亚马逊云科技 | Deloitte.

逐浪数字经济合规新世界

中国企业出海发展建议白皮书 2023 版

2023年9月

本白皮书由德勤企业咨询（上海）有限企业（“德勤企业咨询”）和 Amazon Web Services, Inc. 或其关联方（“亚马逊云科技”）分别撰写，双方就各自撰写的内容分别、独立享有相关知识产权。其中德勤企业咨询负责第一章、第二章、第三章 3.1，单独享有该部分的知识产权；亚马逊云科技负责第三章 3.2 部分（即“技术平台”部分）与 3.3.3 中“云上构建端到端的安全”部分，单独享有该部分的知识产权；双方共同享有第三章 3.3 部分的知识产权。

关于德勤企业咨询部分的声明：本白皮书中所含内容乃一般性信息，任何德勤有限企业、其全球成员所网络或它们的关联机构并不因此构成提供任何专业建议或服务。在作出任何可能影响您的财务或业务的决策或采取任何相关行动前，您应咨询合格的专业顾问。 我们并未对本白皮书所含信息的准确性或完整性作出任何（明示或暗示）陈述、保证或承诺。任何德勤有限企业、其成员所、关联机构、员工或代理方均不对任何方因使用本通讯而直接或间接导致的任何损失或损害承担责任。德勤有限企业及其每一家成员所和它们的关联机构均为具有独立法律地位的法律实体，相互之间不因第三方而承担任何责任或约束对方。德勤有限企业及其每一家成员所和它们的关联机构仅对自身行为及遗漏承担责任，而对相互的行为及遗漏不承担任何法律责任。德勤有限企业并不向客户提供服务。请参阅 www.deloitte.com/cn/about 了解更多信息。

关于亚马逊云科技部分的声明：本部分内容陈述了亚马逊云科技在封面页所示日期的有关服务产品及实践，该等信息可能变化且我们不会另行通知。客户对于本部分的信息以及亚马逊云科技的产品或服务应自己做出独立的判断，该等内容都是“依现状”提供，不包含任何明示或者暗示的保证。本部分内容并没有创设来自亚马逊云科技或其关联方、提供方或许可方的任何保证、陈述、合同性承诺、条件或者担保。亚马逊云科技对其客户的义务和责任均由适用的客户协议管辖。本部分内容不是亚马逊云科技和其客户之间任何协议的组成部分，也不构成对任何协议的修改。

前言

数字化经济在云计算、人工智能、机器学习、区块链、物联网等新兴技术的推动下，正在全面改变人们的生产生活方式，深刻影响人类社会历史发展进程。而数据是这一切的关键生产要素，从数据的来源、使用方式乃至数据衍生驱动的各类算法模型、执行决策都驱动了商业活动中数字经济的快速发展。

“合规是红线，安全是底限”，各国都在不断通过各种立法来规范数字化经济的发展，确保对于数据的主权、维护核心数据资产的安全、保护个人隐私、促进数据必要的合法流动和共享、以及减少广义供应链风险。同时由于大型服务平台以及 AI 应用对于传统商业模式的强劲冲击，这类平台或产品合规已成为全球关注的下一重点。

而对于企业来说，随着全球对于数字经济监管范围的进一步拓展以及公众对于隐私保护的关注度越来越高，数据应用与保护不再是一件仅与自身相关的“家务事”，出海挑战的良好应对更需要企业广泛关注在监管要求的缕清与响应、用户诉求的明确与应对，以及数据、数据处理过程、供应链上下游的全生命周期安全。这就使得企业急需建立一套机制，从内部管理及技术手段两个方面开展行动，以便在应对出海多国的合规目标的同时，拉动企业内部多部门在当前全球经济乏力、降本增效背景下构建覆盖全业务场景的合规协作方式。

本白皮书旨在为帮助中国企业在出海数据安全议题上，解读相应的法律法规，分析面临的问题和挑战，并提出应对策略以建立相应管理体系和构建数据安全技术平台，从而启发企业建立自身有效的数据安全合规保障体系。

吴苹

德勤中国风险咨询全国主管合伙人

顾凡

亚马逊云科技大中华区产品部总经理

目录

Table of Contents

第一章 国际数字经济与科技发展态势 1

1.1 后疫情时代的出海大势 2

1.2 数字科技领域热点趋势 7

1.3 数字科技立法及监管趋势 10

- 1.3.1 个人信息及衍生信息保护 10
- 1.3.2 大型数字平台监管 15
- 1.3.3 人工智能技术监管 17

第二章 中国企业出海面临的合规挑战 20

2.1 数据安全与隐私合规态势概述 22

- 2.1.1 常见数据安全与隐私合规监管事项 23
- 2.1.2 数据跨境流通态势及监管重点 35

2.2 数字平台监管态势概述 39

2.3 人工智能监管态势概述 42

2.4 对中国企业出海的主要挑战 48

2.5 主要行业在出海过程的特殊挑战 55

- 2.5.1 游戏行业 55

- 2.5.2 网联汽车及软硬件服务 58
- 2.5.3 社交 App 行业 63
- 2.5.4 跨境电商行业 66
- 2.5.5 智能设备行业 69

2.6 出海支持行业的特殊挑战 73

- 2.6.1 跨境支付提供商 73
- 2.6.2 企业级 SaaS 服务提供商 75
- 2.6.3 智能广告提供商 77

第三章 中国企业出海发展合规应对建议 79

3.1 健全合规管理体系 80

- 3.1.1 计划出海或准备出海 80
- 3.1.2 已在海外有业务 81

3.2 技术平台 89

- 3.2.1 安全责任共担模型 91
- 3.2.2 亚马逊云科技云上的隐私保护 92
- 3.2.3 亚马逊云科技的合规计划 95
- 3.2.4 亚马逊云科技云上的安全 98

3.3 应对案例 104

- 3.3.1 案例背景介绍 104
- 3.3.2 企业面临的出海安全合规核心挑战 105
- 3.3.3 解决方案 106

1 国际数字经济与科技发展态势

一 国际数字经济与科技发展态势

1.1 后疫情时代的出海大势

全球经济增长仍然面临巨大压力

随着 2023 年 5 月，世界卫生组织宣布新冠疫情不再构成“国际关注的突发公共卫生事件”（PHEIC），人们逐步开始回归疫情前的生活状态。但是，全球经济复苏的前景充满不确定性，依据联合国 5 月发布的《世界经济形式与展望》，预计 2023 年世界经济增长率为 2.3%、2024 年略微增长至 2.5%，仍然远低于疫情前 2018 年的 GDP 增长率 3.7%。与此同时，全球经济增长两极分化的态势逐渐明显，大多数发达经济体经济急剧下滑，而南亚、西亚以及非洲在内的发展中区域虽然仍能保持相对较高的 GDP 增速，但与疫情前、甚至 2022 年相比仍有所下滑。

外资外贸是中国经济增长的重要支撑及成果

根据中国海关总署统计数据，2022 年全年中国货物进出口总额突破 42 万亿元人民币。**推动产业向中高端迈进、促进数字经济和实体经济的深度融合、加快数字经济的发展、推动高质量共建“一带一路”**仍然是未来几年的重点发展方向。

在此背景之下，发展海外市场成为了较多中国企业的优先选择，其中，以跨境电商、游戏互娱、消费电子、新能源汽车为代表的新兴行业更是在出海的道路上大展宏图，形成空前活跃的发展景象，出海规模持续增长，从以下数据可见一斑：

跨境电商：根据中国海关总署的数据显示，2022 年跨境电商进出口规模再创新高，达 2.1 万亿元，同比增长 7.1%，占进出口总额的 4.9%，跨境电商成为外贸重要新生力量。

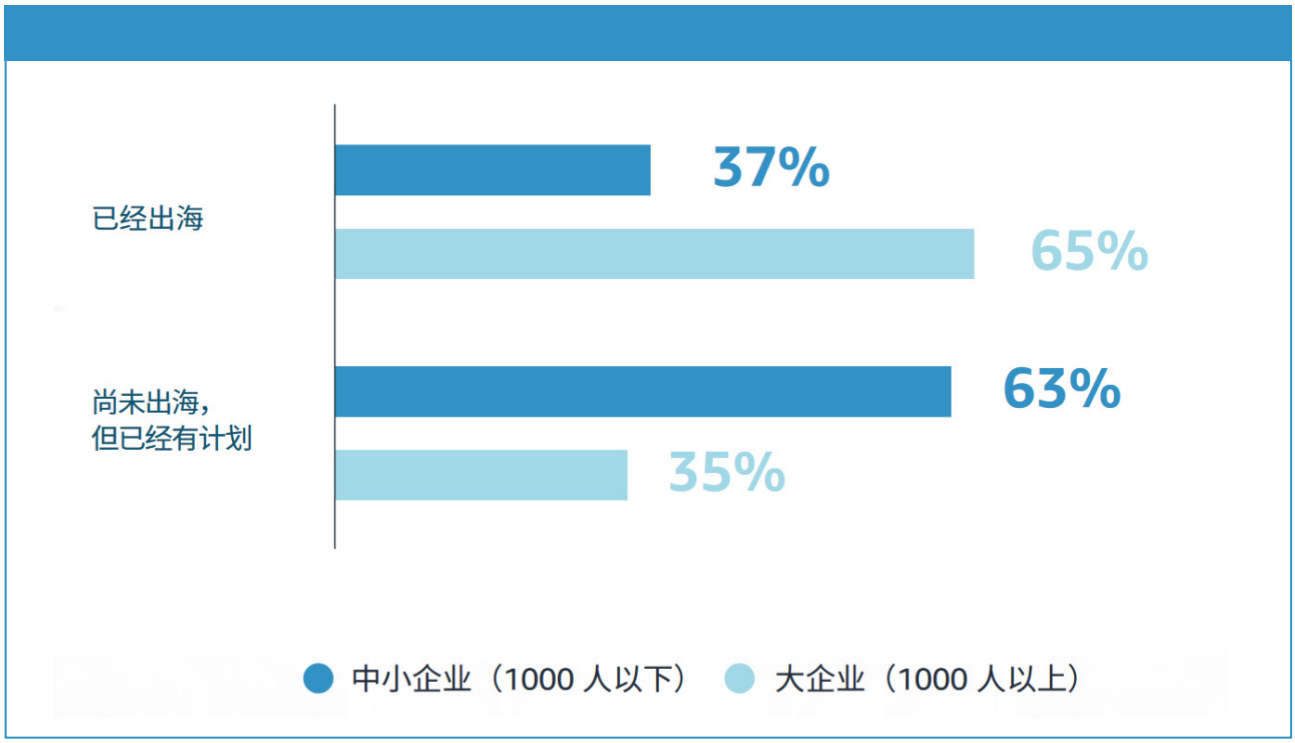
游戏互娱：根据中国音数协游戏工委发布的《中国游戏产业报告》，2022 年 1-6 月，中国自主研发游戏在海外的实际销售收入达 89.89 亿美元，同比增长 6.16%。多款手游在海外的表现，无论是在下载排行还是游戏内付费充值都占据了当地应用榜单的前列。

消费电子：据海关总署数据，2023 年 1-4 月，智能手机出口近 1.6 亿台，手机以及包括智能家居产品、无人机等消费电子早已成为多个国家和地区炙手可热的产品。

新能源汽车行业：据中国汽车工业协会统计分析，继 2021 年超 200 万辆、2022 年超 300 万辆之后，今年上半年中国汽车出口达 214 万辆，同比增长 75.7%，预计 2023 年全年汽车出口有望达到 400 万辆，成为整体汽车市场的重要增长力量。

中国企业出海规模日益增长，中小企业乘上风口

亚马逊云科技于 2022 年 6 月发布的《中国企业上云出海趋势洞察》数据显示，在已经布局全球业务的受访企业中，大型企业依然占据主导地位，占比达到 63%，但是，在计划出海的企业群体中，员工 1000 人以下的中小企业则占据了主流，占比达到 65%。由此可见，面对数字经济所带来的机遇，中小企业将越来越多地参与到出海业务中，借助各类云服务实现跨区域业务的数字化转型与智能化创新。



出海足迹从欧美拓展到东南亚、北美洲、非洲等新兴区域

中国企业出海足迹近年从欧美等传统区域扩展到东南亚、北美洲、非洲等新兴区域。根据亚马逊云科技 2022 年 6 月的《中国企业上云出海趋势洞察》，超过 60% 受访出海企业的全球业务布局覆盖超过 3 个以上海外地区。

- 东南亚作为新兴经济体的代表，由于地理位置优越，人口基数庞大，且拥有接近中国文化习惯的先天优势，成为很多中国企业初次出海的重点考虑地区以及出海业务覆盖最高的地区，尤其是对于从事网络游戏、金融科技以及企业服务的中国企业，东南亚俨然已成为其出海的首选地。

- 欧洲和北美洲作为发达国家集中地区，受到大型企业更高的关注，分别位居出海重点覆盖区域的第二位、第三位。由于欧洲、北美洲的高价值客户较为集中，中国出海企业更加关注对品牌建设的投资力度，提升品牌竞争力。

- 南美洲、非洲以及中东地区作为新兴经济体集中地区，正在成为中国企业出海的“新蓝海”，在 2021 年，中国对非洲出口 1483 亿美元，同比增长 29.9% [1]。

[1] 中华人民共和国商务部统计数据

激烈竞争促进出海业务及盈利模式多样性发展

在竞争日益激烈的国际市场中，传统的业务及盈利模式带来的收入增长有限，中国企业也在探索应用数字经济的东风，开展更为广泛的创新活动。

- 跨境电商供应链相关企业开始分工合作、协同预测、协同供应、协同研发，以提高企业对市场变化的反应速度，强化产品功能质量，提高生产和供应效率。另一方面，与海外消费者建立信任关系，也同样是开拓海外市场的重要一环，企业越发注重对海外消费者权益更进一步的保障，比如对消费者权利以及数据安全和个人隐私保护。
- 传统的游戏行业通过分发平台购买游戏或游戏内的充值内购进行盈利，近年来探索出新的营收模式，例如加入订阅业务，通过运营商资源触达用户获取订阅分成或广告变现等。
- 中国汽车流通协会于 2022 年的调研数据显示，所受访车企在未来 3 至 5 年仍将全部或部分采用经销商模式以及与当地售后合作，少量车企开始尝试直营 / 自建模式。数据将逐渐从分散在经销商回归到车企的掌控范围，助力于车辆研发与优化。
- 跨境支付平台、智能数字营销平台以及助力企业出海的工具平台服务成为热门投资领域，新业务场景得以实现，产品触达更多消费者，更好地跨区域运营。

随之而来的处理数据敏感化、数据处理过程复杂化、数据来源多元化、跨区域数据流动也带来了出海过程合规新挑战。

1.2 数字科技领域热点趋势

工作生活方式的变化带动了线上服务的发展和对远程安全保护的关注

2020 年开始，新冠疫情的爆发引发了人们对于公共卫生安全与个人隐私边界的热烈讨论，社会公众越发注重对自身隐私的保护。

一个典型场景是过去近三年，人们把工作和生活的重心转移到线上，且随着疫情后经济艰难复苏，越来越多的消费者选择更为透明和低廉的线上购物渠道，物美价廉的中国服装快时尚品牌、操作友好的智能互联家电以及与社交网络深度融合的直播购物生态成为海外新宠儿。但在此过程中产生的数据自动化处理、多渠道数据融合化等复杂的新型问题，引发了公众对企业的不信任，以及对 AI 技术背后黑盒的担忧，加大了隐私增强计算的迫切需求。

另一个场景，是疫情期间许多企业被迫转为线上办公。对于网络体系较为健全的互联网企业来说，要求员工使用 VPN 等类似的隐私通道技术可以相对安全高效地实现远程办公，而对于网络边界建设不完全的企业，员工可能不得不在远程办公期间通过互联网接入企业，线上办公所处理的数据大部分也都通过互联网传输，这会大大增加员工受到网络攻击和社会工程的攻击风险，对数据保护是一个巨大的挑战。再者，在工控领域，远程操作的有效性和精准性远远不如实地操作，并且远程接入工控网络也会增加遭遇各种网络攻击的风险。同时，使用个人电脑存放机密材料，因设备损坏、设备被盗等原因导致的信息泄露事件仍时有发生。

AI 等新技术在加速价值产生的过程也带来了新风险

随着 AI（Artificial Intelligence，人工智能）算法及算力基础设施的快速发展，生成式 AI 在商业领域的应用在近两年成为了热点话题，尤其是在人机交互问答、图像生成及美化、文本生成等领域在给商业或人们日常生活带来极大便利的同时，AI 技术的安全性、对人类社会带来的新挑战也成为关注的重点。

AI 的运行除了依赖于大量算力、网络传输的基础设施支持以外，其被“投喂”的数据量级、准确程度以及人为对 AI 的干扰也极大地影响了 AI 的实际表现。由于网络数据以及训练过程的被误导，AI 极有可能提供带有欺骗性、误导性甚至是非理性的信息给到交互人，带来了不可控因素，包括降低了 AI 技术的可信度。

另一方面，在交互人与 AI 进行沟通过程中，可能会无意识地提供个人信息或商业机密。即便存在事前的使用提醒，但是此类信息的被动收集仍有可能发生。对于用户来说机密信息被不恰当地提供，而对于企业来说需要额外考虑应如何处理这类交互过程产生的数据以及如何进行保护，避免此类数据泄露以及进入模型提供给其他用户。

在网络安全领域，AI 在被用于自动化地网络安全运营以减少人工成本、提供筛查效率的同时，也被不法分子用于寻找新的漏洞或生成更有侵犯性的网络攻击策略。企业不得不投入更大地精力提升其网络安全能力，以应对使用了 AI 技术的网络攻击，避免在自身的安全防护中疲于奔命。

但与此同时，企业之间的不信任以及对外的隐私承诺促使了数据保护技术的发展。例如在分布式机器学习技术被质疑可能导致大量隐私数据泄露时，联邦学习提供了一种将隐私保护和机器学习相结合的方法，允许多方企业在不揭露自身敏感数据的同时参与运算，并且得到期望结果。各方企业在参与联邦学习时，中心处理节点会向各个企业节点共享一个初始模型以供建模，在企业节点完成建模之后将建模参数采用同态加密等保密手段传回中心节点，中心节点通过新一轮的计算改进新的模型之后再共享给各节点。此过程不断重复就构成了基本联邦计算。除了采用联邦学习和同态加密等密码学手段保护个人隐私外，可信时空技术和追踪技术也被运用于数据保护。

1.3 数字科技立法及监管趋势

1.3.1 个人信息及衍生信息保护

在数字化时代，随着云计算、移动通讯、物联网、机器学习、人工智能、区块链以及其他技术的蓬勃发展，各行业领域在数据安全方面面临的机遇和挑战伴随其数字化和自动化变革进程而来。各国立法者们正在加紧完善国内立法，并积极参与双、多边数据跨境规则的制定：**从各国视角，完善立法保护了本国重要数据，提升了数据安全治理效能，加快颁布国内数据法律更是规制了各商业主体的收集、使用、分享、存储以及披露数据信息行为；从国际视角，为占据数据国际流动规则话语权，各国纷纷建立严格的数据出境管理制度，积极参与数据跨境流动对话，并共同积极推进数据在全球范围内的安全流动。**

一方面，在各国法律层面，上世纪末至今，各国陆续开启了隐私保护国内立法进程。欧盟《通用数据保护条例》（General Data Protection Regulation，简称“GDPR”）的生效，更催生了新一轮的隐私保护法律体系的完善，各国开始反思过往立法实践并对其补充、优化。其次，除了保护个人信息外，多个国家也开始加强对非个人信息的规制，对可能影响国家安全、经济运行、社会稳定、公共健康和安全的数据进行强监管，例如韩国的《信用信息法》、《信息通信网法》，欧盟委员会发布的《欧盟数据战略》（European Data Strategy）、《2023 数字罗盘》（2030 Digital Compass: Your Digital Decade），美国的《CLOUD 法案》（The Clarifying Lawful Overseas Use of Data Act）等。

另一方面，在国际规则层面，除了个人信息保护，其他的商业数据同样蕴藏着巨大的经济价值。其流动支撑了跨国贸易中商品、服务、人才、资本等几乎所有资源的流动，已成为推动全球经济增长的必要力量。随着全球各国数字产业及大数据、云计算技术的迅猛发展，数据流动将对全球经济产生更深远的影响，由此产生的数据红利与数据安全之间的碰撞将深刻影响着未来数字经济的走向。为了释放数据红利并兼顾数据安全，抢占新一轮经济竞争制高点，美国、澳大利亚、韩国等国纷纷建立、完善数据跨境流动的相关国内规则，并积极推动、参与国际规则的制定。

从上述立法情况，不难预见以下几点趋势：

首先，各国将制定统一专门的“个人信息保护法”并细化其适用规则。目前，全世界有三分之一的国家存在生效的隐私保护法令，超过三分之一的国家正在制定统一立法的过程当中，在未来可预见到将出现更多专门的隐私保护立法。各国在制定统一的个人信息保护立法的同时，将配套出具了更细致的法令的适用规则及操作指引。

第二，将出现更多针对特殊领域的专门立法。统一的隐私保护立法对各行业提出了统一的合规标准，但针对敏感信息集中的针对特殊的领域，例如医疗、金融、财务等行业，统一的要求未能满足敏感信息的保护标准。为解决这一问题，各国将出台针对特殊领域的特别法令，对数据进行风险分级管理，以满足多层次需求。

第三，国际间将逐步形成较为通用的数据保护和隐私原则。现代数据保护和隐私法规具有一些共同的原则，如，数据处理者需要有处理数据的合法理由等。随着各国与国际组织立法的不断深入，这些基本的适用原则将出现更大的趋同趋势。在这样的前提下，双边和多边的数据保护互认机制将出现，这将极大地便利跨国企业对不同地区业务的协调，从而大幅度降低运营成本。

第四，在个性化推荐方面，部分国家已建立算法推荐的监管制度，对算法缺乏透明度、不良内容诱导、用户标签聚合可能导致特定个人被识别等情况进行了相应的规制。例如，我国于去年发布《互联网信息服务算法推荐管理规定》，用以规范互联网信息服务算法推荐活动，规定算法推荐服务提供者应当加强用户模型和用户标签管理，完善计入用户模型的兴趣点规则和用户标签管理规则，并应向用户提供选择或者删除用于算法推荐服务的针对其个人特征的用户标签的功能，同时该规定鼓励算法推荐服务提供者优化检索、排序、选择、推送、展示等规则的透明度和可解释性，避免对用户产生不良影响，预防和减少争议纠纷。而欧盟于 2022 年颁布的《数字服务法案》（Digital Services Act）则要求超大型在线平台和超大型在线引擎应对所使用的推荐算法及其他算法系统进行风险评估，考虑风险的严重性和发生概率，并对此采取风险缓解措施。

第五，除隐私保护的监管外，部分国家也提升了对影响国家安全、公共健康和安全的重要非个人信息的管控。如我国全国信息安全标准化技术委员会于 2022 年发布的《信息安全技术重要数据识别指南（征求意见稿）》，用以对《网络安全法》第 37 条关于重要数据的境内

