数字红利与行业“暴雷”风险：如何避免？

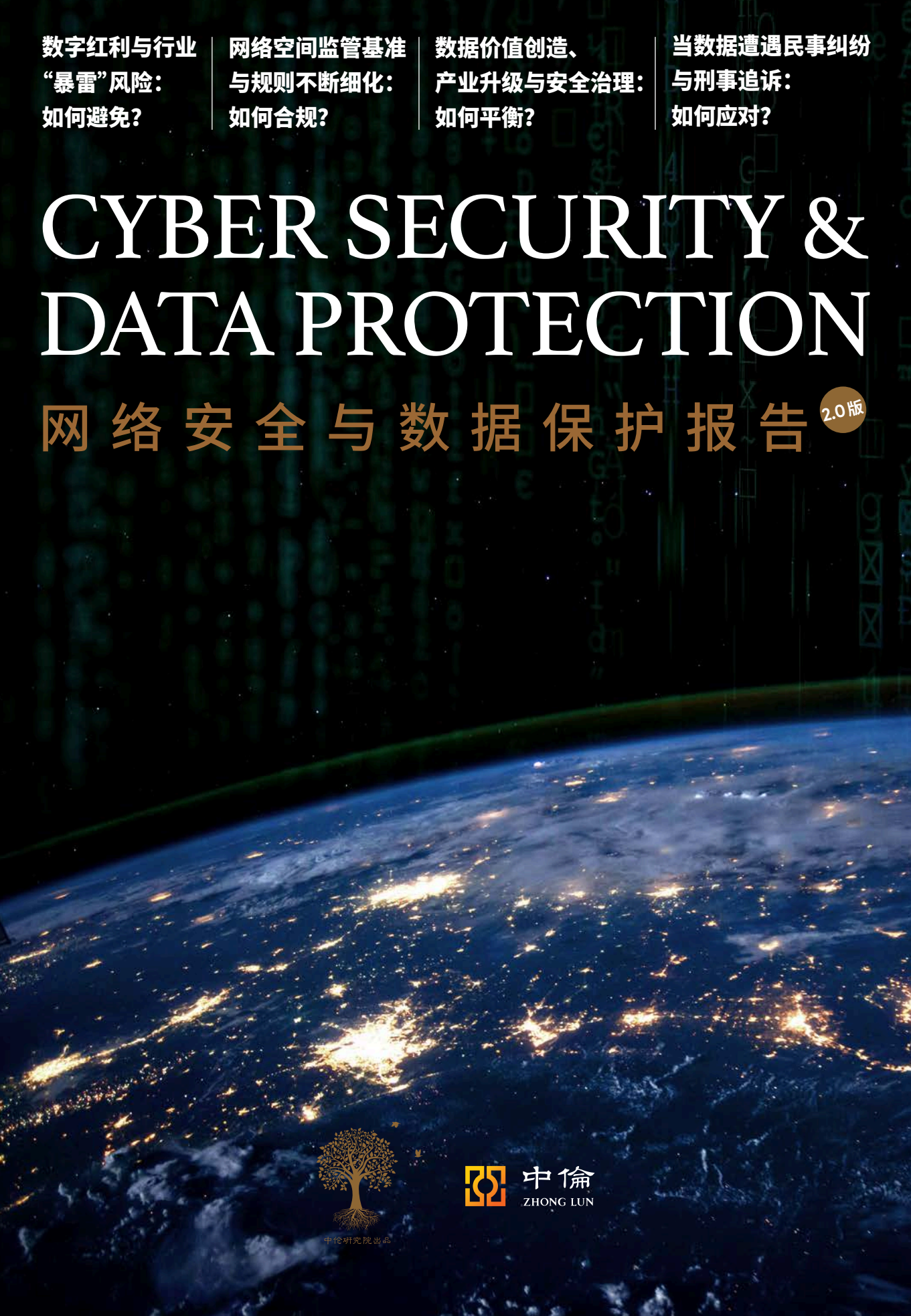
网络空间监管基准与规则不断细化：如何合规？

数据价值创造、产业升级与安全治理：如何平衡？

当数据遭遇民事纠纷与刑事追诉：如何应对？

CYBER SECURITY & DATA PROTECTION

网络安全与数据保护报告 2.0版



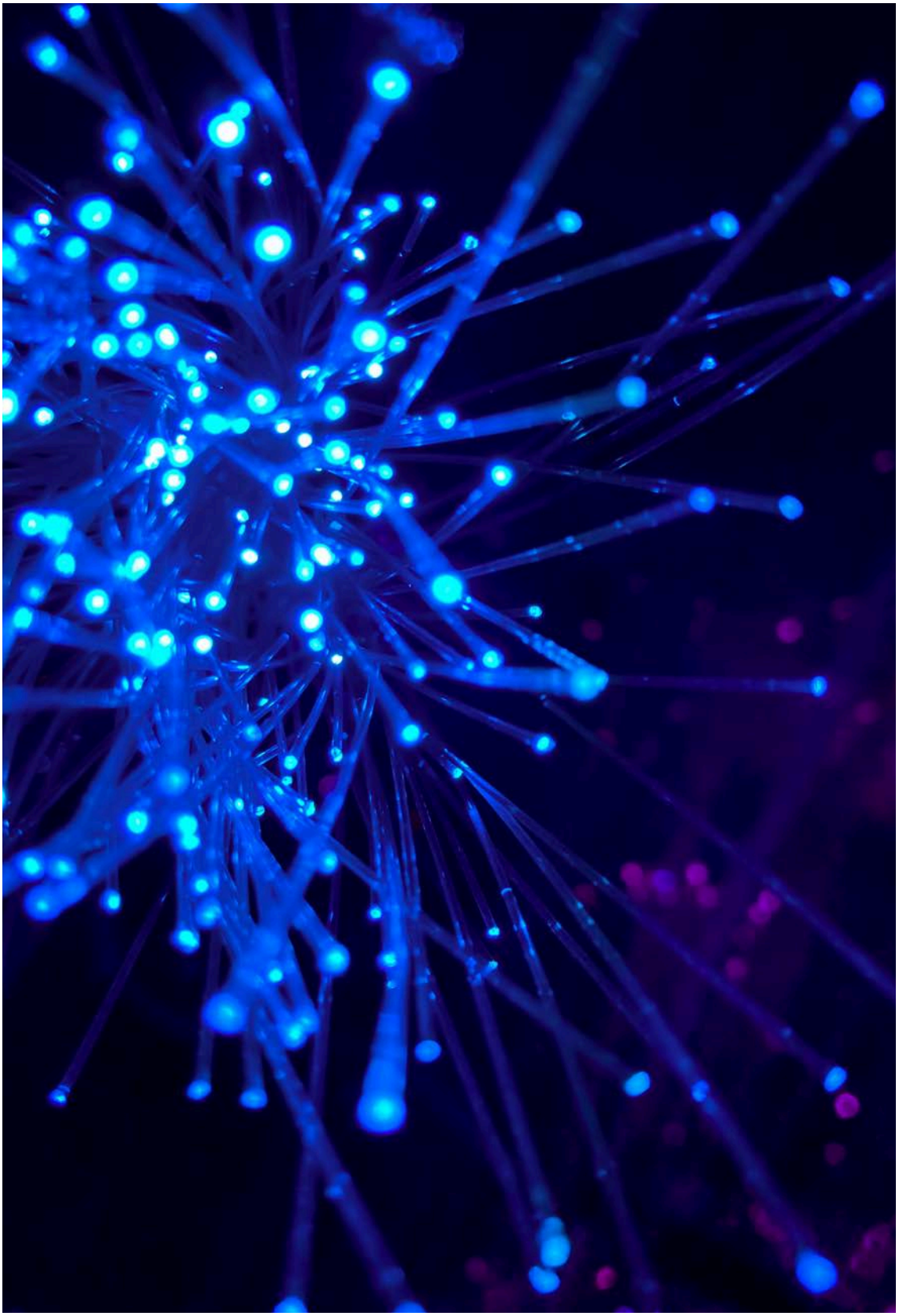
中伦研究院出品

中伦 ZHONG LUN

中伦研究院出品

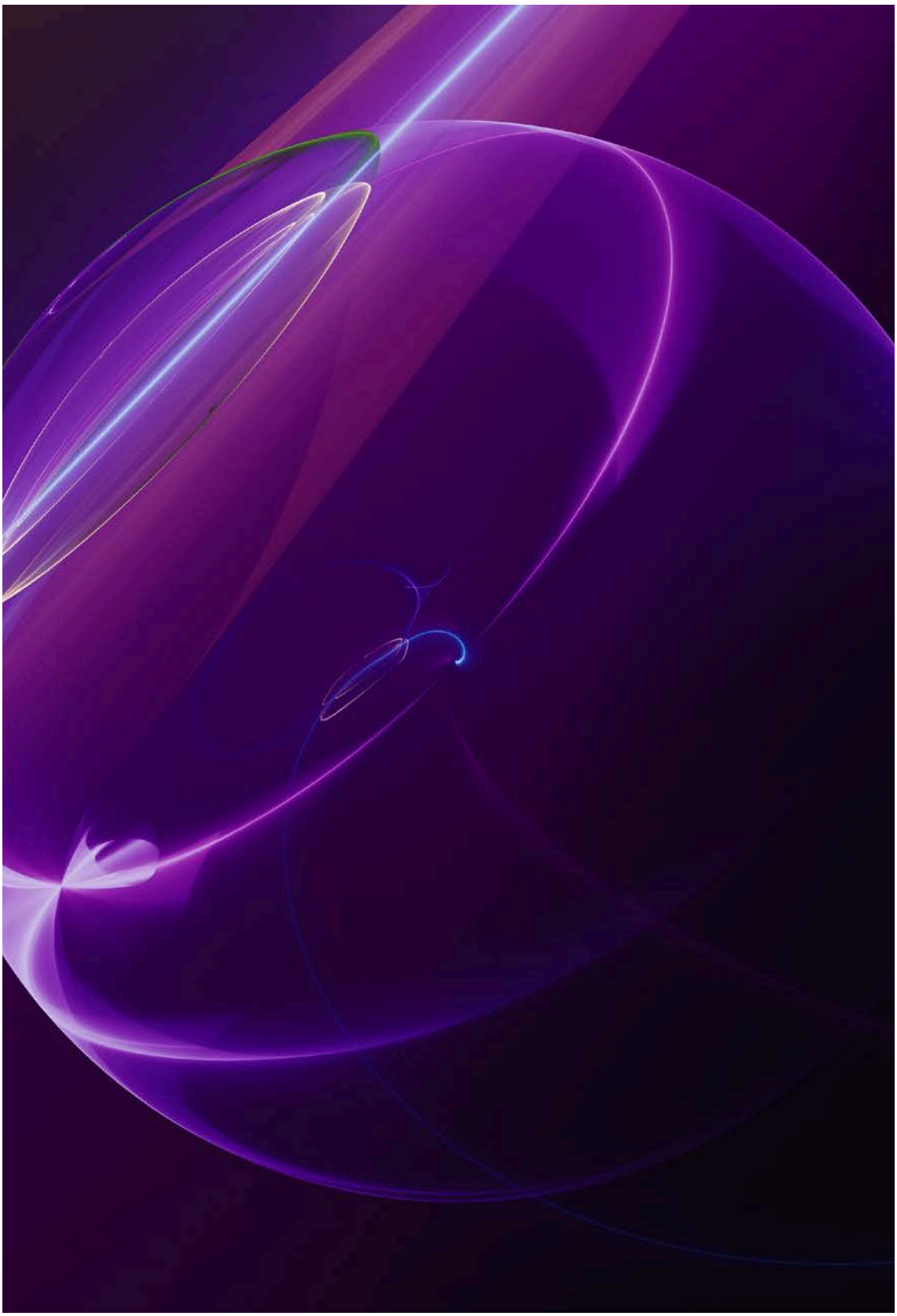

Console
Problems
Ln 11, Col 24
Spaces: 2
UTF-8
LF
JSON

CONTENTS



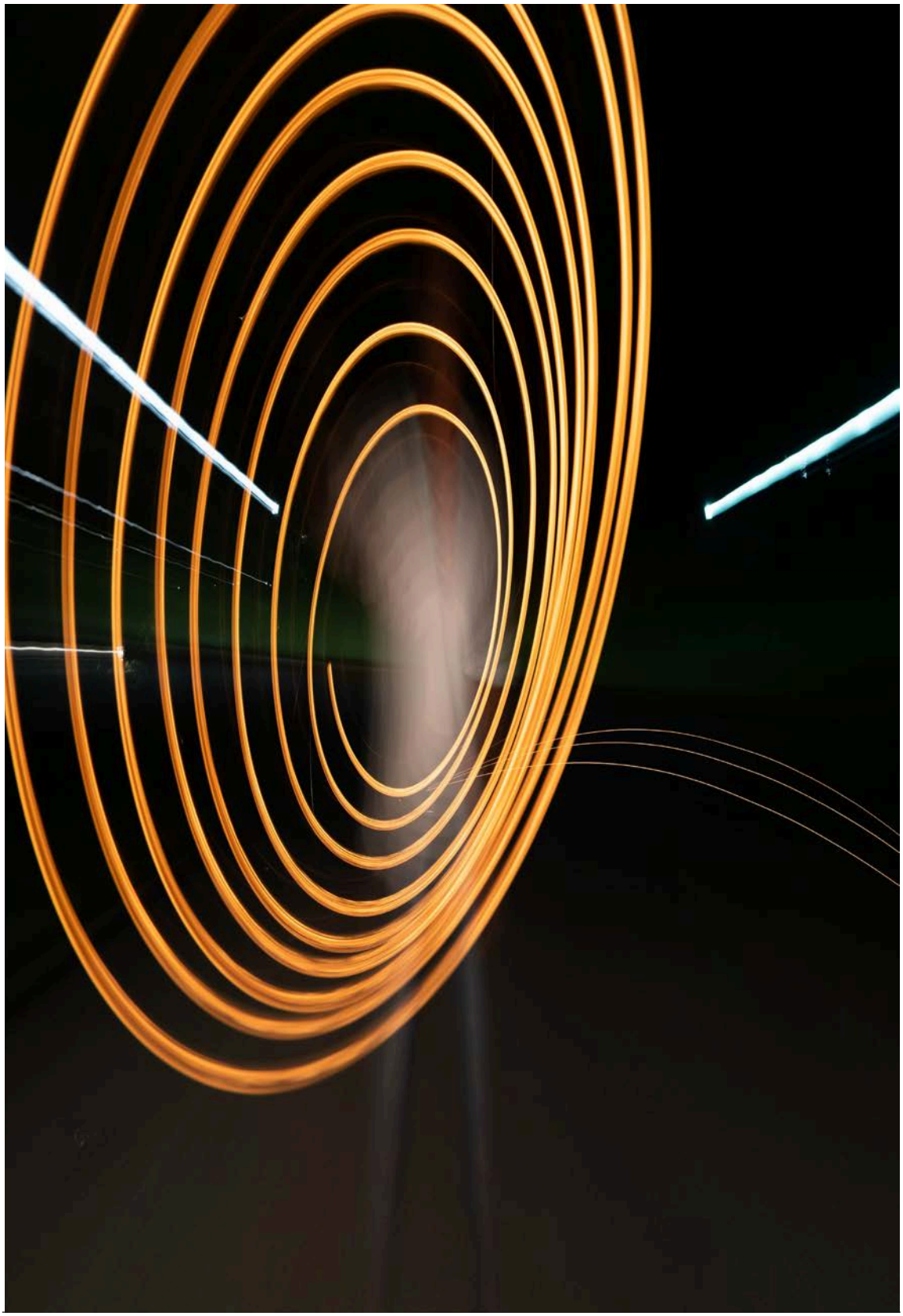
CONTENTS

<第贰部分>



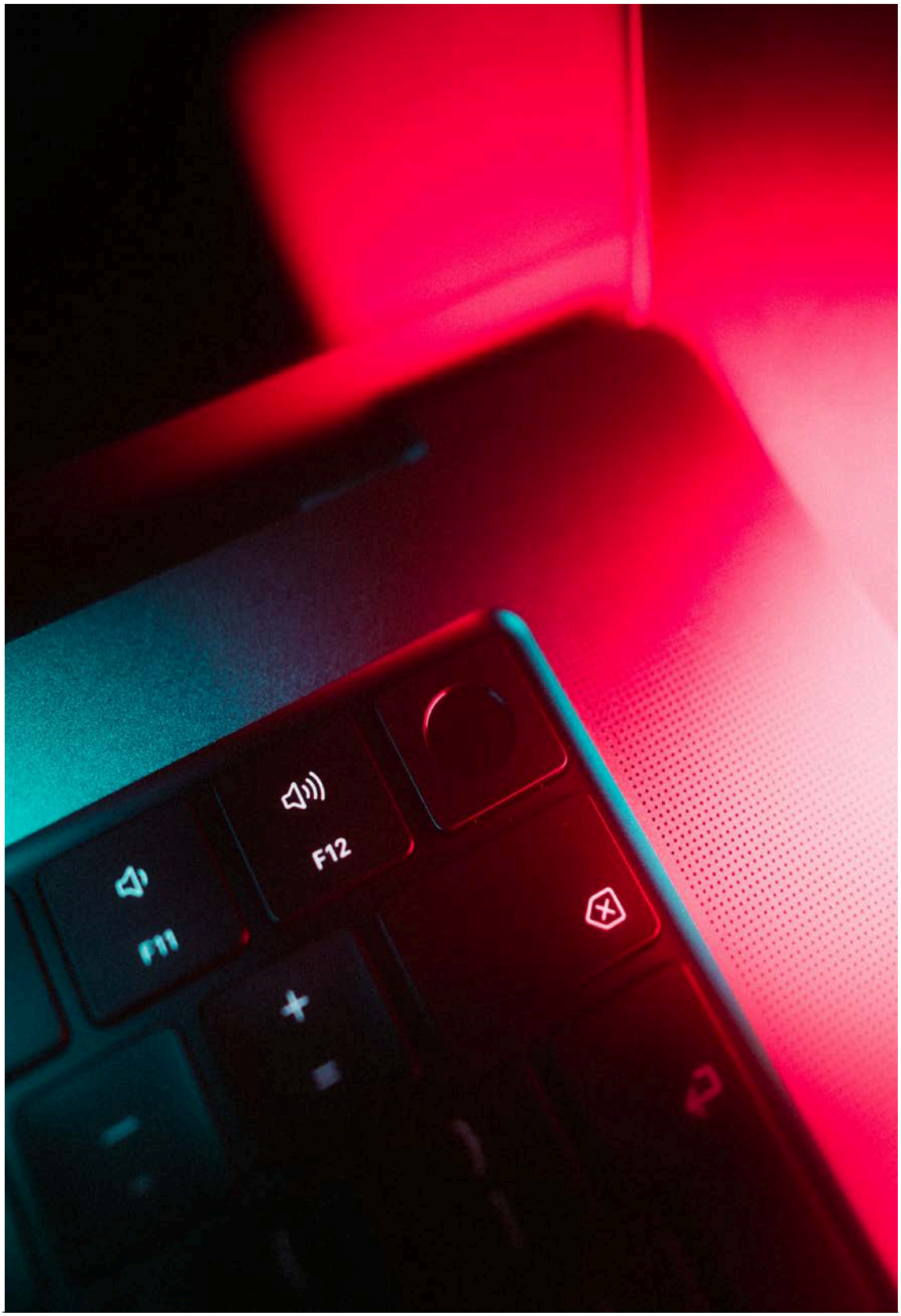
CONTENTS

<第叁部分>



CONTENTS

<第叁部分>


F12
F11

前言 PREFACE

近年来，科技创新赋能网络建设和数据利用的同时，也无可避免地成为全球网络安全与数据保护治理工作中的一大变量。

放眼全球，网络安全与数据保护已经成为世界各国共同面对且必须加以回答的命题。为此，各主要经济体在法律制定和规则设计上积极发力，欧盟《通用数据保护条例》《数字市场法》《数字服务法》、美国《数据隐私和保护法案》《加强美国网络安全法》、英国《数字经济法案》等应运而生，科技驱动下的产业创新和市场实践亦在瞬息万变的数字时代中不断检验和推动着法律制度的发展。

“加快建设网络强国、数字中国”，党的二十大报告擘画未来。借时代浪潮之力，我国从“网络大国”向“网络强国”阔步迈进，而作为上层建筑的法律规范是这一历程的守卫者和助力者。随着《个人信息保护法》于2021年11月1日正式施行，其与《网络安全法》《数据安全法》共同构成的“三驾马车”架构落地，架构之下，《数据出境安全评估办法》《网络数据安全管理条例(征求意见稿)》《个人信息出境标准合同规定(征求意见稿)》等的逐步出台使得网络安全与数据保护法律规范体系日臻完善。在愈发清晰的指引之下，各领域、各行业市场主体更有可能亦更有必要尽快认知、识别风险并寻求应对之道，确保合规落地，谋求规则之下的利益最大化。

以微观视角观察，在技术迅速迭代的背景之下，网络安全与数据保护领域内共性的企业合规问题早已呼之欲出：个人信息保护合规体系如何搭建?个人信息审计工作如何开展?“中国版标准合同”如何适用?数据出境安全评估工作如何进行?而医药、金融、通讯、智能汽车等行业也基于行

业特性提出了个性化问题。诚然，日趋完善的规则体系已为企业提供了标准化的指引，但应用场景层出不穷而监管动态时时更新，网络安全与数据保护合规已经成为一项极富科学性和系统性的工作，专业化法律服务的重要性尤为突显。

2020年，我们曾发布《中伦网络安全与数据保护年度报告》。转眼至今，在网络安全与数据保护实践迅速发展的两年里，中伦律师深度参与了该领域法律实务工作，总结相关经验，我们推出最新《中伦网络安全与数据保护报告》，关注整体趋势、实务场景、前沿动态，希冀用法律赋能企业的网络安全与数据保护合规体系构建工作。

