亚马逊云科技 | pwc 普华永道

合规及跨境数据传输联合白皮书 2024

更新于2024年4月

声明

本《合规及跨境数据传输联合白皮书》由普华永道商务咨询（上海）有限公司（以下简称“普华永道”）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。其中普华永道负责撰写“第一部分 数据跨境传输概述”、“第二部分 合规及跨境数据传输解决之道”、及“附录：普华永道隐私保护合规解决方案---Privacy Ready”、普华永道下一代安全运营服务 MSS（Managed Security Service）”，单独享有该部分的知识产权；亚马逊云科技负责撰写“附录：亚马逊云科技敏感数据保护方案”，单独享有该部分的知识产权。本报告中所有文字、数据、图片、表格，均受中华人民共和国著作权法及其它法律法规保护。未经普华永道和/或亚马逊云科技书面许可，任何机构和个人不得基于任何商业目的使用本报告中普华永道部分和/或亚马逊云科技部分的信息（包含报告全部或部分内容），不得摘录、复制、储存在检索系统中，或以任何形式或通过任何手段（包括电子、机械、影印、录制或扫描）进行传播。如果任何机构和个人因非商业、非盈利、非广告的目的需要引用本报告中内容，需要注明“转载自普华永道商务咨询（上海）有限公司和 Amazon Web Services, Inc. 或其关联方（亚马逊云科技）联合发布的《合规及跨境数据传输联合白皮书》”。本报告仅作为一般性指导，并不构成提供任何形式的法律咨询、会计服务、投资建议或专业咨询。本报告所提供的信息不能取代专业税收、会计、法律咨询或其他相关专业咨询建议。在作出任何决定或采取任何行动之前，您应该咨询专业顾问，并向其提供与您特定情况相关的所有事实。

本报告的信息来源于本次调研所收集的数据以及公开的资料，我们对信息的完整性、准确性或及时性概不作出任何保证或担保，也不提供任何明示或暗示的担保，包括但不限于对业绩、适销性和适用于特定用途的担保，在不同时期可能会得出与本报告不一致的观点。

本报告仅供一般参考使用，不构成具体事项和咨询意见，普华永道不对本报告内容承担审慎责任，并且未就本报告内容做出任何明示或暗示保证。普华永道不就本报告内容向任何人士承担任何责任或义务，也不向任何人士承担因本报告所引起的或与本报告有关的任何责任或义务。读者不应依赖本报告内容做出投资或其他商业决定。如需具体意见，请咨询专业顾问。

本报告中由亚马逊云科技负责撰写的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、供应商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。

方案导览

1 数据跨境传输概述 ---- 01

1.1 数据跨境传输—合规趋势与解读 ---- 02

1.1.1 全球数据安全合规趋势与解读 ---- 02

1.1.2 中国数据安全合规趋势与解读 ---- 03

1.2 数据跨境传输—评估整体过程 ---- 04

1.3 数据跨境传输—申报解读 ---- 05

1.3.1 申报门槛 ---- 05

1.3.2 申报重点 ---- 05

1.4 数据跨境传输—评估结果分析 ---- 07

1.4.1 数据本地化趋势概览 ---- 07

1.4.2 数据本地化路径选择和常见场景 ---- 08

2 合规及跨境数据传输解决之道 ---- 10

附录 ---- 13

亚马逊云科技敏感数据保护方案 ---- 14

普华永道隐私保护合规解决方案--Privacy Ready ---- 16

普华永道下一代安全运营服务 MSS（Managed Security Service） ---- 19

01 数据跨境传输概述


Summary Report
Summary
Summary
Summary
Summary
Summary
Sale report

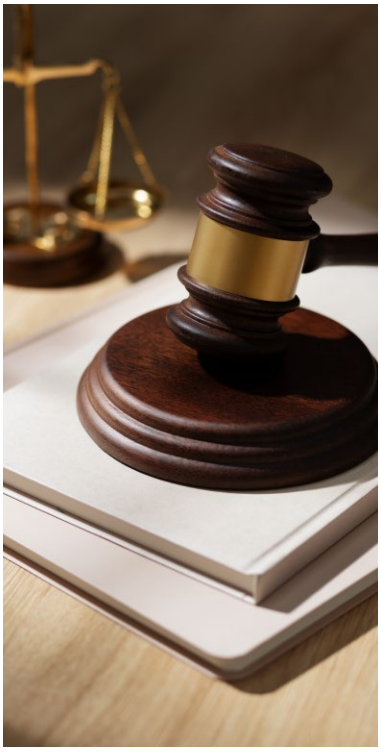
随着全球数字经济规模的持续增长，数据作为重要生产要素，在生产生活各个环节的重要作用正日益显现，数据流动的安全性受到越来越多的关注。全球范围内，对数据跨境活动的管控和监管正在逐步健全；目前，各国针对数据跨境流动密集出台了相关的法律法规，主要国家和地区的监管执行力度增强，数据合规制度数量增长、管辖范围逐步扩大的趋势明显，也让数据跨境传输合规成为了进行跨国商业活动的企业需要格外重视的课题。此外，数据跨境会加剧个人信息、重要数据和商业数据泄露及滥用的风险，导致企业的名誉和利益受损，还可能会给企业带来技术管理、资产管理和组织管理等问题。

数据安全是数字经济发展的底板，明确数据跨境安全合规措施，是保护个人信息、防范化解企业数据跨境安全风险、促进数字经济健康发展的重要保障。

1.1 数据跨境传输—合规趋势与解读

全球数据安全合规趋势与解读

随着互联网迅速发展带来的数据增长，各国更加关注对数据的合法利用。自欧盟推出《一般数据保护条例》（GDPR）以来，已有100多个国家或地区颁布或提出了数据保护或隐私保护法。目前，全球数据跨境流动和数据监管未形成较为统一框架，在各国国情、国家安全、隐私保护、产业能力等多元因素的复杂影响下，跨境数据流动监管制度较为差异化。



