提高数据安全及移动性推动全球发展的国际准则

环球金融市场协会（GFMA）及其成员机构欧洲金融市场协会（AFME）、亚洲证券业与金融市场协会（ASIFMA）以及美国证券业与金融市场协会（SIFMA）联手营造开放而充满活力的世界经济环境，让金融服务推动国际贸易及投资，促进全球经济增长，同时更好地保护个人隐私权。随着数字经济的发展，世界各国的政策制定者都审时度势地加强了数据及隐私保护政策，并继续推进跨境贸易，助力全球经济增长。

本文要点如下：

- 数字经济的背景，以及数据隐私和数据自由流动的重要性
- 支持数字经济与尊重隐私权相关的政策目标
- 我们请求监管部门为实现政策目标而予以考虑的原则

数字经济的背景以及数据自由流动的重要性

数字化服务的跨境贸易呈上升趋势：2016 年全球电子商务交易额接近 28 万亿美元[1]，且零售电商市场的交易额预计将在 2018 年实现比 2014 年增长一倍[2]。基于这些趋势，观察者总结称“几乎每种类型的跨境交易都含有数字化组成部分”[3]。新加坡金融管理局董事总经理拉维·梅农（Ravi Menon）指出，“数据的整合、储存、处理以及传输能力，尤其是数据跨境传输的能力，在当今的数字时代至关重要。”[4]这些能力对于贸易、投资及经济增长也至关重要：跨境数据流动使全球 GDP 在过去十年里增长了 10%[5]。欧盟如果能够解决数据政策碎片化这一问题，到 2020 年，欧洲的数字经济将带来额外 4%的 GDP 增长，价值超过

[1] 数据来源于美国国际贸易委员会，2017 年 9 月，“美国国际贸委会报道，近年全球数字贸易实现巨额增长，有的国家却开始放缓数字化脚步”一文。
https://www.usitc.gov/press_room/news_release/2017/er0928ll836.htm.

[2] 全球零售电子商务 2014-2021 年销售额：https://www.statista.com/statistics/379046/worldwide-retail-e-commerce-sales/

[3] 麦肯锡发布于 2016 年 3 月，《数字全球化：全球流通的新时代》https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows.

[4] https://www.bis.org/review/r181112a.pdf

[5] 出处同上。

1060 亿欧元[6]，并每年能给欧盟带来 80 亿欧元[7]的 GDP 增长。数字贸易对于每一个行业都至关重要，并且能够对本地的商品制造、农业的生产及贸易、创新研发起到支持作用。金融服务能对全世界各国生产商的投资贸易产生倍增效应。在新的数字经济背景下，隐私保护、数据安全以及效率对于企业、政府及消费者而言都至关重要。

尽管数字化能有效推动全球经济的增长，但也有一些司法管辖区采取措施限制跨境数据传输，并建立了新的数据本地化要求以遏制数字贸易的进一步增长。所谓“数据本地化”，指的是国家或者地区出台一些法律法规，要求企业只能在境内进行数据的存储、处理和管理。有的司法管辖区出台相关措施，要求只能使用某些本地生产的科技产品与服务。就业相关的法律法规以及外包服务的限制条款也会影响数据的流动。从 2000 年开始，关于数字本地化的政策数量已经翻了两番（详见附录 1）[8]。这些政策一般针对银行交易、公司记录及会计数据[9]。限制数据自由流动将对跨国企业及其所服务的最终用户产生严重的影响，对于整个经济的增长也是如此。

政策制定者制定数据本地化要求的初衷，是为了提高关键金融服务的弹性、保护隐私并提升数据的安全性。为了实现以上目标，政策制定者有时认为，要求使用本地服务器及计算设备，将促进创新、技术转移、及本地经济增长。而实际上，采用高标准、严要求的系统，才是提高业务弹性、保护隐私及保障安全的最好方式，我们所代表的金融机构都希望能持续致力于优化运营弹性。建立全球的技术网络架构能够有效地为客户提供产品及服务，保护传输中的数据和静态数据的安全，降低成本，并确保合规。全球性的金融机构能够为客户在差旅途中或从事商业活动过程提供服务，采取全球网络风险管理方案保护客户的财务安全，在监管部门及执法部门要求提供数据时及时予以配合，同时为客户及利益相关方降低成本。

