Deloitte.
Insights

本地部署：云主权成为未来焦点

随着数据爆炸式增长、网络安全威胁加剧和地缘政治紧张局势升级，对本地化云解决方案的需求有望增加。满足这一需求可以保护公司的声誉、运营和利润。

预计到2024年，全球数据量将达149ZB。 云计算使该规模的数据创建和处理成为可能。[1]泽字节 (ZB) 代表十万亿亿字节。如果每个字节都是一粒沙子，那么这些沙子几乎可以填满地球上所有海滩两万次。[2] [3]

云计算现已成为重要的基础产业，预计到2023年市场规模将达到近6,000亿美元。[4]云计算是转型变革的驱动力，促进服务交付的改善，帮助实现劳动力流动，并开创分析和人工智能的新领域。云计算基于以下理念——数据位置并不重要，至少没有规模经济或快速启动运行中的计算资源的灵活性那么重要。随着存储数据的数量、价值和敏感性激增，“云主权”，即存储在云中的数据应受其实际所在国法律的约束，这一原则已成为政策制定者关注的焦点。

德勤预计，2024年，所有发达市场的各国政府都将加强对云主权的重视。因此，政务云（为满足政府机构严格的合规要求而设计的解决方案组）市场规模预计将超过410亿美元，比2023年增长16%。[5]分布式云（符合数据驻留限制的解决方案）市场规模预计将从2022年的40多亿美元增至70亿美元。[6]

云计算发展历程简述

云计算的概念可以追溯到互联网的早期，从20世纪60年代的分时共享[7]到20世纪90年代的电信虚拟专用网络（VPN）。[8]但2005年，亚马逊推出了云计算服务Amazon Web Services (AWS)，[9]标志着发生了范式转换，为大众带来了可扩展的按需计算。谷歌、微软等公司纷纷效仿，推出了各自的云平台，巩固了云计算在现代化数字基础设施中的基础地位。

过去二十年中，企业、政府、机构和公民逐渐将其数据和工作负载从私有基础设施（例如办公室橱柜中的服务器机架）转移到一体化云数据中心。在此期间，很多还采用了新的“云原生”应用程序。随着大量数据在全球网络中存储和传输，部分政府和企业开始关注数据的管辖权、治理和所有权，“云主权”一词开始受到关注。

法律冲突引发国际摩擦

数据本地化法律给全球企业运营带来复杂性。随着各国努力应对国家安全、数据保护和新技术，相关法规往往频繁变动。预计企业将越来越依赖数据、自动化和人工智能。他们应该考虑法规变动、失效或增补。当前，确保合规性至关重要，保持运营灵活性亦是如此。能够快速适应监管框架的变化至关重要，数百个国家均表明了自身监管立场，各个国家有着细微差别，其中一些国家的法规可能与其他国家不一致。

迄今为止，欧洲法院已宣布欧盟与美国之间达成的多项跨大西洋数据传输协议无效（见图1）。过去十年中，与主权相关的法规陆续出台，如欧盟《通用数据保护条例》（GDPR）、美国《澄清境外数据合法使用法》（CLOUD Act），以及多项州级立法提案，如《加州隐私权法》（CPRA）。

如前所述，全球企业需应对不同的本地化法律。例如，美国《澄清境外数据合法使用法》授权美国政府出于特定的执法目的访问存储在境外的数据，但根据欧盟《通用数据保护条例》，个人数据只有在得到“充分”数据保护的情况下才能传输至欧洲经济区以外国家。[10] [11]如果公司按照美国《澄清境外数据合法使用法》发布数据，但违反了欧盟《通用数据保护条例》，则可能面临巨额罚款。[12]在某些情况下，各国政府可达成双边协议，如英国与美国之间达成的协议，[13]但这并非一朝一夕可以实现。相反，公司通常会采用端到端加密技术，只有发送方和接收方才能解密数据。这意味着，虽然服务提供商可能会将数据移交执法部门，但如果没有解密密钥，这些数据将无法破解。