由于各国家和地区间立法驱动因素、国情和地区特性不同，其立法侧重点及发展趋势也有所差异，以欧盟和亚太经济合作组织为代表的地区性立法以保护个人数据为出发点，推动地区间数据流通，同时在监管和执法程序上更加标准化和透明化；以美国为代表的国家在合规立法中更看重数据自由流动带来的经济效益，在奉行整体宽松政策的同时，为特殊行业提供不同的法律依据，例如金融、医疗、电子通信、基础设施等行业；以俄罗斯为代表的国家在合规立法方面受政治因素影响较大，更关注以安全为核心的国内治理，对数据跨境流动施行严格管控，形成“内外双严”的数据安全发展态势。

中国数据安全合规趋势与解读

在全球的立法潮流中，中国也在过去的几年中加快了对于数据保护的各类立法。2016年11月7日通过的《中华人民共和国网络安全法》是我国在网络空间治理领域的第一部基本大法，首次在法律上对数据跨境流动进行了阐述，第37条规定：“关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储，因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。”此条款也被认为是对于中国数据跨境流动规则的确立，即“本地存储，出境评估”。

2021年，我国又接连颁布了《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》两部法律，进一步补充和完善了数据流动规则。2022年9月1日，由国家互联网信息办公室（后简称“网信办”）发布的《数据出境安全评估办法》（后简称《办法》）正式实施，将三部法律的原则要求进行了明确，界定了数据出境的适用范围，并对安全评估和申报工作给出了详细的实施程序。2024年3月22日，网信办发布《促进和规范数据跨境流动规定》（后简称《新规》），对现有数据跨境制度的实施和衔接作出了进一步明确。

数据跨境传输常见方式

在《办法》施行一年有余之计，许多头部企业已经积极开展安全评估并向监管机构递交了数据出境申报材料，涉及互联网、零售、医药、金融、汽车、民航、制造等诸多行业。在已经收到监管机构评估结果的案例中，某些企业的部分出境场景或部分数据项因缺乏充分的出境必要性，未能获批，对于这部分数据及系统进行本地化将成为下一阶段整改工作的重中之重。

值得注意的是，为进一步规范和促进数据依法有序自由流动，网信办于2024年3月22日发布的《新规》从不同层面释放了有利于数据跨境流动的积极信号，例如：明确了可豁免数据出境合规监管的场景、提高了数据出境安全评估申报和标准合同备案的适用门槛、提出了在自由贸易试验区施行出境数据“负面清单”制度的规则，等等。

1.2 数据跨境传输—评估整体过程

目前，我国数据出境管理的三种机制：**数据出境安全评估**、**个人信息保护认证**和**个人信息出境标准合同**，均已进入落地实施阶段。其中，本白皮书着重关注的数据出境安全评估的路径程序可以归类为六个阶段，分别为差距分析、整改、自评估、申报、评估、以及持续合规。

阶段一｜差距分析

通过访谈相关人员了解公司数据流转，审阅公司制度、授权同意文件、隐私政策、合同等文件，并对公司业务流程、相关系统进行梳理。以及，结合相关经验从而设计有效的检查点和控制点，发现差距并进行风险评估。

阶段二｜整改

以差距分析结果为基础，法规要求为导向、对公司风险策略及成本、业界趋势等提出合理的整改建议。

阶段三｜自评估

根据《新规》和《办法》要求识别自身是否适用数据出境安全评估，并完成自评估等合规工作。

阶段四｜申报

完成自评估等合规工作之后，数据运营者依照《新规》和《办法》在数据出境前做好风险自评后，并向相关部门提交相关材料。

阶段五｜评估

数据出境安全评估工作本着属地申报原则，由数据处理者向其所在地省级网信办提交申报材料。各地网信办在收到申报材料后，在5个工作日内完成申报材料的完备性查验（即形式审查）。国家网信办自收到省级网信办提交的申报材料之日起7个工作日内，确定是否受理并书面通知数据处理者。国家网信办受理后，将统一开展数据出境安全评估工作，开展实质审查并出具结论，完成数据出境安全评估。

阶段六｜持续合规

在通过安全评估后，企业仍需要对数据出境进行持续的评估监管。

1.3 数据跨境传输—申报解读

申报门槛

所有要向境外提供在我国境内（不包括港澳台地区）收集与产生的重要数据以及个人信息的企业与网络运营者都必须按照《新规》和《办法》要求，进行安全评估。

具体来说，企业开展数据出境安全评估工作的第一步是准确识别数据出境场景，也是至关重要的步骤。其次，在明确自身数据出境场景的情况下，企业需要进一步评估出境场景是否达到数据出境安全评估的申报门槛。《新规》对于哪些情况需要向网信部门申报评估给出了一些量化标准：

1）自当年1月1日起累计向境外提供100万人以上个人信息（不含敏感个人信息），或

2）自当年1月1日起累计向境外提供1万人以上敏感个人信息。

申报重点

《办法》明确要求所有数据处理者需要在向境外提供数据之前开展数据风险的自评估，因此风险自评估成为了一项法律要求。该工作需要企业全面筛查数据出境的场景和情形，并深入评估数据出境的风险。关于其风险的评估将围绕数据处理者和境外接收方两个方面进行展开：

数据处理者：

- 确保数据出境的目的、范围、方式满足合法性、正当性、必要性
- 识别并评估出境数据的数量、范围、种类、敏感程度及带来的风险
- 识别并评估在数据转移环节，采取管理和技术措施、能力等
- 识别并评估数据出境和再转移后泄露、毁损、篡改、滥用等的风险
- 确认与境外接收方订立的数据出境相关合同充分约定了数据安全保护责任义务

