亚马逊云科技 | Deloitte.

打造合规守法的数字化底座

中国企业出海发展建议白皮书 2021 版

2021.9.26

本白皮书由德勤企业咨询（上海）有限公司（“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、第二章和第三章 a 部分，单独享有该部分的知识产权；亚马逊云科技负责第三章 b 部分（即“技术平台”部分），单独享有该部分的知识产权。

关于德勤部分的声明

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，任何德勤有限公司、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，您应咨询合资格的专业顾问。 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。任何德勤有限公司、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。德勤有限公司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。德勤有限公司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。德勤有限公司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

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和核心驱动力。数据资产作为人类最新最有活力的资产形式将成为企业最核心竞争力的来源。同时，数据的流动性、共享性为如何保护这核心资产，如何在统一的规则和共识下进行数据确权、数据估值以及最终的数据贸易带来了巨大的挑战。

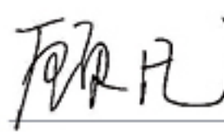
“合规是红线，安全是底限”，各国都在不断通过各种立法来规范数字化经济的发展，确保对于数据的主权、维护核心数据资产的安全、保护个人隐私、促进数据必要的合法流动和共享、以及减少广义供应链风险。其中欧盟的《通用数据保护条例》、《数字服务法》、《数据市场法》都是这方面典型的代表。

虽然受疫情的影响，全球化的进程似乎受到了阻碍放慢了步伐。但全球化是数字化经济的必然趋势，众多中国企业依然在积极进行出海布局，这是一个更加理性和有规划的过程。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，网络安全合规甚至是比业务先行更重要的决定性议题。

本白皮书旨在为中国企业出海数据安全，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，从而建立有效的数据安全合规保障体系。

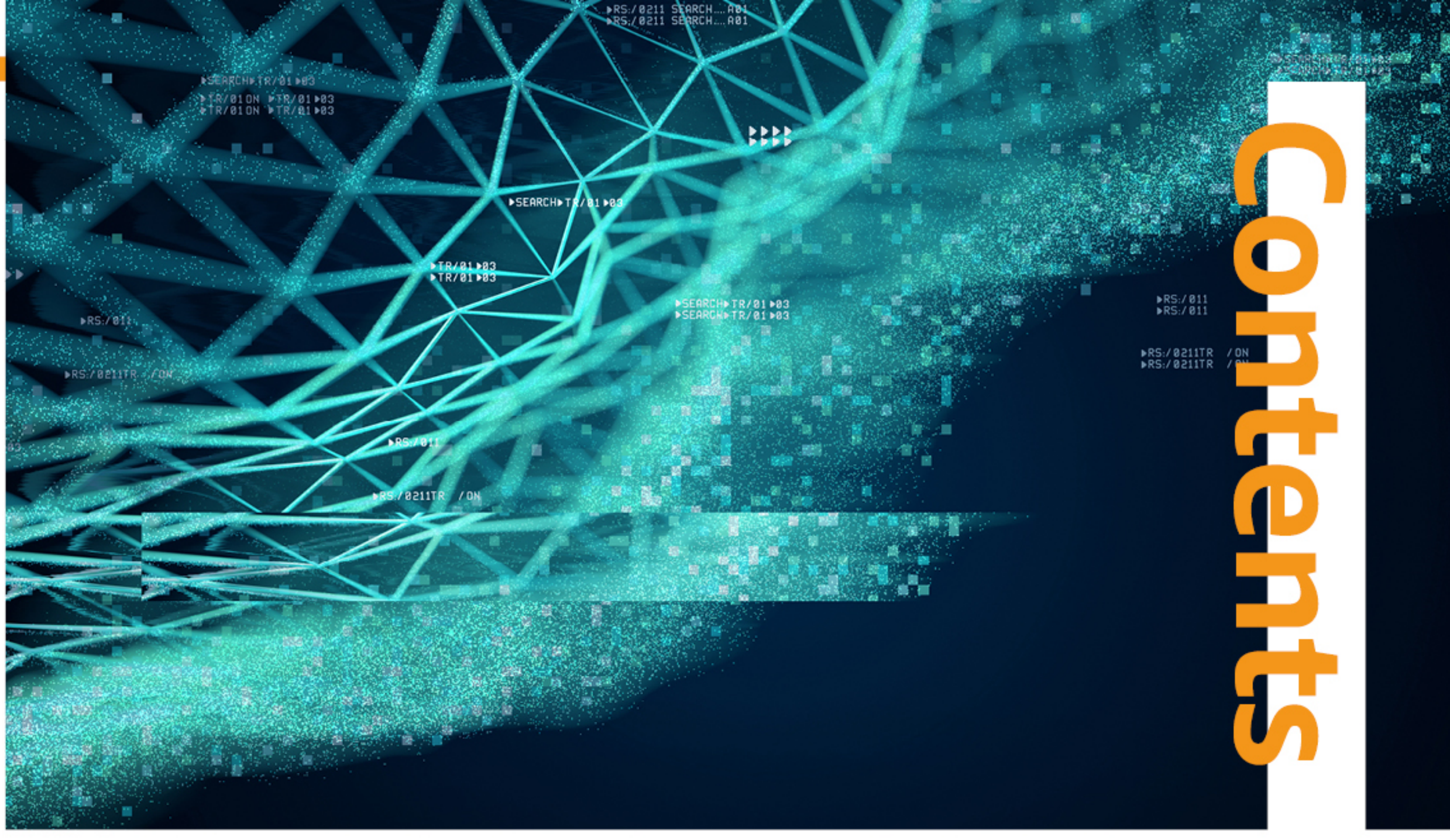
德勤中国风险咨询全国主管合伙人

吴苹



亚马逊云科技大中华区产品部总经理

顾凡



Contents

目录

国际数字经济及数据安全隐私保护发展趋势

a. 数字经济的大势

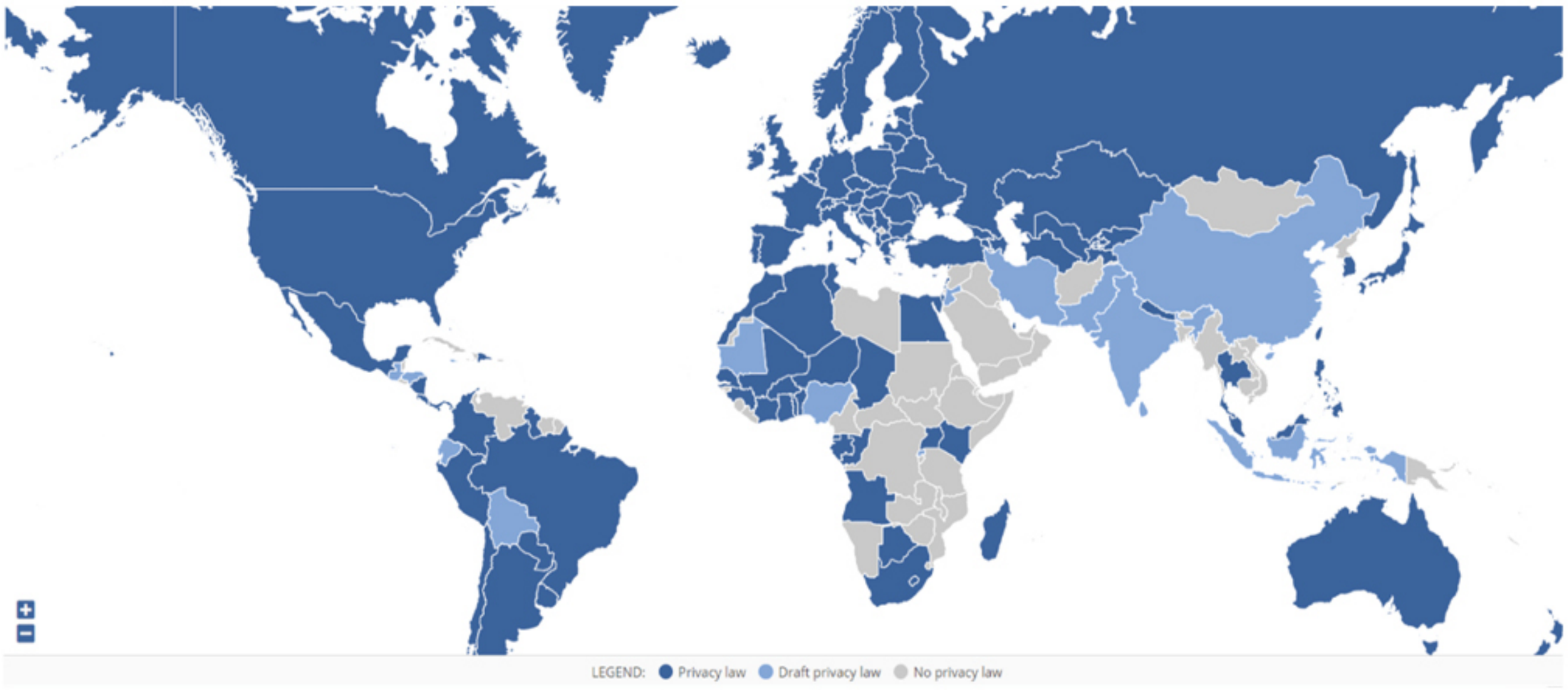
随着数字技术的不断演进，数字经济也随之蓬勃发展。数字经济作为一种无重量经济，在物理空间之外创造了一个新的数字空间，基于数字产品的生产和服务在这个空间内创造价值，并由此催生出了许多全新的产业模式，例如大数据、云服务、人工智能、区块链、数字货币、社交网络等。

《全球数字经济新图景（2020年）》指出，尽管受到全球疫情的影响，全球数字经济仍同比增长 5.4%，高于同期 GDP 名义增速 3.1 个百分点，表现出数字经济在面对冲击时的韧性。2019 年全球数字经济规模达到 31.8 万亿美元。全球数字经济占 GDP 比重达到 41.5%，这表明，数字经济将成为世界经济创新发展的主流模式。

数字经济离不开数据的支撑，大数据作为信息技术发展的必然产物，对于推动数字经济的形成与繁荣起到了至关重要的作用。从 1997 年第一次作为一个专用名词正式出现在公共期刊，到如今逐步渗透到各行各业，大数据一直呈现出蓬勃的发展态势。大数据的作用从最初对数据的描述总结分析层面逐步转化到预测事物的发展模式层面，并在近年来进一步达到分析不同决策带来的后果，并对决策进行指导和优化的层面。未来，随着应用领域的拓展、技术的提升、产业生态的成熟，具有更大潜在价值的预测性和指导性应用将成为大数据技术发展的重点，在这其中非常典型的应用就是人工智能。人工智能的核心在于通过机器学习、自然语言处理、计算机视觉、自动推理和知识表示等方式，对大量有效数据进行分析，推演出合理的决策和行动。从 alphaGo 进入大众视线以来，当前人工智能在自动驾驶、智慧医疗、智能终端等领域都已经有了广泛的应用。未来随着信息技术的发展、计算设备的计算及数据处理能力的提升、机器学习算法的快速演进以及智能传感器的快速普及，基于大数据的人工智能将获得持续发展的动力来源，大数据的价值也会更加明确地展现出来，这些都将有助于催生数字经济背景下的新业态、新模式，为数字经济的发展带来更强的助力。

数字经济以互联网为基础，带动了全球创新链、产业链和价值链的优化与整合，同时推动了全球经济贸易模式的新变革，即带来了全球化的数字贸易。数字贸易的典型特征是通过数字化的贸易方式和贸易对象，提升贸易效率，降低贸易成本，促进可贸易产品的多元化和资源的合理配置。随着云、网、端等数字技术与经济社会各领域的进一步融合，全球数字服务贸易也将迎来新的机遇。

作为数字贸易过程中重要的交付和生产要素，数据已然创造了巨大的价值。为进一步推动数字贸易的发展，数据的交流和共享需求也在逐步增强，如何确定合适的数据共享范围和合适的数据共享方案也日趋成为国际交流合作的关注焦点。



资料来源：Data Guidance

b. 数据安全及隐私保护的趋势

全球隐私保护立法现状及趋势

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：从国内视角，为了保护本国重要数据即个人数据的有序利用，起草法律条文以规制各商业主体收集、使用、分享、存储以及披露数据信息的行为；从国际视角，为了满足本国数据安全的需要，在数据国际流动规则中占据话语权，建立国内数据出境管理制度，积极参与数据跨境流动对话，共同推进数据在全球范围内的安全流动。

一方面，在国内法层面，上世纪末至今，各国陆续开启了隐私保护国内立法进程。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。截止 2021 年 4 月，全球有 85% 以上的国家和地区已有生效的数据保护立法或正在起草流程中的草案，各国也均采取不尽相同的立法模式。

