全球跨境惠赢矩阵
惠天下 赢未来

普华永道 全球跨境服务

链动152处国际级智库
惠赢全球化 梦想无远弗界

数据跨境合规白皮书

2023年5月

pwc 普华永道

奇安信
新一代网络安全领军者

目录

前言

随着全球数字经济规模持续增长，数据作为重要的生产要素，在生产生活各个环节的重要作用正日益显现，数据流动和处理活动安全受到越来越多的关注。世界范围内，对数据跨境活动的管控和监管逐步健全，目前，世界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，是进行跨国商业活动的企业必须重视的课题。此外，数据跨境可能会因个人信息、重要数据、商业数据等引发用户数据易被泄露、滥用等问题，导致的企业名誉受损、利益受损、被通报批评处罚或罚款，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。本白皮书由普华永道中国（简称普华永道）与奇安信科技集团股份有限公司（简称奇安信），双方依托各自深耕领域的技术优势和良好资源，重点围绕数据跨境在金融、科技互联网、汽车以及企业内部管理的场景，分析了数据跨境法规对于具体场景的影响以及典型应对措施，为企业数据合规和安全保障提供有力借鉴。

1

全球及中国数据安全合规趋势

1.1 全球数据安全合规趋势

全球数据合规条例兴起，主要国家和地区执法力度趋严

近年来，随着互联网的迅速发展以及新冠疫情影响带来的数据增长，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》（下文简称“GDPR”或“一般数据保护条例”）以来，已有100多个国家颁布或提出了数据保护或隐私保护法。除此之外，主要国家和地区的监管执行力度增强，2021年GDPR全年罚款金额同比上涨，达到总计11亿欧元，亚马逊也因违反GDPR被罚7.46亿欧元[1]，为保证数据安全和执法透明度，全球数据合规条例增长和范围扩大已成为必然。

欧盟

1981-欧盟《个人数据自动化处理中的个人保护公约》
1995.10-《95指令》
2016.4-《一般数据保护条例》
2019.5-《非个人数据自由流动条例》
2019.4-《网络安全法案》
2020.2-《欧洲数据战略》
2022.2-《数据法案（草案）》
2022.5-《数据治理法案》
2022.9-《数字市场法案》
2022.10-《数字服务法案》

英国

1984-《数据保护法》
2003-《隐私与电子通信条例（PECR）》
2018.5-《网络和信息系统安全法规》
2021.1-《通用数据保护条例》
2022.1-《国家网络安全战略2022-2030》
2022.5-《数据改革法案（草案）》

德国

1976-《个人数据保护法》
2018-《新联邦数据保护法》
2021.1-《联邦数据战略》
2021.5-《IT安全法》2.0版

法国

1978-《信息技术与自由法》
2008.6-《国家安全与防务白皮书》
2011.2-《信息系统防御与安全：法国战略》
2015.10-《法国国家数字安全战略》
2018.2-《网络防御战略评论》
2018.11-《个人数据保护法》
2018.12-《数据保护法》

意大利

1947.12-《宪法》
1996-《数据保护法》
2003-《电子商务法》
2005-《消费者法典》
2012-《个人数据保护法典（修订版）》
2013-《国家网络空间安全战略框架》

加拿大

1983-《隐私法》
1983.7-《信息访问法案》
2000-《个人信息保护和电子文档法案》
2012..3-《加拿大网络安全对关键基础设施威胁的评估》
2018.6-《新版国家网络安全战略》

美国

1974.12-《隐私法案》
1986-《电子通信隐私法》
1986.10-《计算机欺诈和滥用法》
2018.3《澄清海外合法使用数据法案》
2018.6-《消费者隐私法案》（加利福尼亚州）
2021.3-《消费者数据保护法》（弗吉尼亚州）
2021.5-《关于加强国家网络安全的行政命令》
2021.8-《统一个人数据保护法》

[1] 2021年度GDPR罚金和数据泄露调查报告， 欧华律师事务所（DLA Piper）。

俄罗斯

1992-《俄罗斯联邦安全法》
1993.7-《国家秘密法》
1993.12-《俄罗斯联邦宪法》
2004.7-《商业秘密法》
2006-《信息、信息技术和信息保护法》
2006.7-《俄罗斯联邦个人数据法》
2008.9-《不使用自动化设备进行个人数据处理规定》
2012.11-《个人数据相关信息系统在处理个人数据过程中的防护要求》

日本

1988.12-《行政机关计算机处理的个人信息保护法》
2000.1-《保护信息系统免受网络攻击行动计划》
2003.5-《个人信息保护法》
2013.6-《网络安全战略》
2014.11-《网络安全基本法》
2015.9-《网络安全战略（第二版）》
2018.7-《网络安全战略（第三版）》
2022.2-《网络安全战略》

韩国

2001.1-《信息通信网络利用促进和信息保护法》
2001.9-《个人信息保护法施行令》
2008.2-《位置信息保护和使用法实施令》
2008.2-《信息和通信网络利用和信息保护促进法实施令》
2009.4-《信用信息使用和保护法》
2009.10-《信用信息使用和保护法实施令》
2010.3-《位置信息保护和使用法》
2011.3-《个人信息保护法》

中国

2015.7-《中华人民共和国国家安全法》
2017.6-《中华人民共和国网络安全法》
2020.1-《中华人民共和国密码法》
2021.1-《中华人民共和国民法典》
2021.9-《中华人民共和国数据安全法》
2021.11-《中华人民共和国个人信息保护法》
2022.9-《数据出境安全评估办法》
2023.6-《个人信息出境标准合同办法》

巴西

2001.1-《巴西银行保密法》
2011.6-《巴西良好数据法 》
2012.5-《巴西信息获取法》
2014.4-巴西《网络民法》
2018.8-《通用数据保护法》
2019.7-政府第9936/19号法令
2019.7-巴西中央银行第4737/19号决议
2021.2-《网络安全条例》

印度

1999-《信息技术法》
2013.7-《国家网络安全政策》
2017.11-《数据保护框架白皮书》
2022.12-《数字化个人数据保护法草案》

澳大利亚

1988.12-《隐私法》
1997-《电信法》
2013.8-《公共服务大数据战略》
2013.6-《关键基础设施安全法》
2020.8-《网络安全战略》
2022.4-《国家数据安全行动计划》

[2] 此处节选部分法律法规，仅供一般参考之用，不可视为详尽说明。

长臂管辖对数据所在国法规产生冲击

目前，全球数据跨境流动和数据监管未形成统一规制，受本国国情和多种因素影响，各国立法框架仍存在差异，由此导致同一主体可能受到双重法规限制的问题。例如，欧盟《一般数据保护条例》（General Data Protection Regulation）确立的效果原则规定了只要是向欧盟境内的数据主体提供商品服务且存在处理个人数据等行为，其收集到的信息都要受到欧盟管辖，因此，数据处理国不得不通过数据立法进一步应对长臂管辖带来的影响。

各国家和地区立法具有鲜明特点，发展趋势存在差异

由于各国家和地区间立法驱动因素不同、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。

1.2 中国数据安全合规趋势

数据合规管理制度日趋完善

随着《网络安全法》《数据安全法》《个人信息保护法》的相继落地实施，我国网络安全与数据保护领域基本法律框架形成，未来，数据法规整改和内容细化将成为主要趋势。例如，针对数据出境活动相关规范细则不断落地，《数据出境安全评估办法》《数据出境安全评估申报指南》等进一步细化《个人信息保护法》中提到的数据出境安全评估路径的要求，《个人信息出境标准合同办法》《个人信息跨境处理活动安全认证规范》等法律法规则进一步细化《个人信息保护法》中提及的合同备案及数据认证路径，数据出境的基本合规框架亦已搭建完成。

数据分级分类管理趋势

《网络安全法》提出了数据分级分类保护制度，数据可从个人维度、公共管理维度、信息传播维度、组织经营维度和行业领域维度等进行分类，不同数据涉及的法律风险和数据合规要求各有不同；同时，根据对国家安全和公共利益等造成危害的程度，对重要数据提出了严格的监管要求，以此实现数据资源的精细化管理和保护。

分行业进行数据合规管理

监管机构针对不同行业发起了多项监管行动，个别行业数据治理成为重点监督方向。例如，金融领域发布了《征信业务管理办法》，国家市场监督管理总局和国家标准化管理委员会也针对医疗领域发布了推荐性国家标准GB/T39725-2020《信息安全技术—健康医疗数据安全指南》，以及汽车行业的《汽车数据安全管理若干规定（试行）》等。

2

数据跨境法规解读

2.1 全球数据跨境法规

目前，针对数据跨境的治理在全球范围内并未形成统一的规制体系，不同国家和地区主要通过双边或多边区域性合作实现对数据跨境的协调管理，其中最为知名影响范围最广的便是欧盟主导推进的数据跨境治理体系，致力于在数据跨境传输过程中为个人数据主体提供充足保护。此外，经济合作与发展组织（OECD）在1980年已发布《隐私保护和跨境个人数据流动指南》（Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data），鼓励数据跨境和自由流动；亚太经济合作组织（APEC）在2005年发布《APEC隐私框架》（APEC Privacy Framework），提出数据收集目的明确、数据使用范围限制、安全管理等九项原则，对成员国数据跨境立法提出规制建议。

与国际间积极合作的趋势相对应，不同主权国家基于本国国情也纷纷出台相应数据跨境法规。其中美国、澳大利亚等国奉行宽松的数据跨境流动政策，就美国而言，联邦层面并未立法禁止或限制数据跨境，但针对重点行业或领域的数据实行专门管控；而俄罗斯、印度、中国等国受本国特殊政治经济及文化环境影响对国家数据安全及主权更为关注，俄罗斯更是施行数据本地化的治理策略。

