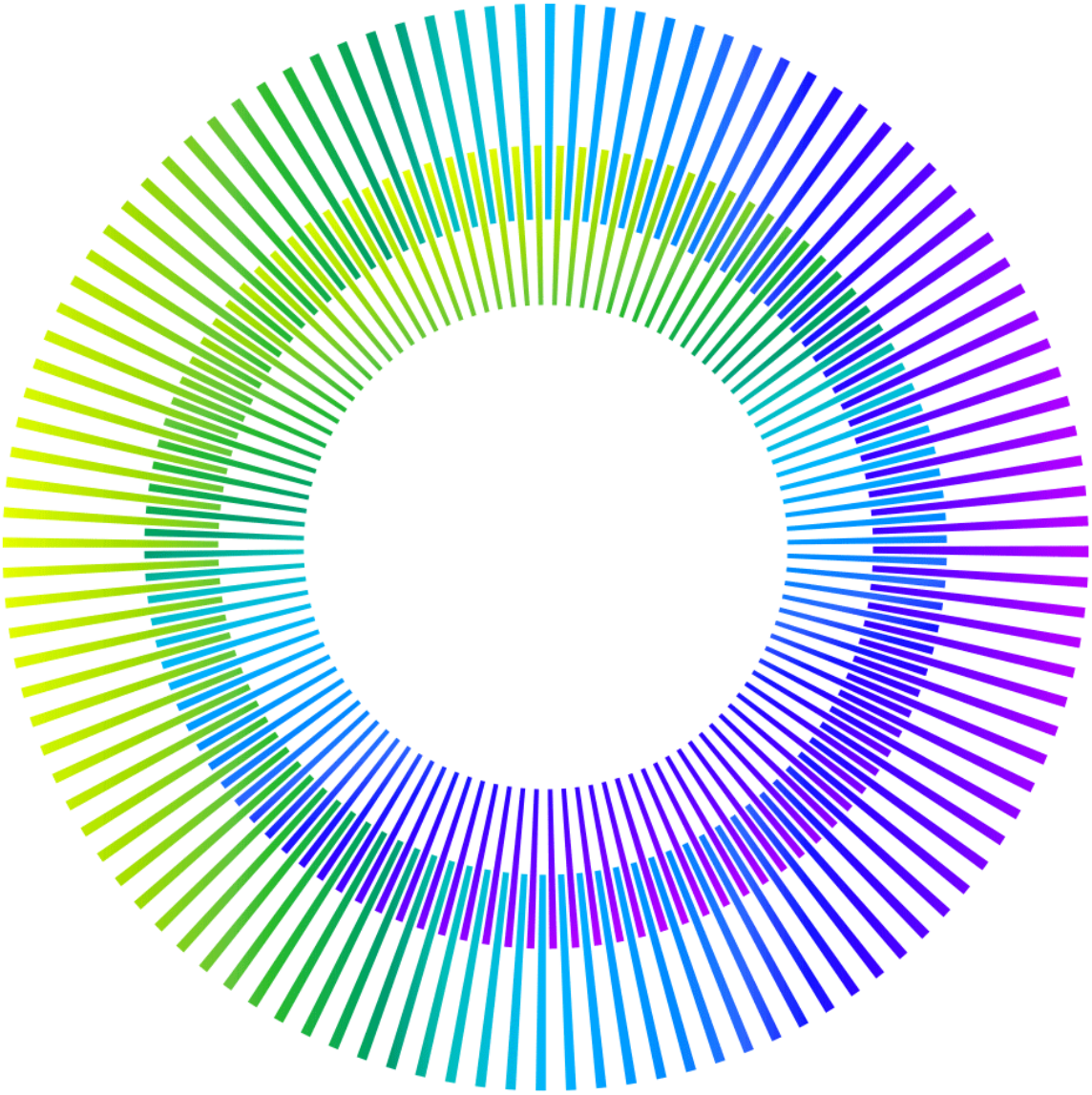
ZTE中兴

Deloitte.



数据跨境合规治理实践

白皮书

2021

序言

数字经济正加快驱动产业融合变革，拓宽和提升经济发展空间。数据流动在数字经济发展中发挥着重要作用，数据要素的市场化配置上升为各国宏观战略考量。为了平衡“数据安全”与“数据红利”，建构和凝聚数字经济优势，主要国家和地区纷纷推进、强化数据跨境内部规则的完善，积极推动、参与数据跨境国际规则的制定，形成了不同的数据跨境流动合规规制圈。

全球数据跨境流动规则框架下，没有企业可以回避数据跨境流动规则的深刻影响。企业应高度重视数据跨境流动管控形势和发展态势，在全球业务和经营活动中应主动进行合规遵从，对冲和降低风险和不确定性压力，并将数据跨境风险控制机制化、常态化。

古语有云：“万物得其本者生，百事得其道者成。”“以风险为导向”的合规治理思想是迎接数据跨境规则挑战的重要方法。确保商业可持续，合规管控与效益追求并重，一方面在制定完善跨境治理方案的基础上完成系统性合规整改，主动降低外部风险；另一方面利用已有的企业统一合规框架基线，以及双边、多边国际包容性规则降低投入和运营成本。数字文明新时代下，共同探索、相互借鉴数据跨境合规治理实践，通过持续和务实的合规建设，有助于优化企业数据合规体系、共建产业数字合作格局。

申楠

主编：高瑞鑫、申燕茹、方圆、何智聪、王晨、刘天雅、杨宇鑫、徐敏、肖腾飞、黄惠娥、Marco、Alberto

参编：周宇心、王志宇、丁沛、魏安迪、梅傲婷、宋伟强、陈立生、文华龙、赵智海、李琳、池逸飞、惠兆帅、曲绅维、龙浩、陈威特、陈正伟、林苏明、胡志强、邓园园、岳艳红、鲁可兴、林峻、张亮、张哲、杨柳

目录

数据跨境合规治理实践白皮书

（2021）

一、全球数据跨境规则现状及发展趋势

1.1 数据跨境规则现状

数据跨境规则模式往往与数据安全政策偏好相关联。现有规则大体分为两类：

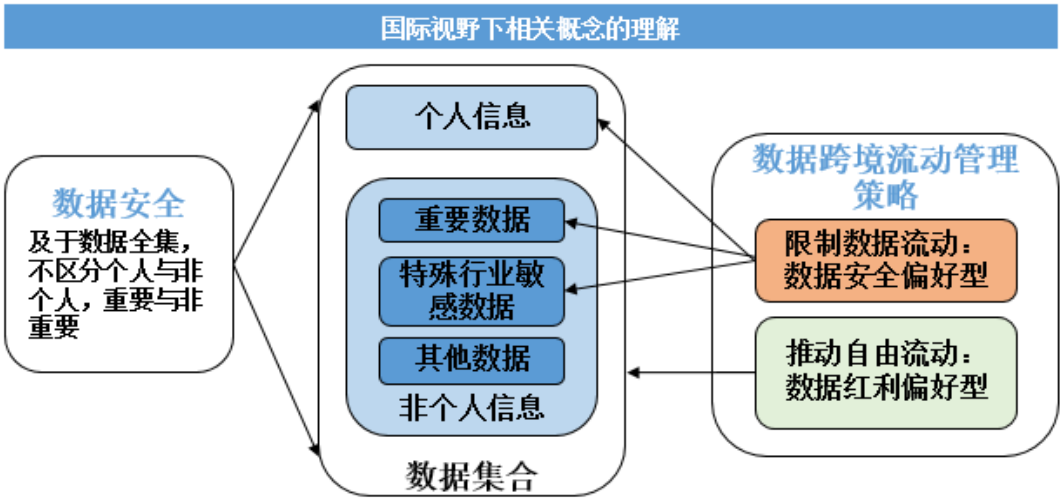
限制性规范，常见为一国家或地区针对重要数据或个人信息进行出境限制，以维护数据安全或数据主权，即数据安全偏好型。

推动性规范，常见为双边、多边或国际组织，为推进数据跨境安全有序地跨境流动，制定双/多边国际协定或条约框架，以促进数据红利最大化发展，即数据红利偏好型。

对数据主体而言，限制性规范中涉及的数据类型一般为个人信息、重要数据或特殊行业的敏感数据；推动型规范中并未对数据性质作显著区分。

对企业而言，限制性和推动性规范均具有现实意义，限制性规范因占据主导地位将成为企业关注的重点。一方面，根据限制性规范要求，严格实施合规治理及管控运行，最大限度规避违规风险；一方面，在合规管控运行前提下，充分利用推动性规则弹性空间，降低企业跨境管控压力和成本。

注：基于“非强制”、“仅约束缔约方”特性，推进性规则多不具备普遍约束力。



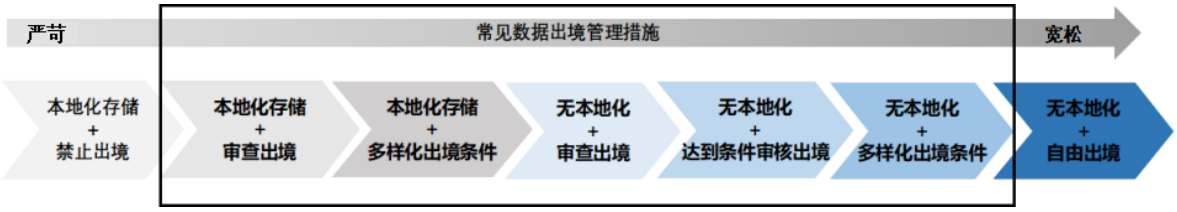
1.1.1 主要国家规则多为限制性规范

限制性规范，即一国家/地区的数据出境规则，根据当地法律体系、历史传统、风险偏好的区别而呈现出不同严苛程度。目前，尚无国家完全禁止数据出境，或者对数据出境完全不加限制，大部分国家/地区集中分布于中段。

中段形式大体表现为：国家安全与数字红利并举，促进数字经济发展的同时寻求本地化，如印度、俄罗斯；市场自由与数字规则并重，提倡数据跨境自由流动的同时规定多样化的数据出境机制，如欧盟、新加坡。

参考附件：《全球主要数据跨境限制模式》

1.1.2 国际组织机制多为推动性规范



国际组织积极制定数据跨境流动规则框架，推动数据在国家/地区间有序流动，以期减少数据跨境流动摩擦，最大限度地发挥数字作用。其中，经济合作与发展组织（OECD）、亚洲太平洋经济合作组织（APEC）等国际组织确立了若干数据跨境流动的原则，建立了若干具有代表性的框架。

国际组织对于成员国间的跨境数据持开放态度，希望通过畅通的数据跨境渠道进一步加强组织内数据的流通效率，但对于数据对组织外的跨境则较为谨慎。欧洲的《通用数据保护条例》（GDPR）提供了目前唯一的对外跨境合规框架，并采取了世界范围内的持续性实质推广，对全球多个国家/地区的相关规则产生了显著影响。