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，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矛盾也将深刻影响着未来数字经济的走向。为了平衡这两者之间的矛盾，抢占新一轮经济竞争制高点，各国纷纷建立、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，在未来不长的事件内，可以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，如我国在个人金融信息保护等分别出台了新的适用标准。英国信息委员会在 1 月份出台了《适龄设计规则》等。

其次，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，对数据进行风险分级管理，各国将出台针对特殊领域的特别法令，以满足多层次需求。日本已率先在敏感行业领域完成了较多立法工作。

同时，国际间将逐步形成通用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，数据处理者需要有进行任何处理活动的合法理由等。随着各国、国际组织立法、指导的不断深入，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、多边的数据保护互认机制将出现，这将极大地便利跨国公司对不同地区业务的协调，从而大幅度降低跨国公司的运营成本。

再次，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。各国在借鉴国外优秀实践的基础上，结合本国产业发展的特点及现有的组织、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，积极探索建立各异的数据管理体系。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。

全球数据安全及隐私保护执法情况

以下为近期个人信息保护立法的执行情况，不难看出，目前的执法重点依然是显性违规，合法基础缺失、有效安全组织与技术措施缺失、未遵守一般处理义务为处罚案例数量 Top 3。

	Violation	Number of Fines
	Insufficient legal basis for data processing	**232** (with total € 165,771,848)
	Insufficient technical and organisational measures to ensure information security	**138** (with total € 65,904,419)
	Non-compliance with general data processing principles	**115** (with total € 24,639,464)
	Insufficient fulfilment of data subjects rights	**60** (with total € 16,026,025)
	Insufficient fulfilment of information obligations	**36** (with total € 5,664,295)
	Insufficient cooperation with supervisory authority	**25** (with total € 183,229)
	Insufficient fulfilment of data breach notification obligations	**17** (with total € 1,238,291)
	Lack of appointment of data protection officer	**5** (with total € 186,000)
	Insufficient data processing agreement	**3** (with total € 89,380)
	Unknown	**1** (with total € 500)

资料来源：Data Guidance

2020-06-01 因泄露前员工个人数据， Citrix 将赔偿 227.5 万美元

2020 年 3 月 8 日，网络软件公司思杰（Citrix Systems）对外表示，该公司发生数据泄露事故，黑客通过侵入多个员工账号获得内网权限，窃取了 6-10TB 的敏感数据，包括电子邮件、网络共享文件，以及项目管理和采购相关文档等。FBI 表示黑客可能使用了一种名为“密码喷雾”（Password Spraying）的密码破解技术。该公司在致被认为受影响的人的信中表示，包括员工、承包商、实习生、应聘者、受益人和家属，其个人数据可能已被盗。其被盗数据可能包括 PII、社会安全号码、护照号码、有限的健康保险数据、驾驶执照和金融账户信息，如支付卡号码。

经美国联邦调查局 (FBI) 提醒，Citrix 才发现其网络遭遇了黑客入侵。Citrix 于 2019 年 3 月披露了这起数据泄露事件。从 2018 年到 2019 年，网络攻击者渗透在这家软件巨头的内部服务器中大约五个月的时间。该公司表示，威胁参与者可以“间歇性地”访问公司资源，而“密码喷射”是获得 Citrix 系统访问权限的一种可能方法。

Citrix 员工因此次威胁事件数据被盗，现将获得 227.5 万美元的和解金。 该和解协议于 2020 年 6 月首次达成，至此，这起涉及约 24300 名成员的集体诉讼将得到和解。Citrix 将提供 227.5 万美元的资金，用于信用监控服务、身份盗窃找回，并为每位索赔人偿还至多 1.5 万美元的费用和损失补偿。

2020-07-09 因非法营销，意大利两家电信运营商被处以 1780 万欧元处罚

2020 年 7 月 9 日，意大利数据保护监管机构（SA）在针对电信运营企业的监管执法中，对电信运营企业 Wind Tre 处以约 1700 万欧元罚款，并发布了禁止令；对电信运营企业 Iliad 处以 80 万欧元罚款。

Wind Tre 存在与市场营销有关的非法数据处理行为：一是该企业在未通过短信、电子邮件、传真或电话等方式征求用户同意的情况下，实行主动营销；二是因企业提供的联系信息不准确，用户不能行使撤回同意的权利，也不能反对因营销目的进行的数据处理行为；三是在个人提出反对甚至反复提出的情况下，该企业仍将个人数据列入公共电话列表。除了上述问题，Wind Tre 还存在下述问题：一是其推出的应用程序存在违规处理数据的行为，要求用户访问时同意其处理用户个人数据，且此类同意 24 小时后才允许撤销。二是其合作伙伴存在侵权行为，为此，意大利 SA 对其中一个合作伙伴处以 20 万欧元的罚款，并禁止该企业违规委托代理机构在国内收集和处理数据。

在 7 月 9 日的监管执法会议上，意大利 SA 还评估了对电信运营企业 Iliad 的调查结果，认为该企业存在一些其他问题，尤其是交通数据采集方面，并决定对该企业处以 80 万欧元罚款。

2020-07-15 因违规处理儿童数据及违规境外传输，Tiktok 被处以 1.86 亿韩元

7 月 15 日，韩国通讯委员会（KCC）宣布对 TikTok 进行处罚，理由是未经家长同意收集 14 岁以下儿童的数据、未通知将用户的个人数据转移海外，总罚款金额为 1.86 亿韩元（约合人民 108.6 万元）。从 2017 年 5 月 31 日到去年 12 月 6 日，抖音国际版至少收集了 6700 个 14 岁以下儿童的个人信息，韩国广播通信委员会已经清除了这些账号。即使 TikTok 有发出隐私政策的通知信息，它不为 14 岁以下的儿童提供服务，但还是可以通过直接在会员注册阶段输入 14 岁年龄以下的出生日期，确认跳过了验证过程。

根据韩国现行法律规定，在将个人信息转移到国外时，必须通过个人信息处理政策，告知用户并得到同意。但 TikTok 忽略了这一过程，并没有通知将个人信息转移到国外时需要告知的事项。因为它将韩国国内用户的个人信息，委托给了美国和新加坡等云服务提供商。

TikTok 已经表示，立即停止违规并制定防止再次发生的对策，包括对个人信息保护人员和业务人员进行定期培训，TikTok 还计划在收到处理通知之日起一个月内，提交执行命令的履行结果。

中国企业出海面临的合规挑战

a. 主要数据安全及隐私法规概述

各国国内数据安全立法概况

欧盟：统一立法模式，制定统一信息保护法典；权利主体本位，以人权保障为基本价值取向；以 GDPR 为核心，补充特定领域立法，并通过一系列指引加以细化。

欧盟的《通用数据保护条例》（General Data Protection Regulation，简称 GDPR）自 2018 年 5 月 25 日起在欧盟成员国内正式生效实施，如今法规实施已两年有余。在这两年时间里，正如欧盟数据保护委员会所言，成功实现了加强保护个人数据保护权和保障个人数据在欧盟内部自由流动的目标，但也发现了一些未来需要进一步改进的领域，例如降低 GDPR 的实施对新技术的应用的阻碍作用。为了解决实施中的系列问题，欧盟的监管机构在这两年里一方面针对特殊领域、特殊事项进行补充立法，另一方面通过发布一系列的指引，细化立法实施。

2019 年 6 月 27 日，欧盟委员会通过了《关于欧盟网络与信息安全局（ENISA）、信息通信技术网络安全认证及废除（EC）第 526/2013 号条例之条例》（即“欧盟《网络安全法》”），与 GDPR、《非个人数据自由流动条例》（Regulation on the Free Flow of Non-personal Data）共同构成欧盟网络与数据安全的顶层立法。主要规定：第一，明确 ENISA 的宗旨、任务和组织事务；第二，建立欧洲网络安全认证机制框架，以确保欧盟境内的信息和通信技术（ICT）产品、ICT 服务和 ICT 流程达到充分的网络安全等级并避免欧盟成员国在网络安全认证机制方面各自为政。

2021 年 1 月 5 日，欧盟委员会发布了新的《电子隐私规定》（ePrivacy Regulation）草案（“电子隐私规定草案”）。该草案旨在代替原有的《电子隐私指令》（ePrivacy Directive），配合《通用数据保护条例》（“GDPR”），以便应对信息技术发展带来的新挑战。电子隐私规定草案将电子通信网络的定义扩展至包括 Whatsapp、Facebook、Messenger 等即时通讯服务，以确保它们在保密性上与传统的电信服务处在同一水平。

除欧盟委员会的立法外，欧盟的主要立法活动还体现在欧盟数据保护委员会（EDPB）发布的有关 GDPR 理解和适用的指引。这些指引虽然没有强制执行力，但对欧盟范围内以统一标准适用 GDPR 及相关规定、促进欧盟各国执法机构合作具有重要意义。EDPB 自成立以来，已发布指引及推荐共 10 份，并采纳其前身 29 条工作组发布的指引和推荐等共 16 份。

美国：联邦未制定统一的数据保护立法，采取州立法 + 分行业立法 + 行业自律相结合模式；倡导自由市场式的数据利用，在保障个人数据的广泛访问权的基础上，兼顾公民隐私保护。

与欧盟统一立法模式不同，美国并未在联邦层面制定统一的数据隐私保护基本法，而是采取了分行业的分散立法模式，形成了针对金融、征信、医疗、电信、教育以及儿童在线隐私等若干领域的个人隐私保护立法体系。在州层面，美国各州亦形成了各自的数据保护法律框架。目前，各州均已制定了应对数据泄露的立法，一些州也出台了不同类型的消费者保护立法。

2018 年 6 月加利福尼亚州通过的《2018 加州消费者隐私保护法》（California Consumer Privacy Act，简称 CCPA），被称为全美最严厉、最全面的个人隐私保护法案，该法案已于 2020 年 1 月 1 日生效，其在数据主体权利、数据泄露的预防和问责机制等方面借鉴了 GDPR 中的某些规定，例如：用户有权查阅自己被收集的数据，要求删除数据，以及选择不将数据出售给第三方。但其也有不同于 GDPR 的内容，例如：基于其高度发达的数字产业，CCPA 中没有数据跨境方面的限制，而更鼓励个人信息的商业流通，以满足聚居在硅谷的众多科技、互联网及新兴产业发展的需要。其适用于所有面向消费者（线上或线下店铺）的商业场景，对美国其他各州后续的立法活动产生较强的带动效应。

2020 年 11 月 3 日，加利福尼亚州又通过了《加州隐私权法案》（California Privacy Rights Act of 2020，“CPRA”）。极大地改变了 2018 年《加州消费者隐私法案》（California Consumer Privacy Act，“CCPA”）确立的隐私保护法律框架，以对标欧盟的 GDPR。与 CCPA 相比，CPRA 拓展了加州居民的隐私权范围，赋予居民更正权，使得其可以要求存有不准确个人信息的商业机构修正这些信息。同时，CPRA 亦创设了“敏感个人信息”（sensitive personal information）这一概念，其中包括政府颁发的个人身份信息（如驾照号码、护照号码）、金融信息、精确的地理位置、种族、信仰、工会成员身份、消费者信件或电子信息内容等。此外，CPRA 完善了有关受监管主体认定、自动化决策以及未成年人保护等方面相关的问题。CPRA 还建立了新的隐私保护主管机关：加州隐私保护局。该机构将调查并举行听证会，以确定受监管主体是否符合 CPRA 的要求，并对违规行为处以罚款。按照计划，CPRA 将于 2023 年 1 月生效。

日本：普通个人信息保护法与特殊领域专门法相结合；增设统一监管机构日本个人信息保护委员；注重行业自律和社团参与。

日本《个人信息保护法》（The Act on the Protection of Personal Information（57/2003））于 2005 年 4 月 1 日起施行。随着信息技术的急速发展和个人信息不断外延拓展，该法于 2015 年进行了大幅修正，最新修订法案于 2017 年 5 月 30 日起施行。修正案在立法目的中增加了“在对个人权利利益加以保护的同时，还考虑到个人信息正确且有效的使用有助于增加经济产出、创造有活力的经济社会、丰富国民生活及其他有用之处”，对个人信息的社会价值予以肯定。 法案还增设日本个人信息保护委员会（ Personal Information Protection Commission，简称 PPC）作为日本个人信息处理从业者的专 门监管机构，PPC 以《个人信息保护法》为法律依据，确立了“保护个人权益利益，兼顾个人信息有用性”的指导原则，行业自治同国家统一立法并行不悖。此外，就境外个人信息的处理，修正案引入了相关限制措施。《个人信息保护法》在日本隐私权行政法规保护方面居于绝对的核心地位，对日本国民隐私起到重要的保护作用。除顶层的《个人信息保护法》外，日本的个人信息保护制度规定根据团体、组织的性质，分别适用不同的法律关系，并且在信用、医疗、电信、教育等领域制定专门法。

