亚马逊云科技

代码出海 合规护航：

中国软件企业在欧洲市场的数据主权与安全合规指南

Contents.

代码出海 合规护航：中国软件企业在欧洲市场的数据主权与安全合规指南

Contents.

代码出海 合规护航：中国软件企业在欧洲市场的数据主权与安全合规指南

ABSTRACT

摘要

当中国的软件开始服务于欧洲大陆，一行行git push指令的背后，可能隐藏着高达数亿欧元的合规风险。欧洲，这个全球软件市场的高地，正通过《通用数据保护条例》（GDPR）、《数据法案》、《网络弹性法案》等一系列严苛法规，为其数字疆域筑起一道无形的“合规之墙”。对于以软件为核心产品的中国软件企业而言，这不仅是法律挑战，更是对产品架构、研发流程、商业模式乃至生存根基的全面考验。

本白皮书将精准聚焦中国软件企业的出海痛点：从SaaS服务的多租户数据隔离，到DevOps流程中的跨境数据风险，再到软件供应链的安全责任。我们将深度剖析亚马逊云科技如何通过其“合规即服务”的理念、强大的数据主权工具箱以及为欧洲量身打造的“主权云”，帮助中国软件企业将合规无缝融入产品生命周期，实现“合规设计（Compliance by Design）”，最终将严苛的合规壁垒，转化为赢得欧洲客户信任、实现可持续增长的核心竞争力。

NO.1

无形之墙——欧洲数字护城河
对中国软件企业的四大“精准打击”

对于追求快速迭代和高效交付的中国软件企业而言，欧洲市场提供了重要的增长机会，但其成熟且严格的法规体系也带来了不可忽视的合规挑战。这些法规涉及产品架构、供应链安全、研发模式以及商业准入四个关键维度，要求企业在进入欧洲市场前进行系统性评估与适应性调整。

1.1 SaaS模式的隐忧：多租户架构下的数据隔离与主权难题

软件即服务（SaaS）模式凭借其灵活性、可扩展性和成本效益，已成为中国软件企业出海的首选模式。然而，SaaS天然的多租户架构——即多个客户的数据在共享的基础设施上运行——在GDPR的放大镜下，却面临严峻的合规审视。欧洲的企业客户，尤其是中大型客户，对于数据主权和隔离性的要求极为苛刻。

> *他们会反复诘问一个核心问题：“你如何保证我的数据，在你的SaaS平台上，与别家公司的数据是绝对隔离、互不可见的？你作为平台方，是否有能力访问我的数据？”*

根据GDPR的规定，SaaS提供商作为“数据处理者”，必须向其客户（“数据控制者”）提供足够的技术和组织措施保证。

这意味着，软件企业不能仅仅满足于应用层面的逻辑隔离，而必须在基础设施层面提供可验证的、强有力的隔离证明。传统的数据库共享、资源池化等为了提升资源利用率的设计，都可能成为合规审查中的致命弱点。如果不能清晰地向客户阐明其数据在平台上的完整生命周期、隔离机制和访问控制策略，软件企业将很难获得欧洲企业客户的信任。

1.2 软件供应链的“连坐法”：《网络弹性法案》下的无限责任

现代软件开发早已不是单打独斗，而是建立在庞大的开源社区和第三方库的基础之上。

然而，即将全面生效的《网络弹性法案》（Cyber Resilience Act,CRA）将彻底改变这一游戏规则，为软件供应链引入了严格的“连坐”责任制。

该法案要求，投放欧盟市场的软件产品，其制造商必须对其整个生命周期内的网络安全负责，这其中就包括其产品所包含的所有第三方组件，例如开源库和依赖包。

这意味着，如果软件企业的产品因为使用的一个开源组件存在漏洞而导致其欧洲客户数据泄露，该软件企业将可能承担直接的法律责任。这对于依赖敏捷开发和快速集成开源技术的中国软件企业来说，无疑是一个巨大的冲击。企业不仅需要建立完善的软件物料清单（SBOM），还需要具备持续监控、评估和修复供应链漏洞的能力。

CRA的出现，意味着软件企业的责任边界被无限扩大，从“写好自己的代码”延伸到了“审查整个软件世界”。

1.3 当git push成为“跨境传输”：研发运维中的合规“雷区”