欧盟数据跨境法规解读

欧盟数据跨境法规规制的出发点在于保障个人数据主体的数据权利，因此并不禁止数据的跨境流动，也不强制要求本地化，但对数据接收方的数据保护水平或保障措施等做出要求，具体而言，数据控制者主要可通过以下三种方式进行个人数据跨境传输活动[3]：

1. 个人数据可传输至获得欧盟“充分性认定”的国家或地区，也即“白名单”制度。

该名单由欧盟委员会根据个人信息保护立法状况、执法能力，是否存在有效的救济机制等做出综合评估。截至目前，中国尚未获得欧盟“充分性认定”，国内企业暂时无法通过该等路径进行数据跨境传输。此外，美国虽未获得充分性认定，但与欧盟不断就数据跨境磋商并达成双边协定，并根据《欧美隐私盾协议》（EU-U.S. Privacy Shield）取得类似“白名单”地位，后该协议在Schrems II案中由欧盟法院宣告无效，但双方于2022年3月25日就新的《跨大西洋数据隐私框架》（Trans-Atlantic Data Privacy Framework）达成原则性一致，欧美数据跨境流动开启了新的可能性。

2. 针对未获得“充分性认定”的国家和地区，企业可采取以下任一由欧盟认可的充分保障措施来进行跨境传输活动：

（1）通过公共当局之间有法律约束力和可执行性的文书。

（2）建立有约束力的公司规则，主要适用于集团型跨国企业，即集团可以就集团内统一适用的数据处理机制申请个人数据监管机构认可，获准后个人数据可以从集团内的一个成员合法传输给另一个成员。

（3）与数据接收方签署欧盟委员会通过或批准的标准合同条款，考虑到操作难度、成本等，该措施实践中为多数企业采纳。此外，2021年6月4日，欧盟委员会对合同条款进行了更新，自2022年12月27日起，双方需签署新版合同并根据要求对境外接收方所在地的法律环境及数据保护水平进行评估。

（4）遵守行业协会拟定的并经欧盟委员会事先认可的行为准则。

（5）数据接收方的数据处理流程通过相关认证，每三年需更新一次。

[3] 欧盟《一般数据保护条例》（General Data Protection Regulation）第44-49条。

3. 特定情形下的豁免。

如跨境流动取得了数据主体的明确同意，或该跨境流动是为了履行与数据主体之间的协议所必需，为公共利益等，应属例外，该条路径实际适用场景较少。

值得注意的是，若公司未按照前述要求进行个人数据传输，则需就相关主体所受损失进行赔偿，并需缴纳最高达2000万欧元或就一项经营而言其上一财政年度全球全年营业额的4%（两者以较高为准）的行政罚款[4]。

美国数据跨境法规解读

美国奉行宽松的数据跨境流动政策，在联邦层面并未明确对数据跨境流动进行限制；但与欧盟立法偏重个人数据权利保护不同，美国数据跨境法规与贸易政策深度绑定，对重要或关键部门或领域的数据跨境流动进行分散但严格的管控，同时通过立法赋予国内执法机构对境外数据进行长臂管辖的权力。

首先，美国针对特殊或关键行业或领域的数据出境构建了分散但严密的监管体系，例如针对外商投资领域，美国将涉及关键技术、关键基础设施或美国公民敏感个人信息的投资或交易纳入国家安全审查的范围，由美国外资投资委员会（CFIUS）进行安全审查[5]，防止外国企业涉足处理美国公民敏感个人数据的美国企业。又如，军用或军民两用物项的进出口管控中要求部分关键技术与特定领域的数据出口传输到位于美国境外的服务器保存或处理的情形，需要取得商务部产业与安全局（BIS）出口许可[6]。同时，针对金融、医疗、电子通信等其他特殊领域的数据出境，亦出台相应的监管措施[7]，从而构建起严密且多层次的数据主权监管体系。此外，美国亦积极通过执法开展数据监管，如中国某知名云服务提供商因被怀疑获取或传输美国数据而被美国商务部调查等。

其次，美国通过长臂管辖授予本国广泛的数据管理权力，例如美国可以基于国家安全需要调取境外存储的数据，并且可调取数据的范围并不限于美国人的数据，所涉企业也不局限于美国企业或总部在美国的外国企业。外国企业只要在美国提供业务并且与美国发生了充分的联系，就可能被要求提供数据[8]。因此，中国企业赴美经营需要更加关注中美贸易政策及其相关合规风险。

[4] 欧盟《一般数据保护条例》（General Data Protection Regulation）第82及83条。

[5] 美国2018年《外国投资风险审查现代化法案》（Foreign Investment Risk Review Modernization Act of 2018）第1703章。

[6] 美国《出口管理条例》（Export Administration Regulations）第730.7章

[7] 美国《金融现代化法》（Gramm-Leach-Bliley Act）、《健康保险隐私及责任法案》（Health Insurance Portability and Accountability Act）、《电子通信隐私法》（Electronic Communication Privacy Act）等

[8] 美国《澄清海外合法使用数据法案》（Clarifying Lawful Overseas Use of Data Act）第103章。

俄罗斯数据跨境法规解读

由于特殊的历史文化背景和政治经济环境，俄罗斯数据跨境法规的一个显著特点是更为关注国内数据安全，对数据跨境流动施行严格管控，提出了数据本地化的监管策略，但这并不意味着俄罗斯禁止数据的跨境流动，在满足特定条件的情况下，数据处理者可以将个人数据传输至境外。

具体而言，俄罗斯数据本地化的要求是指相关公司均需在俄罗斯境内的服务器上存储和处理俄罗斯公民的个人信息，并将境内服务位置告知联邦通信、信息技术和大众媒体监管局（Roskomnadzor，以下简称“联邦监管局”）[9]，受监管主体包括俄罗斯实体、在俄罗斯有官方代表和分支机构的外国实体，以及在俄罗斯没有官方机构但针对俄罗斯消费者开展业务的外国实体。此外，通常情况下，个人数据处理者向境外传输个人数据有以下两条路径：

1. 个人数据可传输至获得“充分性认定”的国家或地区（中国于2022年被列入白名单第二组）。但自2023年3月1日起，个人数据处理者需就跨境意图提前通知联邦监管局，联邦监管局有权限制或禁止其向进行境外传输[10]。

2. 若个人数据传输至未获“充分性认定”的国家或地区，则个人数据处理者需取得联邦监管局申请许可，该种路径下，个人数据处理者和境外接收方都承担更重的合规义务。另一方面，俄罗斯数据执法力度相较而言较轻，其数据存储本土化规则自2015年9月开始实施以来，联邦监管局检查发现的违规企业数量较少，但依据2019年行政罚款规定，对于违反数据本地化要求的运营者，最高将处以1800万卢布的罚款。

2.2 中国数据跨境法规

与美欧相比，中国更多地从维护网络安全和数据主权为目的出发，制定跨境数据流动法规体系。具体而言，现行法律框架可以概括为“1+3+N”的模式，监管机构亦形成“1+X”的多方配合机制，数据跨境监管日益完善。

中国数据跨境法规体系概览

中国现行跨境法律监管体系由“1+3+N”组成，“1”即《国家安全法》，作为整个跨境监管体系的基石，进一步强调数据跨境监管中对国家网络安全和数据安全的保障。“3”即《网络安全法》《数据安全法》以及《个人信息保护法》，作为数据安全监管领域的三驾马车，分别对网络安全、数据安全以及个人信息保护领域提出原则性监管要求，并对关键信息基础设施、重要数据以及个人信息的跨境传输提出法律规制要求。“N”指在《国家安全法》和《网络安全法》《数据安全法》以及《个人信息保护法》基本框架之内，落实四部上位法监管要求针对数据跨境场景出台的法律和监管规定，包括专门的数据安全立法以及行业监管立法，其中数据安全立法包括《数据出境安全评估办法》《数据出境安全评估申报指南》《个人信息出境标准合同办法》及标准合同样本、《网络安全标准实践指南—个人信息跨境处理活动安全认证规范V2.0》《个人信息保护认证实施规则》等，进一步细化数据出境相关路径要求，为企业提供操作指引。此外，针对不同行业领域内的数据跨境，相应行业监管机构从本行业特点出发亦提出相应监管要求，从而构建多维度多层级的数据跨境监管体系。不同行业及领域企业须同时满足数据安全立法及各行业监管机构的数据跨境要求，由此也形成了由国家网信部门负责统筹协调和监督管理网络安全工作，国家电信部门、公安机关以及各行业监管机关共同配合的“1+X”监管机制。

[9] 俄罗斯联邦第242号法令《就“进一步明确互联网个人数据处理规范”对俄罗斯联邦系列法律的修正案》（Federal Law No. 242-FZ of July 21, 2014 On Amendments to Certain Legislative Acts of the Russian Federation for Clarification of the Procedure of Personal Data Processing in Information and Telecommunication Networks ）第2条

[10]《俄罗斯联邦个人数据法》2022年修正案（The Federal Law of 14 July 2022 No. 266-FZ on Amending the Federal Law on Personal Data）第12条。