CHAPTER 01

网络安全与数据保护领域合规趋势观察

观察 ：科技变量下全球网络安全与数据保护

在加快完善数据保护同时，全球主要经济体也在积极推进着数字经济的创新发展及网络空间立法的完善。

PART 001

科技与法治创新发展

虚拟现实、智能设备和人工智能在过去20年内革新了全球商业格局，改变了人们的生活方式。技术向前推进的过程中，立足于极大丰富且多元的数据资源以及技术上多维度、多角度、多形式的应用和衍生，得益于全球化的助力，基于数据的获取、使用及流通而开展的各类商业活动近年来在国际市场上愈发活跃。数据被称为“21世纪石油”，由此不难窥探到，数据生态产业链对全球经济、世界格局都产生了可以称其为颠覆性的影响。

在商业行为中，经营者拥有何种权利、又负有何种义务?因数据共享使用产生的红利如何分配?消费者如何保障个人数据权益?相关纠纷如何合理化解?.....这些都是科技这一变量为法治社会带来的全新课题，对法律法规的制定与更新、行政机关的监管以及司法机关的裁判提出了全新的挑战。

2022年11月7日，国务院新闻办公室发布的《携手构建网络空间命运共同体》白皮书,其中提到“安全是发展的前提，一个安全稳定繁荣的网络空间，对世界各国都具有重大意义。网络安全是全球性挑战，没有哪个国家能够置身事外、独善其身，维护网络安全是国际社会的共同责任。”[1]在加快完善数据保护同时，全球主要经济体也在积极推进着数字经济的创新发展及网络空间立法的完善，通过提出“倡议”、通过“提案”、发布白皮书等方式，展现出深化网络空间国际合作，携手各国打造安全、干净、繁荣的网络环境的美好愿景，也从立法、司法、执法等层面保障网络空间的安全，为全球市场上数据的流通与共享奠定法律基础，提供保障。

PART 002

全球范围内主要法域数据监管观察

1、欧盟

从全球范围内规制数据活动规则制定维度来看，针对个人数据保护的欧盟《通用数据保护条例》(**GDPR**)自2018年5月正式生效以来一直被誉为是世界上最全面的数

1.国务院新闻办:《携手构建网络空间命运共同体》白皮书

GDPR的法规有如下四个主要特征：监管范围广、处罚力度强、对公开性和透明度高要求、赋予个人对抗商业的权利。

据隐私保护法，其重要性不言而喻。据研究，从欧洲视角来看，2018年GDPR生效当年，欧盟监管部门仅发布了19项处罚，罚款总额不到60万欧元。而欧盟真正的执法行动实际上从2019年开始，相比2018年，2019年处罚数量增加了7倍，达到143起，2020年处罚数量又相对19年增加17%达到168起。 2021年欧洲数据保护机构开出了高达11亿欧元（12亿美元）的罚单，罚金总额增长了7倍。 根据GDPR相关规则，如果不遵守GDPR的合规要求，罚款有可能高达企业全球年度营收的4%。

自2018年GDPR的正式施行以来，欧盟的立法和执法活动都为全球范围内的数据隐私保护提供了重要参考，通过个人数据处理行为的规范来保护自然人的基本权利和自由，通过对个人数据处理的规范来保护公民的基本权利和自由，促进个人数据在欧盟境内的自由流通，是一部地地道道的以经济促进和发展为目标的法律。[2]简单归纳而言，GDPR的法规有如下四个主要特征：监管范围广、处罚力度强、对公开性和透明度高要求、赋予个人对抗商业的权利。具体而言：