一个在中国软件企业中普遍存在且极易被忽视的巨大风险，来源于其全球一体化的研发和运维模式。许多企业认为，只要将SaaS服务的生产环境部署在欧洲，就能满足数据本地化的要求。然而，根据GDPR对“数据跨境传输”的宽泛定义，以及欧洲数据保护委员会（EDPB）的解释，任何使得欧盟境外实体能够访问到个人数据的行为，都可能被视为跨境传输。

这一解释的影响是深远的。

案例一

一位身在上海的工程师，为了修复一个紧急Bug，远程登录到位于法兰克福的服务器并查看了包含用户个人信息的日志文件，这构成了跨境传输；一个位于杭州的运维团队，接入了欧洲数据中心的监控仪表盘，仪表盘上展示了活跃用户的相关信息，这也构成了跨境传输；

案例二

一个位于深圳的研发团队，将包含欧洲用户反馈（可能含个人信息）的数据库备份下载到本地进行分析，同样是跨境传输。在未获得充分授权和保障措施的情况下，这些日常的研发运维活动都可能违反GDPR，直接挑战了中国软件企业高效的、全球协作的DevOps文化。

1.4 增长的“天花板”：合规是赢得欧洲大型企业客户的“入场券”

对于初创或中小型软件企业而言，前期的市场拓展可能更侧重于产品功能和价格优势。但在欧洲，当业务发展到一定阶段，试图签约中大型企业、政府或公共部门客户时，会发现一个坚硬的“天花板”——数据安全与合规。根据走出去智库（CGGT）在2025年8月的一项调研，在寻求出海欧洲的企业中，有近半数（45.8%）已经设立了欧盟分支机构，他们对本地化合规方案的需求极为迫切。同一调研还显示，64.5%的受访企业担忧中欧法律冲突，56.1%的企业正在寻求应急管理预案，这充分说明了合规问题已成为出海企业的核心战略议题。

对于成熟的欧洲买家而言，选择一个软件服务，尤其是在核心业务系统中，首要考虑的已不再是功能多寡，而是供应商是否能提供一个可信的、经得起审计的合规承诺。一份详尽的数据处理协议（DPA）、一份来自权威第三方的安全认证（如ISO 27001,SOC 2），远比一份华丽的功能清单更有说服力。合规，已经从一个“最好要有”的加分项，演变成了进入欧洲主流企业市场的“必要条件”和“入场券”。

NO.2

合规即服务——利用亚马逊云科技构建“生而合规”的SaaS产品

面对欧洲市场的合规“高墙”，中国软件企业的出路并非被动地填补漏洞，而是在产品设计之初就将合规能力根植于架构与流程之中，实现“合规设计（Compliance by Design）”。这不仅是技术选择，更是一种战略思维的转变——将合规从发布前的“检查项”变为产品固有的“免疫力”。亚马逊云科技提供了一套完整的“合规即服务”工具箱，使软件企业能够将复杂的合规要求，转化为具体、可落地的技术实现。

2.1 从商业案例出发：构建可信的RoI分析

构建数字边界（Geo-Fencing）

满足数据驻留要求是合规的第一步。亚马逊云科技在欧洲拥有多个Region（如法兰克福、爱尔兰、巴黎等），每个Region都由多个物理隔离、独立供电的可用区（AZ）组成。

软件企业可以通过选择在欧洲境内的Region部署其SaaS服务，轻松实现数据的“地理围栏”。这意味着，从客户数据产生的那一刻起，其存储和处理都严格限制在欧盟的法律管辖范围之内，这是向监管机构和客户展示合规决心的最直观证明。

实现租户数据的强隔离与加密

在多租户SaaS架构中，证明租户间数据的强隔离是赢得客户信任的核心。亚马逊云科技提供了丰富的服务来实现这一目标。

利用Amazon Virtual Private Cloud(VPC)，软件企业可以为每个租户或每个租户群组创建独立的虚拟网络环境，通过精细的子网、安全组和网络访问控制列表（NACL）规则，从网络层面彻底杜绝租户间的未授权访问。