中国数据跨境传输路径

在中国现有法律框架范围内，境内数据处理者向境外提供数据时，需根据出境数据类型、量级和规模等等，选择对应的出境路径。换言之，若境内数据处理者：（1）系关键信息基础设施运营者；（2）传输数据涉及重要数据；（3）处理100万人以上个人信息；或（4）上年度1月1日起累计向境外提供10万人以上的个人信息或上年度1月1日起累计向境外提供1万人以上的个人敏感信息，则需要按照《数据出境安全评估办法》及相关法律法规要求进行数据出境安全评估申报。若境内数据处理者向境外提供数据但量级未达到前述任何一个条件，则需要按照《个人信息出境标准合同办法》及相关法律法规要求进行备案。此外，境内数据处理者在涉及数据出境的情况下亦可按照《个人信息跨境处理活动安全认证规范》及相关法律法规要求申请跨境活动认证，合法进行数据出境活动。

若数据处理者未按照相应监管要求进行数据跨境传输，视情节轻重可能收到警告、罚款（情节严重可处一百万元以上一千万以下罚款）、责令暂停相关业务、停业整顿、吊销相关业务许可证或吊销营业执照，直接负责的主管人员和其他直接责任人员亦需缴纳相应罚款。

1 境外传输重要数据

场景1：数据处理者向境外提供重要数据

向境外传输重要数据的，即需要申报数据出境安全评估。

2 CIIO及100万以上的信息处理者

场景2：关键信息基础设施运营者和处理100万人以上个人信息的数据处理者向境外提供个人信息

以提供人数而非个人信息数量为标准，明确处理100万人以上个人信息的需进行安全评估。

3 自上年1月1日起向境外传输达到上限

场景3：自上年1月1日起累计向境外提供10万人个人信息或者1万人敏感个人信息

以最高两年时长为准，自上年1月1日起算，达不到数量要求的可以不用安全评估，达到数量要求的应当进行安全评估。

（图示为《数据出境安全评估办法》规定需申报数据出境安全评估的情形及判断要点）

3

典型数据跨境场景的风险及应对

3.1 典型跨境场景

在全球化背景下，数据跨境主体涵盖范围众多，跨国企业、具有跨境IPO上市需求的企业、和境外企业有业务往来的企业等都有可能涉及数据跨境传输。数据接收方包括跨国公司总部或其他分支机构、上下游合作伙伴、他国政府部门或监管机构等。数据跨境方式包括数据跨境存储、邮件跨境传输接收数据、网络跨境查询或访问数据、云环境下的应用登录访问、以及API接口等其他链路方式。

3.2 数据跨境带来的风险与挑战

企业数据跨境传输可能面临法律合规和监管风险、网络安全风险、操作风险、业务连续性风险等，从而导致企业财务损失、业务受限、声誉受损。

法律合规和监管风险：就境内而言，《网络安全法》《数据安全法》《个人信息保护法》《数据出境安全评估办法》均规定了网络运营者、关键信息基础设施运营者、个人信息处理者单位及个人对于跨境数据行为承担主体责任，如违反法律要求，可能将承担刑事和行政责任，面临经济和行政处罚。此外，各行业监管部门也对个人信息的保护提出了要求。同时，企业也需关注数据境外接收方所在国家的法律法规要求，并符合当地监管规定。

网络安全风险：在数据跨境传输的过程中，因传输链路较长，暴露面增加，终端设备、通信链路、数据库、应用系统、开放API等都存在受到网络攻击的风险。如在网络和系统中传输、存储、处理等环节的安全保护措施处理不当，跨境传输的数据存在被篡改、泄露、损毁的风险。

操作风险：数据跨境过程中经过多种IT基础设施，涉及不同角色和权限，如遇到业务违规操作、用户权限管理缺失、运维工具连接不当等问题，可能造成数据泄露、损毁等。

业务连续性风险：企业合规经营是业务连续性的关键保障。企业违反数据跨境的相关监管要求，将会面临来自监管机构的调查，进而产生通报批评、巨额罚款、停业整顿等处罚。另一方面，如企业遭受安全攻击并被公众获知，也将导致企业声誉受损，影响投资者信心和用户信任，影响企业业务连续性。

3.3 典型跨境应对

梳理数据跨境场景，掌握跨境整体情况。面对类型众多的数据跨境场景，梳理数据的位置、应用场景等信息，掌握正在进行中的跨境数据传输行为，包括涉及的业务场景和系统、数据类型、数据量、跨境原因、境外接收方信息等，避免隐私合规风险不可控。

加强数据安全整体防护能力。建设数据安全技术体系，根据法律法规要求对数据进行分类分级，加强数据全生命周期的安全防护措施，部署安全工具和技术手段，执行和优化防护策略，防止数据跨境过程中被破坏、泄露、篡改。

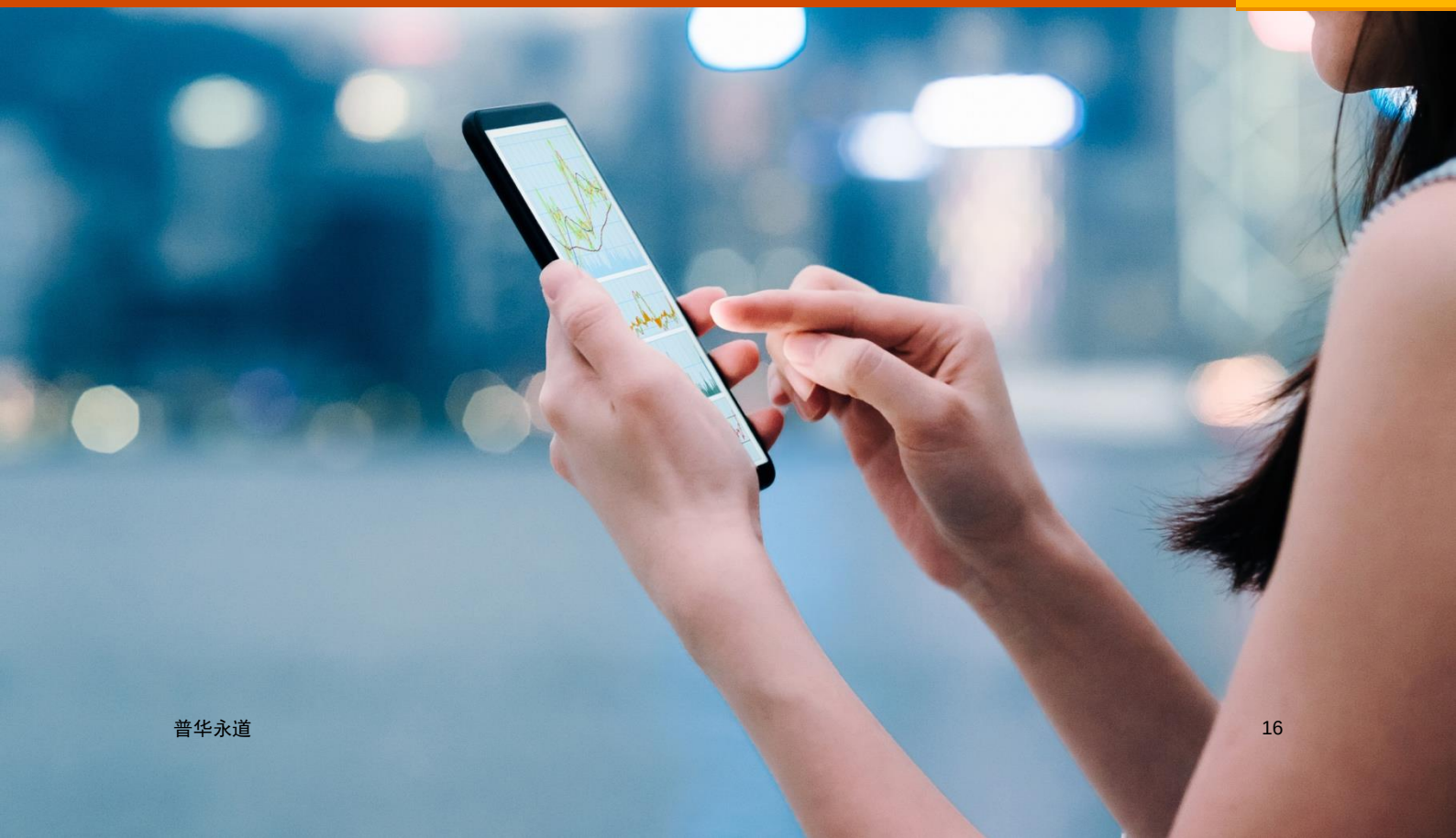
建立数据安全管理的组织和资源保障体系。企业需要建立组织保障体系对企业的数据安全进行全生命周期的管理与监督，对数据跨境法规动态开展跟踪与洞察，并建立及时有效的数据跨境合规的应对机制与体系。根据中国法律法规要求，重要数据的处理者应当明确数据安全负责人和管理机构，处理个人信息达到国家网信部门规定数量的个人信息处理者应当指定个人信息保护负责人，因此，企业应根据自身数据处理情形，按需设置相应管理机构及职位，统筹企业内部数据安全与个人信息保护工作，落实监管要求并促进企业数据安全管理体系的完善。同时，企业需要建立针对数据跨境合规的问责制度，企业可将内部员工对于内部数据跨境合规制度的遵循情况纳入到员工的评价机制中，针对违规情况对相关员工进行追责处理，并建立一套补救处理措施的机制与流程。

实施持续的合规监测、跟踪与改进。企业应对自身数据跨境行为进行持续监测，定期开展自评估，掌握数据安全状态以及接收方处理方式，尤其是个人信息、重要数据等敏感数据，及时发现跨境数据违规情况，保障数据有序依法跨境流动。