境外接收方：

- 确保处理数据的目的、范围、方式等满足合法性、正当性、必要性
- 确保识别了相应责任义务，并履行了相应的管理和技术措施等
- 确保评估并向境内数据处理者提供了境外数据保护相关法律法规的相关信息

安全技术能力要求

在各项评估项中，数据全生命周期安全防护体系尤为重要，企业应考虑网络安全防护能力、监控异常能力、保障数据跨境日志的完整性、保存数据跨境业务系统日志、建立数据全生命周期防护机制和应急处置能力，例如：

- 应具备数据出境前对个人信息进行脱敏处理的能力
- 应具备在数据出境传输时采取相应安全措施的能力（加密传输等）
- 应具备数据传输过程及处理过程中实施身份鉴别和访问控制的能力
- 应具备保留数据发送、接收日志的能力
- 应具备对数据接收、保存、使用、传输、销毁等各阶段进行审计的能力
- 应具备针对数据安全事件的预防、检测及响应能力
- 应具备对数据存储介质安全管理，及对数据进行备份和恢复的能力

数据出境的主要安全技术要求

对于以上安全评估和安全能力建设的要求，可以结合专业工具及相关咨询服务，帮助企业建立合规体系，并通过目标建立落地技术方案，包括在出境前进行数据分类/脱敏、事中监控、事后审计；也需要结合企业内部数据平台或治理平台现有能力，以形成企业内的整体治理的技术解决方案。

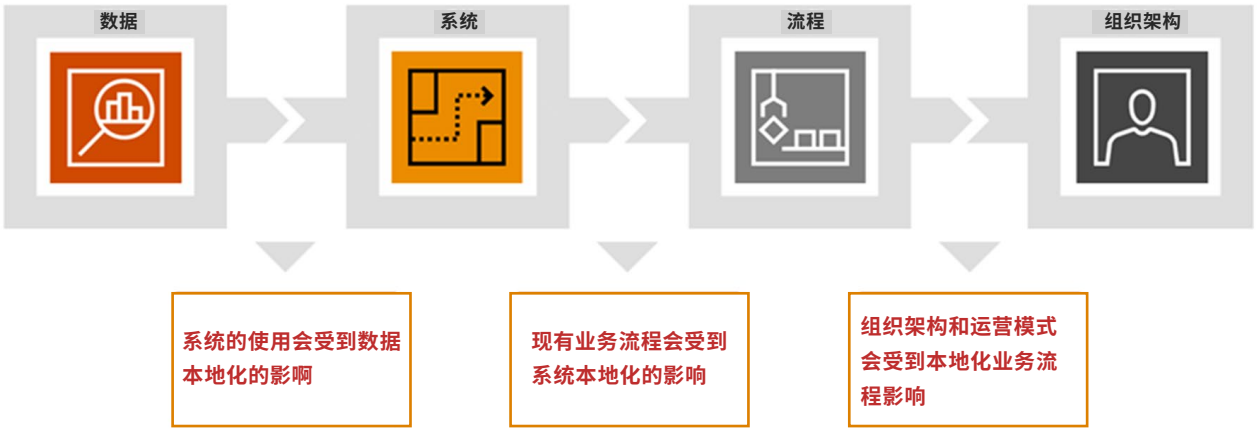
1.4 数据跨境传输—评估结果分析

在国内的数据跨境传输的监管逐步趋严，相关法规和指南密集出台的大背景下，数据跨境传输的申报和备案工作也在进行有序地开展。也随着相关部门逐步下发决定，一些企业的某些数据会面临不被准予出境的情况。

数据本地化趋势概览

由于某些数据面临禁止出境，数据本地化也以及逐渐成为不可绕开的话题。如果把数据出境安全评估比作一场竞赛的上半场，那本地化就是这场竞赛的下半场，企业在下半场更需打起精神，准备好充足的资源，迎接一场“持久战”的考验。

数据本地化是一项复杂的系统工程，它以数据为核心，以系统为载体，是对企业 IT 治理和运营能力的一次考验。对于大部分跨国企业而言，经典的 IT 管理模式是高度集中化的，由集团总部在境外统一提供 IT 基础设施服务，并统一托管主要应用系统，供不同国家的业务团队共享使用。这种模式从运营效率和成本节约的角度符合跨国企业的利益，但却不可避免的造成了数据的高度集中以及从中国境内向境外集团总部的单向流动。而本地化势必对这一既有模式造成颠覆，并且不同程度的本地化对业务的影响程度也不尽相同（如图例）：



尤其考虑到一些跨国企业在业务上须与境外总部保持必要的连通性和联动性，并也有着较为复杂的汇报机制，本地化的进程会对此类企业现有的业务流程和人员组织架构产生一定影响。公司不仅要考虑如何通过一些系统及业务流程方面的快速整改以满足合规要求，也要从长远的角度考虑如何构建一个符合本地化要求的本地业务流程并配备或调整组织架构以实现业务目标。

数据本地化路径选择和常见场景

尽管数据本地化在概念层面，是将数据的存储位置和数据处理的过程从某国家或地区转移到另一物理位置，但落实到具体的应用系统，其技术选择和实现路径则五花八门。目标系统的本地化方案可以被归纳为几种“原型方案”，以便进行分组讨论，降低复杂程度和沟通成本；从成本由低至高排序可以简单分为维持现状，流程变更，本地数据留存，系统迁移到成本最高的境内系统重建。不同的方案所对应的实施成本和剩余风险需要在做决策时予以充分考虑。

基于以上的维度，以企业内部两类最常见的应用场景为例，对其客户关系管理场景以及人力资源管理场景在本地化过程中需考虑的重点事项进行深入讨论分析：

（一）客户关系管理场景

在本地化过程中，大量的客户个人信息甚至敏感个人信息被收集和处理，因此，该场景中较为典型的客户关系管理系统（Customer Relationship Management，CRM）也往往成为企业内部存储个人信息数量最多的系统，自然也是跨境申报的主要系统，此类系统的特点包括：