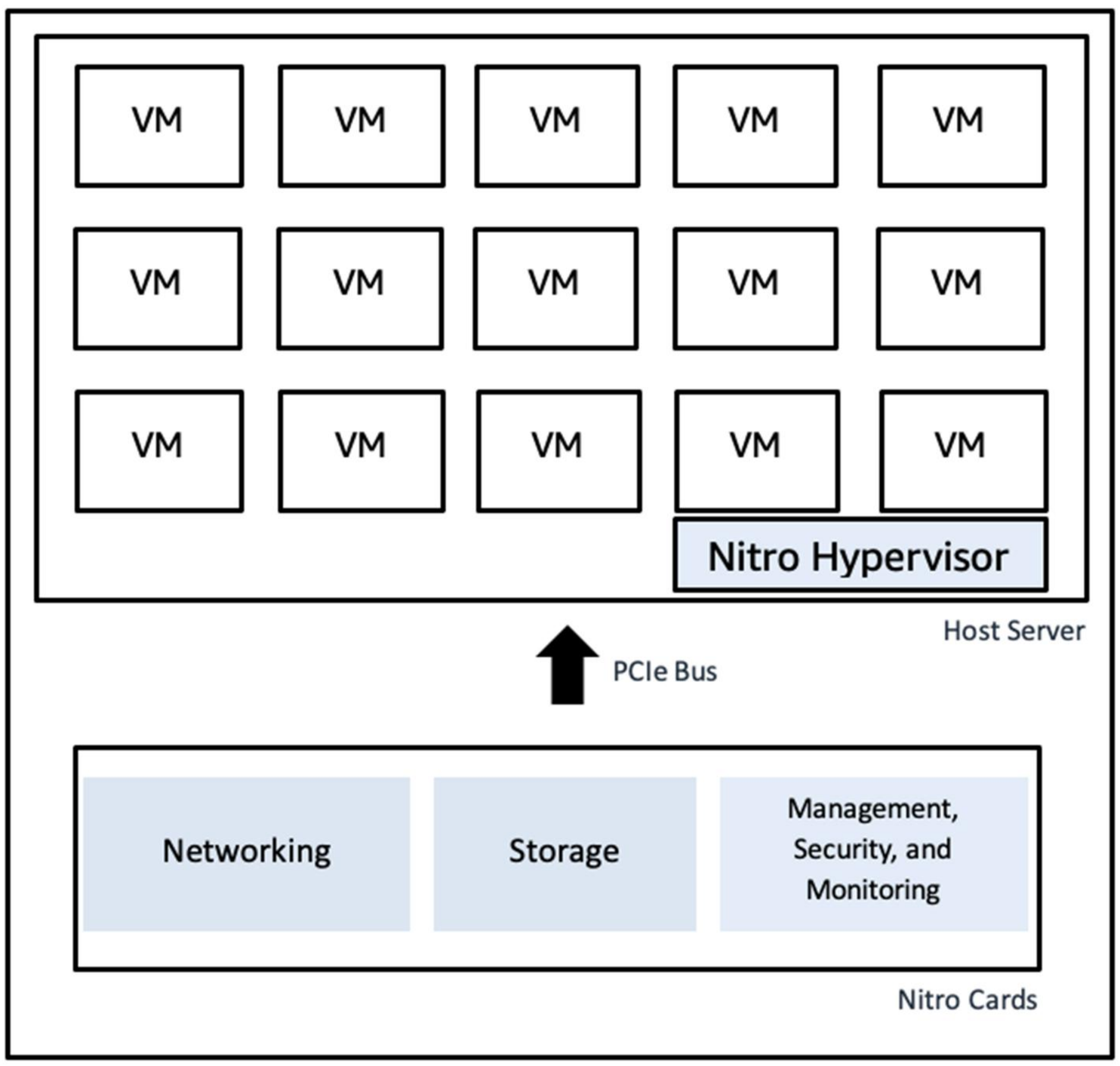
通过Amazon Identity and Access Management(IAM)，可以为不同的租户或应用模块创建拥有最小权限原则的IAM角色，确保任何操作都经过严格的身份验证和授权。