（1）GDPR将“个人数据”定义为包括任何已识别或可识别的自然人（“数据主体”）相关的信息。这意味着几乎每个企业都或多或者有参与到对个人数据的处理中，例如每次发送或接受电子邮件。对于许多企业而言，GDPR影响到企业运营的方方面面，从营销到IT，从人力资源到采购。可以说，任何处理与人员信息相关的环节，都可能伴随着GDPR项下的监管。

（2）GDPR的高额罚金也是其备受瞩目的原因之一。GDPR生效不到四年，其罚款金额逐年增长：2018年仅为43.6万欧元，2019年7200万欧元，2020年1.71亿欧元，2021年上涨至惊人的10亿欧元。[3]在这一罚款名单上出现过大众所熟知的互联网巨头企业（例如某知名跨国电商企业曾被开出一张高达7亿欧元的罚单），也出现过不为大众熟知的小型数据处理主体（例如2019年8月瑞典监管部门依据GDPR对

2.赛博研究院.「观点」高富平：GDPR对我国个保法制定的借鉴意义https://www.sohu.com/a/431828682_120076174
3.数美科技.《通用数据保护条例》(GDPR)系列解读一：如何判断出海企业是否受GDPR管辖?
https://www.sohu.com/a/539884638_99990015

美国法项下目前没有一部单一的占主导地位的数据保护立法，但是在联邦立法及各州立法级别都有大量维护数据安全以及保护隐私数据的相关法案。

一家高中违规使用人脸识别技术的行为实施了罚款）。

（3）GDPR对数据处理者的数据处理活动提出了有关公开透明的高标准，有关企业需要在其公司政策以及对用户作出的通知中对数据处理活动作出广泛而详细的披露。

（4）GDPR明确而系统地建立了数据主体对于个人数据的控制权体系，提供为保障数据主体行使权利而采纳的类型化机制，从而实现GDPR第15条到22条所规定的包括知情访问、更正、删除、限制处理、可携带、反对等权利。[4]

当企业日常商业活动中涉及到跨境传输数据至欧盟无法充分裁决的国家时（例如中国、美国等），企业有义务采用GDPR项下的数据传输标准合同条款（**SCC**），用以保护欧盟数据主体的权利和自由。在2022年12月27日以前，相关企业必须将旧的SCC合同更换成新的SCC合同，这无疑是一项合规挑战。

2.美国

从立法来看，美国法项下目前没有一部单一的占主导地位的数据保护立法，但是在联邦立法及各州立法级别都有大量维护数据安全以及保护隐私数据的相关法案。联邦法层面，《联邦贸易委员会法》*FTC Act*（*15 U.S. Code § 41 et seq.*）广泛授权了美国联邦贸易委员会（**FTC**）采取执法行动来保护消费者权益，使其免受不公平或欺骗性行为的影响，并执行联邦隐私和数据保护法规。联邦贸易委员会的监管标准是“deceptive practice欺骗性准则”，该准则的适用包括公司未能遵守其公布的隐私承诺，以及未能提供足够的个人信息安全，此外还包括使用欺骗性广告或营销方法。[5]

对于关键的几个特定行业，例如金融、大健康、科技通信以及教育，美国法项下，联邦政府出台了特定法案用以规制特定行业或特定类别数据的隐私保护，比如《金融服务现代化法》（*The Gramm Leach Bliley Act*，“**GLBA**”）规定了金融机构处理个人私密信息的方式；再如《儿童在线隐私保护法》（**COPPA**）是分类化立法的典型，是针对未满13周岁的美国公民（下称“**儿童**”）这

4.陈际红：挑战与应对｜企业视角的GDPR，几个重要看点 https://www.zhonglun.com/Content/2018/06-26/1052530848.html
5.ICLG – Data Protection Laws and Regulations USA 2022

一特定人群的特别立法，主要规定了运营者的合规义务以及父母的权利；又如在大健康领域出台的《健康保险携带和责任法案》（*The Health Information Portability and Accountability Act*，“**HIPPA**”）规定了对于个人健康医疗数据的保护路径，在新冠疫情的背景下，2022年10月，该提案还提出，要强化数据主体访问自己个人健康信息的权利；增强医疗合作和个人病例管理中的信息共享；提升家庭成员和医疗服务提供者对于紧急情况和患者健康危机的参与度；在以新冠疫情为代表的公共医疗卫生事件等具有紧迫性、威胁性的情况下，增强数据披露的灵活性。在保护个人健康医疗数据隐私的前提下，减轻HIPAA适用主体的行政负担[6]。

从执法层面来看，目前为止，美国政府并未架设一家政府机关对数据活动进行统一监管，相关执法权力均下放到监管特定领域的相关部门，有些是联邦层面的执法部门，也有些是州层面的执法部门。对于违

6.丁恒、胡运思《美国HIPAA隐私规则对于个人健康医疗数据合规的启示》

最新提出的《美国数据隐私和保护法案》意图从联邦层面推动分散的隐私立法走向统一，以更好地保护公民权利。

法行为是否可能涉及到刑事责任，则需具体结合特定领域法案及个案情节来判断，比如HIPPA项下的执法行动就可能同时带来民事和刑事责任。

2022年6月3日，美国众议院和参议院发布了一项有关国家数据隐私和数据安全框架的讨论草案，意图**从联邦层面推动分散的隐私立法走向统一，以更好地保护公民权利。**[7]该提案文件里提及的法案可被称为《美国数据隐私和保护法案》（以下简称“**《美国法案》**”），也是首个获得两党两院支持的联邦隐私立法草案。目前，该法尚未正式成为联邦法律，但根据相关报道，美国参议院商业、科学和运输委员会高级成员、密西西比州共和党参议员Roger Wicker，密西西比州共和党和众议院能源和商业委员会的Frank Pallone和商业委员会主席兼高级成员Cathy McMorris Rodgers共同起草了该法案，三人表示：“两党和两院对于制定全面数据隐私框架已经筹备多年，这份讨论草案的发布是一个关键的里程碑。在未来几周，将推动建立、支持并最终确定这一标准，让公民对自身的个人数据有更多的控制权。并且欢迎并鼓励更多人加入，使个人隐私得到有意义的保护，并为企业提供运营的确定性。”

3. 其他主要法域

根据全球知名科技行业咨询公司Gartner的数据统计，到2023年，世界上65%人口的个人数据都将受到现代隐私法规的保护。站在全球视角，在过去的两年里，欧洲、美洲、亚太等地区都出台或修改了数据隐私保护的相关法律，这一趋势在未来也将继续延续。

英国是全球首个系统性制定数字经济促进法的国家，旨在提升其全球数字经济领导地位。2017年4月，英国颁布替代2009年旧法的全新《数字经济法案》，成为全球首部系统完整的数字经济促进法，旨在平衡技术创新与风险应对、网络开放与安全保障、数据挖掘与隐私保护、数据垄断与有序竞争，构建一个运用技术持续推动经济、社会及政府转型与变革的良性法律环境。[8]

2021年10月12日，韩国科学和信息通

7.闫晓丽：《美国数据隐私和保护法案》的内容及启示
8.王磊：《欧美数字经济立法最新动态、基本特征及对我国启示》

科技发展滋养了新的商业模式和商业形态，
新的问题也随之而来。

信技术部（**MSIT**）宣布，国务会议通过了《数据产业振兴和利用促进基本法》（以下简称“**《数据基本法》**”），旨在为发展数据产业和振兴数据经济奠定基础，并已于2022年4月全面实施。《数据基本法》是全球首部规制数据产业的基本立法，对数据的开发利用进行统筹安排。[9]

与中国相似，在日本，《个人信息保护法》是日本个人信息保护领域的基本法，基于针对个人信息保护相关国际行动、信息通信技术发展、利用个人信息的新产业和新发展进行的调查分析，日本个人信息保护委员会每三年对该法进行一次审查，以积极回应数据保护的发展需求。相较于此前版本，2020年6月修订的《个人信息保护法》对运营商的信息处理义务和法律责任进行细化，同时，向个人信息的跨境流动投入了更多的关注。

2020年11月，新加坡个人数据保护委员会在2012年《个人数据保护法》的基础上发布了《个人数据保护（修订）法》，强化了对公民个人数据权利的私权保护和合规义务。2018年2月，新加坡议会通过《2018年网络安全法》，作为网络安全领域的综合性立法，该法弥补了原有的《计算机滥用及网络安全法》在行政执法和事前事中监管方面的缺失，可操作性亦有所提升。

可见，随着网络安全风险与数据价值二者的同步增长，如何在法律的适用中实现保护与发展的平衡，已成为各国共同面对的时代命题。

PART 003

规则与创新，风险与合规
——科技变量下的法律问题聚焦

科技发展滋养了新的商业模式和商业形态，新的问题也随之而来。

技术进步与改变无法被预见，从宏观上看，大多数规制数据活动的法律在制定之初，立法者们往往都会考虑留下一定灵活性，以应对瞬息万变的商业社会。从国务院最新于11月14日发布的《关于数字经济发展情况的报告》来看，为了推动数字法治的健康发展我国采用立法、安全与治理“三

9.信通院互联网法律研究中心：韩国率先发布全球首部《数据基本法》，大力发展数据产业

微观视角下，复杂的法律规定及动态变化的监管环境为企业合规带来了不小的困难。

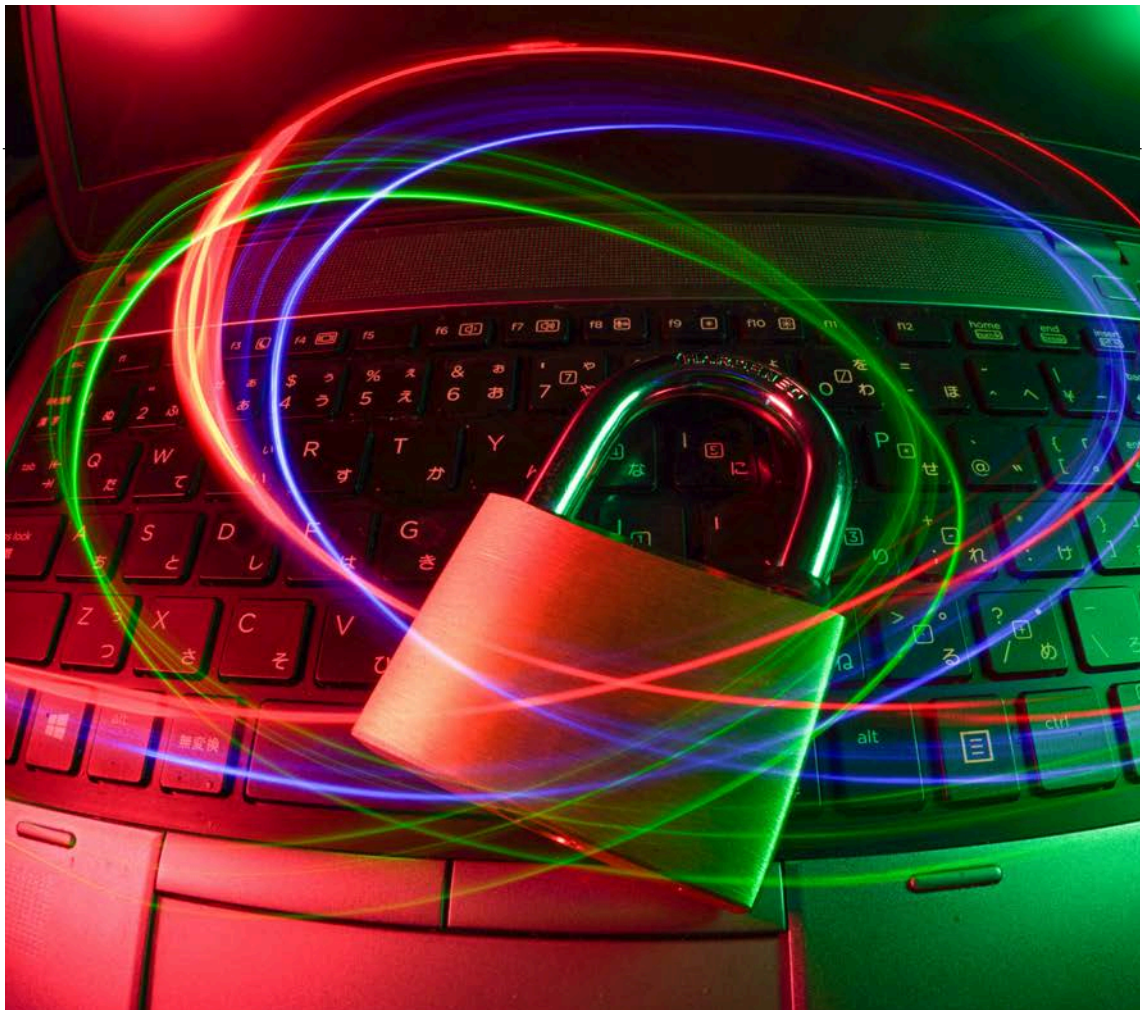
管齐下”的路径：**(1)法律和政策体制体系逐步健全。**相继颁布实施《网络安全法》《数据安全法》《个人信息保护法》初步搭建起网络空间治理体系的“三驾马车”，修改《电子商务法》《反垄断法》，制定新就业形态劳动者权益保障政策，逐步健全完善行业层面的治理框架。**(2)网络安全防护能力持续增强。**完善关键信息基础设施安全保护、数据安全保护和网络安全审查等制度，健全国家网络安全标准体系，完善数据安全和个人信息保护认证体系，确保国家网络安全、数据和个人隐私安全。基本建成国家、省、企业三级联动的工业互联网安全技术监测服务体系；建立数字经济部际联席会议等跨部门协调机制，强化部门间协同监管。**(3)数字经济治理能力持续提升。**提升税收征管、银行保险业监管、通关监管、国资监管、数字经济监测和知识产权保护、反垄断、反不正当竞争、网络交易监管等领域的信息化水平，推动“智慧监管”。有序推进金融科技创新监管工具试点、资本市场金融科技创新试点、网络市场监管与服务示范区等工作，探索新型监管机制。[10]