针对数据跨境合规与个人信息及隐私保护合规进行建立培训机制。随着国际上对于数据跨境及隐私保护的监管力度加强，企业需要建立针对数据跨境合规与个人信息及隐私保护合规方面的专项培训机制，确保企业所有员工都能及时了解相关法规的主要内容与影响，以及企业可能面临的风险与挑战，培养企业从管理层到员工的数据合规意识，将重视数据合规融入企业文化。

4

数据跨境合规应对



4.1 金融行业

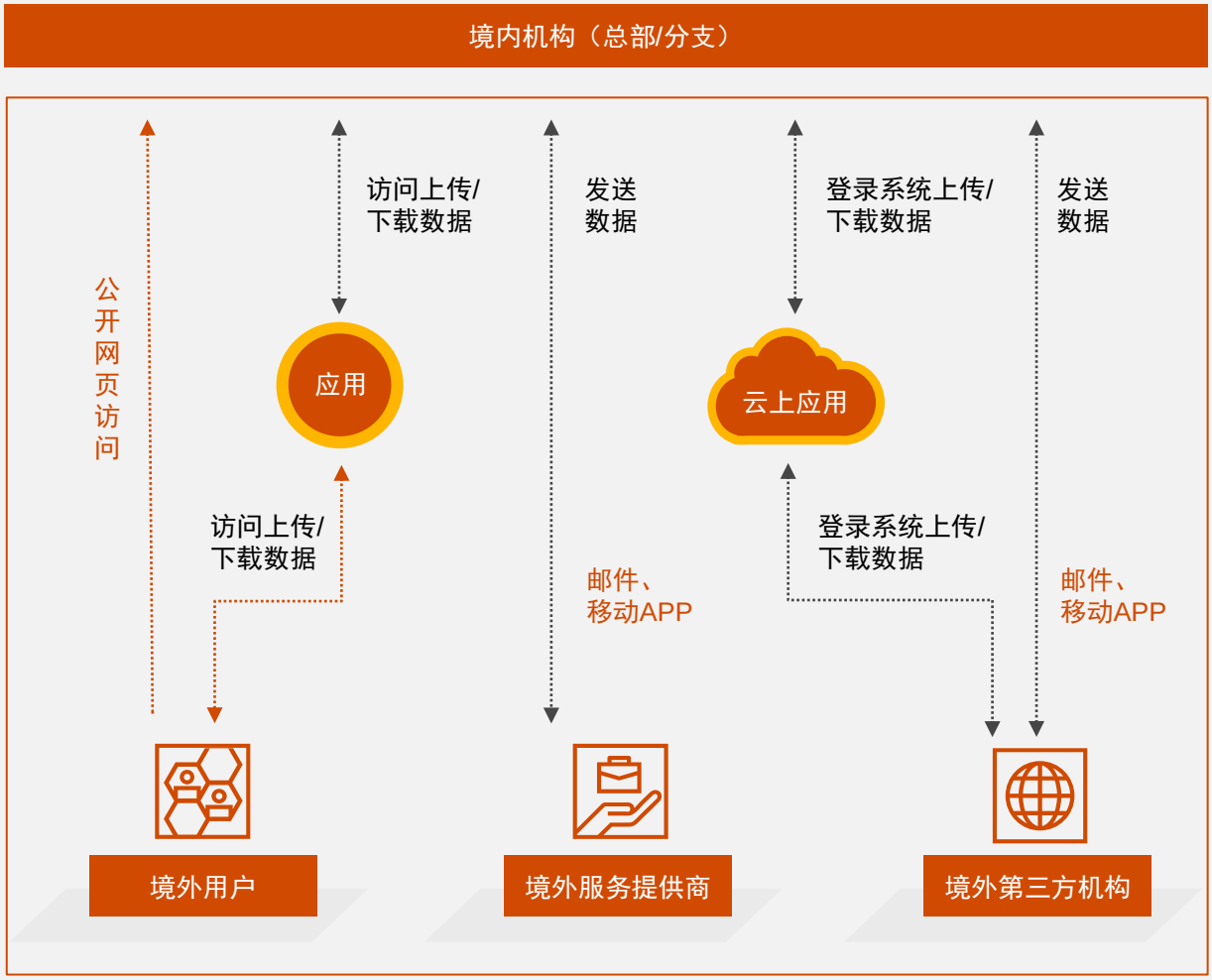
基于金融行业的跨境场景

1. 金融行业基于典型场景的场景描述和场景图

金融机构数据跨境主要包括银行、证券、保险、基金、信托、期货、租赁、第三方支付、财务公司、互联网金融等机构的数据出入境，根据数据发送方和接收方性质，主要存在以下场景：

（1）外部数据跨境场景

主要为存在境外业务及服务的数据主动出境，如境外监管机构基于反洗钱等规则要求传输数据；与境外第三方机构、服务提供商、用户为实现服务的数据传输和处理，包括数据跨境外后的再次传输；境外行业机构关系维护，填写行业调研信息，行业机构会议报名、会员管理等事项信息，报送投资相关数据、报告、非标投资产品信息等。



（2）数据公开出境场景

主要为金融机构公开披露信息的被动跨境，主要为官网或其他渠道公开披露的年度报告、偿付能力报告摘要、其他信息等的被访问和使用。

2. 金融行业典型数据跨境合规场景及字段

以保险公司数据跨境场景为例，保险公司日常向境外股东以及律师提供材料，通过精算软件进行数据分析工作，境外人员对人力资源系统的使用，境外员工通过学习平台进行会议及培训，在境外协会网站注册会员及维护，参加线上境外会议，参与境外调研等。涉及的部门包括集团总部、法律合规部、资产管理部、精算部、内部审计部、培训部、人力资源部、IT部、财务管理部等。

业务场景	业务领域	数据跨境环节	个人信息字段举例	重要数据字段举例	数据跨境合规应对举例
第三方外部数据跨境	境外专业机构会员维护	员工信息明细上传	姓名、协会会员ID、电子邮件地址、身份证号	——	加强与外部组织的合同约定，明确双方跨境数据安全责任，通过技术手段进行跨境数据安全管控，清晰掌握业务数据、重要数据、个人信息等敏感数据跨境流动详情。
数据公开出境	网站公开业务信息	业务类型、产品介绍	——	——	完善数据公开安全管控，通过数据安全治理识别存在数据跨境的人、业务、数据，建立数据跨境流动保障机制和审查机制，对出境数据、途径、行为进行实时检测和管控。

跨境法规对金融行业的影响分析和应对

1. 金融行业典型数据跨境合规场景应对

对于第三方外部数据跨境场景，加强与外部组织的合同约定，明确双方跨境数据安全责任，通过技术手段进行跨境数据安全管控，清晰掌握业务数据、重要数据、个人信息等敏感数据跨境流动详情。

对于数据公开出境场景，完善数据公开安全管控，通过数据安全治理识别存在数据跨境的人、业务、数据，建立数据跨境流动保障机制和审查机制，对出境数据、途径、行为进行实时检测和管控。

2. 金融行业关键应对措施

（1）数据跨境合规管控

从总体上完善内部的数据合规体系。对金融数据采取分级安全管理措施，提升自身的数据保护能力，对数据实施生命周期安全管理，制定和有效落实金融数据生命周期安全管理策略，如提前约定安全保护义务，保障接收方具有对等的数据安全管理及技术能力。在数据出境前，收集并及时关注网信部门和金融监管部门发布的相关法律法规，结合监管要求明确自身向境外提供数据时需要承担的义务，包括但不限于数据出境是否需要经过金融监管部门的提前审批、是否需要进行数据出境安全评估申报等。对于需要申报的情况，开展内部自评估后申请出境安全评估，根据评估结果对开展数据跨境活动的方案进行调整。

（2）出境数据安全性管控

金融机构需结合相关法律法规，明确机构自身的业务性质、主体性质和数据性质，包括但不限于明晰机构业务是否可能被认定为关键信息基础设施、机构自身是否属于关键信息基础设施运营者，以及需要向境外提供的数据是否属于重要数据、个人信息或敏感个人信息，对拟出境数据进行清晰的识别。企业可以通过建立数据跨境技术管理措施构建安全保障能力，包括数据传输保护措施，安全边界防护、安全漏洞技术发现、数据出境监测、数据权限访问控制、数据出境日志等。同时，通过跨境传输检测与跨境攻击窃取检测，清晰掌握数据跨境流动详情，为跨境风险自查和数据安全运营提供技术抓手和依据。

（3）跨境数据流转监控

建立对于数据跨境流转过程的监控机制。通过对个人信息、重要数据、商业数据进行跨境分析，以及失陷主机统计分析，发现什么人在什么时间什么地点以某种方式发送了什么数据。依据出境数据的规模、范围、种类、敏感程度等进行合规分析和关联分析。根据威胁情报、结合异常流量分析模型针对加密出境流量进行检测，发现异常情况。对数据出境的目的地址、传输数据种类、传输数据方向、数据量大小、数据传输频次等维度进行异常行为监控，重点对敏感数据进行分析，对重点事件进行留存取证。

（4）数据跨境事件应急

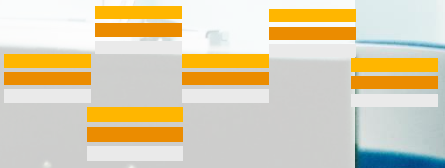
制定数据跨境安全事件应急预案，确定对数据接收方发生数据泄露、损毁、滥用等安全事件的应急处置、安全事件告知和上报等相关内容，根据相关法律法规、安全技术、事件处置经验等及时更新应急响应预案。发生数据跨境安全事件时及时采取有关措施，告知受影响的相关方，按照规定向行业主管部门上报，采取临时中断数据跨境或其他减缓损失的措施，详细记录数据跨境安全事件信息。

