

中国出海互联网公司 数据保护合规对策



普华永道



前言

近年来，在全国数字化和智能设备的普及趋势下，国内互联网行业竞争激烈。根据中国互联网络信息中心（CNNIC）发布的第47次《中国互联网络发展状况统计报告》，截至2020年12月，中国网民规模达9.89亿，较2020年3月增长8540万，互联网普及率达70.4%。各类互联网公司百家争鸣，抢夺剩余的用户增加空间，然而获客成本日益增高，市场的流量与用户渗透率逐步见顶。

为了分流中国互联网产能过剩，下沉或出海成为了众多互联网公司的突围方向。因此，海外市场成了下一个风口。回顾历史，从最初以百度、猎豹、360为代表的工具类产品，到移动游戏和社交APP，再到迅猛增长的各类跨境电商、供应链分销商等电商企业均已走向海外市场。从全球版图来看，印度、印尼、俄罗斯、马来西亚、越南、巴西等东南亚及中东地区，由于人口众多，潜在流量充足，移动互联网渗透率高，成为了互联网公司出海的重点市场。

而随着个人信息隐私保护成为当下全球网络发展的主议题，全球许多国家对数据隐私安全进行了严格的监管。普华永道认为，互联网企业在出海的过程中，应充分识别其服务所涉及国家的法律法规要求，全面了解各国的差异化要求，从而建立有效的个人信息安全合规保障机制。

全球隐私 保护现状

随着全球网络时代的到来，人们的生活更加便利，随之而来是各大软件对个人信息的违规采集。很多人可能有这样的经历：打开叫车软件，家庭住址就自动出现在了目的地栏；打开社交媒体软件，推荐栏赫然显示着刚讨论的商品。类似的事情在全球互联网时代比比皆是。人们在享受便利生活的同时，也放弃了一部分个人隐私。而全球个人隐私监管愈发严格，特别是自2018年5月欧盟《通用数据保护条例》（GDPR）生效以来，互联网公司在海外发展业务时，势必会受到不同法律法规的影响。出海的中国互联网公司亦是如此，面临着来自世界各国针对数据隐私安全的严厉监管。

同时，数据隐私安全监管在各国之间的差异仍然十分明显，有些国家首次引入系统监管措施，而其他拥有既定监管体系的国家正在实施相应的制度变革。虽然监管方式存在差异，但是数据隐私安全综合立法趋势明显。下面介绍几个全球重要市场针对数据隐私安全的最新法律法规。

欧盟

2018年5月25日，《通用数据保护条例》在欧盟范围内生效。此条例被广泛认为是史上最严格的网络数据隐私保护法规。该法规不仅对欧盟范围内的公司生效，同时也拥有域外效力，欧盟以外的公司也可能受到该法案的监管。

印度

新出台的《2019 年个人数据保护法案》深受欧盟《通用数据保护条例》影响，是印度首部全面系统针对个人数据保护的法规。新法案的落地将对出海的互联网企业造成巨大挑战。

美国

美国个人信息立法保护旨在强调信息的隐私性保护，采取公、私有别的分散式立法模式，形成个人信息保护的多元格局。美国除了立联邦的法律法规之外，对个人数据持积极利用的态度。联邦颁布的各项法案相对而言较为宽松，而近年来，各州政府愈加重视隐私保护。以加州为例，加州在2018年通过《加州消费者隐私法》，并在2020年生效。该法案作为目前全美最严格的数据保护法案，制定了一系列强有力的保护措施，以防止消费者个人隐私信息在不知情情况下被收集和用于商业行为。2021 年3月2日，弗吉尼亚州签署了《消费者数据保护法》（CDPA），该法案将于2023年1月生效，适用于拥有10万名及以上用户数据的企业、从个人信息中获得销售总收入50%以上的企业，以及处理至少2.5万名用户个人信息的企业。

俄罗斯

俄罗斯随着国内网络的发展和对个人信息保护的重视，实施了一系列的立法工作以保障国民的个人信息安全。比如在2016年颁布的《信息、信息技术与信息保护法修正案》，指出俄罗斯公民有权要求搜索引擎删除有关自己的不实信息链接。