存储以及出境安全评估及《数据安全法》第 21 条关于国家加强对重要数据保护的初步响应。又如美国国家标准与技术研究院（National Institute of Standards and Technology，简称“NIST”）一直在制定关于受控非密信息的安全保护要求，包括 SP 800-171《保护非联邦系统和机构的受控非密信息》、SP 800-171A《受控非密信息安全要求评估》、 SP 800-171B《保护非联邦系统和组织中的受控非密信息：关键程序和高价值资产的增强安全要求》。800-171B 的范围扩展到了非联邦机构，如联邦政府的合同商跟联邦政府发生了关联，由此产生的数据到了社会领域，非联邦机构就必须落实这些数据的安全要求。

第六，在跨境规则方面，各国将建立完善的数据出境管理机制，数据本地化要求的地区范围将扩大。各国结合本国产业发展的特点及现有政策基础，以维护个人隐私权利、保障企业发展创新、捍卫国家数据主权安全、增强数字国际竞争力四个价值维度为基本考量，积极探索建立各国的数据管理体系。许多国家 / 地区已制定了数据本地化法律，其范围仅限于特定行业（如德国要求电信组织在本地存储通信数据）或特定部门（如澳大利亚要求将健康数据存储在本地）。随着立法的深入和各国公民隐私保护意识的提升，全球各地区将出现更细化的本地化要求。

最后，各国将推动国际数据跨境自由流动规则的构建，促进数字经济稳健发展。通过提高数字基础设施供给标准、完善验证监管机制等措施，为数字网络和创新服务的蓬勃发展创造有序健康的环境，也将是全球各国针对数字价值的普遍追求。各国关注国内规则与不同国际规则的兼容性，降低规则差异给跨境数据流动管理带来的风险和成本，开发与全球跨境流动规则对接的认证机制，争取国际信任及合作空间。

1.3.2 大型数字平台监管

除了对一般数据处理角色的监管，当前欧美发达国家及我国对于一定用户规模的大型数字平台[2]的监管越来越严格，从**公平竞争、用户权益、网络和数据安全**等方面明确平台服务提供者应承担的义务。综合来看，大型数字平台相关监管的法律内容更加详细、其适用范围逐渐扩大，各国执法理念和工具创新等趋势凸显，监管背后的政治经济博弈也在加剧。

在欧洲，2022 年 7 月，欧洲议会高票通过《数字市场法》（Digital Markets Act，以下简称“DMA”）和《数字服务法》（Digital Services Act，简称“DSA”），并将其整合为“数字服务一揽子法案”（Digital Services Package，简称“DSP”），两个法案各有侧重，DMA 重在数字平台反垄断，DSA 重在数字内容治理，实现共同管控互联网巨头在欧洲的活动。法案赋予了欧盟理事会对大型数字平台空前的监管权力，标志着欧洲数字市场监管模式的重大转变。通常在监管过程中，还协同 GDPR 和《反垄断法》（European Competition Law）限制大型数字企业的市场份额和市场行为。

在美国，对大型数字平台监管主要集中在反垄断方面，美国司法部曾对巨头企业展开反垄断调查，意在限制它们在互联网相关领域的市场份额和影响力。2021 年 6 月，美国众议院审议通过了六项反垄断法案，分别是《终止平台垄断法案》（Ending Platform Monopolies Act）《美国创新和线上选择法案》（American Innovation and Choice Online Act）《平台竞争和机会法案》(Platform Competition and Opportunity Act)《收购兼并申请费现代化法案》（Merger Filing Fee Modernization Act）《通过启用服务切换（ACCESS）法案》（Augmenting Compatibility and Competition by Enabling Service Switching Act）以及《州反垄断执法场所法案》（Augmenting Compatibility and Competition by Enabling Service

[2] 大型数字平台泛指如欧洲议会与欧盟根据《数字服务法》（DSA）定义的“连续四个月月均活跃用户的数量大于或等于 4500 万”的超大型在线平台、中国《互联网平台分类分级指南（征求意见稿）》定义的“平台上年度在中国的年活跃用户不低于 5 亿，核心业务至少涉及两类平台业务，上年底市值（估值）不低于 10,000 亿人民币，且具有超强的限制商户接触消费者（用户）的能力”的超级平台。在本文中指代具有较大规模的互联网在线平台。

Switching Act，简称《ACCESS 法案》），旨在控制大型科技企业（年市值或在美年净销售额在 5500 亿美元以上或在美月平均活跃用户在 5000 万以上的平台企业）不断膨胀的权力。与此同时，在 2022 年 3 月，美国司法部正式批准反垄断立法《美国创新和线上选择法案》（American Innovation and Choice Online Act），新法将禁止大型数字平台将自己的产品和服务置于竞争对手的产品和服务之上的行为。

在澳大利亚，2021 年 2 月，澳大利亚议会正式通过《新闻媒体和数字化平台强制议价准则》。该法对社交媒体、数字代理服务平台，以及其他在澳大利亚拥有超过 250 万用户的大型数字平台使用新闻内容作出多项规范，规定澳大利亚新闻机构有权要求大型数字平台为使用其新闻内容付费，并就此开展单独或集体谈判。

在中国，对于大型数字平台的监管主要依赖《网络安全法》和《反垄断法》等法律法规。例如，根据中国《反垄断法》，中国监管部门曾向几个大型平台公司出具限制经营和提高透明度的监管警示，约束其行为。2021 年 10 月，中国国家市场监督管理总局发布了《互联网平台分类分级指南（征求意见稿）》和《互联网平台落实主体责任指南（征求意见稿）》两部指南并向社会公开征求意见，以加强对超级平台的监管，警示各大数字公司合规经营和数据安全等问题。

根据 2017—2021 年的有关公开资料，现有 18 个国家和地区发起了针对全球数字平台头部企业共计 150 起反垄断诉讼和执法案件，总罚金超过 192.6 亿美元。从区域来看，欧盟及其成员国的案件最多，占比 40.7%（其中 40 % 来自欧盟委员会）；美国、英国次之，分别占 21.3%、7.3%；印度、俄罗斯、澳大利亚、日本、韩国等也都加大了对大型数字平台企业的反垄断调查力度。

总体来说，世界各国对数字平台的监管呈现出多样化的趋势，对于中国出海企业来说需密切关注是否会落入监管范畴。在立法方面，数字隐私、数据保护和反垄断法规等日益完善，企图规范数字市场秩序；在社会观念上，市场运作需透明公正，用户权益和个人信息得到应有保护等观念变得越发重要。

1.3.3 人工智能技术监管

人工智能（Artificial Intelligence，简称“AI”）席卷全球的趋势势不可挡，但如何监管却成了棘手的问题。新一代人工智能具有高度的自主性、自学习及适应能力，传统的监管模式已难以适应其发展需求，**在对智能产品应用后果和风险的预判，问题责任归属，以及对潜在安全风险管控等方面都将面临新的挑战。**近年来，各国对于人工智能技术的监管趋势和立法趋势日益增强，主要涉及到数据隐私、算法公正性、安全可靠性、机器人伦理等多个方面。

2020 年 2 月，欧盟委员会发布了三份重要的数字战略文件，其中《人工智能白皮书 - 走向卓越与信任——欧盟人工智能监管新路径》（White Paper on Artificial Intelligence: a European approach to excellence and trust）是欧盟的人工智能发展战略，也是欧盟出台的第一份人工智能白皮书，旨在打造以人为本的可信赖和安全的人工智能，确保欧洲成为数字化转型的全球领导者。白皮书将“人工智能”定义为将数据、算法和计算能力结合起来的技术集合。特别强调，鉴于人工智能系统的复杂性及其潜在的风险，提升人工智能应用的可靠性至关重要。欧盟希望通过制定更加严格的规范，特别要在消费者保护、防止不公平商业竞争、保护个人数据等方面加强立法和管理，最大限度减小人工智能应用风险。2021 年 4 月，欧盟发布《人工智能法案》(Artificial Intelligence Act) 提案，提出了 AI 统一监管规则，旨在从国家法律层面限制 AI 技术发展带来的潜在风险和不良影响，使 AI 技术在符合欧洲价值观和基本权利的基础上技术应用创新得到进一步加强，让欧洲成为可信赖的全球 AI 中心。目前，欧洲议会内部市场委员会和公民自由委员会在 2023 年 5 月 11 日

目前，欧洲议会内部市场委员会和公民自由委员会在 2023 年 5 月 11 日高票通过了《人工智能法案》的谈判授权草案，且已于 6 月中旬提交并通过欧洲议会全会表决，今年晚些时候欧洲议会将与欧盟理事会就法律的最终形式进行谈判。

2020 年 1 月，美国联邦政府发布了《人工智能应用的监管指南》（Guidance for Regulation of Artificial Intelligence Applications）。这是美国发布的首个人工智能监管指南，为联邦政府对 AI 发展应用采取监管和非监管措施提供了指引。该指南要求联邦政府在针对 AI 技术和相关产业采取监管和非监管措施时，要以减少 AI 技术应用的障碍、促进技术创新为原则，随而推动了美国人工智能监管政策在各行各业的积极发展。例如，美国食品和药物管理局和美国交通部一直致力于将人工智能监管纳入其监管框架；美国联邦贸易委员会（FTC）于近期启动了对于人工智能歧视、欺诈和数据滥用等问题的监管规则制定；住房和城市发展部正着手推翻原先制定的一项规则，允许人们对与住房分配有关的算法决策不公提起歧视诉讼和索赔；平等就业机委员会发起了一项在人员雇佣和办公场所管理等方面需合理有限采用人工智能系统的倡议；五大金融监管部门也已开始调查美国金融机构中存在的影响风险管理、公平借贷和信用额度的人工智能应用及相关做法。

2022 年 4 月 22 日，日本内阁发布《AI 战略 2022》，旨在加快人工智能在日本的发展。该战略秉持“以人为本”、“多样性”、“可持续”三项原则，设定了人才、产业竞争力、技术体系、国际合作、应对紧迫危机五大战略目标。此外，政府将从经济安全的角度推出一些举措，希望在以下五点提高 AI 技术，一是提升 AI 的可信性，确保 AI 的透明性和可解释性；二是丰富数据以支撑 AI 的应用；三是面向人才培养打造相关环境；四是推动 AI 在政府的应用；五是促进 AI 与物理、化学、机械等日本具备强大实力的领域的融合，以开发竞争力强的产品与服务。

2019 年中国国家人工智能治理专业委员会发布《新一代人工智能治理原则》、《新一代人工智能伦理规范》，两者不仅提出人工智能相关方的八项原则，更是为“伦理道德”如何融入人工智能研发和应用全生命周期奠定发展基础。随着大数据及相应技术的发展，2021 年 12 月，国家互联网信息办公室联合公安部等四部门联合发布了《互联网信息服务算法推荐管理规定》对算法推荐类等技术服务提出合规要求。

2022 年，随着元宇宙、AI 换脸等技术的发展，监管部门针对深度合成技术，发布《互联网信息服务深度合成管理规定》以规范国内对相应技术的使用。2023 年 7 月，面对 ChatGPT 和大模型领域的科技创新动态，中国网信办联合国家发展改革委、教育部、科技部、工业和信息化部、公安部、广电总局七部门发布《生成式人工智能服务管理暂行办法》（以下简称“《暂行办法》”），这也是全球范围内针对生成式人工智能的首部专门立法。《暂行办法》整体聚焦生成式人工智能的规范应用与发展。在内容方面，《暂行办法》明确了责任主体的义务，不仅对生成式人工智能在具体场景的应用提出合规要求，也针对多领域主管部门所管辖的生成式人工智能服务应用开展了行业垂直监管。此外，《暂行办法》更是增设“技术发展于治理”章节，鼓励 AI 技术发展，推动数据资源平台建设并促进基础技术的自主创新。

总体来说，各国在 AI 技术的立法和监管趋势上多数是为了保护消费者和用户的利益，旨在增强 AI 技术的透明性，促进技术可信的同时限制 AI 对于社会道德、公平性的破坏。

2 中国企业出海面临的合规挑战

二 中国企业出海面临的合规挑战

在数字经济领域，中国企业面临的出海挑战是复合的，其复合一方面体现在对于监管事项的管理是糅合的，例如企业难以为数据安全、AI 安全以及隐私保护建立三套有所关联又不同的体系去应对合规要求，成本以及内部执行的复杂性也会让这种方式难以实施。企业更多地是**建立一套管理体系可以响应不同领域的合规要求，**梳理为可清晰理解的实施与管控路径。

另一方面的复合体现于出海过程的合规不仅仅企业内部管理、内部技术建设就可以满足的，**企业如何面对监管、面对客户以及供应链、合作伙伴的合规与安全也至关重要。**尤其是当出海企业落入数据控制者[3]角色时，对于合作的其他数据控制者或数据处理者仍需审视其是否具有足够的能力保护处理过程的安全与隐私。

因此本章节将以数据安全与隐私合规为主要切入，在其基础上通过分析企业需面对的常见的合规事项，并列举在此基础上数字平台与人工智能监管的要点和补充领域，最后总结其对于中国企业的主要挑战以及主要行业所面临的特殊合规挑战。

[3] *此处为 GDPR 下的数据控制者（Data Controller）与数据处理者（Data Processer）角色，各国的角色命名与定义以各国法律为准。*

2.1 数据安全与隐私合规态势概述

在本章节中，我们将以出海企业在应对合规过程中需重点关注的六类主体为框架，介绍面对不同主体企业需响应的合规监管事项。

合规面向主体	说明
管理层	即出海企业的管理体系，包含公司业务及在数据安全、隐私保护领域的负责人，以及为支持内部运行的管理制度与管理规范。
产品及服务	出海的主要产品或服务，除业务功能外还需满足在设计界面、处理流程、安全管控、功能提供等方面的合规要求。
技术实现	支持公司、产品及服务整体安全运行的基础，包括不限于数据加密、安全事件监控等手段。
监管	本文中主要指需要向监管部门进行登记、汇报、或其他所需的持续沟通与互动的行动。
用户	对于面向消费者的企业，消费者则此处用户。对于面向企业的用户，这里主要为系统承载的个人信息的所属个人。最终指向均为数据主体。
第三方	包括不限于供应商、生态合作伙伴等存在数据流动的第三方组织。

另外由于数据跨境的合规流通是近年来另一热点话题，其所涉及的对象与以上六类合规面向主体存在重叠，且场景较为特殊，将在 2.1.2 章节具体开展介绍。

2.1.1 常见数据安全与隐私合规监管事项

出海企业在内部可粗略按照在监管事项响应的主要负责角色来分为三类职能：**管理职能、产品与服务的设计职能以及技术实现职能。**另一方面在外部，出海企业面对着当地监管机构、数据主体、第三方供应商或合作伙伴的合规需求。

内部及外部的合规面向主体的关系可如下图所示：

管理职能将作为出海合规的核心角色，承担起内部合规的总体职责，同时对外与当地监管机构保持恰当的对接与沟通。

- 任命**数据保护负责人，识别合规要求并监督其落实**

  数据保护负责人（或称数据保护官，Data Protection Officer）是自我约束机制中的重要一环。以 GDPR 的要求为例，数据保护负责人主要有以下职能和角色：一是作为各辖区监管机构的联络点；二是帮助数据控制者 / 处理者识别合规要求并对处理活动中是否满足合规要求进行监督；三是作为和数据主体的联络点；四是作为境外数据控制者或处理者在处理行为发生地的代表。该角色应当具备足够的专业资质背景，同时企业管理层需要提供对于数据保护负责人履行职责应有的地位、资源以及接触个人数据和处理机制的渠道，在其履行职责时不应受干涉，如直接向最高管理机构汇报等。

  但需注意的是，不同国家对于数据保护负责人的要求存在一定差异，主要体现在数据保护负责人任命的触发条件、该个人的工作地点限制、是否属于公司雇员等方面。

- **数据保护负责人登记**

  在任命数据保护负责人之后，如 GDPR、新加坡《个人数据保护法》（Personal Data Protection Act 2012，本文简称“新加坡 PDPA”）、泰国《个人数据保护法》（Personal Data Protection Act 2012，本文简称“泰国 PDPA”）均要求企业需要公示其数据保护负责人以便公众或被处理信息的个人可通过该渠道进行联络，GDPR 与泰国 PDPA 则进一步要求该数据保护负责人需告知监管机构该个人及其联系方式。

- **数据处理活动登记**

在英国、马来西亚及尼日利亚，企业在达到指定条件后还需就其数据处理活动进行登记说明。

在不具备豁免情形的前提下，处理个人数据的出海企业在英国开展业务时，应在每个收费期前 21 天内向英国信息专员办公室（Information Commissioner's Office，简称“ICO”）支付数据保护费并提供与企业相关的信息，如企业的姓名和地址、企业的工作人员数量、企业财政年度营业额等。支付的数据保护费水平取决于企业的类型、性质、规模和营业额而有所不同。

如果数据控制者在 6 个月内处理超过 1000 个数据主体的个人数据，必须向尼日利亚国家信息技术发展局（National Information Technology Development Agency，简称“NITDA”）提交一份审计摘要的副本，说明其隐私保护的内部做法，包括收集的个人身份信息、收集目的、收集和使用的隐私政策声明及获取同意的方法、数据主体权利请求渠道、安全保障措施、个人数据使用说明、组织的隐私和数据保护政策和程序以及对于该政策和程序的监测与汇报记录。在 12 个月内处理超过 2000 个数据主体的个人数据的数据控制者，必须在次年 3 月 15 日之前向 NITDA 提交其数据保护审计摘要。

而马来西亚在《2013 年个人数据保护（数据使用者类别）法令》（Personal Data Protection Regulations 2013，简称“PDPR”）及其修正案注明了需要向个人数据保护委员会（Personal Data Protection Commission）注册的数据控制者类别，涵盖行业包括：银行和金融机构、保险业、健康、旅游和酒店业、运输、直接销售、1961 年《控制用品法》（Control of Supplies Act）规定的零售或批发交易等。如果出海企业是作为两个或以上类别的数据使用者，则出海企业必须就其所属的每个类别分别向个人数据保护委员会提出注册申请。

- **数据泄露事件报告**

  一旦出海企业意识到发生个人数据泄露或重大的数据安全事件，应当按照企业应急预案机制及时控制事件的影响范围，并在指定时间内将事件情况通报监管机构，根据法律要求告知数据主体。

  在 GDPR 中，除非数据泄露不会对个人的权益和自由带来威胁，企业最迟不应晚于意识到泄露发生后的 72 小时通知监管机构，如超出该时间，则需额外对延迟原因进行解释。通知内容包括事件性质、涉及个人的类别与数量、涉及个人数据的类别及数量、数据保护负责人联络方式、后果预估、已采取的措施说明。

  以韩国为例，当企业意识到发生个人数据泄露事件时，必须立刻通知受影响的数据主体。此外，如果发生涉及 1,000 个数据主体或更多的数据泄露事件，数据处理者除了向数据主体发出个别通知外，还必须向个人信息保护委员会（Personal Information Protection Commission，简称“PIPC”）或 PIPA 指定的专业机构报告数据泄露事件，并在其互联网主页上披露规定的信息，如果没有开设互联网主页，则在其营业场所的明显位置披露至少 7 天。

在内部的产品设计层面，产品与服务的负责人则需根据数据保护负责人识别的应履行的合规要求，在设计层面的上对此类要求进行落地。

- **遵从数据处理的基本原则**

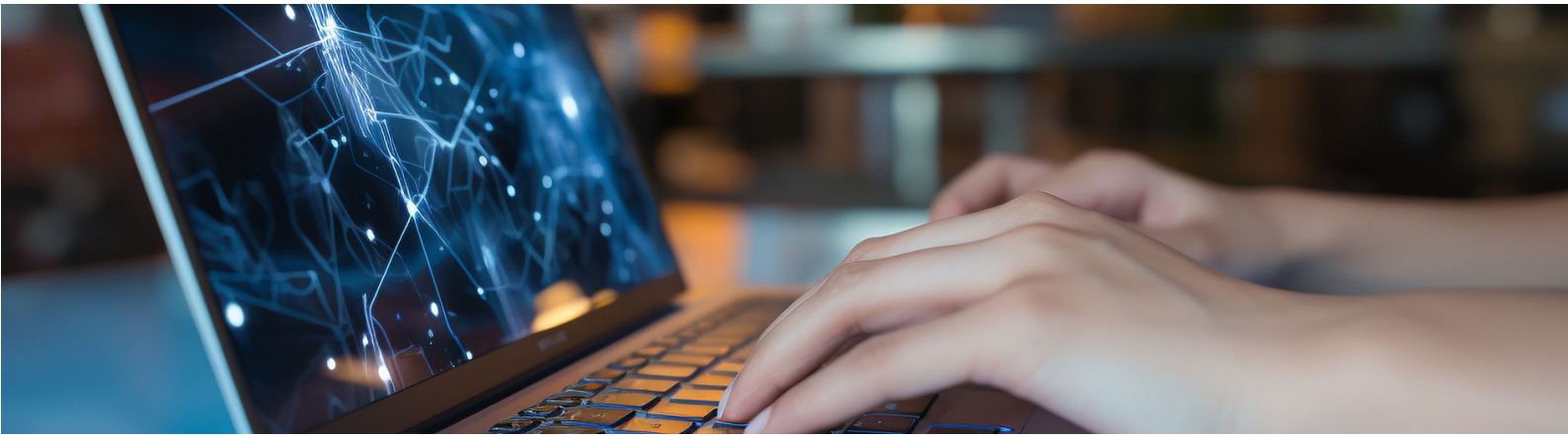
  以 GDPR 为例，处理个人数据应遵循合法性、公平性、透明性、目的限制、数据最小化、准确、存储限制、完整性与机密性、问责制原则。合法性具体体现在数据来源合法、数据处理目的合法等，例如仅在获取个人同意或为了履行合同、履行法律义务或保护数据主体以及公共利益所必要，再对个人数据进行处理。因此该原则应作为指定产品或服务细节时的主要考量依据。

  告知与同意是整个数据处理活动中至关重要的环节，也是合法性中最常见的场景。在告知层面，以 GDPR 为例，在获取数据主体同意收集其个人数据前，应当披露数据控制着的身份和联系方式、数据保护负责人的联系方式、处理目的及法律基础、其他可能接收到数据的第三方、存储期限或期限的确定标准、其所享有的数据主体权利及履行方式、涉及的自动决策机制与分析过程等。若如上信息发生变化，至少需告知数据主体。该同意应当是自由做出的，且该同意应当是有权随时被撤回的。但需要注意的是，同意的形式或根据当地法律法规的要求有所不同，如一般的同意、明确同意或书面同意以及单独同意。在 GDPR 中，对特殊类型的个人数据进行处理、个人数据被用于自动化决策以及数据出境时，需要获取数据主体的明示同意。

- **识别可能处理的特殊类型个人数据以及处置要点**

综合各国家和地区的法律规定来看，特殊类型的个人数据略有不同，企业需根据运营所在地识别当地文化下需特别关注的个人数据类型。常见的、可能被纳入特殊类型的个人数据有：种族、民族起源、政治观点、宗教信仰、哲学信仰、基因、生物特征、健康数据、性生活、性取向等。各国与地区均要求特殊个人数据的处理需具有更高的保护要求，这要求出海企业在海外应先识别所在辖区的特殊类型的个人数据种类，并就这些特殊类型的个人数据种类采取比一般合理措施更为严格的安全控制措施。

而另一类常见的需特别关注的个人数据类型则为儿童个人数据。近年来，因儿童个人数据安全事件频发，各国开始纷纷关注儿童个人信息问题，特别是欧美发达国家对儿童个人信息的关注度较高且对于儿童的定义各不相同，因此在企业出海过程中应首先识别所在辖区对于未成年人或儿童的年龄规定，再针对所在辖区制定相应的儿童个人数据处理与管理流程。例如英国规定年满 13 岁的儿童才可提供有效的同意；日本则要求处理 15 岁及以下儿童的数据时应获得法定监护人同意。