2019 年 4 月 25 日，日本个人信息保护委员会发布了《个人信息保护法》修正案中期汇总。此次中期汇总新增企业停发广告义务，即在个人要求企业停止将收集的地址和姓名等个人信息用于广告时，企业有义务同意。

2020 年 6 月 5 日，日本参议院通过了《个人信息保护法》修订版。该法预计将于 2022 年春季完全生效，修订后的法律将适用于外国主体。个保法修订版扩大了个人的权利。旧的《个人信息保护法》不适用于将在 6 个月内被数据处理者删除的数据，而个保法修订版删除了这一豁免。个人要求数据处理者停止或删除自身数据的权利也在个保法修订版中得到扩张。在向第三方传输问题上，个保法修订版进一步限制了适用 opt-out 规则的传输情形，并赋予个人要求数据处理者披露传输记录的权利。此外，当数据接收方有意将新接收的数据与已有数据结合时，其必须获得个人的同意，而传输方必须提前确认接收方已经获得必要的同意。个保法修订版还增加了信息匿名化处理的相关规则，填补了旧法在这方面的空白。数据处理者现在可以自由处理经过匿名化的个人信息。在数据泄露的情形下，个保法修订版要求数据处理者及时通知个人信息保护委员会以及受影响的个人。

上述三个地区代表了三种典型的立法模式及修订趋势，除此之外，各国呈现出各异的立法情况，无法在此穷尽阐述，但相同的是，各国的立法模式及修订趋势与国内产业特点及数据安全考虑侧重点相关。以下为部分主流国家数据保护立法概况。

印度 PDPA：自 2017 年最高法院在 Puttaswamy 案中宣布隐私是一项基本权利以来，印度的数据保护一直受到越来越多的关注。随后，由政府组成的专家委员会发布了《2018 年个人数据保护法案草案 >。经过利益相关者的建议，修订后的 2019 年《个人数据保护法案》提交给了印度议会下院人民院，预计将在 2020 年获得通过。与 GDPR 及各国数据保护立法不同，PDPA 将个人数据分为：一般个人数据、重要个人数据及关键个人数据三个层级，并且对这三个等级的个人数据提出了不同的合规要求，例如在数据出境方面，未对一般个人数据提出要求，对敏感数据，需要获取同意并且满足一定的目的条件，针对关键数据，需要在极特定情况下经批准出境。

韩国 PIPA：韩国的《个人信息保护法》（Personal Information Protection Act）主要针对与自然人相关的个人信息，包括全名、居民登记号码或者可以用于证明身份的所有信息，所涉信息可能无法立刻证明身份，但可与其他信息结合以证明身份。《个人信息保护法》包括八项隐私原则，公共部门和私营部门的个人信息处理者（无论规模大小）均须遵守这些原则。

巴西 LGPD：LGPD 于 2018 年通过，并于 2020 年 9 月 18 日生效，但其执行条款从 2021 年 8 月 1 日开始生效。LGPD 是一个全面的数据保护法，它涵盖了数据控制者和处理者的活动，对信息处理提出了新的要求，包括关于数据保护官员任命、数据保护影响评估、数据传输和数据泄露等各种问题的规定。它将由 ANPD 执行，当 ANPD 成立时，预计将为 LGPD 的规定提供重要和更明确的指引。此外，2014 年 4 月 23 日的第 12.965 号法律自 2014 年 6 月起生效，确立了在巴西的数据控制者和处理者使用互联网的原则、保证、权利和义务。到目前为止，在 ANPD 成立之前，联邦地区和领土公共部已根据《Marco Civil da Internet》的规定，就隐私问题采取了各种执法行动。

澳大利亚 PAA: 澳大利亚信息专员办公室根据 1988 年颁布的《隐私法》（Privacy Act 1988）对澳大利亚全国范围内的隐私信息进行统一监管。受保护的信息类型包括个人信息和敏感信息。除《隐私法》外，澳大利亚还针对特定行业制定了相应的监管制度，主要适用于医疗卫生行业、 授信机构和征信机构和电信和传媒。

新加坡 PDPA：《个人资料私隐条例》订明一般的个人信息保障规定，并载有有关资料当事人权利、委任资料保护官，以及相关中介人的责任的条文。此外，《PDPA》修正案于 2021 年 2 月 1 日生效，引入了一些更新要点，包括强制性数据违反通知要求、同意义务修正案、严重不当处理个人数据的违法行为、禁止使用地址收集软件等。除《PDPA》外，《2018 年网络安全法案》(2018 年第 9 号) 还规定了新加坡的网络安全监管框架，并规定了关键信息基础设施运营商的要求。

各国及国际组织数据跨境流动管理模式

除了个人信息保护，其他的商业数据，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矛盾也将深刻影响着未来数字经济的走向。为了平衡这两者之间的矛盾，抢占新一轮经济竞争制高点，各国纷纷建立、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。

美国：以反数据本地化的方式推行数据霸权

美国长期致力于树立数据跨境流动政策反数据本地化、维护自由贸易的形象。奥巴马政府时期签订的《跨太平洋伙伴关系协定》（TPP）第 14.13 条规定，缔约方不得将要求受约束的组织和个人使用该缔约方领土内的计算设施或者将设施置于其领土之内作为在其领土从事经营的条件。尽管特朗普政府退出了TPP，但是，2018 年签署的《美国—墨西哥—加拿大协议》（USMCA）完全吸收了上述规定，美国也在与英国、日本、韩国等谈判的贸易协议中，积极推广上述反数据本地化政策。

美国在对外推销反数据本地化政策的同时，于 2018 年 2 月通过了《澄清域外合法使用数据法案》（Clarifying Lawful Overseas Use of Data Act），即《云法案》（CLOUD Act），通过国内立法的方式授予本国广泛的数据权力。根据《云法案》，美国依其国家利益采用“数据控制者标准”划定管辖范围，无论通信、记录或其他信息是否存储在美国境内，服务提供者均应当按《存储通信法案》（Stored Communications Act）所规定的义务要求保存、备份、披露通信内容、记录或其他信息，只要上述通信内容、记录或其他信息为该服务提供者所拥有（possession）、监管（custody）或控制（control），都可以成为调取数据的来源。此外，《云法案》允许“符合资格的外国政府”在与美国政府签订行政协定后，向美国境内的组织直接发出调取数据的命令，美国也相应可以向协议国境内的组织直接调取数据。在签订《云法案》相关的双边协议过程中，美国设立的一项条件就是取消数据本地化政策，由此让需要从美国调取数据的国家将更多的数据流向美国，最终的结果就是对美国产生更强烈的依赖。

欧盟：建立附条件的数据跨境自由流动规则

欧盟致力于在成员国内部推动数据自由流动，但是，德国、法国等出于维护本国数字经济利益的需要而支持必要的数据本地化政策。欧盟在 2016 年颁布的《通用数据保护条例》（GDPR）和在 2018 年颁布的《非个人数据自由流动条例》（Regulation on the Free Flow of Non-personal Data），分别对个人数据和非个人数据采取不同的跨境流动策略。欧盟的数据流动政策制定者在考虑个人信息权利保障的同时，也积极考虑对欧洲数字经济发展利益的影响。

根据《通用数据保护条例》，个人数据可以在欧盟成员国内自由流动，但是，个人数据流出欧盟成员国必须满足法律所规定的条件。欧盟以是否达到“充分保护”作为首要参考规则，可以认定一国、一个区域、一个或多个特定行业或者一个国际组织具备充分保护水平，准许这些符合条件的地区、行业、组织与欧盟进行自由的数据跨境流动。欧盟目前已经认可的充分性保护地区包括安道尔、阿根廷、加拿大（仅限商业组织）、以色列、日本、新西兰、瑞士、乌拉圭，以及分别隶属于丹麦、英国的法罗群岛、根西岛、马恩岛、泽西岛。除此之外，非获认定地区的各类组织和企业可以根据欧盟认可的标准合同条款、约束性公司规则、行为规范、认证机制，或者获得数据主体的明确同意等特定减损情形，作为个人数据流出欧盟的合法根据。

根据《欧盟内非个人数据自由流动框架条例指南》（Guidance on the Regulation on a Framework for the Free Flow of Non-personal Data in the European Union）。欧盟旨在实现成员国内非个人数据的自由流动，激励各行

业在数据服务提供商的转换和数据传输方面制定自律行为准则，禁止成员国对非个人数据的本地化要求做出规定，只能基于符合比例原则的公共安全理由做出例外要求。欧盟建立了一个合作机制，确保各主管当局能够继续行使访问其他成员国正在处理的数据的权力。然而，该条例并不能解决非个人数据向欧盟之外流动的法律要求。

双、多边国际组织对于数据跨境流动方面的推动

经济合作与发展组织（OECD）于 1980 年 /1993 年制定了《关于隐私保护和个人数据跨境流动的指南》（Guidelines on the Protection of Privacy and Transborder Flows of Personal Data），联合国大会在 1990 年通过了《计算机处理的个人数据文档规范指南》（Guidelines for the Regulation of Computerized Personal Data Files），亚太经合组织在 2005 年通过了《隐私保护框架》（Privacy Framework）（2015 年修订），但是，这些规定都是由西方国家主导制定，尚未充分体现数据跨境流动的公平利益和国家安全的关切。近年来，日本政府借助世界经济论坛（World Economic Forum）和 20 国集团（G20）等在 2019 年提出了“可信任的数据自由流动”（Data Free Flow with Trust，DFFT）概念，希望在保障国内和国际法律框架都得到应有尊重的条件下，增强每个框架之间的互操作性，以促进数据更自由地流动。DFFT 不依赖于单一的合作论坛，而是依赖于国际贸易、法律法规、技术和其他治理领域，利用各种双边、多边、区域、国际机制，确定面向政府、企业或用户的具有约束力和非约束性的规则，提出了十余项基本原则供各种机制推动实现。

东盟发布《数据管理框架》。新加坡个人数据保护委员会于 2021 年 1 月 22 日确认，东盟部长级会议已批准《数据管理框架》和《跨境数据流动合同范本》，这是由新加坡主持的数字数据治理工作组制定的两项计划。新加坡个人数据保护委员会（PDPC）特别强调，《数据管理框架》（DMF）和《跨境数据流动合同范本》（MCC）旨在促进数据相关的业务运营，减少谈判和合规成本，同时确保跨境数据传输过程中的个人数据保护。其中，《数据管理框架》旨在为企业提供分步指导，通过完善数据治理结构、保障措施和风险管理等管理规范和基本原则，帮助企业建立有效的数据全生命周期管理系统。其包含六大核心要素，分别是治理与监督、政策与程序、数据清单、风险影响评估、数据保护控件、监测与持续改进。

b. 对中国企业出海的主要挑战

中国企业出海面临多样化的挑战，可能对当地消费者、市场、合作伙伴、文化习俗、法规监管环境等缺乏充分了解。特别是在比较发达的经济体，可能会遭遇当地政府监管，对当地业务运作产生严重影响。随着中国企业逐步开展海外业务，尤其是近几年来各国纷纷颁布或更新其隐私保护法律法规，中国企业需要在隐私保护合规方面投入更多资源。

I. 数据主体同意

欧盟的 GDPR 法规一般而言禁止处理个人数据，除非法律明确允许，或数据主体已同意处理。GDPR 对获得一个有效合法的同意设置了很高的要求，同意应通过明确的肯定行为给予，以自由给出、具体、知情和明确表示数据主体同意处理与其相关的个人数据，例如通过书面声明、电子方式或口头陈述。同时，数据主体有权随时撤回其同意，且撤回同意须与给予同意一样容易。

II. 数据本地化及跨境

中国企业开展海外业务，难以避免会触及数据跨境情形。在欧盟 GDPR 下，将欧盟境内的个人数据跨境传输至第三国，除一些特例外，必须要使用 GDPR 中规定的几种机制之一，如仅将个人数据传输至已获得充分性决定（Adequate Decision）的第三国、签署标准合同条款（Standard Contractual Clause）、遵循约束性企业规则（Binding Corporate Rules）、或获得必要认证。同时，部分国家法律要求个人数据必须在当地存储。

III. 数据主体权利保障

GDPR 赋予了数据主体多项权利，如访问权（Right of access）、更正权（Right to rectification）、删除权 / 被遗忘权（Right to erasure / be forgotten）、限制处理权（Right to restriction of processing）、便携权（Right to data portability）等相关权利，一般情况下企业须在收到请求后一个月内处理。这就要求企业将数据的访问控制与数据主体的授权联动起来，有效的存储管理和灾备机制，并建立受理并处理数据主体主张其权力的渠道和机制。