数据本地化的要求及政策妨碍数据的自由流动，进而增加网络风险，也为贸易、竞争及创新制造了壁垒。数据本地化不仅不利于金融服务公司为客户及市场提供服务，对全面数据保护造成不利影响，也会降低服务效率。比如从安全性的角度来说，数据本地化给恶意入侵提供大量切入点，也不利于发现并应对安全威胁。从经济影响层面来说，由于为遵守数据本地化相关法律法规需要投入大量资源，往往导致企业难以进入市场或进行扩张，同时也限制了竞争、创新、就业机会及投资。而那些成功进入市场的企业会将额外的合规成本转嫁给消费者，进而加大消费者获得产品和服务的难度。数据本地化政策带来的后果最终将限制数字贸易的发展，也将限制全球经济的增长。信息技术与创新基金会通过对几大经济体开展分析后估算，若对跨境数据流设置壁垒，则将使 GDP 下降 0.1%至 1.7%[10]。欧洲国际经

---

[6]《欧洲数据市场研究》，SMART 2013/0063, IDC, 2016, 2013 年 2 月，https://www.key4biz.it/wp-content/uploads/2018/04/SMART20130063_Final-Report_030417_2.pdf

[7]欧盟委员会《国情咨文 2017：非个人数据的自由流动》 http://europa.eu/rapid/press-release_IP-17-3190_en.htm

[8]美国国际贸易委员会，2017 年 9 月，《美国国际贸委会报道，近年全球数字贸易实现巨额增长，有的国家却开始放缓数字化脚步》。

[9]欧洲国际政治经济研究中心(ECIPE)《释放欧盟内部数据流：欧盟成员国数据本地化措施的经济评估》，2016 年 12 月 http://ecipe.org//app/uploads/2016/12/Unleashing-Internal-Data-Flows-in-the-EU.pdf

[10]美国信息科技与创新基金会《跨境数据流;障碍在哪里?它们的代价是什么？》，2017 年 5 月 https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost.

济政治中心（ECIPE）表示，如果对欧盟各成员国实施全面的数据本地化政策，“整个欧盟每年将损失 520 亿欧元”，相当于欧盟 0.37%的 GDP[11]。

金融服务产业一贯支持监管部门保护消费者及投资者隐私和金融数据完整性的正当考虑。同时我们也认识到，为了保证监管机构顺利进行监管监督工作，金融机构必须向监管机构提供合适的数据。但是政策制定者应该重新考虑，基于这些目标出台各种措施来制造障碍而不实现这些目标是否得当。这些措施不仅毫无成效，而且会给数字经济发展和经济增长带来许多负面影响。因此，监管机构应在监管和监督职能合作基础之上，发展数据本地化政策的替代方法，以确保隐私安全和数据完整性。

计算设备的存放位置或云服务的使用并不会影响金融机构确保以监管或监督为目的的数据访问能力。正如欧盟委员会代表在 2017 年 5 月举行的主题为“数字时代金融服务”的圆桌会议上所说，采用云服务对支持开发更高效的金融产品和市场，以及向消费者提供创新安全的数据和服务越来越重要。这次会议还将云计算列为“打造欧盟竞争力的关键技术”[12]。然而，随着云服务的增长和相关政策的制定，为了实现这一目标，所有行业参与者都需要解决跨管辖区域监管碎片化的风险。在区域和全球层面，监管部门需要继续遵循数据自由流动、弹性、隐私和安全的原则，并尊重云技术的现状。可以通过采用相称的办法促进云外包，既要鼓励其发展，同时也要解决任何潜在的监管问题。政策制定者和金融机构需要共同合作，以确保监管机构有足够的信息，便于其对使用云服务的领域开展监管，实现金融稳定和市场监督目标，同时确保公司的防金融犯罪计划不会出现漏洞，也不会推行数字保护主义。监管部门应该认可现代数据存储和处理方法，并做好风险管理，而不是完全规避现代数据存储和处理，这样才可以发挥与外包、网络安全和云服务相关的现代数据存储的优势。

