DHGATE 敦煌网集团

CCIE 中国互联网经济研究院 China Center for Internet Economy Research

亚马逊云科技

Kaamel

# INSIGHT REPORT

# 跨境电商隐私合规白皮书

## Cross-border e-commerce privacy compliance white paper

# 目录

# 引言

作为全球贸易新旧动能转换的重要组成部分，跨境电子商务逐步成为推动经济增长和新旧动能转换的关键动力。国家发改委在 2022 年发表的《大力推动我国数字经济健康发展》分析文章中明确提出我国要“大力发展跨境电商，打造跨境电商产业链和生态圈。”

近十年，国内的互联网快速发展，同样的模式复制到出海场景，尤其是跨境电子商务，水土不服现象频发。一方面，爆点事件频发，引发各国、各区域的隐私合规意识提升；另一方面，各国、各区域内部，国与国之间、区域与区域之间的科技、互联网发展速度差异，为保护各自在数字经济国际竞争中的主动地位，各国各区域已经或纷纷立法，保护数字隐私。

科技创新催生业务创新，业务创新带动科技创新，DNA 双螺旋模式驱动数字经济高速发展。数据就是构成这个 DNA 双螺旋的基本元素，数据在电子商务和数字经济中日益重要的作用。数据驱动的经济为创造财富和应对发展挑战带来了新的机遇，但也引发了与数据隐私和安全、跨境数据流动、市场集中度和税收等相关的各种潜在关切。

随着数字经济的高速发展，在各个行业，各个企业，各个机构，各国各区域政府都汇集了海量的大数据，数据湖技术应运而生、应运而蓬勃发展。这些数据湖可以被挖掘和分析，以找出本来隐藏不显的模式和相关性。其结果可被输入到某些系统中，这种系统使用人工智能、机器学习和自动化决策以升级系统元素甚至整个系统。由阿里巴巴、亚马逊、苹果、 Facebook、谷歌、微软、 SAP、腾讯等公司运营的平台，已经将大数据作为商业模式的核心。监管机构、监管人员和消费者越来越多地关注安全、隐私和个人数据的所有权及其使用影响。

本文旨在更好帮助跨境电商产业把握发展机遇，将挑战转化为内生动力，规范企业运营，行业标准，甚或治理建议。在此背景下，纵观全球合规过去、现在和未来，第一章探讨了隐私合规的价值。第二章阐述了隐私合规的困境。第三章讨论了隐私合规趋势。第四章探讨了隐私合规的实践。第五章给出了跨境电商行业建议。

# 一. 隐私合规的价值

## （一）隐私合规概念界定

### 1. 数据定义

“数据”是指任何以电子或者其他方式对信息的记录。

### 2. 隐私数据定义

本文隐私数据，涵盖个人数据、个人信息、敏感数据等定义（各国各区域立法称呼不同），我们对比分析以下主要法域对隐私数据的定义：

欧盟《通用数据保护条例》[1]（GDPR）第四条规定，“个人数据”指的是任何已识别或可识别的自然人（数据主体）相关的信息；一个可识别的自然人是一个能够被直接或间接识别的个体，特别是通过诸如姓名、身份编号、地址数据、网上标识或者自然人所特有的一项或多项的身体性、生理性、遗传性、精神性、经济性、文化性或社会性身份而识别个体。

《加州消费者隐私法》[2]（CCPA）《加州隐私权法案》（CPRA）规定，**个人信息**是指直接或间接地识别，关联，描述，或能够合理地联系到一个特定的消费者或家庭的信息。包括但不限于：

a. 标识符：真实姓名；昵称；邮寄地址；电子邮箱；唯一个人或网络标识符；IP 地址；账 户名；社保号码；驾照或护照号码；其他持续的或可能性的标识符用于标识一个特定消费者，家庭或设备；

b. 1798.80 条款中定义的个人信息： 个人签名；州身份证件号码；身体特征或描述；保险单号码；教育信息；就业信息；银行账号，信用卡号，借记卡号以及其他的财务信息；医疗信息或医疗保险信息；

c. 受加州或联邦法律保护的特征信息，例如种族，国籍，宗教，性别，性取向；

d. 交易信息：包括个人资产记录，购买的商品和服务，其他购买或消费的记录以及倾向；

e. 生物计量信息：包括基因，心理，行为以及生物特征，可提取模型的行为模式信息，或其他标识符信息，例如：指纹，人脸模型，声纹；虹膜、视网膜扫描；笔迹，步态或其他物理模型；睡眠，健康或活动信息；

f. 网络活动信息：浏览历史，搜索历史，或消费者与网站，应用或广告的交互信息；

g. 地理位置信息；

h. 声音，电的，视觉，热感，嗅觉或其他类似的信息；

i. 职业或就业相关的信息；

j. 非公开的教育信息；

k. 基于任何以上信息的推测建立的画像信息，反映特定消费者的喜好、特征、心理趋向、倾向、行为、态度、智力、能力和天赋等。

注：个人信息不包括公开信息，公开信息是指可以从联邦、州或当地政府记录中获取的信息。

《中华人民共和国民法典》第一千零三十四条规定 自然人的个人信息受法律

[1] 《通用数据保护条例》（General Data Protection Regulation，简称 GDPR）为欧洲联盟的条例，前身是欧盟在 1995 年制定的《计算机数据保护法》。2018 年 5 月 25 日，欧洲联盟出台《通用数据保护条例》

[2] CCPA，即 2018 年颁布并于 2020 年 1 月 1 日生效的《加州消费者隐私法》。CPRA，即《加州隐私权法案》，于 2023 年 1 月 1 日生效。这是两部关于保护加州居民个人信息的立法。它们旨在加强个人隐私权，提高企业对消费者个人信息的保护水平。CCPA 的出台旨在加强加州消费者隐私权和数据安全保护，被认为是美国当前最严格的消费者数据隐私保护立法

保护。

个人信息是以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人的各种信息，包括自然人的姓名、出生日期、身份证件号码、生物识别信息、住址、电话号码、电子邮箱、健康信息、行踪信息等。

个人信息中的私密信息，适用有关隐私权的规定；没有规定的，适用有关个人信息保护的规定。

《中华人民共和国个人信息保护法》第四条规定： 个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。其中“匿名化”是指个人信息经过处理无法识别特定自然人且不能复原的过程。

**3. 地域间界定方法和概念差异**

从 GDPR、CCPA、中国的《个人信息保护法》以及《民法典》中关于个人信息的定义来看，虽然都致力于保护自然人的个人信息权益，但具体的界定方法、概念的内涵存在差异。

首先，GDPR 和中国的《个人信息保护法》在定义上较为类似，都致力于保护所有可识别和已识别的自然人相关的个人信息。具体包括个人身份信息，如姓名、地址、身份证号码等；个人偏好信息，如购物习惯、浏览记录等；以及个人的网络身份信息，如用户名、密码等。同时，二者都将匿名化信息排除在个人信息保护范围之外。

相比之下，CCPA 则采用定义、列举、排除并行的方法对个人信息进行界定，它更强调“合理性”。具体来说，CCPA 规定下的个人信息包括：识别信息（如姓名、地址、电话号码等）、健康信息、财务信息等。同时，CCPA 也明确排除了一些不适用的信息类型，例如：公开信息、匿名信息等。值得注意的是 CCPA 排除适用的信息类型远多于 GDPR 与《个人信息保护法》。

综上所述，GDPR、CCPA、中国的《个人信息保护法》以及《民法典》都对个人信息保护做出了规定，虽然具体界定方法和概念内涵存在差异，但都以保护自然人的个人信息权益为主要目标。

**4. 隐私数据泄露**

GDPR 规定，个人数据泄露是指数据处理者意外或非法破坏、丢失、更改、未经授权的披露或访问传输、存储或以其他方式处理的个人数据。在无正当理由的情况下将个人数据传输到不被授权接收这些数据的第三方。这种泄露可能会导致个人隐私的侵犯，给个人带来不利的后果。GDPR 强调了数据处理者的责任，要求其采取适当的措施来保护个人数据的安全。

CCPA 规定，个人数据泄露是指未经授权获取计算机化信息，损害了个人信息的安全性、保密性或完整性，但不包括某些善意取得。未经授权的访问、获取、使用、披露、修改或破坏个人信息的行为。与 GDPR 相比，CCPA 的定义更加具体，涵盖了更多的情况。此外，CCPA 还强调了个人数据的可识别性，即使数据经过处理或匿名化，只要能够重新识别个人身份，仍属于个人数据。

中国的《民法典》规定，个人信息受到法律保护，任何组织或者个人不得以刺探、侵扰、泄露、公开等方式侵害他人的隐私权。个人信息包括自然人的姓名、出生日期、身份证件号码、生物识别信息、住址、电话号码等。《民法典》没有关于个人数据泄露的具体定义，但其规定了隐私权的概念和保护措施。

中国的《个人信息保护法》第五十一条规定，个人信息处理者应采取措施确保个人信息处理活动符合法律、行政法规的规定，并防止未经授权的访问以及个 人

信息泄露、篡改、丢失因自身管理不善或者疏漏导致个人信息发生泄露的情形是信息泄露。此规定注重个体权益的保护，并给个人信息处理者提出了相应的处理措施建议。关注规避侵犯个人信息权利的潜在人员构成以及个人信息内容类型并给予解决相关争议的途径和方向。