参考附件：《国际组织数据跨境流动框架》

1.1.3 中国具有差异化和多层次特征

中国数据跨境法律法规处于创新制定和持续完善的过程。随着《网络安全法》《数据安全法》《个人信息保护法》（以下简称“个保法”）发布，数据保护相关上位法的“三驾马车”已然形成；相关规范性文件、国家标准等陆续出台构成规则体系。

中国数据跨境规则体现出分层管理特征，对重要数据和个人信息的合规管控进行了差异化设计。对于特定行业的特定类型数据，明确本地化要求；数量较大的个人信息和重要数据进行境内存储，经监管机构审批出境；一般个人信息出境，规定了标准合同、安全认证等多样化合规措施。

参考附件：《中国数据跨境相关法律法规》《中国特殊行业数据跨境要求》

1.2 数据跨境发展趋势

1.2.1 数据分级分类管理成为主流

个人信息、重要数据、核心数据等不同数据类型涉及的法律风险和所需的保护要求各有不同，主要国家尝试采取数据分级分类监管，形成宽严不同的数据跨境流动管控政策。

1.2.2 探索促进统一数据跨境规范

随着数据跨境流动规模的扩大，各国家和地区已试图将数据跨境流动治理纳入国际贸易规则，现有国际治理框架难以满足全球数据治理的特点和需要，需要为由无形资产主导的新的数字世界建立一个新的治理结构，以最大限度的发挥数据价值。

1.2.3 数据主权管辖博弈冲击持续

长臂管辖会将一国的执法效力扩展至数据所在国，对数据所在国数据保护法实施产生冲击，对国际司法适用原则产生冲击，进而对全球的数据安全合规框架产生深远影响，并在很大程度上改变全球数据主权的游戏规则。

1.3 数据跨境类型

当前各界对数据跨境界定仍存在差异，尚未形成统一认知。通常将其理解为“数据从一法域被转移至另一法域的行为”或“跨越国界对存储在计算机中的机器可读数据进行处理”。以“境外实体接触”为标准，数据跨境主要包括两类：

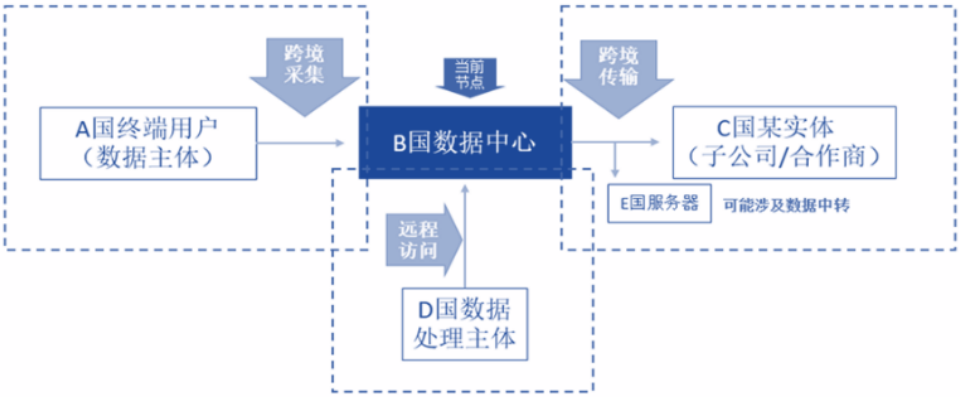
第一类：数据跨越国界的传输、转移行为；

第二类：尽管数据尚未跨越国界，但能够被境外的主体进行访问。

其中，一种特殊情形为直接的跨境数据采集，即数据直接从位于 A 国的数据主体处被采集至 B 国的数据中心，并未在 A 国进行存储落地。由于实践中难以在全球范围内部署服务器，必然存在大量的跨境采集情况。

概念	定义	场景类型	场景示例
数据跨境	任何正在转移数据到其他司法管辖区或是转移到其他司法管辖区之后意图再转移的行为。	**1. 跨境传输** 数据的接收方，基于合同或其他基础，接收来自于其他法域的数据。	某跨国企业的子公司通过内部的系统传输数据至位于另一司法管辖区的总部。
		*跨境采集 跨境传输是跨境传输的一种特殊情况：数据的采集方基于某种需求，直接从位于另一法域的数据主体处采集数据至处理方所在地，而未在数据主体所在法域进行任何处理行为。	某跨国企业的员工使用内部系统填报个人信息，而该系统的服务器与该员工所在地不属于同一司法管辖区。

概念	定义	场景类型	场景示例
		2. 跨境访问 数据的访问方基于某种需求，访问位于另一法域的系统服务器，读取其数据库中的部分或全部数据并进行一定的自动化处理动作。	某跨国企业在中国为欧盟境内的客户提供系统远程运维服务。

跨境流转示意图


1.4 数据本地化模式

数据本地化是数据跨境管理的一种措施，通常理解为某一主权国家/地区，通过制定法律或规则来限制本国/地区数据向境外流动，是对数据出境进行限制的做法之一。

数据本地化要求数据服务器位于本法域境内，在境内存储或处理数据。目前，全球多个国家/地区提出了本地化要求，宽严程度有所不同，几种模式交织并行。

模式	具体情况	代表国家	涉及数据类型
无本地化要求，但有出境限制	原则上允许数据合规流动	欧盟、日本	一般个人信息
境内存储副本，对转移或出境无限制	仅要求将数据副本存储在国内计算机设备中，对外转移或处理数据副本无限制，其通常的目的是为了确保监管需求。	印度（2018 年个保法草案）	一般个人信息
境内存储，可境外处理	数据必须首次存储在国内，满足出境合规条件的情况下可以向境外传输，在境外处理数据。	俄罗斯	一般个人信息
境内存储、处理	数据只能在境内存储、处理，仅在特定的条件下（如国家安全需求）的情况下，经审批出境。	美国、土耳其、澳大利亚	特殊类别非个人信息/重要数据

本地化通常为非“全量”的本地化：

（1）对数据类型进行划分：对不同的数据类型提出不同的保护要求，对特定类型的数据提出本地化要求。最常见的受限的数据类型包括生物健康、金融、征信等重要数据。

参考示例：印度政府将数据类型划分为关键个人信息、敏感个人信息和一般个人信息，关键的个人信息必须存储在印度境内，但也提供了例外条件；对于敏感的个人信息，必须存储在印度境内，但其副本可以按照跨境转移的要求进行传输到印度境外。

（2）对收集数据的主体进行划分：对不同的特定主体提出了不同的本地化存储要求。

参考示例：印度尼西亚政府要求只有公共电子系统运营商才必须将其电子系统和数据放置在印度尼西亚本地。美国国防部规定所有为该部门服务的云计算服务提供商须在境内储存数据，美国国家税务局发布规定要求税务信息系统应当位于美国境内等。

二、企业数据跨境典型场景及管控要点

2.1 数据跨境合规主要痛点难点

随着经济全球化、数字化的深入发展，企业开展境外业务时面临的数据跨境监管形势日益严峻，数据跨境管控过程的痛点、难点，成为数据合规治理的热点、焦点。

2.1.1 数据多样，跨境数据的法律属性识别与分类困难

数据体量大。大数据背景下，企业生产经营过程中产生的数据呈爆炸式增长，且涉及数据类型丰富多变。从数据主体角度，包括客户数据、用户数据、合作方数据、供应商数据、内部员工数据等；从业务经营角度，包括产品数据、日常经营数据、研究\研发数据、内务管理数据等，极大增加了企业数据管理的难度和成本。

属性识别难。关于个人信息、重要数据等在监管定义上通常采用“概括式”的表达形式，虽为企业提供了一定灵活度，也为企业对数据的法律属性类型识别带来了模糊性和不确定性；不同法域对个人信息、重要数据等概念定义存在差异甚至冲突，对企业跨境数据的属性识别和应用管控造成困难。

参考示例：在与欧盟的电讯运营商合作的国内手机厂商可能会碰到类似的数据合规困局，欧盟的电讯运营商会要求合作的中国手机制造商提供其手机设备的标识符如 IMEI 信息，以保障网络运营商对设备的使用，根据中国标准，设备硬件标识符属于个人信息，于是国内的手机制造商会要求欧盟运营商签署数据处理协议；但欧盟运营商依据所在国法律，认为因整个业务流程中，运营商仅获取了硬件标识符，未能获取其他任何数据，进而无法通过硬件标识符识别到特定使用该硬件的用户，不具备可识别性，不是个人信息，于是拒绝签署数据处理协议（DPA）。

载体拆分难。多种类型的非结构化数据，可能同时集合在同一载体或分散在不同载体中，难以拆分、合并和精准识别，如何按照数据来源、内容、用途等进行数据分类梳理，成为企业数据跨境合规管控的实务难题。

参考示例：公司内部搭建的文档管理平台，存储了内部包括项目业务资料、商务合同、财务单据等大量文件，文件中的业务资料如果标识了他国的交通路网、能源节点、敏感区域位置则可能涉及他国重要数据；商务合同中可能包含签署双方的法人代表个人信息；财务金融单据中可能涉及敏感个人信息等。但因为数据量大，且以非结构化的形式出现，难以对每类数据做精准识别。

2.1.2 场景复杂，数据跨境的路径、角色及责任识别困难

企业业务场景多样。随着企业成长与发展，业务版图和业务领域不断扩展或变化，配套的内部支撑流程也随之细化，各业务场景交互融合，业务数据随之交互融合，加大了数据跨境路径梳理和相关责任方识别的难度。

参考示例：某大型企业旗下存在多个业务板块：金融业务板块包括银行、保险、证券等；非金融业务板块包括系统产品开发、供应链管理、市场营销等；同时还包括人力资源、财务管理、行政管理、法律合规、内控审计等内部支撑板块，均涉及大量的数据处理活动。

数据流转路径复杂。数字化转型背景下，企业的业务数据往往通过线上系统进行流转处理，业务系统间数据存在交叉传输的情况；同时，出于成本、效率等多因素考虑，企业的系统服务器通常集中部署、统一管理，导致在全球化业务开展过程中涉及频繁、复杂的数据跨境流转。

参考示例：某企业的系统服务器集中部署于总部所在地、由总部统一运维管理，导致在开展境外业务过程中涉及大量数据跨境流转场景，例如数据从境外分支机构传输至总部服务器存储，境外分支机构从总部服务器调取数据，境外发分支机构直接访问总部服务器数据等。若多家境外分支机构纳入数据跨境传输管控全景，各分支机构之间也可能通过总部服务器相互调取/访问数据。

角色法定含义不同。不同的数据处理角色承担相应的责任和义务，准确识别企业在数据跨境场景下承担的角色、清晰界定双方责任和义务，对数据跨境合规管控非常重要；不同法域对数据处理角色的定义、相应责任与义务的规定不尽相同，复杂的数据流转链条下，企业难以准确判断自身角色、明确责任和义务，为企业数据跨境合规管控的力度决策带来障碍。