- **识别并管理数据跨境活动**

企业应识别并管理自身数据跨境的活动，并评估境外接收方是否有足够的能力保护个人数据的安全以免损害数据主体的利益，同时也需符合当地法律对于数据出境的必要条件。针对于数据跨境活动而言，除需通过所在国家规定的数据出境管理要求外，通常还需在数据跨境前需要获取数据主体的明示同意，并告知供其进行决定的必要信息，如出境后接收国及接收方、可能带来的风险等。

详细内容可参见 2.1.2 章节。

- **开展数据保护影响评估**

数据保护影响评估（Data Protection Impact Assessment，简称“DPIA”）为在 GDPR 下引申出的一种对于特殊处理活动所产生的后果及影响分析的手段，如自动化决策或大规模对敏感个人数据的处理。其至少应包括对于数据处理技术和处理目的的描述、处理目的的必要性分析、对于数据主体可能带来的影响及风险的评估以及预想的应对风险的措施。

出海企业应在处理数据之前进行 DPIA，识别可能导致自然人的权利和自由面临较高风险的可能性和严重性，特别需要考虑数据处理的范围、背景和目的以及风险的来源、概率、特殊性和严重性，并帮助识别为消减此类风险需采取的安全技术保障措施。

修订前的加利福尼亚州消费者隐私法案（California Consumer Privacy Act，简称“CCPA”）并没有强制要求出海企业进行此类评估，然而，2020 年通过的加利福尼亚州隐私权利法案（California Privacy Rights Act，简称“CPRA”）在 CCPA 的基础上进行了拓展，其指出加州隐私保护局（California Privacy Protection Agency，简称“CPPA”）有权发布法规，要求处理消费者个人信息对消费者隐私或安全构成重大风险的企业定期提交个人信息处理风险评估，包括处理过程是否涉及敏感个人信息 确定并权衡处理过程中给企业、消费者、其他利益相关者和公众利益带来的影响和潜在风险，如果处理的风险大于给消费者、企业、其他利益相关者和公众带来的利益，则限制或禁止这种处理。出海企业应时刻关注加州隐私保护局针对风险评估的监管动态，并按照最新监管要求制定处理个人信息风险评估的流程。

出海企业若在加拿大魁北克省开展业务，则需要按照修订后的《魁北克私营部门个人信息保护法》（Privacy Protection In Quebec: An Overview Of Amendments To The Law Governing The Private Sector）要求，对涉及获取、开发或重新设计涉及个人信息的信息系统或电子服务交付的任何项目，以及在个人信息被转移到魁北克区域外时，进行数据保护影响评估。

阿根廷数据保护机构已于 2020 年 1 月 28 日发布《数据保护影响评估指南》（Data Protection Impact Assessment Guidelines），该指南给出了开展数据保护影响评估应包含如下阶段：

a. 第一阶段是确定参与者并记录评估的过程，目的是确定初步分析和评估的参与者，并确定记录过程；

b. 第二阶段是适用法律的分析，目的是分析适用于所进行的数据处理的法规，以了解它们对该处理的不同阶段的适用性；

c. 第三阶段是初步分析，目的是对影响后续评估需求的几个因素进行初步分析；

d. 第四阶段是处理背景梳理，目的是从个人数据保护的角度分析所有处理阶段的情况；

e. 第五阶段是风险管理对第四阶段确定的处理背景的每个阶段进行风险分析，以充分管理这些风险；

f. 第六阶段是风险处理计划，目的是对第五阶段确定的风险进行处理计划的制定。

另外，该指南还提供了一个企业在进行数据保护影响评估之前应该考虑的问题清单，如该项目是否涉及敏感数据的收集；所处理的数据是否来自弱势群体；该项目是否涉及使用会因其性质或程度而对隐私或人们的权利构成风险的技术；是否与组织外的第三方签订合同来进行数据处理活动；数据是否转移到第三国；这些国家是否有被认为是适当的立法。

除了在内部关注对于产品设计上对隐私的保护外，安全保障部门在产品或服务以及公司内部对于数据保护的技术手段实施，从安全角度提供合规能力的支撑。

- **采取与数据类型相匹配的保护手段，并持续监测其有效性**

  对于数据处理过程，考虑到目前的技术水平、实施成本、数据处理的性质、范围、内容、目的，以及数据处理给自然人的权利和自由带来的不同可能性和不同严重程度的风险，控制者和处理者应当采取适当的技术和组织措施，以确保安全保障等级和预期风险是相匹配的。企业可采取的技术措施包括不限于个人数据的匿名化和加密、对数据处理系统或服务的安全保障、数据备份及恢复、对措施的有效性进行检测、评估。目前全球的此类法规中，几乎未见直接约束企业需采取的具体保护手段，更多从原则上进行要求。

- **管理数据留存期限**

  数据保留指对特定类型的数据设定保留期限，在期限截止日期到来之前对指定数据进行安全存储。如欧盟、泰国、新加坡及尼日利亚，提出了企业应根据最小化原则来管理数据的留存期限，通常不会强制设定一个固定值。出海企业需要时刻关注监管要求变化，对所在辖区法律以及自身业务实际需要对需保留的数据类型进行识别并设置保留期限，或设置到期后强制删除。

- **对数据处理活动进行记录**

部分国家和地区对于不同类型的数据提出了保留处理记录的合规要求，出海企业应在职责范围内保存数据处理活动的记录，并有义务配合辖区数据保护监管机构的调查，根据要求提供记录，以便监管机关能够对数据处理行为进行监测。

GDPR 要求每一位数据控制者或数据处理者均需保留数据处理活动的记录，记录包括数据控制者姓名及联系方式、数据主体的类别和个人数据类型的描述、数据传输的接收方、跨境传输的接受方及目的地国、删除数据的时限、技术和组织管理措施等信息。泰国 PDPA 也有类似的要求，并对记录内容提出了更细致的要求，如需记录收集个人数据的目的、使用及披露情况、数据主体权利及请求提出方法。

韩国 2011 年的《个人信息保护法》(The Personal Information Protection Act，简称“PIPA”）要求数据控制者存储和管理登录记录，记录包含在数据控制者的指导和监督下处理个人数据的负责人、雇员和工人在内的角色对数据处理系统的访问，时间至少为一年。这种登录记录应包含 ID、访问日期和时间、识别访问者的信息，以及个人数据处理者在连接到数据处理系统时执行的任务。

如前文所说与供应商和合作伙伴的数据流动过程中，书面及技术上的责任划分是有所必要的。

- **与第三方签署合同约定责任义务**

数据处理协议是数据控制者和共同控制者或数据处理者之间的合同，旨在确保双方遵守所在辖区的数据保护法律法规，通常它将约定了与双方主要协议相关的数据处理活动的性质、目的和持续时间以及如何响应数据主体的权利。

以加拿大联邦的《个人信息保护和电子文件法》（Personal Information Protection and Electronic Documents Act，简称“PIPEDA”）的规定为例，当信息由第三方处理时，该组织应使用合同或其他方式提供相当水平的保护。依据加拿大隐私专员办公室（Office of the Privacy Commissioner of Canada，简称“OPC”）对该规定的解释，合同应包括：1. 要求第三方处理者制定隐私政策和程序，包括其对员工的培训和有效的安全控制措施；2. 要求个人信息在任何时候都能得到第三方处理者的妥善保护；3. 组织有权审计和检查第三方。根据修订后的《魁北克私营部门个人信息保护法》（Privacy Protection In Quebec: An Overview Of Amendments To The Law Governing The Private Sector），各组织还需要在合同中明确规定对个人信息的使用限制、保留期限，以及要求第三方提供安全事件的通知。基于此，出海企业在外包个人信息处理给第三方时应该确保已签署包含前述内容的数据保护合同。

- **对第三方的数据安全能力进行审查**

  除合同协议外，当出海企业作为数据控制者选择供应商作为数据处理者时，需审查其是否有足够的能力在受托处理过程中保证数据的安全性、完整性以及评估数据泄露的风险。若出海企业自身作为整个出海过程中的一部分受托处理数据的处理者时，则仍需满足响应的数据保护要求，以应对可能的来自于数据**控制者的审查**。

  在日本的个人信息保护法（Act on the Protection of Personal Information，简称“APPI”）中则要求若将部分或全部数据处理行为委托至其他人，那么则应当实施必要且足够的监督，来保证个人数据处理过程中的安全管理。

  从数据安全与隐私合规法律来说，通常没有对具体审查的方式进行强制约束，但对于特定行业，如新加坡银行业要求外包服务供应商提交 OSPAR 审核报告（Outsourced Service Provider’s Audit Report，简称“OSPAR”）以证明其符合该行业的特定安全要求水平。

最后，企业还需在产品或公司官网等渠道，服务于数据主体的合理权利请求：

- **提供数据主体权利请求的渠道与响应**

  通常隐私保护法规会赋予了数据主体多项权利，但各法律具体规定的权利有所不同，常见的权利如知情权、访问权、数据更正权和删除权、撤回同意等权利。

  这就要求了一方面数据控制者需要为数据主体提供便捷、公开的渠道，另一方面数据的控制者及处理者需要协同对数据主体的具体请求进行响应，并且该响应应当在当地法律法规要求的特定时间内进行处理及回复。

  当出海企业在美国加利福尼亚州开展业时务，除了注意常规的数据主体权利保护外，还应注意保障消费者不受歧视的权利，禁止的歧视行为包括但不限于：1. 拒绝向消费者提供商品或服务；2. 对商品或服务收取不同的价格或费率；3. 向消费者提供不同水平或质量的商品或服务；4. 暗示消费者将获得不同的商品或服务价格或费率，或不同水平或质量的商品或服务；5. 对雇员、求职者或独立承包商进行报复，这些雇员、求职者或独立承包商因行使 CPRA 规定的权利而受到威胁。

2.1.2 数据跨境流通态势及监管重点

国家执法机构对数据跨境的监管一方面是为了满足公民对个人信息保护的需求，也是为了维护自身在政治经济方面的利益。数据价值实现和数据安全保障的融通对数字经济的发展具有深刻的影响。因此，世界各国、各地区立法机构和政策制定机构纷纷建立和完善数据跨境流通相关的国内法规政策，并积极制定数据跨境流通的国际协议，以平衡两者矛盾，从而促进经济安全快速发展、抢占数字经济市场先机。

国家层面对于数据跨境的监管重点

各国出于对国家安全和隐私保护的考量，会提出数据跨境流通的“门槛”，不同国家在数据跨境的态度上各不相同，常见的数据跨境合规路径包括以下方式。

- **数据本地化**

  俄罗斯是要求数据本地化存储的最具有代表性的国家。俄罗斯有关法律要求，俄罗斯公民的个人数据必须首先在俄罗斯数据库中存储，随后才能按照数据跨境流通的规则传输至其他国家。

  另一个具有代表性的国家是印度，不同于俄罗斯，印度不是对所有类型的数据都要求本地化传输，而是将个人数据划分为一般个人数据、敏感个人数据和关键个人数据，并对每类数据的跨境传输做出了不同的要求：敏感个人数据必须存储在境内，但副本可以按照跨境传输的要求传输到境外；关键个人数据要求只能在印度境内处理，只有在满足极其特定的条件方能批准出境。

  数据本地化存储要求企业在当地拥有数据中心或服务器，相关设施的建设会增加企业在当地开展业务的运营及合规成本。企业在严格执行数据本地化存储的国家和地区开展业务，需要充分评估在当地存储数据的成本、数据在当地存储后跨境传输的必要性、开展业务的利益前景等诸多方面的因素，进行合理决策。

- **基于一定的出境保护机制**

  该条件要求数据的传输方或接收方采取一定的隐私安全保护措施，以确保跨境传输的数据的安全。世界大部分国家都采用了出境保护的机制，规定了出境保护的具体情形，同时也给出了例外情形，以最大限度覆盖商业、公共管理等数据跨境流通场景。

常见的出境保护措施包括：

1. **对接收方法律环境的要求**：接收方国家应具有与发送方国家同等标准的个人信息保护体系。部分国家会在监管过程中对此类国家和地区的范围进一步进行明确，如俄罗斯《个人信息保护法》（Personal Data Protection Laws）第 12 条即说明个人数据可传输至欧洲委员会《个人数据自动化处理时个人保护公约》（The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ）的公约国及其他充分维护个人数据主体权利的国家。

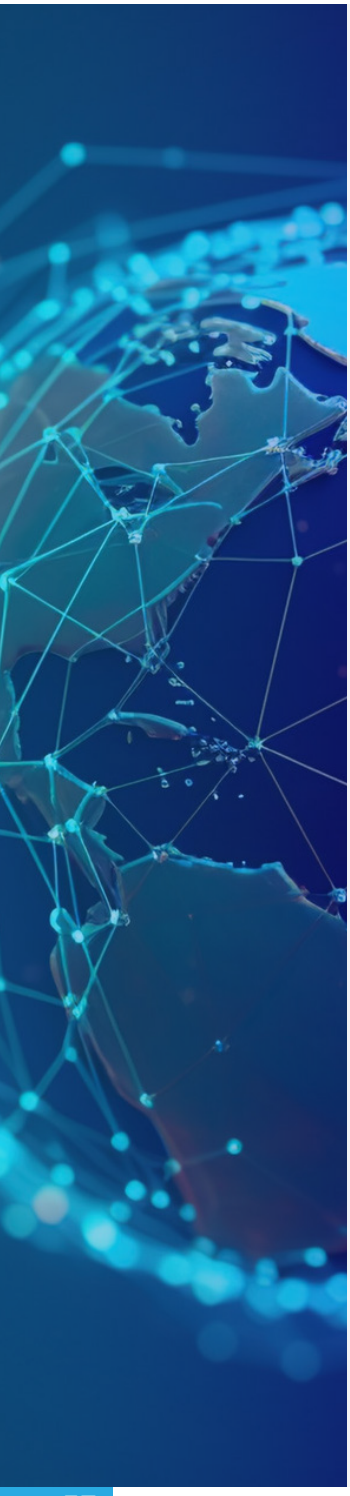
2. **使用标准合同条款（Standard Contractual Clause, 简称“SCC”）：**以欧盟及我国为代表，均将数据传输与接受方之间签订标准合同条款作为一定条件下数据跨境的合规前提。

3. **有约束力的企业规则（Binding Corporate Rules, 简称“BCRs”）：**在 GDPR 中，BCRs 主要适用于大型跨国企业在不同区域的企业内部的数据跨境流通。

4. **监管机构认可的认证或评估：**欧盟数据保护委员会（EDPB）通过了《关于认证作为数据跨境传输工具的指南》（Guidelines 07/2022 on Certification as a Tool for Transfers），探索将认证作为数据跨境传输合规机制的一种手段中的具体规则。

国家间 / 区域间协议

除了本国立法外，为了提高数据跨境流通的效率，更加充分地发挥数据价值，从而促进跨境数字经济快速发展，一些国家和地区也在积极建立数据跨境流通相关的协议，促进数据在达成协议的国家、区域之间流通。对于中国出海企业，可关注中国参与的商业关系组织之间对于数据流通的协议。



- **《全面与进步跨太平洋伙伴关系协定》（CPTPP）**

  CPTPP 协定由十一个太平洋地区的国家签署并于 2018 年生效，是太平洋地区的重要自由贸易协定。CPTPP 对个人信息保护和数据跨境流动的规则在第十四章“电子商务”中进行了规定，接收各缔约方数据跨境规则的多样性，但是不允许对数据跨境传输进行变相的限制，也不允许将数据本地化作为市场准入条件。这些约定充分显示了 CPTPP 协定对于数据跨境的推动于支持态度。对企业来说，需要注意的是，即使开展业务的国家加入了 CPTPP 协定，数据跨境也并非完全自由，也依然要在遵守所在国家数据跨境要求的前提下进行。

- **《区域全面经济伙伴关系协定》（RCEP）**

  RCEP 的协定国由 6 个东盟成员国和中国、日本等 4 个非东盟成员国组成，该协定于 2022 年 1 月 1 日正式生效。RCEP 协定在鼓励为电子商务创造有利环境的同时，也在第十二章“电子商务”明确约定了各缔约方可以有各自的监管要求。对于金融服务数据跨境流动，RCEP 特别规定，在要求保障日常运营所需数据正常传输和处理以提高金融服务销量的同时，认可各国监管机构出于监管或审慎原因制定法律法规的正当性。但是，对于企业来说，RCEP 协定为企业创造的数据跨境流动便利较为有限，企业仍需对参与协定的各国的数据跨境要求进行深入调研，以确保数据跨境业务的顺利进行。

在国际上，部分协定划定了在一定的国家范围或条件下，数据跨境可以相对自由地实现。

- **欧盟充分性认定**

  欧盟在 GDPR 中制定了“充分性认定”程序，即如果第三国具有和欧盟同等水平的数据保护标准从而经过认定进入欧盟的白名单，则第三国企业可以不受限制地将在欧盟收集的个人数据引入第三国。“充分性认定”的条件包括：法治程度、是否尊重人权和自由、是否具有个人数据保护相关立法并有效实施、是否有独立的数据保护监管机构并有效运作、是否加入个人数据保护的国际条约或协定并承担保护个人数据的义务等。目前已有日本、新西兰、瑞士等国家或地区通过了“充分性认定”，也有很多国家正在积极加入欧盟设立的白名单，但是中国尚不在白名单中。欧盟的“充分性”认定机制给为企业部署数据中心提供了更多的空间，即可以将数据中心部署在白名单国家，以实现经济或者商业目的，并在同时实现欧盟境内个人数据的跨境流通。

- **APEC 全球跨境隐私体系 CBPR**

  CBPR 在亚太经合组织 APEC 第 19 次领导人非正式会议上得到认可。CBPR 的核心由数据保护基本框架、认证机构、内部执行机制三部分组成的隐私保护认证机制，APEC 经济体中的数据控制者在满足数据保护基本框架、并按照内部执行机制执行可以申请加入该认证体系，获得认证的企业可证明自身的数据保护水平。当前加入的国家和地区包括：美国、墨西哥、日本、加拿大、韩国、新加坡、澳大利亚、菲律宾和中国台湾。目前已有来自美国、新加坡、日本、韩国的 67 家企业经过了 CBPR 体系的认证。虽然 CBPR 也为由数据跨境传输需求的企业提供了一种数据跨境传输的合规途径，但是认证成本也不可忽视。

2.2 数字平台监管态势概述

随着数字化时代的不断推进，数字平台已经成为了社会经济发展的重要组成部分。然而，数字平台的快速发展也带来了监管难题，数字平台的垄断、数据融合等监管问题越来越受关注，公平竞争和保障用户权益成为立法重点。

- **欧盟**

  2022 年 7 月，欧洲议会高票通过《数字市场法》（Digital Market Act，简称“DMA”）和《数字服务法》（Digital Services Act， 简称“DSA”），旨在明确数字服务提供者的责任，加强对社交媒体、电商平台和其他在线平台的监管。

  DSA 的前身是欧盟《电子商务指令》，颁布时仍处于互联网发展初期，以鼓励电商发展为要旨，规定法律责任较轻。然而，在网络信息技术发展的同时，互联网中介服务提供商也造成了非法商品或服务的大范围泛滥和非法内容的加速传播，对消费者权利带来了不良影响。为兼顾欧洲数字化发展转型和消费者权利保护，欧盟大力修订指令，DSA 已于 2022 年 11 月 16 日正式生效。**DSA 针对向欧盟用户提供网络信息服务的中介服务提供者划分了不同层次，包括一般中介服务提供者（如提供信息传输、缓存或托管服务的提供商）、托管服务提供商（如云计算、虚拟主机等存储信息的服务）、在线平台（应用程序商店、电商平台、社交平台）以及月均活跃用户超 4500 万人被欧委会指定的超大型在线平台（VLOPs）和超大型在线搜索引擎（VLOSEs），**需履行的主要义务包括透明度报告、非法内容举报、内容审核、用户协议、推荐透明度、广告透明度、与监管和用户建立单一联络点等。此外，VLOPs 和 VLOSEs 还需要承担系统性风险评估、设立合规职能部门、向监管提供数据访问共享等额外义务。如不履行义务，最高处以全球年营业额 6% 的罚款，对提供不正确、不完整或误导性信息的行为，处以全球收入或营业额 1% 的罚款。下图则展示了对于超大型在线平台（VLOPs）和超大型在线搜索引擎（VLOSEs）的额外监管要求的说明。

DMA 试图构建一个数字化的公平竞争环境，为大型在线平台（“守门人”）明确权利和义务规则，并要求企业不可滥用其优势地位。若一个大型在线平台可能对市场产生重大影响、提供“核心平台服务”，且目前或将来具有根深蒂固和持久的地位，将会被欧委会认定为守门人。守门人如果达到相关的看门人门槛而未能按照 DMA 的要求告知欧盟委员会，则可能会被处以其上一财政年度全球总营业额 1% 的罚款。DMA 要求守门人应允许第三方在特定情况下与网守企业[4]提供的服务进行交互操作；应允许业务用户访问在使用守门人服务时生成的数据；应允许用户在守门人平台之外推广他们的产品等应做义务。如果守门人不遵守 DMA 的关键义务，欧盟委员会可以处以上一财政年度全球总营业额的 10% 的罚款，或者在屡次不遵守的情况下处以最高 20% 的罚款。

[4] *据《数字服务法》（DSA），网守企业指大型互联网公司，也是所谓的“守门人”（gatekeeper）企业。其规模足够大，是具有系统性影响的平台企业，且连接了广泛的个人和企业用户，具有强大的经济地位，对所处市场具有重要影响。*

- **美国**

  美国参议院和众议院在 2022 年 6 月发布了《美国数据隐私和保护法》（the American Data Privacy and Protection Act，简称 ADPPA）的草案，该立法草案是第一个获得两党两院支持的美国联邦全面隐私保护提案，并且联邦贸易委员会（FTC）专门设立一个新部门，负责执行这项法律。这项具有分水岭意义的隐私保护法案，将为数据隐私保护引入一个美国联邦标准，通过为个人提供广泛的保护，对非营利组织和电信企业等所有组织提出严格的要求，为保护个人数据创建一个强有力的国家框架。此外，美国政府还出台了《加强美国网络安全法》（Strengthening American Cybersecurity Act）等法律，旨在加强对数字平台的监管。

总体来看，在数字平台监管方面仍处于不断探索、完善、升级的过程中。监管机构需要密切关注数字平台行业动态和风险发展趋势，寻求有效的监管手段与技术工具。中国出海企业前往海外如欧美、澳洲等发达国家出海的过程中，需特别识别是否落入了平台类的监管要求，及时分析与当地政策之间的合规差异，在职能建立、风险管理、透明及可信度方面进一步补强能力。

2.3 人工智能监管态势概述

人工智能的跳跃式发展在给人类社会带来广阔前景的同时，也给个人安全和保障带来很大风险，增加了侵犯人类基本权利的可能性。随着人工智能技术的发展和应用逐渐广泛，相关立法需求越发迫切，欧盟、美国、加拿大、中国等国家先后出台了一系列相关法律法规，以保护国家及个人的信息安全及隐私权利。