3. 金融行业数据跨境合规最佳实践

某大型跨国金融企业，在境外有分支结构和大量合作伙伴，和境外的交互有多条专线，涉及邮件、ERP、音视频会议等多种业务系统。作为金融行业重点企业，该企业面临监管部门针对数据出境情况的约谈，亟需通过技术等手段梳理数据出境场景，加强数据出境监控，应对监管需要和自身管理需要。

进行跨境数据检查共发现数据出境事件939次，其中938次为境外主动获取，1次为境内主动外发。传输敏感个人信息包括user ID、密码、省份、手机号、银行卡号等，涉及境外地区包括新加坡、匈牙利、瑞典等地区的境外IP7个。发现内部设备通过http传输音视频会议的地址信息超过800次，传输设备维修单、说明书等，主动向境外发送工资单多次。

全方位的梳理数据出境情况，包括传输的敏感个人信息类型、详情等、传输的源头，包括客户业务系统主机、个人主机等，跨境传输的目的地国家、IP地址等。有效梳理数据出境，不仅应对监管需求，同时发现内部可疑的数据出境事件，便于制定针对数据安全的技术和管理手段，保证安全生产。



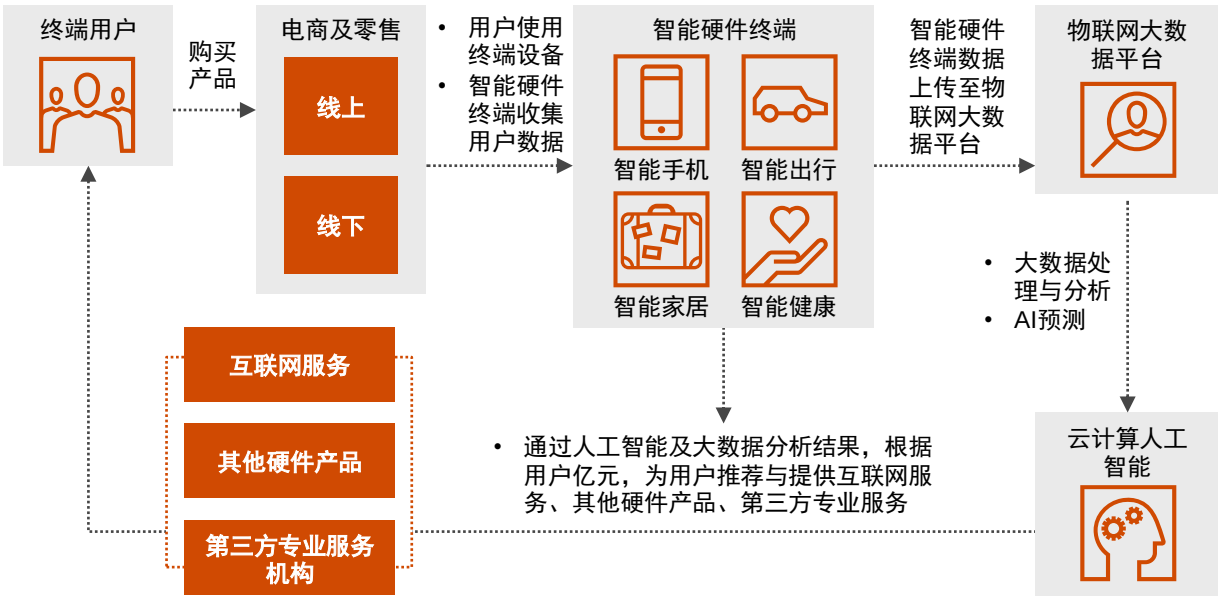
4.2 科技互联网行业 — 以智能硬件为例

科技互联网行业包含的细分领域众多且复杂，不同细分领域的业务场景与商业模式差异性较大，本章节仅针对智能硬件领域，并以中国企业向欧洲出海为前提，因此企业主要面临在欧洲市场向中国总部进行数据跨境传输的风险以及GDPR合规的挑战。

基于智能硬件行业的跨境场景

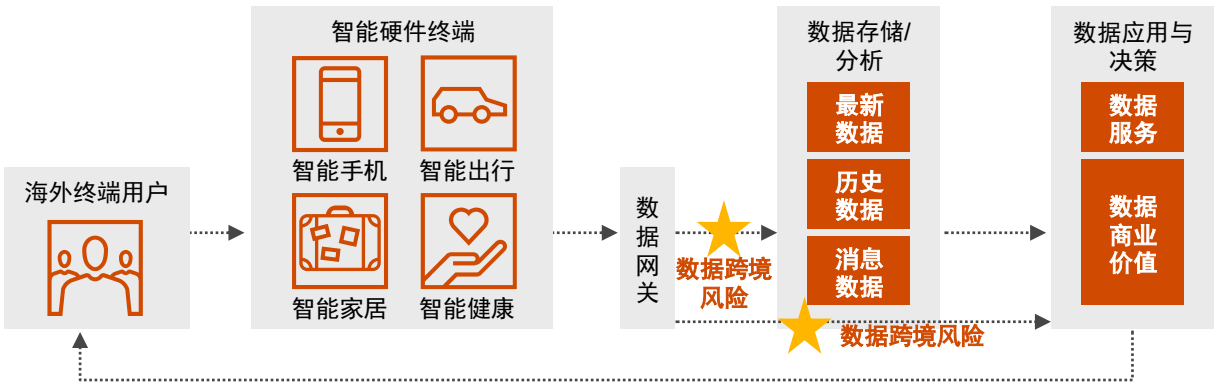
1. 智能硬件行业基于典型业务场景的数据流转过程

智能硬件行业的业务场景复杂，涵盖的领域众多，个人信息及数据主要是通过物联网生态进行数据流转与传输。



2. 智能硬件行业全球数据跨境

对于智能硬件行业来说，其数据流转过程中最容易发生数据跨境风险的是终端数据经过数据网关上传至数据存储与分析平台的环节，由于数据存储与分析平台的数据中心有可能遍布全球不同国家，因此极容易产生数据跨境风险；同时，另一个最容易发生数据跨境的环节就是数据应用与决策环节，因为对于全球化的企业来说，其数据决策者有很大的可能不在数据收集地境内。



跨境法规对智能硬件行业的影响分析和应对

1. 智能硬件行业典型数据跨境合规场景及应对举例（以GDPR为例）

随着数字化基础设置的普及与物联网生态体系的不断完善、智能硬件行业快速发展，中国智能硬件企业不断创新并纷纷拓展全球市场。其中，欧洲市场凭借其庞大的智能硬件产品市场与较高的消费水平成为了企业出海的主战场，而布局欧洲意味着智能硬件企业需要面对欧洲GDPR数据合规的严苛要求。

业务场景	相关信息	主要风险	数据跨境合规应对举例
用户获取	• 用户购买信息 • 从第三方社交网络服务商获取的个人信息	• 违反隐私政策透明性风险 • 用户同意的获取不充分的风险	展示隐私政策，取得用户同意： • 用户在使用产品之前，商家应当采用显著方式向用户提示平台的隐私政策，阐明所收集的个人数据的种类、处理用途、存储期限等，在充分尊重用户知情权的情况下获得其明确的同意与授权。 • 同意应当由用户自行选择，不能默认设置，预先勾选。不恰当的做法可能被认为没有有效地取得用户同意。
用户服务	• 用户使用相关硬件的应用程序的基础信息 • 用户使用售后及支持服务的信息 • 对用户使用个性化推荐服务时的信息	• 隐私政策不完整风险 • 未充分履行个性化广告提示义务风险 • 数据处理范围等隐私政策未进行明显标识的风险	• 采取充分适当的安全保护措施，比如对个人数据进行加密、假名化处理等，保护数据不被未经授权访问、毁损或丢失。具体安全措施可以参考国际标准ISO 27001。 • 完善隐私权政策，在隐私权政策中应当披露对于用户个人数据收集与处理活动。
智能硬件通用场景	• 智能设备信息 • 用户账号基本信息 • 设备定位信息	• 未充分获取用户同意的风险 • 对于位置数据，存在违规使用的风险	• 移动应用未经用户同意，私自收集设备识别信息、商品浏览记录、搜索使用习惯、常用软件应用列表等个人信息，并且未经同意就共享给第三方； • 位置数据的使用应进行匿名化处理，位置数据处理应遵循数据最小化原则。
智能手机	• 用户手机端个性化活动记录信息 • 部分具有NFC功能的手机将采集用户支付信息	• 手机应用信息违规采集信息风险	• 对手机内的应用进行全生命周期的合规检测； • 建立与完善应用程序隐私合规审批与下架机制。