新加坡

2012年10月新加坡议会通过了《个人信息保护法》（PDPA），并于2014年7月生效。2020年5月14日至28日，新加坡通信和信息部（MCI）和个人数据保护委员会（PDPC）联合发布了《个人数据保护法（修订）》草案。其中对“数据泄露”行为的最高罚款提高至企业在新加坡年营业额的10%或100万新元（折合约516万元人民币），两者取最高项进行罚款。修订草案对各类企业机构的违规行为的严重性及其影响、罪责程度、威慑力以及处罚金额的整体比例都进行了更为严厉的调整，对收集、使用或披露个人数据的范围、条件或要求做了更为严格的定义。

日本

2005年4月1日正式实施的日本《个人信息保护法》，在历经2015年第一次大幅度修正后，于2020年再次被修改。由日本个人信息保护委员会（PPC）于2021年3月宣布，《个人信息保护法修正案》将于2022年4月1日起正式实施。在日本，包含企业或政府等团体在内，泄露的个人信息数量在2018年就超过了1000万件。2019年8月，日本某求职信息网站的运营公司——Recruit Career，利用Cookie技术，通过调取求职者的个人信息再将这一数据贩卖给38家客户企业。在此过程中未对信息采集做任何说明也未取得用户授权。事件一经曝光，引起了日本个人信息保护委员会及公证交易委员会的高度重视，此次修正案中就针对Cookie事件暴露的问题做了相关规定，对6个月内可以消除的短期网站访问记录（如Cookie技术）纳入到“个人数据保存”的定义范畴。

中国

中国作为一个法治国家，立法工作不断发展和完善，先后出台了个人信息保护的法律法规，涉及多部法律和多个领域，有近40部法律、30余部法规，以及近200部规章涉及个人信息保护，其中2019年新增10个，2020年新增13个。

备受瞩目的《个人信息保护法（草案）》于2020年10月13日正式提请十三届全国人大常委会第二十二次会议审议。《个人信息保护法（草案）》全文共八章，内容涵盖个人信息处理规则、个人信息跨境提供的规则、个人在个人信息处理活动中的权利、个人信息处理者的义务、履行个人信息保护职责的部门、法律责任等。在2017年推出实行的《网络安全法》和2021年1月1日起施行的《民法典》等现行法律法规的基础上，强化了对个人信息的保护，明确了个人信息保护的监管职责并设置严格的法律责任。

自1973年《瑞典数据法》推行实施历史首部个人信息保护相关的法律法规以来，世界各国和地区结合时代背景和文化内涵、经济社会发展现状，相继建立了有效的个人信息安全合规保障机制。依法依规经营是企业持续发展的根本，因此互联网企业应充分识别出各国的潜在法律风险，在海外开展业务的同时，建立系统的风险防范措施与有效的个人信息安全合规保障机制。



四大主要 合规挑战


法律的符合性通常是合规要解决的首要问题，这意味着一旦合规性没有被满足，企业不但面临业务、声誉损失的风险，也有可能背负严重的法律后果。监管要求、业务需求和安全事件成为企业合规的几大驱动力，企业合规建设已迫在眉睫。现阶段，普华永道结合在出海互联网公司安全合规领域的咨询经验，归纳和总结了出海互联网公司面临的四个主要挑战：用户同意风险、数据跨境风险、数字营销风险、技术出口风险。

挑战1 用户同意风险

现如今数据作为企业运行的基础，地位日益凸显。随着人工智能、云计算、大数据等信息技术日趋成熟，以及企业数字化程度的提高，企业对数据的依赖性也随之增强，对数据安全的保护便尤为重要。然而，各国对于数据收集使用时的法律法规各有不同。以欧盟为例，《通用数据保护条例》第9条规定，生物特征数据属于个人数据的“特殊类别”，除非某些特殊情况外，不得处理该类数据。在美国，西雅图和马萨诸塞州剑桥市也宣布，任何市政部门需经过市政会的批准后方可采取与监控技术有关的