参考示例：欧盟 GDPR 对个人数据的控制者与处理者的责任分别有详细的规定；而中国个保法没有区分个人信息处理过程中控制者与处理者角色，统一称为“个人信息处理者”，并规定个人信息处理者共同处理个人信息将承担连带责任。

2.1.3 规则变动，规则要求多层次、多类型、不断演进

全球规则层次多样。全球尚未形成统一的数据跨境治理框架，各国家/地区受国家安全、数据主权、人权保护、地缘政治、贸易模式等因素影响，制定了侧重点不同、各个层次的数据跨境规则，数据治理和数据跨境流动政策具有很大差异，并积极寻求扩大各自数据生态系统，企业数据跨境规则研究和遵从难度显著增加。

不同法域规则冲突。企业在开展数据跨境流动活动时，需要同时考虑数据输出地和输入地的数据跨境规则，但不同法域数据跨境规则的不同，对企业“双向合规”带来困难；由于长臂管辖等因素，同一法域的数据处理行为也可能需要满足多法域规则，存在法律冲突隐患，对企业数据跨境合规应对和治理能力提出考验。

参考示例：数据的处理必须具备合法基础，但各法域的数据处理的合法基础不尽相同。在我国境内处理欧洲公民的数据，需要同时满足个保法及 GDPR 的要求。我国个保法为避免扩大解释，未将“数据主体利益”及“控制者合法利益”两个边界较模糊的合法基础纳入条款范围。若以“合法利益”为基础在中国境内进行进行数据处理，则可能因失去法律承认的合法基础而违规。

规则动态发展变化。自欧洲 GDPR 正式发布以来，隐私和数据保护的立法和更新浪潮在全球范围内迅速蔓延；各国家/地区对数据保护的重要性形成了普遍认知，基于公民权益、国家安全、数据主权等多重考量的数据跨境规则呈现明确化、具体化的特征，使企业数据跨境合规体系的设计、执行和维护成本进一步加大。

参考示例：GDPR 第 15 条对隐私仪表盘提出了要求：“数据控制者不得使用任何的技术手段阻止用户行使访问权，在可能的情况下，数据控制者应该给予数据主体远程访问其数据的权利，特别是提供在线服务的访问工具，例如隐私仪表盘。”两年后，西班牙通过《默认数据保护指南》，对隐私仪表盘提出了十分详尽的配置要求。即便其不具备强制执行的效力，也有着极高的参考价值。西班牙作为欧盟成员国之一，率先在用户控制方面提出了要求，将会影响到其他国家细化规则的进度，这将大大增加企业合规成本。

参考附件：《全球数据跨境法律法规清单》《全球数据跨境管控要求清单》

2.2 数据跨境典型场景管控要点

2.2.1 数据跨境合规典型场景

基于企业常见业务活动，结合数据跨境基本模式，企业存在若干数据跨境典型场景。

（1）集团管理中的数据跨境。在跨国企业的集团内部日常运营管理过程中，一方面，总部对分支机构有集中管理的客观需要；另一方面，分支机构对总部也有对数据调用的实际需求，数据跨境成为企业运营中必要、高频且规模化的常规数据处理活动。常见的数据跨境场景有：

业务场景	数据跨境场景	相关字段
供应商管理	为进行供应商管理，企业会收集全球供应商相关个人信息录入位于总部的供应商管理系统进行维护。	供应商联系人、接口人、高层个人的姓名、职务、电话号码、传真、电子邮件、财务账号等信息
采购管理	为进行采购事宜的商谈及合同履行，企业会收集全球相关对接人的个人信息，并传输至总部采购部门进行管理、使用。	客户对接人姓名、国籍、地址、邮编、联系方式等信息
财务管理	企业总部统一管理境外子公司员工的薪酬发放、报销、报税等相关事宜，员工账户信息、报销单据等将涉及跨境传输。	员工账户信息、薪资数据、报销单据、税务单据等信息
人事管理	企业总部为完成招聘、公司内部人力资源管理等工作，需要上传境外员工或候选人个人信息至总部进行统一的管理。	员工信息包括姓名、电话号码、职位、教育背景、工作表现、薪资福利等信息 候选人信息包括姓名、电话号码、资格证书、教育背景、工作经历等信息
文档管理	为便于内部文档共享和管理，企业通常建立全球文档管理平台对企业内部文档进行整合。	企业内部制度、合同、过程性文档等内部文件中可能包含的个人信息

（2）业务活动中的数据跨境。企业业务活动中同样涉及大量数据跨境情况，一方面，企业为扩展海外市场产生大量产品销售、品牌推广、售后维护相关数据跨境传输；另一方面，企业为节约成本部署全球供应链时也致使数据跨境流转路径复杂。常见的数据跨境场景有：

业务场景	数据跨境场景	相关字段
供应链	企业在供应商采购、国际货运及仓储等环节，企业会收集供应商、收货人、仓库对接人等相关个人信息，并上传至总部供应商部门进行管理、使用。	供应商、收货人、仓库对接人的姓名、国籍、联系方式、收发地址等信息
市场销售	企业在进行全球市场调研、客户关系维护等过程中，需要收集、使用和维护客户信息。	客户/潜在客户个人信息，包括姓名、电话号码、电子邮箱等信息
远程运维	企业通过网络远程接入境外客户的系统网络进行技术支持、故障处理等，其中会涉及客户个人信息的处理。	客户电话号码、IMSI、IP address、呼叫记录等信息
电商平台	电商平台一般由总部或第三方运维管理。企业在全球开展线上产品销售业务时，总部需跨境处理电商平台用户订单、物流信息等。	平台用户姓名、电话号码、订单信息、收获地址等信息
品牌管理	企业在境外组织开展品牌宣传、展会等活动，需采集参会者个人信息并传输至组织方所在境内。	参会人员个人信息，包括姓名、性别、国籍、电话号码、电子邮箱等信息

2.2.2 数据跨境合规要点

各企业的数据跨境场景各不相同，各法域的数据跨境规则也并未具体到场景维度，合规管控一般进行统一基线。各个场景的风险环节存在差异，在将统一基线下沉到具体业务活动中时，侧重点可能有所不同。对于企业，合规管控全景大体包括两部分：

一是针对全业务活动的合规管控基线，基于对各法域跨境规则分类、整理而形成基线；

二是针对特殊场景中的管控侧重点，设置特殊的管控要点。

（1）通用合规管控要点

结合法律法规的要求、相关行业标准，形成数据跨境合规管控关键管控点。

- 数据跨境前的评估
- 数据跨境中的执行
- 数据跨境后的管理

适用范围	阶段	合规管控要点
数据跨境合规管控关键控制点	跨境前：评估	1.1 数据字段清单梳理
		1.2 数据跨境流转路径识别
		1.3 数据境外接收方识别和能力评估
		1.4 跨境目的的合法性、必要性评估
		1.5 跨境字段最小化评估
		1.6 特殊类型数据筛查、拦截（国家秘密、核心数据、个人信息等）

适用范围	阶段	合规管控要点
		1.7 约定数据发送方与境外接收方的数据安全保护责任义务
		1.8 企业内部相关方会签审批
		1.9 向监管机构备案/获得授权
		1.10 相关人员培训
	跨境中：执行	2.1 加固跨境保障机制（签署跨境转移协议、隐私告知书等）
		2.2 保障传输安全性
		2.3 记录数据处理过程
		2.4 严格管控访问权限
		2.5 监控和防范数据泄露风险
		2.6 保障数据主体权利响应通道
	跨境后：管理	3.1 目的完成后及时删除/销毁数据
		3.2 如超出目的范围跨境，重新进行合规评估
		3.3 开展数据跨境合规审计

（2）特殊场景合规管控要点

针对特殊场景，在管控基线之外设置特殊的管控要点，制定场景化合规管控措施。

参考示例：境外分支机构在与当地客户开展业务过程中，需将客户数据传输至境内总部进行处理。为保障数据跨境传输的合法性，境外分支机构与该客户签署数据处理协议（DPA）并列明子处理者清单，以特定授权境内总部作为子处理者参与数据处理；同时，境外分支机构与境内总部签署数据跨境协议（DTC），约定数据跨境过程中双方的责任义务。

三、企业数据跨境合规治理思路与良好实践

3.1 数据跨境合规治理路径

随着数字经济和数字贸易日益深入的发展，企业势必会被卷入全球数据跨境合规体系的洪流中。企业必须迎接数据跨境合规的挑战，一方面，了解内部数据跨境现状和外部监管规则，了解企业数据跨境合规管控重点，另一方面，以风险为导向，建立完善企业数据跨境合规管控机制，搭建立足自身、内外联动、成本效益并举、灵活可持续的数据跨境合规体系。

数据跨境合规治理思路主要包括：明确管控数据对象、摸查关键情形场景、识别外部合规需求、开展数据跨境风险评估、数据跨境风险治理以及重要数据合规延展（如下图），下文将作详细探讨。

3.2 数据跨境合规治理实践

3.2.1 明确管控数据对象

企业需要首先梳理和明确企业内部受管控的数据对象，主要包括个人信息和重要数据。

（1）个人信息的识别

根据欧洲 GDPR、我国个保法、《个人信息安全规范》等制度规范中对个人信息的定义，“直接或间接的可识别性”是判断个人信息的根本依据。直接可识别性的例子如姓名、身份 ID 等基本身份信息，指纹、声纹、虹膜、面部识别特征等生物识别数据等。

个人信息的认定难点在于具有“间接可识别性”的数据，即与其他信息结合能够识别出特定个人的数据范围的不确定性，例如常用设备数据、位置数据等，各法域对间接识别性的解释也存在差异。

参考示例：国际社会针对设备标识符的可识别性存在争议。因可能与其他信息组合而识别到个人，所以系统版本、软件版本、log 日志信息均为个人信息，但在很多场景中，某软件采集了上述信息和其他一些信息，但经过组合亦无法识别到某个特定个人。
因此，在涉及硬件标识符或间接识别信息的场景中，要从以下两点出发，不能机械套用定义。

- IMEI，GAID 等硬件标识符，应考虑其与个人身份的关联性，如处理者无法获取其他信息，则该硬件标识符仅为硬件身份，不具备标识意义。
- 在间接识别的场景中，应考虑处理者所管理的数据集合，对所有数据进行组合，是否能够识别到具体的个人，如无法识别，则不认定为个人信息。