在数据加密方面，软件企业可以利用Amazon Key Management Service(KMS) 来创建和管理加密密钥，更进一步，可以向客户提供“客户管理密钥（Customer Managed Key）”选项，允许客户使用由自己创建和管理的密钥来加密自己的数据——在这种模式下，即使是软件企业本身，也无法解密客户的数据，从而实现了最高级别的控制权交还。

以Nitro系统证明“云厂商不可见”

在向欧洲企业客户推销SaaS服务时，一个终极问题常常被提出：“我如何相信你和你的云服务提供商不会偷看我的数据？”对此，亚马逊云科技的Nitro系统提供了决定性的技术答案。Nitro系统是亚马逊云科技EC2实例的底层硬件基础，它通过专用的硬件芯片将网络、存储、安全等虚拟化功能从主CPU上剥离出去。这一设计的革命性之处在于，它在物理层面消除了任何管理员（包括亚马逊云科技的员工）通过宿主机登录和访问客户EC2实例的可能性。

软件企业可以自信地向客户声明：“我们选择的云平台，其设计理念就是’云厂商不可见’。这是由硬件决定的，并经过了独立的第三方审计。”这种基于技术事实的承诺，是在欧洲市场建立信任、赢得大客户的“杀手锏”。



附图:Nitro系统虚拟化架构

2.2 流程的“洁净室”：打造合规的全球DevOps流水线

解决了架构问题后，下一个挑战来自于人——全球化的研发和运维团队。软件企业需要建立一个“洁净室”般的流程，确保中国的工程师在支持欧洲业务时，既能高效工作，又不会触碰合规的“高压线”。

“假名化”的日志与监控：在数据中“去毒”

为了进行故障排查和性能优化，运维团队不可避免地需要访问日志和监控数据。为了降低这些数据中包含个人信息的风险，软件企业应在数据采集阶段就进行“敏感信息脱敏”处理。例如，利用Amazon CloudWatch Logs的过滤和转换功能，或通过Amazon Lambda函数，在日志写入中心存储之前，自动对IP地址、用户名、联系方式等敏感字段进行假名化（替换为无意义的标识符）或完全脱敏。

这样，中国团队在分析数据时，看到的是不含个人身份信息的、可安全使用的数据集，从而在源头上规避了跨境传输的合规风险。

最小权限的堡垒机：建立受控的运维通道

对于必须进行的远程运维操作，绝对禁止直接将生产环境的SSH端口或数据库端口暴露给公网。软件企业应使用 Amazon Systems Manager Session Manager作为唯一的、受控的运维“堡垒机”。

Session Manager允许运维人员通过一个经过IAM严格授权和MFA（多因素认证）保护的界面来访问欧洲的服务器实例，而无需开启任何入站端口。

所有的会话操作都可以被完整地记录和审计，并存储在Amazon S3或CloudWatch Logs中。这种方式既为全球团队提供了必要的运维通道，又确保了每一次访问都是最小权限、可追溯、可审计的，从而向监管机构证明了其运维流程的合规性。

2.3 认证的“加速器”：将亚马逊云科技的合规认证转化为商业优势

获得一项安全合规认证（如ISO 27001,SOC 2）对任何一个软件企业来说都是一项耗时耗力的巨大工程。然而，通过选择亚马逊云科技，软件企业可以站在巨人的肩膀上。

亚马逊云科技在全球范围内获得了数百项安全合规认证和证明，其中包括许多欧洲特有的、极为严格的标准，如德国的C5认证和泛欧的CISPE数据保护行为准则。

根据责任共担模型，亚马逊云科技负责“云自身”的安全合规，而客户（软件企业）负责“在云中”的安全合规。这意味着，当软件企业构建其SaaS服务时，其底层基础设施的合规性已经由亚马逊云科技保证。在进行自身的合规审计时，软件企业可以直接“继承”亚马逊云科技的认证，只需向审计师提供亚马逊云科技的相关合规报告（可通过Amazon Artifact服务获取），然后将审计重点放在自己的应用层安全和管理流程上。

这极大地降低了软件企业的合规成本和认证周期，并使其能够在市场营销中理直气壮地宣称：

> “我们的服务构建在已获得德国C5认证、符合CISPE行为准则的云平台之上。”