微观视角下，复杂的法律规定及动态变化的监管环境为企业合规带来了不小的困难。共性问题例如企业如何搭建个人信息保护合规体系?如何开展个人信息审计工作?中国版标准合同如何适用?跨国公司员工个人数据如何管理?数据出境安全评估新规出台，企业如何抓重点?处理方和接收方的权利义务如何划分?随着司法力量的介入以及跨境合作的愈发频繁，涉数据的民事、行政和刑事案件数量都在不断增加，跨国企业也可能面临外国司法调查，此时企业该如何应对?在共性问题的基础上，不同商业模式和行业特点也会碰撞出个性化的合规需求。例如在大健康行业对个人信息的特殊合规要求之下，临床试验数据如何出境?自动驾驶领域的个人信息保护合规问题，科技企业上市的数据合规问题等。

网络安全与数据保护这个语境下，所涉及行业包括金融、IT与互联网、电信、移动支付、智能网联汽车、大数据、生命科学与大健康、传媒、能源、航空、化工和制造等多个领域，在科技变量的影响下，未来已

10.国务院关于数字经济发展情况的报告_中国人大网（npc.gov-.cn）

至，市场将会对企业的变通能力，立法者的思路与布局，乃至国家的现代化治理能力都提出越来越高的要求；我们将会持续关注，以法律实践助力企业发展，赋能未来。



中国网络安全、数据安全和个人信息保护法概览

斯响俊 蔡荣伟

近年来，中国政府加强了对网络安全、数据安全和个人信息保护的监管。本文梳理了中国目前基于“三大基本法”而初步构建的网络安全、数据安全和个人信息保护监管体系。

近年来，中国政府加强了对网络安全、数据安全和个人信息保护的监管。自2016年以来，有三部重要的法律（以下简称“**三大基本法**”），即：(i)《中华人民共和国网络安全法》（“**《网安法》**”），(ii)《中华人民共和国数据安全法》（“**《数安法》**”）和 (iii)《中华人民共和国个人信息保护法》（“**《个保法》**”）相继颁布，使相关领域的法律监管有据可循。

一些监管部门，例如国家互联网信息办公室（“**国家网信办**”），已经出台了系列法规及规范性文件来贯彻落实“三大基本法”。此外，其他政府监管部门和相关机构，如全国信息安全标准化技术委员会，也发布了许多国家标准以提供更详细的合规指引。与此同时，更多的实施细则和国家标准也在筹备中。

本文梳理了中国目前基于“三大基本法”而初步构建的网络安全、数据安全和个人信息保护监管体系。

PART 001

网络安全

A.《网安法》的适用范围与适用对象

根据《网安法》，在中华人民共和国境内建设、运营、维护和使用网络，以及网络安全的监督管理，都将适用网安法。即使运营者仅为了内部管理目的而建设、运营内部网络，也会被认定为属于受到《网安法》规制的“网络运营者”。

B.网络安全等级保护制度（“等保”）

根据《网安法》，所有网络运营者都需要按照等保制度的要求，履行安全保护义务，包括等保定级和评估。

1.等保定级

等保制度包含五个级别。级别越高，相应的保护措施要求就越严格。

a.等保定级的考量要素

在等保定级时，需考虑以下因素

(1)网络在国家安全、经济建设、社会生活中的重要程度；以及

(2)一旦网络系统遭到破坏后，对国家安全、社会秩序、公共利益以及相关公民、

关键信息基础设施运营者需要根据适用的法律和法规实施特别保护措施，以保护其关键信息基础设施。

法人和其他组织的合法权益的危害程度。

b.等保定级的流程

(1)网络运营者应当自行确定网络的安全保护等级。

(2)一级网络系统的运营者不需要将定级结果提交公安部门审核。

(3)对拟定为第二级以上的网络，其运营者应当(i)组织专家评审定级合理性；(ii)在评审后报请主管部门核准（如有）；(iii)将结果报公安部门核准。如果核准不通过，需要重新认定。

2.等保评估

a.等保评估的目的在于检验网络运营者的保护措施是否能够满足相应级别的保护要求。

b.等保评估的程序

(1)网络运营者应该聘请由政府部门授权的测评机构进行检测评估，并出具评估报告。

(2)二级或更高级别的网络系统运营者需要向相应的公安机关备案，并提交评估报告，如果该报告被核准，主管部门将颁发备案证书。

C.关键信息基础设施的安全保护

1.关键信息基础设施和关键信息基础设施运营者的定义

关键信息基础设施是指与国家安全和公共利益相关的、重点行业的重要网络设施和信息系统。

关键信息基础设施运营者是经营关键信息基础设施的实体。关键信息基础设施运营者需要根据适用的法律和法规实施特别保护措施，以保护其关键信息基础设施。

2.关键信息基础设施的认定

根据《关键信息基础设施安全保护条例》的要求，重点行业主管部门需结合本行业实际，制定本行业的关键信息基础设施认定规则。

典型的重点行业包括公共通信服务、信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等。

在实践中，被认定为关键信息基础设施运营者的实体可能会收到主管部门的通知。一旦被确定为关键信息基础设施运营者，该实体需根据相关法律法规实施更严格的安全保护措施。

《数安法》设置了数据分类分级保护制度，要求相关部门根据数据的重要程度以及发生泄漏或遭滥用后所造成的损害程度对其进行分级分类。

PART 002

数据安全

A.《数安法》的适用范围与适用对象

在中华人民共和国境内开展数据处理活动及其安全监管，适用《数安法》。

如果在中国境外进行的数据处理活动危及 (i) 中国的国家安全；(ii) 中国的公共利益，或 (iii) 中国公民、组织的合法权益，也将适用《数安法》。

根据《数安法》，“数据”不仅包括电子数据，还包括以非电子形式记录或存储的数据（如纸质文件中记录的数据）。

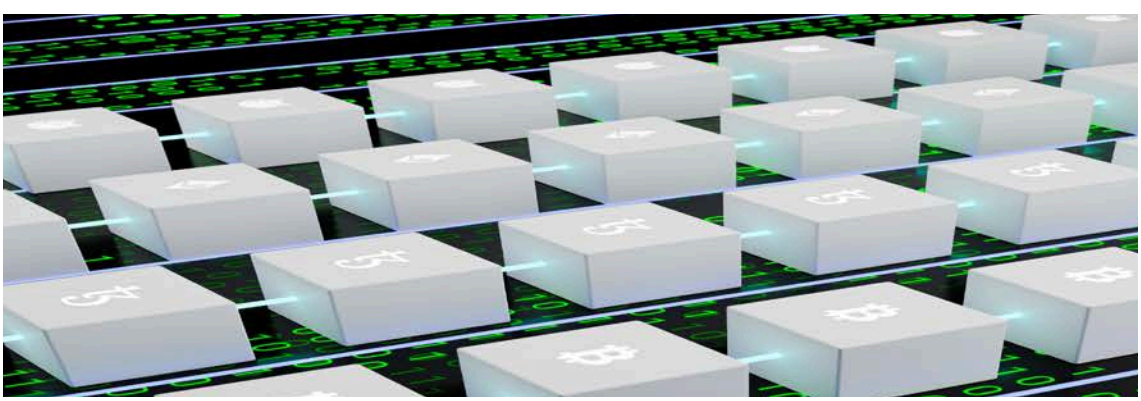
B.数据分类分级保护制度

数据分类分级保护制度要求相关部门根据数据的重要程度以及发生泄漏或遭滥用后所造成的损害程度对其进行分级分类。

1.在工业制造、金融、电信等行业，相关行业主管部门已经发布了具有行业针对性的数据分类和分级指南。

2.2021年11月，国家网信办发布了《网络数据安全管理条例（征求意见稿）》（“**《管理条例》**”），向公众征求意见。《管理条例》将数据分为三类，即 (i) 一般数据，(ii) 重要数据，以及 (iii) 核心数据。然而，《管理条例》并没有提供这三类数据的详细目录。

3.在2021年12月，《网络安全标准实践指南-网络数据分类分级指引》（“**《数据分类分级指引》**”）发布。《数据分类分级指引》将数据分为三个类别和四个等级。



《数据分类分级指引》将数据分为一般数据、重要数据、核心数据三个类别和1级数据、2级数据、3级数据、4级数据四个等级。

类别	一般数据	
	重要数据	
	核心数据	
级别	1级数据	数据一旦遭到篡改、破坏、泄露或者非法获取、非法利用，不会对个人合法权益、组织合法权益造成危害。
	2级数据	数据一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能对个人合法权益、组织合法权益造成轻微危害。
	3级数据	数据一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能对个人合法权益、组织合法权益造成一般危害。
	4级数据	数据一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能对个人合法权益、组织合法权益造成严重危害，但不会危害国家安全或公共利益。

4.《管理条例》与《数据分类分级指引》的内容存在不一致之处。截至本文发布之日，《管理条例》仍是一个征求意见稿，尚未正式生效。《数据分类分级指引》业已生效，然而它是一个推荐性标准，并不具备法律强制力。因此，对于数据分类和分级规则的最终方案，我们尚无法得知。

C.对重要数据的保护

1.重要数据目录的制定

《数安法》要求中央政府在数据分类分级制度的基础上制定重要数据目录，而各地区、各部门应当按照数据分类分级保护制度，确定本地区、本部门以及相关行业、领域的重要数据具体目录，对列入目录的

《管理条例》和《信息安全技术重要数据识别指南（征求意见稿）》都为识别重要数据提供了指导规则。

数据进行重点保护。

2.重要数据的识别

《管理条例》和《信息安全技术重要数据识别指南（征求意见稿）》（"**《重要数据识别指南》**"）都为识别重要数据提供了指导规则。其中，《重要数据识别指南》是全国信息安全标准化技术委员会发布的非强制性的国家标准。

重要数据是指一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能危害国家安全、公共利益的数据。

《管理条例》和《重要数据识别指南》中的识别规则大致相同。然而，《重要数据识别指南》明确将个人信息排除在重要数据的范围之外，但《管理条例》则要求处理一百万人以上个人信息的处理者需采取与重要数据处理者相同的安全措施。

3.重要数据处理者的义务

重要数据的处理者需要（i）明确数据安全负责人；（ii）明确数据安全管理机构；（iii）对其数据处理活动定期开展风险评估以及（iv）向有关主管部门报送风险评估报告。

根据《网络安全法》的要求，关键信息基础设施运营者原则上应将重要数据存储在中国。如果需要将重要数据转移到境外，则需要（i）通过国家网信办组织的安全评估；（ii）自行或者委托网络安全服务机构对其网络的安全性和可能存在的风险每年至少进行一次检测评估，并（iii）将检测评估情况和改进措施报送相关负责关键信息基础设施安全保护工作的主管部门。

2022年7月7日，国家网信办发布了《数据出境安全评估办法》（"**《安全评估办法》**"）。《安全评估办法》要求除关键信息基础设施运营者之外的其他数据处理者在向境外传输重要数据前也应当向国家网信办申请进行安全评估。

D.向境外司法机构或执法机构提供数据

如处理者需要将数据传输至境外司法或执法机构，其必须事先获得来自主管部门的批准。但是，截至本文发布之日，相关批准程序和"主管部门"的具体指代仍然不明。此外，关于"外国司法或者执法机构"的定义也尚未得到明确。

《个保法》明确了个人信息处理的合法依据。

PART 003

个人信息保护

A.什么是个人信息?