（2）重要数据的识别

目前国际社会尚未对重要数据形成统一定义，企业需要持续关注重要数据相关监管政策出台和解读案例，以及时调整对于重要数据的合规策略。

- **我国相关规定**

根据我国《网络安全法》的定义，重要数据指一旦泄露可能直接影响到国家安全、经济安全、社会稳定的数据，如未公开的政府信息、大面积人口、基因健康、地理、矿产资源等。

我国《信息安全技术 重要数据识别指南（草案）》详细明确了重要数据的特征，将重要数据分为经济运行、人口与健康、自然资源与环境、科学技术、安全保护、应用服务、政务活动等类型；并首次提出了识别重要数据的基本原则、重要数据的识别流程和对重要数据的描述格式，为企业梳理本企业重要数据具体目录提供参考和规则支撑。

针对工业和信息化领域，我国《工业和信息化领域数据安全管理办法（试行）》提出先分类后分级，形成和维护数据分类清单；然后根据数据遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者个人、组织合法权益等造成的危害程度，将工业和电信数据分为一般数据、重要数据和核心数据三级；并明确提出我国境内收集和产生的重要数据，应当依照法律、行政法规要求在境内存储，确需向境外提供的，应当依法依规进行数据出境安全评估，在确保安全的前提下进行数据出境，并加强对数据出境后的跟踪掌握。核心数据不得出境。

- **其他法域相关规定**

其他国家/地区暂未针对重要数据进行清晰定义，但针对特殊数据或特殊行业，均有不同程度的合规要求。对于企业来说，企业在日常运营过程中的一些商业数据，或数量有限的个人信息通常不被视为是重要数据。但针对一些特殊的行业如测绘、勘探、电信，日常运营过程中的商业数据可能被认定为重要数据。

3.2.2 摸查关键情形场景

关键动作一：开展现状调研，识别数据跨境场景

企业对内部数据跨境场景进行识别，为合规差距分析和明确合规治理重点提供坚实的事实基础。企业通常采用以下几种方法展开内部调研工作：

- 信息采集和人员访谈：制定跨境要素识别表，通过下发信息采集表，调研跨境业务需求、数据保护现状和数据流转情况；
- 制度流程及法务文件审阅：审核企业现有制度、流程、隐私通知书等相关文档，梳理合规现状；
- 实地走查观察：对现有跨境业务流程的执行情况进行实地走查观察，随机挑选或者针对企业关注的业务场景，从数据发出地采集、跨境传输到数据接收国落地整个过程进行跟踪，了解传输链路各环节的控制措施和实际的执行情况。

关键动作二：清晰梳理路径，制定数据流转摸底工具

由于数据跨境流转情况复杂，需要采用工具表单和数据流转示意图的方式对数据跨境情况进行记录和清晰梳理，可以通过构建信息采集工具进行协助，例如：

- 构建跨境场景识别表：根据业务单位填写的数据跨境场景识别要素表，梳理出数据跨境流转情况，包括具体业务场景、涉及部门、文件形式、具体字段、数据来源地区、

数据跨境识别、涉及系统；呈现各业务场景数据跨境转移的类型：跨境传输、跨境访问、跨境采集以及是否存在跨境中转的情况。

- 绘制跨境数据流转图：根据数据跨境场景识别要素表，绘制跨境数据流转图，理清各业务细分场景下数据跨境流转逻辑与路径，包括涉及系统、数据主体所在地、跨境流转情况等内容，汇总成公司业务数据跨境全景图。

同时，应设置针对上述工具的更新机制，定期对工具的符合性、实用性进行审核、调整。

3.2.3 识别外部合规要点

完成上述两个步骤之后，企业对自身的数据跨境现状和合规需求已有清晰的认识。企业需结合自身业务分布情况，搜集和研究外部监管合规的要求，以明确数据跨境合规治理要点。

关键动作一：梳理和研究数据跨境监管规则

在合规运行的前提下，充分利用数据跨境流动的国际规则，将极大降低企业的跨境运维成本。通过对全球 50 多个国家和地区的跨境规则进行研究，我们发现了全球数据跨境规则的主要逻辑结构如下：

1） 跨境模式：数据跨境模式通常分为不允许出境、满足条件出境、自由出境三类，其中“满足条件出境”为多数模式，也是下列监管应对的重点和前提；

2） 跨境核心要求：数据保护法令往往在跨境章节的首段列明数据跨境的核心要求，包括同意、同等/充分性保护和批准/评估。各法域的核心要求为其中的一项或者两项的组合；

3） 充分性保障措施：保障条件是针对同等保护作为核心条件的国家而言的，部分国家规定了具体的条件，例如：标准协议、集团内部规则等；部分国家未规定具体条件，企业可以采用最佳实践做法，以自证满足充分性保障要求；

4） 克减条件：即在满足某些条件的情况下，可以不履行同等的保障条件，即对保障条件的克减。但有些国家并未规定克减条件，如中国。

参考示例：以欧盟数据出境为例，可以对条款进行如下解读：
1）GDPR 语境下数据出境的核心要求为：同等/充分性保护；
2）GDPR 规定了满足充分性保障的多样化的形式，同时提供了标准的跨境协议；
3）GDPR 也规定了包括同意在内的克减条件，只有在清晰解读逻辑层次的基础上，才能明确各层级条款的运用规则。

参考示例：俄罗斯的数据跨境的核心要求为：同等/充分性保护；但在保障措施方面，俄罗斯仅规定了白名单一种保障形式。在实践中，若企业向非俄罗斯监管机构白名单国家传输数据，则必须通过克减条件进行传输。

关键动作二：划分各法域跨境风险等级

不同国家/地区的数据跨境合规管控强度不同，致使企业面临的执行难度、合规风险存在差异。

1） 针对部分国家，如埃及、俄罗斯，仅能传输到充分性认定的国家或需要监管机构的批准才能出境，又如赞比亚，必须就其标准协议获取监管机构注册，即必须通过监管机构参与才能达成合规条件，合规难度较高；

2） 另外一部分国家规定了多样化的出境合规保障条件，其中包括了不需要监管机构参与、企业可以自由裁量选用的方式，合规难度相对较低；

3） 相同风险等级国家对应的合规措施大体相同。

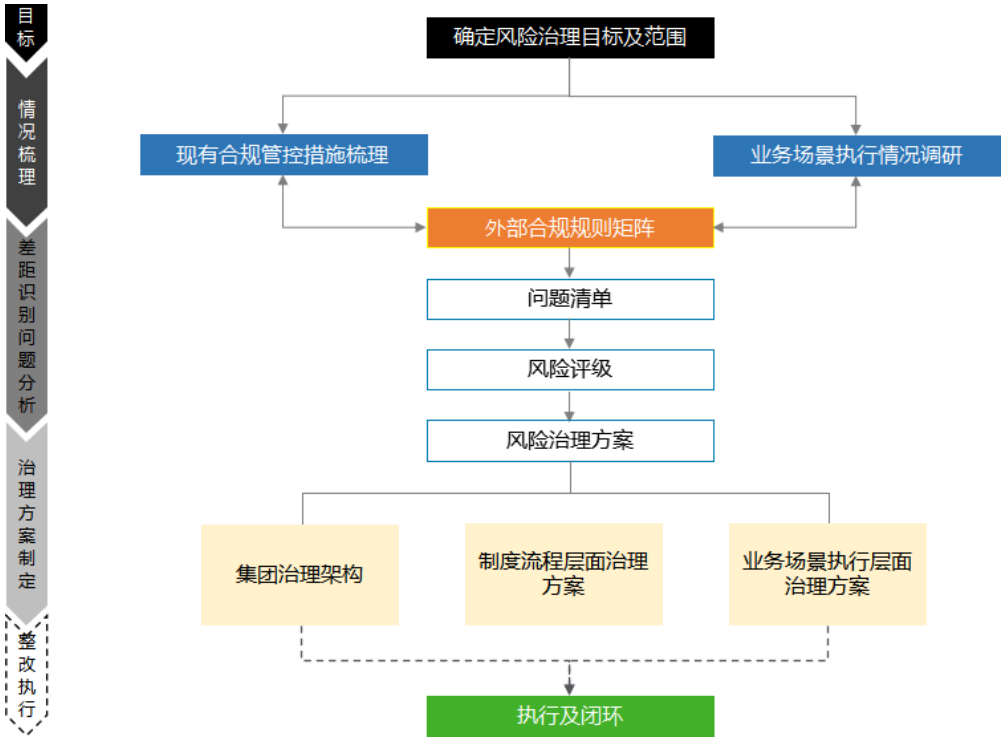
因此，对全球重点国家的数据跨境转移要求划分成高中低风险，依据风险的高低即合规措施模式对各国家/地区进行归类分级，并给每一等级的国家适配统一的合规措施，最终形成包含合规措施的数据跨境传输风险矩阵：严格管控（三级）、适度管控（二级）、宽松管控（一级）（如下图）。

风险等级	国家举例	风险详情	应对原则
3 级	埃及、俄罗斯、乌克兰等	仅通过充分性认定或监管机构批准的方式出境，需要基于监管机构的参与结果，难把控。	通过监管机构授权实施跨境传输；未获授权情况下，通过满足特定“克减”条件实施跨境传输；否则不开展数据跨境。
2 级	巴西、EEA、新加坡等	规定了同等保护的保障措施形式，可选择适用协议、BCR 等合规保障措施（监管机构发布或自行拟定）；或未规定同等保护的保障措施形式，可使用自行拟定的协议模板。	通过签署标准合同条款实施跨境传输；通过满足特定“克减”条件实施跨境传输；否则不跨境或自行评估备案。
1 级	印度尼西亚、孟加拉国、越南等	暂未有数据跨境合规要求。	合规整改优先级排后，并动态跟踪立法更新情况。

同时，企业需要立足自身管理实践，制定重点国家/地区的数据跨境合规策略。企业可根据国别数据跨境风险矩阵，基于自身业务场景、风险偏好等，对不同风险等级的国家/地区制定数据跨境合规管控策略和控制点，包括风险等级、跨境传输路径指引、相关示例/工具、相关责任方和审核方等；并结合各国家/地区的执法力度最终确定数据跨境合规管控策略和控制点，为全球跨境传输提供路径指引。

3.2.4 组织合规风险评估

为评估企业数据跨境活动中的合规风险，提升企业数据跨境管理能力、为业务发展提供可靠保障，企业需要对标监管要求对企业全跨境场景开展风险评估，整体的流程如下图：



关键动作一：制定跨境风险评估标尺

企业需基于监管规则和国际标准，参考同业先进实践，从数据跨境全生命周期维度制定数据跨境风险评估矩阵。跨境前、数据跨境执行和跨境后评估内容大致如下所示：

1） 跨境前环节：数据字段/流转情况梳理、最小化评估、合法性评估、第三方合规性等内容是否已评审通过等；

2） 跨境传输执行合规措施：监管机构审批/备案、标准合同条款（SCC）协议、数据主体同意是否已合规执行，跨境传输过程是否完整记录等；

3） 跨境数据的后续使用：目的完成后数据是否及时删除、是否有超出传输目的的使用情况等。

关键动作二：确定风险评级方法

基于风险评估整理问题清单，以“风险为导向”的合规策略对问题进行风险等级划分。结合实践经验，数据跨境风险的评级可以从风险影响程度及风险发生可能性两个维度出发，认定方法如下：