活动；旧金山在人体的生物识别方面也有严苛的规定，其中包括带摄像机的无人机购买需经许可等。因此，“用户充分告知与授权同意”已经成为欧洲及美国数据安全领域的关键议题。数据驱动型的互联网公司将是该类监管的重点对象。所有商业模式依赖于将数据主体同意作为数据处理前提的企业，无论规模大小，确保其数据活动对数据主体的透明性同时使数据主体控制其数据，都将是明智的选择。隐私声明简洁明了同时又完整全面，极具挑战性。





挑战2 数据跨境风险

数据跨境传输的定义是把数据（通常指个人数据）从一个法域传输到另一个法域，数据传输的流程周期一般是数据产生、数据传输到数据接收，三个环节的挑战各有不同。

- **数据产生环节：**首要难题是本地合规限制，指的是当地法律对数据收集的要求，例如数据本地化存储、数据主体同意、政府申报、任命数据保护官（DPO）等。
- **数据传输环节：**对传输目的会有较大限制，简单来说，作为数据控制者或处理者的互联网企业，需要合适合理的理由，才能将数据从当地转移到另一个国家，且对于个人数据的出境目的，主要以经济目的为主。
- **数据接收环节：**接收国的数据保护水平也会成为限制因素，一般会要求接收国的数据保护水平达到充分水平，至少与出口国旗鼓相当，且经过数据输出国认可。

以印度为例，作为对数据存储本地化有严格要求的国家，印度的《个人数据保护法案》草案里明确要求，个人数据跨境传输须在印度境内留有副本，并且关键个人数据必须在位于印度的服务器或数据中心进行处理；而对个人敏感数据的要求则更加严格。对掌握大量个人敏感信息的互联网企业来说，这样的要求无疑增加了企业在数据存储上的支出。

俄罗斯对个人数据存储本地化的要求也非常严苛，个人数据需要满足最先、最全、最新的原则，企业需要在俄罗斯本地增设服务器的解决方案。这个要求会严重阻碍企业运用云服务来提高效能，对互联网这种“云上”企业来说无疑挑战更大。

因此，企业进行数据出入境时，必须注重到可能存在的未知安全隐患，应按法律法规标准要求开展跨境安全风险评估与处置、监管报备、DPA协议签署、出入境计划与报告等材料的编制及相关工作。



挑战3 数字营销风险

随着电子计算机技术的飞速发展，数字营销逐渐成为了各行各业的重要工作之一。如今，数字营销不仅能帮助企业与客户建立有效沟通，而且还可以为企业带来更高的投资回报率和更大的市场拓展范围，因此数字营销在企业的广告策略的首选。然而，不断扩大的数字营销市场同时也充斥着较高的风险及挑战，夹杂着不合规、不透明、不真实的虚假广告。

以谷歌为例，作为跨境电商最常用的搜索引擎网站，在2019年更新了广告政策，对广告的内容、行为、编辑及技术要求提出了违规点。2019年7月，中国互联网公司触宝（CooTek）因违反了谷歌的广告政策，数十款旗

下产品被Google Play Store及广告平台封禁。英国在2020年年初，发布了广告行业新规，禁止企业发布涉及性别偏见和负面性别刻板印象的广告，并统一下架或禁播了已发布的违规广告。

而我国在2020年8月31日，工信部发布《通信短信息和语音呼叫服务管理规定（征求意见稿）》，并向社会公开征求意见。该规定是在《通信短信息服务管理规定》（工业和信息化部令第31号）的基础上进行修订。8月31日，工信部网站发布，其中规定任何组织或个人未经用户同意或者请求，或者用户明确表示拒绝的，不得向其发送商业性短信息或拨打商业性电话。



挑战4 技术出口风险

根据《中华人民共和国技术进出口管理条例》，凡是涉及向境外转移技术，无论是采用贸易还是投资或是其他方式，均要严格遵守《中华人民共和国技术进出口管理条例》的规定，其中限制类技术出口必须到省级商务主管部门申请技术出口许可，获得批准后方可对外进行实质性谈判，签订技术出口合同。