- **欧盟**

  欧盟于2021年4月21日公布了首个全面覆盖人工智能的法规草案《人工智能法案》(The Artificial Intelligence Act）是人工智能发展的重要里程碑。该草案目的在于降低人工智能风险，发展统一、可信赖的欧盟人工智能市场，保护欧盟公民基本权利。草案设置的监管结构兼顾了可能面对的企业面对内部和外部风险，细化了人工智能风险等级，并制定了相对应的监管措施。草案适用于在欧盟内运行的所有当地和第三方国家的人工智能系统。

草案把人工智能系统分为不可接受的风险、高风险、有限风险和极低风险四种类型：

不可接受风险：含被禁止的人工智能行为的实践，如可能对个人或公众产生威胁，例如对人或特定人群的认知行为操纵，会影响社会公平的对人的分类，实时且远程进行生物特征识别的系统等。

高风险：可能对安全或人的基本权利产生负面影响的人工智能系统，其分为两类，一类适用于欧盟产品安全法规（EU’s product safety legislation）的产品中的人工智能，如玩具、航空、汽车、医疗等，以及特定领域中的人工智能，如用于自然人的生特征识别和分类、教育和职业培训、影响就业职业机会的人工智能系统。

有限风险：需要符合最低透明度要求的风险有限的人工智能系统，主要用于使用户做出合理决策或其他不包含不可接受风险和高风险的 AI 交互。

其中着重指出对于具有高风险的人工智能产品和服务需要实施上游治理防范，规定了严格的前置审查程序和合规义务。高风险人工智能在使用时应受到严格的监管，严格遵守数据管理、记录保存、透明度、人为监管等规定，以确保系统稳定、准确和安全，具体如下。

生命周期	管理措施
进入市场前	• 建立和维持风险管理系统，风险管理系统需要能够识别已知的和可预见的以及使用后可能存在的风险； • 进行数据治理，训练人工智能系统的数据应当满足一定的质量标准要求，并且在对于数据的训练、验证、测试等环节，需要遵循相应的管理规定； • 在人工智能系统入市前，应当制定并更新技术文档，并向主管部门提供所有必要的信息； • 人工智能系统应当在技术上设计为自动记录相关日志，并且能够进行追溯。日志至少应当包括记录时间、参考数据库、输入数据以及参与自然人等； • 人工智能系统应当确保其操作足够透明，附有简明、完整、正确和清晰的信息，使得用户能够正确理解和使用系统； • 人工智能系统的设计应当保证人能够实施干预。
进入市场中	• 人工智能系统应当进行合格评估，由相关机构验证人工智能系统是否满足前述入市前的各项管理要求；并起草一份合格声明，交由国家监督机构和主管部门保管； • 人工智能系统在投放入市场或投入使用时，应当在欧盟建立的数据库中进行备案。该数据库可以为公众免费使用浏览，并可以被机器所读取；

生命周期	管理措施
进入市场中	• 人工智能系统在投放入市场时，应当贴上实体 / 数字形式的 CE 标志。
进入市场后	• 人工智能系统入市后，应当建立入市后检测系统，收集、记录和分析人工智能系统在整个生命周期的性能数据； • 在人工智能系统发生严重事件时，人工智能系统的提供者应当在意识到该严重事件后 72 小时内向国家监督机构报告。

初版草案并未提及生成式人工智能和聊天机器人，但在修正案中，将生成式人工智能与高风险人工智能划分在了同一级别。对于草案明确的不可接受风险，包括利用人的潜意识扭曲个人行为给他人带来身体和心理伤害，利用特定群体的脆弱性影响个人行为给他人带来身体和心理伤害，以及任何形式的社会信用分级以及实时的远程生物识别技术，均予以明令禁止。属于有限风险的人工智能系统，需要履行包括告知用户等透明义务，以确保用户的知情权和选择权。对极低风险的人工智能系统，例如垃圾邮件过滤器，草案没有进行干预。

该草案在欧盟一般数据保护条例（GDPR）的基础上进一步明确了人工智能系统方向的法律框架，明确了数据治理和技术监管方面的要求。目前，欧洲议会内部市场委员会和公民自由委员会在 2023 年 5 月 11 日通过了《人工智能法案》的谈判授权草案，并已于 6 月 14 日在欧洲议会表决通过，欧洲议会、欧盟委员会与欧盟理事会进行谈判后预计将于今年晚些时候通过。

- **美国**

美国白宫于 2022 年 10 月发布了《人工智能权利法案蓝图》（Blueprint for an AI Bill of Rights），该蓝图虽不具有强制性，但其重要性不应被低估。该蓝图指出，确保个人数据不被误用或滥用，是开发或部署人工智能的企业需要自愿遵循的准则。在没有颁布具体法律之前，遵守这些准则将是选择性的。该文件制定了设计、使用和部署自动化系统时应遵循的五项原则，包括：**（1）安全有效的系统；（2）算法歧视保护；（3）数据隐私；（4）通知和解释；（5）人工替代、考虑和回退。**该文件的出台将为美国人工智能发展提供指引。

2023 年 1 月，美国国家标准与技术研究院（NIST）发布了《人工智能风险管理框架》（AI Risk Management Framework，简称“AI RMF”），旨在指导机构组织在开发和部署人工智能系统时降低安全风险，避免产生偏见和其他负面后果，提高人工智能可信度。该框架主要提出了两个视角，一是为识别人工智能环境中的风险提供了一个概念性路线图，概述了与人工智能相关的一般风险类型与来源，并列举了可信赖的人工智能的七个关键特征：**安全、可靠和有韧性、可解释性、隐私增强、公平、负责任且透明、有效且可靠。**二是提供了一套评估和管理风险的组织流程，将人工智能的“社会技术”维度与人工智能系统生命周期的各个阶段，以及相关参与者联系起来。这些过程和活动的关键步骤是“测试、评估、验证和确认”，并被分解为治理、映射、测量和管理四大核心功能，每个功能项下还分为不同的类别和子类别，通过多元化展开，帮助机构组织在实践中应对人工智能系统带来的风险和潜在影响。

- **加拿大**

在加拿大，2022 年 6 月，联邦政府在下议院提出了 C-27 法案，C-27 法案的一个新特点是提议颁布《人工智能与数据法案》(Artificial Intelligence and Data Act，简称“AIDA”)。AIDA 是加拿大第一部规范 AI 系统创建和使用的联邦法律，将对不遵守规定的行为进行处罚，旨在以减轻伤害和偏见风险的方式开发和部署高影响力的 AI 系统来保护加拿大人。AIDA 将“人工智能系统”定义为一种技术系统，它通过使用遗传算法、神经网络、机器学习或其他技术，自主或部分自主地处理与人类活动相关的数据，以生成内容或做出决策、建议或预测。AIDA 的既定目的主要有两点，一是通过建立适用于全加拿大的 AI 系统的设计、开发和使用的共同要求，规范 AI 系统中的国际和跨省贸易和商业；二是禁止与 AI 系统相关的某些行为，这些行为可能对个人或其利益造成严重伤害。AIDA 将“伤害”定义为对个人的身体或心理伤害、对个人财产的损害，或对个人的经济损失。

- **中国**

2023 年 7 月 10 日，中华人民共和国国家互联网信息办公室联合多个部委发布了《生成式人工智能服务管理暂行办法》（以下简称“办法”），对生成式人工智能在我国的开发及应用进行规范。该办法中，对于生成式人工智能的定义是指具有文本、图片、音频、视频等内容生成能力的模型及相关技术。该办法面向与公众服务的生成式人工智能，不

适用于新闻出版、影视制作、文艺创作等活动以及不面向境内公众提供的服务。办法的核心内容如下图。

总则

坚持正向价值观	避免歧视	商业公平	尊重合法权益	透明、准确、可靠

技术发展与治理

- 鼓励**内容、应用场景、生态的创新**
- 鼓励**算法、框架、芯片及软件平台的自主创新**，以及数据资源平台建设
- **依法开展训练数据处理活动**，包括来源合法、保护知识产权、个人信息保护、提高训练质量、遵循法律法规提出的安全要求
- 数据标准活动应制定**清晰、具体、可操作的标注规则**，对标注质量进行**评估**，对参与人员进行**培训**

服务规范

- 承担**网络信息内容生产者责任，履行网络信息安全义务，以及可能涉及到的个人信息保护义务**
- 与使用者**签订服务协议**
- 明确及**公开其服务的适用人群、场合、用途**，指导使用者科学理性认识和依法使用生成式人工智能技术
- 依法履行输入信息和使用记录保护义务，**不得收集非必要个人信息**
- 提供**安全、稳定、持续**的服务
- 发现**违法内容时的处置措施**以及**模型优化整改**
- 建立**投诉、举报机制**，公布投诉举报入口，公布处理流程和反馈时限，及时受理、处理公众投诉举报并反馈处理结果

除此之外，中国在近几年陆续发布了《互联网信息服务算法推荐管理规定》《互联网信息服务深度合成管理规定》，并已经开启了算法备案等行动。

作为中国企业，需要做好灵活应对，及时进行政策调整。中国人工智能系统研发企业在符合我国合规要求的同时，如果想要出海在欧盟，应及时通过欧盟要求人工智能企业完成的前置审查程序，确定企业自身研发的人工智能系统属于哪种风险类型，并进行相对应的合规检查，以确保企业满足数据管理、透明度、人为监管等规定；如果想要出海美国，则需更多的考虑自身是否属于大型科技企业，是否需要承担更多的责任。企业在明确出海目标后，应及时制定相应的出海战略，并落地执行一系列关于如何做、怎么做的具体方案。

2.4 对中国企业出海的主要挑战

综合前文所述，企业出海过程中面临的监管要求是非常多样化的，面向这些监管要求的应对需要从管理、业务与技术三个维度进行考量。

第一个维度为企业管理面临的上层设计挑战。

- **跨多个国家的合规要求融合**

  不同国家与地区之间的合规要求有所差异的，大的差异包括需履行职责的不同或特定国家提出特定的合规要求，小的差异包括如 21 天、72 小时内等时间范围的差异。但企业无法对每一个出海国家都建立一套独立的管理制度体系，建立共性的管理目标、标识各国特例的管理要求，对于企业来说是减少合规压力、提高管理效率的手段之一。但此类管理体系的建立，必须基于对当地法律法规的充分理解上，因此合规追踪是企业管理的必修课。

- **海外合规负责人的选定与协作**

  企业需根据自身业务涉及的数据规模与范围，考虑在海外的合规负责人，如数据保护负责人以及平台合规负责人。

  - **成本的规划：**海外合规负责人的设置不可避免的导致人力和管理成本的增加，企业除任命该负责人外，还需考虑该角色履行职责需具备的团队规模以及招聘成本。
  - **人员的选用与管理：**海外合规负责人需具备一定的专业资质背景、工作能力，在全球安全与合规人才紧缺的当下，企业需面临雇佣当地专家还是从中国派驻专

关联主体：

- 监管机构
- 数据主体

家的抉择，其难免存在当地人才与与国内工作文化适配，或国内员工在与当地合规监管部门沟通、与当地团队探索协作方法的权衡。

- **协作模式：**企业如何为其提供足够的资源以支持其履行其职责带来的团队规模、团队架构、合作模式都将与国内的本土业务有所差异，尤其是不同文化背景下、甚至跨国间的沟通与协作成为另一难点。

- **数据跨境传输**

  数据跨境的合规难点在于场景的识别以及对于合规传输的路径选择。

  - **跨境场景的多样化：**中国企业出海常涉及到数据由中国境外传输至境内处理、跨区域数据访问、数据在境外不同国家与区域间跨境传输等不同的情况，迫使企业需要应对境内外的因不同文化、政治及经济因素产生的多样化的数据合规要求和执法政策。

  - **对于不同国家数据跨境的监管要求的识别：**不同国家之间的数据传输往往需要通过特定的合同或规则才可进行，这给企业进行业务所在地的决策、数据中心选址带来了挑战，企业需考虑不同决策之间的各类成本及风险，如合规风险、实施成本、招聘及资源投入等。虽然大多数国家都提供了多种数据跨境的途径，例如标准合同条款或监管审查等，但是途径适用条件相对复杂，需要专业人士分析在不同国家、不同场景下应该如何选择跨境的合规途径。

关联主体：

- 跨国供应商及合作伙伴
- 跨国子企业或母企业

- **供应商及合作伙伴管理**

  出海企业为了满足业务支持与运营，采购或联合境内外的第三方、合作伙伴提供的服务或工具。这些第三方 / 合作伙伴或与出海企业都会或多或少地在数据处理活动中产生交集，或与出海企业共同处理数据，或受出海企业委托处理数据。

  - **明确责任：**第三方 / 合作伙伴与出海企业均属于数据处理行为链路上的责任人，任何一方的安全性存在纰漏都可能对其他各方的数据合规态势产生影响。因此，签署合同协议的前提即为识别各方在监管要求下的角色，以及该角色需履行的责任义务。
  - **对第三方的安全管理深度及成本平衡：**为确保第三方或合作伙伴不会成为出海链路上的合规“弱点”，除合同协议外，对于第三方实际的安全保证措施的评估也成为关键行动。但若每个合作方都进行实地评估其安全水平并不实际，公司需要根据不同风险程度的数据处理活动对不同的合作方提出具体请求。

关联主体：

- 供应商及合作伙伴

- **数据主体权利响应**

  企业需对数据主体的合理请求进行回应以满足对于数据主体基本权利的保障。

  - **标准化的需求识别机制：**数据主体的需求是多样的，如何准确分析收到的热线电话、Email、网站反馈、线上客户等渠道不同语言风格下的实际诉求，判断其合理性，以及需开展的具体行动，都需要基于前期对于

关联主体：

- 数据主体

诉求的分类以及标准化的响应规则，以指导执行人员的行动。

- **从个人数据到个人的关联管理：**对于数据主体的请求可能会涉及到对于个人名下所有处理的个人数据情况的汇总。例如在提出删除权请求时，企业如何保证删除了“所有”该个人的数据，而非是某个特定系统的该个人的数据。这就需要企业从原本的仅管理特定数据库表的个人数据，延伸至以人维度拉齐其在企业内部的所有关联信息。这也有助于进一步分析数据之间的关联性，企业可在用户同意的情况下通过数据分析寻找新业务机会。

- **透明性与独立第三方审查**

  透明、可信是当前监管的重点方向，尤其是对于复杂的大型数字平台或者参数上亿的人工智能算法，其披露必要的规则、内部开展的技术与管理手段，都将是监管未来关注的重点。若企业落入了大型数字平台或高风险人工智能算法的监管，在对外披露或引入第三方就自身合规情况进行审查之前，企业需要对该类信息进行整理，做到“心中有数”，这迫使企业需要预先开展此类自检自查，并提前进行整改。

第二个维度为内部业务治理中的合规挑战。

- **数据保护影响评估**

  数据保护影响评估对企业的挑战主要体现在数据收集的商业目的和产品方案隐私合规的权衡方面。

  产品和服务的开发涉及产品开发和合规的各部门，各方的诉求不同，需要通过一套机制拉齐各方，让业务部门了解需要如何开展才能符合合规要求，同时合规及法务等部门同事则需要全面了解业务的开展形式、涉及到的个人信息等情况，以综合评估数据收集活动对于数据主体的影响。

- **在产品中融入隐私设计（Privacy By Design，简称“PbD”）**

  PbD 最早在 GDPR 中提出，旨在提倡在产品设计、开发、测试等生命周期阶段就将隐私保护的需求融入其中，而非等产品上线再补充隐私保护的功能或模块。这需要企业对现有的产品研发流程进行改造与优化，识别在不同阶段应由哪些角色采取的具体行动，例如隐私需求整理、隐私界面设计等工作。

- **对外披露及声明**
  - **对外披露的准确与持续一致：**如隐私政策类文件中需要清晰、明确且没有误导地体现数据处理的实际目的与范围，需要企业对于自身的个人数据处理活动了如指掌，并随着业务设计的变化而可及时反馈与外部隐私政策，保持其一致性。
  - **额外的信息披露准备：**如大型数字平台，若涉及到在线广告，还需建立公共信息库，对外就广告信息进行披露，并提供外部查阅的渠道。这需要非常强的信息管理能力以及额外的渠道构建工作。

第三个维度要求安全技术的投入应与数据的敏感级别及时代发展相匹配。

- **数据安全控制措施**

  信息安全技术地不断进步为出海企业提供了更多的工具维护用户的个人数据安全。注入攻击、模糊攻击、网络钓鱼等多样化的网络安全攻击手段，以及逐步发展的密码破解方法，使得个人数据安全遭受到更大的风险。一旦发生数据泄露数据，可能面临监管处罚、用户投诉的风险，甚至可能因此陷入诉讼，对品牌形象造成威胁。

  - **与数据的敏感程度及技术发展相匹配：**企业提供数据安全保障措施应当足够满足所处理个人数据的安全性，另一方面与外部的网络攻击、行业安全发展趋势相匹配，但这也不可避免地导致在安全设备、软件和人员投入上的增加。

  - **与数据处理场景相匹配：**另一方面跨国企业内部通常会进行大量的远程办公，远程办公可能涉及数据的跨境传输，也会涉及数据传输中的安全问题。传输数据不仅涉及企业业务和商业机密，也可能涉及大量员工和用户的个人数据，一旦出现泄露，将对企业业务造成严重影响。

- **数据处理记录留存**

  数据处理记录留存不会显著地影响企业经营的成本，若数据处理过程没有得到恰当的记录，从对外合规来讲，难以自证是否以按照约定方式对数据进行处理，而从自身的企业管理视角，也难以判断是否存在数据泄露、数据篡改等情况发生。同时在欧盟、美国、泰国、韩国等国家，数据处理过程的记录是一项强制性的要求。

- **数据留存期限的设置**

  监管一般要求的保留期限是实现数据主体授权使用目的所必须的最短时间，这就使得数据需要在一定期限内删除或者被匿名化。而个性化推荐和用户画像等数据价值的实现方式都完全依赖可以关联到数据主体的个人数据，被删除和匿名化的数据会导致企业无法实现数据收集的商业目的。同时，不同的保留期限也为企业建立数据保留的管理机制制造了挑战。

  但需要注意的是，某些特定数据由其他法律规定了最短留存期限的，不应与其他法律法规冲突，例如合同履约信息。

2.5 主要行业在出海过程的特殊挑战

2.5.1 游戏行业

随着技术和互联网的发展、游戏内容不断丰富，用户数量也在持续的增加，游戏市场规模（尤其是手机游戏）同样水涨船高。越来越多的企业开始进入游戏市场竞争，为了寻求更高的回报，出海成为游戏企业拓展市场的重要途径。在大环境的推动下，各国政府逐渐加强对游戏行业的监管和立法，韩国于 2020 年及 2022 年先后发布的《游戏产业促进法》（Game Industry Promotion Act）、《游戏产业促进法的执行法令》（Enforcement Decree of the Game Industry Promotion Act），欧洲议会也在 2022 年 11 月高票通过了首项电子游戏相关决议。可见，游戏企业在开展全球业务时需要关注各地的游戏法规要求，遵守不同的法规，包括游戏内容审查、虚拟物品交易、用户数据保护、未成年人保护等方面。

游戏内容审核

游戏玩法及游戏内容是吸引用户的重中之重，然而不同国家地区对游戏内容的监管松紧不一，根据调研得出，部分发达国家对游戏内容的监管较为严格。韩国在《游戏产业促进法》（Game Industry Promotion Act）中就有明确规定在韩国市场推广和发行的游戏需采取评级程序、随机型内容概率的要求、游戏广告的规制，以及负责视频游戏评级和监管的游戏评级和管理委员会（Game Rating and Administration Committee，简称“GRAC”）、游戏内容分级委员会（Game Content Rating Board，简称“GCRB”）以明确标识各类游戏的年龄分级符号及游戏内容说明。游戏企业在选择出海地区时，也需充分考虑当地的监管要求，如游戏内容及角色对话是否涉及血腥、色情或者其他当地监管无法接受的元素，游戏玩法是否涉及赌博元素等。

游戏年龄适应性评估

部分国家地区针对游戏内容和元素进行了年龄适应性划分，如美国的 European Systemic Risk Board（ESRB）、日本的 Computer Entertainment Rating Organization（CERO）、澳大利亚的 Australian Classification Board（ACB）、俄罗斯的 Russian Age Rating System（RARS）、欧洲的 Pan European Game Information （PEGI）等，其目的一方面可以防止未成年人接触不符合其接受能力的内容，另一方面也能有效保护电子游戏的创作自由。

企业应根据游戏内容的特性，按照当地要求对出海游戏进行年龄适应性评估，针对游戏目标群体做好对应的保护措施或内容编辑。

儿童隐私保护

因游戏行业的用户群体中未成年人、青少年人占据较大的比重，部分国家和地区对于未成年人的隐私监管较高，如美国的《儿童在线隐私保护法》(COPPA) 和欧洲的《通用数据保护条例》（GDPR）等对儿童信息收集有明确要求和约束。游戏企业应根据自身用户群体采取相应措施，如针对未成年人使用的游戏，企业应明确对未成年人同意认定的标准、方法、程序等详细规定，设置有效的隐私声明和监护人同意机制，明确告知收集、存储、使用或披露儿童个人信息的目的、范围、方式和期限。

虚拟物品交易

因游戏业务营收模式主要集中在虚拟物品、广告等方面，游戏企业将面临各国关于游戏交易的监管。如欧盟要求游戏企业公开游戏中的随机奖励概率，规范虚拟物品交易，监管虚拟货币等操作。监管者在保护游戏消费者权益的同时也在防范非法金融操作。游戏企业应妥当设置并公开随机奖励的概率，也应主动监控并分析异常交易。

广告投放

部分游戏企业为扩大宣传力会在海外投放游戏宣传广告，同时也有部分游戏企业会在游戏内投放他人广告作为盈利来源。部分发达国家对广告内容会有较强的监管，如日本对虚假广告和虚假宣传的监管力度相对严格。游戏企业应在广告投放上采取合理的措施规避风险，如通过专业广告企业进行投放，或成立内容审核部门等。

2.5.2 网联汽车及软硬件服务

随着越来越多国内汽车企业战略出海，海外业务发展过程中面临的国内外网络安全和数据合规风险对**国内汽车整车企业、零部件提供商、软件服务提供商**提出了新的挑战。

个人信息保护

在服务于海外市场时，车辆生命周期过程中提供服务时不可避免需要收集用户的个人数据。尤其是随着智能汽车行业的发展，车辆的智能生态也会愈发成熟，但为提高人车交互体验，除了基本个人信息，还可能涉及监控影像、地理位置、行为习惯以及面容、声纹等个人生物识别信息的收集和处理，甚至还包括了违章、事故以及犯规行为的记录数据。数据类型的复杂、数据收集和处理场景的复杂以及涉及多类第三方，给汽车整车和汽车生态的上下游供应商带来了如下挑战：

- **收集数据范围与目的的最小化：**智能汽车车内车外集成了多类传感器，包括车内部的疲劳监控、语音助力、行车记录仪，车外部的监控摄像头等。这些传感器无时不刻不在预备着进行收集信息，例如语音助理通过特殊引导词唤起，需要避免录制到车内无关的背景声音以及情景信息，以规避刺探客户隐私。荷兰个人数据管理局（Dutch Data Protection Authority）就在 2023 年发布了对于车辆“哨兵”模式的监管意见，调整后仅在车辆被触碰时才进行反应，车主收到警报后查看情况时才记录画面，同时通过车辆灯光闪烁提示车外人员。