根据《个保法》,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。

B.《个保法》的适用范围与效力

1.《个保法》适用于在中国进行的所有个人信息处理活动。

2.《个保法》也有域外适用效力。在中国境外处理中国境内自然人个人信息的活动,有下列情形之一的,也适用本法:

a.以向境内自然人提供产品或者服务为目的;

b.分析、评估境内自然人的行为;或

c.法律、行政法规规定的其他情形。

3.境外的个人信息处理者,应当在中国境内设立专门机构或者指定代表,负责处理个人信息保护相关事务,并将有关机构的名称或者代表的姓名、联系方式报送履行个人信息保护职责的部门。该点的详细实施细则还有待立法者进一步明确。

C.个人信息处理的合法性依据

1.根据《个保法》,个人信息处理者可以根据以下依据之一来处理个人信息。

a.取得个人的同意;

b.为订立、履行个人作为一方当事人的合同所必需,或者按照依法制定的劳动规章制度和依法签订的集体合同实施人力资源管理所必需;

c.为履行法定职责或者法定义务所必需;

d.为应对突发公共卫生事件,或者紧急情况下为保护自然人的生命健康和财产安全所必需;

e.为公共利益实施新闻报道、舆论监督等行为,在合理的范围内处理个人信息;

f.依照《个保法》规定在合理的范围内处理个人自行公开或者其他已经合法公开的个人信息;或

g.法律和法规规定的其他情况。

2.值得注意的是,如果是基于个人的同意而进行处理的,在对同意的有效性产生争议时,个人信息处理者应承担举证责任。

处理个人信息应遵循最小必要原则和公开透明原则；在法定情形下，个人信息处理者应当主动删除个人信息。

D.处理个人信息的原则

1.最小必要原则

个人信息的收集和处理范围应控制在实现处理目的所必需的最小范围。处理行为对个人合法权益的影响也应被控制在最小范围内。

2.公开透明原则

个人信息处理者应向个人明确披露：(i) 收集个人信息的范围，(ii) 处理活动的规则和目的，(iii) 处理者的名称和联系方式，以及 (iv) 个人行使《个保法》项下权利的行权方式。

E.个人信息的删除

1.有下列情形之一的，个人信息处理者应当主动删除个人信息。个人信息处理者未删除的，个人有权请求删除。

a.处理目的已实现、无法实现或者为实现处理目的不再必要；

b.个人信息处理者停止提供产品或者服务，或者保存期限已届满；

c.个人撤回同意；

d.个人信息处理者违反法律、行政法规或者违反约定处理个人信息；

e.个人行使其权利要求个人信息被删除。

2.如果法律和法规要求长期存储个人信息，处理者应采取相应措施，确保这些个人信息不会被用于存储以外的任何目的。

F.个人信息的跨境传输

1.跨境传输的要求

a.处理者应告知个人 (i) 接收方的名称或者姓名和联系方式；(ii) 接收方的处理方法和目的；(iii) 将要传输的个人信息的类型，以及 (iv) 个人向接收方行使权利的方式。除此之外，处理者应当依照《个保法》规定取得个人的单独同意。

b.处理者需要对该等跨境传输进行个人信息保护影响评估。

c.如果处理者是关键信息基础设施运营者，它应该事先通过国家网信办组织的安全评估。

d.如果处理者不是关键信息基础设施运营者，根据其需要转移的个人信息的数量和性质，有可能需要通过国家网信办的安全评估。具体来说，根据《安全评估办法》的规定，如果处理者并非关键信息基础设

《安全评估办法》《安全认证规范》《标准合同规定》为个人信息跨境传输提供指引；个人在个人信息处理活动中享有查阅、复制、可携权等权利。

施运营者，且(i)处理一百万人以上的个人信息或(ii)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的，应当在向境外传输个人信息前向国家网信办申请进行安全评估。

e.如果处理者不是关键信息基础设施运营者，且无需接受国家网信办的安全评估，则应满足以下要求之一：(i)获得专业机构颁发的个人信息保护认证；(ii)按照国家网信办的标准合同模板与接收方签订标准的数据保护合同；或(iii) 满足法律、行政法规或者国家网信部门规定的其他要求。

2.2022年6月24日，全国信息安全标准化技术委员会发布了《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》(“**《安全认证规范》**”)。该文件为如何针对个人信息跨境传输进行个人信息安全认证提供了指引。但《安全认证规范》仅为推荐性的指南文件，并不具有强制力。

3.2022年6月30日，国家网信办发布了《个人信息出境标准合同规定(征求意见稿)》(“**《标准合同规定》**”)以及标准合同模板。但是，《标准合同规定》以及标准合同模板目前均为征求意见稿，尚未正式实施。

G.个人的权利

个人在个人信息处理活动中享有以下权利。

1.查阅和复制的权利。个人有权向个人信息处理者查阅、复制其个人信息。

2.可携权。个人请求将个人信息转移至其指定的个人信息处理者，符合国家网信办规定条件的，个人信息处理者应当提供转移的途径。

3.更正和补充的权利。个人发现其个人信息不准确或者不完整的，有权请求个人信息处理者更正、补充。

4.请求删除的权利。如果满足法律规定的条件，个人有权要求处理者删除其个人信息。

5.撤回同意的权利。基于个人同意处理个人信息的，个人有权撤回其同意。个人信息处理者应当提供便捷的撤回同意的方式。

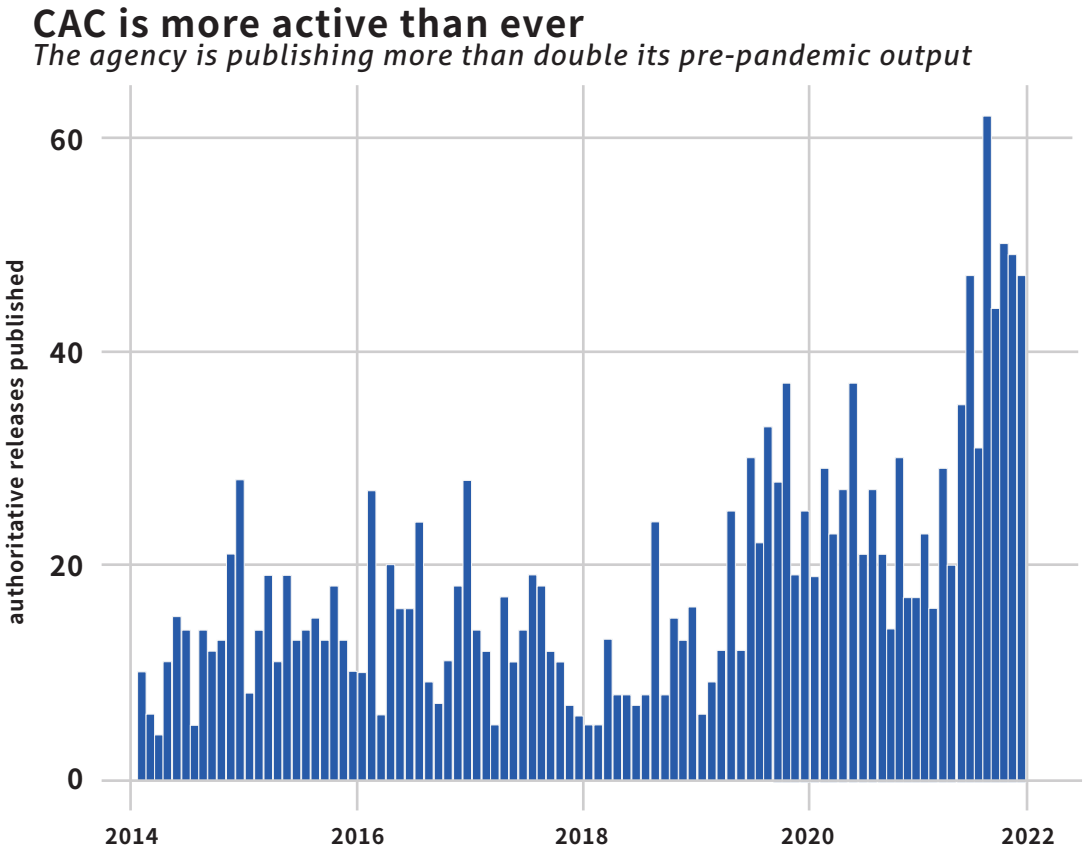
6.要求解释的权利。个人有权要求个人信息处理者对其个人信息处理规则进行解释说明。

中国的网络安全、数据安全和个人信息保护的监管体系仍处于高速发展的过程中，众多问题仍亟待解决。

PART 004

我们的展望

中国的网络安全、数据安全和个人信息保护的监管体系仍处于高速发展的过程中，众多问题仍亟待解决。据美国科技媒体Protocol报道，在过去的几个月里，国家网信办平均每个月发出40份官方通知。[1]



《国家网信办比以往任何时候都要活跃——该部门这两年来发布的文件数量是疫情前的两倍以上》

1.Lu S. et al. (2022, February 9). Loud and Clear: CAC' s Growing Public Voice. Protocol. https://www.protocol.com/newsletters/protocol-china/china-beijing-olympics-opening-ceremony?rebelltitem=1#rebelltitem1

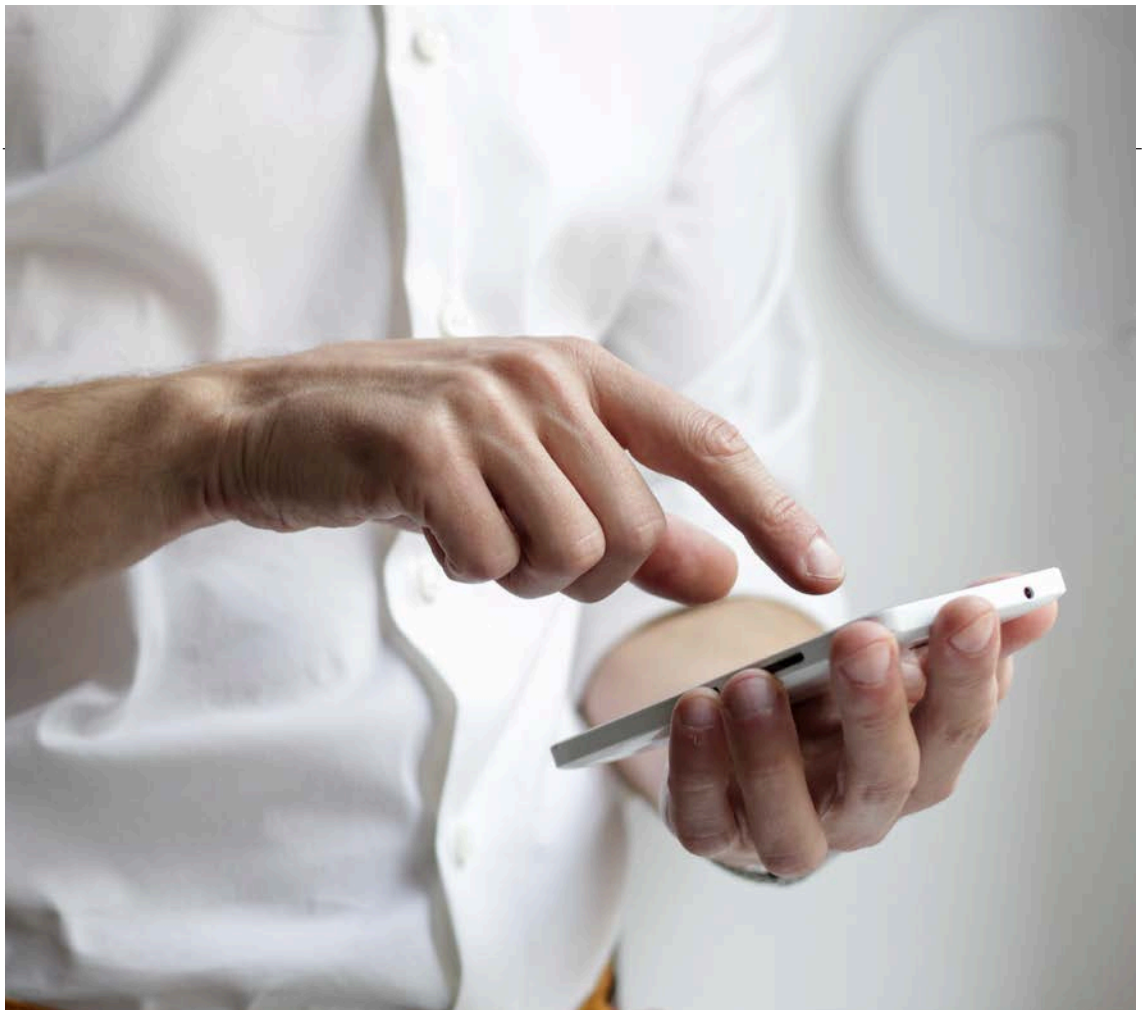
网络运营者和数据处理者应密切关注国内立法动态，必要时向专业人士寻求法律意见。

在2022年及今后的一段时期，预计将会有更多的专项法规、国家标准和规范性文件陆续出台。为了能够充分准备，以应对不确定性带来的诸多挑战，网络运营者和数据处理者应密切关注国内立法动态，必要时向专业人士寻求法律意见。