2020年8月，商务部、科技部调整发布了《中国禁止出口限制出口技术目录》，对出口的各种技术进行了严格要求。限制出口的技术中与互联网行业息息相关的包括：语音合成技术，语音信号特征分析和提取技术，文本特征分析和预测技术，人工智能交互界面技术，语音评测技术，智能阅卷技术，基于数据分析的个性化信息推送服务技术。对于专注电商、社交、游戏、工具等领域的互联网公司来说，原本具有较强竞争力的智能技术，如今成为了出海过程中的一大挑战。

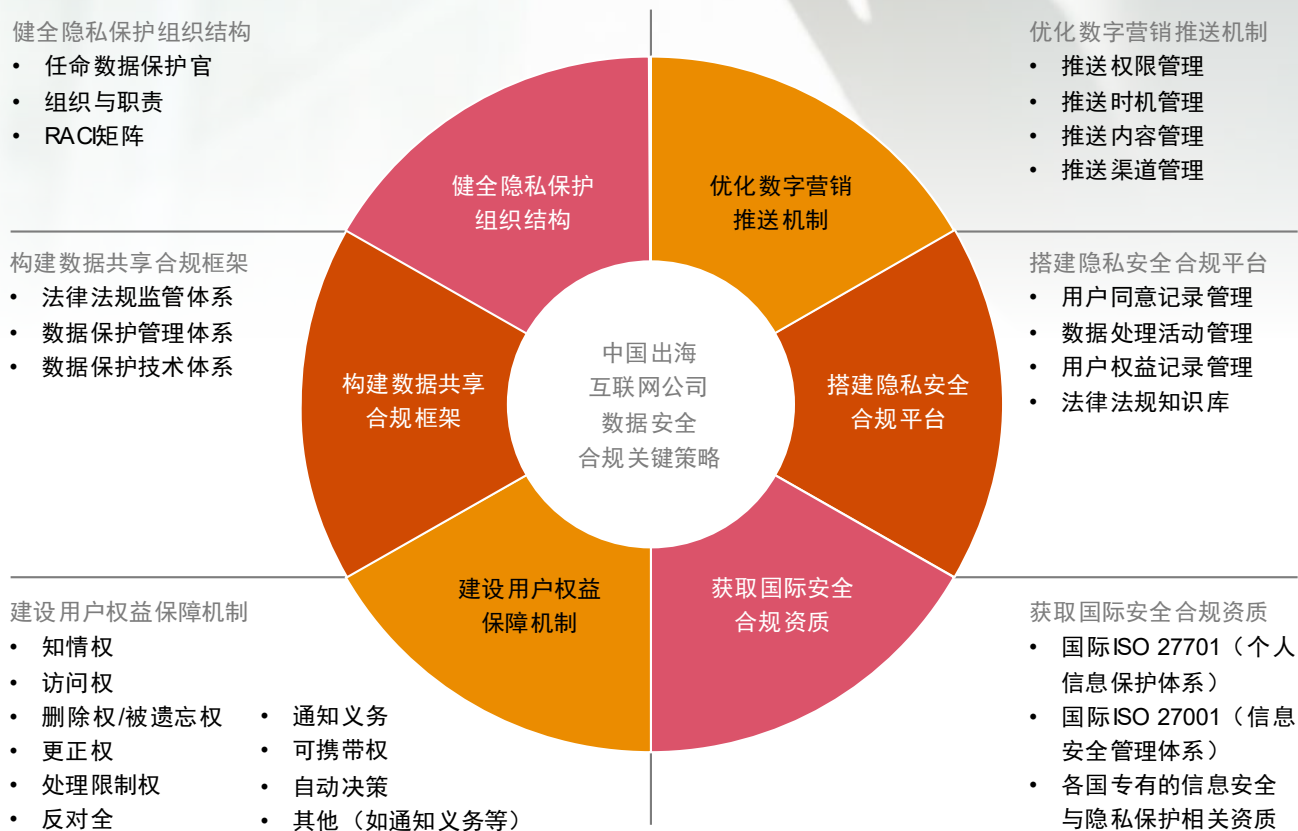


关键解决 应对措施

随着互联网数据的极速增长和数据价值的不断攀升，数据已经成为当下最重要的资产。据《2020全球数据合规法律观察报告1.0版本》统计，在全球所有国家和地区中，132个国家已完成了对数据和隐私保护的立法，此统计数量仍在增长中。中国互联网企业在出海过程中，可以借鉴包括美国、欧盟和其他亚太地区国家的数据安全相关法律法规，来构建数据共享的合法利用和安全保护。普华永道认为，企业可以从六个方面着重考虑应对措施（见图1）。



图1：出海互联网公司安全合规的应对措施

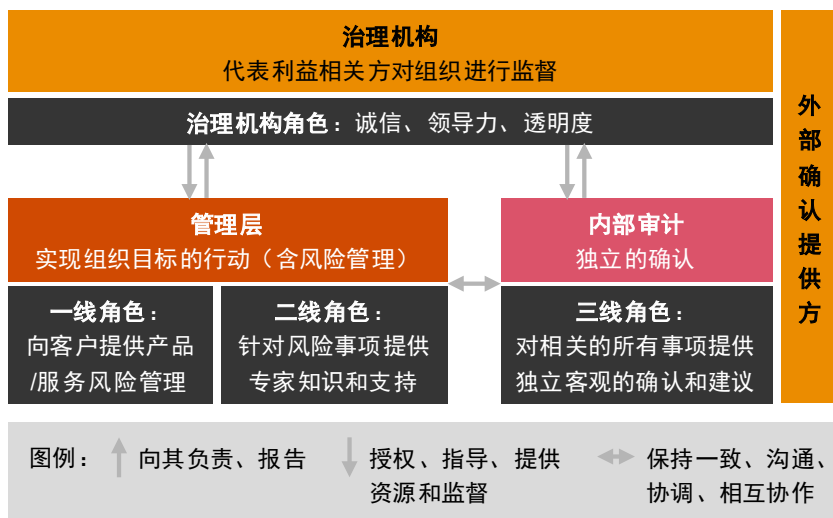


应对1

健全隐私保护组织机构