IV. 用户画像，自动化决策

在欧盟 GDPR 下，数据主体有权不受仅基于自动化处理（包括画像）的决定的约束，若这会对他或她产生法律效力或类似的重大影响。不仅如此，如果出于直接营销目的处理个人数据（包括画像），则数据主体有权随时反对出于此类营销目的处理与其相关的个人数据。这就要求企业充分考虑合适的加密、去标识化及其他隐私技术。

V. 隐私技术及隐私设计

GDPR 要求，考虑到现有技术、实施成本和处理的性质、范围、背景和目的，以及处理对自然人权利和自由造成的不同可能性和严重程度的风险，企业应在确定处理方式和处理个人数据时，实施适当的技术和组织措施（如假名化 pseudonymisation），有效地实施数据保护原则（如数据最小化 Data Minimization，默认情况下仅处理每个特定目的所必要的个人数据）。

VI. 应急响应及通知

GDPR 要求，在个人数据泄露的情况下，企业应在 72 小时内及时将数据泄露情况通知数据监管机构。当个人数据泄露可能对自然人的权利和自由造成高风险时，企业还应及时将个人数据泄露情况通知数据主体。这就要求企业建立实时的监控系统及有效的应急响应机制。

VII. 域外管辖

还应注意到，企业即使在当地未设立实体，不在当地处理数据，也有可能需要遵循当地隐私法规。如在 GDPR 下，企业若因向欧盟境内的数据主体提供商品或服务，在欧盟境外收集和处理个人数据，也适用 GDPR 管辖。

VIII．亚马逊云科技云上的 GDPR 合规

亚马逊云科技作为数据处理者：当客户和亚马逊云科技解决方案供应商使用亚马逊云科技服务来处理其内容中的个人数据时，亚马逊云科技充当数据处理者。客户和亚马逊云科技解决方案供应商可以使用亚马逊云科技服务中提供的控制措施（包括安全配置控制措施）来处理个人数据。在这些情况下，客户或亚马逊云科技解决方案供应商可能充当数据控制者或数据处理者，而亚马逊云科技则充当数据处理者或子处理者。亚马逊云科技提供了一项符合 GDPR 的数据处理附录 DPA，其中包含亚马逊云科技作为数据处理者的承诺。

亚马逊云科技作为数据控制者：当亚马逊云科技收集个人数据并确定处理此类个人数据的目的和方式时，此时它充当数据控制者。例如，亚马逊云科技作为数据控制者，可存储账户信息，用于帐户注册、管理、服务访问、客户联系和支持。 GDPR 第 32 条规定，控制者和处理者必须“实施适当的技术和组织措施”，同时考虑到“现有技术和实施的成本与处理的性质、范围、背景和目的，以及处理给自然人的权利和自由带来的不同可能性和严重程度的风险”。GDPR 针对可能需要采取的安全措施提供了具体建议，包括：

- 对个人数据进行假名和加密处理。
- 能够确保处理系统和服务的持续机密性、完整性、可用性和恢复能力。
- 在发生物理或技术事故时，能够及时恢复个人数据的可用性和访问权限。
- 制定一个流程来定期测试、评估和评价技术和组织措施的有效性，以确保处理的安全性。

c. 主要行业的特殊挑战

金融行业

相比与出海的其他行业，金融机构面临更严格的安全合规挑战。不同国家和地区的监管政策差异增加了合规风控难度，客户数据隐私的高要求带来数据存储和数据传输的额外成本，而跨境交易的特殊性也要求相关机构不断提升反洗钱的管控力度。

一、出海企业金融监管要求

中国金融机构的出海之路中，一方面要保证满足中国金融监管机构的相关要求，还需要满足东道主国家的监管法规制度。

以下整理了不同国家在数据合规性、业务连续性、反洗钱管理、支付服务管理等方面的监管规定和主要监管要求。

1. 数据合规性

《中华人民共和国网络安全法》第 37 条；《数据安全法》第 31 条、36 条；《个人信息保护法》第三章（38-43 条）；证券法第 177 条；反洗钱法第 5 条；《网络安全审查办法 - 修订草案征求意见稿》第 6 条，第 10 条，《个人金融信息（数据）保护试行办法》第 20 条；《个人金融信息保护技术规范》7.1.3.d；《商业银行信息科技风险管理指引》第 11 条等都对金融行业的数据跨境提出了要求。金融机构在出海布局尤其是向海外监管报送数据的时候一定要审慎考虑。

另一方面，美国证券交易委员会（SEC）已开始向寻求赴美上市的中国企业提出新的披露要求，其中包括披露更多首次公开募股中使用VIE的情况，以及所谓“中国监管者干预企业数据安全政策”的风险，以提高投资者对于风险的认知。

2. 业务连续性

《增强美国金融系统恢复力的文件措施白皮书》

《增强美国金融系统恢复力的文件措施白皮书》由美联储、美国货币监理署、美国证监会等在 2003 年颁布，其中确定了三个业务连续性目标，确定四个措施确保美国金融系统的恢复力。

《美国金融机构业务连续性计划实施和检查手册》

《美国金融机构业务连续性计划实施和检查手册》由美国联邦金融机构检查委员会在 2003 年颁布，其中对金融系统在业务连续性上的组织架构和管理工具方法提出要求。

《业务连续性管理指引》

《业务连续性管理指引》由新加坡金融管理局在 2003 年颁布，其中提出了金融机构业务连续性管理的七项原则。

《业务连续性管理实践手册》

《业务连续性管理实践手册》由英国金融服务管理局在 2006 年颁布，其中从危机管理、基础设施、职工人员三方面提出业务连续性管理建议。

《金融市场基础设施原则》

《金融市场基础设施原则》由国际清算银行等机构在 2012 年颁布，其中明确规定金融基础设施需要在中断事故发生后的两小时内恢复运行。

3. 反洗钱管理

AMLD5（第五号反洗钱指令）

AMLD5 由欧盟于 2018 年颁布，于 2020 年 1 月 10 日生效实施。AMLD5 涉及的领域包括虚拟货币、高风险第三方国家、实际所有权的识别以及跨国界国家所有权登记的统一，明确提出要加强金融机构执法权力和促进信息共享。

《中国银保监会办公厅关于加强中资商业银行境外机构合规管理长效机制建设的指导意见》

《中国银保监会办公厅关于加强中资商业银行境外机构合规管理长效机制建设的指导意见》由中国银保监会于 2019 年 1 月 9 日发布，其中明确规定“银行保险监督管理机构应将中资商业银行境外机构合规管理情况纳入监管评级体系。提高对境外重要性实体的监管关注，加大对业务复杂程度较高和合规压力较大的境外机构合规风险监测力度。加强对国别风险、反洗钱和反恐怖融资等重点领域的监管。”

4. 支付服务管理

欧洲银行管理局（EBA）制定的 PSD2 监管技术标准（RTS）于 2019 年 9 月生效，其中包括以下要求：

- 为电子支付交易进行强大的客户身份验证（SCA）
- 支付服务提供商进行安全的通信

据了解，欧盟将于近期发布在 PSD2 版本的基础上更新的 PSD3 监管要求。

金融行业

二、对应建议

通过梳理以上监管法规，从以下四方面对出海的中国金融机构提出对应的建议:

1. 系统建设及数据管理

中资金融企业在海外机构的系统建设的过程中，在满足当地金融监管机构的数据隐私安全合规性（如 GDPR）的前提下，需要充分考虑国内金融监管机构对核心业务系统管理权限、跨境数据存储和重要数据跨境转出的合规性。

2. 业务连续性管理

（1）中资金融企业要以满足机构所在各国监管要求为目标，提升规定时间内恢复核心业务的能力；

（2）健全业务连续性组织架构，明确职责分工和实施流程；

（3）完善异地灾备基础设施，保障业务恢复能力。

3. 反洗钱管理

（1）中国金融机构总部需要加强对境外机构监督与支持的力度，熟悉不同地区反洗钱监管要求的差异，建立对应的标准以满足高风险客户识别的要求；

（2）发展反洗钱领域的新技术，提升反洗钱管理的识别能力和准确性。

4. 支付服务方面

（1）确保遵守 PSD2 中要求的上报准则，及时向监管当局报告重大事件；

（2）完善 IT 系统的配置和升级，提高客户身份验证能力、在线支付能力以及规范访问客户账户的能力。

汽车行业

随着国内汽车企业越来越多的战略出海，海外业务发展过程中面临的网络安全和数据合规风险对国内汽车企业走出去提出了新的重大挑战。

在这其中，海外特别是欧盟地区的 GDPR 通用数据保护条例和 UNECE WP.29 CSMS 车辆网络安全法规是国内车企走向海外特别是走向欧盟地区面临的主要合规要求，更重要的是 GDPR 和 CSMS 对车企的车辆产品的数据合规和网络安全提出要求，即意味着车辆产品如果不合规将无法在海外国家或地区上市进入当地市场，因此国内车企需要重视和积极应对。当前国内汽车企业的网络安全合规意识以及网络安全技术措施与海外网络安全合规要求还存在不小的差距例如国内企业在海外市场的业务触点无法及时，完整的识别海外网络安全合规风险，也无法及时有效的传导给国内产品市场和研发团队导致车辆正向研发时和海外合规要求有差距。

一、UNECE WP.29 CSMS 车辆网络安全法规要求

UNECE WP29 车辆网络安全合规 CSMS 要求

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）颁布 GRVA 新法规，要求 OEM 车企需要符合 CSMS（Cyber Security Management System） 体系，只有 OEM 和其车型满足监管要求的认证后才能够上市销售。其中欧盟地区在全球范围内率先明确欧盟地区的合规时间表，2020 年 6 月 25 日在欧盟国家正式生效，将于 2022 年 7 月正式对 OEM 欧洲发布的新车型生效并施行，2024 年对 OEM 生产的所有车型生效并施行。

WP29 CSMS 体系的主要要求包括：

- 车企 OEM 首先需建立完善的车辆网络安全管理体系并通过欧盟监管机构的 CSMS 认证，需 OEM 在车辆的全生命周期包括研发，生产，售后，下市都要建立车辆网络安全管理流程，以确保车辆在各阶段都有充分的网络安全控制措施应对安全风险；
- 除了 OEM 公司层面的 CSMS 认证以外，OEM 还需要对欧盟地区上市的车型完成网络安全相关的 VTA（Vehicle Type Approval）认证 - 车辆型式审批认证，VTA 是针对 OEM 在网络安全的具体执行工作进行检查，确保具体车型在工程层面已经设计和实施安全措施，确保目标车型安全防护技术已有效实现；
- OEM 只有首先获得 CSMS 认证后，才能针对具体车型获得 VTA 审批认证，最终才可以在欧盟地区上市，两者缺一不可。

一、UNECE WP29 SUMS 软件更新管理体系

与上述 CSMS 管理要求同时发布的还有 SUMS（Software Update Management System）， 在欧盟地区 2022 年 7 月针对 OEM 新上市车型正式生效并施行，2024 年针对所有车型生效并施行。

WP29 CSMS 包括的主要法规要求包括：

- 软件升级法规中主要从流程体系与技术需求上对软件升级提出了具体的要求，OEM需要通过SUMS公司层面的认证。其中流程体系要求是建立软件升级管理体系（Software Update Management System，以下简称“SUMS”），主要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。
- 技术需求则涵盖通用软件升级需求及 OTA（Over-the-Air Technology，无线传输）附加需求，也是针对车型从工程角度对 OTA 方案进行验证和认证。软件升级通用需求中要求软件升级需确保真实性和完整性，同时对软件标识码（RX Software Identification Number，以下简称“RXSWIN”）的更新及访问控制提出了要求。而 OTA 附加需求主要从安全和应用场景出发，提出了相应要求，

三． 欧盟 EDPB 在联网车辆和出行相关应用环境下处理个人数据的指南（车联网个人数据保护指南）

欧洲数据保护委员会（EDPB）于 2020 年 1 月 28 日发布了在联网车辆和出行相关应用环境下处理个人数据的指南并于 2021 年 3 月发布经过公众咨询后的指南，此指南作为 GDPR 法规下专门针对车辆产品相关的个人信息保护指南，国内 OEM 在欧盟满足 GDPR 通用法规的同时，还应特别考虑车辆产品是否满足 EDPB 此份指南的要求。

- 此指南关注数据主体包括驾驶员，乘客，车主，承租人对联网车辆相关的个人信息处理的规定，这些个人信息场景包括

车内处理个人信息；车辆和连接的设备之间个人信息；向外部实体输出的个人信息等场景；

- 此指南列举车辆相关个人信息处理时的隐私和数据保护风险并提出个人信息搜集和处理的建议和要求；
- 指南对于部分案例例如第三方服务；E-Call；汽车盗窃等情况下个人信息处理的具体建议。