- 可收集、关联和分析所有相关客户数据，包括联系人信息、与企业销售代表的互动信息、历史购买记录、服务请求、资产和报价/提议等。
- 企业销售人员可访问这些数据，并了解触点的最新动态，并据此创建完整的客户档案，进而建立牢固的客户关系。

CRM 本地化的重点事项：

- CRM 本地化，或将中国市场的数据从全球应用实例中剥离，对现有业务模式产生影响；在系统进行任何重大变更前，应对潜在影响进行充分评估，确保重大变更符合中国市场的长期业务战略。
- CRM 系统功能复杂、数据项繁多，不建议对合规要求作“一刀切”式的简单解读，而应逐个功能模块、逐个数据项的进行评估和整改，精准应对合规挑战。
- CRM 系统接口较多，上下游依赖关系复杂，在为 CRM 设计本地化方案的时候，应同步考虑其关联系统，评估变更后的数据流，避免因考虑不周而形成新的风险敞口或造成上下游系统的中断。

（二）人力资源管理场景

作为企业管理的一个通用场景，员工个人信息的出境也是广大跨国企业无法绕过的问题。在已获得批复的跨境申报案例中，监管机构对于员工个人信息的出境采取了相对包容的态度，但对于应聘者的个人信息以及员工的部分敏感个人信息采取了更严格的立场。对于企业而言，需考虑对该场景中现有较为典型的人力资源管理系统(Human Resource Management system, HRMS)进行必要的改造，以满足监管要求，此类系统的特点包括：

- 涵盖人事管理、能力素质模型、绩效管理、考勤管理、薪酬管理、招聘管理、培训管理、查询报表等功能的一体化整合应用系统，也是企业内部处理员工个人信息的主要系统。

HRMS 本地化的重点事项：

- 明确允许出境的数据项，对外传设置明确规则，以确保实际出境数据和允许出境数据保持一致，并留存传输日志。
- 对于禁止出境的数据项，考虑通过流程变更的方式对原有的数据采集和录入流程进行必要的改造。
- 对于应聘者的个人信息收集和处理，考虑境内的替代解决方案，并从原有的 HRMS 进行必要的剥离。

虽然数据本地化可以缓解数据跨境所带来的一些风险，但考虑到本地化的时间及成本问题，无论从短期或长期趋势所看，企业仍需在现下时间点，对在持续进行的数据出境的活动的风险进行的分析把控，并积极探索其各类可行的解决方案。