2020年7月，国际内部审计师协会（IIA）发布了新版“三道线模型”（Three Lines Model），通过更全面地理解风险，涵盖内控、协作、保证和问责制等因素，从而更好地反映业内对风险管理和治理原则的最新看法。新版三道线模型分别是治理机构线、管理层线和内部审计线（见图2），旨在帮助组织确定能够实现目标并促进强有力治理和风险管理结构和流程。风险管理不只是防御，而是保护价值。

图2：国际内部审计师协会的新版三道线模型



1. 治理机构对组织进行检视监督，并对组织的利益相关者做出回应，将组织的利益与利益相关者的利益联系起来。治理机构建立治理机制并将职责授权给内部各条线，并创建组织的文化。
2. 管理层直接领导为实现组织目标而采取的行动，同时也要密切关注风险并确保组织符合法律、法规和道德标准。管理层创建结构以确保组织的有效性，并管理内部控制以减轻风险。
3. 内部审计职能向治理机构负责，并向理事机构和管理层提供客观的建议和报告，说明其职能的有效性。内部审计相对独立于管理层，确保了内部审计在计划和执行工作中不受任何障碍和偏见，

在以前的模型中，三道防线分别是运营管理防线，风险和合规性监督防线，以及内部审计防线三道防线。换句话说，以管理控制

为第一线，风险和控制监控为第二线，通过内部审计职能的独立保证为第三线。关于内部审计，应从报告损失风险转变为就如何更好地经营业务向董事会和管理层提供建议，通过更有效的决策实现有效的风险管理和控制。