**5. 隐私合规**

GDPR 规定，隐私保护是指个人数据的处理过程不得侵犯自然人的基本权利，包括个人数据的收集、使用、存储、传输、处理等环节。GDPR 强调了数据处理者对个人数据的责任，要求他们采取适当的措施来保护个人数据的安全，包括但不限于加密、匿名化等。此外，GDPR 还规定了隐私保护的最低标准，包括数据处理者在收集、使用个人数据时必须告知个人数据的处理目的、范围、是否与第三方共享等，并需要获得个人的授权同意。

CCPA 规定，隐私保护是指个人信息的收集、使用、存储、传输、处理等环节应当符合法律、法规的规定，不得侵犯他人的合法权益。与 GDPR 相比，CCPA 的定义更加具体，涵盖了更多的情况。此外，CCPA 还从实质辨别角度强调了个人信息的可识别性，即使数据经过处理或匿名化，只要能够重新识别个人身份，仍属于应当保护的个人数据。

中国的《民法典》规定，自然人享有隐私权，任何组织或者个人不得以刺探、侵扰、泄露、公开等方式侵害他人的隐私权。隐私权包括私人生活安宁和不愿为他人知晓的私密空间、私密活动和私密信息等。与 GDPR 和 CCPA 相比，《民法典》更加注重隐私权的保护，规定了更广的保护范围，如禁止任何组织或者个人侵扰他人的生活安宁和私密空间等。

中国的《个人信息保护法》规定，任何组织、个人不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开他人个人信息；不得从事危害国家安全、公共利益的个人信息处理活动。它主要在于注重个体的权益，重点关注谁可能会侵犯个人信息权利、侵犯了什么样的个人信息权利，并且给出了解决相关争议的途径和方向。此外，《个人信息保护法》还规定了任何单位不得公开散布含有个人隐私信息的条款，即使运用大数据可推演出来的信息也仍在保护范围之内，包括一些利用大数据推演出来的信息也不得公开传播。

综上对比分析，GDPR、CCPA、《民法典》和《个人信息保护法》对个人数据、个人信息、隐私的不同概念的具体的内涵和外延都有所不同。这与各个国家和地区既有的法律体系和实际国情有关。跨境电商隐私合规，重在适配各个国家和地区的法律、法规，使用法律、技术和管理等机制来保护个人信息以免受到任何侵害。

## （二） 隐私合规的全球背景

以《中美经贸协议》知识产权保护为例，无论采用“下架优先于侵权判断”的倒置程序规则、免除善意提交错误下架通知的责任、延长权利人采取后续措施的期限、处罚恶意提交通知或反通知主体或增设吊销经营许可证的法律责任，无疑是一把悬在跨境电商企业头顶的达摩克利斯之剑，昭示着一个不争的事实，跨境电商平台、企业必须正视将会承担双重或多重法律风险。需要了解经营区域的政策、法规、法律。

考虑跨境电商企业必须处理大量的用户数据的特性，必须遵守经营区域不同国家和地区各自的隐私合规法规。如若跨境电商企业在数据处理方面违背相关法规，就要承担面临巨大的罚款和法律诉讼的责任。

**1. 隐私立法潮流**

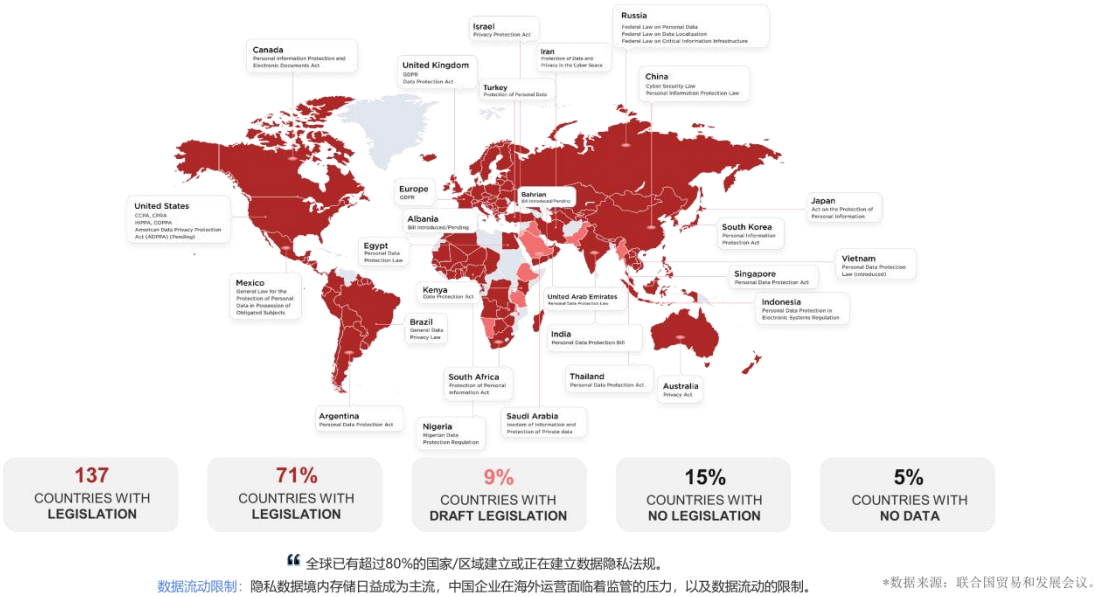
在欧美 GDPR、CCPA 为首的两大主流法域影响下，各国隐私数据保护政策纷纷

出台，据联合国贸易发展会的最新统计，

✓ 194 个国家中有 137 个国家和地区通过立法来保护数据和隐私法益，比例高达 71%，其中有 75 个国家设立独立的个人数据保护机构，以保障数据规范的落实与执行。

✓ 仅欧盟、美国、日本、法国、意大利、加拿大、德国、英国、印度、南非、韩国、俄罗斯、澳大利亚、巴西，14 个地区和国家就有 87 项数据安全法规。

✓ 此外，还有 9%的国家和地区正在起草相关法律法规。




❝ 全球已有超过80%的国家/区域建立或正在建立数据隐私法规。

数据流动限制：隐私数据境内存储日益成为主流，中国企业在海外运营面临着监管的压力，以及数据流动的限制。

*数据来源：联合国贸易和发展会议。

可以看到并预见，各个国家和地区的隐私数据保护立法会逐渐赶超商业步伐，其判罚严格“宁可错杀”的法律法规建构旨在侧重发挥对隐私的保护功能以及对隐私侵犯事件的震慑功能。

**2. 隐私违规判罚案例统计概览**

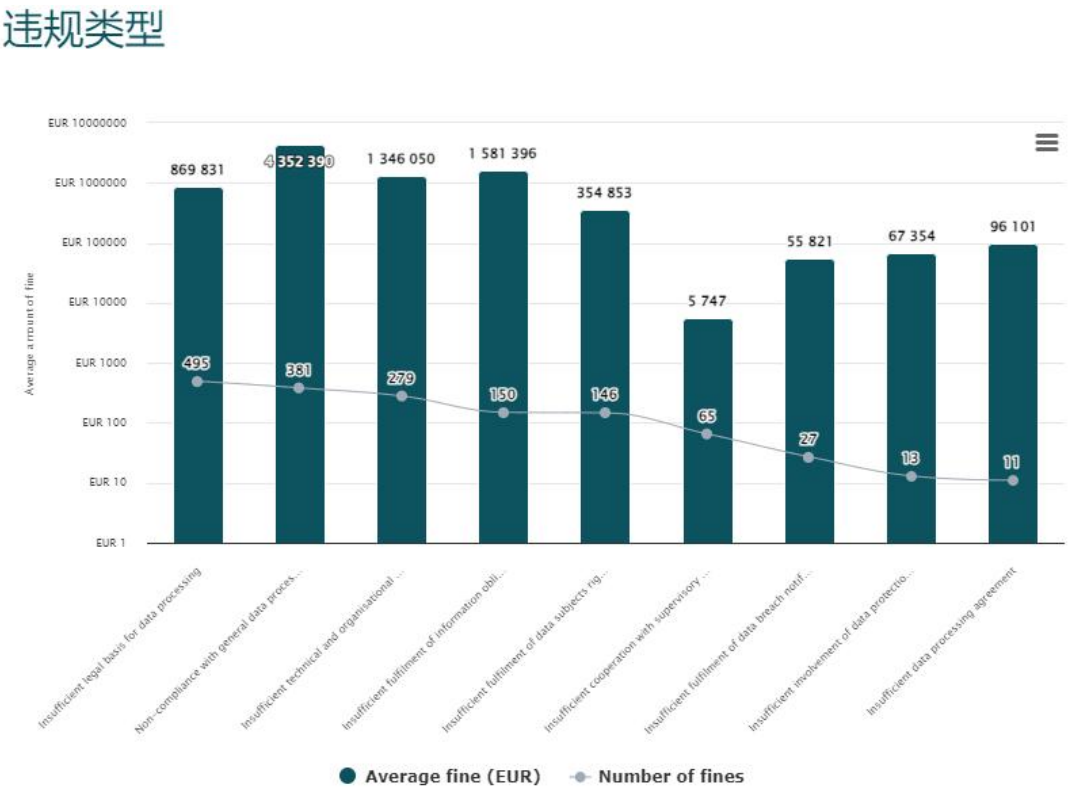
根据 CMS[3]的统计数据，分析截至 2023 年 3 月累计 27.7 亿欧元罚款。GDPR 执行跟踪报告和 GDPR 执行跟踪网站中的每项罚款均归因于以下九个类别之一：