图1：欧盟与美国主权法规的重大变动：不断变化的政策环境

欧盟与美国之间达成了多项重要的跨大西洋数据传输协议：

2020	**《安全港协议》**	该框架确保美国公司可将个人数据从欧盟传输至美国，同时遵守欧盟数据保护标准。[14]
2013	**斯诺登泄密事件**	美国国家安全局大规模监控事件的曝光，引发了全球对数据隐私、政府监控的关注，并再次引发了对数据主权的讨论。
2015	**安全港协议》失效（又称Schrems I）**	由于担心美国监控法律损害欧洲隐私权，欧洲法院宣布《安全港协议》无效。[15]
2016	**欧盟-美国隐私保护框架》**	欧盟与美国达成新框架，即《欧盟-美国隐私保护框架》，以弥补安全港协议的不足，并制定新的跨大西洋数据传输机制。[16]
2016	**欧盟《通用数据保护条例》**	欧盟出台了《通用数据保护条例》（GDPR），对欧盟境外的数据传输制定了严格规定，要求企业确保欧盟个人数据按照适当的保护措施进行处理。[17]
2018	**美国《澄清境外数据合法使用法》**	出台了《澄清境外数据合法使　法》（CLOUD Act），允许美国执法机构出于特定的执法目的，要求科技公司提供其存储在任何地理位置的个人数据。[18]
2020	**《欧盟-美国隐私保护框架》失效（又称“Schrems II”）**	欧洲法院宣布《欧盟-美国隐私保护框架》无效，同样是出于对美国监控法律和美国对欧洲公民数据保护不足的担忧。[19]
2023	**《欧盟-美国数据隐私框架》**	美国和欧洲领导人宣布了一项框架，取代《欧盟-美国隐私保护框架》，其中包括制定新的补救机制设和设立数据保护审查法院，来审理跨大西洋数据传输案件。[20]

来源：德勤研究

为了应对复杂的监管环境，数据管理至关重要。企业应了解其拥有的各种数据类型，以及各系统中的数据分类（例如，个人信息、支付数据、受监管的金融信息等）。企业还应考虑从当前云服务提供商的“退出战略”，以防未来主权受到侵犯或监管环境发生变化。然而，云计算服务合同期限（可能长达五年或以上）和高昂的出口费用（从云服务提供商处迁移数据的费用）或将阻碍客户在云服务提供商之间的数据迁移。

本地部署是一项全球性挑战

欧盟和美国之间的关系是制定数据主权框架的典型例子，但并非唯一的例子。全球范围内，许多其他国家也对数据本地化表明了自身立场（以下并非详尽清单）：

俄罗斯：俄罗斯是最早和最严格实施数据本地化部署的国家之一，俄罗斯第242-FZ号联邦法规定，俄罗斯公民的个人数据须存储在本国境内。[21]这对全球公司和品牌产生了深远影响。例如，自2016施行数据本地化法律以来，LinkedIn在俄罗斯的访问受到限制。[22]

中国：《中华人民共和国网络安全法》（2017年）规定关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。[23]随着《中华人民共和国数据安全法》和《中华人民共和国个人信息保护法》（2021年）相继颁布，中国坚定了数据本地化立场，对数据进行分类，并根据分类情况对跨境数据传输进行管理。[24]

沙特阿拉伯：沙特阿拉伯于2018年颁布了《云计算监管框架》（CCRF），[25]该框架规定了云服务提供商的数据主权条件，并对某些类型的数据实施数据驻留。2021年，沙特阿拉伯颁布了《个人数据保护法》，根据该法，公民个人数据仅在少数情况下可传输至境外。[26]