（曹泽坤对本文亦有贡献）

斯响俊
合伙人
公司业务部
上海办公室
+86 21 6061 3771
jaysi@zhonglun.com

蔡荣伟
合伙人
公 司业务部
上海办公室
+86 21 6061 3175
roncai@zhonglun.com



超大型互联网平台合规之路：中欧监管趋势异同

侯彰慧 许聿宁 李梦涵

本文尝试以尽可能简洁的方式，通过制度对比，梳理并总结DMA和《分类分级指南》《主体责任指南》提出的合规要求，以期帮助企业更好理解中欧对超大型平台的监管思路，提高企业的合规水平。

2022年7月18日，欧盟理事会最终批准了《数字市场法案》(Digital Markets Act，**DMA**)，旨在规范大型网络平台的竞争行为，维持核心平台服务市场的可竞争性和公平性。DMA的出台突破了传统竞争法的监管思路，只要互联网平台符合DMA的适用条件而被认定为守门人(Gatekeeper)，DMA就可以对其特定行为进行规制，而无需就“相关市场”“支配地位”“竞争影响”等问题展开分析论证。

无独有偶，中国市场监督管理总局曾于2021年10月29日发布《互联网平台分类分级指南(征求意见稿)》(“**《分类分级指南》**”)和《互联网平台落实主体责任指南(征求意见稿)》(“**《主体责任指南》**”)，拟对互联网平台进行分类分级，并对符合标准的超大型互联网平台(“超大型平台”)进行行为规制。《分类分级指南》和《主体责任指南》两部征求意见稿与DMA的监管思路存在诸多近似之处，在公平竞争、平等治理、开放生态、平台内部治理、经营者集中申报等方面均有所突破。

本文尝试以尽可能简洁的方式，通过制度对比，梳理并总结DMA和《分类分级指南》《主体责任指南》提出的合规要求，以期帮助企业更好理解中欧对超大型平台的监管思路，提高企业的合规水平。

PART 001

守门人的认定思路

DMA第2条和第3条规定，提供核心平台服务的经营者，若(a)同时满足欧盟营业额门槛和核心平台用户规模门槛，或(b)虽不满足相关门槛但根据其它考量因素可以认定符合相关标准，其可能被认定为守门人，受到DMA的监管。

(一)核心平台服务

DMA列出了10类核心平台服务，除“网络浏览器”“虚拟助理”“在线广告服务”3类外，其他核心平台服务均在《分类分级指南》中有所体现。通过对比可以发现，DMA对核心平台服务的分类更侧重于其功能，而《分类分级指南》对平台服务类型的分类更侧重于其内容。

DMA对核心平台服务的分类更侧重于其功能，而《分类分级指南》对平台服务类型的分类更侧重于其内容。

	《数字市场法案》	《分类分级指南》
1	**“在线中介服务（online intermediation services）”**指满足下列各项条件的服务： （1）属于应服务接受者要求，以电子方式提供的有偿远程服务； （2）允许商业用户向消费者提供商品或服务，促进商业用户和消费者之间的直接交易； （3）在与商业用户的合同关系基础上，向为消费者提供商品或服务的商业用户提供服务。	**网络销售类平台，包括但不限于：** （1）综合商品交易类：专门或者主要从事提供衣帽鞋靴、箱包饰品、数码电器、食品洗护等各类商品的综合平台。 （2）垂直商品交易类：专门或者主要从事某一类型产品交易的平台，具有精准的差异化定位和独特的品牌附加值。 （3）商超团购类：专门或者主要从事供给蔬菜水果、肉蛋水产、粮油调味、酒水饮料、日用百货等生活用品，并提供团购等配送服务的平台。 **生活服务类平台，包括但不限于：** （1）出行服务类：专门或者主要从事提供出行相关服务的平台，如共享单车、打车软件、公交地铁查询软件等。 （2）旅游服务类：专门或者主要从事招徕、接待游客、为其提供交通、游览、住宿、餐饮、购物、文娱等服务的平台，如旅游定制、门票购买、酒店预订等。 （3）配送服务类：专门或者主要从事外卖、物流等服务的平台，如外卖送餐、同城配送、快递配送等。 （4）家政服务类：专门或者主要从事保姆、护理、保洁、家庭管理等家政服务的平台。 （5）房屋经纪类：专门或者主要从事房地产销售、租赁的平台，包括房屋买卖、房屋租赁等。
2	**“独立于号码的人际通信服务（number-independent interpersonal communications services）”**指不与公开分配的号码资源相连接的通信服务，以及不与国家或国际的通信号码计划中的任何号码进行通信的通信服务。[1]	**社交娱乐类平台：** 即时通讯类：专门或者主要从事即时传递文字讯息、档案、语音与视频交流的平台。

1.实践中，独立于号码的人际通信服务通常包括应用程序提供的互联网通信服务，例如 WhatsApp、Messenger、Zoom 等，以及 SkypeOut 等半在线通信服务。

	《数字市场法案》	《分类分级指南》
3	**“在线社交网络服务（online social networking services）”**指使终端用户能够通过多重设备，以聊天、发帖、视频和推荐等形式，相互连接、交流、分享以及发现的平台。	**社交娱乐类平台：** 即时通讯类：专门或者主要从事即时传递文字讯息、档案、语音与视频交流的平台。 **信息资讯类平台：** 用户内容生成（UGC）类：专门或者主要从事用户将自己原创内容上传到互联网或者提供给其他用户的平台。
4	**“视频共享平台（video-sharing platform services）”**指为提供信息、教育或娱乐等目的，通过呈现、标记和排序视频，向公众提供其不具有编辑责任的节目和用户制作的视频的平台。	**社交娱乐类平台，包括但不限于：** （1）视听服务类：专门或者主要从事供给各类多媒体资料的平台，包括歌曲、电影等。 （2）直播视频类：专门或者主要从事利用互联网及流媒体技术进行直播的平台。 （3）短视频类：专门或者主要从事几秒到几分钟不等的短视频内容推送的平台，包括技能分享、幽默搞怪、时尚潮流、社会热点、街头采访、公益教育、广告创意、商业定制等主题。
5	**“在线搜索引擎（online search engines）”**指允许用户以关键词、语音、短语等输入形式进行查询并以任何格式反馈与用户请求相关的内容的数字服务。	**信息资讯类平台：** 搜索引擎类：专门或者主要从事对互联网上采集的信息进行组织和处理后，为用户提供检索服务，并将检索的相关信息展示给用户的平台。
6	**“操作系统（operating systems）”**指控制硬件或其他软件的基本功能，并能使其他软件在其上运行的系统软件。	**计算应用类平台：** 操作系统类：专门或者主要从事移动操作系统、分布式操作系统等操作系统的研发、生产、销售等的平台。
7	**“云计算服务（cloud computing services）”**指提供对可扩展和弹性的可共享计算资源池的访问的数字服务。	**计算应用类平台：** 云计算类：专门或者主要从事为企业提供云计算服务的平台，包括提供网络基础设施服务（IAAS）、平台服务（PAAS）、应用软件服务（SAAS）等的平台。

	《数字市场法案》	《分类分级指南》
8	**“网络浏览器(web browsers)”**指使终端用户能够访问发布于联网的服务器上的内容并与该等内容互动的软件应用程序,包括独立的网络浏览器以及集成或嵌入软件的网络浏览器。	无对应平台服务类型
9	**“虚拟助理(virtual assistants)”**指能够处理用户的需求、任务或问题的软件,包括基于音频、视频、文字输入、姿势或动作进行处理的软件,以及可以基于该等需求、任务或问题,向用户提供对其他服务的访问或对物理设备的控制的软件。	无对应平台服务类型
10	**“在线广告服务(online advertising services)”**指向上述各项核心平台服务的经营者提供在线广告互联服务、在线广告交换服务等在线广告中介服务的平台。	无对应平台服务类型

(二)认定标准

DMA根据“对内部市场具有重大影响”“提供核心平台服务,且该服务是商业用户与终端用户接触的重要门户”和“在其经营中占据稳固且持久的地位,或者可预见其将在不久的将来占据稳固且持久的地位”3项定性标准认定守门人,并针对这3项标准设计了可量化的“营业额门槛”和“用户规模门槛”。同时,DMA还设计了兜底条款,欧盟委员会可以基于“企业规模”

《主体责作指南》根据“用户规模”“经济体量”“业务情况”和“限制能力”4项标准界定超级平台。

“用户锁定效应”“网络效应”“纵向整合”和“集团结构”等其他考量因素，将未达到“营业额门槛”和“用户规模门槛”，但仍然符合3项定性标准的企业认定为守门人。对于欧盟委员会认定结论，企业具有提出异议的权利。[2]

《主体责任指南》则是根据“用户规模”“经济体量”“业务情况”和“限制能力”4项标准界定超级平台。与DMA不同的是，《主体责任指南》仅关注过去1年的“用户规模”数据和“经济体量”数据，且其对“业务情况”和“限制能力”标准的评价缺乏量化指标，企业自我评估时存在一定不确定性。

	《数字市场法案》	《主体责任指南》
经济体量	欧盟营业额在过去三个财务年度内均达到或超过75亿欧元，或者其在过去三个财务年度中的平均市值或等值市场公允价值均达到或超过75亿欧元，并且其在至少三个成员国提供相同的核心平台服务。[3]	上年底市值（或估值）不低于1000亿人民币
用户规模	三个财务年度中，其每个年度提供的核心平台服务中，均有4500万月活跃终端用户建立或位于欧盟境内，并且有1万家年活跃商业用户设立于欧盟境内。[4]	在中国的上年度年活跃用户不低于5000万
限制能力	无类似规定	具有较强的限制平台内经营者接触消费者（用户）能力
业务情况	无类似规定	具有表现突出的主营业务

2.见《数字市场法案》第三条第5款(a)项。
3.见《数字市场法案》第三条第2款(a)项。
4.见《数字市场法案》第三条第2款(b)项。

DMA为守门人设置了必须履行的行为义务和欧盟委员会可视情况指定守门人应履行的行为义务。

	《数字市场法案》	《主体责任指南》
其它考量因素	(a) 规模，包括核心平台服务提供者的营业额以及市值、运营情况以及地位； (b) 依赖于核心平台服务来接触终端用户的商业用户的数量以及终端用户数量； (c) 网络效应和数据驱动优势，特别是访问和收集个人和非个人数据以及数据分析的能力； (d) 规模和范围效应，包括与数据相关的或在欧盟外的规模和范围效应； (e) 对商业用户和终端用户的锁定效用，包括阻碍商业用户或终端用户转换平台或使用多个平台的转换成本和行为偏见； (f) 集团结构或纵向整合，例如使之能够交叉补贴、合并不同来源的数据以利用其地位的集团结构或纵向整合。[5]	无类似规定

PART 002

守门人的行为义务

DMA为守门人设置了两类行为义务，一类是守门人必须履行的行为义务（“**必要义务**”），另一类是欧盟委员会可视情况指定守门人应履行的行为义务（“**指定义务**”）。这些义务包括公平竞争、平等治理、开放生态、规范数据合并、保障数据互联互通等内容。

（一）公平竞争义务

DMA从数据使用和捆绑服务两方面对守门人的行为做出禁止性规定。**在数据使用方面**，DMA明确禁止守门人对核心平台服务所产生数据的两类利用：(1) 出于提供在线广告服务的目的，处理或利用终端用户在平台上使用第三方服务产生的个人数据；(2) 出于竞争的目的，利用竞争对

5.见《数字市场法案》第三条第8款。

DMA从数据使用和捆绑服务两方面对守门人的行为做出禁止性规定。

手使用守门人核心平台服务产生的非公开数据。第二类数据使用也受到《主体责任指南》的重点关注，《主体责任指南》同样禁止超大型平台利用平台服务形成的非公开数据，在与平台内经营者开展竞争时获得不正当的竞争优势。

在捆绑服务方面，DMA与《主体责任指南》均禁止守门人/超大型平台将使用其他关联平台服务作为用户获取自身所需平台服务的前提条件。

	《数字市场法案》	《主体责任指南》
数据使用	守门人不得为提供在线广告服务目的，处理或利用终端用户在守门人平台上使用第三方服务产生的个人数据，除非获得终端用户符合GDPR要求的知情同意。[6]（必要义务）	无类似规定
	守门人不得使用商业用户或其客户在其核心平台服务中产生或提供的非公开数据，以与商业用户竞争。[7]（指定义务）	超大型平台经营者在与平台内经营者开展公平竞争时，无正当理由不得使用平台内经营者及其用户在使用平台服务时产生或提供的非公开数据。
捆绑服务	守门人不得将商业用户或终端用户订阅或注册其他关联平台核心平台服务或达到本法案用户规模门槛的核心平台服务作为能够使用、访问、订阅或注册守门人核心平台服务的前提条件。[8]（必要义务）	平台内经营者或用户访问、注册、登录、获取其所需的超大型平台服务时，不将使用其他关联平台提供的服务作为前提条件。