1) 数据处理的法律依据不足
2) 确保信息安全的技术和组织措施不足
3) 不遵守一般数据处理原则
4) 数据主体权利未充分履行
5) 信息义务履行不足
6) 与监管机构合作不足
7) 未充分履行数据泄露通知义务
8) 缺乏数据保护官员的任命
9) 数据处理协议不足

在这些类别中，罚款最多（同时罚款总额第二高）的原因是针对法律依据不足的数据加工活动。第二个最常见的罚款原因是不遵守一般数据处理原则的数据处理活动。第三个原因是因确保信息安全的技术和组织措施不足、未充分履行信息安全保护义务和未充分履行一保障数据主体权利而被罚款。

[3] CMS: GDPR 执法数据，CMS Legal Services EEIG is a European Economic Interest Grouping that coordinates CMS Member Firms. Content Management System 的缩写，意思为“网站内容管理系统”， 用来管理网站后台，编辑网站前台。

虽然不遵守一般数据处理原则不仅是第二大常见的罚款原因，但对 Meta 处以的极高罚款导致此类违规行为的平均罚款金额明显高于任何其他类型的违规行为。到目前为止，只有很少的罚款是由于缺乏与监管机构的合作、违反数据泄露义务、数据保护官员的参与不足或缺少数据处理协议的情况而被处以的。




数据来源：CMS，GDPR 执法跟踪数据库

回顾以下几个案例，以便大家思考可能触发的判罚违规类型：

**案例一：**剑桥分析丑闻，指 8700 万 Facebook 用户数据被不当泄露给政治咨询公司剑桥分析，用于在 2016 年总统大选时支持美国总统特朗普。2020 年 4 月 23 日，美国联邦法院终于批准了 Facebook 与美国联邦贸易委员会就剑桥分析丑闻的 50 亿美元和解协议。

违规类型：确保信息安全的技术和组织措施不足

**案例二：**因处理儿童隐私数据不当，图片分享平台 Instagram 所有者 Meta 被爱尔兰数据隐私监管机构处以创纪录的 4.05 亿欧元（约合 27.9 亿元人民币）罚款。据英国路透社，爱尔兰数据保护委员会的一名发言人对媒体表示，自 2020 年起，该机构主要针对 Instagram 上 13 至 17 岁的青少年用户展开调查，发现这些青少年用户被允许运营企业账户，这会导致他们的电话号码和电子邮件地址被公开。

违规类型：确保信息安全的技术和组织措施不足】

**案例三：**因未允许法国用户便捷地拒绝 cookie 跟踪，法国数据监管机构 CNIL（法国国家信息与自由委员会）对谷歌处以 1.5 亿欧元（约合 10.81 亿人民币）的罚款。因谷歌违反了 GDPR 的两项规定：

一是未满足透明度和信息披露的相关要求，比如数据用途、存储时限、个性化广告所需的个人数据类型等重要条款分散在不同的文件里，获取全部披露信息有时需要跳转五到六次，繁杂程度高，有设置障碍之嫌。

二是未尽到为个性化广告提供法律依据的义务，主要表现为用户的知情权没有

被充分保障。以“个性化广告”段落为例，用户无法从文本中充分了解数据处理过程中可能涉及的其他产品，如谷歌搜索、YouTube、谷歌地图等。

违规类型：确保信息安全的技术和组织措施不足，不遵守一般数据处理原则，数据主体权利未充分履行保障，信息安全保护义务履行不足，数据处理协议不透明不足

**案例四：**因数据共享不透明，2021 年 9 月，爱尔兰数据保护委员会 DPC 向 WhatsApp 开出 2.25 亿欧元罚单。爱尔兰数据保护委员认为，WhatsApp 在介绍数据处理方式、隐私政策以及与母公司 Facebook（现更名为 Meta）共享数据方面未能充分提示和说明，违反了 GDPR 的多项规定，因而处以罚款。

违规类型：不遵守一般数据处理原则，数据主体权利未充分保障履行，信息安全保护义务履行不足，数据处理协议不足不透明

### 3. 以隐私合规之名竖高墙

如今许多国家将数字经济视为贸易发展的源动力，为了弥补自身在技术研发上的相对劣势，争先通过严格的数据立法在数据治理的国际博弈中谋求制度先机。特别是以美欧为首的西方国家，为遏制中国互联网等高新技术产业的发展，设立了极其严格的合规标准以提高数据市场准入门槛，增强本国互联网企业同外国巨头的博弈筹码。由此，外国极有可能以“隐私保护”为由否定我国互联网企业的隐私保护措施，从而构建阻碍我国互联网企业扩大海外市场份额的贸易壁垒。

美国当地时间 3 月 23 日，TikTok 首席执行官周受资（Shou Zi Chew）受邀出席美国国会举行的听证会，成为全球瞩目的焦点。一方面大众看到的正面，信息透明、用户隐私、未成年人保护、消费者信息安全等成为热议话题（或者是改成“被热议”）。真实的反面另一方面，《福布斯》采访其中一位众议员公允地说，“我们有隐私立法，有透明度立法，但如果我们只是让这些听证会成为政治舞台，我们就没有做任何事情来保护美国人民。”

2020 年 6 月 30 日凌晨消息，印度政府在《印度快报》《印度斯坦时报》《今日印度》等印媒于 29 日晚宣布禁止包括微信、TikTok、美图、百度地图等 59 款中国应用在印使用，这 59 款中国应用将被禁止在移动平台和非移动平台使用，《印度快报》在报道中显示，印度政府以该国信息技术法案第六十九条第一款为基准，以及《2009 年信息技术（阻止公众获取信息的程序和保障措施）规则》的相关规定，认为公布的 59 款来自中国的应用有“在安卓和 iOS 系统上存在数据滥用情况，这些应用有以未经授权的方式窃取用户数据秘密传输到印度境外的服务器的行为”。

## （三） 隐私泄露事件反思

### 1. 企业数据泄露事件反思

2023 年 10 月，英国航空公司因 2018 年数据泄露事件，被 ICO 罚款 2000 万英镑，理由是其“未能保护其 40 万以上客户的个人和财务详细信息”，这也是 ICO 迄今为止的最大罚单，根据英国航空的说法，数据泄露事件发生在 2018 年 8 月 21 日至 9 月 5 日之间。网络攻击者在英国航空公司的网站与移动应用程序中植入了一个病毒版本的 Modernizr JavaScript [4]库。随后，用户被转到一个虚假欺诈网站，导致约 50 万名用户的多种信息被攻击者窃取。其中包括用户姓名与地址、登录信息、支付卡信息、旅行预定详情等[5]。但是，据 ICO[6] 了解，此次数据泄露早在 2018 年 6 月已经开始。

[4] 用于检测用户浏览器中的 HTML5 和 CSS3 特性打造出来的一台精密的现代化机器
[5] 引自王文婧井玉倩：数据泄露天价罚单开出英航、万豪将为用户损失买单，2019 年 7 月 12 日 https://www.infoq.cn/article/H1AoXid8baqPXbT-zdqy
[6] ICO(Information Commissioners Office )是英国为维护信息权利而设立的独立机构

无独有偶，万豪国际也同样出现了数据泄露的问题，与英国航空的情况不同，万豪的数据泄露事件还涉及 2015 年 11 月对喜达屋的收购。ICO 在一份声明中说：“在 2014 年，一个未知的攻击者在喜达屋系统中的设备上安装了一段称为 web shell 的代码，使他们能够远程访问和编辑该设备的内容。”而直到 2018 年底，用户数据泄露的情况才被万豪发现。这四年间，全球约 3.39 亿条客座记录中的个人数据泄露。其中，约 3000 万条与欧洲经济区（EEA） 的 31 个国家的用户有关，700 万条与英国居民有关。这些数据包括客户姓名、邮寄地址、电话号码、电子邮箱、护照号码、喜达屋首选的客户账户信息、抵离信息、预订日期和沟通偏好等等。

此次数据泄露事件引发了很多思考，例如英国律师事务所 Mishcon de Reya 的合伙人尼尔·拜利斯思考，在收购一家公司前也需注重对其数据保护政策的尽职调查，尤其是在处理个人数据量和业务结构高风险性的行业企业当中。[7] 从中可以得出，企业作为数据控制持有者需要把保护个体隐私纳入企业管理团队的战略规划、运营各个环节。

**2. 私人照片泄露事件反思**

2014 年 8 月 31 日，图片板 4chan 上发布了近 500 张各种名人（主要是女性）的私人照片，并在 Imgur 和 Reddit 等网站和社交网络上被其他用户迅速传播。这次泄密事件被普遍称为“The Fappening[8] ”和“ Celebgate [9]”。这些图像最初被认为是通过破坏苹果云服务套件 iCloud 或 iCloud API 中的安全问题而获得的这使得他们可以无限制地尝试猜测受害者的密码。苹果在一份新闻稿中声称，访问权限是通过鱼叉式网络钓鱼攻击获得的。