数据主权问题或将升级

数据主权已成为全球焦点议题，其重要性可能还会上升。2024年及以后，以下因素可能会变得更加突出：企业与政府之间有关个人数据的紧张关系、俄乌战争等地缘政治紧张局势、混合云与多云结构混合的云复杂性以及数据保护和网络安全问题。企业和政府对数据的依赖性极强，云或将成为数据存储、管理和分析的实用解决方案。

企业与政府：国家安全与个人隐私之间需找到平衡，引起高度关注的案件往往敦促政府对数据设定明确的管辖界限。例如，2016年，在美国联邦调查局 (FBI) 的恐怖袭击事件调查中，苹果公司 (Apple) 拒绝解锁疑犯的iPhone手机，该事件被炒的沸沸扬扬。[27]虽然此案未跨司法管辖区，但凸显了权衡国家安全机构的利益与数据隐私权及科技公司保护用户数据的责任的复杂性。不过，类似案件也发生过跨司法管辖区的情况，例如2013年微软与美国政府之间就存储在爱尔兰的与毒品调查有关的数据所产生的纠纷。[28]

地缘政治：大国之间的全球紧张局势导致技术和数据成为外交和贸易冲突的领域。[29]俄乌战争使数据管辖权问题成为焦点议题，乌克兰迅速将人口登记、土地和财产所有权、纳税记录和教育记录等关键数据迁移至云端。[30]另一方面，美国云服务提供商在俄罗斯入侵后不久就暂停了在俄罗斯的销售。[31]

云复杂性：最初，云服务是指将本地业务转移至单个云服务提供商。然而，当前企业往往同时使用多个云平台（被称为多云策略），从每个提供商的功能中获益，削减成本，提高业绩和提升可扩展性。另一种常见策略是混合云——将私有 (本地) 云和公共云解决方案相结合，让数据敏感型应用程序保留在内部，而其他工作负载则可从公共云的庞大资源中获益。多云和混合云策略在提供灵活性和实现优化的同时，也带来了挑战。数据分散在不同环境中，可能跨越不同司法管辖区。每家云服务提供商的数据中心可能分布在诸多国家，各国均颁布了独特的数据保护法规。这使得数据主权的管理和治理比以往更加错综复杂，已不再仅需遵循某个国家的规则，而是要了解复杂的全球法规情况。

数据保护与网络完全：生成式人工智能、机器学习和自动化 (通常采用云计算实现) 或将成为企业运营的关键，促使政府在数据管辖权方面更趋严格。数据泄露事件已屡见不鲜，在某些情况下，数据本地化可降低风险。2020年，多个美政府机构遭受SolarWinds黑客攻击事件的影响，凸显了集中式云系统的脆弱性。[32]在此次攻击事件中，黑客在例行软件更新中插入恶意代码，这表明应在整个供应链中强调安全和主权问题的重要性，而不仅仅是在其中某个环节。企业应了解其使用的软件即服务和第三方提供商：在哪个云平台上运行、处理的数据类型、加密等级、以及存在的风险。此类事件充分说明，各国有必要对涉及本国公民的数据加强控制和监督。网络安全挑战将进一步加剧：预计到2024年，网络犯罪造成的损失将达14.6万亿美元，是2021年6万亿美元损失的两倍多。[33]

数据主权没有地理边界，还涵盖运营和治理。阿姆斯特丹贸易银行 (Amsterdam Trade Bank) 就是一个例子，2022年，该银行因所有权归属于俄罗斯而受到美国政府的制裁。[34]该银行的数据可能驻留在欧洲，但拥有运营控制权的云服务提供商却位于美国，且仍能撤销对公司电子邮件账户和相关数据的访问权限。为应对此类风险，云服务提供商与本地运营商开展合作，一些政府和其他实体要求，光是确保数据驻留在某个地区还不够；还需确保云基础设施运营商也位于本地。[35]

随着世界变得更加数字化，划定边界、确保安全和保护公民权利的需求变得日益重要。在地缘政治、安全问题和个人权利保护的推动下，预计未来几年对数据和云主权的重视程度将进一步加强。