风险级别				
风险影响	高	中	高	高
	中	低	中	高

风险级别				
	低	低	低	中
		低	中	高
		风险发生可能性		

风险影响等级具体判断标准如下：

风险影响等级定义说明	
风险影响等级	**描述**
高	高危风险项会导致很高的数据跨境合规风险，是监管机构关注的重点，一旦被监管机构查处，会严重影响此模块业务的正常运营；或一旦被发现和利用，可能会直接导致数据泄露，对公司造成重大经济损失或产生重大声誉风险，对模块业务运行造成较大的影响。
中	中危风险项会导致一般的数据跨境合规风险，一旦被监管机构查处，有中等或较高概率影响此模块业务的正常运营；或一旦被发现和利用，可能会直接导致数据泄露，对公司造成一定的经济损失，对模块业务运行造成一定的影响。
低	低危风险项会导致较低的数据跨境合规风险，对模块业务正常运营、个人信息安全以及公司经济损失等的影响较低且发生的几率较低。此类问题对模块业务的影响受限于特定的条件或需与其他问题组合才能导致较大的危害，从而问题发生的可能性低于风险级别为中的问题。

资料来源：德勤分析与研究

3.2.5 开展合规风险治理

企业基于数据跨境风险评估结论，结合监管要求和同业先进实践，从制度流程设计与业务单位落地执行两个层面，制定数据跨境风险治理方案，主要包括以下两方面：

1） 风险控制与治理：针对风险评估结论，制定风险治理方案并进行优先级排期，优先处置影响重大、高紧迫度的风险，缓释影响中小、低紧迫度的风险，适配可落地的技术和组织措施，包括对各业务执行问题的纠正，以及对现有合规管控基线的优化；

2） 成果内化与长效运维：坚持合规与业务发展相结合、体系完善与落地执行相结合的治理原则，制定可落地、可推广、可持续的数据跨境风险管控和合规治理规则、指引、方法和工具，逐步完善的数据跨境风险治理体系。

关键动作一：监管方交流与报批报备

大多国家/地区的数据跨境管控要求涉及监管方的参与，例如跨境前监管审批、标准协议的报备等。目前，部分国家/地区的监管机构出具了具体的报批报备流程指引，例如欧盟的约束性公司规则（BCRs）审批流程；部分国家/地区的监管机构尚未对监管报批报备流程给出公开的清晰指引，企业需与监管机构进行积极沟通。

参考附件：《部分监管机构联系方式》

关键动作二：合理部署数据中心

跨国企业在部署业务系统服务器时，应以合规为前提，结合成本、技术等因素进行服务器选址部署。

- **合规考量**

一方面，需遵循本地化要求。按照一般个人信息的本地化要求及针对敏感个人信息的本地化要求的区分，总体分为以下两种情况：

1） 对一般个人信息有本地化要求的国家，如俄罗斯，其人力资源管理、供应商管理等业务系统中包含较多个人信息，建议本地部署服务器；

2） 对敏感个人信息有本地化要求的国家，如印度、巴基斯坦、阿联酋、赞比亚，若业务系统中包含敏感数据较多，从风险控制的角度，亦建议本地化存储。

另一方面，对于没有本地化要求的国家，在考虑数据中心选址时，应考虑拟布局国家/地区的数据保护能力被认可的程度。在被国际广泛认可的“充分保护”国家建立数据中心或数据港，以便其数据存储及合理利用，实现业务和数据保护的平衡，降低数据跨境传输的合规风险与合规成本。

- **成本、技术考虑考量**

在境外数据中心选址，需要同时将成本呢、技术等纳入考量，比如：

1） 对企业政策：企业税收、企业激励政策、商业环境等；

2） 当地环境：气候与环境、文化教育和能源通讯，人口密度等；

3） 当地网络水平：上网/移动用户、交通数据、骨干网节点数量、本地数据中心数量等。

4） 技术成本：选择公有云服务还是租用数据中心（IDC）也需要全面进行成本评估。

关键动作三：调整 SCC 模板体系

部分国家要求签署本国监管机构的 SCC，例如迪拜国际金融中心，或者签署当地监管机构认可的标准协议，例如赞比亚。如企业针对所有跨境场景采用统一版本的 SCC，未能满足部分国家的特殊要求，同时，对于合规要求较低的国家，可以考虑签署合规标准较低的 SCC。

短期，以欧盟版本 SCC 为基础，兼顾已明确、可落地规则：

1） 对于未明确规则的国家/地区，企业可暂以欧盟版本 SCC 为基础；

2） 对于有特殊监管要求的国家/地区，签署当地监管机构发布的 SCC 协议；

3） 涉及有审批或备案要求的国家/地区，与监管机构确定 SCC 协议的认可程序，并对现有 SCC 进行认证审批。

长期，关注国别差异、主体角色差异，调整 SCC 模板及使用规范：

1） 规划集团 SCC 模板体系：根据各国家/地区对 SCC 的不同要求和监管严苛程度，设计若干套集团内部 SCC 模板；

2） 在确定模板的基础上，制定相关的使用规则及指引；

3） 持续关注各国家/地区的监管动态，及时更新 SCC 模板。

参考附件：《欧洲数据跨境管控机制范式》

关键动作四：数据出境征得个人的单独同意

企业若以同意作为数据处理的合法性基础，在涉及个人信息出境时，需要获得个人对数据出境事项的单独同意。企业应充分履行告知义务，向个人信息主体告知境外接收方名称或者姓名、联系方式、处理目的、处理方式、个人信息的种类以及个人向境外接收方行使本法规定权利的方式和程序等事项；并与企业产品或服务中其他业务功能相分离，征得个人信息主体的单独同意。

关键动作五：建立数据跨境前评估机制

企业需要建立数据跨境前评估机制，在数据跨境前至少对以下事项进行评估：

1） 数据跨境可行性评估：对数据跨境目的、范围、方式等合法性、正当性、必要性进行评估，对境外接收方的安全管控能力进行评估；

2） 数据跨境字段最小化评估：判断跨境数据字段是否为最小化，是否涉及敏感信息等；

3） 数据跨境安全性评估：对数据跨境环节的安全管控能力进行评估，包括组织管理和技术管控两个层面，例如访问权限管控、传输通道、脱敏加密保障等。

另外，应着重建立完善评估的具体程序，包括评估流程的触发机制、评估执行参与主体、评估工具的使用、评估结果的应用、评估流程的闭环等。

3.2.6 重要数据合规延展

目前，各国家/地区对于重要数据的定义和跨境规则较为模糊，监管执法情况存在诸多不确定性。

在数据识别方面，世界范围内对于重要数据的监管定义尚未统一且较为模糊，企业需结合当地法律及自身业务场景，对重要数据进行场景化分析和识别，建立重要数据清单并单独维护；同时坚持较为“保守”的重要数据定义原则，以应对监管执法的不确定性。

在外部规则方面，重要数据的跨境规则大体分为以下两种要求：

1） 本地化存储及处理，原则上不允许向境外传输；

2） 向境外传输需符合特定目的要求，并且经过严格的审批制度。

除上述要求外，对重要数据跨境的监管要求与个人信息无实质区别，如事先风险评估、安全性保障措施等。因此，对于重要数据的跨境合规管控，可优先考虑本地化部署的方式，从源头规避数据跨境合规风险；其次，严格评估重要数据跨境的必要性和合法性，如确需进行重要数据跨境，应按规定进行监管报批报备，并做好组织层面和技术层面的安全保障措施；同时，企业应做好数据跨境外部规则的排查、梳理及跟踪，以应对随时可能面临的重要数据合规风险。

附录

附件一：全球主要数据跨境限制模式

模式	国家	立法概况	立法详情
国家安全与数字红利追求并举，在促进数字经济发展的同时寻求本地化中间路线	印度	提倡对个人数据进行分级，对一般个人数据、敏感个人数据、关键个人数据实施不同的数据本地化和跨境流动限制。	从 2018、2019 两部个人信息法案针对数据跨境规则的变化可以看出，印度并不想实施严格的“数据保护主义”，但又不能放任数据的自由流动，因此其数据本地化策略在想要融入数据全球化趋势，刺激印度数字经济发展的同时，保护数据安全。其最终确定的中间路线是：在实施本地化要求的同时，印度提倡对个人数据实施分级分类。对敏感数据、关键个人数据提出严格的本地化要求：在印度境内存储副本，在极少特定的情况下可以跨境流动，其中，关键个人数据离境条件比敏感个人数据更为苛刻；而对一般个人数据不做要求。
	俄罗斯	通过数据本地化政策要求数据首次存储在俄罗斯境内，满足合规条件的情况下有序出境。	2014 年，俄罗斯通过了个人数据本地化规则，要求收集和处理俄罗斯公民个人数据的所有运营者使用位于俄罗斯境内的数据中心，要求数据首次存储必须在俄罗斯境内的服务器上。在执法层面，俄罗斯也希望通过数据本地化存储加强政府执法权和对数据的控制力。“Yarovaya’s Law”要求在互联网上传播信息的组织者保留俄罗斯用户的互联网通信数据、用户本身的数据和某些用户活动的数据，在俄罗斯境内留存数据 6 个月，并应要求向俄罗斯当局披露。
提倡数据跨境自由流动，推动跨境数据自由流动规则构建	美国	主张将“数据跨境自由流动”纳入协议条款、限制重要技术数据、确定长臂域外管辖。	基于当前在信息通信产业、计算机行业和数字经济上具有绝对的全球领先优势，美国的数据流动政策更注重个人数据跨境自由流动，主要目的在于利用数字产业全球领导优势主导未来数据的流向。因此，美国在与各国的新一轮贸易谈判中都主张将“数据跨境自由流动”纳入协议条款，以破除许多国家利用数据跨境流动而设置的市场准入壁垒；同时，限制重要技术数据出口和特定数据领域的外国投资，最后，通过“长臂域外管辖”扩大国内法域外适用的范围，进一步扩展数据主权，以满足新环境下美国政府跨境调取数据的执法需要。
	欧盟	对内实施单一化战略，对外设置较为灵活的数据出境模式。	在成员国内部，欧盟数据流动政策旨在消除欧盟境内数据自由流动障碍，实施欧盟数字化单一市场战略。为了实现数字化单一市场，欧盟通过 GDPR 在成员国间的直接适用，消除成员国数据保护规则的差异性，实现个人数据在欧盟范围内的自由流动。通过《非个人数据在欧盟境内自由流动框架条例》则致力于消除各成员国的数据本地化要求的壁垒。针对数据向成员国之外的出境，欧盟为企业提供了遵守适当保障措施条件下的转移机制，包括公共当局或机构间的具有法律约束力和执行力的文件、约束性公司规则（BCRs）、标准数据保护条款（欧盟委员会批准/成员国监管机构批准欧盟委员会承认）、批准的行为准则、批准的认证机制等。这些机制为在欧盟收集并处理个人数据的企业提供了可选择的数据跨境流动机制。
	新加坡、日本	主张数据保护和数据自由流动相结合，为企业设置多样化的出境条件，并积极参与数据跨境流动合作机制。	以建设亚太地区数据中心为导向，新加坡建立了与欧盟类似的弹性化的数据跨境传输要求，使其成为跨国企业设立亚太区域数据中心的有利助力。同时，新加坡积极加入 CBPRs（APEC 跨境隐私规则体系），寻求区域内数据自由流动。虽然日本在数据跨境转移的规则形式上参考了欧盟，但对规则的解释更为弹性，为数据跨境自由流动提供了更多的空间。与此同时，日本积极积极参与美国为主导的跨太平洋伙伴关系协定(TPP)和 APEC 的 CBPR 规则体系，也通过制定补充规则以弥合欧盟和日本在数据保护规则上的差异，于 2019 年实现了日欧之间双向互认。