该事件引起了媒体和名人的不同反应。批评者认为此次泄露是对照片拍摄对象隐私的重大侵犯，而一些被指控的拍摄对象否认了这些图像的真实性。

从上例可反思，个人该如何保护自己的隐私？在互联网如此发达的时代，各种社交平台，各种学习打开平台，在打造各自人设、品牌、社交圈的同时，需要时刻保持警惕意识，保护好自己的隐私空间。诚然，个人、企业外，行业、国家层面需要反思顶层立法、行业守法、企业执法及个人隐私保护如何更好落地。

**（四） 隐私合规的价值**

从跨境电商微观主体、行业、国家三个层面分析隐私合规的价值：

**1. 微观层面：数据保护惠及商家、平台和用户三方**

对于商家，在跨境电商中，商家需要收集和处理大量用户数据以提供服务和改善用户体验。有效地保护用户隐私对于商家来说是至关重要的，它有助于维护品牌形象、减少法律风险，并保持用户的信任和忠诚度。

对于平台，跨境电商平台作为用户和商家之间的桥梁，保护用户隐私极其重要，有助于减少法律风险、保持用户和商家的信任及忠诚度，促进平台的长期发展。

对于用户，保护用户隐私是用户的根本权益。保护用户隐私是跨境电商应尽的法律义务和社会责任，有助于提升用户的购物体验，维护社会的公平和正义。

综上所述，跨境电商的隐私保护对于商家、平台和用户都具有非常重要的价值。只有充分认识到这一点并采取有效的措施来保护用户隐私，才能建立起一个安全、可信赖的跨境电商环境。

[7] 引自：郑萃颖万豪在英国被罚 1.6 亿元，因为泄露了 3 千万客人信息，2020 年 11 月 03 日，界面新闻，有改动。
[8] 艳照门事件
[9] 名人门

**2. 中观层面：促进行业可持续发展**

在跨境电商行业中，隐私保护不仅是个体企业的行为，更是整个行业可持续发展的关键因素。跨境电商行业的发展依赖于消费者和企业的信任和参与。如果缺乏对隐私保护的重视，将导致消费者和企业的信心下降，进而影响整个行业的健康发展。因此，行业内的企业应共同遵守隐私保护的原则和规定，建立行业内的信任体系，促进跨境电商行业的可持续发展。

**3. 宏观层面：推动国家经济增长和国际形象提升**

对跨境电商进行隐私保护，于国家的经济增长和国际形象提升具有积极的影响。一方面，隐私保护能够促进跨境电商的健康发展，推动国家经济的增长；另一方面，隐私保护也是国际社会关注的热点问题，一个国家在隐私保护方面的表现，直接影响到国家的国际形象和国际竞争力。因此，国家应加强对跨境电商隐私保护的监管和管理，建立健全相关的法律法规，提升国家在这方面的监管水平，树立良好的国际形象。

综上所述，隐私保护在跨境电商微观主体、行业、国家三个层面都具有重要的价值。企业、行业和国家应共同努力，加强对跨境电商隐私保护的重视和实践，从而促进跨境电商行业的健康发展，提升国家的经济增长和国际形象。

## 二. 隐私合规的困境

### （一） 创新带来的隐私挑战


**来源：作者自绘**

随着底层的技术进步，5G 网络快速应用，加速物联网、区块链迅速发展；大数据遇到大模型，机器智能摆脱人工；虚拟现实、增强现实，数字人商业普及。业务创新快速迭代。

业务创新迭代速度，远远高于行政立法的速度，行业规范紧追步伐。而技术是把双刃剑，在推动业务创新发展的同时，也带来了更多的隐私数据泄露风险。

首先，个人数据被大量收集、存储和使用以服务于商业发展。这些数据很可能被用于广告推送、市场分析、商品推荐等。例如，社交网络、在线购物和移动应用

程序等都会收集和分析用户的个人数据，包括位置、购买习惯、浏览偏好等。这些数据一方面有利于个性化的推荐和营销策略，另一方面也增加了隐私泄露的风险。

其次，新技术也提升了追踪和监视的难度。例如，人工智能技术可以用于个人的追踪和监视，从而侵犯个人隐私。同时，监控和追踪技术、深度学习技术也被广泛应用于从个人数据中推断出更多信息。这些技术的应用可能涉及用户的行为、位置、偏好等敏感信息，如果使用不当或缺乏必要的监管，就可能侵犯个人隐私。

此外，新技术的发展也带来了数据安全和隐私保护的挑战。例如，大数据技术被发展应用于公共管理、科学研究、企业营销等各个领域，广泛的应用也带来广泛的数据泄露风险。从宏观的大数据统计来看，2020 年互联网数据泄露总条数约为 360 亿条，数据泄露事件给企业造成的平均损失高达 386 万美元。从具体的例子来看，人工智能发展如火如荼，最新消息，人工智能可以根据房间内 WIFI 的信号扫描建模，实时呈现房间里的三维全景。在技术层面是很大的突破，但是无疑是对隐私的巨大威胁不用破解 WIFI，直接通过 WFI 信号扫描，貌似没有违规违法。但是全息建模是否侵犯个人隐私呢？值得企业、行业、国家深思！

总之，技术创新对隐私保护带来了新的挑战和机遇。需要采取有效的措施来保护个人隐私，包括建立健全相关的法律法规、加强行业自律和技术创新等。只有这样，才能确保个人数据的安全和隐私权益得到充分保障。

### （二） 地区差异带来的法域冲突

欧盟坚持规则先行，重视数据治理和人工智能伦理。由于缺乏全球领先的科技企业，欧盟在数字经济国际竞争中逐渐失去了主动地位，为逆转这一局面，欧盟积极构建数字经济相关监管规则。在数据保护方面，欧盟于 2018 年 6 月正式实施的《通用数据保护条例》（General Data Protection Regulation，简称 GDPR）堪称最严厉的个人数据保护法，极大提升了隐私保护标准和科技企业合规成本，引领了全球个人隐私保护立法热潮。

《加州消费者隐私法案》（California Consumer Privacy Act，简称 CCPA）是继欧盟《一般数据保护条例》（GDPR）颁布后又一部数据隐私领域的重要法律。2020 年 7 月 1 日开始正式执行。CCPA 是美国首部关于数据隐私的全面立法。美国目前并没有 GDPR 一类的通用数据保护法律，只在一些特殊行业或领域立法里，有关于隐私保护的内容散落在其中。例如，《健康保险流通与责任法案》（HIPAA）中提到如何保护患者隐私信息，《儿童在线隐私保护法案》（COPPA）是专门为保护儿童个人信息制定的联邦法律。**CCPA 的出台弥补了美国在数据隐私专门立法方面的空白，它旨在加强加州消费者隐私权和数据安全保护，被认为是美国当前最严格的消费者数据隐私保护立法。**

GDPR 强调数据所有者的主体优先性，通过赋予数据权利以提高个人数据保护力度的同时，又限制了企业的数据使用及处理行为。而 CCPA 在注重个人信息保护的基础上，高度重视产业利益，合理地削弱个人对数据信息的绝对控制权，为数据所有者与控制者留有探索创新性数据交易商业模式的空间。

具体来说，比如两者对于境外管辖权问题便有着不同规定。GDPR 除了常规的属人、属地管辖之外， 还纳入了保护性管辖。对于互联网企业而言，这意味着只要企业向欧盟数据主体提供产品或服务、监控其 行为或处理其数据，都将受到 GDPR 的管辖。而 CCPA 虽有扩大管辖范围的趋势，但其综合衡量各方要素，通过设置一定门槛对某些营利性企业统一进行保护性管辖，一定程度上限制了管辖权的过度扩张。

不难看出，欧美在数据治理问题上存在着本质性不同，其归因于两者数据保护

的差异取向。 进一步究其原因，根本在于世界数字技术发展的不平衡。以欧盟为代表的国家或地区，为了弥补自身 技术产业劣势，通过实施严格的数据法案限制外来互联网企业的侵袭以净化本地的数据竞争环境；而以美国为代表的技术优势地区，通过放宽数据规则，致力于实现数据保护与产业发展的良性互动。也正是价值取向的差异，直接决定了各国对于企业数据处理有着不 同的标准及要求。

对比分析 GDPR 和 CCPA 在隐私保护的差异：

1)适用范围和定义：GDPR 适用于在欧盟境内设立的主体，以及处理欧盟公民个人数据的非欧盟主体。它定义了个人数据包括任何与已识别或可识别的自然人相关的信息。相比之下，CCPA 主要适用于加州居民，定义的“个人信息”范围较广，包括一些难以识别的信息。但其影响力也不容忽视，因为许多在加州开展业务的公司选择遵守 CCPA。

2) 隐私权利：GDPR 赋予了个人更广泛的隐私权利，包括数据访问权、纠正权、删除权等。而 CCPA 则只赋予了加州居民一些有限的隐私权利，如访问权、改正权和删除权等。 GDPR 赋予了个人更多对其数据的控制权，如数据可携权、被遗忘权等。CCPA 则侧重于限制企业出售用户数据的行为。

3)数据处理和保护要求：GDPR 要求组织在处理个人数据之前获得明确和肯定的同意。不要求事先获得明确的同意，但允许数据主体选择退出其个人信息的销售。GDPR 要求数据处理者在整个数据处理过程中都要遵守隐私保护原则，包括在数据收集、存储和使用等各个环节。CCPA 则要求在收集、使用和披露个人信息时遵守隐私保护原则。

4)跨境数据传输：GDPR 对跨境数据传输有严格的规定，要求数据必须在具有适当隐私保护水平的地方处理。CCPA 则没有此类规定，只要求企业制定合理的隐私政策并获得用户的同意。