因此，企业应健全个人信息保护组织，明确企业业务部门、内控部门、合规部门、信息安全部门、风险管理部门、内审部门的职责，使各部门明确各自所处的位置，健全三道防线的职责。任命数据保护官，保护个人信息安全，筑牢三道安全合规防线。

应平衡协调三道线，创造和保护价值，即风险管控、审计检查，应更多站在“安全合规”基础上，促进“挖掘数据价值，推动企业数字化发展”，而并不是采用“一刀切”的方式阻止过于冒险激进的运营举措，拖运营积极探索新业务的后腿，这有可能加剧部门间的对抗，丧失了开拓业务增加收益的机会。

应对2

构建数据共享合规框架

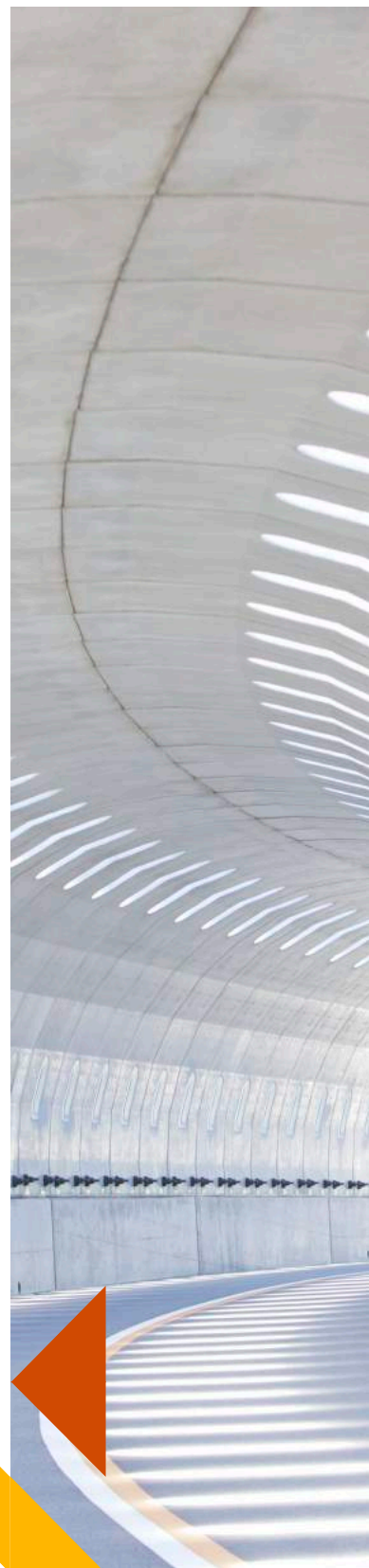
出海互联网公司应基于对国内外数据共享安全现状的分析，推进数据共享的健康发展，加强政策、法律、管理制度、标准规范和技术体系的统筹协调，构建符合本企业的数据共享安全框架。框架的建设可从法律法规体系、安全管理体系、安全技术体系、数据保护法律文件体系等维度进行考量。

1. 法律法规监管体系：如梳理并明确各国法律法规对数据本地化和数据出境的要求。

从目前来看，立法的重点在于个人信息保护、数据资源确权、数据跨境监管和数据交易监管等方面。以美国为例，美国的互联网经济极度发达，从产业利益出发，相较其他国家而言，更鼓励数据自由流动，因此美国允许数据有条件地向域外提供。而作为中国互联网企业近几年进军的热门国家俄罗斯，则对个人数据存储本地化的要求相当严苛，规定数据本地化是跨境传输的前提。因此，互联网企业应充分识别其所服务国家立法状态，并梳理各项条款，形成法律法规库，并采用动态观察机制，对监管趋势进行实时观察与应对。