数据主权解决方案对云服务提供商来说既是机遇也是挑战

云服务提供商认识到数据主权日益重要，因此推出了各种产品、服务和功能。政务云解决方案就是一个例子，旨在为满足政府机构严格的监管和合规需求而量身定制的云计算环境。

云服务提供商已将云服务扩展到企业边缘。其中一个例子是完全托管服务，对客户基础设施（以及云服务）进行本地化部署。[36]另一项服务允许企业从自身数据中心运行云服务，确保数据储存在本地或特定管辖区内。云服务提供商往往会提供各种解决方案组合，以满足因监管要求而需将数据保留在特定区域内的企业的需求。[37]

此类产品与“分布式云”相一致，尽管所有产品可能未严格标注为“分布式云”。分布式云是指将公共云服务分布到不同的物理位置，由原始公共云服务提供商负责云服务的运营、治理、更新和演进。简单而言，就是让云服务更接近数据产生和使用的地方。

虽然分布式云服务能带来诸多益处，包括提供低时延，但与传统云服务相比，也存在一些劣势，例如：

- **高成本**：分布式云解决方案通常需要在硬件和基础设施方面进行前期投资，而传统云服务则采用即付即用模式。此外，即使大型云服务提供商负责管理软件堆栈，本地硬件也可能带来额外的维护成本。最后，IT团队需进行培训，从而高效管理和运行这些全新分布式云环境。
- **复杂性**：将分布式云服务与现有本地系统集成可能较为复杂。以混合云或多云模式运行可能意味着要在不同环境中管理工作负载。
- **应用范围较小**：分布式云服务可能不具备集中式公共云可用的全套功能。集中式云可用的功能和更新可能需要一段时间才能在分布式云平台上提供。
- **缺乏可扩展性**：传统公共云服务具有几乎无限的可扩展性，而分布式云解决方案可能会受到本地基础设施容量的限制。增加容量或需进行额外的硬件投资，而在传统云中，通常只需通过软件提供更多资源。
- **供应商锁定**：依赖特定云服务提供商的分布式解决方案可能会导致供应商锁定，使得在不付出巨大努力和支付高昂成本的情况下变更供应商或采用多云策略极具挑战。
- **性能**：本地分布式云硬件的性能可能并不总是与位于云服务提供商数据中心的基础设施性能相匹配。即使进行本地部署或边缘部署，也可能会出现数据需传输至集中式云的情况，进而造成潜在的网络瓶颈。

对云服务提供商而言，主权云需求增长将为销售更多高价值服务创造机会，但总体而言，这可能会削弱其盈利能力。对云服务提供商来说，经济上的最优结果是在每个司法管辖区不受限制地销售超大规模公共云。但全球云基础设施分散化，以及根据严格的合规要求定制架构，会导致运营成本上升，压缩利润空间，即使这些服务以更高的价格出售。尽管如此，对于本地服务提供商和传统硬件供应商来说，这是一个机遇，尤其是在客户越来越依赖混合云（因此需要大量基础设施）的情况下。

小结：企业应积极采取行动，而非被动应对

对于在当今全球数字经济中运营的企业来说，遵守数据存储、管理和处理的相关法规至关重要，不仅能避免重大的法律后果和巨额罚款，还有助于维护与客户和合作伙伴之间的信任。随着地缘政治紧张局势加剧，法规亟需更新，对数据隐私的担忧也将加剧，企业应对数据和云主权问题的能力直接影响其市场声誉、运营和利润。企业应积极采取行动，使自身处于有利地位。

首先，企业应进行全面的数据审计，包括确定数据来源，并根据数据敏感度进行分类。例如，个人用户数据与匿名分析数据或元数据的处理方式不同。如企业未采用数据驻留策略，也应考虑采用该策略。包括根据技术性能需求（如时延）和监管要求决定数据驻留位置，且可能意味着使用本地数据中心、分布式云或云区域。最后，企业应审查其数据存储和传输政策，确保数据在静态和传输过程中都经过加密。如果数据跨越国界，加密可提供额外的保护，防止未经授权的访问。