NO.3
终极选项——当你的客户是政府或银行时

对于大多数商业应用场景，通过在标准的亚马逊云科技欧洲Region上实施前述的最佳实践，已经足以构建强大的合规壁垒。然而，当中国软件企业的目标客户是欧洲的公共部门、银行、能源、医疗等受到最严格监管的行业时，仅仅满足GDPR的标准条款可能还不够。这些行业的客户及其监管机构，往往对数据主权有着更为极致的要求，不仅关心数据本身，还关心处理数据的运营体系，乃至运营人员的身份。为了服务这类金字塔尖的客户，软件企业需要一个“终极选项”——亚马逊云科技欧洲主权云（Amazon European Sovereign Cloud）。

3.1 主权云的适用场景：软件企业的“特供”模式

亚马逊云科技欧洲主权云于2026年1月正式在德国启动，并计划在2040年前向相关基础设施投资78亿欧元。它并非为了取代现有的欧洲Region，而是作为一种“特供”模式，专门为有最高主权要求的客户而设计。对于软件企业而言，以下场景是考虑使用主权云的关键决策点：

适用场景	典型客户类型	关键监管要求
目标客户为公共部门	政府机构、地方市政、科研院所	强制要求供应商使用满足特定主权标准的云基础设施
服务于关键基础设施行业	银行、保险、能源、交通、医疗	DORA法案等行业特定法规要求IT供应链具备最高级别韧性
处理极其敏感的数据	国防、基因研究、国家安全相关机构	对数据驻留和访问控制有超越GDPR的额外要求

在这些场景下，欧洲主权云不再是一个“可选项”，而是软件企业能够参与竞标、获得订单的“准入门槛”。

3.2 不仅仅是数据驻留：主权云的“三权分立”

与标准Region相比，欧洲主权云的核心价值不在于提供了更强的计算或存储能力，而在于它在数据、运营、身份三个维度上实现了彻底的独立，堪称云端的“三权分立”。

数据的彻底驻留是第一重保障

欧洲主权云在物理上和逻辑上都与亚马逊云科技的其他Region完全隔离。客户在主权云中创建的所有内容，包括数据和元数据（如资源标签、配置信息等），都将严格保留在欧盟境内，绝不会流出。

运营的完全本地化是第二重保障

主权云的所有日常运营、技术支持和客户服务，都仅由位于欧盟境内、且居住在欧盟的欧盟公民来执行。这从人员层面杜绝了任何来自欧盟境外的潜在访问和干预风险，满足了最严格的运营主权要求。

身份的独立堆栈是第三重保障

也是主权云最独特、最关键的特征。它拥有一个完全独立的IAM（身份与访问管理）堆栈。在欧洲主权云中，客户创建的所有用户、角色、权限策略等身份信息，其本身的数据和元数据都100%留存在欧盟，实现了身份层面的主权，是对数据主权概念最彻底的诠释。

附图:欧洲主权云的三权分立

3.3 商业决策：如何评估主权云的ROI

对于软件企业决策者而言，选择欧洲主权云无疑是一项战略投资。评估其投资回报率（ROI）应从以下几个角度考量：其一，市场准入价值——主权云能够为你打开多大的、原本无法进入的市场？一个价值数百万欧元的政府软件采购合同，可能会因为你使用了主权云而变得触手可及。其二，信任溢价——在高端企业市场，能够提供基于主权云的SaaS服务，本身就是一种强大的信任背书，可以转化为更高的合同价值和更低的销售摩擦。其三，风险规避成本——与可能面临的巨额罚款（GDPR罚款可高达全球年营业额的4%或2000万欧元，以较高者为准）相比，投资主权云的成本实际上是一种高度确定性的风险规避支出。

NO.4

从代码到合同——软件企业在欧洲的合规增长飞轮

在欧洲市场，合规并非终点，而是增长的起点。当中国软件企业成功地将合规能力融入产品与流程的血液中，它就不再是成本中心，而是驱动业务增长的强大飞轮。一个“生而合规”的产品，能够更快地赢得客户信任，缩短销售周期，签订更高价值的合同，并建立起竞争对手难以逾越的护城河。