- **数据存储和分析的本地化：**驾驶员的生物识别数据，例如面部、语音、指纹等用于解锁、启动或激活车辆某些命令的应用程序建议本地进行存储，尽量规避传输至云端、甚至通过跨区域访问造成被动的数据跨境。汽车主机厂、零部件供应商以及软件服务供应商，都需识别各类场景下需处理的数据类型、规模、敏感程度，注意评估数据回传的必要性。

- **与第三方信息分享的范围最小化：**除汽车厂商自身对于车辆内产生、收集数据的分析外，智能化功能也往往依赖于第三方提供的服务。例如车辆提供当前所在区域的天气情况，车辆向提供天气服务的供应商提供位置信息，由天气服务供应商反馈天气信息到车辆。在这个过程中需要注意地理位置的获取需在车载终端获取同意，并且位置信息的提供为可满足服务的最小范围，例如仅到市、区级，而非具体的坐标信息，且该信息不应持续收集。

- **同意获取的方式：**在当前的智能汽车上，与车辆的交互主要通过车载终端进行，因此车载终端将成为同意获取以及同意撤销的主要窗口。汽车软件设计过程中，应尽量避免打包同意的情况，针对于各项较为敏感的信息收集，建议以单独同意的方式为主，并且在不影响安全地前提下，可以便捷、快速地关闭授权。若涉及到跨区域或跨国家的场景，数据控制者发生变化时，需要提示告知车主。

- **数据安全性保护：**车辆驾驶相关的核心功能应与信息娱乐等互联网功能相隔离，汽车核心功能直接影响了车辆以及车主的安全性，互联网功能的宕机不应影响到车辆的驾驶系统的正常运作。另一方面生物识别数据的收集、识别方案应当能够抵抗一定强度的攻击，并设置验证尝试的有限次数，避免对于生物识别信息或用户身份信息的原始信息的本地存储。

网络安全体系建设

由于以新能源汽车为代表的智能汽车越来越受到消费者的认可，智能汽车中的车载网关、T-BOX、传感器、OTA、车载 OS、车载信息娱乐系统、ECU、OBD-II 接口等数据处理组件也面临了巨大的安全挑战。联合国欧洲经济委员会（UNECE）下属世界车辆法规协调论坛（Working Party 29，简称“WP29”）发布了第 155 号法规《网络安全与网络安全体系 CSMS》（简称 UN-R155）和第 156 号法规《软件更新与软件更新管理体系 SUMS》（简称 UN-R156），是国内车企出口海外所面临的主要网络安全要求，是车型在 WP29 成员国[5]上市销售的必备条件。

1. UN-R155 是一个关于车辆网络安全管理体系（Cyber Security Management System，简称 CSMS）和车型认证（Vehicle Type Approval，简称 VTA）的法规，2021 年 1 月生效，自 2022 年 7 月起对 WP29 下所有国家新上市的车型施行，2024 年尚未停产的车型也必须获得该认证。其主要内容包括：

   a. 企业层面获得 CSMS 认证，即需 OEM 建立覆盖车辆全生命周期（研发，生产，售后，下市）的网络安全管理流程，从管理上确保车辆在生命周期各阶段都得到有效的安全管控；

   b. 车型层面获得 VTA 认证，即需 OEM 针对具体车型在工程层面设计和实施安全措施，确保目标车型安全防护技术有效实现；

[5] *WP29 成员国包括欧盟、韩国、日本、泰国、马来西亚等国家*

c. 企业获得 CSMS 认证是具体车型获得 VTA 认证的前提，两个认证均获取才可以在 WP29 成员国内上市。

2. UN-R156 是一个关于软件更新管理体系 SUMS（Software Update Management System，简称 USMS）和车型认证的法规，在 2022 年 7 月针对新上市车型正式生效并施行，2024 年针对所有车型施行。其主要主要内容包括：

a. 企业层面获得 SUMS 认证，即需 OEM 建立软件升级管理体系，体系由软件升级评估流程、软件升级文档管理及安全的软件升级流程这三部分构成。

b. 车型层面获得 VTA 认证，即针对车型从工程角度对 OTA 方案进行验证和认证，验证车型符合通用软件升级需求及 OTA（Over-the-Air Technology，无线传输）附加需求。

自动驾驶算法

自动驾驶算法可能影响到个人的生命安全，依据待正式发布的欧盟《人工智能法案》，其极有可能落入高风险人工智能类别。一旦法案正式生效，汽车企业急需建立全流程的算法管理措施。此外德国以开始针对自动驾驶的立法《自动驾驶法》（Gesetz zum autonomen Fahren），其中对自动驾驶的行使条件、参与方义务、数据处理场景、功能测试要求进行了规定。在 2022 年英国网联和自动驾驶汽车中心发布《自动驾驶汽车：联合报告》中，对安全使用自动驾驶汽车提出了诸多立法建议，涉及自动驾驶概念、自动驾驶的分级、设定安全标准、初始准入和授权、使用中的安全保障和数据使用民事责任等多个方面。

2.5.3 社交 App 行业

近年来大数据时代下，部分互联网企业利用已采集的海量消费者数据进行大数据包括用户画像分析，为消费者提供精准推荐、个性化广告等服务。虽然一定程度上为消费者带来便利，但随着各国的个人信息保护宣传和监管力度加强，消费自身者对个人隐私意识也在不断提高，企业需要更加注重这些行为便利以外带来的合规风险。

- **用户画像**

  在移动互联网和大数据普及的今天，大部分企业，尤其是高科技行业为分析用户的群体分布特征和个性化需求，都会使用用户画像。GDPR 对用户画像定义为“通过自动化方式处理个人数据的活动”，并且在第 2 条“适用范围”中明确规定：“本条例适用于个人数据的全自动或部分自动处理，以及形成或旨在形成用户画像的非自动个人数据处理”。也就是说，在 GDPR 语境下，不仅用户画像自身是“处理个人数据的活动”，而且“形成或旨在形成用户画像”的活动亦属于个人数据处理。因此，基于用户画像收集的与自然人相关的数据也构成个人数据，和其他个人数据一并受到法规监管。

  而对于用户画像的使用前提，在 GDPR 中规定应符合以下条件之一：（1）用户画像对于数据主体与数据控制者的合同签订或合同履行是必要的；（2）用户画像是欧盟或成员国的法律所授权的，数据控制者是用户画像的主体，并且已经制定了恰当的措施保证数据主体的权利、自由与正当利益；（3）基于数据主体的明确同意。即使符合上述第（1）种和第（3）种情形，数据控制者也应当采取适当措施保障数据主体的权利、自由与正当利益，以及数据主体对数据控制者进行人工干涉，以便表达其观点和对用户画像进行异议的基本权利。如果使用用户画像对与自然人相关的个人因素进行系统性与全面性的评价，数据控制者应当在处理之前评估计划的处理进程对个人数据保护的影响。

就上述三种使用用户画像的情形，由欧盟或成员国的法律授权使用的情形较为少；而在大数据业务模式中，多数情形下使用用户画像也很难说对于数据主体与数据控制者的合同签订或合同履行是必要的。因此，在绝大多数情形下，需要取得数据主体对使用用户画像的明确同意。对此，GDPR 法规的要求包括：

1. 应当告知数据主体存在用户画像并提供相关逻辑、包括此类处理对于数据主体产生的预期后果的有效信息。

2. 应当明确告知数据主体享有对用户画像的反对权。如果数据主体表示反对，数据控制者须立即停止针对这部分个人数据的处理行为，除非数据控制者能够证明，相比数据主体的利益、权利和自由，具有压倒性的正当理由需要进行处理，或者处理是为了提起、行使或抗辩法律性主张。此外，数据主体有权随时反对为了直接营销目的而处理个人数据，包括反对和直接营销相关的用户画像。

3. 针对特殊类型个人数据，例如性取向、性生活、宗教信仰、政治信仰等敏感数据，除非数据主体明确同意基于一个或多个特定目的而授权处理其个人数据（但成员国可以通过立法明确规定即便数据主体同意，也禁止基于特殊类型个人数据的用户画像），或对数据的处理对实现实质性的公共利益是必要的，并且已经采取了保护数据主体权利、自由与正当利益的措施，用户画像不应基于特殊类型个人数据。

- **大数据分析**

在互联网企业的大数据分析场景下中，用户画像往往只是其中的一个环节。在形成基本画像后，随之而来的是各种个性化推荐，更甚会碰到某些企业采用大数据杀熟 。杀熟一般有三种表现形式：1）根据用户使用的设备不同而差别定价，比如针对苹果系统用户与安卓系统用户制定不同的价格；2）根据用户消费时所处的场所不同而差别定价，比如对距离商场远的用户制定的价格更高；3）三是根据用户消费频率的不同而差别定价，一般来说，消费频率越高的用户对价格承受能力也越强。

在 GDPR 中 7 大数据主体权利中明确定义了反自动化决策权，反自动化决策个人信息处理涉及传统隐私和数据保护问题之深层原因在于社会要求保障人权，在高度强调人文精神的现代社会里，尤其是不歧视、言论自由和信息自由等人权要求。但是自动化决策过度依赖数据，而这些数据可能本身就包含个人或社会成见，形成基于偏见数据所做出的自动化决策，其结果不公平地歧视个人或群体，干扰个人权利，导致人们被排除在社会生活的某个领域之外，使个人无法享受某些服务或福利待遇。

不仅在出海业务中，国内运营场景对于此类监管也愈发严格。我国在 2021 年 11 月 1 日施行的《中华人民共和国个人信息保护法》对大数据杀熟有着明确的规定，要求“个人信息处理者利用个人信息进行自动化决策，应当保证决策的透明度和结果公平、公正，不得对个人在交易价格等交易条件上实行不合理的差别待遇”。

因此，企业在出海需格外注意对于个人信息的分析处理行为，避免杀熟等违规操作。

2.5.4 跨境电商行业

互联网时代下，电商行业快速发展，国内出现了大量的跨境电商平台，形成了多领域复合型综合改革开放态势，未来跨境电商在我国国际贸易中的比重会不断加大，跨境电商服务国家对外开放战略的意义也将会更加明显。

跨境电商经营过程中，常见的经营模式包括入驻电商平台以及通过独立站建站运营。两种模式下，卖方更多基于电商平台或独立站 SaaS 服务作为平台来向海外买家提供服务。在本章节中，将会从两个角度分析卖方与平台分别面临的合规挑战。

平台内置的隐私功能

平台方虽然只是依托于卖方的委托，提供如客服功能、浏览记录功能、广告引流及对接以及甚至代发货功能。但该类会直接接触到买方个人信息的功能服务，需在设计之初就考虑并可满足海外的合规需求，例如获取同意的弹窗、隐私政策预留位置及自定义、用户提出数据主体权利请求的入口等。

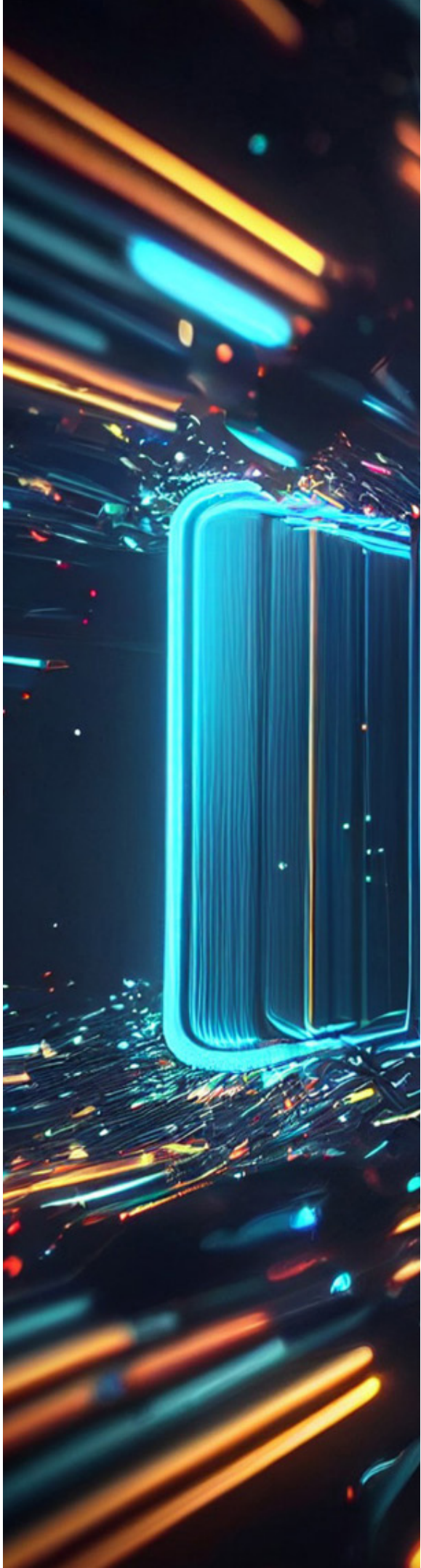
平台安全及数据安全选项

另外以电商平台及独立站 SaaS 服务为代表，数据将托管于该类电商或独立站平台所处的环境内，其整体环境的安全性通常需要电商平台及独立站进行负责。

对于具体的数据处理活动，例如卖方基于品牌管理的需求建立会员库，平台应至少提供该会员库构建过程中可供选择的满足数据保密与安全要求的数据加密方法、数据传输通道以及数据存储位置的选择，甚至进一步的可供选择的数据脱敏方法。同时买家选择数据存储所在国家或区域时，平台也需提醒有可能的数据跨境，并最终由客户确认选择。

数据共享过程的最小范围及安全保障

买家在线上浏览并下单的过程中，涉及到广告投放、支付、物流运输、海外快递派送等与第三方进行交互的环节，才能最终完成交易。在这个过程中，卖方作为数据控制者，需要基于最小化、必要性原则考量需要分享给第三方的个人数据范围，并考量第三方对于此类数据保护的能力，最终签署数据处理的协议以通过书面形式约定责任与义务。



卖方对于数据的使用以及保护职责

卖方仍然是电商运营过程中的最终负责人，卖方需要与平台、第三方明确各自负责的安全与合规范围，如何去确定此类安全与合规的边界成为一个核心挑战。另一方面，卖方需要知悉在跨境电商场景下的数据合规要求，内部制定规范以约束员工的数据处理行为，避免随意下载、共享及发送给外部。同时对于平台内数据安全，卖方应充分了解其需采取的安全保障措施，选择与数据的敏感程度相匹配的加密举措。

2.5.5 智能设备行业

随着智能设备的技术不断发展，智能设备的应用场景和市场规模也在不断扩大。因消费者需求差异，不同品类的智能设备在不同国家地区所面临的竞争环境和监管环境都有差异，企业不仅需要考虑市场机会，也需要慎重应对不同国家和地区的法律法规要求。

智能设备作为终端设备收集并根据信息进行响应，并通过蓝牙、Wifi 等方式与 Web、手机 App 进行交互与数据传输，最终数据将通过 Web 或 App 传输至云平台进行管理。因此除了网络安全法规、隐私保护法规、数据安全法规等通用法规，还需要关注产品安全、无线通讯相关的法律法规，企业根据当地的法规进行适应性调整。

产品及云端安全

出海智能设备企业应全面识别出海目标国家地区针对产品安全的相关安全标准和法律要求，如欧盟颁布的 CE 认证标准，智能设备企业若要将产品在欧洲市场贸易，则必须通过 CE 认证，并在产品上贴上 CE 标签。

智能设备企业重视运用技术的同时也需要注意安全控制和满足合规要求，如欧洲电信标准协会 (ETSI) 针对 IoT 产品推出了 ETSI TS 103 645 和 ETSI EN 303 645 安全标准来保障的合规基础，企业应积极参考并保障产品满足合规基线。

另外，智能穿戴设备以及智能家居 IoT 产品在设计过程的安全性一般不如 App 以及手机等设备的安全性程度，其漏洞的暴露可能使得攻击者以 IoT 产品作为突破口，例如蔓延获取 Wifi 凭据，进一步获取连接到该网络的所有设备的访问权限，抑或是对目标直接发动攻击。

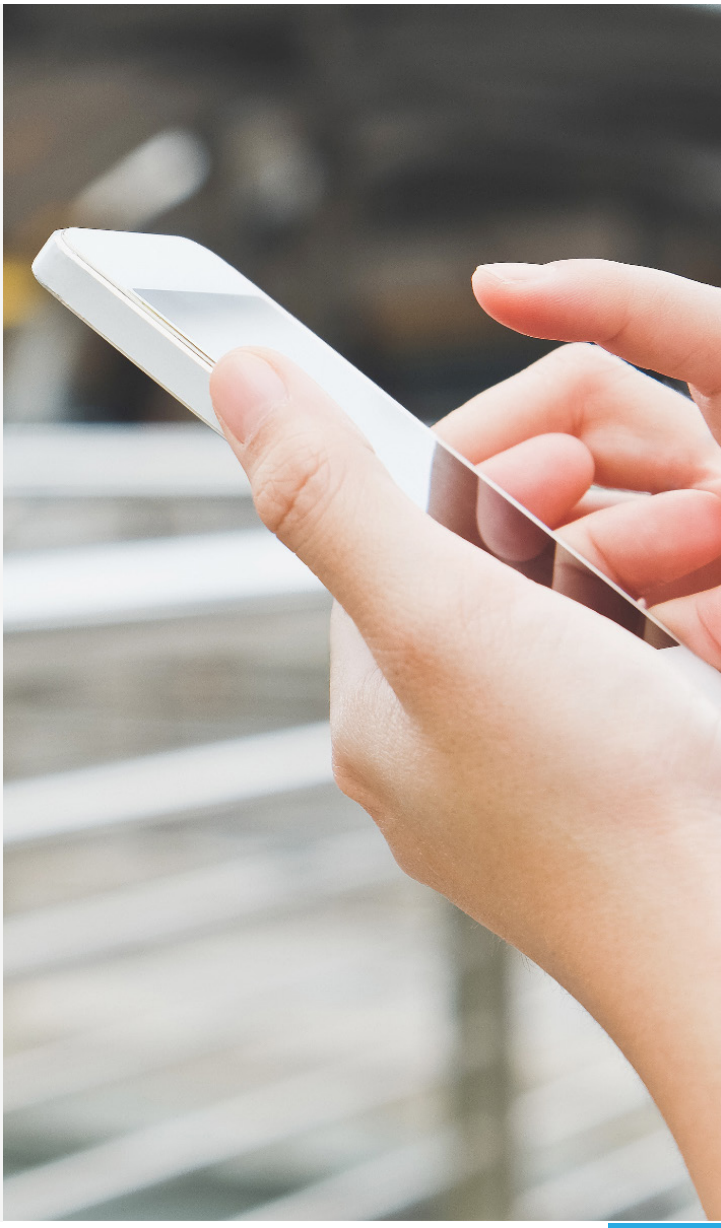
智能穿戴设备的多种功能也依赖于第三方 SDK 实现，在手机或设备端的应用包括地图类、统计类、广告类、短信验证类以及支付类 SDK。在引入 SDK 前，智能设备企业应对于 SDK 的安全性进行测试，检查其是否存在安全漏洞、收集个人信息的范围是否合理、隐私政策告知内容与实际收集、处理机制是否一致等问题，并以书面形式协商双方的责任边界。

由于终端存储的有限性、以及对于云端分析的依赖，云端平台是众多终端设备数据的最终载体，因此云端的防护同样需要智能设备供应商重点关注，尤其是云上的数据库访问权限以及数据库内对数据本身的保护。

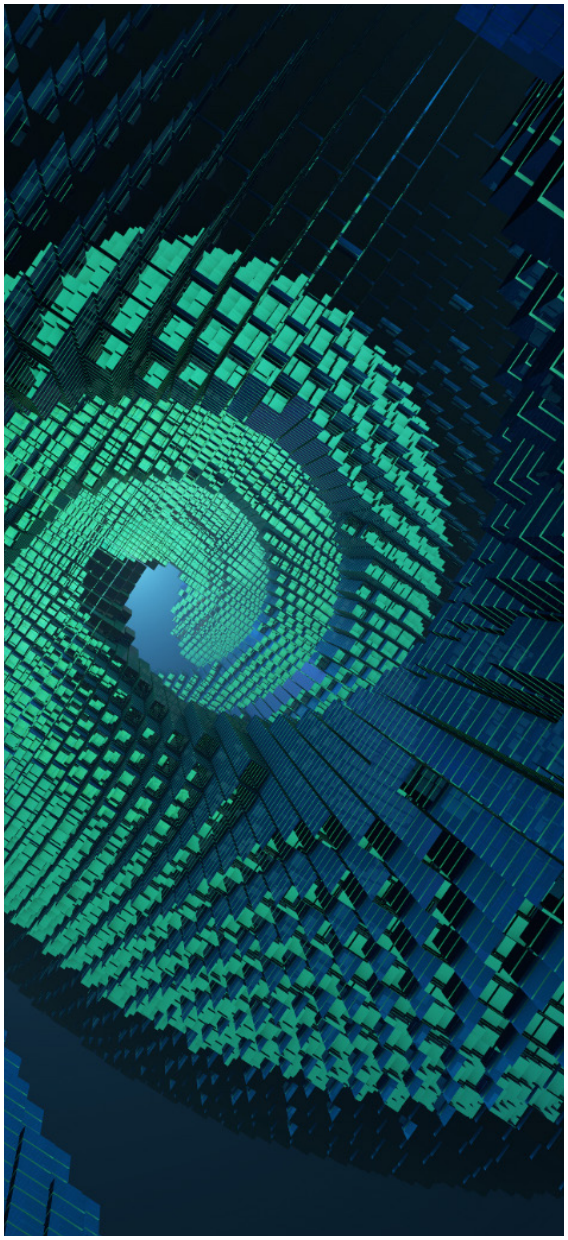
移动通信技术运用的合规

IoT 智能设备需要借助相关通讯技术（Wifi、蓝牙、RFID、MQTT 等）来实现与 APP、平台、用户的交互，在使用这些通讯技术时可能会存在相关隐私泄露的场景，如 IoT 设备的平台和 APP 可能会在业务场景中收集用户 Wifi 信息（ssid、密码、位置等）；智能设备之间通过蓝牙技术、MQTT 协议的交互可能会被监听或者重放；使用射频识别技术 RFID 可能造成的隐私泄露风险等。

故而智能设备企业不仅需要从自身产品的安全性出发，也需要关注以下相关协会或联盟所制定的标准，并充分地实现合规。如欧洲的 ETSI（欧洲电信标准协会）、日本的 ARIB（社团法人电波产业会）和 TTC（情报通信技术委员会）、中国的 CCSA（中国通信标准化协会）、韩国的 TTA（情报通信



技术协会）、北美洲的 ATIS（电信工业解决方案联盟）和印度的 TSDSI（电信标准开发协会）。



海量 IoT 数据收集与传输

智能 IoT 设备安全运行时会随之而产生的海量数据，这些数据可能会直接或者间接的揭示用户的隐私信息，企业需充分考虑是否需要收集处理和储存该设备的运行数据，从而达到满足产品性能的同时也符合监管要求。例如在智能灯光系统及空调远程打开或预约回家时间，体重秤等健康类应用会通过设备、用户输入收集身高、体重、身体状态，甚至是饮食过敏信息。而像手环、手表等穿戴设备，除了监控用户日常的身体状态、运动状态、作息状态外，还有可能记录用户的日常访问位置、接打电话等通讯记录。