三、车企走向海外的应对建议

1． CSMS 网络安全管理体系建设

基于 UNECECSMS 法规要求，国内车企需建立完整的针对车辆的网络安全管理体系并实施运行，此体系包括车辆网络安全治理、网络安全风险管理、网络安全事件管理、漏洞管理、供应商网络安全管理、网络安全监控等核心管理程序和控制要求。

（1）网络安全治理应充分考虑网络安全管理的组织架构与角色、合规管理、认证管理、意识文化管理、能力管理、合规审查、可持续改进等核心流程活动确保网络安全治理的工作有效执行。

（2）网络安全风险管理应充分考虑风险识别、分析、处置、上报等核心活动，确保车辆网络安全风险的有效控制。

（3）网络安全事件管理应充分考虑事件收集、分类、响应、处置等核心活动，确保网络安全事件及时的处置。

（4）漏洞管理应充分考虑内部的安全测试、外部的漏洞信息的收集与分析、漏洞处置以及漏洞管理等重要活动。

（5）供应商网络安全管理应充分考虑供应商的能力审查、产品技术管理、运营协同义务等重要活动，确保车企的产品网络安全的技术方案的有效实施，车辆网络安全运营的协同应对。

（6）网络安全监控应通过有效的售后流程活动或监控平台，及时有效的识别网络安全事态或事件，积极应对，降低网络安全事件发生的概率或影响。

2．SUMS 软件更新管理体系建设

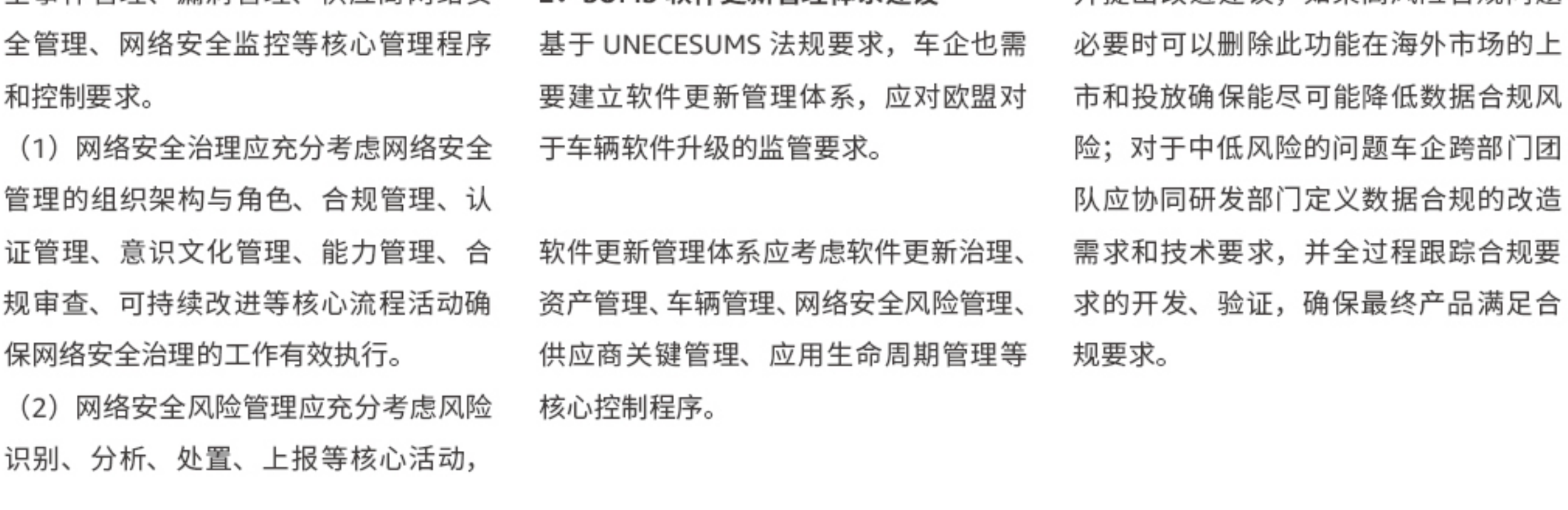
基于 UNECESUMS 法规要求，车企也需要建立软件更新管理体系，应对欧盟对于车辆软件升级的监管要求。

软件更新管理体系应考虑软件更新治理、资产管理、车辆管理、网络安全风险管理、供应商关键管理、应用生命周期管理等核心控制程序。

车企建立软件更新管理体系可以适当的结合业务实际情况，考虑与网络安全管理体系的融合。网络安全管理体系与软件更新管理体系在核心控制程序中存在重叠，通过体系融合，降低运营成本和精简体系业务架构，提高体系运营效率。

3. 智能网联车辆的个人数据保护合规 (EDPB 车联网个人数据保护指南)

基于车辆产品层面个人数据保护合规的要求，车企的相关业务部门包括法务合规，研发，IT 等团队应主动积极关注海外市场当地的数据保护合规要求和实践指南，及时有效的进行产品合规影响分析，例如针对 EDPB 列举的场景和其他车辆场景，进行个人信息数据流盘点和隐私影响风险，识别现有数据合规问题并提出改进建议，如果高风险合规问题必要时可以删除此功能在海外市场的上市和投放确保能尽可能降低数据合规风险；对于中低风险的问题车企跨部门团队应协同研发部门定义数据合规的改造需求和技术要求，并全过程跟踪合规要求的开发、验证，确保最终产品满足合规要求。



高科技行业

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分析，为消费者提供“精准推荐”、“个性化广告”，虽然一定程度上为消费者带来便利，但随着我国的个人信息保护宣传，消费自身者对个人隐私意识的不断提高，这种便利也成为困扰，更甚会碰到某些企业采用“大数据杀熟”的行为，“杀熟”的形式，主要有三种表现：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有反自动化决策权，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，尤其是不歧视、言论自由和信息自由的人权要求，在高度强调人文精神的现代社会里，需要更广泛地考虑人权的需求。但是自动化决策具有过度依赖数据的缺点，自动化决策所依靠的数据来自广泛获取的个人数据，而这些数据可能本身就包含个人或社会成见，导致基于偏见数据所做出的自动化决策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。值得关注，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》对大数据杀熟有比 GDPR 更明确的规定，起要求“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。”

最小化原则

最小化原则在“信息安全领域”由来已久，要求在履行工作职责和职能的安全主体，在法律和相关安全策略允许的前提下，对受到保护的敏感信息仅能在一定范围内被共享，即俗称的知所必须 (need to know) 原则。该原则在个人信息保护领域中具有相似的应用，并赋予对个人信息采集和处理的要求。国内 GB/T 35273-2020《个人信息安全规范》定义个人信息安全基本原则为：只处理满足个人信息主体授权同意目的所需最少个人信息类型和数量。目的达成后，应及时删除个人信息。

自 2018 年欧盟 GDPR 正式施行以来，“最小化原则”被认为是个人信息采集和利用的底线，GDPR 在个人数据处理的原则中强调充分、相关和以该个人数据处理目的最小必要为限度进行处理。另外，在数据系统保护和默认保护中，要求数据控制者应当实施相应的技术和组织措施以确保在默认 (by default) 情形下，被处理的个人数据对每个特定处理目的都是必要的。该最小必要义务适用于被收集的个人数据的数量、处理规模、存储期限与其可访问性。

对于企业后端个人信息保护最小化治理主要体现在产品开发和数据使用，一是 APP 或业务产品开发引入隐私设计理念。APP 在开发过程会进行隐私设计的考量，其中包含最小原则。产品在设计之初就会定义为满足功能所最少必要的个人信息类型，并尽可能让个人信息在 APP 端侧本地处理，如果需要回传，采集和回传的频率也按照实现业务的最少必要频率进行定义，产品上线前会开展隐私影响性分析评估（DPIA），以确认产品是否满足相关个人信息保护的合规要求；二是个人信息数据的良好治理便于数据及时删除。企业通过对个人数据进行充分识别和分类存储，可有效实现个人数据在与用户隐私声明约定的使用期限期满之后自动索引进行删除或通过去连接化处理使数据条目变为匿名化数据。

高科技行业

技术出口

我国已施行的《中华人民共和国数据安全法》中明确了数据出口管制的要求，其第二十五条提到“国家对与维护国家安全和利益、履行国际义务相关的属于管制物项的数据依法实施出口管制”。而具体哪些数据涉及受到出口管制，我们可以通过在去年 2020 年 12 月 1 日施行的据《中华人民共和国出口管制法》及在同年 8 月份，我国首次调整的《中国禁止出口限制出口技术目录》中找到答案。值得注意的是这份“目录”的调整体现的核心精髓是“规范技术出口管理，促进科技进步和对外经济技术合作，维护国家经济安全”。由于我国自 2008 年修订目录 12 年来，国家安全观不断深化，而且很多领域技术也取得突飞猛进发展，对有的技术继续禁止或限制意义已经不大，但同时一些新技术不断涌现，因此某些前沿技术可能会对国家安全、社会公共利益或公共道德产生一些影响，因此纳入了管理目录。

2020 年我国某巨头短视频互联网企业因海外业务受到当地国家政府以“国家安全”为由，要求其在有限的时间内剥离该企业在海外的业务品牌，但由于修订后的“目录”在限制出口部分，新增的第 21 条关于“基于数据分析的个性化信息推送服务技术”、第 18 条关于“人工智能交互界面技术”等控制要求，导致该海外交易被迫中止。

企业应如何应对，技术出口分自由、限制和禁止三类。企业在进行上述技术交易前先比对“目录”自评估所出口技术是否涉及其中，另外考虑出口管制国家的问题，如果对外销售国家涉及其它发达国家的国家安全，应考虑建立黑名单机制，禁止向一些地区和国家进行技术出口。如果上述两项评估均无合规风险，填写《中国限制出口技术申请书》，报送省级商务主管部门进行申请，按技术出口流程执行相关审批申报。

另外，该《中华人民共和国数据安全法》的第二十五条，还衔接《网络安全审查办法》，通过制定数据安全审查制度进一步针对涉及国家安全数据的入境与离境活动实施审查机制。在今年 6 月份，某大型互联网智慧出行企业低调赴美上市，由于受到群众举报疑似涉及转移中国用户数据及将中国道路地图卖给美国。在 7 月初，国家网络安全审查办公室立即采取紧急行动，对该企业启动网络安全审查并发出公告，该公告显示为防范国家数据安全风险，维护国家安全，保障公共利益，依据《中华人民共和国国家安全法》《中华人民共和国网络安全法》，网络安全审查办公室按照《网络安全审查办法》，对该企业实施网络安全审查。并为配合网络安全审查工作，防范风险扩大，审查期间将该企业 APP 停止新用户注册，仅在约 1 周内，国家互联网信息办公室发布通报将该企业旗下的 25 款 APP 立即下架，下架原因为存在严重违法违规收集使用个人信息问题，并且各网站、平台不得为该 25 款已在应用商店下架的 App 提供访问和下载服务。虽然该事件在本文发稿前仍没有最终定论，但此次监管动作也反映国家对可能影响国家安全的数据出口行为是采取坚决的态度，建议各企业应以此为鉴，在出海前将数据出口事项作为合规评审之一，落实数据出口的自查自评工作。

高科技行业

儿童隐私

儿童隐私是世界各国隐私保护法关注的重中之重，以美国 " 儿童在线隐私保护法 " COPPA 作为行业内相对严格的标准，在收集儿童个人信息前需要获得父母或者监护人的同意，且该法律补充说明了具体认可的操作方案：

1. 提供一份由家长签字并通过美国邮政、传真或电子扫描返回的同意书（“打印并发送”方式）；

2. 要求母公司在进行货币交易时使用信用卡、借记卡或其他在线支付系统，该系统向主要账户持有人提供每项独立交易的通知；

   在通知中询问账号持有人：1. 是否是儿童监护人 2. 是否同意收集信息；

3. 让家长拨打由受训人员提供的免费电话号码，或通过视频会议与受训人员联系；

4. 通过核对政府签发的身份证明表格，对照数据库核实父母的身份，前提是你在完成核实后立即删除父母的身份证明；

5. 要求父母回答一系列基于知识的挑战性问题，这些问题对父母以外的其他人来说很难回答，这是委员会根据常见问题中规定的程序单独批准的；

6. 验证家长提交的其他照片 ID 的驾照照片，然后使用面部识别技术将该照片与家长提交的第二张照片进行比较，这是委员会根据常见问题 I.12 中规定的程序单独批准的；

7. 在合理的时间延迟后，通过家长的在线联系信息发送另一条消息以确认同意。在本确认信息中，您应包括直接通知中包含的所有原始信息，告知家长他或她可以撤销同意，并告知家长如何撤销。