4.1 客户之声：一个中国SaaS的欧洲合规之旅

（本案例基于对多家出海软件企业实践的整合与匿名化处理）

“数翼科技”是一家提供营销自动化SaaS服务的中国公司。2023年，他们满怀信心地进军欧洲市场，凭借出色的产品功能很快获得了一批早期采用者。然而，当他们试图签约一家德国中型制造企业时，却碰了一鼻子灰。对方的法务和IT部门提出了一份长达50页的安全合规问卷，问题从数据加密、租户隔离，一直追问到他们中国研发团队的访问权限和运维流程。

> “数翼科技”的CTO王先生回忆道：“我们当时完全蒙了。我们以为把服务器放在法兰克福就万事大吉，但他们的问题细致到我们运维工程师的每一次数据库查询是否会被记录。我们意识到，我们卖的不仅是软件功能，更是一种数据安全的信任承诺，而我们当时完全没有准备好。”

痛定思痛，“数翼科技”决定暂停市场扩张，转而与亚马逊云科技的出海专家团队合作，开启了一场彻底的“合规重构”。他们利用VPC和IAM为欧洲客户创建了独立的“数字安全区”，并采纳了KMS的客户管理密钥方案，将数据加密的最高控制权交还给客户；废除了直接的SSH访问，全面转向Systems Manager Session Manager进行远程运维，所有操作均被记录；同时改造了日志系统，在数据进入中心分析平台前就完成了脱敏。完成改造后，他们借助亚马逊云科技提供的合规报告和责任共担模型，在短短四个月内就通过了ISO 27001审计。

一年后，“数翼科技”不仅成功签下了那家德国制造企业，还赢得了一家法国银行的试点项目。王先生总结道：“这次重构投入巨大，但它为我们扫清了通往大客户市场的所有障碍。现在，合规是我们最好的销售工具。当我们能把一份SOC 2报告和一份清晰的架构图放在客户面前时，我们知道这单生意已经赢了一半。”

4.2 ISV合规路线图：“三步走”构建你的合规护城河

数翼科技”的成功并非个例，其路径揭示了软件企业在欧洲构建合规护城河的通用法则，可总结为“三步走”策略。

第一步：架构先行（Architecture First）

在编写第一行代码之前，就应将合规要求作为产品设计的最高优先级。与亚马逊云科技的解决方案架构师合作，基于“安全、隔离、可审计”的原则，设计你的云上基础设施。思考你的多租户隔离模型，规划你的数据加密和密钥管理策略，定义你的网络边界。一个好的架构设计，可以在早期避免后期90%的合规风险和改造成本。

第二步：信任前置（Trust by Default）

不要把你的合规能力藏在技术文档里。学习将亚马逊云科技提供的安全与合规能力，转化为面向客户的、清晰易懂的“信任报告”、产品功能和市场语言。在你的网站上建立“信任中心”，在你的销售材料中突出你的合规认证，在你的合同中明确你的数据处理承诺。主动、透明地沟通你的安全态势，是赢得信任的唯一捷径。

第三步：持续验证（Continuous Verification）

合规不是一次性的冲刺，而是一场持久的马拉松。利用Amazon Security Hub、Amazon GuardDuty、Amazon Inspector等自动化工具，将安全合规检查和安全监控融入你的CI/CD流水线，实现从“一次性过审”到“持续性合规”的转变。自动化的持续验证不仅能有效降低人为错误，还能在监管机构审查时，提供一份无可辩驳的、持续合规的证据记录。

4.3 您的下一步行动

欧洲市场的合规之墙既是挑战，也是机遇。

它筛选掉了投机者，为那些真正致力于构建安全、可信赖产品的软件企业留下了广阔的增长空间。将合规从负担转变为核心竞争力，是中国软件企业在欧洲走向成功的关键一步。

亚马逊云科技拥有专业的出海专家团队和丰富的全球实践经验，致力于帮助中国软件企业顺利跨越合规门槛。我们诚挚地邀请您立即行动，与我们的专家团队取得联系，获取一份针对您业务场景的专属合规评估与架构咨询服务，为您的代码出海之旅保驾护航。