02

合规及跨境数据传输解决之道

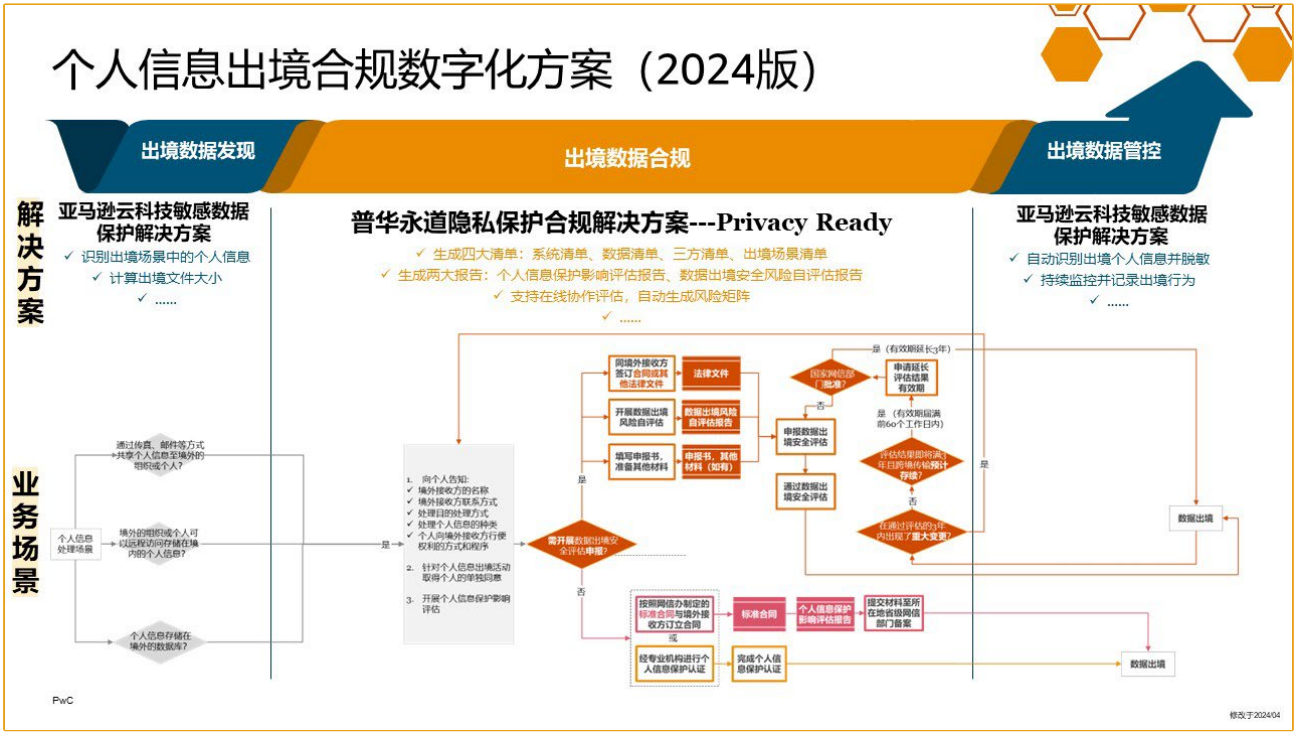
总的来说，现中国监管对于个人数据及重要数据的宏观监管要求为：

> 在境内收集和产生的个人信息应存储在境内

> 确需向境外提供的，应当通过国家网信部门组织的安全评估

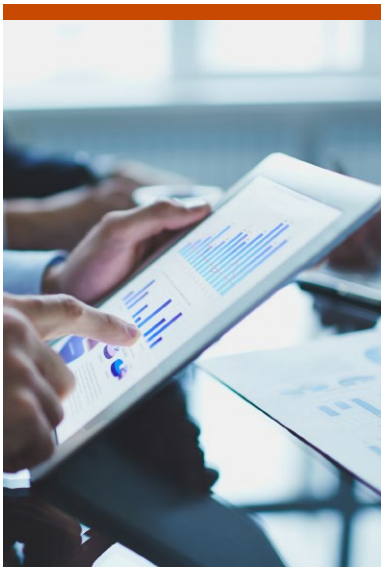
在这样的政策导向下，跨国公司将工作负载比如客户关系管理系统，人力资源管理系统及相关数据平台在国内落地的方向在逐步明确，速度也在逐步加快。

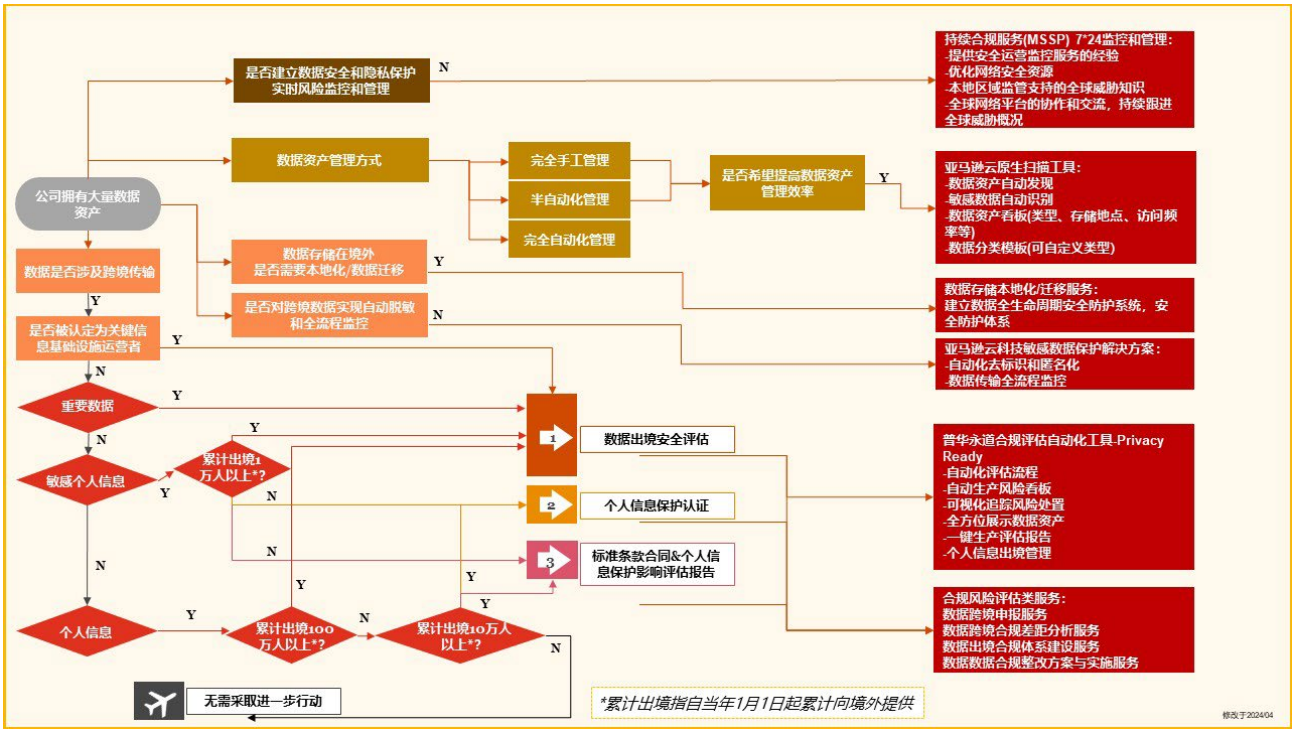
普华永道借助亚马逊云科技并结合双方的优势，提出“**合规及跨境数据传输**”解决方案，建立数据全生命周期安全防护系统，安全防护体系，在数据跨境合规评估，结果分析及长远合规规划及落地的全周期上，为企业保驾护航。



在使用本白皮书时，企业可参考如下问题核查业务场景是否适用：

1. 数据是否涉及跨境传输
2. 业务是否涉及个人信息
3. 是否已开展数据资产梳理和跨境场景识别
4. 主要应用系统和数据是否由亚马逊云科技托管
5. 是否已开展CBDT安全评估或标准合同备案工作
6. 是否已实现CBDT合规管理流程自动化
7. 是否已实现隐私合规管理流程自动化
8. 是否已制定本地化计划
9. 是否已实现自动化安全事件监测响应





更多解决方案，请参考附录以获取更为详细信息。 >>

附录

亚马逊云科技敏感数据保护方案

敏感数据保护解决方案 (Sensitive Data Protection Solution) 为客户提供了一个云原生的、开箱即用的企业数据资产管理平台，帮助客户定期了解敏感数据的分布与变化情况，为客户安全合规从技术角度提供依据。客户可以在中国区和海外区部署和使用该方案。

该方案支持企业添加多个亚马逊云科技账号，并自动发现各账号下的数据源 (如 Amazon S3、Amazon RDS 等)；提供200多种覆盖50多个国家和地区的敏感数据类型，也支持客户自定义敏感数据类型；支持配置数据分级分类模版，快速开启敏感数据扫描任务；基于 Amazon Glue 构建企业内部数据目录 (有些场合也称为数据字典、元数据管理、数据资产地图等)，提供可视化面板和发现任务报告；使用机器学习和模式匹配等技术高效地发现多种数据源中的敏感数据，以便于后续分类分级，以及通知相关的业务团队采取相应的保护措施。此外，方案还提供数据脱敏、全流程数据传输与监控能力。