2. 数据安全管理体系：如识别个人信息资产分布，建立数据分级分类标准，建设数据安全管理制度。

对数据共享的安全管控，除了充分识别各国、行业监管要求之外，结合本企业业务特色，以及对数据共享与委托方的充分识别，建立健全数据安全管理体系，以落实各项数据安全要求。数据安全应覆盖数据全生命周期，包括分类分级、去标识化、数据跨境、风险评估等内容，对数据的收集、存储、传输、处理、使用、删除和销毁进行全方位的安全管理。管理制度的设计上承法律要求、下接标准支撑，在实践方面能有效规范数据共享行为，确保数据共享组织管理机构职责明确、数据共享活动流程清晰、数据共享过程安全可控。





3. 数据安全技术体系：如研发和应用数据安全技术，保障数据全生命周期的安全合规性。

被视为黄金标准的欧盟《通用数据例保护条例》自实施以来，已公开宣布了493起违规案件，从罚款原因上看，有近三分之一是未充分采取技术和管理措施确保信息安全而造成的数据泄露。因此，互联网企业应针对数据共享所依托的平台，以及数据共享安全研发和应用新兴技术，包括安全监测、安全存储、数据溯源、密钥服务、基础设施、网络系统、数据采集、数据管理和数据存储等。

4. 法律约束力文件体系：如识别数据共享、委托处理等相关方，与相关方之间签署有一定法律约束力的文件。

企业应充分识别与数据处理活动相关联的实体，识别多方角色，如是控制者、处理之、共同控制者等，并结合数据处理活动具体场景，与外部相关方签署有法律约束力文件、与内部相关方（如集团型企业）通过有管理制度等约束力文件来明确多方在数据保护方面的权利、义务。

应对3 建设用户权益保障机制

企业应充分识别各国法律法规及标准对用户权益方面的要求，包括数据主体的知情权、访问权、更正权、可携带权、被遗忘权、限制处理权、反对权以及自动化决策个人相关权利。

企业应当建立健全的用户权益保障机制，明确各部门职责、义务，同时应明确用户权益响应处理相关的各项活动要求。此外，企业应审核自身的隐私声明和政策，以确保数据主体充分了解其各项权利。此外，从执行落地角度，各机构还应有更详细的落地执行方案，例如，如何从IT系统层面实现对数据流转的跟踪、控制、标记等。

应对4

优化数字营销推送机制

数字营销是指企业利用数字化的媒体、载具与目标受众人群进行互动，向其推广产品或品牌信息，目的是刺激目标人群的购买兴趣并促成购买交易。随着互联网的飞速发展，企业营销的主阵地逐步转化为数字化媒体，广告

形式的多样性也逐年增加。从传统的程序化广告、网页横幅广告、动态广告，到社交媒体账号等不同形式的推送。普华永道认为企业应顺应现有的数字营销趋势，加速优化现有的数字营销推送机制，体现在以下四个方面。

1. 推送权限管理

常见的授权包括通讯录访问、推送通知许可、无线网络使用权、用户隐私协议和地理位置访问等。企业只有获得了用户的许可和授权，才能让营销推送起作用，从而享受到数字化营销带来的优势和利益。

2. 推送时机管理

通过把握用户使用APP的频率，以及常规的生活习惯和受众人群的关注点等进行即时推送、定点推送或周期推送。

3. 推送内容管理

企业可以通过挖掘和产生出受众感兴趣、对受众有价值、能产生共鸣的信息进行营销推送。除了结合企业的品牌策略进行营销创意和内容制作，企业还可以采取针对不同用户标签进行内容编辑及推送。常见的用户标签有商业价值标签、用户偏好标签和生命周期标签等。

4. 推送渠道管理

企业应利用内外部平台对已知和未知客户进行营销。内部平台拥有流量渠道，包括官方网站、自助媒体平台、自我经营的社区等。外部平台即第三方流量渠道，主要利用第三方媒体、粉丝、资源等具有一定影响力的渠道，抓住客群激发涟漪效应，为品牌减少信任壁垒，达成高效的数字营销推送。



应对5

搭建隐私安全合规平台

互联网企业拓展海外业务的同时，也让网络安全、数据隐私等问题浮出水面。企业握有海量用户数据和大量公司内部机密数据，应承担保护信息安全的责任，并建立起隐私安全合规平台。平台应设立相关机制动态，关注当地政府的监管及合规要求，特别是对于出海东南亚以及