附件二：国际组织数据跨境流动框架

国际组织	概况	框架详情
经济合作与发展组织(OECD)	促进成员国内部数据跨境流动。	2013 年，OECD 对 OECD1980 年指南进行了一次全面修订，形成了《隐私保护和个人数据跨境流通指南》（简称“OECD2013 年指南”）。指南中将个人数据跨境流通定义为“个人数据跨越国家边境流动”，并明确促进数据在成员国之间的自由流动。其中第四部分为数据自由流通和合法限制的原则（第 15-18 条），主要内容包含成员国应履行的再出口影响评估义务、确保通畅、安全的义务、管理与保护责任，克制态度、禁止妨碍数据流动、确保限制和风险成比例的义务。2007 年，在 OECD1980 年指南的基础上，OECD 通过了《隐私保护及跨境合作执行建议》，要求成员国执行跨境合作执行隐私保护相关法律时，对企业提出了便利执行合作的行动要求。不难看出，OECD 对于成员国内部的数据跨境流通总体持较为开放的态度。
亚太经济合作组织(APEC)	建立跨境规则体系，确立具体评估标准	2013 年，亚太经济合作组织（以下简称“APEC”）通过了《跨境隐私规则体系》（《Cross Border Privacy Rules System》，以下简称“CBPR”）。CBPR 旨在“确保个人信息跨国界自由流动的同时，为个人信息的隐私与安全建立有意义的保护”，要求“各国政府应确保跨境数据传输不存在不合理的障碍，同时应在国内以及与外国政府合作在国际上保护其公民个人信息的隐私和安全。” APEC 弹性化的多边隐私与数据保护监管合作模式取得了一定的成效，作为是亚太地区第一个数据保护协同框架，APEC 隐私框架建立了一整套的落实措施，其跨境隐私规则体系（CBPR）是当前多边监管合作中较为成熟的机制，确立了评估标准：国内隐私法、隐私保护执法机构、信任标志（trust-mark）提供商、隐私法与 APEC 隐私框架的一致性等，要求各成员国确保跨境数据传输不存在不合理的障碍。
东南亚国家联盟(ASEAN)	通过数字治理框架对成员共进行监管指导，重点发展示范合同条款及跨境流动认证	第一届东盟数字部长会议批准发布《东盟数据管理框架》（ASEAN Data Management Framework，简称 DMF）以及《东盟跨境数据流动示范合同条款》（ASEAN Model Contractual Clauses for Cross Border Data Flows，简称 MCCs），以期促进东盟地区数据相关的商业业务运营，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。东盟数据保护框架旨在灵活适应成员国在数据和隐私保护监管方面的不同的成熟度，但不具有国内和国际的约束力。2018 年，基于《东盟经济共同体蓝图 2025》和《东盟个人数据保护框架》的号召，东盟发布了《东盟数字数据治理框架》（ASEAN Framework on Digital Data Governance），规定了战略重点、原则和倡议，以指导东盟成员国在数字经济中对数字数据治理（包括个人和非个人数据）的政策和监管方法。2019 年 11 月，东盟通过《东盟跨境数据流动机制的关键方法》，建议东盟重点发展其中两个机制，即“东盟示范合同条款”和“东盟跨境数据流动认证”。

附件三：中国数据跨境相关法律规定

法律法规名称	相关条款	核心规定	时间	性质	废存情况
《网络安全法》	第 37 条	1. 框架性规定，主体限于关键信息基础设施运营者在境内搜集的个人信息 2. 需境内存储，若有需要境外提供，需经安全评估	2017 年生效	法律	现行有效
《个人信息和重要数据出境安全评估办法（征求意见稿）》	全篇	1. 涉及个人信息和重要数据未做区分设计 2. 自评估的具体内容 3. 监管进行安全审查的标准 4. 不得出境的情况	2017 年发布征求意见稿	行政法规（网信办）	征求意见稿
《信息安全技术 数据出境安全评估指南（征求意见稿）》	全篇	1. 自评估具体流程 2. 个人信息及重要数据的评估要点（合法正当、风险可控） 3. 发送方的技术和管理能力要求 4. 接收方的安全保护能力及所在地区政治法律环境要求	2017 年发布征求意见稿	国家标准（国标委）	征求意见稿
《个人信息出境安全评估办法（征求意见稿）》	全篇	1. 仅涉及个人信息 2. 安全评估申报材料 3. 重点评估内容 4. 出境记录保存要求 5. 不得出境的情况	2019 年发布征求意见稿	行政法规（网信办）	征求意见稿
《数据安全管理办法（征求意见稿）》	第 28 条	1. 涉及个人信息和重要数据未作区分设计 2. 网络运营者发布、共享、交易或向境外提供重要数据前，应当评估风险，并报监管部门同意 3. 向境外提供个人信息按有关规定执行	2019 年发布征求意见稿	行政法规（网信办）	征求意见稿
《网络安全审查办法》	第 6 条	1. 掌握超过 100 万用户个人信息的运营者赴国外上市，必须向网络安全审查办公室申报网络安全审查。	2020 年生效	行政法规（网信办）	现行有效
《数据安全法》	第 5 条 第 33 条	1. 数据指各种形式的信息记录，未作其他区分 2. 未有细致的规定，仅规定了促进数据有效利用，促进数字经济发展的基本立场 3. 境外调取需经批准	2021 年生效	法律	现行有效
《个人信息保护法》	第 36 条 第 38 条 第 39 条 第 40 条 第 41 条 第 42 条 第 43 条	1. 国家机关处理的个人信息应在中国境内存储；确需向境外提供应进行安全评估 2. 境外提供的合法基础：安全评估、认证、标准合同、其他 3. 告知义务 4. 关键信息基础设施运营者和处理个人信息达到规定数量的个人信息处理者需境内存储，出境需评估 5. 司法协助需经批准，并遵从国际条约规定 6. 可对境外组织采取的行动 7. 对境外组织的反制	2021 年生效	法律	现行有效

《数据出境安全评估办法（征求意见稿）》	全篇	1. 需申报数据出境安全评估的条件和情形 2. 数据出境风险自评估及评估重点 3. 申报数据出境安全评估的材料、流程、有效期、注意事项等	2021 年发布征求意见稿	行政法规（网信办）	征求意见稿
《网络数据安全管理条例（征求意见稿）》	第五章	1. 数据处理者向境外提供数据的必要条件 2. 数据出境需要获得个人单独同意要求 3. 数据出境安全评估要求 4. 数据处理者向境外提供数据所履行义务要求 5. 企业向市级网信部门进行数据安全报告要求 6. 数据处理者从事跨境数据活动需建立健全相关技术和管理措施	2021 年发布征求意见稿	行政法规（网信办）	征求意见稿

附件四：中国特殊行业数据跨境要求

行业	法律法规名称	发布机构	具体要求
金融	《关于银行业金融机构做好个人金融信息保护工作的通知》	中国人民银行	在中国境内收集的个人金融信息的存储、处理和分析应当在中国境内进行。
	《个人金融信息（数据）保护试行办法》	中国人民银行	在中国境内收集的个人金融信息的存储、处理和分析应当在中国境内进行。除法律、法规、规章及有关主管部门菱形规定外，不得向境外提供境内个人金融信息。境内金融机构未处理跨境业务时，应当事先取得信息主体的明示同意，并依法开展出境安全评估。个人金融信息出境后，境内金融机构应当建立个人金融信息出境记录并且至少保存 5 年。
	《JR/T0171-2020 个人金融信息保护技术规范》	中国人民银行	因业务需要，确需向境外机构提供个人金融信息的，具体要求如下：应符合国家法律法规及行业主管部门有关规定；应获得个人金融信息主体明示同意；应依据国家、行业有关部门制定的办法与标准开展个人金融信息出境安全评估，确保境外机构数据安全保护能力达到国家、行业有关部门与金融业机构的安全要求；应与境外机构通过签订协议、现场核查等方式，明确并监督境外机构有效履行个人金融信息保密、数据删除、案件协查等职责义务。
	《中国人民银行金融消费者权益保护实施办法》	中国人民银行	在中国境内收集的消费者金融信息的存储、处理和分析应当在中国境内进行。因业务需要，确需向境外提供消费者金融信息的，应当同时符合以下条件：为处理跨境业务所必需；经金融消费者书面授权；信息接收方为完成该业务所必需的关联机构（含总公司、母公司或者分公司、子公司等）；通过签订协议、现场核查等有效措施，要求境外机构为所获得的消费者金融信息保密；符合法律法规和其他相关监管部门的规定。
	《保险公司开业验收指引》	中国保险监督管理委员会	业务数据、财务数据等重要数据应存放在中国境内，具有独立的数据存储设备以及相应的安全防护和异地备份措施。
	《征信业管理条例》	国务院	征信机构在中国境内采集的信息的整理、保存和加工，应当在中国境内进行。
交通	《网络预约出租汽车经营服务管理暂行办法》	交通部、工信部等七部委	网约车平台公司应当遵守国家网络和信息安全有关规定，所采集的个人信息和生成的业务数据，应当在中国内地存储和使用，保存期限不少于 2 年，除法律法规另有规定外，上述信息和数据不得外流。
医疗	《人口健康信息管理办法（试行）》	卫计委	不得将人口健康信息在境外的服务器中存储，不得托管、租赁在境外的服务器。
出版	《网络出版服务管理规定》	国家新闻出版、广电总局、工业和信息化部	图书、音像、电子、报纸、期刊出版单位从事网络出版服务，应当具备以下条件：有从事网络出版服务所需的必要的技术设备，相关服务器和存储设备必须存放在中华人民共和国境内。
测绘	《地图管理条例》	国务院	互联网地图服务单位应当将存放地图数据的服务器设在中华人民共和国境内，并制定互联网地图数据安全管理制度和保障措施。