功能特色

该方案是云原生亚马逊云科技解决方案，采用无服务器架构，可无缝地与其他亚马逊云科技的服务集成，支持在全球区与中国区部署；该方案的功能主要有以下特点：

- **中心式的管理界面：**

支持接入同一区域内多个亚马逊云科技的账号，可以自动发现各个账号下的数据资产，并自动生成数据目录。方案支持亚马逊云科技云上多种数据源，也支持介入其他云上及离线数据库的扫描。

- **可视化的结果呈现：**

提供直观的 Web 控制台，内置数据目录和敏感数据状态概览的仪表板，清晰展示数据位置、数据源、对象类型等信息，并为发现任务提供下载报告，为客户实现持续合规提供技术依据。

- **全面的数据发现：**

利用机器学习、模式匹配等技术自动发现和标记多个账户、多种数据源中的敏感数据，并且支持客户轻松设置和运行敏感数据发现作业，提供定期扫描的能力。

- **灵活的数据脱敏：**

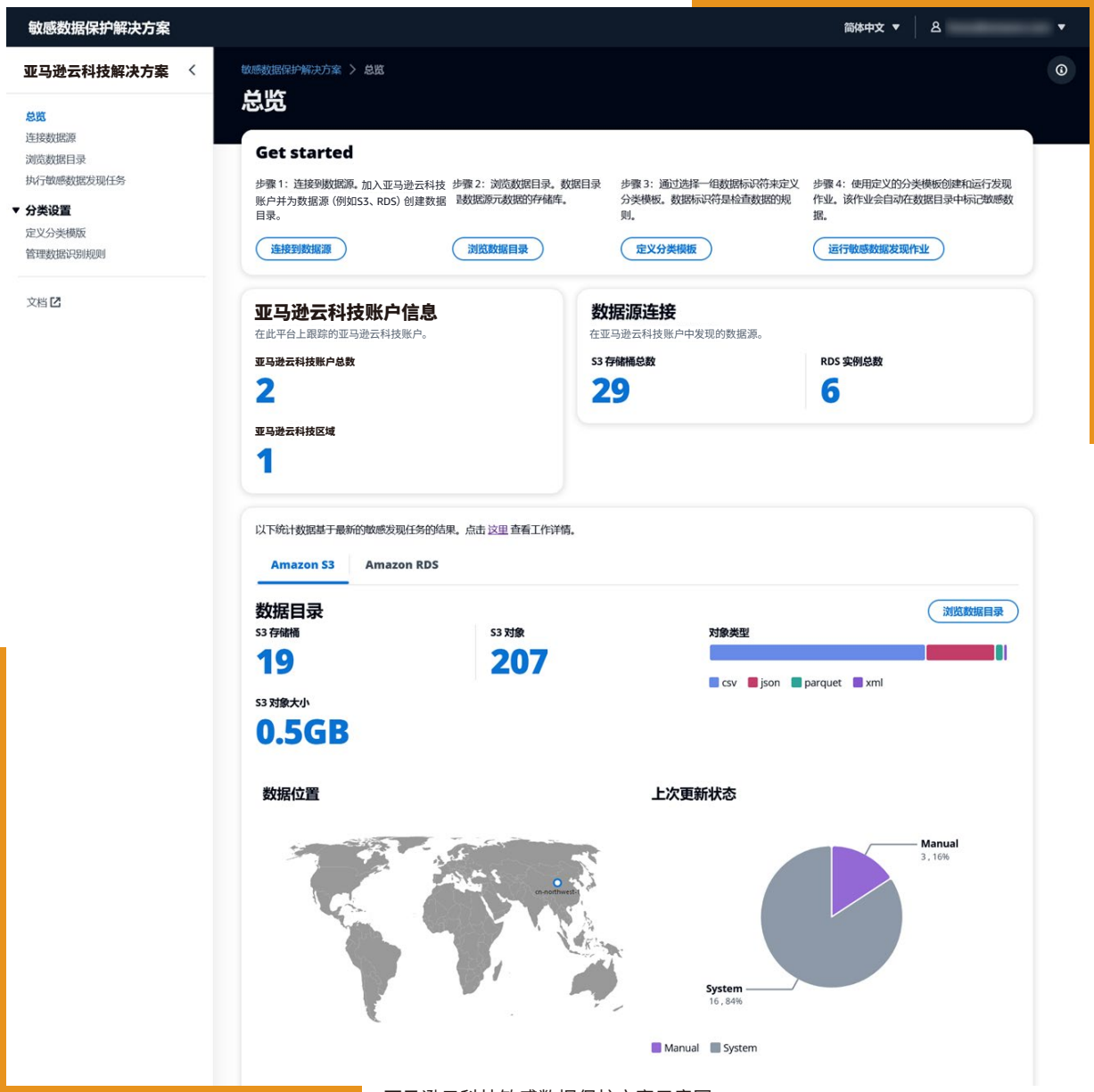
方案内置脱敏规则，可以帮助客户以 API 的方式行基于规则的脱敏和反脱敏 API。

- **丰富的数据分类：**

基于全球主要国家和地区的法律法规设置匹配规则，支持200多种内置数据类型，提供多种检测隐私数据的分类模板，并允许客户自定义敏感数据类型。

- **全流程的数据传输与监控：**

方案内置传输网关，客户可以采用此网关对于数据进行传输，方案可以对此网关传输的数据做审计。支持不同云环境数据传输。



亚马逊云科技敏感数据保护方案示意图

普华永道隐私保护合规解决方案--Privacy Ready

Privacy Ready 为企业提供了一个线上协作的个保法合规评估门户，帮助企业实现自动化风险隐私合规管理。重点提供五大业务功能模块以满足企业实现多场景隐私合规需求：