业务场景	相关信息	主要风险	数据跨境合规应对举例
智能健康	• 用户健康基本信息 • 用户运动信息 • 用户睡眠信息	• 对于健康数据这类的特殊种类个人数据，企业需要满足相关资质才可以收集与处理，企业存在违规收集与处理的风险 • 对于健康数据，成员国可以设置额外限制条件，企业需要防范不同国家法律合规差异的风险	GDPR对健康信息等具有敏感特性的个人数据的处理确立了更高的保护标准，要求企业必须满足相关资质并获得数据提供者关于某明确合法用途的授权，并出示数据获取方法的证明。 • 对于具有个人健康数据的特殊数据，其数据使用和处理必须获得数据主体的明确同意； • 数据处理者应获得由欧盟或会员国法律或集体协议授权，才可以进行特殊数据的处理活动； • 设定数据保护官来负责监控健康数据的保护与合规情况，数据保护官不应参与个人数据处理活动的决策，主要职责是向企业提供数据保护的建议； • 为健康数据在不同系统间的交互、共享和运营提供安全与便利条件； • 建立健康数据安全监测和预警系统，建立网络安全通报和应急处置联动机制。
智能家居	• 用户作为会员的订阅信息 • 智能家居设备个性化设置信息	• 对于人像数据这类的特殊种类个人数据，企业需要满足相关资质才可以收集与处理，企业存在违规收集与处理的风险	• 对于具有人像信息的特殊数据，其数据使用和处理必须获得数据主体的单独明确同意； • 设定数据保护官来负责监控特殊个人数据的保护与合规情况，数据保护官不应参与个人数据处理活动的决策，主要职责是向企业提供数据保护的建议； • 对于视频监控和访问控制，GDPR规定的一个主要内容就是能够持续记录系统运行情况并确保其免受网络攻击，因此需要企业建立统一流畅的安全管理流程，并支持自动化记录这些流程。
智能出行	• 设备功能及状态信息 • 设备与用户的交互信息	• 对于位置数据，存在违规使用的风险	对于位置数据的使用和接触追踪应用，应该： • 通过匿名化手段来满足GDPR对于位置数据使用的合规要求，匿名化是指使用一套技术以消除数据与已识别或可识别的自然人间的联系能力，即便经过任何“合理”努力也无法恢复这种联系，为了实现匿名化，必须仔细处理位置数据以满足合理性测试。 • 在进行位置数据跟踪处理时，应通过数据最小化原则来进行数据合规处理，例如：除非处理个人数据有绝对必要，企业应特别警惕不要收集位置数据。接触跟踪应用程序应使用邻近数据并且采取适当措施防止重新识别；所收集的信息应存放在用户的终端设备上，只有在绝对必要时才应收集相关信息。 • 当个人数据被转移到欧盟境外时，应采取特殊的保障措施，以确保保护随数据一起进行。

2. 智能硬件行业关键应对措施

（1）企业自我风险评估

风险评估贯穿于企业GDPR合规制度的建立、实施以及更新完善的每一步，也是企业判断GDPR合规制度是否必要以及如何建设的首要步骤。企业首次进行GDPR风险评估的重点为：GDPR是否适用企业；对GDPR所涉业务领域筛查及其生命周期分析。企业需要自身的业务活动和领域进行梳理和筛查，并对相关数据的收集、使用、处理、保存和跨境传输的状态进行具体的梳理和分析。对于智能硬件企业，需要首先按照其产品经营模块进行梳理和筛查，确定GDPR合规风险较大的业务模块和领域，其次需要对识别出来的业务模块根据所涉及的相关数据的收集、使用、处理、保存和跨境传输的状态的每一个环节，比照GDPR的规定，进行风险识别与问题发现。

（2）根据GDPR的相关规定，任命数据保护专员（DPO）

对于智能硬件行业来说，大量业务涉及特殊种类的个人数据，例如生物特征数据以及健康数据，企业需要任命数据保护专员（DPO）来保障特殊种类的个人数据的安全，并及时公布数据保护专员（DPO）的联系方式并向监管进行告知。企业需要尤其注意保障DPO的独立性，同时，企业可以通过整合现有的内部合规资源、识别并避免各组织团队间的利益冲突、构建DPO对业务活动的定期参与机制来确保DPO履行其职责。

（3）基于不同产品条线及业务场景，建立从产品前端到IT系统架构的风险管理体系企业风险管理体系主要包括以下五点：

a. 企业应该首先设计并建立全面的、有效的基于GDPR的隐私政策及相关协议，并充分落实隐私政策和相关协议文档的内容。

b. 建立用户权利响应机制，需要明确该机制是否充分覆盖所有涉及GDPR规定的个人数据的业务及场景、用户权利的响应时效是否满足GDPR要求、是否全面覆盖用户的所有个人数据、用户权利中心自身的数据安全性控制是否有效。

c. 数据全生命周期安全风险管理，主要包括：所有智能硬件产品的个人数据采集安全，欧洲地区用户营销的数据合规管理、使用第三方服务时的数据合规管理、员工个人信息安全及数据跨境合规管理。

d. IT系统安全风险管理，主要指承载业务功能的信息系统在安全控制方面的合规风险。

e. 隐私管理机制，主要包括隐私管理相关的组织架构、制度和流程的执行情况。

（4）新产品的GDPR合规管理

对于企业未来将要投入到欧盟市场的产品和服务，企业应该在研发与设计过程中就嵌入GDPR的合规要求。例如通过对产品开发人员与设计人员的合规培训，培养其数据合规理念，并建立必要的保障制度或审批流程，建立产品合规的责任机制。

3. 智能硬件行业数据跨境合规最佳实践

某科技互联网企业是一家以手机、智能硬件和IoT平台为核心的科技互联网企业，也是中国科技互联网企业出海队伍的第一梯队，随着该企业全球化程度的加深，其境外市场规模逐渐扩大，其中欧洲市场已逐渐成为其核心收入来源，相关产品出货量的同比增长也不断刷新记录。而欧洲作为全球范围内对用户隐私保护最严苛的地区，如何在保持市场增长的同时满足当地数据法规的要求，成为该企业长期发展的主要挑战之一。

在组织建设方面，早在2014年，该企业就正式成立了信息安全与隐私委员会，并通过技术防护、流程制度、评估和审查机制等，为其建立一套完善的安全与隐私管理体系。

在合规体系的监督与审计上，在GDPR正式生效前，该企业就通过专门实施的涵盖企业所有产品线及部门的GDPR合规项目，通过了GDPR第三方审核与认证，并且持续进行年度审核与评估，以保证该企业持续符合GDPR规定。

在技术创新方面，该企业通过在终端系统中推出了照明弹、拦截网、隐匿面具、剪切板隐私保护、沙盒机制、模糊定位等诸多业界领先的隐私保护创新功能，来促进用户隐私及数据合规，充分贯彻了GDPR数据处理关于最小化、准确化、存储限制化等原则。

在合规文化建设上，该企业会定期举办安全与隐私宣传月，包含安全隐私学堂、安全隐私技术公开课、科技园互动体验展、专项培训营、系统隐私功能揭密等活动。在合规培训上，安全与隐私委员会为该企业全体员工提供了数十小时的在线安全与隐私课程，帮助上万名员工提升安全与隐私的防护意识。此外，该企业还为隐私工程师提供了IAPP（国际隐私专家协会）的专项认证培训，有效促进专业人才培养，确保该企业的硬件产品在用户数据保护方面建立坚实的防线。

4.3 汽车行业 — 以车联网为例

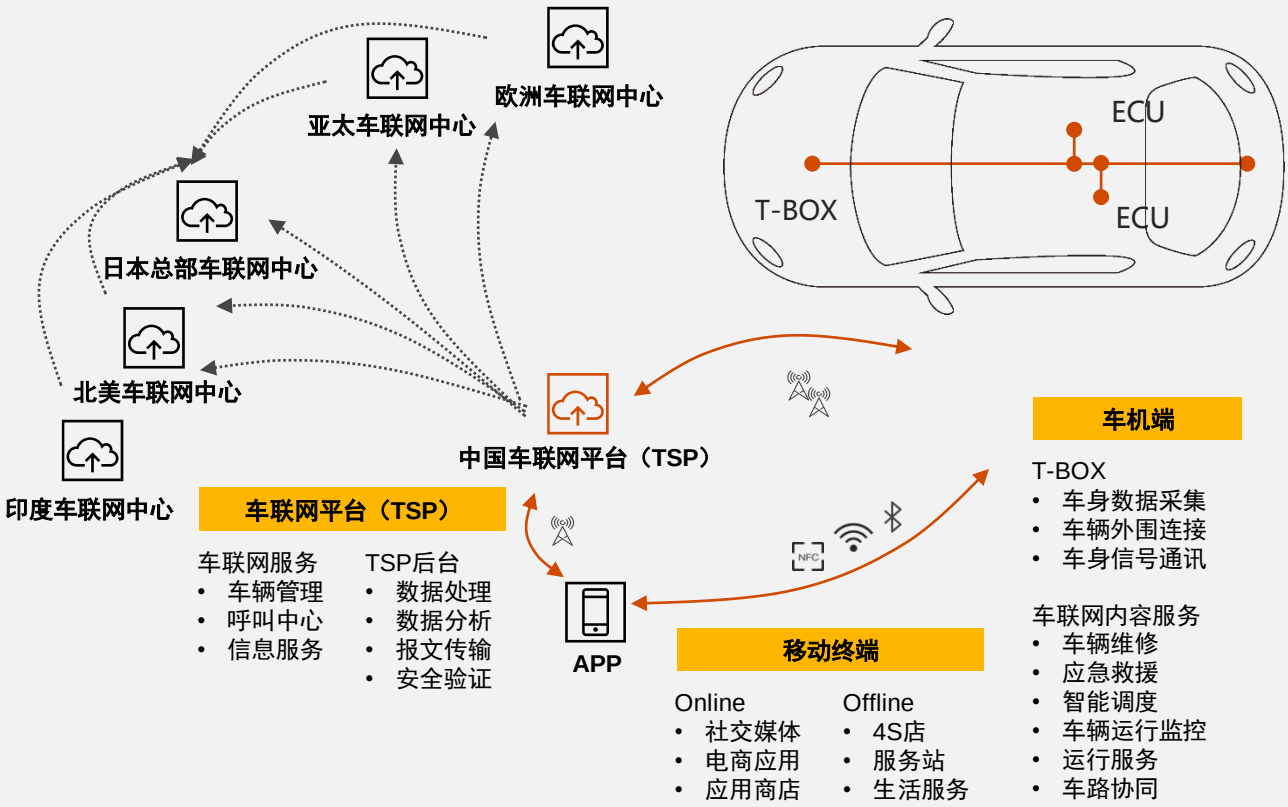
近年来，车联网产业呈现蓬勃发展的势头。本章节以车联网领域为例，以海外企业在中国运营为前提，阐释汽车企业面临的数据跨境风险以及中国网络安全、个人信息保护及汽车行业合规的挑战。