附件五：全球数据跨境法律法规清单

国家/地区	法律法规名称
EEA	GDPR
英国	GDPR 英国数据保护法
墨西哥	《关于私主体个人数据保障义务的联邦法律》
土耳其	《个人数据保护法(LPPD)》
巴西	《巴西通用数据保护法(LGPD)》
哥伦比亚	2012 年《第 1581 号成文法》 2013 年《第 1377 号成文法》
秘鲁	《个人数据保护法 N° 29733》
俄罗斯	《第 152 FZ 号数据保护法》 《第 242 FZ 号数据保护法》 《第 405 FZ 号数据保护法》
印度	2019 年《个人数据保护法案》草案
印度尼西亚	未有个人数据保护法，《政府电子系统和交易实施条例》对公共电子系统提出了若干要求，对私数据库没有相关要求
日本	《个人信息保护法》
菲律宾	《2012 年数据隐私法》
巴基斯坦	2020 年个人数据保护法案（草案）
孟加拉国	暂无成文个人信息保护法，仅有《 2018 年数字安全法案》，其中暂无数据跨境传输相关内容。
越南	暂未有成文个人信息保护法
缅甸	暂未有成文个人信息保护法
泰国	《个人数据保护法》2020
马来西亚	《2010 年个人数据保护法令》
乌克兰	关于个人数据保护的第 2997-VI 号法律 第 4452-VI 号法律（修正案） 第 5491-VI 号法律（修正案）
尼泊尔	暂未有个人数据保护法令
新加坡	《个人信息保护法案》2012，2020 年的修订并未涉及数据跨境传输部分

国家/地区	法律法规名称
韩国	《个人信息保护法》
埃及	《数据保护法》
埃塞俄比亚	无生效数据保护法，仅关于支付类的指引规则中有本地化的要求。
南非	《南非个人信息保护法》
尼日利亚	《2019 年尼日利亚数据保护条例》
阿尔及利亚	《2018 年第 18-07 号法律》
赞比亚	《2020 第 3 号数据保护法》
利比亚	目前利比亚没有数据保护法，亦无相关规定。
乌干达	《数据保护和隐私条例》
安哥拉	《数据保护法》
摩洛哥	《个人信息保护第 09-08 号法律》
阿联酋	阿联酋暂无隐私保护法令，信息和通信技术保健法第 13 条中提到了本地存储要求 DIFC 于 2007 年制定了隐私保护法令、于 2020 年进行了补充修订，Data Protection Law（DIFC Law No. 5 of 2020）
香港	《个人资料（私隐）条例》（未有关于数据跨境的规定）
中国	《网络安全法》
	《数据安全法》
	《个人信息保护法》
	《网络安全审查办法》
	《数据出境安全评估办法（征求意见稿）》
	《数据安全管理办法（征求意见稿）》
	《信息安全技术 数据出境安全评估指南（征求意见稿）》
	《个人信息和重要数据出境安全评估办法（征求意见稿）》
	《个人信息出境安全评估办法（征求意见稿）》

附件六：全球数据跨境管控要求清单

国家/地区	法律法规名称	相关规定/要点解读
中国	《中华人民共和国网络安全法》	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。
	《个人信息和重要数据出境安全评估办法（征求意见稿）》	网络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，应当按照本办法进行安全评估。
	《数据安全法》	在一般数据安全保护义务之上，对重要数据的处理者规定了“增强型”的保护义务： 1. 重要数据的处理者应当设立数据安全负责人和管理机构，落实数据安全保护责任； 2. 重要数据的处理者应当按照规定对其数据活动定期开展风险评估，并向有关主管部门报送风险评估报告；风险评估报告应当包括本组织掌握的重要数据的种类、数量，收集、存储、加工、使用数据的情况，面临的数据安全风险及其应对措施等。
	《信息安全技术 重要数据识别指南（草案）》	首次提出了重要数据的完整定义（从数据的作用、受破坏后可能带来的影响等角度，将重要数据分为国民经济运行类、安保类、自然资源与环境类、健康类、敏感技术类、用户类及政府工作秘密类）。并列举了 28 个行业的重要数据类型、范围。在重要数据的定义中，附带给出了重要数据判定准则，按照数据未经授权披露、丢失、滥用、篡改或销毁，或汇聚、整合、分析后可能造成的后果，列出了 9 种情况。
	《基础电信企业重要数据识别指南（草案）》	内容涉及重要数据的定义，运营基础电信业务过程中识别重要数据的原则、规则、工作流程等。
德国	《电子通信法》	原始数据的本地存储进行规定
印度	《国家电子商务政策》	将要创建法律和技术框架为如下情形的跨境数据流动施加限制提供依据：（1）安装在公共场所的物联网设备收集的数据；以及（2）印度用户通过各种来源产生的数据，包括电子商务平台、社交媒体、搜索引擎等。但是也列出了一些允许跨境流动的例外情形，例如云计算服务中不涉及个人和社区数据的技术数据。
	《统一许可规章》	许可不得将下列内容传输给任意其他人/印度之外的场所： 1. 与订阅者有关的任何会计信息（除了国际漫游/账单）（注意：该要求不限制根据法定要求披露财务信息）； 2. 用户信息（除了在漫游期间使用印度运营商网络的外国订阅者或 IPLC 的订阅者）
	《电子药房规则草案》	以电子医药行业为试点推行了反对数据跨境流动的政策
	《国家数据分享和准入政策》	所有通过使用公共基金收集的数据均存储于本国境内
印度尼西亚	《电子系统和交易条款的 2019 年第 71 号政府法规》	公共电子系统运营商必须将其电子系统和数据（包括政府、能源、交通、金融、医疗、IT 和通信、国防等战略性数据）放置在印度尼西亚。除非公司另有规定，否则私人电子系统运营商可以将其电子系统和数据放置在印度尼西亚境内或境外。但是，私有电子系统运营商必须允许政府机构进行“监督”，包括访问电子系统和数据，以进行监控和执法。

国家/地区	法律法规名称	相关规定/要点解读
越南	《互联网服务和在线信息管理、提供和使用条例》	要求信息收集网站、社交网站、移动通信网络服务提供者、在线游戏服务提供者等，至少将一个服务器设置在越南境内 同时，在《网络安全法》中，要求互联网和在线附加服务提供服务的国内外企业，收集，利用，分析和处理信息数据，个人，服务用户的关系数据以及越南服务用户创建的数据必须进行存储。
韩国	《电子金融交易监管条例》	数据本地化措施适用于金融领域。电子金融交易监管条例禁止韩国金融机构跨境传输持有的可识别信息，并要求这些机构在韩国安装服务器和灾难恢复设施。只有对电子金融交易的安全性和可靠性影响有限、且可能因此被指定为“非关键”的信息处理系统，才可建立在国外。
	《金融机构外包数据处理业务和 IT 设施条例》	金融领域的数据处理外包适用特定的限制。26 韩国境内的金融公司必须向金融服务委员会（FSS）报告法律在外包数据处理规定的特定事项，无论此类数据处理发生在韩国境内或外国管辖范围内。
美国	受控非密数据清单	1.根据适用法律、法规和政府政策进行保护或传播控制的信息，分为： 仅供官方使用信息(FOUO INFORMATION)； 执法敏感信息(LES INFORMATION)； 国防部受控非密核信息 (Do D UCNI)； 限制分发信息(LIMITED DISTRIBU-TION INFORM ATION)、国务院敏感非密信息(Do S SBUI)； 缉毒署敏感信息 (DEA Sensitive Information)； 外国政府信息(FOREIGN GOVERNMENT INFORMA-TION)； 技术文件分发声明(DISTRIBUTION STATE-M ENTS ON TECHNICAL DOCUM ENTS) 2.受控非密信息的管理包括： 监管机构创建或处理非机密信息的机构应采取保护措施和控制措施，以保护 CUI 免受未经授权的侵害访问； 法律、法规或政府范围的政策是否应包括传播控制应遵循特定说明，并在 CUI 注册表中提供参考； 当不再需要采取保护措施时，应尽快解除 CUI 的控制和相关当局的传播控制等
俄罗斯	《互联网主权法案》	1.俄罗斯互联网稳定运行的主要责任主体是电信运营商以及技术通信网络、网络流量交换点、自治系统号码（ASN）的所有者； 2. RKN 通过定义路由政策、协调电信运营商和责任方以及他们之间的连接，从而执行集中化的通信网络管理职能。 3.责任方义务包括：参加稳定俄罗斯网络的常规演习；安装技术设备，以防范对俄罗斯境内互联网运营的稳定性、安全性和完整性的威胁等。
土耳其	/	土耳其信息技术和通信管理局发布了两项决定，以管制在该国引起轰动的嵌入式 SIM 技术，尤其是电子呼叫系统的 SIM 卡本地化要求，以防止车辆永久漫游：第一个决定规范车辆中的电子呼叫服务，第二个决定规范远程可编程的 eSIM 技术。
阿尔及利亚	/	阿尔及利亚通过立法要求电子商务运营者从阿尔及利亚境内的数据中心提供服务。

附件七：全球主要监管机构联系方式

国家/地区	监管机构	官网	联系方式	沟通事宜
中国	中华人民共和国国家互联网信息办公室/中共中央网络安全和信息化委员会办公室	*http://www.cac.gov.cn/*	地址：北京市西城区车公庄大街 9 号 电话：(010)68365570	1. 沟通安全评估、安全相关认证相关程序及执行细节； 2. 沟通确定同等保护标准协议订立情况，及现阶段集团内部 SCC 的适用性； 3. 关键基础设施运营者及达到一定数量的个人信息处理者的界定。
法国	法国网络和信息安全局	*https://www.ssi.gouv.fr/*	邮箱： communication@ssi.gouv.fr	数据控制者注册
意大利	网络安全管理委员会	*https://www.sicurezzanazionale.gov.it*	邮箱： info@sicurezzanazionale.gov.it	
波兰	数字事务部	*https://www.gov.pl/*	邮箱：mc@mc.gov.pl 传真：+48228294850	
英国	信息专员公署	*https://ico.org.uk/*	电话：0303 123 1113 传真：01625 524510	标准数据传输协议发布情况（标准数据传输协议）
马来西亚	马来西亚国家网络安全局	*https://www.nacsa.gov.my/*	地址：Level LG & G, West Wing, Perdana Putra Building, Federal Government Administrative Center, Putrajaya, Malaysia.	1. 白名单的发布情况； 2. 中国充分性保障认证情况； 3. 数据控制者/数据库注册情况
	马来西亚通信和多媒体部	*https://www.kkmm.gov.my/*	电话：03-80008000 传真：03-89115183 邮箱： webmaster@kkmm.gov.my	
印度	印度中央信息委员会	*http://www.cic.gov.in/*	传真：26186536 电话：011-26183053 邮箱:fdesk-cic@gov.in	1. 草案的生效情况； 2. 标准合同或内部集团计划批准程序；
埃及	通信和信息技术部	*https://www.mcit.gov.eg/*	电话：（+202）35341300	1. 向监管机构报备跨境传输合规执行情况，自证满足同等保护要求； 2. 获取监管机构对于跨境传输的批准。