领先实践还包括投资以了解本地法规，需聘请本地专家，并为多个部门（如信息技术、法律、运营部门）的员工提供培训，特别是在法规发生变化时。除此之外，企业还应尽可能对合作伙伴保持透明度，向客户和供应链清晰传达数据存储和处理的方式和位置。特别是对于供应链而言，企业应确保了解供应商数据存储和处理的方式和位置。最后，企业还需制定数据遣返策略，以应对需将数据从云服务器或境外服务器移回本地服务器的情况。企业应确保与云服务提供商签订的任何合同中均有变更条款规定（如可行）。

云主权旅程应纳入当前云策略，所有云用户均需为可持续的云主权平台进行设计和架构。该旅程应包括三个阶段：

1. **建议阶段**：企业应确定其云主权立场，设计云主权策略（包括数据和工作量分类），并提供概念证明，为云主权做好准备。
2. **实施阶段**：企业应构建云主权并实施数据控制
3. **运行阶段**：企业应管理云主权生态系统，构建用于提高可观测性和风险监测水平的方法，并考虑实现自动化和成本优化。[38]

云主权是跨国企业的一项重大战略议题。妥善处理这些问题有助于增强客户信心，降低法律风险，并确保企业数据资产的安全。监管环境不可能一成不变。如果把每字节数据比作沙滩上的一颗沙粒，则监管变化就是能破坏、重塑和冲走沙粒的潮汐。企业应确保合规性，提高信任度，其中一个方法就是时刻保持警惕，不断学习，做好充分准备，以顺应监管变化趋势。