模块一

场景化隐私管理评估

建立业务场景合规管理闭环

全方位展示状态与风险

模块二

企业总体隐私管理评估

助力企业完善个人信息保护

管理制度与流程

模块三

资产清单

自动生成响应监管要求的

资产清单

模块四

个人信息主体同意管理

多渠道推送隐私声明

一站式管理同意记录

模块五

个人信息主体权利响应管理

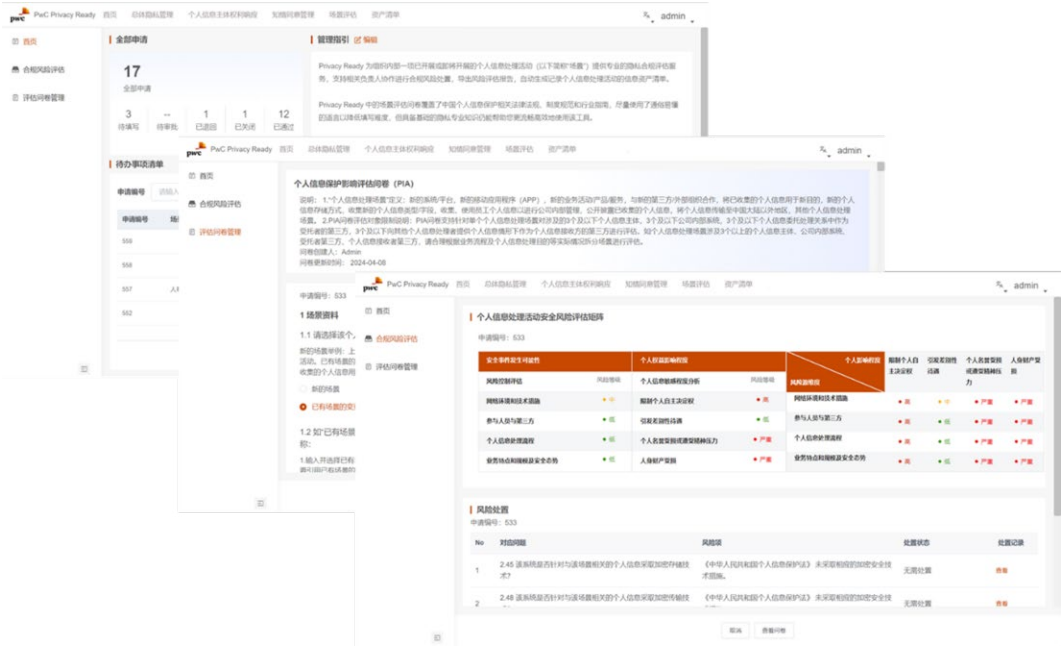
线上线下同步管理

协助企业快速响应行权需求

Privacy Ready 产品亮点

亮点一：自动精准

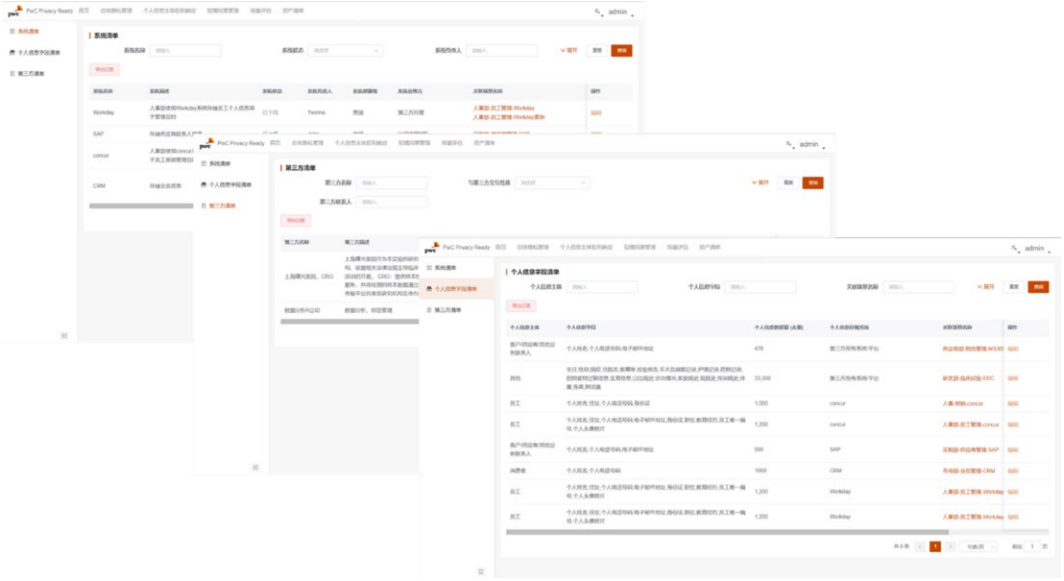
场景感知评估问卷及风险识别



此功能内嵌风险因子与规则引擎，一键自动生成评估结果，帮助企业实现简易清晰的合规评估方式、精准识别其合规风险，并审查追踪其合规活动。

亮点二：专业可信

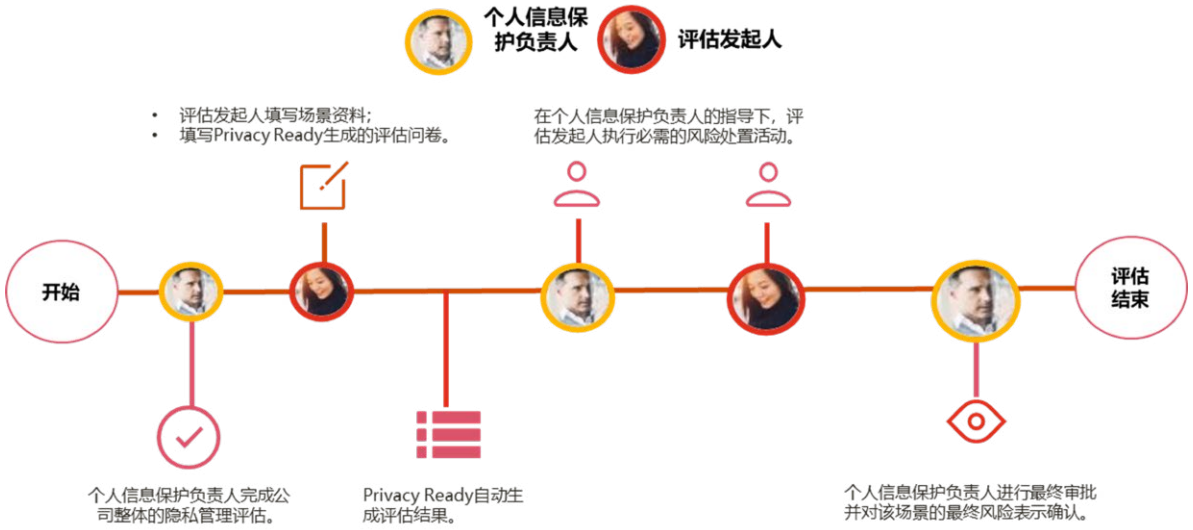
专业资产清单及评估报告



Privacy Ready 能够帮助企业实现自动化生成响应监管要求的资产清单，例如个人信息数据清单、个人信息处理系统清单、以及与第三方共享的个人信息清单。其能够根据场景评估中的数据实时更新各个清单中的内容，并且一键导出企业资产汇总表单与场景评估报告，帮助企业完成后续风险分析，处置与留档。

亮点三：高效便捷

预定义的工作流促进多方高效协作



Privacy Ready 帮助企业实现多角色协同工作，其端到端的流程使不同的用户角色能够同步进行线上协作模式，促使评估过程更加高效化。

在多变的监管环境和业务环境下，Privacy Ready 作为可定制的个人信息保护合规管理平台可以根据企业日常隐私合规管理与需求快速响应业务和法规变化，帮助企业有效应对个保法合规与风险处置。

普华永道下一代安全运营服务 MSS（Managed Security Service）

传统安全运营的痛点

其中主要包括：**安全人才管理，运营合规，运营投资，工作效率，技术复杂性，技术成本**等问题。

客户需求

数字化时代背景下，企业客户的安全需求主要如下：

- 随着组织的数字化转型不断发展，导致攻击面增长，组织需要更加灵活、全面、高效、经济的安全运营方案来应对各种安全事件。
- 不断出台的安全法规、政策，行业行规，及违规可能带来的处罚加重，使得组织需要在实现业务战略目标的同时保护业务及安全合规。
- 网络攻击不断地演变，组织在引入更高级安全功能方面需要更专业更有经验安全团队的帮助来规避潜在的风险。