国家/地区	监管机构	官网	联系方式	沟通事宜
阿尔及利亚	阿尔及利亚邮电部	*https://www.mpt.gov.dz/en*	邮箱：contact@mpttn.gov.dz 电话：+213(0)21 711 220 传真：+13(0)21 730 047	1. 向监管机构报备接收国立法情况及集团公司数据跨境合执行情况，自证满足同等保护要求； 2. 获取监管机构对于跨境传输的批准。
安哥拉	安哥拉电信和信息技术部	*https://www.missionangola.ch/_english/* *http://www.mtti.gov.ao/*	地址：Rue de Lausanne 80, Genève, 1202, Suisse 电话：41 22 732 30 60	1. 个保法生效后中国是否可以被认定为适当保护水平的国家； 2. 根据中国的认证情况，报备评估或机构审批。
俄罗斯	联邦通信、信息技术和大众媒体监督局	*http://www.rsoc.ru/*	地址：7, bldg 2, Kitaigorodskiy proezd, Moscow, 109995, Russia	1. 数据处理活动开始前的报备批注； 2. 中国充分性保障认定情况
乌克兰	国家网络安全协调中心	*https://zakon.rada.gov.ua/laws/show/2163-19*	因官方网址无法打开，暂无法获取联系信息。	1. 白名单的发布情况； 2. 中国充分性保障认证情况
尼日利亚	国家中心或负责机构	*https://www.cert.gov.ng/*	邮箱：info@cert.gov.ng 电话：+234 905 555 4499	
迪拜 DIFC	迪拜金融服务管理局	*https://www.dfsa.ae*	/	标准数据传输协议发布情况（标准数据传输协议）
土耳其	土耳其国家网络安全委员会	*www.udhb.gov.tr*	/	数据控制者注册
乌干达	乌干达国家信息技术管理局	*https://www.nita.go.ug*	电话：+256-417-801038 邮箱：info@nita.go.ug	
安哥拉	电信、信息技术和媒体部	*https://minttics.gov.ao/*	电话：+244 222 210 740 邮箱：geral@minttics.gov.ao	
哥伦比亚	哥伦比亚工商监督局 哥伦比亚信息和通信技术部	*https://mintic.gov.co/portal/inicio/*	/	数据库注册

附件八：欧洲数据跨境管控机制范式

（1）标准合同条款

标准合同条款（Standards Contractual Clauses，SCCs）是由欧盟委员会“预先批准”的合同范本条款，根据《通用数据保护条例》（GDPR），确保适当数据保护保障措施的合同条款可作为从欧盟向第三国传输数据的依据。

2021 年 6 月 4 日，欧盟委员会发布了 GDPR 下的现代化标准合同条款，用于从欧盟/欧洲经济区（或以其他方式受 GDPR 约束）的控制者或处理者向欧盟/欧洲经济区（不受 GDPR 约束）以外的控制者或处理者传输数据。一项适用于数据控制者与数据处理者之间的数据委托处理活动，一项适用于向第三国传输个人信息的情形。

【访问下载】*https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en*

（2）充分性认定国家

充分性认定是只有当第三国对于个人数据的保护水平达到欧盟的要求，欧盟成员国的个人数据才能进行数据跨境流动。根据《通用数据保护条例》（GDPR）规定，认定第三国是否提供了“充分的”数据保护，通过第三国个人数据保护相关法律制度的完备情况、执行情况等因素判断。

目前，充分性决定的国家包括:安道尔、阿根廷、加拿大(商业组织)、法罗群岛、根西岛、以色列、马恩岛、日本、泽西岛、新西兰、瑞士、乌拉圭、韩国。

【访问下载】*https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en*

（3）约束性企业规则

约束性企业规则（Binding Corporate Rules，BCRs）是个人数据从欧盟出口到其他没有被欧盟确认满足充分性保护的国家，而提供的对个人数据足够保护的法律手段。跨国公司、集团公司如果具备欧盟成员国数据管理机构认可的约束性企业规则，则可以直接进行集团内部的数据跨境传输，而无需在另行批准。

跨国公司、集团公司如果具备欧盟成员国数据管理机构认可的约束性企业规则，可以直接进行集团内部的数据跨境传输，无需在另行批准。约束性企业规则制定出后需经主导性的欧盟成员国内的数据保护机构批准授权方可实施。

目前，欧盟委员会以及各成员国的数据保护机构会公示已经授权的 BCRs 的企业包括：

【访问下载】*https://edpb.europa.eu/our-work-tools/accountability-tools/bcr_en*

附件九：数据跨境司法执法舆情案例

- **西班牙监管因违反数据法对 Vodafone 罚款 815 万欧元**

2021 年 3 月，西班牙数据保护局，对跨国电信公司沃达丰（Vodafone）及其服务提供商多次违反 GDPR 和国家法律罚款 815 万欧元，其中 200 万欧元的罚款归因于其服务提供商向不符合欧洲数据保护要求的国家进行个人数据国际传输。

- **挪威数据保护部门对 Ferde 公司处以罚款，涉嫌向中国跨境传输图片数据**

2021 年 5 月，挪威数据保护局，决定对 Ferde 公司罚款 500 万挪威克朗（约 498,065 欧元）。根据调查显示，Ferde 公司因缺乏数据处理协议、在人工处理超过 1200 万张车牌图像之前没有进行风险评估、同时涉嫌在 2017 年至 2019 年期间向中国进行缺乏适当法律依据的数据转移，违反 GDPR 第 28 条第三款、第 32 条、第 44 条而招致罚款。

- **日本个人信息保护委员会对 LINE 中国子公司访问日本用户数据进行调查**

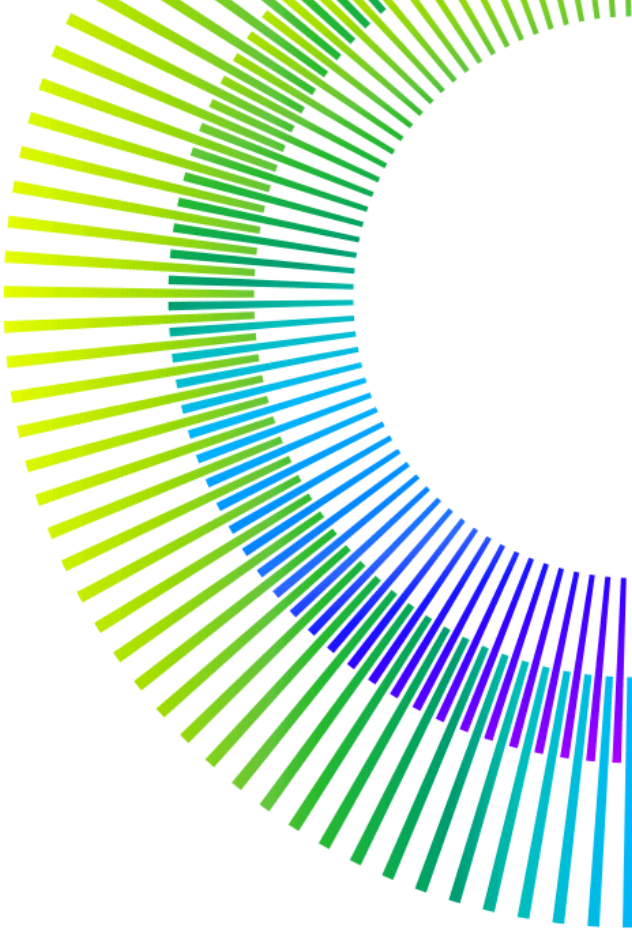
2021 年 3 月，日本个人信息保护委员会对 Line Corp. 进行调查，该消息应用程序提供商的日本用户数据被一家中国子公司访问，该中国子公司的工程师能够看到 2018 年 8 月至 2021 年 2 月期间存储在日本的用户个人信息。委员会于要求 Line 提交事件报告之后进行现场检查，调查人员根据个人信息保护法访问了 Line 及其母公司 Z Holdings Corp. <4689>，表示检查“旨在准确判断是否遵守法律”， Line 对附属公司的监督及其对数据的访问。Line 公司表示已终止其在中国的对话系统的开发、维护和运营。

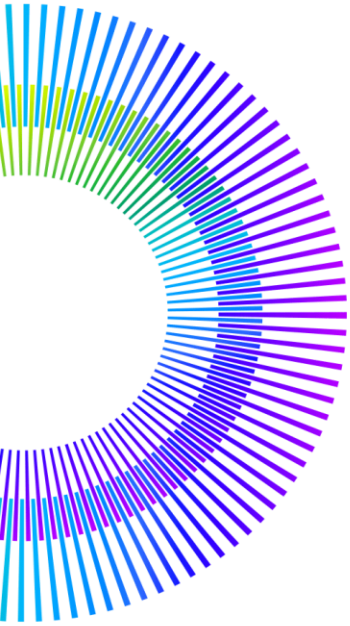
- **法国 CNIL 按照 GDPR 规定对 Google 开出 5000 万欧元罚单**

2019 年 1 月，谷歌（Google）被法国监管机构国家信息与自由委员会（CNIL）处以 5000 万欧元巨额罚款，缘由是谷歌未能履行《通用数据保护条例》（GDPR）规定的义务，其中包括谷歌在跨境数据运营过程中违反了 GDPR 规则中的透明度要求及信息告知义务。

参考文献

[1] 竺彩华，“市场、国家与国际经贸规则体系重构”
[2] 许多奇，“论跨境数据流动规制企业双向合规的法治保障”
[3] 阿里巴巴数据安全研究院，“全球数据跨境流动政策与中国战略研究报告”
[4] 综合开发研究院，“跨境数据流动：全球态势与中国对策”
[5] 东盟发布《东盟数据管理框架》和《东盟跨境数据流动示范合同条款》，网安寻路人微信公众号
[6] European Data Protection Board (EDPB) “Standard contractual clauses for international transfers”
[7] European Data Protection Board (EDPB) “Adequacy decisions: how the EU determines if a non-EU country has an adequate level of data protection.”
[8] European Data Protection Board (EDPB) "Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data-Version 2.0"
[9] UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT (UNCTAD) "Digital Economy Report 2021: Cross-border data flows and development: For whom the data flow"





声明：

本文档仅作为中兴通讯股份有限关于数据跨境合规治理实践研究的参考性资料。除非另有约定，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。由于外部法律环境变化、内部合规体系不断优化完善等因素，可对文档内容进行增加、修改、删减、废止，或不定期更新。任何单位和个人使用本文档的任何内容，应获得授权或注明出处。

本文档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。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。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，请参阅