作者

Ben Stanton
United Kingdom

Alfons Buxo Ferrer
Spain

Gillian Crossan
United States**Ben Stanton**
United Kingdom

Paul Lee
United Kingdom

Adam Gogarty
United Kingdom

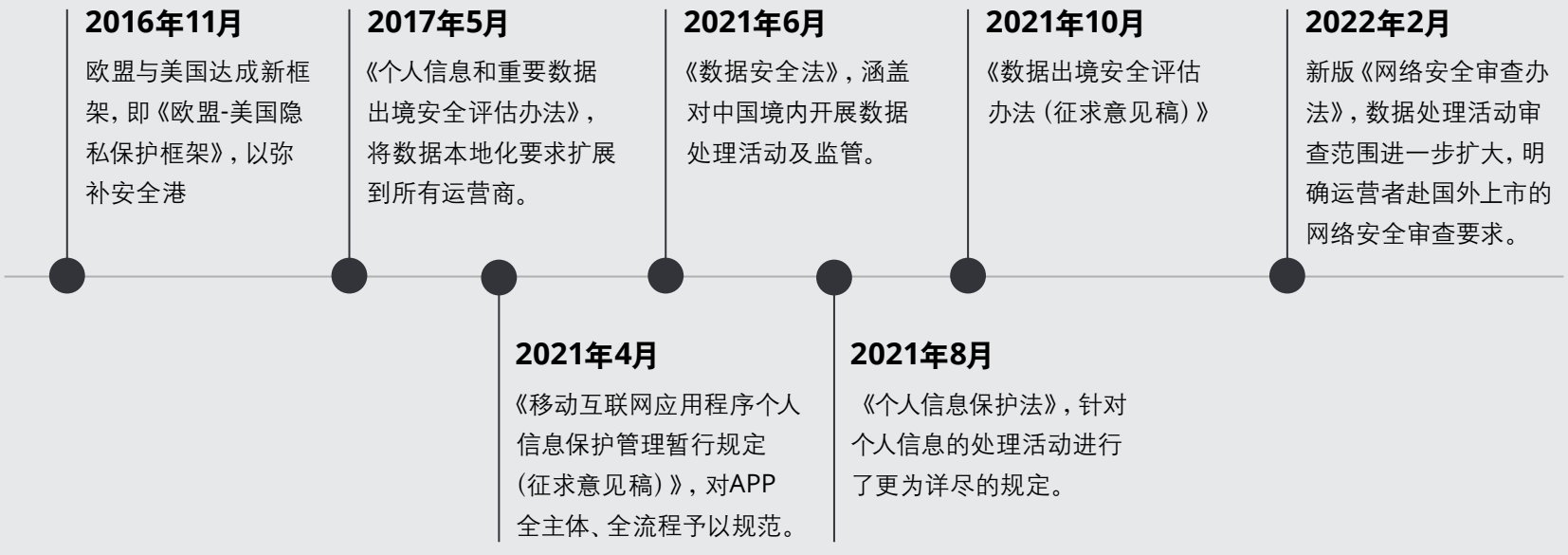
Kevin Westcott
United Kingdom

中国各行业企业迎来更为严格的数据安全监管要求

在东数西算、云网融合等重要国家战略规划的背景下，云计算正在为数字经济发展提供强有力的基础支撑。当前，云计算在金融、制造、服务、政务、电信等行业的应用占比持续攀升。从整体来看，我国云计算市场保持高速增长。2022年我国云计算市场规模达4,550亿元，相较于全球增速，我国云计算市场仍处于快速发展期，预计2025年我国云计算整体市场规模将突破万亿元。

虽然具有高性价比、高灵活性、动态可扩展特点的云计算技术得到了迅速发展和广泛应用，但云计算服务给数据存储带来极大的变革，最为突出的问题即是“数据”的主权归属问题。出于保护本国数据的目的，目前全球大部分国家和地区围绕数据的本地存储、利用、控制、隐私保护等开始构建其数据主权相关制度，中国也开展了相关立法和政策探索，确保我国的数据主权保护得到落实。

图：中国关于数据保护的代表性法律法规发布



来源：外部资料、德勤研究

2021年是我国数据安全立法元年，在《网络安全》的框架下，我国相关部门陆续制定了一系列法规标准，进而落实了跨境等数据处理活动的具体责任方、流程以及安全要求等，形成完善的数据主权保护体系。当前数据安全政策呈现出新趋势，各行业企业应抓好重点，在未来一年里加快提升数据安全保护能力。

1. **各行业企业需更加注重网络安全内容申报**。当前关于网络安全审查的申报条件逐步清晰和细化，涵盖了包括关键信息基础设施运营者采购活动，公司赴国外上市或境外设立总部、运营中心和研发中心等条件。未来审查内容将在实践中持续优化。
2. **金融机构在信息获取和使用、数据处理等方面面临更加严格的管理要求**。依照《个人信息保护法》，金融机构在线上、线下收集客户个人信息、数据流转共享、跨境提供客户个人信息的场景下，将打破“一揽子”格式条款，转变为需要取得个人的单独同意，并赋予客户便捷的行使撤回同意权。对于委托第三方供应商处理个人信息，金融机构应以显著的方式、清晰易懂的语言真实、准确、完整的向个人逐项告知委托处理具体场景等信息。因此，下一步金融机构将逐步开始调整系统设置和业务模式。
3. **智能网联汽车行业企业趋于强监管模式**。一方面，相关法律法规明确要求智联网汽车生产企业、车联网服务平台运营企业严格落实网络安全分级防护要求，按照危险程度采取相应的补救措施。另一方面，实施数据分类分级管理，定期开展数据安全风险评估，对需要跨境的数据，及时向所在省(区、市)主管部门报备。
4. **移动互联网平台企业提供的APP应用迎来更加严格的个人信息保护**。《个人信息保护法》禁止了“捆绑式同意”行为，要求APP平台企业在收集用户个人信息时从不同个人信息的适用场景、敏感度进行风险评估，并适配不同的同意机制。 这将对APP运营者的业务模式及合规管理产生较大影响。对于日常业务中涉及体量较大的个人（敏感）信息的关键信息基础设施运营者可能会涉及到履行数据本地化的义务，如生物医药、跨境电商、金融等行业。