新兴的中东、非洲等地区的企业来说，这些地区的法律制度、法律环境和执法力度仍在完善中，因此需要及时把握政策变化的趋势及风向。平台还应该设有相关的监察机制，对企业内部涉及隐私合规的操作进行审核，从源头避免用户信息和公司内部信息的泄露。



应对6

获取国际安全合规资质

随着经济全球化的发展，合规也大步向国际化迈进，这意味着在合规全球化的浪潮中没有企业可以独善其身。不同国家、地区的合规要求差异巨大，企业国际合规的适应力和包容度决定了企业的生命力。目前已有多家出海互联网公司获取了国际通用认可的数据安全、云安全、隐私保护、信息安全等相关认证资质，以参照国际成熟标准体系，构建与运行一系列安全合规体系，同时通过获取国际认可的安全合规认证体系，进一步提升社会公信力。

例如，2019年8月，国际标准化组织（ISO）和国际电工委员会（IEC）发布了新的隐私标准ISO 27701，目的在于帮助组织建立符合国际隐私框架和法律基准的隐私信息管理体系（PIMS）。作为全球最大、最权威的国际标准化组织之一，ISO 27701的认证能在极大程度上表明组织符合《通用数据保护条例》的要求，即欧盟最严格的合规政策之一。ISO 27701提供

一种公正的认证方案，向数据主体证明其个人信息被企业妥善处理，能够为数据主体提供连续安全性和稳定合规的业务服务，有利于阐明组织内的角色和职责，提高企业内部能力和流程，避免违规，以及明确组织机构与其他利益相关者间的PII（Personal Identification Information，个人身份识别信息）处理方式。互联网企业需要依据国际标准ISO 27701，加强数据保护架构，增强企业在海外监管机构、海外合作伙伴、海外客户和海外雇员间的信任度，为企业赢得更多的机遇。

普华永道认为，企业除了关注国际上通用的安全合规体系认证之外，还应当关注各国特有的安全合规资质，例如中国的网络安全等级保护MLPS、新加坡的多层云安全MTCS、韩国的信息安全保护管理体系KISMS认证等，以全面提升企业出海发展中的安全合规能力。





小结

海外各国法规法律内容繁多，当地监管审查严格。对出海企业来说，如果不符合当地的法律法规，在当地就是违法经营，企业的经营行为不受当地法律与法规保护，并可能因违反法律法规而带来巨大损失。在跨国经营中，企业如果没有遵纪守法的意识，因利益驱动铤而走险，投机取巧，必然是无法在当地长期生存和发展。因此，互联网公司需要在跨国经营中，入乡随俗，遵纪守法，把安全合规放在首要位置，才能真正融入当地市场，打造坚强稳定的全球价值链，成为中国对外开放的“形象大使”。

普华永道拥有成熟的海外数据安全合规咨询服务方法论，已协助多家出海互联网公司建设数据安全合规体系、构建数据安全合规平台，同时协助企业获取了多项国际体系认证，包括ISO 27001、ISO 27701、CSA-STAR、ISO 27018等等。此外，普华永道从多维度，包括政治风险、数据合规风险、业务合规风险等方面进行风险地图建设，并结合普华永道的数据安全合规平台，辅助企业真正有效地落地健全的隐私保护体系。



联系我们

李扬

普华永道中国网络安全合伙人
电话：+86 (10) 6533 7800
邮箱：dennis.y.li@cn.pwc.com

包红霞

普华永道中国网络安全业务总监
电话：+86 (10) 6533 7958
邮箱：alice.h.bao@cn.pwc.com



本文仅为提供一般性信息之目的，不应用于替代专业咨询者提供的咨询意见。

© 2021 普华永道。版权所有，未经普华永道允许不得分发。

普华永道系指普华永道网络中国成员机构，有时也指普华永道网络。详情请进入www.pwc.com/structure
每家成员机构各自独立，并不就其他成员机构的作为或不作为负责。