- 越来越多的关键服务逐步迁移上亚马逊云科技云上，迁移过程中，组织需要统一可靠的安全运营平台及定制化方案来应对日益变化的业务环境。
- 自新冠疫情发生后的远程办公普及，业务多依托于线上，因此网络环境安全重要性突显，很多企业希望拥有强大的安全运营服务但无力分配时间、空间来投资于自身的设备和员工，因此如何获得专业又多快好省的安全运营服务成为组织亟待解决的问题。

方案优势

普华永道基于 Amazon CloudTrail, Amazon Config, Amazon Key Management Service (Amazon KMS), Amazon GuardDuty, Amazon WAF, Amazon S3 Server Access logs, Amazon VPC logs, Amazon Cloud-Watch logs 等服务实现数据采集，同时使用全球知名的 MITRE ATT&CK（网络安全攻击矩阵）框架的异常检测和关联规则，结合安全编排和自动化响应，持续监测并应对不断进化的网络攻击。安全运营中心所采用的技术工具，也均符合《网络安全法》等相关规定的要求。拥有世界级的红队攻击经验，深度防御；可根据最新的威胁情报，及时更新和改进网络攻击用例。同时将您组织视为一个整体进行保护，实时监控以提供全天候保护。通过安全专家和人工智能引擎的帮助，您的团队将集中精力应对关键事件，而无需面对密集的告警。服务采用高度灵活的可扩展模块化交付模式，它将满足您企业不同阶段的特定需求。

+150个 *威胁团队追踪*

+10亿 *每天事件监控*

+17年 *安全监控服务经验*

+200位 *全球客户*

安全运营中心（SOC）& SIEM 平台

联合署名

编写指导

- **普华永道**

徐世达 — 中国内地及香港地区风险及控制服务市场主管合伙人

黄思维 — 中国网络安全和隐私服务合伙人

黄财明 — 中国网络安全和隐私服务合伙人

- **亚马逊云科技**

王承华 — 大中华区专业服务事业部总经理

陈晓建 — 大中华区产品部总经理

白　帆 — 安全合规服务总监

主编人员

- **普华永道**

徐　静 — 中国网络安全和隐私服务经理

陈雪凝 — 中国网络安全和隐私服务经理

- **亚马逊云科技**

苏　璠 — 解决方案中心高级产品经理

周玉林 — 解决方案架构师高级总监

杨　波 — 合作伙伴高级解决方案架构师

杨帅军 — 资深数据架构师

邵士毅 — 解决方案架构师高级经理

徐　丽 — 合作伙伴拓展经理

亚马逊云科技 | pwc 普华永道

扫码关注
亚马逊云科技公众号

扫码查阅
亚马逊云科技合作伙伴
资料中心

扫码查看更多
亚马逊云科技全球咨询合作伙伴
—普华永道解决方案