对于跨境电商企业来说，需要：

1)了解适用法规：跨境电商企业应该了解自己在处理个人数据时应当遵守的法律规定，特别是对于同时处理欧盟公民和加州居民的个人数据的企业，需要注意这两方面的法律规定。

2)强化数据处理流程：跨境电商企业需要加强个人数据处理流程的合规性，确保在数据收集、存储和使用等各个环节都遵守法律规定。

3)重视用户隐私权益：企业应当尊重用户的隐私权益，尤其是对于跨境传输的个人数据，要采取适当的措施保护用户的隐私权，并按照法律规定的要求给予用户相应的隐私权利。

4)制定合理的隐私政策：企业应当制定合理的隐私政策，并在收集、使用和披露个人信息时遵守隐私保护原则，确保用户能够明确了解自己的个人信息被如何使用和保护。

5)加强培训和教育：企业应当加强员工对隐私保护法规的培训和教育，增强员工的隐私保护意识和能力。

总之，跨境电商企业需要关注不同国家和地区的隐私保护法律规定，并采取有效的措施确保个人数据的合规性和安全性，以满足企业发展需要，降低企业经营风险。

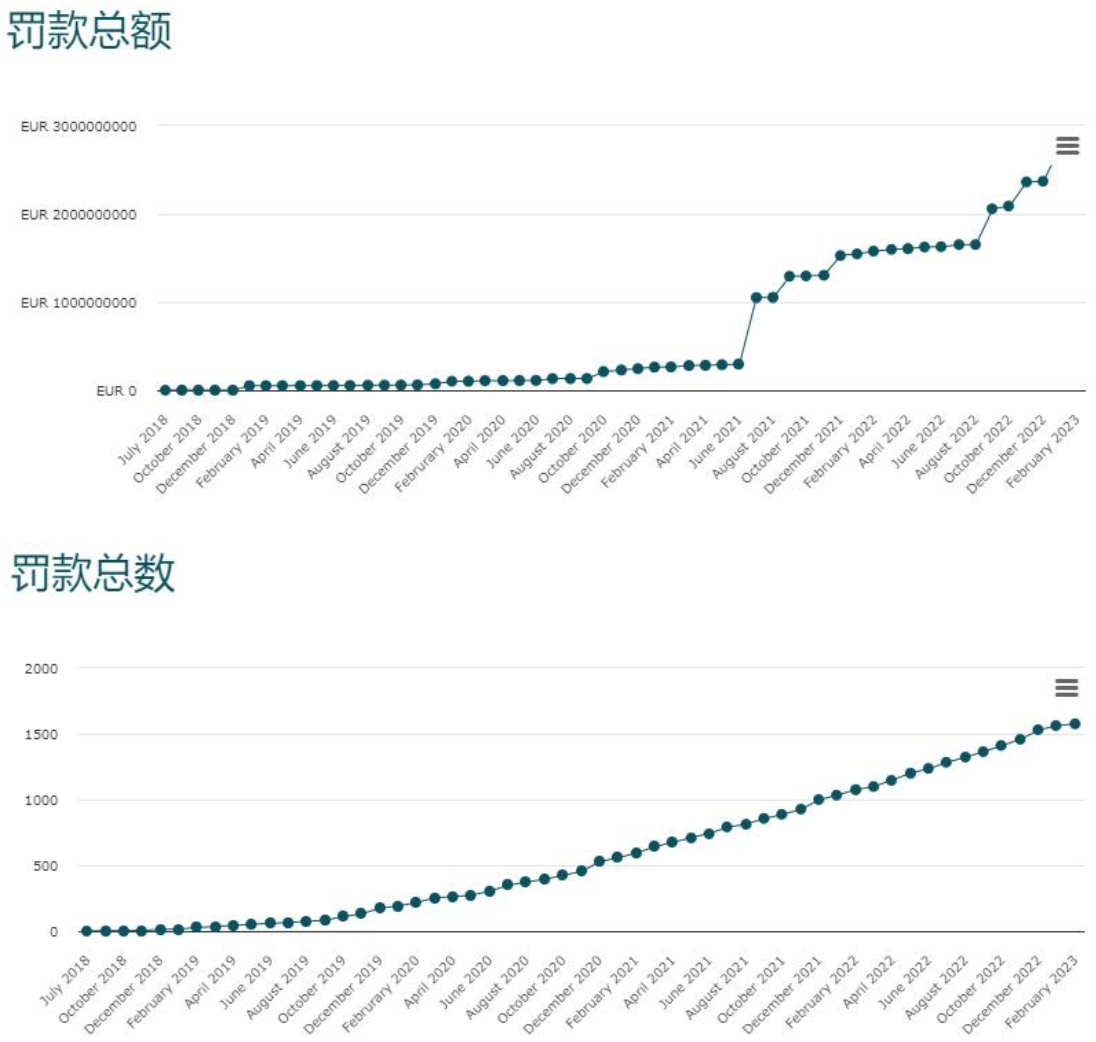
### （三） 隐私合规成本大幅提升

#### 1. 罚没成本高

在 GDPR 实施 5 周年之际，截止日期为 2023 年 3 月 1 日，CMS 执法跟踪数据库中共记录了 1,576 笔罚款（与 2022 年 GDPR 执法跟踪报告相比增加了 545

笔）（ 1,672 笔罚款（如果金额或日期信息有限）也计算在内），罚款总额约为 27.7 亿欧元（与 2022 年 GDPR 执法跟踪报告相比增加了 11.9 亿欧元）。在 2018-2023 年报告期内，所有国家的平均罚款约为 1,755,366 欧元。

2018 年，当局似乎允许数据控制者和他们自己在初始阶段熟悉 GDPR 下的新数据保护制度。在此阶段，罚款相对较少。这一阶段已经结束，自 2019 年以来，罚款数量不断增加。2022 年，“大型科技”成为监管机构关注的焦点，并处以前所未有的罚款。虽然 2021 年也出现过这种情况，但 2022 年，社交媒体平台运营商再次面临数亿欧元的巨额罚款，导致迄今为止最大的 5 项罚款均在 2.25 亿欧元至 7.46 亿欧元之间。




数据来源：CMS，GDPR 执法跟踪数据库

根据世界各国的数据立法趋势，数据主体的权利愈加完善。以知情权、被遗忘权为代表的新设数据权利，昭示着各国立法已将数据主体一般的数据权利上升到基本人权的高度，同时数据保护周期也随之延伸。而这也对应地增加了互联网企业的义务负担。GDPR 等法规对企业都提出了较高的要求。

**2. 合规投入大**

需要投入大量的资源重塑其内部的运行规则。而当入不敷出的情形出现时，企

业便会因此而退出某一国家的数据业务。仅针对 GDPR 的合规要求，全球便有 20%的企业因违反合规要求而导致破产，甚至出现了美国洛杉矶时报及芝加哥论坛报等企业因 GDPR 合规成本过高而直接退出欧盟市场的现象。由此可见，现如今互联网企业跨境数据规模的压力随着新设数据权利的出现而随之陡增。

**3. 运营消耗巨**

各项数据处理流程的规范性尚需提高。在各国立法对个人数据全生命周期予以保护的情况下，互联网企业需要针对每一 项数据处理流程进行合规性检查并进行合规文档记录，以应对日渐严苛的数据行为要求。数据全生命周期的保护需要互联网企业在每一项数据处理过程中提高行为的规范性，而这往往需要耗费大量的资源成本。

**4. 创新枷锁生**

个性化创新技术与应用服务遭遇阻碍。互联网企业依靠算法技术，运用机器学习将原始数据自动转化为计算编码，从而针对用户实现个性化广告的投放。而在各国数据法赋予用户的私权中，许多新设权利将与机器学习的特性产生冲突，从而影响人工智能及其关联技术的应用。从根据用户喜好精准推送短视频的抖音，到交易数据不可篡改以提高效率的区块链，再到 C2C 模式下的电子支付、电子商务，互联网企业的许多创新科技与应用都将因此而受到影响。

## 三. 隐私合规的趋势

在数据经济发展全球化、数据治理现代化的时代 大背景下，全球各国立足于本国的核心价值诉求、产业 发展需要，积极出台了数据治理的国家政策及法律规范，同时配套系统的司法执法机制以保护国民数据权 益、构建体系化的数据治理结构、推进高新技术产业发展。从欧盟强调数据主体优先权的 GDPR，到美国洲际私权产业并驾推进的 CCPA，再到我国继《网络安全法》和《数据安全法》之后再审议的《个人信息保护法（草案）》（以下简称“草案”），都昭示着互联网大国围绕数据 治理展开的竞争与合作持续深化。而以欧美为代表的 数据治理进程，在可预见的时间内将达到更高的境界， 从而给我国互联网企业的跨境数据合规带来新的挑战。

### （一）国家间、区域间数据流转规则逐渐明确

以 GDPR、CCPA 为代表的数据立法潮流，影响着世界各国的立法风格，许多国家也陆续出台了跨境数据流动规则。日本与 GDPR、CCPA 等机制衔接， 建立“匿名化数据处理”的跨境数据自由流动规则；印度受 CCPA 影响，根据数据是否为敏感数据，采取数据 主体同意转移制等方式，在融入数据全球化、保护数 据主体私权、促进国家产业发展之间达到了合理的平衡。