如果您只打算将儿童的个人信息用于内部目的，即您不会将信息披露给第三方或公开，那么您可以使用上述任何方法，或者您可以使用“电子邮件 +”的家长同意方法。“Email plus”允许您请求（在发送到家长在线联系地址的直接通知中）家长在返回消息中表示同意。要正确使用 email plus 方法，您必须在收到家长的消息后采取额外的确认步骤（这是“加号”因素）。确认步骤可以是：

在您向家长发出的初始信息中，要求家长在回复信息中包括电话或传真号码或邮寄地址，以便您随后向家长发出确认电话、传真或信函。

绝大部分国家的隐私法律法规中都要求收集儿童信息时需要获得监护人或者父母的额外同意，建议企业在实际操作中提供多种验证方式，避免存在没有信用卡或者教育程度等因素无法完成智力题，最稳妥的方式就是提供确认函的打印和发送，并且能向监护人或者家长提供身份验证流程，例如提供单独的账号密码，以满足明确验证家长的身份，后续产品功能改变时可以更容易地获取到父母的同意和访问或获取儿童的信息时的身份验证功能。

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。虽然 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”，但其在第 2 条“适用范围”中规定：“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构成个人数据。在 GDPR 中，使用用户画像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特定，而在大数据业务模式中，大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。

中国企业出海所面临的法律法规要求更加严格，近年来针对 Facebook，谷歌等大型科技企业的处罚也佐证了监管对于用户画像使用合规性的重视。

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。

数据跨境流动成为常态，对国家安全、行业安全以及个人隐私安全都产生了深刻影响。从 2018 年欧盟《通用数据保护条例》（General Data Protection Regulation，简称 GDPR）出台以来，各国纷纷加强隐私保护立法，制定数据出境管理规则。

跨境电商业务涉及个人信息广泛、业务所需的系统功能和部署复杂、涉及的第三方供应商和商家众多，如何满足不同地区和国家的隐私保护监管要求，成为企业面临的首要挑战。

用户权利行使

跨境电商企业需识别全球范围内适用的隐私保护与数据跨境的法律法规，不同区域的法律法规对用户权利的定义略有不同，企业应明确其个人信息的存储地点，厘清个人信息所涉及的业务场景，是否与特定用户相关等关键因素。

- **应自动化实现用户权利**

企业应让用户自助行使个人权利，也应要求第三方配合实现用户权利。如提供接口实现用户权利；

- **分享时数据最小化、时间最短、尽可能匿名**

提供给第三方的数据应最小化、尽可能去标识化、尽可能处理完后删除此类数据；能做到匿名，合规风险就很低；

- **应做好数据治理**

企业应先制定数据治理方案，再实施隐私安全合规，以确保数据存储位置，使个人信息删除干净；

- **个人信息包括分析得出数据**

只要与个人相关，都是个人信息，都需要删除，不论如何获得、生成。

隐私技术

跨境电商在各业务环节掌握着大量的用户数据，供应链中所涉及第三方供应商众多导致权责不清晰，在不同的场景使用合适有效的隐私保护技术就变得尤为重要。

- **差分隐私：** 在数据集 (DataSet) 中添加噪声，防止通过逆向工程分析还原个人数据。
- **联合分析：** 各方仅共享分析数据所得洞察而不共享数据本身。
- **同态加密：** 在不解密的条件下对加密数据进行分析并共享。
- **零知识证明：** 用户能够在不透露自身有价值信息的情况下证明自己的合法权益。
- **安全多方计算：** 各参与方对数据进行分析，输出计算结果，并保证任何一方均无法得到除应得的计算结果之外的其他任何信息。

供应链安全

随着供应链、价值链的不断延展，互联网、云计算和大数据的不断渗透，业务模式和技术架构的创新在给企业带来信息共享程度提升的同时，传统意义上安全防范的边界也变得模糊，网络安全的共享共治成为企业应对新态势下的安全挑战的基本理念和要求。

近年来，针对供应链的攻击事件频发，供应链安全是保证跨境电商业务正常开展的基石。

- **合规风险**

企业在全球化扩张的同时，必须识别全球合规性对供应链产生的影响，评估风险与合规性，建立有效的安全治理框架，从基础设施安全、数据安全、隐私保护、开发安全及第三方管理领域对企业进行全面评估，识别风险并制定安全管控措施，提高企业供应链安全防护能力。

• 第三方风险

随着公司与第三方供应商之间的合作需求在供应链生态中不断增长，组织需要建立供应商风险管理能力。由于第三方供应商在企业业务开展过程中承担着复杂且多样的业务承载，从选择供应商开始，企业就需投入资源，对供应商的安全能力进行评估，确保供应商的安全水平满足企业安全要求，同时，企业在在第三方网络风险管理生命周期的每个步骤设置安全指标，开展对第三方风险端到端的安全管控。

• 主动威胁管理

随着针对供应链的外部攻击初年增多，只进行偶尔的、间歇的、以合规为重点的技术安全评估是不够的。企业需要发展自身的信息安全能力，以更快的响应，更有效的工作，更好的保护他们的核心业务。为了实现这一点，他们必须具备成熟的主动威胁管理能力。

通过建立安全运营中心，企业通过持续监控、日志分析、发现信息安全威胁，在事前，事中，事后过程中将保护，监控，预警，响应和分析等控制于一体， 并借助标准化的流程管理实现持续的安全运营。

中国企业出海发展的合规应对建议

a. 管理体系

组织架构

海外的众多隐私法案都在一定的条件下要求有专门的 DPO 负责隐私保护工作。尤其是欧盟 GDPR 中第 39 条和欧盟第 29 条数据保护工作组 2016 年 12 月的《数据保护官指引》（简称《指引》）：

- DPO 需要向服务的企业和企业员工提供 GDPR 数据保护方面的信息和建议；
- 对企业 GDPR 合规以及数据保护方面所做的工作进行监管；
- 对企业 data protection impact assessments(DPIAs) 方面工作的参与和管理；
- 作为沟通渠道同欧洲 GDPR 监管部门保持联系，负责数据外泄的紧急汇报；
- 负责同数据主体沟通和联系，协助实现数据主体的数据权利；
- 客观独立的履行自己的职责，不应因雇主行政命令而影响客观事实和结论；
- 有权限可直接向企业最高管理决策层汇报工作。

其中特别强调的是 DPO 的其他只能不能与 DPO 职能产生利益冲突，也就是说 CEO、CFO、COO、市场总监、IT 总监和 HR 总监等都不合适兼任 DPO。

鉴于中国出海的企业不仅有欧洲市场，也在北美、南美、中东和东南亚各市场都有发展，建议应该按照相应最严厉最全面的要求设立隐私保护组织并任命必要的数据保护官。可以有一个全球的首席隐私保护官，然后在必要的地区分别设立本地隐私保护官。

在整体组织架构上，要充分发挥一二三道防线的作用，尤其是操作层面第一道防线必须充分担责。

流程制度

国内企业往往在内部的流程制度上尤其是安全及隐私保护的流程制度上的建设是有所缺失的。而海外的法规尤其是欧盟的 GDPR 对于流程制度的要求是非常严格的。以下是需要注意的要点：

- 关于各种隐私保护声明的文档（知情权）
- 关于获得数据主体同意的各种文档（同意权）
- 关于受理数据主体各种需求的流程文档（访问权、更正权、异议权、遗忘权、携带权等等）
- 数据处理记录
- 隐私影响评估报告
- 跨境影响评估报告
- 数据泄露事件处理制度及流程
- 各地区数据泄露事件通知模板
- 数据安全生命周期管理政策
- 访问权限管理制度及流程
- 数据留存、销毁制度及流程
- 数据传输、共享制度及流程，相应的标准合同条款
- 隐私设计制度及流程

有基础和条件的情况下，应该将隐私设

计的概念融入以上各个流程制度中，使得隐私设计成为各个流程环节内嵌的一部分。并在产品设计中充分考虑实现。

中国出海企业在逐步成为真正的全球跨国企业的过程中，应具有前瞻性的建立一套将各国各地区的隐私保护合规要求综合考虑进去的可动态更新的隐私保护管理体系，并充分利用各种平台和工具实现自动化智能化的落地。

意识培训

组织架构的落地，流程制度的实施，平台工具的使用最终都是需要人来实现的。员工的隐私保护保护意识培训，尤其是针对一线业务部分的培训尤为关键。海外的合规成本非常高昂，民众的隐私保护意识也非常强，还可能面临政治贸易等因素的挑战。员工有意无意的失误都可能给企业海外业务的拓展带来不可估量的损失。

将隐私保护的意识培训变成公司整体培训体系的一部分并融入考评体系，使其成为每个工作流程环节的一部分，是确保隐私保护管理体系真正落地的必需。

b. 技术平台

亚马逊云科技是一家成熟的云服务提供商，提供诸多基于订阅的基础设施产品，这些产品从美国、澳大利亚、巴西、中国、德国、爱尔兰、日本、韩国和新加坡等全球 25 个区域的数据中心通过互联网按需提供。自成立以来，亚马逊云科技致力于通过快速将新产品交付到客户手中，然后根据客户反馈快速迭代和改进这些产品，保持着定义云计算的创新者的身份。创新的节奏和持续的服务改进是越来越多的组织为其关键任务系统 选择使用亚马逊云科技产品的原因。

类别	产品
计算	Amazon EC2、Amazon EC2 Container Service、Amazon Elastic Beanstalk、Amazon Lambda、Amazon 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 SDK
管理工具	Amazon CloudWatch、Amazon CloudFormation、Amazon CloudTrail、 Amazon Config、亚马逊云科技管理控制台、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 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、Amazon、SNS、Amazon SQS、Amazon SWF
企业生产力应用程序	Amazon WorkSpaces、Amazon WAM、Amazon WorkDocs、 Amazon WorkMail

安全责任共担模型

安全性和合规性是亚马逊云科技和客户的共同责任。这种共担模式可以减轻客户的运营负担，因为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安全性的组件。客户负责管理来宾操作系统（包括更新和安全补丁）、其他相关应用程序软件以及亚马逊云科技提供的安全组防火墙的配置。客户应该仔细考虑自己选择的服务，因为他们的责任取决于所使用的服务、，这些服务与其 IT 环境的集成以及适用的法律法规。责任共担还为客户提供了部署需要的灵活性和控制力。如下图所示，这种责任区分通常涉及云“本身”的安全和云“内部”的安全。

亚马逊云科技负责“云本身的安全” – 亚马逊云科技负责保护运行所有亚马逊云科技云服务的基础设施。该基础实施由运行亚马逊云科技云服务的硬件、软件、网络和设备组成。

客户负责“云内部的安全” – 客户责任由客户所选的亚马逊云科技云服务确定。这决定了客户在履行安全责任时必须完成的配置工作量。例如，Amazon Elastic Compute Cloud (Amazon EC2) 等服务被归类为基础设施即服务 (IaaS)，因此要求客户执行所有必要的安全配置和管理任务。部署 Amazon EC2 实例的客户需要负责来宾操作系统（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，以及每个实例上亚马逊云科技提供的防火墙（称为安全组）的配置。 对于抽象化服务，例如 Amazon S3 和 Amazon DynamoDB，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。

亚马逊云科技云上的隐私保护

客户的信任是亚马逊云科技的第一要务。我们为 240 多个国家和地区的数百万个活跃客户提供服务，包括企业、教育机构和政府机构。我们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给我们，给予我们充分的信任。

我们知道，客户十分注重隐私和数据安全。因此，亚马逊云科技通过简单而强大的工具让您拥有和控制自己的内容，这些工具可以让您确定内容的存储位置、保护动态和静态内容，并为用户管理对亚马逊云科技服务和资源的访问权限。我们还采取了适当和可选的技术和物理控制措施，帮助客户预防其内容被非法访问或披露。

亚马逊云科技持续监控不断变化的隐私监管和立法领域，以识别变更并确定我们的客户可能需要哪些工具来帮助其满足合规性需求，具体取决于他们的应用程序。我们建议在亚马逊云科技和数据保护法规方面有问题的客户和 APN 合作伙伴先联系自己的亚马逊云科技客户经理。注册了企业支持的客户也可以联系自己的技术客户经理 (TAM)。TAM 会与解决方案架构师合作，帮助客户确定潜在的风险和可能的缓解措施。TAM 和客户团队还可以根据客户和 APN 合作伙伴的环境和需求，为其指明特定资源。亚马逊云科技无法提供法律建议，我们建议客户在遇到法律问题时咨询其法律顾问。

维护客户信任是一项持续的承诺。我们力求让您了解我们实施的隐私和数据安全政策、实践和技术。这些承诺包括：

- **访问：**作为客户，您可以完全控制自己的内容，并负责配置对亚马逊云科技服务和资源的访问。我们提供了一系列先进的访问、加密和日志记录功能（例如 Amazon Identity and Access Management、Amazon Organizations 和 Amazon CloudTrail），可以帮助您有效达成这一目标。我们为您提供了 API，以便为您在亚马逊云科技环境中开发或部署的任何服务配置访问控制权限。未经您的同意，我们不会出于任何目的而访问或使用您的内容。我们绝不会出于营销或广告目的而使用您的内容或从中提取信息。