综上，我国企业，特别是涉及国际业务、跨境业务、为国外机构或人员提供服务的企业，应当采取更为审慎和主动的态度经营业务，并及时采取细致和全面的应对措施，履行数据安全保护义务，具体可以从以下几个方面入手：

- **全面梳理企业自身业务和数据**。企业需首先明晰业务中可能涉及管控的数据类型，主要包括个人信息和重要数据。与此同时，审视各类业务场景中的数据需求和合规要求，明确合规治理以及应急处理机制重点。
- **完善企业数据分级管理保护机制**。根据产品或服务采集的数据来源、方式、类型的不同对数据进行划分，分类别、分级对数据管理，建立多元化有效的合规流程。对于具有敏感性、重要性的数据跨境采取谨慎态度，必要时遵循本地化要求；在涉及第三方数据处理时，应以协议明确共享数据的范围、内容、使用方法等权利义务，对第三方供应商提出要求并定期监督和审计，避免对跨境数据的滥用。
- **加强跨境业务和数据跨境中的数据安全保障能力**。一方面，企业对内部数据跨境场景进行识别，梳理出数据跨境流转情况，包括具体业务场景、涉及部门、数据主体所在地、涉及系统等；并立足自身业务场景、风险偏好等，制定重点国家/地区的数据跨境合规管控策略和控制点，以高中低风险形成适配统一的合规措施，避免陷入法律风险。另一方面，企业内部制定数据出境风险评估具体要求，包括跨境数据传输的合法性和必要性，数据敏感性、技术措施、以及境外接收方的安全管控能力等；组建涵盖技术、法务、安全等主体的评估小组，负责对数据出境的审核以及使用情况跟踪。
- **定期开展数据安全培训，积极配合监管需求**。在企业内部成立一个由IT和高级业务领导人组成的治理机构，结合最新监管趋势制定数据安全培训计划，定期对相关技术和管理人员进行数据、网络安全教育和培训。

作者

钟昀泰
中国

尾注

1. IDC and Statista, https://financesonline.com/how-much-data-is-created-every-day
2. How many grains of sand are on earth (7.5 x 1018), All The Trivia, https://allthetrivia.com/how-many-grains-of-sand-are-on-earth
3. 泽字节 (ZB)（1021, 因此149ZB = 149 x 1021) TechTerms, https://techterms.com/definition/zettabyte
4. Gartner, https://www.gartner.com/en/newsroom/press-releases/2023-04-19-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-reach-nearly-600-billion-in-2023
5. 德勤估计, 基于初步研究及IMARC Group、Mordor Intelligence、Straits Research和Data Bridge Market Research所开展的行业研究。
6. Markets and Markets, https://www.marketsandmarkets.com/Market-Reports/distributed-cloud-market-165173185.html
7. “By the early 1960s many people can share a single computer, using terminals... these are the first common multi-user systems.”, Computer History, https://www.computerhistory.org/timeline/1961
8. “PPTP & IPSec: VPN history starts when these protocols officially saw the light of day in 1995. But they were in development years before that date.”, TechNadu, https://www.technadu.com/vpn-history-over-the-years/89703
9. Amazon.com Launches Web Services (2002), Amazon Press Release, https://press.aboutamazon.com/2002/7/amazon-com-launches-web-services-developers-can-now-incorporate-amazon-com-content-and-features-into-their-own-web-sites-extends-welcome-mat-for-developers
10. 《澄清境外数据合法使用法》或CLOUD Act, https://www.congress.gov/bill/115th-congress/house-bill/4943
11. 欧盟《通用数据保护条例》(EU Directive 95/46/EC) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504
12. U.S. CLOUD Act vs. GDPR, activeMind.legal, https://www.activemind.legal/guides/us-cloud-act/
13. UK/USA: Agreement on Access to Electronic Data for the Purpose of Countering Serious Crime, UK Government, https://www.gov.uk/government/publications/ukusa-agreement-on-access-to-electronic-data-for-the-purpose-of-countering-serious-crime-cs-usa-no62019
14. 安全港历史简述 (2000-2016) IAPP, https://iapp.org/media/pdf/resource_center/brief_history_of_safe_harbor_2000_to_2016.pdf
15. 欧盟法院, https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf
16. 欧盟委员会, https://ec.europa.eu/commission/presscorner/detail/en/IP_16_216
17. 欧盟《通用数据保护条例》(EU Directive 95/46/EC) , https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504
18. 《澄清境外数据合法使用法》或CLOUD Act, https://www.congress.gov/bill/115th-congress/house-bill/4943
19. 欧洲议会, https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf
20. 欧盟委员会, https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en
21. WKO, https://wko.at/ooe/Branchen/Industrie/Zusendungen/FEDERAL%20LAW2.pdf
22. LinkedIn blocked by Russian authorities, BBC, https://www.bbc.co.uk/news/technology-38014501
23. The Diplomat, https://thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-need-to-know/