收集的数据类型的多样化，需要智能设备提供商梳理其可以收集的信息类型，分析其目的，制定与信息类型匹配的同意获取方式。例如仅在需要的时候获取地理位置信息，并且在第一次接入时告知收集目的并获取同意。

生物数据的收集与识别

智能设备可能会使用到用户的生物信息，如指纹、掌纹、声纹、面部特征等常见生物特征数据，例如指纹锁、人脸解锁、声纹唤醒等场景，在给用户带来便捷的同时，此类生物信息的特征化提取、原始信息的留存成为需关注的重点问题。企业应当特别关注并遵守当地对生物特征信息收集与使用的要求，并谨慎应对生物信息的收集与处理，如制定完善的隐私说明；从业务逻辑出发实现生物信息本地存放；提供更多的可选项等应对措施。

维修及报废处理

同时由于智能设备的互联特性，在维修过程中存在其本地数据的被不当获取、甚至冒用权限的情况。智能设备企业出海后面临着在当地构建售后团队需细化维修人员可接触的数据边界及范围，并且在硬件层面严格遵循销毁标准要求；若通过远程方式进行售后，例如寄回维修，则建议提醒用户提前对数据进行备份，在可开机的情况下删除数据再寄出，规避数据跨境和可能在寄送过程中的数据泄露。同时企业应提供一键清除设备内数据的功能，包括不限于用户信息、使用信息、日志信息，以免在报废或二手买卖过程中的信息泄露。

2.6 出海支持行业的特殊挑战

随着全球贸易回暖，越来越多的中国企业将市场目标扩展向海外，与此同时，也促生了一些为需要出海的企业提供各类服务的企业，如跨境支付提供商、云服务提供商、和智能广告提供商等类型的企业。这些企业可以在相对陌生且复杂的海外环境给需要出海的企业提供专业的解决方案和应对方式，同时自身也面临着来自海外日趋严格的监管约束。

2.6.1 跨境支付提供商

自 2018 年到 2022 年，跨境电商零售进出口额在中国外贸进出口总值的占比逐年上升。即使在新冠疫情的影响下，中国跨境电商进出口额由 2020 年的 1.69 万亿元增长至 2022 年的 2.11 万亿元，总体呈上升趋势。对于现在的跨境支付服务，单纯提供不同地域之间的资金转换已经满足不了现在多变的海外环境。为客户提供海外调研材料，为客户定制专属化的支付收款方式已经成为新的行业特征。除支付行业特有的监管，如欧盟《支付服务指令（修订版）》（Payment Service Directive 2，简称 PSD2）、美国《统一货币服务法》等法律法规之外。同时，跨境支付行业在交易透明度，收付款，数据保护与合规等方面都面临着诸多挑战。

敏感个人数据的处理

跨境收付款的过程中，服务对象不仅仅企业的对公账户，也包含个体工商户或独立开发者在内的个人用户，通常需要收集姓名、身份证件、交易数据以及银行卡等信息以实现收款、入账、客户服务及反洗钱调查等正常运营工作的开展。而身份识别信息和与财产息息相关的数据在中国以及美国加利福尼亚州等国家或地区被认为是敏感个人数据，此类信息泄露对于数据主体即个人的影响较大，更容易造成经济方面的损失。对于这类的数据处理除需要明示或单独同意外，还需要进一步增强对其的安全保护，并对其进行必要的脱敏处理。

目前全球多个金融机构也在探索在交易、支付、结算等过程中引入隐私增强技术，例如基于多方安全计算、联邦学习的反欺诈模型、反洗钱模型等。

另一方面，以支付卡行业安全标准协会（Payment Card Industry，简称 PCI）为代表的行业协会，也发布了多份数据安全标准，如支付卡行业数据安全标准（PCI DSS）和支付应用程序数据安全标准（PA DSS）。企业可根据业务需要，获取相应的安全认证以对外说明自身的安全性。

对共享第三方的管理

跨境支付提供商由于需要提供面向多个国家、不同支付渠道的资金流转渠道，在此过程中无可避免地需提供个人数据至合作的第三方，其中包括金融类服务商，如银联、中国及海外银行、非银支付机构等，以及如 Amazon、Shopee 在内的购物平台。在此过程中，应当与存在数据互通的第三方根据其合作类型签署相应的合同协议，明确双方对于数据处理的角色、责任以及义务，并且在特定场景下，例如第三方作为供应商提供服务时，应当对第三方供应商的安全保障能力进行检查，确保其符合应满足的数据安全及隐私保护要求。

境外调查取证

随着各国对于数字主权的进一步关注和争夺，控制和处理着大量交易数据的跨境支付提供商不可避免地会面临数据主权与海外国家长臂管辖的问题。如美国的云法案（Clarifying Lawful Overseas Use of Data Act，CLOUD Act）就涉及了美国执法过程中对于数据调取的管辖要求。但此可能与我国的《个人信息保护法》第四十一条 “非经中华人民共和国主管机关批准，个人信息处理者不得向外国司法或者执法机构提供存储于中华人民共和国境内的个人信息”存在冲突，因此企业应谨慎处理海外执法机构提出的数据调取请求。

2.6.2 企业级 SaaS 服务提供商

国内企业为非洲、中东等新兴市场提供的计算机与软件服务越来越多，类型也趋于广泛，例如 ERP 类企业资源管理服务、报表管理工具、自动工单及应答系统、协同办公工具、出海支持平台等。此类工具虽然是面向企业发布并不直接面向消费者，但是其工具本身可能承载着大量个人数据，这类服务提供商仍然需要满足相应的合规要求。

产品或服务应包含合规支持功能

面向与企业提供的如 EPR、SAP 等企业管理工具，虽然服务提供商通常作为 GDPR 定义下的数据处理者，但提供服务的产品仍需支持购买产品的企业实现数据安全与隐私保护相关的合规要求，例如提供保留数据处理记录、可选择数据存储所在地区、可实现不同级别的权限管控以及加密策略等功能。

产品数据的触碰边界

企业级 SaaS 服务提供商应当与客户签订的合同协议中明确双方的职责范围以及操作边界，原则上尽量避免运维或客服人员触碰客户的内容数据，即客户环境中的经营数据、收集的个人信息等。

在收到客户请求下进入客户环境进行操作时，建议提前获取客户的书面同意，并全程记录操作过程，并在操作结束后及时关闭或返还操作权限。

如因经营活动必需收集云环境或产品运行数据，例如云资源使用情况、服务可用性指标等记录，应注意其中避免包含客户内容数据。

安全水平证明

部分国家的重点行业会对于外包服务的风险进行管理，通常提供云服务或 SaaS 级企业服务也被视为外包服务的一种。以新加坡为例，新加坡信息通信发展管理局推出了多层云安全认证（Multi-Tier Cloud Security Certification，简称 MTCS），认证共分为三级，包含在数据保留、数据主权、数据可移植性方面的安全要求。部分新加坡的组织或企业，如金融机构，基于政府要求仅可购买符合相应 MTCS 标准的云服务提供商的服务。

2.6.3 智能广告提供商

从 2015 年开始国家推动“大数据战略”以来，大部分企业以数字化转型为目标，推动了广告行业商业模式和范围的扩张。由于新冠疫情的影响，进一步的促进了广告行业向互联网发展的趋势。自 2018 年开始，中国移动互联网广告在总体广告行业份额的占比逐年稳步增长，到 2021 年，中国移动互联网广告份额占比达到 56%。广告行业结合大数据分析和 AI 自主学习的技术是目前的大势所趋，广告商需要通过大数据收集受众的信息和喜好并且根据 AI 进行个性化推送。这个过程会涉及大量的个人数据。基于此，各国针对广告行业的信息收集出台了更加严格的监管，例如欧盟的 GDPR、中国的《中华人民共和国个人信息保护法》和美国的 HIPPA、COPPA 等。此外，广告行业在与投放方的交互中，需要共同计算出最优方案。在这个过程中，双方或者多方需要在不互相泄露敏感数据的情况下共同计算出结果。由此可见，智能广告提供商须在符合中国和相关过法律法规的前提下，才可以为需要出海的企业提供服务。

自动化决策与广告推送

互联网数字广告往往通过搜集个人在网络的浏览数据，形成其数据画像从而进行分析、预测个人偏好，可以高效地精准投放信息以增强商业竞争力。依据 GDPR 等法规，数据主体，即个人应当拥有拒绝信息被用于自动化决策 的权利，包括直接营销相关的特征分析。

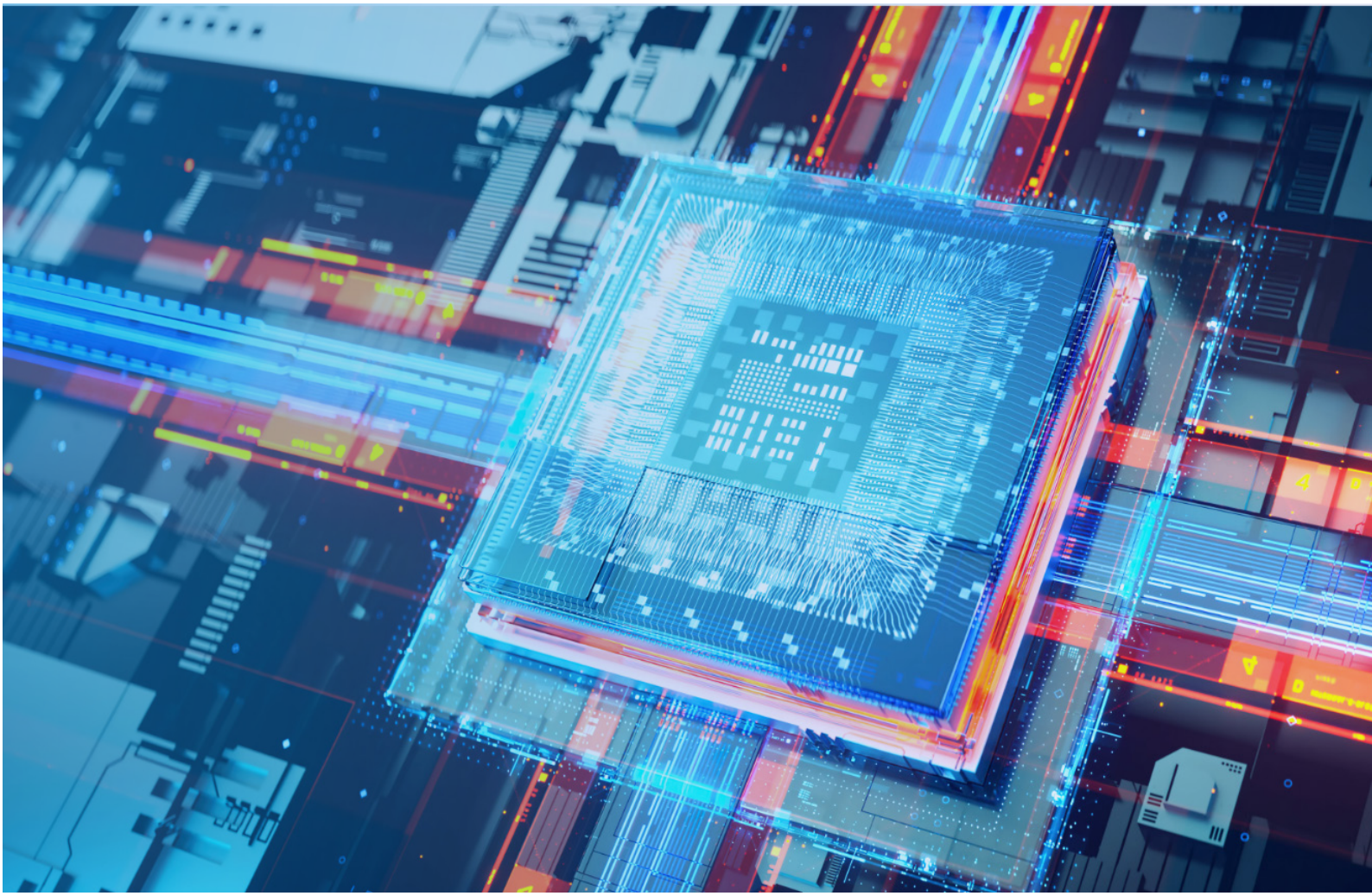
素材合成和使用

近两年深度合成技术一度非常火爆，不少广告企业开始尝试使用深度合成技术生成广告素材，但需注意的是如果合成技术使用到了人脸、人声等生物识别信息，支持生成或编辑该类信息的，需要按照各国对于生物识别信息或敏感个人数据的实际要求，获取该主体的同意。若该类素材的合成在我国境内实现，依据《互联网信息服

务深度合成管理规定》，企业还应进行安全评估并在对外展示区域提示观众或读者此类信息为深度合成。

算法的合规

无论是推荐算法还是素材合成的算法，都应关注国家对于此类技术的规则、输入数据、结果验证、应用范围等内容的规定，例如算法注册、算法规则解释、算法模型运行日志监控、人工介入机制、结果公平验证方法、模型安全性等内容。



3 中国企业出海发展合规应对建议

三 中国企业出海发展合规应对建议

3.1 健全合规管理体系

对于中国企业出海来说，面临的是双向合规的强监管时代，在某些场景下，合规甚至是比业务先行更重要的决定性议题，出海业务需未雨绸缪，从人员意识、管理体系、技术支撑等多方面入手开展合规准备，提前识别并满足适用的网络安全、数据安全和隐私保护相关监管要求，结合企业自身业务特点兼顾所在的行业监管重点，积极拥抱监管要求，主动合规。在深入理解当地法规、文化和经济的基础上，在隐私数据生命周期各阶段中采取相应的数据安全与隐私合规措施，实现数据“可管、可控、可信”，构建合规管理体系，保障为出海业务的长效合规。

3.1.1 计划出海或准备出海

在出海前，企业首先应当对当地法规、当地文化和经济进行充分调研，了解当地的网络安全、数据安全和隐私保护相关监管环境，识别新业务是否受到当地法规的监管，评估当地数据合规要求对业务发展的潜在影响，为业务决策提供支持。

其次，梳理计划出海的新业务和新产品相关的前端及后端隐私数据，开展隐私安全合规自评，充分考虑可能存在的个人数据处理情形，结合业界优秀实践对计划出海新业务和新产品的规划和设计进行针对性调整，以最大程度防范合规风险。如果涉及数据跨境，应当在考虑数据存储位置时结合当地法律对于数据出境的要求提前布局

3.1.2 已在海外有业务

对于已经出海的企业而言，首要需应对来自外部各方的合规挑战，面向监管、最终用户、企业客户 / 合作伙伴 / 供应商等第三方时均有不同的侧重点。

面向监管侧的合规

公开数据保护负责人：

对于重点目标市场在欧盟、泰国、新加坡的企业，应当通过隐私声明等容易被外界获取的渠道公示企业数据保护负责人以便公众或被处理信息的个人可通过该渠道进行联络，在欧盟和泰国还应将数据保护负责人及其联系方式告知监管机构；

数据泄露事件报告：

一旦出海企业意识到发生个人数据泄露或重大的数据安全事件，应当由数据保护负责人按照事件涉及国家或区域所在地的适用法规要求，在指定时间内将事件情况通报监管机构；

数据处理活动登记：

在英国、马来西亚及尼日利亚，企业在达到指定条件后还应当就其数据处理活动向当地数据保护监管机构进行登记说明；

透明性与独立第三方审查:

对于复杂的大型数字平台或者参数上亿的人工智能算法，还应当提前对于披露必要的规则、内部开展的技术与管理手段进行整理和准备，以便在对外披露或引入第三方就自身合规情况进行审查之前，做到“心中有数”。

面向企业客户 / 用户侧的合规

应当分析在不同业务场景下出海企业自身的角色，明确处于不同角色时需要承担的隐私合规义务。

直接面向最终用户提供服务：

该场景下大多数情况下企业作为数据控制者角色，应当重点关注隐私政策及相关协议合规、告知用户以及同意获取的合规、用户数据主体权利响应渠道打通、数据泄露事件应急响应等合规事宜；

面向 B 端客户提供服务：

该场景下通常企业作为数据处理者角色，则应当重点关注与数据控制者的合同协议是否涵盖充分的数据合规相关条款，根据需要配合数据控制者响应数据主体权利请求，并在发生个人数据泄露事件时及时通知数据控制者。

面向合作伙伴 / 供应商的合规

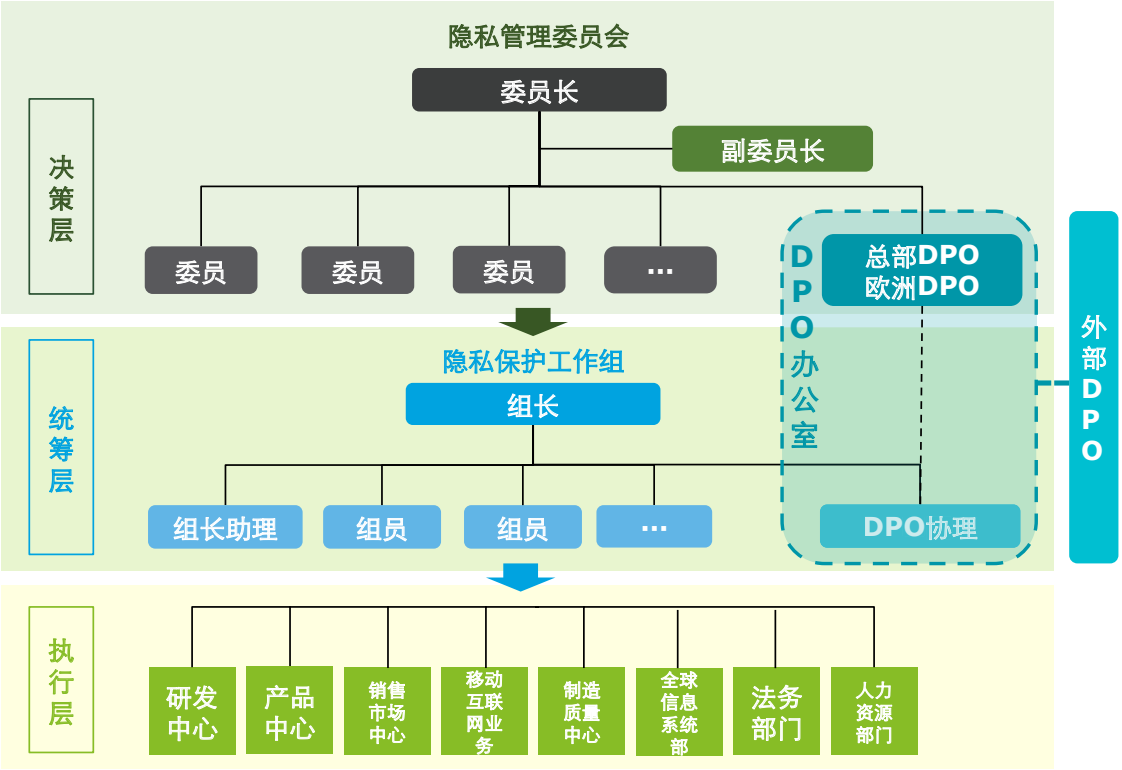
出海企业在选择第三方合作伙伴、供应商时，应当提前考虑对于数据合规能力的考量，并在合同协议中提出满足数据合规的要求。

在解决外部合规问题的基础上，企业还应当进行“内功”的修炼，持续建设和提升内部隐私合规能力。

构建隐私合规组织

对于重点目标市场在欧盟的企业，应当设立数据保护负责人角色，建议在欧盟选择一个能够涵盖欧盟大多数国家且监管力度适当的国家设立 GDPR 要求下的数据保护官（Data Protection Officer，简称 DPO），该数据保护官可由企业内部具有数据保护法律与实践的专业知识、了解公司业务活动和组织架构、能够保证较充分的独立性并且可以直接向企业最高管理层报告的人员担任，也可由外部专业人士担任；而对于出海业务横跨多个市场，在欧洲、北美，南美，中东，东南亚各市场都可能存在业务运转的跨国企业，则建议按照相对严格的区域法规要求设立隐私保护组织并任命全球首席数据保护官，然后在必要的地区分别设立本地数据保护官。

除数据保护负责人以外，为实现管理体系在公司的有效运作与维护，还需建立覆盖面广且强有力的合规管理组织架构。结合德勤实践经验，建议合规管理组织由决策层、统筹层、执行层三个层级构成，所有相关的业务部门和组织均需参与该管理组织，包括但不限于公司的高级管理层、法务、合规、质量体系管理、产品与研发、销售与市场人员、IT、HR 等，示例如下图。



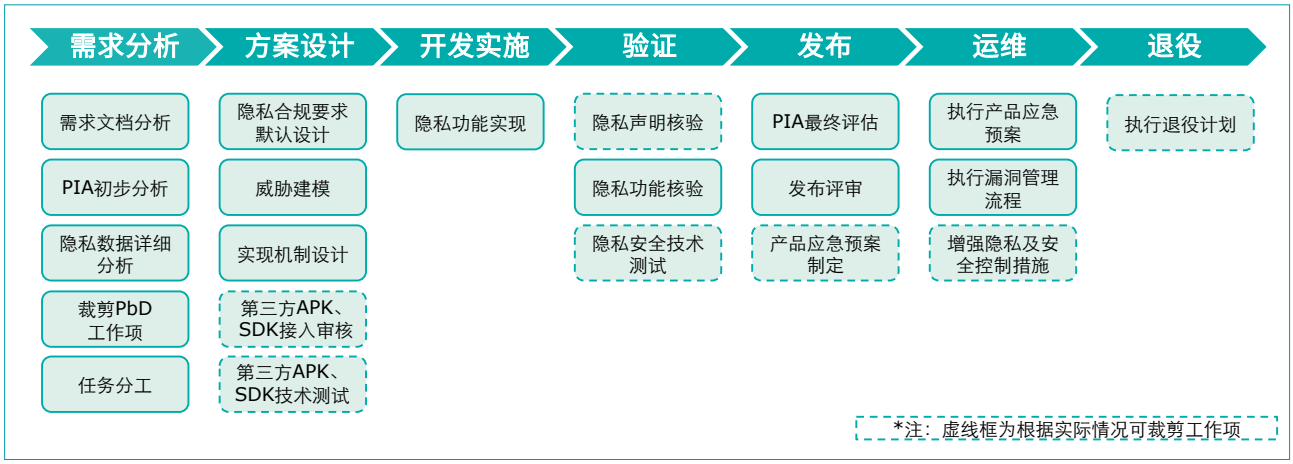
- 决策层：战略决策。负责制定企业合规战略目标、进行重大事项的最高决策，并推动战略与政策的落地。
- 统筹层：统筹管理。负责制定企业合规管理的制度与工作方案，统筹各部门合规需求与活动，并开展合规方面的沟通与咨询。
- 执行层：工作执行。负责执行与配合具体的合规任务，跟进职责范围内的合规问题与风险。

产品 / 服务 / 解决方案合规

对于面向海外市场提供的产品或解决方案，建议重点考虑以下三个方面的合规准备。

- **数据梳理：**出海企业相关主导人员应当组织出海产品 / 服务 / 解决方案相关的前端及后端负责人，理清隐私数据及其全生命周期合规管控现状
- **合规风险评估及整改：**产品部门协同法务、研发、运维等开展数据保护影响评估，重点考虑是否满足数据处理的范围最小化、目的合法正当、第三方数据合规、数据跨境和数据本地化相关风险、以及贯穿数据生命周期的技术保护，识别为消减此类风险需采取的技术和组织措施，并结合企业实际情况制定整改计划和推行整改落地。其中可采取的技术措施包括不限于个人数据的匿名化和加密、对数据处理系统或服务的安全保障、数据备份及恢复等。