6.见《数字市场法案》第五条第2款。
7.见《数字市场法案》第六条第2款。
8.见《数字市场法案》第五条第8款。

DMA与《主体责任指南》均要求遵守公平、合理和非歧视（”FRAND“）原则，且关注自我优待问题。

（二）平等治理义务

DMA与《主体责任指南》均要求遵守公平、合理和非歧视（“**FRAND**”）原则，且关注自我优待问题。但DMA较《主体责任指南》更为细化，明确规定守门人在“排名、相关索引与抓取”“访问条件”“传达和推广报价”三个场景下的FRAND义务，并要求守门人不得在“排名、相关索引与抓取”场景下实施自我优待。

	《数字市场法案》	《主体责任指南》
FRAND原则	在排名、相关索引与抓取中，守门人不应给予其自身提供的服务和产品比第三方的类似服务或产品更优惠的待遇。守门人应秉承透明、公平和无歧视的原则进行排名。[9]（指定义务）	超大型平台经营者应当遵守公平和非歧视原则。提供相关产品或服务时，平等对待平台自身（或关联企业）和平台内经营者，不实施自我优待。
	守门人对商业用户接入其软件应用商店、在线搜索引擎和在线社交网络服务应适用公平、合理和非歧视性的通用条件。为此，守门人应公布通用接入条件，包括替代争端解决机制。[10]（指定义务）	

（三）开放生态义务

DMA针对互操作性和操作限制两方面，要求守门人维持平台开放生态，尊重终端用户的选择权，保护市场的可竞争性。与之相对，《主体责任指南》采用“推动其提供的服务与其他平台经营者提供的服务具有互操作性”这一较为宽泛的表述为超大型平台施加义务，并允许超大型平台将安全、主体权益保障等事项作为不保障互操作性的正当理由。

9.见《数字市场法案》第六条第5款。
10.见《数字市场法案》第六条第12款。

DMA针对互操作性和操作限制两方面，要求守门人维持平台开放生态，《主体责任指南》则采用较为宽泛的表述为超大型平台施加义务。

	《数字市场法案》	《主体责任指南》
互操作性要求	守门人应允许终端用户使用商业用户的应用，通过守门人的核心平台服务，访问和使用内容、订阅、功能或其他项目，包括终端用户在不使用守门人核心平台服务的情况下，从相关商业用户处获得此类项目。[11]（必要义务）	超大型平台经营者应当在符合安全以及相关主体权益保障的前提下，推动其提供的服务与其他平台经营者提供的服务具有互操作性。超大型平台经营者没有正当合理的理由，应当为符合条件的其他经营者和用户获取其提供的服务提供便利。
	守门人应允许并确保第三方应用软件或应用商店的安装和有效使用，且能与守门人的操作系统之间具有互操作性，并允许通过不依赖于看守门人核心平台服务的方式访问这些应用软件或应用商店。[12]（指定义务）	
	守门人不得限制终端用户利用守门人核心平台服务在不同应用软件和服务之间切换或订阅的能力，包括对互联网接入商的选择。[13]（指定义务）	
	守门人应允许服务提供者和硬件提供者免费实现与通过操作系统、虚拟助手获取或控制的软硬件功能的互操作性（该等互操作性应与守门人提供的软硬件所享有的互操作性一致），并为互操作性目的访问这些软硬件功能。此外，守门人应允许商业用户和替代供应商免费实现与操作系统、软硬件功能的互操作性（该等互操作性应与守门人提供类似服务时所享有的互操作性一致），并为互操作性目的访问操作系统、软硬件功能。[14]（指定义务）	
操作限制	守门人应允许终端用户卸载任何预装应用（系统运行所必须的除外），并便利终端用户更改产品或服务的默认设置。[15]（指定义务）	无类似规定
	守门人不应为终止核心平台服务设定不相称的通用条件，应确保终止条件的实施不存在不合理的困难。[16]（指定义务）	

11.见《数字市场法案》第五条第5款。
12.见《数字市场法案》第六条第4款。
13.见《数字市场法案》第六条第6款。
14.见《数字市场法案》第六条第7款。
15.见《数字市场法案》第六条第3款。
16.见《数字市场法案》第六条第13款。

DMA规定守门人在获得终端用户符合GDPR要求的知情同意后，方可进行各类型数据合并。《主体责任指南》将数据合并行为的知情同意义务覆盖所有互联网平台经营者。

（四）规范数据合并义务

DMA规定守门人在获得终端用户符合GDPR要求的知情同意后，方可进行各类型数据合并。值得一提的是，在德国联邦卡特尔办公室（“**FCO**”）调查Facebook案中，FCO认为Facebook滥用其在德国社交网络市场上的支配地位，将同意相关条款作为使用Facebook的必要条件，强制用户同意将来自第三方（如WhatsApp）的用户数据与Facebook数据进行合并，于是要求Facebook根据GDPR的规定进行调整。尽管本案后续引发诸多诉讼争议，但这一执法思路如今已被吸收进DMA中，对守门人的数据合并活动进行规范。

根据《主体责任指南》，对数据合并行为的知情同意义务不局限于超大型平台，而是覆盖所有互联网平台经营者。《主体责任指南》的这一规定也是《个人信息保护法》中个人信息处理者处理个人信息应符合“知情同意”原则的体现。

	《数字市场法案》	《主体责任指南》
数据合并	守门人不得将来自相关核心平台服务的个人数据与来自任何其他核心平台服务的个人数据或来自由守门人提供的任何其他服务的个人数据或第三方服务的个人数据相结合，除非获得终端用户符合GDPR要求的知情同意。[17]（必要义务）	未经用户同意，互联网平台经营者不得将经由平台服务所获取的个人数据与来自自身其他服务或第三方服务的个人数据合并使用。
	守门人不得将来自相关核心平台服务的个人数据交叉用于守门人单独提供的其他服务中，反之亦然，除非获得终端用户符合GDPR要求的知情同意。[18]（必要义务）	
	守门人不得为合并个人数据而使终端用户登录守门人的其他服务，除非获得终端用户符合GDPR要求的知情同意。[19]（必要义务）	互联网平台经营者不得以合并个人数据为目的诱导、强迫用户登录并使用自身提供的其他服务。

17.见《数字市场法案》第五条第2款(b)项。
18.见《数字市场法案》第五条第2款(c)项。
19.见《数字市场法案》第五条第2款(d)项。

（五）保障数据互联互通义务

DMA要求守门人保障终端用户的数据可携带权，并向商业用户、在线搜索引擎第三方经营者和广告主/广告发布者等数据主体提供其使用守门人核心平台服务所产生的数据，从而保障平台间的数据互联互通，提高市场的可竞争性。此前，关于不同平台间数据的互联互通开放问题，在境外也屡发争议，境外司法实践对数据开放通常持肯定态度。如在某数据抓取相关案件中，H公司作为一家以公共数据源为基础的数据分析公司，被L平台拒绝访问和复制平台会员的公开数据资料。经各级审理，法院最终支持了H公司的诉求，要求L平台清除访问其公开数据的技术障碍，并允许H公司访问L平台的公开数据。

而《主体责任指南》并未就保障数据互联互通进行任何规定，其仅从保护数据安全的角度出发，要求超大型平台建立健全数据安全审查与内控机制，对涉及用户个人信息的处理、数据跨境流动，涉及国家和社会公共利益的数据开发行为，必须严格依法依规进行。我国现行法律中，仅有《个人信息保护法》对个人信息的可携带权进行规定。

《主体责任指南》并未保障数据互联互通进行任何规定，仅从保护数据安全的角度要求超大型平台建立健全数据安全审查与内控机制。

	《数字市场法案》	《个人信息保护法》
终端用户的数据可携带权	守门人根据终端用户及被授权第三方的请求，保障终端用户所提供或因核心平台服务相关活动产生数据的可携带权，包括免费提供工具以便利行使数据可携带权，并允许用户持续且实时访问这些数据。守门人不得为此收取任何费用。[20]（指定义务）	个人有权向个人信息处理者查阅、复制其个人信息；有本法第十八条第一款、第三十五条规定情形的除外。 个人请求查阅、复制其个人信息的，个人信息处理者应当及时提供。 个人请求将个人信息转移至其指定的个人信息处理者，符合国家网信部门规定条件的，个人信息处理者应当提供转移的途径。[21]
向商业用户提供数据	对于商业用户在使用核心平台服务或通过核心平台服务的支持开展服务时提供或产生的数据，守门人应向商业用户或商业用户授权的第三方免费提供有效的、高质量、可供实时访问及使用的聚合/非聚合数据。 对于前述数据中的个人数据，守门人仅能在个人数据的产生与终端用户使用商业用户的产品或服务直接相关，且终端用户同意共享数据的情况下提供。[22]（指定义务）	无类似规定
向在线搜索引擎第三方经营者提供数据	守门人应根据提供在线搜索引擎的第三方经营者的请求，以公平、合理和非歧视的条件，向其提供终端用户在守门人的在线搜索引擎上生成的免费和付费搜索数据，包括排名、查询、点击和浏览等产生的数据。但该等数据应以匿名化方式呈现，这一过程中的个人数据都应被匿名化。[23]（指定义务）	

20.见《数字市场法案》第六条第9款。
21.见《个人信息保护法》第四十五条。
22.见《数字市场法案》第六条第10款。
23.见《数字市场法案》第六条第11款。

DMA还为守门人施加了必要义务，以提高守门人为商业用户提供在线广告服务的透明性，并降低守门人作为企业与用户之间媒介的唯一性。

	《数字市场法案》	《个人信息保护法》
向广告主、广告发布者提供数据	守门人应根据广告主、广告发布者及其授权第三方的请求，免费提供业绩测量工具及他们自行对广告清单开展核查所需的聚合/非聚合数据。此类数据的提供方式应使广告主、广告发布者能够运行自己的测量及核查工具，评估守门人所提供核心平台服务的业绩表现。[24] (指定义务)	

(六)其它义务

在前述义务外，DMA还为守门人施加了数项必要义务，以提高守门人为商业用户（包括广告主和广告发布者）提供在线广告服务的透明性[25]，并降低守门人作为企业与用户之间媒介的唯一性[26]。后者反映了DMA试图引导守门人去中介化，为市场中其它核心平台服务提供者参与市场竞争创造环境的立法目的：

- “守门人不得阻止商业用户通过第三方在线中介服务或通过其自己的在线直接销售渠道，以不同于守门人在线中介服务的价格或条件，向终端用户提供相同的产品或服务”[27]；
- “守门人应允许商业用户免费通过核心平台服务或其他渠道，在不同条件下向终端用户传达和推广报价，并签订合同，无论商业用户是否以此为目的使用核心平台服务”[28]。

PART 003

经营者集中

DMA对守门人的经营者集中施加了额外的报告义务，要求守门人就所有目标公司提供核心平台服务，或数字行业任何其他服务，或从事数据收集工作的经营者集中向欧盟委员会报告，并在集中所获得

24.见《数字市场法案》第六条第8款。
25.见《数字市场法案》第五条第9款和第10款。
26.见《数字市场法案》第五条第3款和第4款。
27.见《数字市场法案》第五条第3款。
28.见《数字市场法案》第五条第4款。

DMA对守门人的经营者集中施加了额外的报告义务，《主体责任指南》仅对所有互联网平台经营者应遵守的经营者集中申报义务做了重申。

核心平台服务触及用户规模门槛时进一步报告。若守门人违反报告义务，将被处以不超过其上一财年全球总营业额10%的罚款。[29]而《主体责任指南》仅对所有互联网平台经营者应遵守的经营者集中申报义务做了重申。

	《数字市场法案》	《主体责任指南》
经营者集中	如果守门人拟从事合并或集中的目标实体提供核心平台服务或数字行业任何其他服务，或从事数据收集工作，无论本次合并或集中是否需要依法进行申报，守门人都应向欧盟委员会报告。 守门人向欧盟委员会报告的时间点应在签订协议或竞标公告后，实施集中前。[30]	互联网平台经营者应当遵守反垄断领域的法律、法规、规章等规定，不得从事垄断协议、滥用市场支配地位等垄断行为。互联网平台经营者在实施经营者集中前，应根据有关法律法规履行申报义务，在获得有关部门批准之前，不得实施集中。
	如果前述合并或集中完成后，存在额外的单个核心平台服务触及本法案规定的用户规模门槛，则守门人应当在实施集中后2个月内向欧盟委员会报告此情况，并提供相关信息。[31]	