- **存储：**您可以选择存储自己的内容的亚马逊云科技区域以及存储类型。您可以在多个亚马逊云科技区域中复制和备份您的内容。未经您的同意，我们不会将您的内容移到或复制到您所选择的亚马逊云科技区域之外，除非法律要求或者政府部门发布有约束力的指令要求。

- **安全性：**您可以选择自己的内容的保护方式。我们为您的传输中和静态内容提供行业领先的加密功能，而且您可以选择自行管理自己的加密密钥。这些数据保护功能包括：
  - o 在 100 多种亚马逊云科技服务中可用的数据加密功能。
  - o 使用 Amazon Key Management Service (KMS) 的灵活密钥管理选项，让客户能够选择是让亚马逊云科技管理加密密钥还是自行完全控制密钥。

- **客户内容的披露：**我们不会披露客户内容，除非法律或者政府机构具约束力的指令有此要求。如果政府机构向亚马逊云科技发送客户内容的要求，我们将尝试重定向政府机构，以直接向客户要求提供数据。如果我们被迫向政府机构披露客户内容，我们将向客户发出合理的通知，以便客户可以寻求保护令或其他适当的救济，除非法律禁止亚马逊云科技这样做。

- **安全保证：**我们制定了一项安全保证计划，使用全球范围内的隐私和数据保护最佳实践来帮助您在亚马逊云科技内安全运行，并充分利用我们的安全控制环境。这些安全保护和控制流程分别通过多个第三方独立评估进行了验证。

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。在亚马逊云科技隐私保护页面上我们可以看到全球各地主要的隐私保护洞见。

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

亚马逊云科技云上的合规计划

亚马逊云科技合规计划可以帮助客户了解亚马逊云科技用于维护亚马逊云科技云中安全性和实施数据保护的强大控制措施。如果系统是在亚马逊云科技云中构建的，那么双方将共同承担合规性责任。通过将以治理为中心、便于审计的服务功能与适用的合规性或审计标准结合起来，亚马逊云科技合规性工具（如 Amazon Config、Amazon CloudTrail、Amazon Identity and Access Management、Amazon GuardDuty, Amazon Audit Manager 和 Amazon Security Hub）基于传统流程构建，可以帮助客户建立亚马逊云科技安全控制环境并在该环境中运营。亚马逊云科技为客户提供的 IT 基础设施的设计和管理方式符合安全性最佳实践和一系列 IT 安全标准，包括：

- SOC 1/SSAE 16/ISAE 3402（以前是 SAS 70）
- SOC 2
- SOC 3
- FISMA、DIACAP 和 FedRAMP
- DoD SRG
- PCI DSS 1 级
- ISO 9001/ISO 27001
- ITAR
- FIPS 140-2
- MTCS 3 级

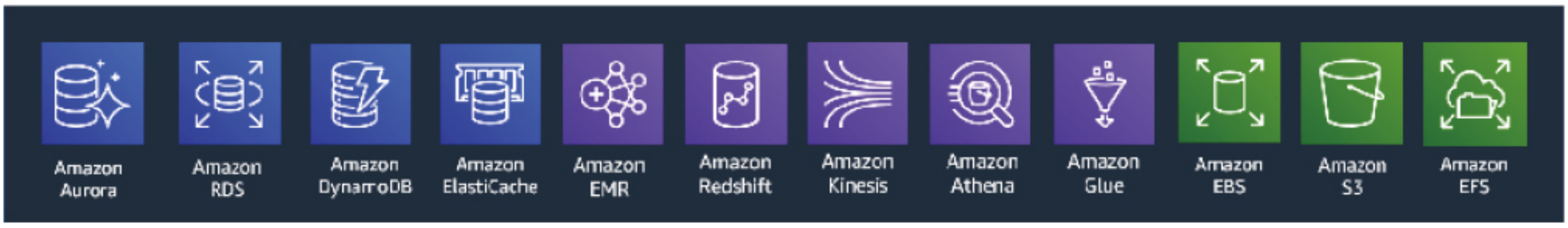
此外，亚马逊云科技平台提供的灵活性和控制让客户可以部署符合多项行业特定标准的解决方案 。亚马逊云科技通过白皮书、报告、认证、评估认证和其他第三方证明向客户提供与 IT 控制环境相关的各种信息。有关更多信息，请参阅亚马逊云科技：风险与合规性白皮书。

亚马逊云科技云上的数据安全

亚马逊云科技提供很多安全服务，帮助客户实现云端的数据安全，以帮助满足各类数据保护与隐私保护相关的合规。这些服务涵盖数据访问的数据资产识别与发现、身份与权限管理、数据加解密、探测与分析、响应与处置、持续合规检查等几个方面。

数据资产的识别与发现

云上的数据可能分布在关系型数据库类，非关系型数据库类，大数据分析类，数据仓库类，存储类等服务中，如下图列举了各类具体的服务：



我们可以通过 Amazon Config 发现云端的数据资产，并作配置管理和变更管理。Amazon Config 服务可供客户评估、审计和评价亚马逊云科技云上的资源配置。Amazon Config 持续监控和记录云上资源配置，并支持自动依据配置需求评估记录的配置。借助 Amazon Config，客户可以查看配置更改以及 云上资源之间的关系、深入探究详细的资源配置历史记录并判断您的配置在整体上是否符合内部指南中所指定的配置要求。这样客户能够简化合规性审计、安全性分析、变更管理和操作故障排除。

Amazon Macie 是一项完全托管的数据安全和数据隐私服务，它利用机器学习和模式匹配来发现和保护云中的敏感数据。随着组织管理越来越多的数据，大规模地识别和保护它们的敏感数据会变得越来越复杂、昂贵和耗时。Amazon Macie 可以大规模自动发现敏感数据，同时降低保护数据的成本。Amazon Macie 会自动提供 Amazon S3 存储桶的清单，包括未加密的存储桶、可公开访问的存储桶以及与云账户共享的存储桶的列表，其中这些账户不属于客户在 Amazon Organizations 中定义的账户。然后，Amazon Macie 将机器学习和模式匹配技术应用于您选择的存储桶，以识别敏感数据，并向您发出警报，例如个人身份信息 (PII)，医疗健康数据，信用卡信息等金融数据以及亚马逊云科技云上的 AK/SK 等 Credential 数据。 同时，客户可以在管理控制台中搜索和筛选 Amazon Macie 的警报或调查结果，并将其发送到 Amazon EventBridge（前称 Amazon CloudWatch Events），以便轻松与现有工作流程或事件管理系统集成，或与 亚马逊云科技其他服务（例如 Step Functions）结合使用，以执行自动修复操作。这可以帮助您满足法规要求，例如《健康保险携带和责任法案》(HIPAA) 以及《通用数据隐私条例》(GDPR)。

身份与权限管理

云上的数据访问，需要有合理的使用账号管理与权限控制。身份管理服务 IAM 和目录服务 Directory Service 可以帮助客户在云上建立和管控对数据访问的权限管理。

Amazon Identity and Access Management (IAM) 使客户能够安全地管理对亚马逊云科技服务和资源的访问。客户可以使用 IAM 创建和管理亚马逊云科技用户和组，并使用各种权限来允许或拒绝他们对亚马逊云科技资源的访问。

借助 Amazon IAM，客户能够控制对亚马逊云服务 API 和特定资源的访问。这类控制能力已经达到了操作级别，也就是对云资源的操作权限，都可以通过 Amazon IAM 的策略控制权限。在 Amazon IAM 的访问策略中添加特定的条件（例如时间，IP 等），以控制用户使用 云服务的方式、其来源 IP 地址、是否使用 SSL，或是否通过多重验证设备进行身份验证。

IAM 还允许创建角色。通过角色定义一组权限，然后让通过验证的用户或 EC2 实例承担这些角色，通过授予对定义资源的临时访问权限改善安全状况。

IAM 支持多因子身份认证 MFA ，提供除用户名称和密码凭证外的更多的验证方式来保护客户的亚马逊云科技云环境。

通过 Amazon IAM，客户还可以使用现有的身份验证系统（如 Microsoft Active Directory）向员工和应用程序授予对云管理控制台和云服务 API 的联合访问权限。使用任何支持 SAML 2.0 的身份管理解决方案都可以实现这类功能。

Amazon IAM Access Analyzer 功能，可以帮助客户分析其账号的用户访问权限使用情况。Amazon IAM 访问分析器提供超过 100 个策略检查，可帮助您在策略编写期间主动验证策略。这些检查将分析您的策略并报告错误、警告和建议，并提供指导您设置安全和功能权限的可行建议。Amazon IAM 访问分析器还可使您在部署权限更改之前验证对资源的公有访问权限和跨账户访问权限。您可以在 Amazon S3 控制台中或使用 Amazon IAM 访问分析器 API 预览访问权限。当客户需要实施最小权限原则时，最大的困难是如何确定当前使用的权限是最小的并且是够用的，Amazon IAM 访问分析器可以帮助您检查现有的访问，从而使您能够识别和删除意外的外部权限或未使用权限。为了使您能够识别具有公有或跨账户访问权限的资源，Amazon IAM 访问分析器生成全面的结果，访问分析器持续监控新资源策略或更新资源策略，并分析针对 Amazon S3 存储桶、Amazon KMS 密钥、Amazon SQS 队列、Amazon IAM 角色、Amazon Lambda 函数和 Amazon Secrets Manager 授予的权限。为了帮助您删除未使用的权限，Amazon IAM 还会提供最后一次访问的信息，以指定 Amazon IAM 实体最后一次使用服务或操作的时间。这可以帮助您轻松识别和删除未使用的权限，从而减少访问，并帮助您设置权限边界。

数据加解密

亚马逊云科技云上数据加解密是保证数据的重要手段，其中包括对保存在各种存储和数据库中的静态数据加密和对传输的动态数据进行加密。

Amazon Key Management Service (KMS) 可让您轻松创建和管理加密密钥，并控制其在各种云服务和应用程序中的使用。Amazon KMS 是一种安全且有弹性的服务，它使用已经过 FIPS 140-2 验证或正在验证的硬件安全模块来保护您的密钥。Amazon KMS 还能与 Amazon CloudTrail 集成，从而为您提供所有密钥的使用记录，帮助您满足监管和合规性要求。

Amazon KMS 与 Amazon Encryption SDK 集成，使您可以使用受 Amazon KMS 保护的数据加密密钥在应用程序中进行本地加密。使用简单的 API，您还可以在自己的应用程序中构建加密和密钥管理，无论应用程序在何处运行。

Amazon KMS 与亚马逊云科技云服务集成，可简化密钥使用以加密亚马逊云科技工作负载中的数据。客户可以选择所需的访问控制级别，包括在账

户和服务之间共享加密资源的能力。Amazon KMS 会将密钥的所有使用记录到 Amazon CloudTrail，以便为您提供访问加密数据的用户的独立视图，包括代表您使用这些数据的亚马逊云科技服务。

Amazon CloudHSM 是基于云的硬件安全模块 (HSM)，让您能够在亚马逊云科技云上轻松生成和使用自己的加密密钥。借助 Amazon CloudHSM，您可以使用经过 FIPS 140-2 第 3 级验证的 HSM 管理自己的加密密钥。Amazon CloudHSM 让您可以灵活选择使用行业标准的 API 与应用程序集成，这些 API 包括 PKCS#11、Java 加密扩展 (JCE) 和 Microsoft CryptoNG (CNG) 库等。此外，Amazon CloudHSM 符合标准，让您可以将所有密钥导出到大多数其他商用 HSM，具体取决于您的配置。它是一项完全托管的服务，可为您自动执行耗时的管理任务，例如硬件预置、软件修补、高可用性和备份。借助 Amazon CloudHSM，您还能够通过按需添加和删除 HSM 容量进行快速扩展和收缩，无任何预付费用。

针对传输中的数据，亚马逊云科技云上提供的 Amazon Certificate Manager 可帮助您轻松地预置、管理和部署公有和私有安全套接字层 / 传输层安全性 (SSL/TLS) 证书，以便用于亚马逊云科技服务和您的内部互联资源。SSL/TLS 证书用于保护网络通信的安全，并确认网站在 Internet 上的身份以及资源在私有网络上的身份。使用 ACM，您无需再为购买、上传和续订 SSL/TLS 证书而经历耗时的手动流程。利用 ACM，您可以快速请求证书，在与 ACM 集成的服务（例如 Amazon Elastic Load Balancer、Amazon CloudFront 分配和 Amazon API Gateway 上的 API）上部署该证书，ACM 可以处理证书续订事宜，并为内部资源创建私有证书并集中管理证书生命周期。通过 ACM 预置的用于 ACM 集成服务的公有和私有证书均免费。您只需为您创建的用于运行应用程序的亚马逊云科技资源付费。