附 录

附录A：中国软件企业出海欧洲合规自查清单

类别	检查项	说明与建议
数据治理	是否已任命数据保护官（DPO）？	对于核心业务涉及大规模、系统性监控或处理敏感数据的企业，此为强制要求。
	是否已绘制并维护数据处理活动记录（RoPA）？	清晰了解处理了哪些个人数据、为何处理、存储在哪里、保留多久。
	是否为SaaS产品的客户准备了标准数据处理协议（DPA）？	这是作为“数据处理者”的法律义务。
架构与安全	生产环境是否部署在欧盟境内的Region?	满足数据驻留的基本要求。
	多租户架构是否实现了网络、计算和存储的强隔离?	建议为每个租户使用独立的VPC或账户。
	是否对所有静态数据和传输中数据进行加密?	使用KMS、ACM等服务。
	是否为客户提供了由其自己管理加密密钥的选项?	这是赢得高度关注数据主权客户的关键。
	是否已禁用所有不必要的端口，特别是SSH/RDP的公网访问?	所有运维应通过堡垒机（如Session Manager）。
研发与运维	中国研发运维团队的访问权限是否遵循最小权限原则?	确保中国团队只能访问其工作必须的数据和资源。
	是否对所有远程运维操作进行记录和审计?	Session Manager可以自动记录所有会话。
	访问生产日志和监控数据前，是否进行了脱敏或假名化处理?	从源头降低数据跨境传输风险。
商业与合同	网站上是否有清晰的隐私政策，并明确告知用户其数据权利?	透明度是GDPR的核心要求。
	是否获得了任何第三方安全合规认证（如ISO 27001, SOC 2）？	这是向客户证明合规承诺的有力工具。

附 录

附录B：亚马逊云科技助力软件企业合规的核心服务矩阵

合规领域	核心服务	核心价值
身份与访问控制	Amazon Identity and Access Management (IAM)	精细化权限管理，实现最小权限原则。
	Amazon IAM Identity Center	集中管理用户对多账户的访问。
检测与监控	Amazon GuardDuty	智能威胁检测，持续监控恶意活动。
	Amazon Inspector	自动化的漏洞管理和安全评估。
	Amazon Security Hub	集中查看安全告警，自动化合规检查。
	Amazon CloudWatch	日志记录、监控和告警。
	AmazonCloudTrail	记录所有API调用，实现操作可追溯。
基础设施安全	Amazon Virtual Private Cloud (VPC)	构建逻辑隔离的虚拟网络。
	Amazon Network Firewall	部署网络层威胁防护。
	Amazon Shield	DDoS攻击防护。
数据保护	Amazon Key Management Service (KMS)	创建和管理加密密钥，支持客户自管密钥。
	Amazon Certificate Manager (ACM)	轻松预置、管理和部署SSL/TLS证书。
	Amazon Macie	发现和保护S3中的敏感数据。
合规性与审计	Amazon Artifact	按需访问亚马逊云科技的合规报告。
	Amazon Audit Manager	持续审计使用情况，简化风险评估。
安全运维	Amazon Systems Manager Session Manager	提供无需开放端口的受控运维通道，全程可审计。

参考文献

References

[1] 欧洲议会. (2024). Cyber Resilience Act. European Commission. https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

[2] European Data Protection Board. (2021). Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR. https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052021-interplay-between-application-article-3_en

[3] 走出去智库. (2025, August 20). 中企欧盟数据合规“突围战”：监管挑战与实战策略. 安全内参. https://www.secrss.com/articles/82219

[4] Amazon Web Services. (n.d.). Amazon Nitro System. https://aws.amazon.com/ec2/nitro/

[5] Amazon Web Services. (n.d.). Amazon Compliance Programs. https://aws.amazon.com/compliance/programs/

[6]商务部. (2026, January 21). 亚马逊云计算部门Amazon在德国启动“欧洲主权云”业务. https://www.mofcom.gov.cn/tjsj/gbdqmytj/ozgjdqmytj/art/2026/art_7d062058f36e4a899288a0dd1e7ae81b.html

[7] Amazon Web Services. (n.d.). Amazon European Sovereign Cloud. https://aws.amazon.com/compliance/europe-digital-sovereignty/