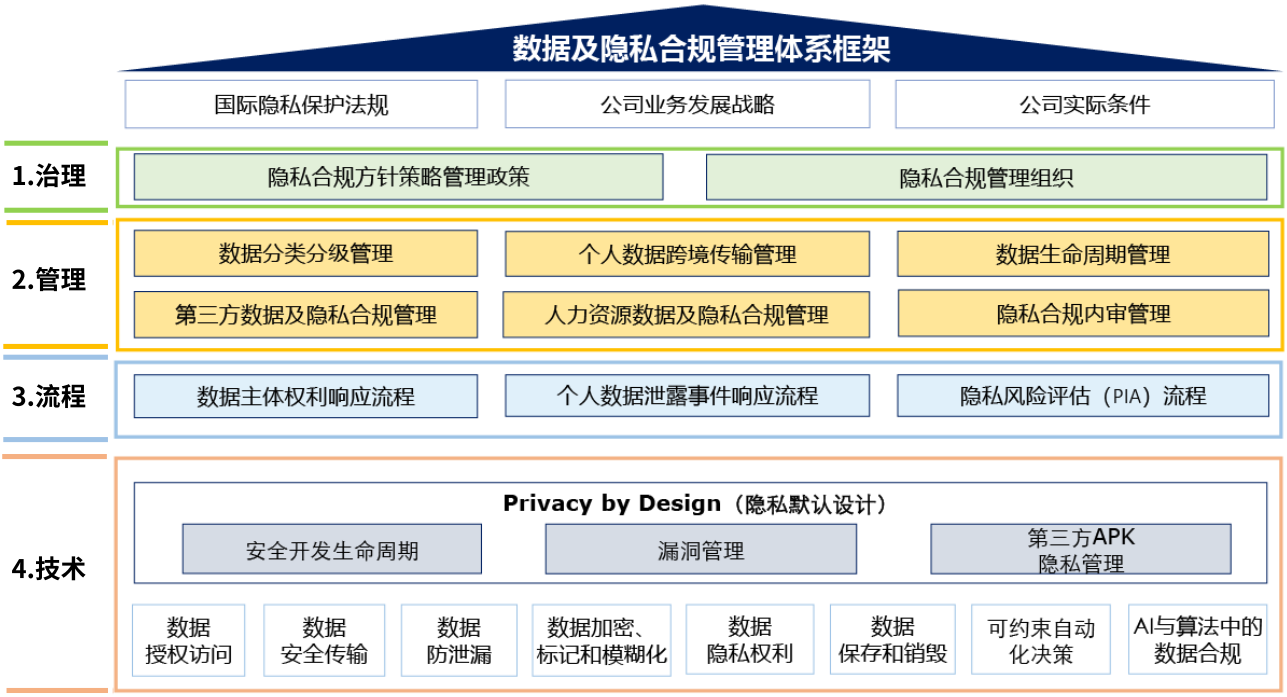
- **隐私默认设计（PbD）：**结合现有产品的研发流程，设计 PbD 流程，将隐私安全要求融入开发全过程，持续保障产品 / 服务 / 解决方案的合规，开发生命周期各阶段明确应采取的隐私管理活动如下图所示。



建立合规管理体系和流程制度

管理制度的完善有利于推进企业执行层面人员了解应满足的合规要求、自身所应承担的责任以及所需采取的行动，提供落地实践的原则性指导。出海企业应当融合业务所涉及主要国家和地区的监管要求，结合企业未来发展需求、行业最佳实践、以及管理层的合规期望，总体规划合规体系框架，搭建和不断完善合规管理体系，整体提升数据安全与隐私保护水平。

依据国际知名标准组织对此类管理体系的要求，结合德勤实践经验，建议企业以确立相关高阶合规政策、构筑合规组织架构、建立相关规范与流程、融入隐私安全技术为导向，建立从管理层面到技术细节的四层管理机制，由上至下的将合规思想渗透到整个管理体系框架，帮助管理和执行人员有法可依、有路可行，形成标准化、流程化的内部管理机制，指导企业合规工作的持续有效开展。我们结合业界实践设计了以下合规管理体系基础框架，出海企业可根据实际情况进行定制。



- **第一层：企业层面的原则、方针及政策，**包括企业整体的总体合规管理方针策略为公司合规管理工作提供基本原则和方向、明确合规管理工作领域与任务范围，合规组织架构及职责说明以明确管理体系中各项活动的权责，确保每项任务的管理、推进和有效实施；

- **第二层：企业层面的管理规范，**包括数据分类分级制度、数据生命周期管理规范、数据跨境传输规范、第三方数据及隐私合规管理规范、人力资源数据及隐私合规管理规范等；

- **第三层：业务层面的流程指引和操作指南，**包括隐私风险评估 (PIA) 流程、数据泄露事件报告及处理流程、数据主体权利响应流程等；

- **第四层：技术层面的支撑，**通过 Privacy by Design（隐私默认设计）流程将隐私及安全的考虑嵌入到业务流程、IT 系统、产品研发中，将相关管控措施作为产品的默认配置。

体系运转与合规审计

合规管理体系在全公司的有效运转，需要在合规管理组织的带领下，通过下图所示从计划、实施推进、监督审计全面推进合规体系运转。

- **制定和推行合规工作计划：**合规职能应每年制定下年全公司的合规工作计划，询问 DPO 办公室的建议，并在通过合规管理委员会审批后，在全公司推行工作计划，并每月至少与执行层进行一次工作计划实施进度的全面沟通。
- 定期开展**意识宣贯培训，**建设全公司的隐私保护文化，并提升员工隐私保护意识；
- 定期召开**合规管理工作会议，**例如每年至少召开一次合规管理组织决策层会议，进行年度重大事项决议；每半年至少召开一次合规管理工作会议，跟进合规整体工作情况；在数据泄露等紧急事项发生时，及时召开临时工作会议。
- 定期开展**自查与监督，**例如每年展开一次体系工作评估，了解体系运转效率、管控效果、执行情况，同时对管理体系也进行检查，在外部监管环境、内部管理机制变动时及时对管理体系进行更新，实现体系的持续改善；基于监管需要、企业数据保护负责人提出的建议、客户的要求等，结合实际工作需求和情况，由企业内部审计部门或邀请外部第三方机构，开展合规管理专项评估或审计，定期对自身的合规情况进行识别与评估。

合规能力对外展示

- **获取合规认证：**随着企业出海的足迹不断扩展，企业会越来越多地收到来自不同市场的客户对于企业合规能力的期望，根据出海业务常见目标国家的合规发展情况，结合德勤在安全合规领域的服务经验，我们建议出海企业可考虑以下认证，彰显企业的合规遵从性，从而获得现有客户的更高认可。
    - **针对组织的认证：**ISO 27001 信息安全管理体系认证，ISO 27701 隐私管理体系认证，ISO22301 业务连续性管理认证等
    - **针对行业的认证：**PCI-DSS 支付卡行业数据安全标准认证，CSMS 车辆网络安全管理体系认证和 VTA 车型认证等
    - **针对产品的认证：**ePrivacyseal EU 认证，ePrivacyseal Global 认证，EuroPriSe 认证等
- **发布合规白皮书：**出海企业还可通过白皮书向客户传递企业在合规方面所做的工作，让客户更加便捷的了解企业对业务目标国家法律法规、行业标准的遵从以及高度的合规性，增强市场潜在客户对选择和使用企业出海产品 / 解决方案 / 服务的信心。

出海企业要实现业务长效合规发展，不仅需要通过本章节包含的在企业管理层面的各项准备工作搭建起来整体的合规体系，技术层面的合规也非常重要。我们将在下一章节详述技术平台的合规，并在 3.3 章节通过德勤与亚马逊云科技合作的典型成功案例来详细讲解出海合规的应对实践

3.2 技术平台

亚马逊云科技（Amazon Web Services）是全球云计算的开创者和引领者，自 2006 年以来一直以不断创新、技术领先、服务丰富、应用广泛而享誉业界。亚马逊云科技可以支持几乎云上任意工作负载。亚马逊云科技目前提供超过 200 项全功能的服务，涵盖计算、存储、网络、数据库、数据分析、机器人、机器学习与人工智能、物联网、移动、安全、混合云、虚拟现实与增强现实、媒体，以及应用开发、部署与管理等方面；基础设施遍及 32 个地理区域的 102 个可用区，并计划新建 4 个区域和 12 个可用区。全球数百万客户，从初创企业、中小企业，到大型企业和政府机构都信赖亚马逊云科技，通过亚马逊云科技的服务强化其基础设施，提高敏捷性，降低成本，加快创新，提升竞争力，实现业务成长和成功。

亚马逊云科技在中国的愿景是，作为全球云计算的开创者和引领者，利用与生俱来的创新文化，赋能客户的重塑，加速客户全球业务拓展，加强本地人才培养，从而促进行业转型，助力数字经济的可持续发展，并让全社会共同受益。

安全是亚马逊云科技最高优先级的工作，“引领行业的安全合规理念和实践”是亚马逊云科技服务全球数百万客户的五大全球优势之一。亚马逊云科技秉承安全责任共担模型，既保证其全球底层云基础设施和服务的安全合规，让客户可以直接继承，又为客户提供“洋葱型”的多层次安全防护，帮助客户提升云上应用的安全合规。

类别	亚马逊云科技提供的相关产品与服务
计算	Amazon EC2、Amazon EC2 Container Services、Amazon Elastic Beanstalk、Amazon Lambda、Auto Scaling
存储	Amazon S3、Amazon CloudFront、Amazon EBS、Amazon EFS、Amazon Glacier、Amazon Storage Gateway、Amazon Snowball
数据库	Amazon RDS、Amazon DynamoDB、Amazon ElastiCache、Amazon Redshift
网络	Amazon VPC、Amazon Direct Connect、Amazon Elastic Load Balancing、 Amazon Route 53、Amazon Network Firewall
开发人员工具	Amazon CodeCommit、Amazon CodePipeline、Amazon CodeDeploy、Amazon Web Services SDK
管理工具	Amazon CloudWatch、Amazon CloudFormation、Amazon CloudTrail、Amazon Config、Amazon Web Services Management Console、Amazon OpsWorks、Amazon Service Catalog、Amazon Trusted Advisor、Amazon Tools for Windows PowerShell
安全和身份	Amazon Identity & Access Management、Amazon Directory Service、 Amazon GuardDuty、 Amazon Inspector、Amazon CloudHSM、Amazon KMS、Amazon WAF、 Amazon Audit Manager
分析	Amazon EMR、Amazon Data Pipeline、 Amazon Elastisearch Service、Amazon Kinesis、Amazon Kinesis Firehose、Amazon Machine Learning、Amazon QuickSight
移动及物联网 (IoT)	Amazon IoT、Amazon Mobile Hub、Amazon API Gateway、Amazon Cognito、Amazon Device Farm、Amazon Mobile Analytics、Amazon Mobile SDK、Amazon SNS
应用程序服务	Amazon API Gateway、Amazon AppStream、 Amazon CloudSearch、Amazon Elastic Transcoder、Amazon FPS、Amazon SES、AmazonSNS、Amazon SQS、Amazon SWF
企业生产力应用程序	Amazon WorkSpaces、Amazon WAM、Amazon WorkDocs、Amazon WorkMail

3.2.1 安全责任共担模型

亚马逊云科技首创 “安全责任共担模型”， 亚马逊云科技负责云自身的安全，客户负责云中自身业务的安全，亚马逊云科技通过提供多层次的安全防护服务帮助客户提升云中的安全防护。亚马逊云科技“安全责任共担模型”不仅使客户能够继承亚马逊云科技全面的安全性，降低客户管理、运营底层基础设施的复杂性并节省了成本。

- 亚马逊云科技负责云自身安全，包括其底层云基础设施和云服务，让客户继承亚马逊云科技全面的安全性，在安全的云环境中开展业务。亚马逊云科技负责运行、管理和控制从主机操作系统和虚拟层到服务运营所在设施的物理设备以及提供的云服务的安全。

- 客户负责云中自身业务的安全，包括选用哪个区域、使用哪种服务、访问控制的授权、安全防护的手段等。客户的安全责任在使用亚马逊云科技不同服务时会有所不同。例如，客户使用 Amazon Elastic Compute Cloud (Amazon EC2) 服务，客户需要负责操作系统（包括更新和安全补丁）的管理、客户在实例上安装的任何应用程序软件或实用工具，以及每个实例上配置亚马逊云科技提供的防火墙（称为安全组）的配置。客户使用如 Amazon S3 和 Amazon DynamoDB，由亚马逊云科技运营基础设施层、操作系统和平台，而客户通过访问终端节点存储和检索数据，客户负责管理其数据（包括加密选项），对其资产进行分类，以及使用 IAM 工具分配适当的权限。

3.2.2 亚马逊云科技云上的隐私保护

亚马逊云科技始终坚持客户拥有和控制数据的理念，并以隐私和数据安全最高标准构建基础设施和服务，确保客户数据安全，同时为客户提供所需的控制权、可见性以及安全保护。

- 亚马逊云科技严格遵从客户拥有和控制数据的理念，不会未经客户同意访问或使用其数据。亚马逊云科技的客户对自己的数据拥有完整控制权，可以自主选择数据的存储位置，包括存储类型和存储区域，可以控制访问数据的权限，并自由选择任何方式对数据进行加密、移动以及管理。
- 亚马逊云科技以数据隐私和安全最高标准构建基础设施及服务。亚马逊云科技提供网络安全技术、物理访问控制以及人员管理来防止未经授权的访问，所有流经连接亚马逊云科技基础设施和区域互连的全球网络的数据在离开安全设施之前，均在物理层自动加密。
- 亚马逊云科技提供客户所需的控制权、可见性和安全保护。亚马逊云科技细粒度的身份和访问控制，可确保客户无论数据存储何处，都能始终让正确的资源拥有正确的权限。亚马逊云科技还提供了加密、删除和监控数据处理的功能，其中加密服务涵盖了数据的存储、传输以及使用各个环节数据全生命周期；亚马逊云科技安全自动化和安全事件监控服务可帮助客户检测整个系统中的可疑安全事件（例如配置更改），从而在扩展时降低风险。使用亚马逊云服务的客户可以保持对其数据的控制，并根据其特定需求实施额外的安全措施，包括内容分类、加密、访问管理和安全凭据。

赢取客户信任是亚马逊云科技开展业务的基础。亚马逊云科技致力于满足客户的隐私需求，并以公开透明的态度对待隐私承诺，从而赢得信任。亚马逊云科技行业领先的隐私保护和安全控制体系使客户能够自信地开展运营，助力客户在全球范围内实现并超越隐私与合规性要求。客户可以根据特定行业要求实施隐私保护，并使用亚马逊云科技的服务、工具和资源来控制和保护数据，以满足监管机构和审计人员的要求。

针对出海客户，全球各地的隐私保护纷繁复杂，亚马逊云科技为 190 多个国家 / 地区的数百万个活动客户提供服务，包括企业、教育机构和政府机构。亚马逊云科技的客户包括金融服务提供商、医疗保健提供商和政府机构，他们将一些最敏感的信息托付在亚马逊云科技云上，给予我们充分的信任。 由此我们积累了丰富的全球隐私保护的经验和知识。亚马逊云科技隐私保护页面上提供了全球各地主要的隐私保护洞见。

- https://aws.amazon.com/cn/compliance/data-privacy/

美洲：

- 关于某些健康信息共享的法案 – 魁北克省
- 阿根廷数据隐私法
- 巴西数据隐私法
- 加利福尼亚州消费者隐私法案 (CCPA)
- FERPA
- 信息自由和隐私保护法案 (FOIPPA) – 不列颠哥伦比亚省
- 健康信息法案 (HIA) – 亚伯达省
- 个人健康信息保护法 (NL PHIA) – 纽芬兰与拉布拉多省
- 个人健康信息法案 (PHIA) – 新斯科舍省
- 个人健康信息隐私和访问法案 (NB PHIPAA) – 新不伦瑞克省
- 个人健康资讯保护法案 (PHIPA) – 安大略省
- 个人信息保护及电子文档法案 (PIPEDA) – 加拿大

亚太地区：

- 澳大利亚数据隐私法
- 日本数据隐私法
- 菲律宾数据隐私法
- 中国香港数据隐私法
- 韩国数据隐私法
- 新加坡数据隐私法
- 印度数据隐私法
- 马来西亚数据隐私法
- 中国台湾数据隐私法
- 印度尼西亚数据隐私法
- 新西兰数据隐私法
- 泰国数据隐私法

欧洲，中东和非洲

- 欧洲云基础设施服务提供商联盟 (CISPE)
- 通用数据保护条例 (GDPR)
- 南非数据隐私法
- 欧盟 – 美国隐私护盾

3.2.3 亚马逊云科技的合规计划

亚马逊云科技支持众多安全标准与合规性认证，几乎满足全球所有监管机构的合规性要求，客户可全面继承。

- 亚马逊云科技云自身的安全合规。亚马逊云科技致力于在全球业务范围内建立严格的安全性和合规性标准，在其基础设施覆盖区域支持众多安全标准并获得多项合规认证。亚马逊云科技目前获得了 98 项安全标准与合规认证。这些认证和资格鉴定也印证了亚马逊云科技行业领先的安全合规能力，例如，技术措施方面的 ISO 27001、云安全性方面的 ISO 27017、云隐私方面的 ISO 27018、SOC 1、SOC 2 及 SOC 3、PCI DSS 1 级，以及 Common Cloud Computing Controls Catalogue（C5）等面向欧洲地区的认证。这些技术和组织安全措施由独立的第三方评估机构验证，旨在防止未经授权访问或泄露客户内容。例如，ISO 27018 是首个面向云中个人数据保护的国际行为准则。它基于 ISO 信息安全标准 27002，并针对 ISO 27002 控制体系提供了实施指南，适用于由公有云服务提供商处理的个人可识别信息 (PII)。亚马逊云科技集成了风险管理和合规机制，采用包括广泛使用自动化工具、独立风险评估、定期接受独立的第三方审计等多种措施，确保亚马逊云科

技运营的有效性和严格遵守合规制度。

- 亚马逊云科技定期对数千个全球合规性要求进行第三方验证，并持续监控这些要求，帮助客户满足财务、零售、医疗保健、政府及其他方面的安全性与合规性标准。亚马逊云科技支持包括 PCI-DSS、HIPAA/HITECH、FedRAMP、GDPR、FIPS 140-2 和 NIST 800-171 在内的安全标准和合规性认证，几乎满足全球所有监管机构的合规性要求。

- 亚马逊云科技确保每个服务的合规性，基于预期使用案例、反馈和需求将正式发布的各项服务纳入合规性工作范围内，并对每个服务都做了合规性验证。以 Amazon Aurora 为例，作为亚马逊云科技合规性计划的一部分，第三方审计员将评估 Amazon Aurora 的安全性和合规性，包括 SOC、PCI、FedRAMP、HIPAA 等。

- 客户可继承亚马逊云科技全球基础设施覆盖区域的各地安全合规认证，以及亚马逊云科技在其基础架构上使用的最新安全控制措施。这些控制措施可加强客户自己的合规性和认证计划，同时还可以访问可用于降低运行自己的特定安全保障要求的成本和时间的工具。

亚马逊云科技中国大陆区域的合规性

- 亚马逊云科技中国（宁夏）区域和亚马逊云科技中国（北京）区域严格按照中国法律法规的监管要求依法合规经营。亚马逊云科技向西云数据和光环新网提供行业领先的技术、指导和专业知识，西云数据和光环新网运营并向本地客户提供亚马逊云科技云服务。

- 中国大陆的两个区域所提供的云服务与其它亚马逊云科技区域所提供的云服务相同，但是又与所有其它亚马逊云科技区域隔离，客户可以完全控制数据实际所在的区域，从而满足数据驻留要求。

- 亚马逊云科技中国（北京）区域和亚马逊云科技中国（宁夏）区域通过独立的第三方机构验证其标准符合能力，已经完成了网络安全等级保护三级测评（等保三级是授予公有云服务最高级别，阿里云、腾讯云、华为云等宣布获得的等保四级认证，是针对其私有云的），还获得了中国信息通信研究院可信云服务评估，以及在国内也通行的 ISO9001 质量管理体系认证、ISO20000 信息技术服务体系认证、ISO27001 信息安全管理体系认证、ISO27018 云隐私安全管理认证、ISO22301 业务连续性管理认证、PCI-DSS 支付卡行业数据安全标准认证、SOC 认证。

3.2.4 亚马逊云科技云上的安全

亚马逊云科技为客户提供全方位的安全服务，目前有 300 多项安全、合规服务及功能，涵盖威胁检测和事件响应、身份认证和访问控制、网络和基础设施安全、数据保护与隐私以及风险管控及合规五大领域。

- **威胁检测与事件响应：**检测是安全生命周期的重要组成部分，可用于支持安全流程、法律符合或合规义务，还可以用于威胁识别和响应工作。客户使用检测服务和功能，可以识别潜在安全配置错误、威胁或意外行为。重点服务：威胁检测服务 Amazon GuardDuty 可持续监测恶意活动和未经授权的行为，该服务具有丰富的情报源并集成了机器学习的能力，可实现威胁的精准定位，并对安全事件进行快速反应；Amazon Security Hub 安全事件统一管理平台为客户提供了统一的安全事件视图，并可根据不同的标准和最佳实践持续对客户的云环境进行合规性检查，快速发现技术差异并提供修复方案。

- **身份认证与访问控制：**亚马逊云科技为客户提供强大的身份管理和权限管理，确保适当的人员在适当的条件下有权访问适当的资源。亚马逊云科技提供了大量帮助客户管理客户身份及其权限的服务及功能，客户可以根据业务的需要，进行最小化的授权并且对授权策略进行审核，以确保访问策略的安全性。重点服务：Amazon Identity and Access Management 以细颗粒度的身份认证与访问控制机制，结合对安全事件的持续监控和精准的安全权限设置，保障正确资源被相应正确人员访问。