亚马逊云科技加密开发工具包是一个客户端加密库，旨在让每个人都可以使用行业标准和最佳实践轻松加密和解密数据。它使您能够专注于应用程序的核心功能，而不是关注如何最好地加密和解密数据。亚马逊云科技 加密开发工具包是根据 Apache 2.0 许可证免费提供的。

使用亚马逊云科技加密开发工具包，您可以定义主密钥提供程序（Java 或 Python）或密钥环（C 或 JavaScript），用于确定用于保护数据的主密钥。然后，您可以使用亚马逊云科技加密开发工具包提供的直接方法对数据进行加密和解密。其余的是亚马逊云科技加密软件开发工具包。

Amazon KMS 推出了多区域密钥，这项功能允许您将一个区域的密钥复制到其他区域。借助多区域密钥功能，您可以更轻松地在区域之间移动加密数据，同时无需在各个区域使用不同的密钥进行解密和重新加密。使用 Aamzon 加密 SDK、Aamzon S3 加密客户端和 Amazon DynamoDB 加密客户端的客户端侧加密都支持多区域密钥。此功能简化了将受保护的数据复制到多个区域的过程，例如灾难恢复 / 备份、Amazon DynamoDB 全局表或者需要在多个区域使用同一签名密钥的数字签名应用程序。Amazon KMS 可让您轻松创建和管理加密密钥，并控制其在各种亚马逊云科技服务和应用程序中的使用。Amazon KMS 是一种安全且有弹性的服务，它使用经过 FIPS 140-2 验证的硬件安全模块。

探测与分析

Amazon CloudWatch 是一种面向开发运营工程师、开发人员、站点可靠性工程师 (SRE) 和 IT 经理的监控和可观测性服务。Amazon CloudWatch 为您提供相关数据和切实见解，以监控应用程序、响应系统范围的性能变化、优化资源利用率，并在统一视图中查看运营状况。Amazon CloudWatch 以日志、指标和事件的形式收集监控和运营数据，让您能够在统一查看在亚马逊云科技和本地服务器上运行的资源、应用程序和服务。您可以使用 Amazon CloudWatch 检测环境中的异常行为、设置警报、并排显示日志和指标、执行自动化操作、排查问题，以及发现可确保应用程序正常运行的见解。

Amazon GuardDuty 是一种威胁检测服务，可持续监控恶意活动和未经授权的行为，从而保护您的云账户、工作负载和在 Amazon S3 中存储的数据。迁移到云后，账户和网络活动的收集与聚合变得异常简单，但安全团队对事件日志数据进行持续的分析以发现潜在的威胁，则可能十分耗时。Amazon GuardDuty 为您提供了经济高效的智能选项，从而持续检测在亚马逊云科技中发生的威胁。此服务使用机器学习、异常检测和集成威胁情报等手段，识别潜在的威胁并确定优先级别。Amazon GuardDuty 对来自多个亚马逊云科技云上的数据源（例如 Amazon CloudTrail 事件日志、Amazon S3 数据访问日志，Amazon VPC 流日志和 DNS 日志）的数百亿事件进行分析。只需在云管理控制台中几次点击，就可以启用 Amazon GuardDuty，无需部署或维护任何软件或硬件。Amazon GuardDuty 警报与 Amazon CloudWatch Events /Event Bridge 集成，具有极好的可行动性，非常便于跨多个账户聚合，并且可以直接推送到现有的事件管理和工作流程系统。

响应与处置

Amazon Security Hub 可让您全面查看亚马逊云科技云账户中的高优先级安全警报与合规性状态。客户可以任意使用一系列强大的安全工具，从防火墙和端点保护到漏洞和合规性扫描程序。但是，这通常会让安全或运维团队在这些工具之间来回切换，每天处理数百甚至数千个安全警报。借助 Amazon Security Hub，客户现在可以设置单个位置，对来自多个云服务（如 Amazon GuardDuty、Amazon Inspector 和 Amazon Macie），以及来自合作伙伴解决方案的安全警报或检测结果进行聚合、组织和设置优先级。Amazon Security Hub 的检测结果可在具有可操作图形和表格的集成控制面板上进行直观汇总。客户还可以使用自动合规性检查（基于您的组织遵守的亚马逊云科技安全最佳实践和行业标准），持续监控您的环境。Amazon Security Hub 的集成控制面板将所有账户的安全检测结果汇总起来，向您显示当前的安全性与合规性状态。客户可以基于此采取必要的后续步骤。例如，使用与 Amazon CloudWatch Events 的集成，您可以将检测结果发送到开单、聊天、电子邮件或自动修复系统。

同时，围绕 Amazon Security Hub，我们也构建了一个生态，很多安全公司的如防火墙，漏洞发现与管理工具等可以使用 Amazon Security Hub 开放的接口标准，把安全相关的发现和信息发送到 Amazon Security Hub 中。Amazon Security hub 作为云端安全运维管理的集成服务，也可以把发现的威胁与安全风险信息，通过 Amazon CloudWatch Event 或 Amazon Event Bridge 发送到其他安全相关服务中，如通过 Amazon SNS 发送邮件通知相关人员，通过 Amazon Lambda 自动在工单系统中创建工单。通过 Amazon Kinesis 把发现发送到类似 Amazon Splunk 这类 SIEM 平台，调用安全自动化响应的 Amazon Lambda 函数，实现安全的自动化响应。

Amazon Lambda 是一种无服务器的计算服务，让您无需预置或管理服务器、创建可感知工作负载的集群扩展逻辑、维护事件集成或管理运行时，即可运行代码。借助 Amazon Lambda，您几乎可以为任何类型的应用程序或后端服务运

行代码，而且完全无需管理。只需将您的代码以 ZIP 文件或容器映像的形式上传，Amazon Lambda 便会自动、精确地分配计算执行能力，并根据传入的请求或事件运行您的代码，以适应任何规模的流量。您可以将您的代码设置为自动从 200 多个亚马逊云科技服务和 SaaS 应用程序触发，或者直接从任何 Web 或移动应用程序调用。您可以使用自己喜欢的语言（Node.js、Python、Go、Java 等）编写 Lambda 函数，并使用无服务器和容器工具（例如 Amazon SAM 或 Docker CLI）来构建、测试和部署您的函数。Amazon Lambda 通过和 Amazon Security Hub，Amazon CloudWatch 或 Amazon Event Bridge 集成，可以实现安全的自动化响应。

持续合规检查

Amazon Audit Manager 帮助持续审计客户在亚马逊云上的资源和服务的使用情况，以简化评估风险以及针对相关法规与行业标准的合规性的方式。Amazon Audit Manager 将证据收集自动化，减少审计时经常发生的需要全部人员投入的手动操作， Amazon Audit Manager 会帮助您管理利益相关者对您的控件的审核，让您能够创建审计就绪报告，且大幅减少手动操作。Amazon Audit Manager 的预构建框架通过将您的云上资源映射到行业标准或法规的要求，帮助把来自云服务的证据转换成对审计员友好的报告，此类行业标准或法规如下列表所示，该列表还在不断更新中。

- Amazon Audit Manager Sample Framework
- Amazon Control Tower Guardrails
- Amazon License Manager
- Amazon Foundational Security Best Practices
- Amazon Operational Best Practices (OBP)
- Amazon Well-Architected
- CIS Benchmark for CIS Amazon Web Services Foundations Benchmark v1.2.0
- CIS Benchmark for CIS Amazon Web Services Foundations Benchmark v1.3.0
- CIS Controls v7.1 Implementation Group 1
- FedRAMP Moderate Baseline by Allgress
- GDPR
- GxP 21 CFR part 11
- GxP EU Annex 11
- HIPAA
- HITRUST v9.4 Level 1
- NIST 800-53 (Rev. 5) Low-Moderate-High
- NIST Cybersecurity Framework version 1.1
- NIST SP 800-171 (Rev. 2)
- PCI DSS v3.2.1
- SOC 2

客户还可以针对自己的特别业务要求完全自定义框架及其控件。基于您所选择的框架，Amazon Audit Manager 会启动评估，持续从亚马逊云科技云账户和资源收集与整理相关证据，如资源配置快照、用户活动和合规性检查结果等。在管理控制台中启用框架后 Amazon Audit Manager 自动开始收集和整理证据。

数据分析中的安全

亚马逊云科技的数据分析服务，主要在数据湖，数据仓库等上面，其中数据湖又是各个行业用户以及跨国公司重要的分析工具。

亚马逊云科技云上数据湖的安全主要分为两个方面：一个是数据本身的安全，另一个是访问权限的安全。企业无论是为了内部合规还是符合外部监管，会有对于当前收集到的数据做分级。一些关乎客户个人信息的数据可能会被分类为 PII 高度敏感数据如姓名、身份 ID、电话等，需要最高级别的安全管控。亚马逊云科技的分析服务提供各种安全功能来帮助客户实现对数据安全的需求。

传输中加密

数据从客户端到服务器端加密可以更好

的保证传输过程中不被篡改和窃取。大数据服务一般是集群模式以保证大数据量下的计算性能，集群节点之间的数据传输也非常的频繁。集群节点间的传输加密也很重要。

亚马逊云科技的大数据托管服务全部提供传输中间加密的功能：Amazon EMR、Amazon Redshift、Amazon Elasticsearch、Amazon Kinesis、Glue、Amazon Athena、Amazon QuickSight、Amazon Managed Streaming for Apache Kafka

数据存储加密

数据存储在云上，要保证数据不被窃取则需要数据存储加密。亚马逊云科技的托管服务提供多种不同的数据存储加密方式以满足不同数据分级的要求。不同的服务支持的数据存储加密种类会不同，具体请参照服务的加密选项。

例如 Amazon EMR 的存储加密选项 https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-data-encryption-options.html

访问控制

大数据服务会有很多终端用户访问，不同用户的访问级别不同，需要表级别的访问控制的机制来满足安全合规需求。所有大数据服务都使用 Amazon IAM 的细粒度权限管理可以管理用户在 API 级别的操作权限，Amazon Lakeformation 可以提供基于 Amazon Glue、Amazon Athena、Amazon EMR 数据湖之上 Amazon S3 数据存储、表级别、字段级别和行级别的细粒度权限控制。其他服务如 Amazon Redshift、Amazon Elasticsearch、Amazon QuickSight 都提供类似的用户权限体系细粒度的管理用户访问权限。

机器学习的安全

Amazon SageMaker 通过整合专门为机器学习构建的广泛功能集，帮助数据科学家和开发人员快速准备、构建、训练和部署高质量的机器学习 (ML) 模型。Amazon SageMaker 使用专用工具为机器学习开发的每个步骤加速创新，包括标签、数据准备、功能工程、统计偏差检测、自动机器学习、训练、调优、托管、可解释性、监控和工作流。作为托管服务，Amazon SageMaker 自动继承亚马逊云科技的全球基础设施及其网络安全功能。Amazon SageMaker 还提供全面的功能集，因此客户可以运行机器学习工作负载灵活而安全的机器学习环境今天可用。Amazon SageMaker 的安全功能很容易满足客户面临的数据安全与合规的挑战。

基础架构和网络安全：控制跨越的数据流量，Amazon SageMaker 组件超过私人网络。确保合适单租户的入口 / 出口，所以你的数据和资源是安全的。

认证与授权：定义、执行和审谁可以进行身份验证并授权使用 Amazon SageMaker 资源。

数据保护：获取灵活的，自动的加密能力，包括对数据静态和传输中的数据，支持自带密钥。

监控与审计：跟踪、跟踪和审核所有 API 调用、活动、数据访问、和互动直至用户和 IP 级别。

合规：继承最多全面的合规控制并轻松与客户所在行业的监管要求。

第三方解决方案

亚马逊云科技在云市场 Marketplace 上，已经为客户提供了来自大量本土安全厂商和国际安全公司提供的有数百种产品，其中有大量的安全产品，包括主机安全，网络安全，数据安全，安全运维，合规检查，网络等级保护等。同时中国区 Marketplace 也支持 SaaS 化的安全方案的部署。

致谢

编写指导

德勤中国：薛梓源 江玮 张震 石沛恩 阎光 林松祥

亚马逊云科技：顾凡 王晓野 江学森

主编人员

德勤中国：须文东 何智聪 申燕茹 傅栌峰 李颖 王嘉晖 屈俊

亚马逊云科技：韩旭明 贺浏璐

协助编辑

亚马逊云科技：王焘 张亮 李昕 吴佳敏