### （二）国际数据治理的规定范围更加精细

在对现有内容细化的同时，也从个人数据信息延伸到了非个人数据等新领域。各国加速本国数据法律体系建设，通过数据法律规范的完善以在数据治理的法律博弈中抢占先机。比如欧盟自 2019 年 5 月始实行的《非 个人数据自由流动条例》（Regulation on the Free Flow of Non-personal Data），与 GDPR 联合施效，增强欧盟对 数据的管控力；再如美国于 2018 年 3 月通过了《澄清境外数据的合法使用法案》（Clarifying Lawful Overseas Use of Data Act，CLOUD 法案），它使美国政府更容易获取存储在海外的数据。这对于调查犯罪和恐怖主义活动可能很有帮助。但是，它也引发了人们对隐私的担忧，因为美国政府可以获取这些数据而无需获得搜查令或通知数据所有者。适用“控制者原则”细化数据执法争议。

### （三）各国、各区域数据主体的数据权利愈加完善

比如 GDPR、CCPA 及草案《个保法》都为数据主体规定了知情权、拒绝权、更正权、删除权等新设权利，在保障数据主体合法权益的同时，也增加了互联网企业等数据控制者的义务负担。

### （四）各国、各区域数据法案执法范围逐步扩大

在世界数据立法 中“扩大域外管辖范围”并非个例，其反而代表了一股 国际潮流。除了欧盟 GDPR、美国 CLOUD、CCPA 法案 外，许多国家通过数据立法扩大本国域外执法管辖权， 尽可能地将境外互联网公司纳入本国法律的规制范围 之列。我国个人信息保护法的出台 2020 年 6 月出台的草案，超越了《网络安全法》等法律中传统的属人、属地管辖，将管辖范围延伸到境外主体在境外的管辖权，也明显地体现了域外管辖范围扩大的趋势。

### （五）各国完善数据立法配套制度框架

如今世界上 194 个国家中有 137 个国家或地区制定了立法来确保数据和隐私的保护，比例高达 71%，其中便有 75 个国家设立了独立的个人数据保护机构，以保障数据规范的落实与执行。

以欧盟为例，GDPR 第 51 条要求成员国建立国 家数据保护机构（National Data Protection Authorities， DPAs），以监控跨境数据流通与处理行为的合规情况。 法国 CNIL&Google 一案中对 Google 做出巨额罚款裁 定的机构 CNIL 便是 DPAs 的代表之一。而美国则希望通过推动联邦层面的统一国家隐私立法引入以总检 察长为核心的中央集中执法体制，消除地方分散执法 体制。此外，各国结合《布达佩斯公约》等公约，积极打造全球执法合作网络，共同打击数据违规现象。

总之，以欧美为代表的国际数据治理框架正朝着 一个数据立法愈加完备、执法机制更为严格的方向发 展，其中对于互联网企业的跨境数据合规要求势必会逐步严格。在多重数据规则中，互联网企业将会面临更高的违规风险。

## 四. 隐私合规的实践

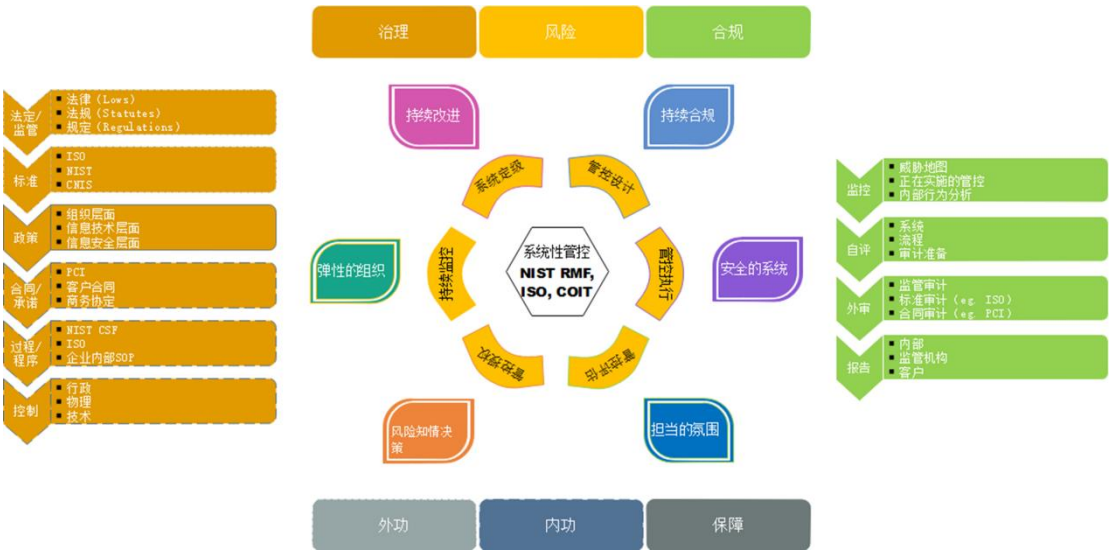
隐私合规治理的核心是如何收集、传输、保留、处理数据，包括与任何第三方共享数据，以及遵守适用的隐私法。从决策层到技术层，从管理制度到工具支撑，自上而下建立的数据安全保障体系和保护生态。

### （一）借鉴 GRC 框架，构建成熟的管理、技术、运营体系

通过采用 GRC [10]框架，可以管理风险并符合所有行业和政府法规。其中包括将组织的治理和风险管理与其技术创新和采用相统一的工具和流程。公司使用 GRC 可靠地实现组织目标，采取积极主动的方法来降低风险、做出明智的决策、满足合规性要求，并确保业务连续性。

公司通过采用包含与组织战略目标一致的关键政策的 GRC 框架来实施 GRC。关键利益相关者在制定政策、构建工作流程和治理公司时，将工作建立在对 GRC 框架的共同理解的基础上，使用系统和工具协调和监控 GRC 框架的成功落地。

[10] GRC（即 治理、风险与合规）是一种用于管理治理、风险管理以及行业和政府法规合规性的组织策略。 GRC 还指用于实施和管理企业 GRC 计划的整套集成软件功能。 GRC 的整套实践和流程为使 IT 与业务目标保持一致提供了一种结构化的方法。 GRC 可帮助公司有效管理 IT 和安全风险、降低成本并满足合规性要求。 通过利用综合视图展现组织的风险管理状况，它还有助于改进决策和绩效。




来源：作者自绘


来自网络

GRC 将治理、风险管理与合规结合在一个协调的模型中。这有助于您的公司减少浪费、提高效率、降低不合规风险，并更有效地共享信息。 基于 GRC 框架，来思考安全战略规划，信息安全治理，合规遵从。将组织与人员，制度规范，安全技术，安全运营系统性规划设计，以确保企业履行信息安全保护的责任和义务。

**（二）抓住跨境电商隐私合规要点**

中国的跨境电商交易近年来呈现迅猛增长的趋势。政府工作报告中提到要“加快跨境电商等新业态发展”，这表明未来跨境电商在中国国际贸易中的份额将持续扩大，而且跨境电商将在国家对外开放战略中发挥更加重要的作用。

随着跨境电商行业的迅速崛起，随之而来的数据量不断增加，涉及的领域也愈发广泛。跨境电商的整个生命周期与数据息息相关，跨境电商企业需要深入分析和利用这些用户信息，这成为企业竞争的核心要素之一。数据和信息也成为企业的重要估值依据。在跨境电商的完整运营过程中，国内外消费者、跨境电商企业、电商平台公司以及第三方服务提供商等各方在线上和线下场景中紧密交互，形成了复杂的数据互动网络。每一笔跨境电商交易都涉及用户信息、支付数据、物流信息等个

人数据，这些数据是跨境电商活动的重要组成部分。

然而，跨境电商领域的隐私合规和数据安全问题仍然突出存在。正所谓，随心所欲不逾矩。如何在合法合规的前提下开展业务并且释放数据价值，成为一个值得关注的话题。具体来看，跨境电商在数据合规领域面临着如下几个要点：

**1. 电商业务场景下的同意管理**

基于同意作为数据处理合法性基础的前提下，在收集用户数据前，是否以明示，清晰的方式获取了用户的同意是最易感知的、易引发用户关注及投诉的个人信息收集问题。

确保获取用户的合法有效授权同意是电商企业应优先考虑的合规问题。通常情况下，以下数据收集情景，电商企业应特别留意：

1）应设立隐私政策等明确的个人信息收集处理规则；

2）以醒目、显著、易于察觉的方式呈现隐私政策（例如使用弹窗、明显的选择框等），方便用户查阅或获得他们的清晰同意；

3）隐私政策内容需要详实，真实明示产品和服务所涉及的收集和处理的数据类型、数据共享和数据跨境的情况。

此外，需要特别关注的是，除了上述提到的途径外，考虑到电商的多样性和便捷性，数据收集也可能隐藏在私域流量运营等典型情境中，例如在即时通讯应用的群组聊天或评论中。除了依赖平台提供的隐私政策外，电商企业应结合平台特点，在实施具体数据收集处理活动之前，通过友好的提示或对用户友好的设计，引导用户仔细阅读个人信息收集处理规则，了解并同意规则内容，以确保数据收集场景的合法性。