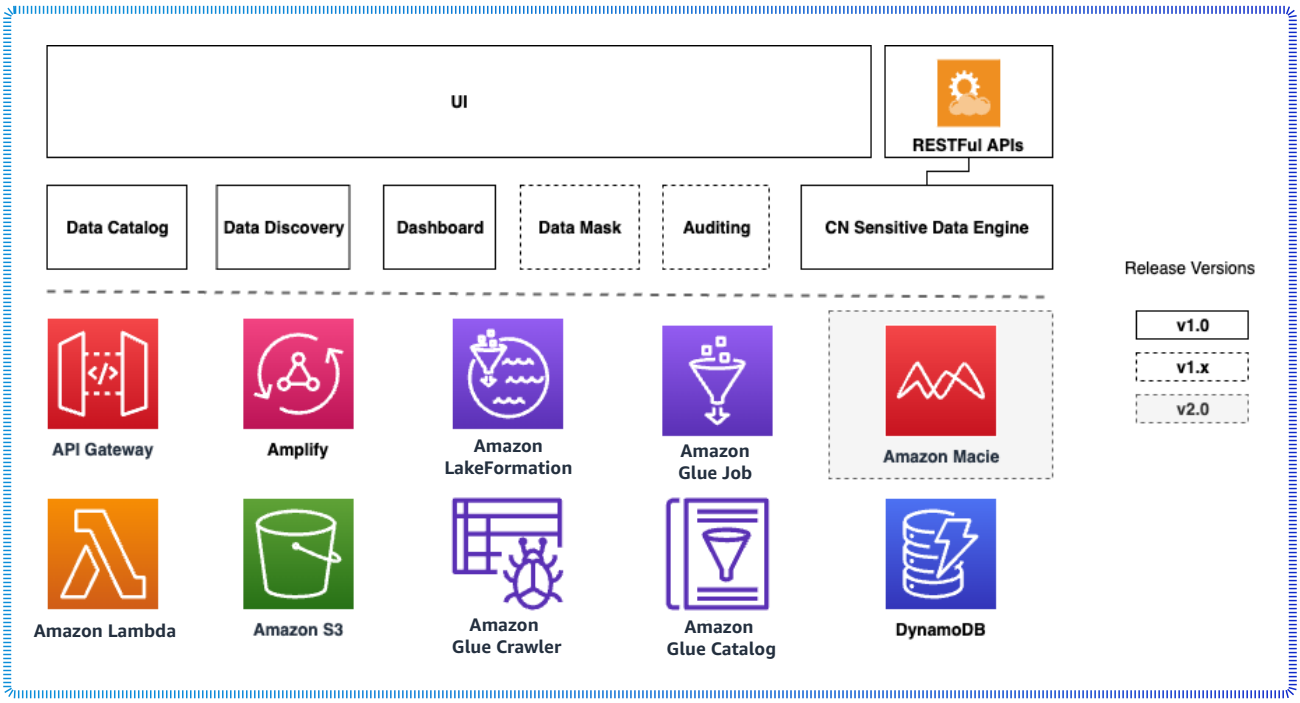
- **网络与基础设施安全：**亚马逊云科技在主机、网络和应用程序级别边界为客户提供细粒度的保护。 其中，Amazon VPC 安全组在主机级别为亚马逊云科技工作负载中的资源提供保护。在网络级别，Amazon Network Firewall 允许客户通过状态检查、入侵防护和 Web 过滤等功能严格控制进出 VPC 和 VPC 之间的流量。对于 Web 应用程序保护，Amazon Web Application Firewall 等服务允许客户过滤 Web 请求的与规则不匹配部分，以阻止常见的攻击模式。Amazon Shield 可以保护客户的网络和应用程序免受恶意的 DDoS 攻击，并提供托管检测和响应以抵御有针对性的攻击。客户还能通过与 Amazon Firewall Manager 的集成，实现对不同账号的网络安全防护实施统

一的策略。

- **数据保护与隐私：**亚马逊云科技数据保护服务提供加密、密钥管理和威胁检测功能，可以持续保护客户数据、监控和保护客户的账户和工作负载。亚马逊云科技使用很多不同的方法实施数据保护。其中，自动识别和分类数据可以帮助客户快速地根据合规的需要，发现并定位包括个人数据在内的敏感数据。Amazon Macie 使用机器学习技术来自动发现和保护客户的敏感数据并对其分类，可以识别个人可识别信息 (PII) 或知识产权之类的敏感数据，并为客户提供控制面板和警报，让客户了解此类数据的访问或移动方式。Amazon Key Management Service (Amazon KMS) 为客户提供数据加密，该服务深度集成于亚马逊云科技的 140 多项服务中，可帮助客户大幅减少人工操作，降低出错概率。对于数据保密要求更高的客户，还可使用 Amazon CloudHSM 来获得云上专属加密机服务。在数据计算过程中，客户可使用 Amazon Nitro Enclaves 的云端机密计算的技术，创建严密隔离的环境处理敏感数据。

- **风险管控及合规：**亚马逊云科技可帮助客户全面了解合规状况，并使用自动合规性检查，持续监控客户的环境。例如，Amazon Artifact 自助门户，允许客户按需访问并免费获取亚马逊云科技的合规性报告。为避免客户在合规审计与评估中消耗过多成本，亚马逊云科技提供 Amazon Audit Manager，可自动扫描、搜集证据，还提供了各种合规认证的模板，简化合规审计的证据收集工作，实现高效的自动化合规审计与评估。

亚马逊云科技云原生敏感数据识别解决方案是**亚马逊云科技根据中国客户的需求，以及最新的合规要求，专门研发的解决方案。**客户可以同时管理多个账号内的资源，自动构建资产目录，并且定期扫描数据源中的敏感数据。



客户可以使用这个方案快速发现云环境中的敏感数据，目前已经支持了 200 多种敏感数据类型，客户还可以根据需要自定义敏感数据。发现敏感数据后，可以对数据进行自定义分类分级，再根据分类分级的结果选取合适的保护措施。

此方案可以数据治理地图的形式展示企业内部的数据状况，如下图。

亚马逊云科技通过安全合规相关的在线工具、资源和支持，为客户提供指导和专业知识分享。

- **多种在线工具：** 如 Amazon Trusted Advisor 在线工具就像一个定制的云计算专家，让客户配置资源时遵循最佳实践。Amazon Security Bulletins 围绕当前的漏洞和威胁提供安全公告，使客户能够携手亚马逊云科技的安全专家，应对云资源滥用、漏洞和渗透测试等安全关切。

- **自动化工具，简化客户评估风险及合规：** 如 Amazon Audit Manager 提供映射亚马逊云科技资源到控制要求的预构建框架，控制要求会根据行业标准或法规要求进行分组，例如 CIS 基准、GDPR 或 PCI DSS。Amazon Audit Manager 通过自动收集和整理由每个控制要求定义的证据为客户节省时间。

- **资源，如云安全白皮书：** 描述了如何利用云技术来保护数据、系统和资产，以提升安全水平，提供了有关在亚马逊云科技云上构建工作负载的最佳安全实践指导；一系列的合规资源，例如如何在亚马逊云科技上构建符合 PCI-DSS 的应用，亚马逊云科技云中的 DoD 合规性实施，亚马逊云科技上的 GxP 系统等等。

- **亚马逊云科技客户团队支持：** 指导客户完成部署和实施，为客户寻找合适的资源来解决客户可能遇到的安全问题；并开设了安全合规的社区，为客户提供各类安全合规解答。

亚马逊云科技合作伙伴网络 (APN) 提供数百种行业领先的安全及合规解决方案，多层保护客户的应用和数据安全。

- 客户可以使用他们已经了解和熟悉的解决方案，选择信赖的安全技术和咨询服务来扩展亚马逊云科技的优势，通过结合亚马逊云科技安全服务，实现多层保护其应用和数据安全。我们持续引入全球最新的安全合作伙伴的技术到中国，加强和本土安全合作伙伴的合作，更好地满足客户在国内安全合规方面的需求。

- 以德勤为例：德勤是亚马逊云科技全球核心级咨询合作伙伴，双方在中国也开展了多年的战略合作。在安全合规领域，德勤中国和亚马逊云科技携手创建了云上安全实验室，为客户提供网络安全事件管理解决方案，并发布了一系列企业安全白皮书，为企业解读不同国家和地区关于数据安全和保护的法律法规。双方还携手推出安全运营中心服务。该安全运营中心集成了亚马逊云科技云原生安全能力和德勤中国安全合规服务能力，将赋能企业提升五大层面的安全管理能力：安全态势洞察、威胁预防与控制、降低安全风险和业务中断时间、降低管理成本，以及合规支持，从而帮助企业规避网络攻击带来的额外成本、以及网络安全带来的生意损失，保护品牌声誉、提高信息安全投资的百分比和投资人的信心，助力企业平稳快速发展。

3.3 应对案例

对于出海企业而言，亟需一个高效的整体解决方案，消除出海过程中的合规关键痛点。本文将以当下热门的全球电商独立建站平台作为典型案例，展示出海过程中，德勤与亚马逊云科技将如何帮助企业构建基于自身业务的合规体系并选择恰当的技术实现方式。

3.3.1 案例背景介绍：

案例企业是一家为全球 B2C 跨境电商提供独立站建站 SaaS 服务的企业，为跨境电商客户提供品牌出海主题、订单管理、营销插件、多语言店铺、数字营销等多种服务，助力客户打造专属的自建站和品牌。

该企业总部设在中国大陆境内，提供面向欧洲、美国、东南亚等多个地区进行销售的电商支持服务，企业规模约为 100 名员工，主要为销售人员、技术工程师与客服人员。在业务开展之初，考虑到海外客户访问的便捷性与网络延迟问题，将其应用和数据部署在亚马逊云科技的美国区域。

而作为跨境电商平台作为直接面对消费者的业务平台，处理着大量敏感的个人数据，包括姓名、住址、电话号码、银行卡号等。同时跨境电商平台要维持 7x24 小时的不间断运营，任何业务中断都可能会造成订单损失、客户体验下降等业务影响。又由于跨境电商平台面对的消费者通常来自于不同的国家和地区，这就使得跨境电商平台要适应不同区域的合规要求。

跨境电商平台的安全合规具有行业特性，例如在产品的设计阶段（例如服装）就要特别注意信息的保密；在促销季，新品发布季就要特别注重网络的 DDoS 防护 ；在日常的售后发货环节，则需要保护客户的个人联络和地址位置信息。

3.3.2 企业面临的出海安全合规核心挑战：

- **隐私合规。**企业收集、处理了大量客户的个人数据，其处理的合规性、数据的安全性以及数据传输过程的合规性成为核心挑战，这包括两个维度：
  - **隐私保护。**使用技术、流程以及合同等手段对客户的个人数据进行保护。
  - **数据跨境。**数据跨境传输和访问成为中国企业出海的头等大事。收集必要的数据来为数据分析提供支持，收集的数据可能用于产品或服务的改进、用于审计或数据分析等内部目的或用于故障诊断等，这会涉及到数据的跨境。这需要考虑到数据本地化以及减少非必要的数据传输。
- **行业合规。**不同的行业也加强的合规要求。以支付行业常见的 PCI-DSS 为例，支付卡行业数据安全标准 (PCI-DSS) 是一组专有信息安全标准，由 PCI 安全标准委员会管理，该委员会 由 American Express、Discover Financial Services、JCB International、MasterCard Worldwide 和 Visa Inc. 创建。PCI DSS 适用于存储、处理或传输持卡者数据 (CHD) 或敏感身份验证数据 (SAD) 的实体，包括商家、处理机构、购买方、发行机构和服务提供商。PCI DSS 主要分为 6 部分，包括建立并维护安全的网络和系统、保护持卡人数据、维护漏洞管理计划、实施强效访问控制措施、定期监控并测试网络、维护信息安全政策。
- **安全要嵌入到业务发展的每一个阶段，在云上构建端到端的安全。**加强业务安全建设，实现产品和服务的高质量发展，加速业务创新和上线速度。需要将安全嵌入到业务发展的每一个阶段，包括设计，研发，布署和运维的不同阶段，手段包括安全介入，架构审核，威胁建模，安全 360 度扫描，架构复审，渗透测试，审批和安全运维等。

3.3.3 解决方案

隐私合规体系建设策略步骤：

- **第一步，构建隐私合规管理体系：**德勤以出海核心国家的隐私合规法律 GDPR 的要求为基准，协助该客户构建企业隐私合规制度文件，组成企业内部隐私合规组织和确立数据合规负责人，形成完善的管理机制。

- **第二步：从客户感知层面到后台能力支持逐步进行完善**
  - **产品合规：**

    产品隐私政策完善：德勤帮助客户审阅已有的隐私政策条款，对于其数据字段的准确性、数据使用目的、适用范围是否符合最小化原则、条款是否通俗易懂、同意方式是否与数据的敏感程度相匹配等事项进行检查，并提供整改建议，帮助业务及法务部门员工完善隐私政策。

    产品自身合规性：德勤协助该客户拆解 GDPR 对于数据控制者、数据处理者以及处理活动的要求，构建了公司内部使用的数据保护影响分析模板（Data Protection Impact Assessment，简称 DPIA），并以此模板为基准与核心产品比对是否存在合规风险，并协作优化产品设计与功能界面；

    产品流程优化：另一方面德勤在该客户已有的对产品设计、开发、上线等流程进行改造，将隐私合规需求融入流程，以降低后期进行隐私合规改造花费的合规成本。

  - **数据跨境管理：**德勤协助客户梳理自身的数据流转情况，包括不限于消费者的个人信息、供应商联络人信息、员工个人信息等，并与亚马逊云科技基于业务需求、行为属性、数据类型、法规要求角度为客户推荐合适的区域来部署海外应用和数据分析方案，客户最终可选择合适的亚马逊云科技云区域来符合数据本地化的要求。同时亚马逊云科技提供敏感数据保护识别和保护，提供敏感数据识别、数据打标、数据脱敏、数据跨境传输监控、跨境审计等能力，帮助客户持续监控数据资产及传输情况。

- **数据主体权利响应：**德勤协助客户构建数据主体权利响应流程，并逐渐通过工具的开发实现自动化的数据主体权利响应窗口功能，该窗口集成常见的数据主体权利响应能力，并构建了将请求者身份信息匹配以识别其关联个人数据的机制，以帮助 SaaS 客户实现支持多国多语言的 24 小时自助服务。

- **安全事件响应机制：**除部署边界防护工具、入侵检测等工具检测是否存在数据安全事件的同时，德勤帮助企业内部构建了一套对发生安全事件时的定级、上报、对外沟通、解决确认和最终复盘在内的机制，以便满足多个国家要求的在发生事件后指定时间内进行处置和上报的合规需求。

- **第三步：形成定期合规状况复核机制，**监管环境、企业业务环境、系统配置环境、外部安全环境不断变化的同时，企业的合规性也并非一成不变。德勤为客户提供了隐私合规自评估工具 D.PAsS，客户可以定期对自身在 GDPR 的合规管理状态、产品合规状态进行自评估，该工具还关联了 Amazon Config 产品，可以依据其扫描结果自动判断合规状态。同时该工具为客户提供了 GDPR 处罚库以及整改建议库，帮助企业识别当前监管重点以及提升方向。

德勤隐私合规自评估工具 D.PAsS

*该功能需单独购买 Amazon Config 产品。

- **第四步：通过国际权威的在隐私管理、数据安全、信息安全等领域的第三方认证，**比如 ISO27701、EuroPrivacy 等增强对于自身合规性的认可与市场信任程度。
  - **PCI-DSS 合规：**亚马逊云科技提供了满足 PCI 合规的全套云上解决方案，确保出海企业在持卡人数据环境 (CDE) 下每一笔交易都安全可靠，全方位的安全服务可为出海企业提升 PCI 审计效率、减轻架构搭建压力、缩短产品交付周期提供了强大支撑。亚马逊云科技还专门推出了 CAA PCI-DSS 课程，辅助支付相关企业快速通过 PCI DSS 审计。

云上构建端到端的安全

以下从电商平台外部，内部，日常管理效率和反欺诈四个场景来展开，将亚马逊云科技云安全服务应用到这四个场景中去。

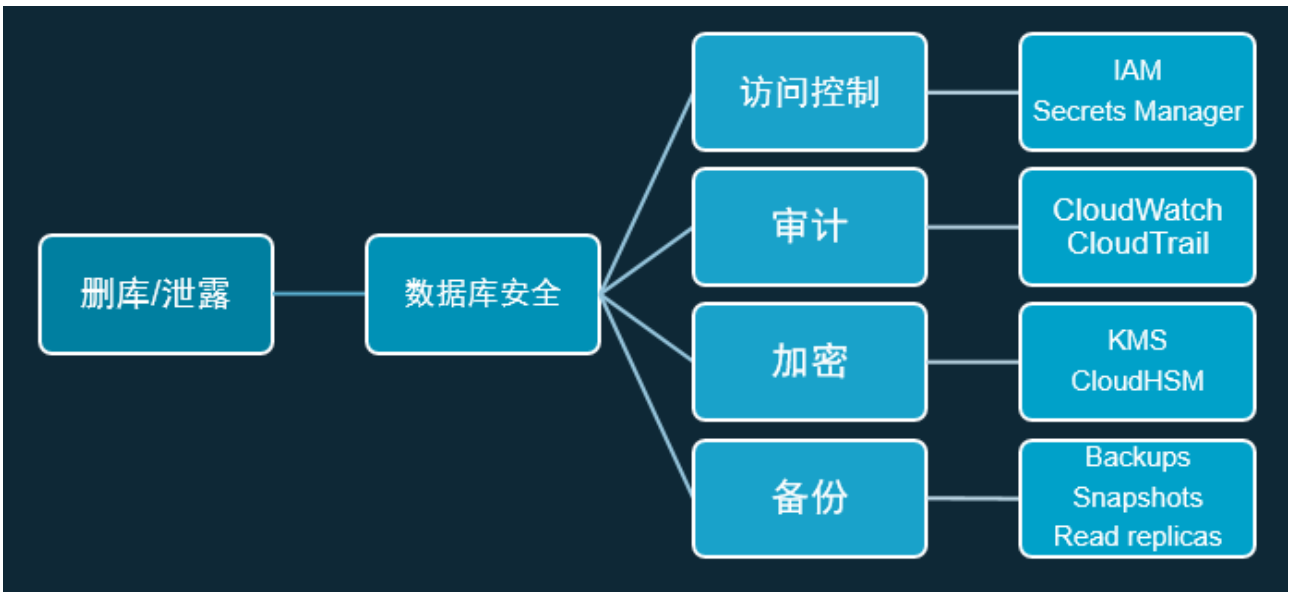
- **平台外部的安全。**电商平台需要关注的安全问题包括 DDoS 攻击，非法扫描攻击，账户盗用，存储桶入侵等。在 DDoS 防护方面，亚马逊云科技提供了 Shield 和 WAF 两种服务。

  亚马逊云科技观察到之前未出现过的攻击峰值 2.3Tbps，这是通过一个已知的 UDP 反射攻击 -- CLDAP 反射达到的。如此大规模的 CLDAP 反射攻击发生在 2020 年 2 月的第三周，亚马逊云科技针对此次攻击采取了最高级别响应，最终成功防御了此次攻击。

  针对应用层的攻击，亚马逊云科技提供了 WAF 服务，并为客户提供了简易上手的自动化布署模板，客户可根据此模板加载相关规则，设置白名单，黑名单，SQL 注入防护等规则，该服务还提供了蜜罐功能用于反爬虫和恶意机器人。同时可使用亚马逊云科技 Athena 对 WAF 日志进行分析，再根据分析结果去更新规则。客户除了可以使用亚马逊云科技提供的托管规则，或自定义规则外，客户还可以在 Marketplace 上选用第三方的规则并加载到 WAF 上，以此来实现多 WAF 规则的布署。

在应对外部的安全危胁时，电商平台客户可以通过 Amazon GuardDuty 威胁检测功能来持续监控和保护亚马逊云科技 账户、工作负载以及 Amazon S3 中存储的数据。特别是对于存放客户敏感数据 ，交易信息，产品设计文稿的 Amazon S3，更加应该注意非授权的访问，非授权的外部分享，恶意 IP 的访问等。

- **平台内部的安全。**安全的问题就集中在访问控制，网络和实例的安全以及数据的保护和备份。在今年，频频出现数据泄露，数据被恶意删除等事件，电商平台处理的数据多且集中。数据的安全，需要在以下四个维度做好功课，访问控制，审计，加密和备份。亚马逊云科技在这四个维度都提供了相应的服务供客户使用。



以访问凭证的管理为例，在日常工作中，凭证管理容易出现各种疏忽，比如用邮件传送相关凭证，开发者可以看到或者共享相关凭证，凭证的管理杂乱无序，对凭证的使用没有跟踪记录，缺乏可见性，凭证的产生和获得完全依靠安全团队，耗费时力，凭证轮换会影响系统运行的稳定性。 这时可以通过 Amazon Secrets Manager 进行管理，获取和轮换凭证 , 解决凭证明文使用的问题，可以更频繁地进行轮换更新，实现程序化地运行，减少人工参与，同时可审计并追溯凭证使用的情况。

对于内部的网络可到达性和实例的安全性，亚马逊云科技提供了 Inspector 服务，在网络层面 可以检测到具体哪个端口在哪条路径被打开，以及正在被哪个进程以什么样的方式使用，在实例层面，可以检测到 CVE 漏洞，并告知客户可能产生的影响，以及推荐的改进措施。

数据是一切安全合规的本源，对数据进行分类并保护是所有合规的基础。随着业务的发展，生产数据越来越多，各个国家和地区对敏感数据的定义也越来越广，同时数据分布也越来越分散，这一切都使得对敏感数据的识别和保护变更日益重要，特别是电商行业客户。亚马逊云科技 Macie 根据现行的 GDPR， PCI，HIPAA 等合规要求定义出了敏感数据的类型，包括个人信息，家庭信息，健康信息，同时也支持客户自定义敏感信息，亚马逊云科技 Macie 可以根据预置的和自定义的敏感数据规则进行分类筛选，并根据发掘出来的数据类型提供不同的保护建议。

对于已经查找出来的敏感数据 ，亚马逊云科技提供了不同的加密服务，包括 ACM, KMS, CloudHSM 来满足不同的加密场景，例如传输加密，存储加密，数据库加密和应用加密。

提高安全管理的效率。虽然事关安全无大小，但还是应该简化安全的管理流程，将更多的精力和时间投入到业务创新中去。例如针对证书管理和 APP 客户管理耗时耗力的问题，亚马逊云科技 ACM 可支持通过邮件或 DNS 进行认证，证书有效期是 13 个月，支持全托管的更新和布署，被多个浏览器信任，并且完全免费，非常适用于初创企业，客户也可以导入第三方证书到 ACM 进行简化管理。 在 APP 客户管理方面，亚马逊云科技提供了 Cognito，可结合多种社交应用进行注册登陆，也可以支持对注册账号进行综合的安全认证，例如邮件，电话号码唯一性。Cognito 可结合亚马逊云科技 Pinpoint 对客户进行分类和分析，并产生分析报告，例如客户的区域，注册时间，消费偏好等。

反欺诈。在疫情过后，经济正在逐渐恢复，但也出现了各种网络欺诈事件，包括假合同，虚假信用卡支付等。传统应对欺诈的做法是组织人工团队，并针对已发生的欺诈行为进行总结归纳找到规律，再制订相关规则更新到系统中进行防护，此做法通常会滞后，缺乏实时性。近几年也出现了专门提供反欺诈解决方案的企业，但由于欺诈行为通常发生在不同的行业，例如电商，游戏等，这种方案显得针对性不够。亚马逊云科技 Fraud Detector 可以用来解决欺诈识别，该服务先构建一个机器学习的模型，同时结合了亚马逊云科技和 AMAZON.COM 多年的反欺诈经验，最后允许客户上传历史欺诈交易数据，这三方面的结合就给客户提供了一个可用于识别虚假账户，虚假交易，虚假信用卡的方案。此服务还提供了 API， 在客户对某一笔交易存疑时，可以实时调用 API 进行欺诈评估。

致谢

- **编写指导**

  德勤中国：薛梓源

  亚马逊云科技：顾凡 陈晓建 白帆

- **主编人员**

  德勤中国：何微 邓娜 万芷辰 张繁 张文瑾 王琳

  亚马逊云科技：江学森 张亮 谢燕敏

- **协助编辑**

  德勤中国：康轩瑜 赵育彤 陈思阳 章桁 张权 黄彦恺

  亚马逊云科技：王焘 王骞 庞硕

亚马逊云科技 | Deloitte.

亚马逊云科技官方微信

扫码查阅
亚马逊云科技合作伙伴资料中心

扫码关注德勤公众号