基于车联网行业的数据跨境场景

车联网行业基于典型场景的场景描述和场景图

在智能汽车领域政策法规层面，规章制度和行业标准方面逐步出台了诸多具有深远影响的规定，例如《汽车数据安全管理若干规定（试行）》《关于加强智能网联汽车生产企业及产品准入管理的意见》《关于加强车联网网络安全和数据安全工作的通知》《车联网信息服务用户个人信息保护要求》《汽车采集数据处理安全指南》。因此，厘清数据跨境场景、梳理数据跨境合规应对、建设数据安全和隐私保护体系对车联网企业尤其重要。

随着车联网“人、车、平台”的建设，车联网行业可分为移动终端、车机端和车联网平台（TSP）三个场景。特别是车联网平台（TSP），数据出境场景尤其复杂。以某日本车企为例，目前，该车企除日本互联总部外，共创建北美、中国、印度、欧洲、亚太共5个互联中心，为车主提供标准统一、内容多元的车联网服务。从2019年开始，该车企开始在中国市场全面推广车联网服务，所有新上市的汽车均标配车载数据通信模块。由于车联网平台将通过遍布全球的资源和服务器提供产品或服务，个人信息可能会被转移到使用产品或服务所在国家/地区的境外管辖区，或者可能被来自这些管辖区的个人或组织访问，构成数据出境。



跨境场景跨境法规对车联网行业的影响分析和应对

1. 车联网行业典型数据跨境合规场景应对

业务场景	相关信息	主要风险	应对举措
车机端	• 车机登陆信息 • 车控信息 • 售后服务信息 • 支付信息 • 包含人脸信息、车牌信息等的车外视频、图像 • 汽车充电网的运行数据 • 车辆位置数据 • 驾驶员监控数据	• 车机端辅助驾驶感知功能可能收集敏感地区的视频、图像以及道路交通流量等信息，充电功能可能收集充电网运行数据，均属于重要数据，存在重要数据泄露风险 • 车机端重要数据的出境合规风险	重要数据管理： 1. 明确数据安全负责人和管理机构，落实数据安全保护责任； 2. 重要数据收集后应当在境内进行存储；确需向境外提供个人信息和重要数据的，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； 3. 企业自行或者委托数据安全服务机构每年开展一次数据安全评估，并在每年1月31日前将上一年度数据安全评估报告报设区的市级网信部门； 4. 处理重要数据的系统原则上应当满足三级以上网络安全等级保护和关键信息基础设施安全保护要求等。
APP端	• 账号信息 • 车主信息 • 车辆状态信息 • 用户社区浏览记录 • 客服沟通记录	• 随着车联网服务发展，APP端功能增多，可能涉及收集用户身份证号、银行账号、交易信息、浏览记录（埋点）等个人敏感信息，可能造成用户告知不及时、不充分，不能及时响应客户诉求，侵犯用户权利 • 个人信息跨境未单独获取用户授权	用户告知： 1. 个人信息符合开展业务所需的最小必要原则； 2. 确保“告知-同意”隐私政策中明示收集使用相应个人信息字段的业务场景，收集信息的目的、方式、范围；在用户同意隐私政策后，调用采集个人信息相关接口； 3. 梳理敏感权限的申请目的告知文案，避免敏感权限强制、频繁、过度索取权限。 用户权利响应： 1. 保障用户权利反馈渠道畅通，在30天内响应用户权利请求，如不能响应，需向用户说明具体原因； 2. 日志记录各业务团队涉及个人数据的存储平台中的增、删、改、查等操作。 数据跨境： 在隐私政策中，向用户告知数据出境的境外接收方的名称或者姓名、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，并取得个人的单独同意，保留单独同意记录。
车联网平台-TSP	• 车联网服务信息	• 车联网平台可能涉及在多个国家间共享数据，存在数据跨境合规风险； • 车联网供应商众多，可能涉及复杂的数据共享场景，易造成用户告知不充分、数据保护权责不明确等风险	数据跨境： 车联网平台建立本地数据中心，数据本地存储，如涉及数据跨境，需进行合规评估，并满足监管备案或申报要求 第三方个人信息共享： 明确车联网平台（TSP）的角色，如涉及个人信息的共享、转让、间接收集等，需承担相应的安全保护义务，并告知用户。

2. 车联网行业关键应对措施

结合车联网行业的监管要求和业务特点，企业应从强化风险应对能力、合规运营能力和产品合规能力三个维度出发，建立健全风险管理的制度设计、组织建设、机制运转和产品设计，全面提升企业风险承受能力。

（1）强化风险应对能力

面对日益趋严的监管要求和公众对隐私保护的关注与担忧，企业应建设车联网信息安全组织与架构，明确各角色分工与职责，建设车联网治理文化，及时回应舆情和用户诉求，并建议通过取得相关合规认证的方式进行外部建信。

（2）搭建合规运营能力

从车联网的产品运营到平台运营，贯彻安全设计（Secure by Design）和隐私设计（Privacy by Design）的理念，设计包括用户身份管理、授权管理、用户权利响应、数据处理行为监控、数据安全和个人信息安全事件应急机制在内的数据安全和隐私保护流程。

（3）建设产品合规能力

从需求、设计、开发、测试、部署、运维等各流程把握安全合规基线，明确用户敏感数据和个人信息保护的场景、规则、技术保护方法（包括加密、匿名化、去标识化、数据脱敏等）。开展车联网平台的数据治理工作，解决数据共享风险和数据商业化开放风险，搭建数据出境合规框架，落实数据出境监管要求。

3. 车联网行业数据跨境合规最佳实践

作为行业引领者，某跨国车企将数据安全和用户隐私保护深植于公司文化，不仅建立了一套完善的全球通用的数据安全和隐私保护流程与规范，同时针对中国监管进行了一系列公司管理、业务流程和产品设计的定制，从用户隐私保护、重要数据管理和数据跨境合规三个维度提升合规水平和风险管理能力。

（1）用户隐私保护

依据隐私说明，该车企收集来自或有关用户、用户的车辆的信息或来自第三方的信息，其披露的内容囊括了《汽车采集数据处理安全指南》的数据类型分类，并对其具体字段和合法处理理由进行了说明，符合《个人信息保护法》要求的对“个人信息的处理目的、处理方式，处理的个人信息种类、保存期限”进行告知的基本披露要求。

（2）重要数据管理

车外数据涉及包括重要敏感区域地理信息、流量信息、人脸信息在内的大量敏感个人信息和重要数据。对此，该公司对车外摄像头数据处理方式进行了改造。一方面，该公司在隐私政策中提示，用户必须查阅并遵守当地法律法规以及场所对使用摄像头的相关规定并独自承担全部责任；同时，在实操中进一步防范了合规风险，其在中国区提供的远程监视功能中不会捕捉连续的视频录像，也不具有实时取景功能，用户无法访问车外摄像头拍摄的视频影像。

（3）数据跨境合规

目前，该公司已经在中国建立了上海超级工厂数据中心，并完成了数据中心相关审批备案要求。该数据中心用来存储中国用户的所有数据，包括生产、销售、服务、充电数据等，以及所有个人信息都安全储存在中国国内，不会转移到海外。只有在需要从海外订购备件等特殊情况下，个人数据才会在获得相关批准后进行转移。

4.4 企业内部管理场景

基于企业内部管理的数据跨境场景的风险和应对

<table>
<tr><th>场景分类</th><th>具体场景</th><th>相关信息</th><th>主要风险</th><th>应对举措</th></tr>
<tr><td>人力资源管理</td><td>候选人简历及面试、员工管理、员工/家属福利、员工差旅报销、员工薪资发放等</td><td>• 员工个人敏感信息
• 员工家庭信息</td><td rowspan="5">1. 数据违规收集：
过度收集、不合理索取权限、违规收集、企业未告知员工/第三方以何种方式收集哪类数据信息，甚至非法获取（盗取）数据等，如未经同意收集人脸、指纹、身份证号、进行录音等
2. 数据保护管理：
• 由于企业关键基础设施存在漏洞，数据安全系统容易遭到攻击/破坏/数据窃取，或员工故意/过失泄露信息，导致数据泄露
• 各类数据规定的存储期限不明确
• 与第三方合作时（例如体检机构、社保机构、招聘网站等）/第三方再委托丙方代理时，签署的协议中没有覆盖数据保护相关内容，或未对受委托方/委托行为进行安全评估审查
3. 数据非法使用：
未经员工/第三方同意，私自将设备识别信息、交易记录、工作经历、健康状况等个人信息共享给其他第三方
4. 数据跨境：
企业并未关注数据存储的地点，未在必要时进行数据本地化的备份</td><td rowspan="5">1. 数据内容合规：
关注收集的数据是否涉及个人信息、个人敏感信息、重要数据等
2. 数据来源及收集方式合规：
数据的来源及获取途径及方式是否合法合规，是否得到信息主题的同意并告知收集后的用途；当数据系第三方提供是，确保第三方资质符合要求，并对第三方来源数据设置审核机制等
3. 数据跨境合规：
企业需关注数据存储的地点，并在必要时进行数据本地化备份</td></tr>
<tr><td>第三方管理</td><td>供应商采购、国际货运及仓储等环节，企业会收集供应商/合作商、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</td><td>• 供应商与第三方合作商的商业信息</td></tr>
<tr><td>内部汇报审核</td><td>向企业海外总部进行汇报或法务审核</td><td>• 汇报审核人的个人敏感信息
• 分支机构合作商的商业信息</td></tr>
<tr><td rowspan="2">IT管理</td><td>IT运维：远程访问各类数据</td><td>• 相关员工的个人信息
• 相关的业务数据</td></tr>
<tr><td>安全：通过客户端监控收集浏览记录，Cookies，MAC地址等</td><td>• 员工的设备信息、位置信息、使用信息等</td></tr>
</table>