**2. 定向营销**

在定向营销场景下，隐私合规问题成为极为重要的考虑因素。定向营销依赖于个人数据的收集和分析，以精准地针对特定用户进行广告投放。如何确保决策过程的透明度和结果的公正性，以降低合规风险并保护消费者权益，一直是需要关注的隐私挑战。应满足的合规要求如下：

1）**用户同意和知情权：**收集用户数据前，必须以明确、透明的方式告知用户数据将如何使用，并获得他们的明示同意。用户应该清楚了解他们的数据将用于定向广告。

2）**退出和选择权：**用户应具备随时退出定向广告或选择不接收个性化广告的权利，并且这些选项应该易于实现。当用户明确表示拒绝接收个性化推荐时，不得再继续向其发送商业性信息。对于采用自动化决策方式进行商业营销的情况，应同时提供不基于个人特征的选项。

3）**数据最小化原则：**企业应仅收集为实现定向营销目标所必需的数据，而不是过度收集用户信息。这有助于减少潜在的隐私风险。

4）**个人信息的匿名化和去标识化：**在使用个人数据进行定向广告时，最好使用匿名化和去标识化技术，以减少用户被识别的风险。

**3. 第三方数据共享**

电商企业在使用数据的过程中，会出于各种目的与外部第三方进行数据共享，可能涉及的第三方包括物流供应商，支付服务提供商，第三方平台供应商和广告和营销服务提供商等。在数据共享的过程中，涉及大量的隐私合规风险，跨境电商企业应采取足够的组织和技术措施进行管控。应重点关注的领域包括：

1）**识别角色并明确义务：**识别企业和第三方的数据处理角色，明确双方在数据保护方面的权利和义务。

2）**明确数据使用目的：**确保合同中明确定义了共享数据的使用目的，并限制第三方只能按照这些明确的目的使用数据。这有助于避免数据被滥用。

3）**授权和知情权：**确保数据主体已明确同意数据共享，并清楚了解他们的数据将与哪些第三方共享。透明地向数据主体提供共享细节是合规的关键。

4）**数据安全保护：**确保第三方有足够的安全措施来保护共享的数据，包括数据传输和存储的加密、访问控制、漏洞修复等。

5）**监管和审计：**建立监管机制，允许企业对第三方进行定期审计以确保合规性。这包括审查数据的使用情况以及数据安全措施的有效性。

有时在跨境电商的场景下，需要实现与合作伙伴一起利用数据，但需要找到更好地保护数据方式。当前通用的做法是企业向合作伙伴提供数据副本，并依赖合同协议防止滥用。但企业更希望尽可能限制数据移动，以保护其数据，防止误用，并避免泄漏风险。因此，需要找到合适的方式做到数据可用不可见。在业界常见的最佳实践包括像亚马逊云科技提供的数据共享协作服务，可以让多方更轻松地分析和协作处理集体数据集，从而获得见解，而不泄露基础数据。在广泛应用于跨境电商、广告等行业中，帮助客户在共享数据集上进行协作，同时仍然保护底层原始数据。

**4. 数据安全**

跨境电商面临着多个环节的数据安全问题：

首先，在跨境电商企业在用户注册、购买和支付等环节积累了大量用户数据。数据安全管理欠佳可能有内部工作人员通过用户数据倒卖牟利的风险，这是信息泄露的一个重要的风险点。因此，企业的数据保护要求至关重要，包括在内部建立信息安全体系。

其次，在跨境电商物流环节，物流系统漏洞和物流单据的交易也带来了数据安全问题。物流代理点的松散管理可能导致风险。同时，由于跨境电商市场竞争激烈，物流企业在构建交易系统时可能会忽视数据保护技术和人力投入，容易产生系统安全漏洞，导致商家和用户数据的泄露。

最后，在跨境电商用户环节，常见的数据安全问题包括钓鱼攻击、账号被盗和木马病毒。钓鱼攻击是一种欺诈行为，攻击者通常伪装成合法的实体，欺骗用户提供个人敏感信息，如密码和信用卡信息。账号被盗是另一个问题，攻击者可能通过密码猜测、社会工程学手段或已泄露的账号信息入侵用户的电商账户，可能导致财务损失和信任问题。此外，木马病毒常伪装成合法应用程序，一旦用户安装，会执行恶意操作，如窃取信息或监控用户活动。这些威胁可能导致用户的个人和金融信息泄露。

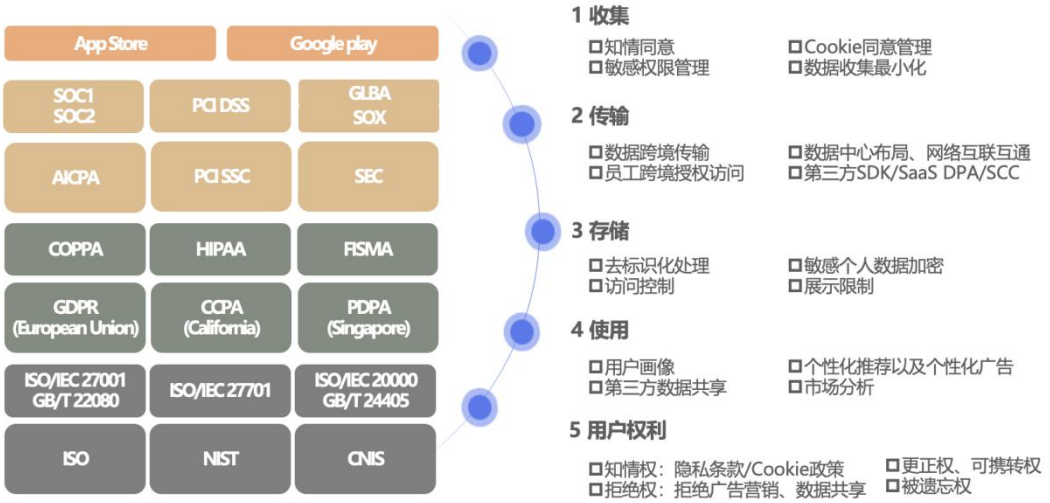
因此，跨境电商必须全面关注并解决这些不同环节的数据安全问题，采取合适的措施以保护用户和企业的数据安全。

在跨境电商领域，企业将面临许多隐私合规和数据安全问题。重视并解决这些数据和隐私风险对于企业的顺利出海至关重要。然而，商业竞争日益激烈，这也使得企业在发展过程中不可避免地会面临业务发展和监管要求之间的矛盾。如何取得平衡，找到合理的解决机制，是电商企业必须认真思考的问题。

### （三） 建立完善隐私成熟度评估体系

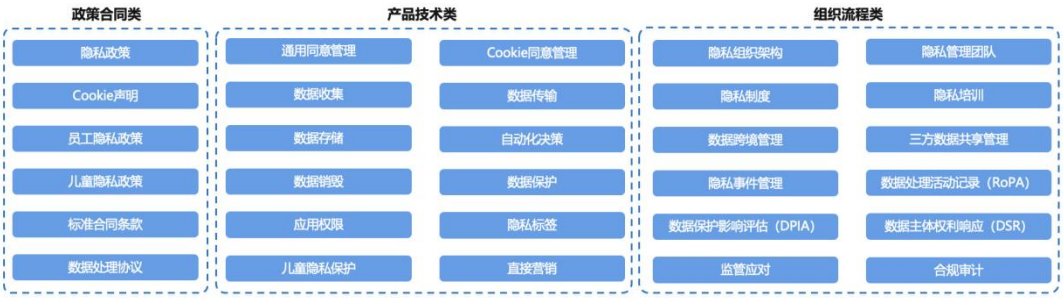
从目标地区和国家用户视角，串行、并行检测、监测数据收集、传输、保留、使用和销毁串行运营体系设计模型中的数据暴露点，严重用户体验、安全性、可靠性。通过 PDCA[11]模型，持续优化、改进用户体验、安全性和可靠性。

[11] PDCA 循环是美国质量管理专家沃特·阿曼德·休哈特（Walter A. Shewhart）首先提出的，由戴明采纳、宣传，获得普及，所以又称戴明环。全面质量管理的思想基础和方法依据就是 PDCA 循环。PDCA 循环的含义是将质




来源：Kaamel 和作者联合绘制

隐私成熟度评估体系将隐私工作分为多个领域，每个领域内细分不同的成熟度等级定义。不同的隐私成熟度评估体系划分领域的方法有所不同。根据实践经验，推荐可以将各个领域分为政策合同、产品技术以及组织流程三个类别。政策合同类下的领域关注企业面向用户，面向合作伙伴，以及面向监管是否准备了全面的政策合同文本。产品技术类下的领域从数据生命周期的维度出发，关注产品设计以及技术实践上是否保障了用户的数据安全以及各项合法权益。组织流程类则关注企业在组织维度的隐私合规管理体系的建设是否符合认证标准以及监管机构的要求。具体各类别下的详细领域可以参考下图。




来源：Kaamel 提供

在使用隐私成熟度评估体系进行自我评估的过程中，推荐在人工访谈的基础上配合以自动化检测，这将会大幅提升评估的效率以及准确性。在评估过程中，需要对每个领域分别进行隐私成熟度的打分，最终将各领域的分数按照领域的重要程度进行加权，从而得到最终的隐私成熟度得分。