对金融服务的影响

金融服务行业也随着数字经济在不断发展，利用信息技术的进步来提高面向全球投资者和最终用户的金融服务的质量、效率和弹性。因此，我们鼓励政策制定者去支持金融服务行业及其服务的最终用户。

跨境数据传输对于金融服务行业至关重要，有助于：

（1）向客户提供核心产品和服务，包括在全球市场上执行买卖订单，因为法规通常具有域外效力，要求将更多数据纳入订单；

（2）全面管理跨境和跨关联公司的整体风险；

（3）遵守各司法管辖区的金融监管规定，包括“了解您的客户”（KYC）及反洗钱（AML）法规；

（4）监控和保护全球网络免受恶意网络攻击。此外，跨境数据流动是包括区块链应用在内的金融技术发展必需的前提条件。

---

[11] 欧洲国际政治经济研究中心(ECIPE)《释放欧盟内部数据流：欧盟成员国数据本地化措施的经济评估》，2016 年 12 月 http://ecipe.org//app/uploads/2016/12/Unleashing-Internal-Data-Flows-in-the-EU.pdf

[12] https://www.bbva.com/en/financial-services-era-cloud-computing/

全球若干司法管辖区对数据跨境流动的限制对金融服务部门产生了不利影响，例如：

（1）出台限制性法规，且未适当有针对性地规定例外情况；

（2）提出不必要的限制性隐私要求；

（3）要求建立低效的本地服务器和数据中心在岸存储数据；

（4）设置外包限制。

虽然政府有责任保护消费者隐私和数据完整性，但这些措施的实际效果，从全球范围来看，适得其反，因为它们导致企业在全球的运营碎片化，限制网络和数据的防护，降低效率，增加成本，从而抑制跨境贸易和投资。详情如下[13]。

2018 年 11 月 14 日，欧洲议会和欧盟理事会批准了一项立法改革提案，禁止在欧盟境内设置数据本地化限制措施。（EU）2018/1807 号新法规（“法规”）于 2018 年 11 月 28 日在欧盟官方公报上颁布，并将于 2019 年 5 月 28 日适用于所有欧盟成员国[13]。该法规为欧盟的电子非个人数据自由流动数据构建了框架，而目前这种流动在许多欧盟成员国中受到本地化限制或市场法律不确定性的限制。除了涉及公共安全的情况，该法规要求从国家层面取消任何数据本地化要求。该法规还有助于监管机构获取数据，采用云计算，并增强云服务提供商之间的数据可移植性。

该法规将会给在欧盟内部环境中直接或间接（即通过其供应商）运营的全球公司带来的一个关键的挑战。由于合规要求越来越复杂，例如数据保护法规、就业和外包法律，这些公司在欧盟成员国内进行存储和处理数据时可能会遇到阻碍。同样，企业在欧盟持有和处理数据，也需要厘清非欧盟数据与欧盟个人数据权利之间的关系。欧盟委员会现在的任务是在 2019 年 5 月 28 日之前就该法规和《一般数据保护条例》如何适用于此类混合数据集发布指导。

最近签署的《美国、墨西哥加拿大协议》（USMCA）提供了另一个数据条款的例子。该协议载列了一条有关数据自由流动的条款，更新了 1997 年达成的《服务贸易总协定》采取的方式。《美国、墨西哥加拿大协议》还规定，在金融监管机构可以访问所需数据来履行监管职能的情况下，不得要求数据本地存储。

促进数据隐私、安全和流动的国际准则

金融服务业一贯支持监管部门保护消费者及投资者隐私和金融数据完整性的正当考虑。我们鼓励全球监管机构考虑以下原则，并采用最佳实践来提升数据保护和数据流动性——因为我们认为这两者是相辅相成的，并同时继续促进数据隐私保护。

1.认可跨境传输数据并在不同管辖区内存储数据并提供充分保护的能力，对于促进全球金融体系的安全、创新和繁荣以及推动全球经济增长至关重要[14]。

[13] https://www.bbva.com/en/financial-services-era-cloud-computing/

[14] 全球金融市场协会、国际掉期交易协会和欧洲银行联盟，国际网络安全，数据和技术原则， 2016 年 5 月，http://www.gfma.org/correspondence/item.aspx?id=807.

