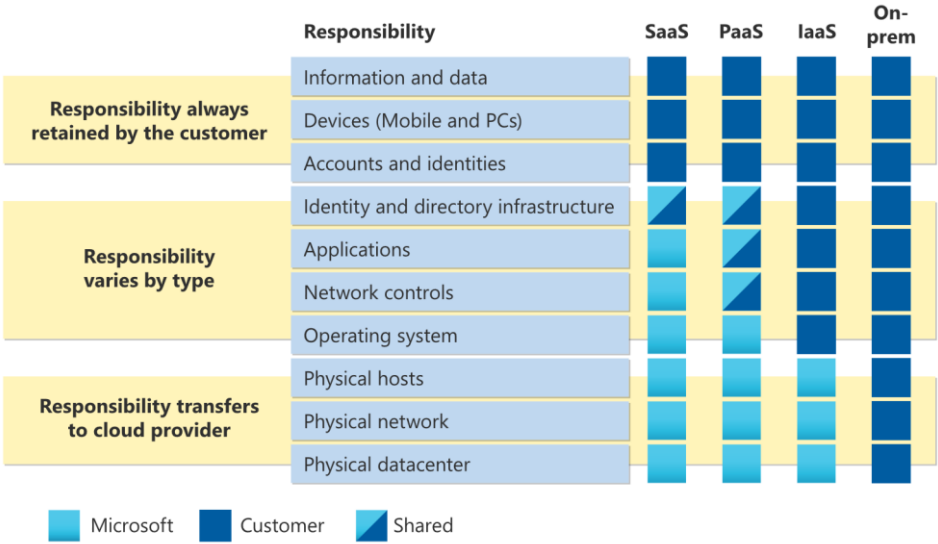
		数据迁移安全	云用户/云服务商
		数据销毁安全	云服务商
		数据安全	云用户
		安全审查和取证	云服务商
		个人隐私信息安全	云服务商
	身份识别和访问管理(IAM)安全		云用户/云服务商

可以看出，在 IaaS 模式下，底层的物理基础设施安全、资源抽象和管理安全一般应由云服务商提供者负责，而操作系统安全、网络控制安全、应用安全、数据安全、IAM 安全由云服务商提供者和云服务用户共同负责。

2. 实践

上一部分已详述工信部和行业白皮书中对两者安全责任的界限划分，而实践中，一些知名云服务商所采用的责任共担模型则略显不同。以国外的微软 Azure，以及国内的腾讯云为例（见下图），他们搭建的责任共担模型的安全层级更多且更精细，但总体上仍然遵循了“底层安全云服务商负责，上层安全云用户负责，中间安全共同承担”的责任分配思路，与相关标准基本一致。

微软 Azure 责任共担模型³:



腾讯云安全责任模型⁴:

³ Azure 云中责任分担, <https://learn.microsoft.com/zh-cn/azure/security/fundamentals/shared-responsibility>

⁴ 腾讯云安全责任共担, <https://cloud.tencent.com/services/security>

	IaaS	PaaS	SaaS
客户的责任	数据安全 终端安全 访问控制管理 应用安全	数据安全 终端安全	数据安全
责任共同部分	主机和网络安全	访问控制管理 应用安全	终端安全 访问控制管理
腾讯云责任	物理和基础架构安全	主机和网络安全 物理和基础架构安全	应用安全 主机和网络安全 物理和基础架构安全

下篇我们将从云服务用户的角度解析云服务合同的主要风险及注意要点。

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

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

北京市朝阳区光华东里 8 号
中海广场中楼 30 层
T: +86 10 5081 3888
F: +86 10 5081 3866

深圳

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

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

伦敦

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

免责声明：

本出版物仅供一般性参考，并无意提供任何法律或其他建议。我们明示不对任何依赖本出版物的任何内容而采取或不采取行动所导致的后果承担责任。我们保留所有对本出版物的权利。

© 通力律师事务所 2023