企业内部管理的数据跨境合规应对

1. 企业内部管理数据跨境合规关键应对措施框架

（1）企业需关注数据来源的合法性。具体而言，企业在获取信息数据时，应以合规为导向，仅收集正当的、必要的信息，需确认已经获得信息主体有关于信息收集的同意，并及时告知信息使用场景。

（2）企业需对内部的数据安全进行管理，制定覆盖全数据生命周期的安全管理制度，合规运作应有高层的参与，形成较为成熟的合规组织体系与架构，并组织定期的培训和沟通。具体来讲，企业需建立隐私评估机制，对每一项业务流程或系统进行个人隐私及数据保护影响的评估，需以最小化数据存储及最大化保护数据安全为目标，同时具备数据检索能力，了解数据存储的位置、哪些员工有访问权限及存储的期限等。

（3）企业的数据的使用与处理应当采取合法、正当的方式。具体而言，企业内部需建立成体系的数据合规保障制度，明确数据合规保障步骤、明确相关的负责人员、确保所有的实施细节都做到合法合规，并对安全保障实施过程及情况做出记录，以便被监管机构检查时有迹可循。

2. 企业内部管理数据跨境合规最佳实践

以全球某知名上市咨询公司为例，公司在全球拥有超过50万名员工，在全球超过200个城市开展业务，并且，公司后端涉及大量重要数据及个人信息，因此，大量公司内部敏感数据在全球流通，需要同时符合欧盟、中国、美国等多地区的数据合规要求。为保障企业后端数据合规，公司从以下四方面构建数据合规体系：

（1）公司总部制定了道德规范纲领性文件，将隐私保护、数据合规安全纳入其中，推动合规文化。其次，公司各职能部门在总部指导性文件的基础上，制定了符合各自实际情况的合规管理规章制度及实施流程。

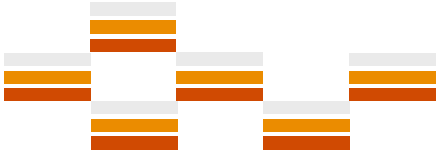
（2）公司组建专业的数据合规团队，搭建符合实际情况的数据合规组织架构，并有公司高层参与合规运作。设立数据合规委员会，进行每半年一次的通查，委员长定期向CEO汇报工作进展。委员会定期组织公司内部的组织培训和沟通，确保员工了解最新的监管要求，保证公司高层与其他层级的员工就数据安全、数据合规方面维持稳定的沟通。

（3）公司使用数字化合规工具，在隐私支持、尽职调查、风险评估等方面形成了统一的数字化数据安全合规中台，辅助形成了数据合规的自动化管理模式。

（4）公司建立数据合规的监控与防范体系。公司实施每两年为一周期的风险评估，不仅内部会自评估，还会聘请外部律师进行风险评估审查。

（5）通过数字化数据合规中台，梳理了公司内部目前数据收集和数据处理使用的现状、对现状实行了核查，再根据现状制定风险识别合规方案，将公司目前的形势与监管要求对比、进行差距分析，结合实际情况建立数据合规规则，完善数据合规制度及流程，开展相应的员工培训，并持续追踪实际情况并及时改善。

（6）公司设立数据合规评估制度，会在每一批大规模新员工入职后及每一批供应商/合作商清单大规模更新后，从多维度对数据信息安全进行综合评估，从源头掐断数据安全合规风险。



5 总结

伴随着全球化与数字经济的发展，数据安全和技术主权也逐渐成为全球基础性战略资源和社会经济发展的重要驱动力。各国在近年来纷纷通过技术创新、制度完善、监管执法，加强对数据安全和技术主权的管控，构筑维护国家安全、网络安全及数据安全的护城河。

当前，数据跨境监管力度将逐渐加深，通过审查评估认证等多种手段约束数据跨境行为，从数据存储位置、数据范围、数据内容等多个角度和多重指标要求企业加强数据跨境行为的管控。

因此，无论是对于在中国开展业务的跨国企业、还是即将或已经开始全球化的中国企业，普华永道中国与奇安信科技都建议企业建立一套专门的应对管理体系，主要包括：

制定跨境数据安全合规准则及基线

1. 基于国际与国内相关法律法规和标准规范，形成管理类、技术类、运营类等合规域，作为数据跨境合规应对的基础准则并保证执行。

2. 管理类包含建立组织架构、形成制度体系、实施人员培训及教育、加强供应链管理等。

3. 技术类包含对数据进行分类分级、权限管控、加密脱敏、数据库审计、防泄露、安全审计、备份恢复等。

4. 运营类包含数据安全事件应急处置、安全评估、风险监测等。

建立数据出境常态化风险监控体系

1. 建立分级分类标准，从数据全生命周期进行管理。

2. 根据数据出境的风险场景，建立数据安全事件应急处置机制及事件安全应急预案。

建立基于数据生命周期的安全技术体系

企业通过数据加密存储、数据权限管控、数据安全传输、匿名化和去标识化处理等方法保障出境数据的机密性。

与监管机构建立良好沟通关系

企业紧密跟进国内的立法节奏，与监管机构保持沟通，并定期对自身数据保护能力进行自查。

加强对数据接收方的审查与监督

公司对数据接收方的数据安全保障能力、管理和技术措施进行审查，并通过制定数据出境协议约定双方的数据保护义务。

实时跟进境外接收方所在国家监管要求

实时跟进境外接收方所在国家/地区的数据安全保护政策变动，并实时监督数据接收方在履行协议过程中的数据安全保障能力。

联系方式 – 普华永道

指导委员会成员

梁伟坚
普华永道中国内地及香港市场主管合伙人
普华永道中国内地及香港管理委员会成员

吴家裕
普华永道中国咨询部主管合伙人
普华永道中国内地及香港管理委员会成员

黄耀和
普华永道全球跨境服务中国主管合伙人
普华永道企业融资与并购部中国主管合伙人

傅毓敏
普华永道中国数智化中心主管合伙人

陈志坚
普华永道中国企业融资与并购部北区主管合伙人

庄树清
普华永道中国亚太区国际税务服务主管合伙人

王鹏
普华永道中国国际税务服务主管合伙人

路谷春
普华永道中国企业购并服务部国企业务主管合伙人

鲍海峰
普华永道中国企业购并服务部合伙人

蔡凌
普华永道中国企业融资与并购部中区主管合伙人

冯昊
普华永道中国管理咨询数字化和技术服务合伙人

编写委员会成员

李睿
普华永道中国网络安全和隐私服务中国内地主管合伙人

黄思维
普华永道中国网络安全和隐私服务合伙人

翁泽鸿
普华永道中国网络安全和隐私服务合伙人

李扬
普华永道中国数据洞察、云转型及数据安全合规合伙人

叶天斌
普华永道中国数字咨询合伙人

李钧
普华永道中国数字咨询合伙人

廉洁
普华永道中国并购交易服务高级经理

徐骆宁
普华永道中国风险与控制服务经理

费凡凡
普华永道中国风险与控制服务高级顾问

张丹丹
普华永道中国风险与控制服务高级律师

陆思嘉
普华永道中国风险与控制服务高级律师

孙静
普华永道中国风险与控制服务顾问

苑瀚方
普华永道中国风险与控制服务顾问

联系人

黄耀和
普华永道全球跨境服务
中国主管合伙人
gabriel.wong@cn.pwc.com

李睿
普华永道中国网络安全和隐私
服务中国内地主管合伙人
lisa.ra.li@cn.pwc.com

李扬
普华永道中国数据洞察、
云转型及数据安全合规合伙人
dennis.y.li@cn.pwc.com

联系方式 — 奇安信

指导委员会成员

陈华平
奇安信集团副总裁

刘川意
哈工大（深圳）— 奇安信数据安全研究院院长、中国密码学会常务理事

罗海龙
奇安信西部CBU总经理

刘洪亮
奇安信数据安全PBU副总经理

马兰
奇安信法律合规部负责人、总法律顾问

编写委员会成员

梁伟
奇安信安全专家

姚磊
奇安信数据安全子公司副总经理

康乐
奇安信证券军团技术总监

王伟涛
奇安信保险军团技术总监

姚翼雄
奇安信数据安全第一产品部负责人

路俊杰
奇安信数据安全第一产品部产品经理

李丹阳
奇安信战略生态合作总监

孟鑫
奇安信安全咨询顾问

王彤
奇安信安全咨询顾问

钟君毅
奇安信解决方案总监

李博
奇安信企业行业方案行销专家

联系人

陈华平
奇安信集团副总裁
chenhuaping@qianxin.com

刘洪亮
奇安信数据安全PBU副总经理
liuhongliang@qianxin.com

姚磊
奇安信数据安全子公司副总经理
yaolei@qianxin.com