为数据安全高效的流动扫清障碍，给数字经济的发展创造有利环境，完全符合监管部门的利益。当数据保护的法律法规与国际标准和最佳实践不一致时，就会形成非关税贸易壁垒并限制经济活动。政策制定者在认识到隐私和数据保护政策对国际贸易和投资的影响后，可以根据目标来制定政策，保护个人的隐私权，进一步打击金融犯罪，并促进经济增长。政策制定者还应支持制定通用框架，使跨国金融机构在国际化的运作环境中有章可循。政府之间可以通过签署跨境执法、监管和数据分享的合作协议来支持数据访问，同时解决金融市场完整信和主权风险问题。

增强不同司法管辖区内隐私相关法律法规的互操作性，有助于推动安全高效的跨境数据流动，改善国际贸易和促进投资，并提高数字贸易渠道的利用率。亚太经贸合作组织（APEC）通过的《跨境隐私规则》（CBPR）是很好的范例。另外，随着英国脱欧临近，清晰地保证个人数据能够继续在欧盟和英国之间进行传输[15]至关重要。

2. 与业界合作，协同监管要求，采纳有关数据安全和流动的最佳国际实践

我们鼓励以下做法：

（1）政府可以咨询金融服务机构，更好地了解数据存储和跨境传输过程中的数据保护标准和最佳实践。在制定保护隐私和数据安全的法规之前，先征求私营部门的意见，可以在贸易、投资和经济增长方面规避意想不到的后果。

（2）政策制定者可以参考现有的网络安全风险管理体系：ISO 27103、美国国家标准与技术研究院(NIST)发布的《网络安全框架》（CSF），以及《金融服务业网络安全框架》都是在国际、国家和特定行业层面上协同一致的风险管理框架。

（3）进一步采纳《网络安全、数据和技术的国际准则》[16]。当今世界，数字化加速发展、科技日新月异，政府之间应签署合作协议，解决跨境弹性、隐私和安全的问题；市场应发展和壮大数字化相关的准则和能力，而非制定数据本地化限制要求。总体而言，监管机构应该探索数据本地化政策的替代方法。

3. 认可在充分的控制和监管下，跨境数据移动可以支持数据保护和系统的弹性。

出发点良好但数据本地化过于严格的规则实际上可能会削弱全球金融体系和单个机构的弹性。如果没有有效的安全措施，隐私就得不到保护。有效的安全措施取决于数据分享和存储的方式，而无关乎存储的位置。跨境处理并适当分享顾客信息对于防止滥用至关重要，尤其是在确保网络安全和制裁/反洗钱执法方面。对跨境数据访问设置不当限制会削弱公司多方面的能力，包括：有效设置和执行技术控制措施；监控公司网络和基础架构面临的威胁；与合作伙伴、执法机构共享信息，以降低更加广泛的系统性风险。此外，在分散的或不同的设施中存储数据的要求，会增加数据访问入口，给不法分子渗入网络带来更多可乘之机。外包或整合区域数据中心或信息技术中心，有助于公司将资源专门用于保护数据和技术安全，并确保其具备强大的弹性，如数据备份能力。从这个意义上说，数据本地

[15] https://www.afme.eu/en/reports/publications/effective-flow-of-personal-data-post-brexit/

[16]全球金融市场协会、欧洲银行联盟和国际掉期交易协会，“国际网络安全，数据和技术原则”，2016 年 5 月，http://www.gfma.org/correspondence/item.aspx?id=807。