隐私成熟度的得分对于企业的隐私合规工作有着重要的意义：

1）企业可据此对于其隐私合规水平进行评估，直观发现待改善的工作领域；如果基于相同的成熟度标准持续评估打分，企业还可以将隐私工作进展可视化。

量管理分为四个阶段，即 Plan（计划）、Do（执行）、Check（检查）和 Act（处理）。在质量管理活动中，要求把各项工作按照作出计划、计划实施、检查实施效果，然后将成功的纳入标准，不成功的留待下一循环去解决。这一工作方法是质量管理的基本方法，也是企业管理各项工作的一般规律

2）隐私成熟度的得分在企业第三方合作工作的开展上，也会起到至关重要的作用。甲方企业在遴选供应商的过程中，衡量供应商隐私合规水平时，隐私成熟度的得分将会是重要的参考依据。

3）企业可以根据隐私成熟度评估体系领域的划分明确内部职责。因为，隐私合规是跨法务、产品和技术等多职责岗位的事情。隐私成熟度评估体系将隐私工作划分为多个领域，法务、安全和产研团队之间可以讨论，认领主要负责的领域，从而达到按块划分明确职责。

## 五．跨境电商行业建议

### （一） 市场层面

#### 1. 推动行业自律和标准制定

跨境电商行业应当积极推动行业自律和行业标准制定，共同遵守隐私保护的原则和标准，加强行业内部的监督和管理。同时，行业也应当积极参与相关法律法规的制定和完善，为隐私合规提供更加明确和具体的法律依据。

#### 2. 加强与用户的沟通和互动

跨境电商企业应当加强与用户的沟通和互动，及时响应用户的积极反馈和投诉，了解用户的隐私保护需求和诉求，不断优化企业的隐私保护方案和服务。

#### 3. 推动与其他企业的合作和交流

跨境电商企业应当积极与其他企业加强合作和交流，共同探讨和研究隐私合规的策略和方法，共享资源和信息，提高整个行业的隐私保护水平和竞争力。

### （二）政府层面

#### 1. 完善法律法规和监管机制

政府应当不断完善相关法律法规和监管机制，加强对跨境电商企业隐私保护的监管和管理。同时，政府也应当加大对违法行为的打击力度，严格惩处侵犯用户隐私的行为，维护市场的公平公正。

#### 2. 提供指导和支持

政府可以提供指导和支持，帮助跨境电商企业更好地理解和遵守相关法律法规和标准。政府还可以提供技术培训和支持，帮助企业提高技术应用和管理能力。

#### 3. 加强国际合作和交流

政府应当积极推动与其他国家和地区的合作和交流，共同探讨和应对跨境数据传输和隐私保护的问题和挑战，加强国际合作和交流，提高全球的隐私保护水平和治理能力。

### （三）全球治理层面

#### 1. 积极参与国际组织和倡议

跨境电商企业应当积极参与国际组织如 GDPR 等框架下的倡议和合作，共同探讨和研究全球范围内的隐私合规问题。同时，企业也应当关注并参与国际标准的制定和完善，为全球隐私合规提供更加明确和具体的标准。

#### 2. 遵守国际规则和原则

跨境电商企业应当遵守国际规则和原则，尊重其他国家和地区的法律法规和文化差异，加强不同国家和地区之间的合作和交流，共同推动全球隐私合规的发展和完善。

### 3.关注全球治理动态和趋势

跨境电商企业应当关注全球治理的动态和趋势，了解国际政治、经济、社会等领域的最新变化和发展趋势，及时调整自身的业务模式和隐私保护策略，以适应全球市场的变化和发展。

综上所述，从企业、市场、政府和全球治理等维度出发，跨境电商企业应当积极应对并遵守相关法律法规和标准，加强技术应用管理，推动行业自律和标准制定。同时，政府应当完善法律法规和监管机制并提供指导和支持，而全球治理则需要在不同国家和地区之间加强合作和交流的基础上实现共同发展和进步。

## 六、总结

据麦肯锡[12]预测，数据流动量每增加 10%，将带动 GDP 增长 0.2%。预计到 2025 年，全球数据流动对经济增长的贡献将达到 11 万亿美元。根据经济合作与发展组织（OECD）测算，数据流动对各行业利润增长的平均促进率在 10%，在数字平台、金融业等行业中可达到 32%。根据国际数据公司 IDC 的预测，我国的数据量在 2021-2025 年间平均增长速度为 30%左右，将成为全球数据量最大的国家，实现经济的稳步高效发展离不开数据赋能这关键一环，规避数据带来的道德和法律的风险，需要建立和完善数据管理规则，数据跨境流动规则正在成为高水平贸易协定的重要标志。如何合规开展跨境数据流动，保护跨境数据已不是一种简单的个别提升的要求，而是社会趋势的必然要求，跨境电商行业作为跨境数据流动的主流行业，更应顺应潮流，把握机遇，采取先进的技术和经验，走在安全的康庄大道上，才能实现可持续性的发展。

# 参考资料

【1】梅傲，侯之帅，《互联网企业跨境数据合规的困境及中国应对》

【2】LC 数据合规法律研究团队，《全球个人信息保护立法概况及趋势丨凌科安时法律评论》

【3】六大洲 14 国数据安全政策汇总

【4】CMS，GDPR 执法跟踪数据库

【5】UNCTAD，联合国贸易发展会数据

【6】NIST，NIST Risk Management Framework

【7】联合国：数据在电子商务和数字经济中的价值和作用及其对包容性贸易和发展的影响

[12] 麦肯锡公司是世界级领先的全球管理咨询公司，由美国芝加哥大学商学院教授詹姆斯·麦肯锡（James O' McKinsey）于 1926 年在美国创建。自 1926 年成立以来，公司的使命就是帮助领先的企业机构实现显著、持久的经营业绩改善，打造能够吸引、培育和激励杰出人才的优秀组织机构。

# 参与创作

**敦煌网集团：**

敦煌网集团是领先的跨境数字贸易生态平台，旨在帮助中国供应链对接全球采购，助力中小微企业和个人创业者通过跨境电商进入全球市场，“让人人都能参与全球贸易”。旗下包括 B2B 跨境电商平台敦煌网（DHgate）、社交电商平台 MyyShop、智能物流平台驼飞侠 DHLink、金融支付服务驼驼数科。

**中央财经大学中国互联网经济研究院：**

中央财经大学中国互联网经济研究院是中央财经大学的实体研究机构，是清华大学电子商务交易技术国家工程实验室成员单位——互联网经济与金融研究中心、北京市哲学社会科学重点研究基地——首都互联网经济发展研究基地。研究院围绕数字经济理论、数据要素、数字金融和电子商务四个研究方向，组建了三十余人的专职研究团队。研究院成立以来获批国家级重大和重点项目十余项，承担国家和省部级一般项目三十余项。研究院入选中国核心智库，商务部内贸智库联系机制成员单位，国家数字贸易专家工作组支撑单位，首批中国智库索引（CTTI）来源智库（2017—2018），荣获 2015 中国电子商务创新发展峰会颁发的“最具影响力研究机构奖”。

**亚马逊云科技：**

作为全球云计算的创造者和引领者，利用与生俱来的创新精神，亚马逊云科技致力为中国本地企业打造全球化发展的技术桥梁，助力中国企业成功走向世界。安全合规是亚马逊云科技的首要任务，也是创新的根本保障。亚马逊云科技的技术架构保证了它可以为客户提供灵活、安全的云计算环境，支持 143 项安全标准和合规性认证，包括 PCI-DSS、HIPAA/HITECH、FedRAMP、GDPR、FIPS 140-2 和 NIST 800-171，以帮助客户满足全球各地的合规要求。

**Kaamel 公司：**

Kaamel 致力于为出海企业提供全面、有效、便捷的隐私合规解决方案及专家服务。提供创新的【AI 隐私技术+专家服务】模型和隐私风险评估和诊断服务，0 侵入性地分析网站、应用、云、第三方服务等模块，轻松实现网站的 Cookie 同意管理功能，自动化生成隐私政策、Cookie 声明等协议文本，并高效完成其他相关的隐私管理和运营工作。

# 鸣谢

感谢以下专家与人员参与本次制作：

| | |
|---|---|
| 敦煌网集团技术中心架构运维总监 | 窦东员 |
| 敦煌网集团董事长执行助理 | 田梅 |
| 敦煌网集团敦煌网研究院院长 | 李丽 |
| 敦煌网集团高级法务总监 | 解一峰 |
| 敦煌网集团法务经理 | 尹吉尧 |
| 敦煌网集团敦煌网研究院高级研究员 | 刘帅 |
| 敦煌网集团敦煌网研究院高级研究员 | 张磊 |
| 中央财经大学中国互联网经济研究院院长 | 孙宝文 |
| 中央财经大学中国互联网经济研究院副院长 | 欧阳日辉 |
| 中央财经大学中国互联网经济研究院副院长 | 何毅 |
| 中央财经大学中国互联网经济研究院助理研究员 | 张文韬 |
| 中央财经大学中国互联网经济研究院助理研究员 | 李东阳 |
| 亚马逊云科技行业解决方案架构师经理 | 刘春华 |
| 亚马逊云科技零售电商行业方案总监 | 许丹丹 |
| 亚马逊云科技解决方案架构师 | 唐健 |
| 亚马逊云科技解决方案架构师 | 裴秋利 |
| 亚马逊云科技行业拓展经理 | 刘继鸿 |
| Kaamel Technology Inc.隐私合规专家 | 王一迪 |

# 跨境电商隐私合规白皮书

Cross-border e-commerce privacy compliance white paper