24. Skadden, https://www.skadden.com/Insights/Publications/2021/11/Chinas-New-Data-Security-and-Personal-Information-Protection-Laws
25. Saudi Arabia CCRF, https://www.cst.gov.sa/en/RulesandSystems/RegulatoryDocuments/Pages/CCRF.aspx
26. Clydeco, https://www.clydeco.com/en/insights/2021/09/saudi-arabia-issues-personal-data-protection-law
27. FBI ends stand-off with Apple over iPhone, Financial Times, https://www.ft.com/content/d1090a5c-0905-11e6-b6d3-746f8e9cdd33
28. Microsoft battles US over warrant for drugs case emails, BBC, https://www.bbc.co.uk/news/technology-34185575
29. 《云主权：欧洲公共领域的三大要务》, 德勤, https://www2.deloitte.com/uk/en/insights/technology-management/cloud-sovereignty-three-imperatives-for-the-european-public-sector.html
30. 'Russian missiles can't destroy the cloud': Ukraine leader describes emergency migration, The Register, https://www.theregister.com/2022/11/30/ukraine_cloud_migration/
31. Amazon, Microsoft and Google have suspended cloud sales in Russia, TechCrunch, https://techcrunch.com/2022/03/10/amazon-microsoft-and-google-have-suspended-cloud-sales-in-russia
32. SolarWinds hack explained, TechTarget, https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know
33. Cybercrime Expected To Skyrocket in Coming Years, Statista Technology Market Outlook, National Cyber Security Organizations, FBI, IMF, https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/
34. Solvent but bankrupt: how sanctions felled Amsterdam Trade Bank, Global Trade Review, https://www.gtreview.com/news/europe/solvent-but-bankrupt-how-sanctions-felled-amsterdam-trade-bank/
35. 例如, Hyperscaler和VMware主权云解决方案表明, 本地合作伙伴关系是产品和服务的关键, Analysis Mason, https://www.analysysmason.com/research/content/articles/sovereign-cloud-local-ren01/
36. AWS Outposts, https://aws.amazon.com/outposts/
37. Google Cloud Anthos, https://cloud.google.com/anthos/
38. 《云主权白皮书》, 德勤, https://www2.deloitte.com/content/dam/Deloitte/be/Documents/technology/be_Cloud%20Sovereignty%20White%20Paper.pdf

致谢

The authors would like to thank **Jean Gil Barroca, Robert MacDougall, Lucia Lucchini,** and **Leslie Wolf of Deloitte LLP,** and **Vipul Mehta and KirtiKhattri** of Deloitte SVCS India Pvt L for their contributions to this article.

Cover image by: **Manya Kuzemchenko**