化会对公司业务的连续性和灾难复原产生负面影响。

4. 实现精准跨境信息共享。

金融机构必须向监管机构提供适当、及时的数据，使其在不同的司法管辖区履行监管义务。对跨境数据流动设置限制可能会给公司带来合规风险：由于跨国公司受到多重监管报告制度的约束，制定隐私法和封闭性法规可能会给他们带来法律冲突问题。因此，数据本地化政策可能会阻碍金融监管机构获得有效开展工作所需的数据，使企业难以符合监管要求。例如，依据全球适用的相关“反洗钱”法规，金融机构需要跨境与附属机构共享信息，才能获得提交可疑活动报告所需的信息。我们呼吁政策制定者注意数据本地化政策对企业继续执行重要投资者保护协议（包括“反洗钱”、“了解您的客户”或金融犯罪调查）能力的影响。我们鼓励数据保护部门与其他金融犯罪和网络安全监管部门协调，确定使用数据的范围，促进跨境数据传输，以履行监管义务和加强投资者保护。

5. 促进足够安全的外包安排，提高金融服务提供商的效率和竞争力。

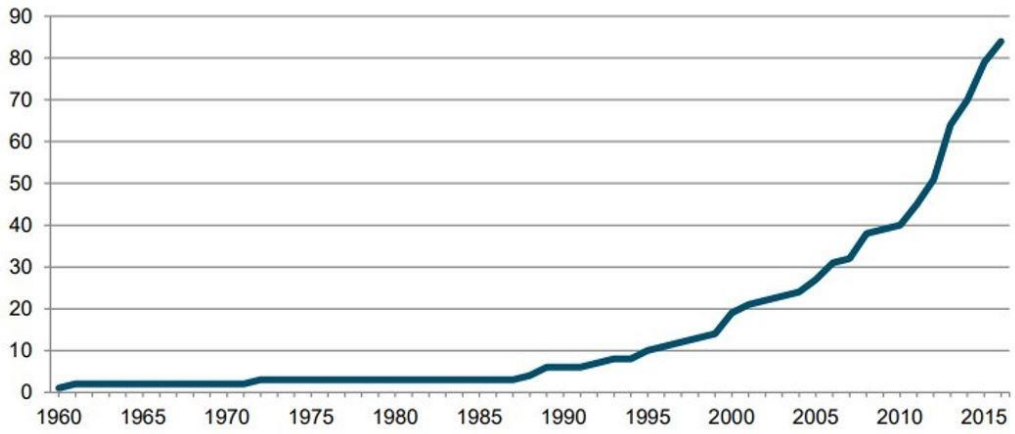
外包对于提高金融服务业的效率至关重要，有助于企业提供优质的客户服务，保持国际竞争力，并降低运营成本，以促进其他领域的投资，深化本地资本市场的发展。跨国金融机构经常将业务密集型的职能外包给集团内的其他附属机构，以一种竞争、高效和有效的方式利用内部能力。这样做可以使金融机构最大限度地利用现有的基础架构，从而提高效率，以更有效的方式增加投资。

然而，限制金融服务业业务外包的政策往往会导致数据的实际本地化，阻碍企业进入某市场或扩张业务，不利于经济增长，使当地消费者处于不利地位。在不违反总体监管要求的情况下，外包管理政策的制定应以原则为基础，技术和服务实体中立，不应受到地理位置的影响，以便于金融机构根据自己的业务模式和风险进行外包安排，而有关监管部门不应该在现有外包法规之外提出新的要求或施加限制[17]。

[17]欧洲金融市场联合会对欧洲银行业管理局关于云外包建议草案的咨询文件的回应，2017 年 8 月，https://www.afme.eu/globalassets/downloads/consultation- resp，onses/AFME-TAO-Response-to-EBA-Consultation-Paper-on-Draft-Recommendations-on-Cloud-Outsourcing.pdf

附录 1：全球新增数据本地化措施

图 ES.1： 全球数据本地化措施的数量（1960–2015）



来源：美国国际贸易委员会，“全球数字贸易 1：市场机遇和主要外贸限制”，2017 年 9 月，https://www.usitc.gov/publications/332/pub4716.pdf，第 17 页。