PART 004

内部治理

在内部治理方面，DMA对守门人内部合规部门的机构设置、人员配置、权限职责、运行机制都做了较为详细的规定，譬如，(1) 要求保障合规部门的权力、地位和资源，并有权接触守门人的管理机构[32]，(2) 要求合规负责人应当为对合规职能负明确职责的独立高级管理人员[33]，(3) 规定

29.见《数字市场法案》第三十条第1款。
30.见《数字市场法案》第十四条第1款。
31.见《数字市场法案》第十四条第3款。
32.见《数字市场法案》第二十八条第2款。
33.见《数字市场法案》第二十八条第3款。

内部治理方面，《主体现作指南》较DMA更关注超大型平台的合规机制建设工作。

未经守门人的管理机构事先批准，合规部负责人不得被免职[34]，(4)明确合规人员监督守门人管理层和雇员，并与欧盟委员会进行合作的职责。[35]若守门人未按要求引入合规职能部门，将被处以不超过其上一财年全球总营业额10%的罚款。[36]

《主体责任指南》较DMA更关注超大型平台的合规机制建设工作，明确要求超大型平台建立平台内部预防腐败机制和平台内部定期教育培训机制。

	《数字市场法案》	《主体责任指南》
内部治理	守门人应引入独立于运营职能的合规职能部门，该部门由一名或多名合规人员组成，包括合规部负责人。[37]	超大型平台经营者应当设置平台合规部门，不断完善平台内部合规制度和合规机制，积极响应监管部门的监管要求。应当建立平台内部预防腐败机制，有效防范平台内部人员商业贿赂等违法行为。应当建立平台内部定期教育培训机制，提高平台整体依法合规经营意识。

PART 005

豁免与罚则

就豁免而言，DMA仅将公共健康和公共安全作为豁免守门人义务的合理理由。《主体责任指南》规定的豁免理由范围则更广，不仅包括“公共利益、国家安全”，也包括“超出控制范围与技术能力，严重影响正常经营活动”。或许这意味着，相较于市场可竞争性等价值，《主体责任指南》更重视互联网平台的正常经营与发展。

就罚则而言，DMA与欧盟竞争法一样将企业上一财年全球总营业额作为罚款基数，且还将行为性救济与结构性救济作为守门人系统性违法的处罚和救济措施，对守门人具有极强的震慑性。《主体责任指南》未就罚则进行任何规定。

34.见《数字市场法案》第二十八条第4款。
35.见《数字市场法案》第二十八条第5款。
36.见《数字市场法案》第三十条第1款。
37.见《数字市场法案》第二十八条第1款。

就豁免而言，DMA仅将公共健康和公共安全作为合理理由，《主体责任指南》规定范围则更广；就罚则而言，《主体责任指南》未就罚则进行任何规定。

	《数字市场法案》	《主体责任指南》
豁免	只有在涉及公共健康或公共安全的理由下，欧盟委员会才能根据守门人提出的合理理由豁免守门人的特定必要义务或指定义务。[38]	互联网平台落实本指南所列各项主体责任时，如存在下列情形之一，可以根据具体情况，适当予以变通： （一）平台落实主体责任会导致公共利益、国家安全受到损害； （二）在具体情形中落实平台主体责任的要求，明显超出平台经营者的控制范围以及技术能力，严重影响其正常经营活动，且对于实现监管目的的意义不大； （三）法律法规以及国家政策所规定的其他允许除外或做变通处理的情形。
初次违法	如果欧盟委员会认定守门人因故意或过失而未能遵守必要义务或指定义务，可对守门人处以不超过其上一财年全球总营业额10%的罚款。[39]	无类似规定
多次违法	如果欧盟委员会认定守门人在8年内，于同一核心平台服务中，多次违反相同或类似必要义务或指定义务，可对守门人处以不超过其上一财年全球总营业额20%的罚款。[40]	
系统性违法	如果欧盟委员会调查发现守门人存在系统性违规行为，即8年内欧盟委员会至少3次认定守门人违反DMA[41]，欧盟委员会可以决定对守门人实施必要的结构性或行为性救济措施。[42]	

38.见《数字市场法案》第十条第3款。
39.见《数字市场法案》第三十条第1款。
40.见《数字市场法案》第三十条第2款。
41.见《数字市场法案》解释性备忘录第（75）段。
42.见《数字市场法案》第十八条第1款。

未来我国针对超大型互联网平台的监管思路是否会向DMA靠拢等问题，值得相关企业密切关注。

	《数字市场法案》	《主体责任指南》
其它违法	如果欧盟委员会认定守门人违反经营者集中报告义务或未按要求引入合规职能部门，可对守门人处以不超过其上一财年全球总营业额10%的罚款。[43]	

PART 006

结语

超大型互联网平台的自我优待、封锁外部链接等不利于市场竞争的运营方式已受到全球各司法辖区的高度关注。欧盟此次出台DMA，可能使数字经济市场的竞争格局向中小型互联网平台企业倾斜，重塑电子商务、搜索引擎、在线广告、应用商店和其它核心平台服务的运营模式，改变超大型互联网平台企业的商业模式。未来我国针对超大型互联网平台的监管思路是否会向DMA靠拢，《分类分级指南》和《主体责任指南》的生效版本是否会在《平台经济领域反垄断指南》的基础上，对平台企业互联互通、有序竞争提出更高要求，值得相关企业密切关注。

（赵雨杨、刘松林对本文亦有贡献）

43.见《数字市场法案》第三十条第3款(c)项和(j)项。

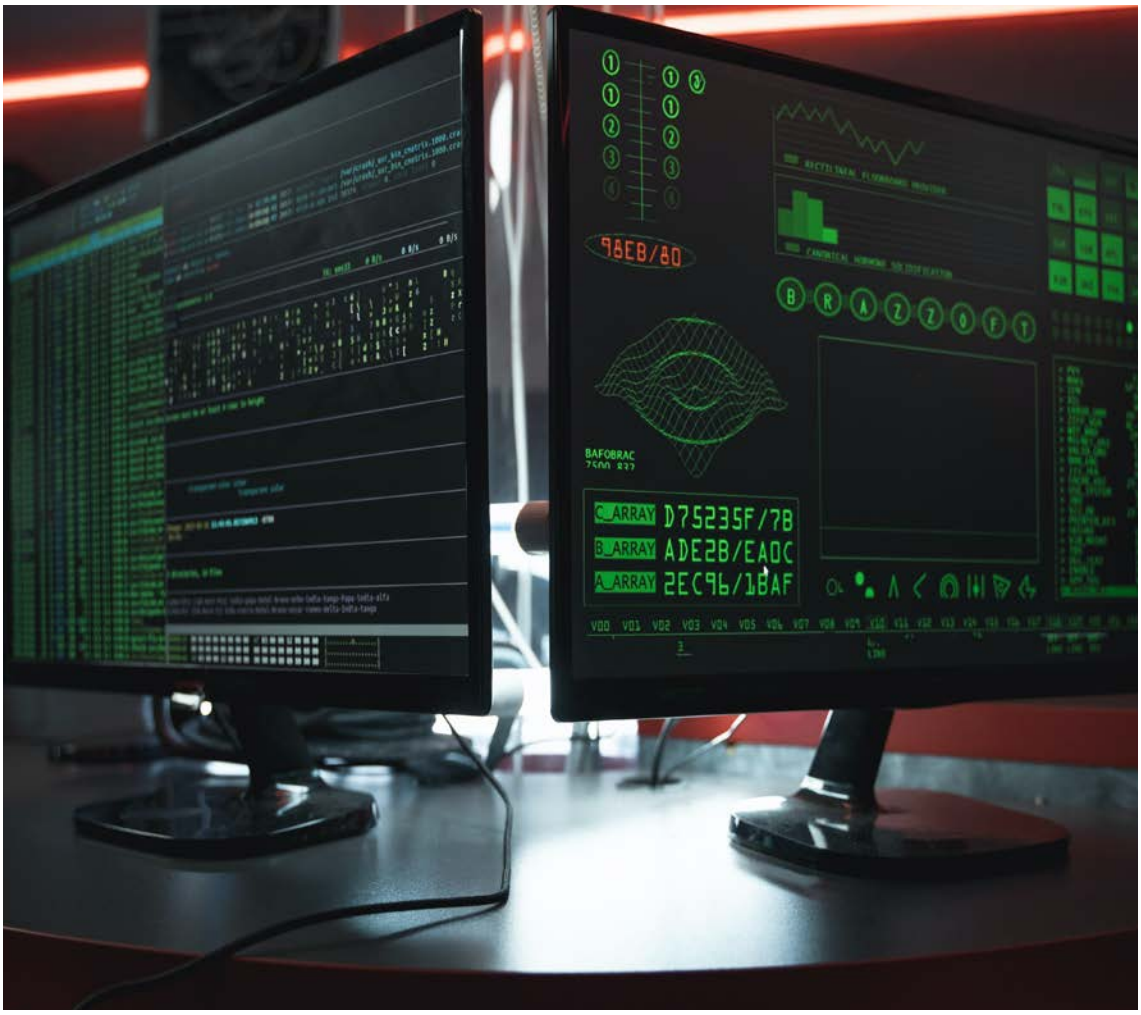
侯彰慧
合伙人
公司业务部
北京办公室
+86 10 5957 2336
houzhanghui@zhonglun.com

CHAPTER 02

个人信息保护实务观察

PART ONE

《个保法》下的企业合规之道



《个人信息保护法》正式生效，我们聊聊合规落地中的“五六七”

陈际红 吴佳蔚 陈煜烺

本文将逐步解读企业将面临的五大合规风险，六项合规难点，结合实际，对企业提出七点合规建议，以期能够在控制风险的前提下为数字化业务发展保驾护航。

PART 001

五大合规风险

2021年11月1日，《中华人民共和国个人信息保护法》（以下称“**《个保法》**”）即正式生效，新的个人信息保护时代已然来临。

在《个保法》建立的个人信息法律框架下，企业合规将面临前所未有的挑战。《个保法》生效伊始，我们认为企业所面临的突出合规风险主要包括行政处罚、民事诉讼、公益诉讼、高管责任、媒体舆情及协会组织的质疑等五大方面：

风险	典型违规事项	风险来源	后果
行政处罚	■ 处理个人信息不具备法律基础； ■ 未告知个人信息处理规则；或告知的方式、内容不合规； ■ 以同意作为法律基础时未获得有效授权同意；需单独同意的场景下未获得单独同意； ■ 自动化决策不符合透明性、公平性要求； ■ 跨境传输个人信息不符合法定条件，或未履行法定的本地化存储和跨境前安全评估的义务； ■ 未保障个人信息主体行权； ■ 未依法开展个人信息保护影响评估； ■ 大型互联网平台未履行法定义务。[1]	■ **收集侧**：用户投诉举报；监管部门主动检测、审查； ■ **使用侧**：个人信息泄露；违法开展自动化决策、跨境传输、向第三方提供等处理活动引发用户投诉举报或监管调查。	■ 责令改正，给予警告，没收违法所得；责令应用程序暂停或者终止提供服务；拒不改正的，并处一百万元以下罚款； ■ 情节严重的，并处五千万元以下或者上一年度营业额百分之五以下罚款，并可以责令暂停相关业务或者停业整顿、通报有关主管部门吊销相关业务许可或者吊销营业执照； ■ 记入信用档案，并予以公示。
民事诉讼	■ 处理个人信息侵害个人信息权益造成损害[2]。	■ 个人因权益受到损害而主张侵权责任。	■ 承担损害赔偿等民事侵权责任。

1.此处仅列举具有外部性的高风险违规事项，除前述列举事项外，《个保法》中规定的违法事项还包括违法公开个人信息、未履行个人信息处理者的基本义务（制定内部管理制度和操作规程、实行分类管理、采取加密、去标识化等安全措施）等。
2.具体免责事由可参见《中华人民共和国民法典》第一千零三十六条：
处理个人信息，有下列情形之一的，行为人不承担民事责任：
（一）在该自然人或者其监护人同意的范围内合理实施的行为；
（二）合理处理该自然人自行公开的或者其他已经合法公开的信息，但是该自然人明确拒绝或者处理该信息侵害其重大利益的除外；
（三）为维护公共利益或者该自然人合法权益，合理实施的其他行为。

企业所面临的突出合规风险主要包括行政处罚、民事诉讼、公益诉讼、高管责任、媒体舆情及协会组织的质疑等五大方面。

风险	典型违规事项	风险来源	后果
公益诉讼	■ 违法处理个人信息，侵害众多个人的权益； ■ 个人信息检察公益诉讼的重点方面包括敏感个人信息、特殊群体、重点领域；处理个人信息达100万人以上；对因时间、空间等联结形成的特定对象。[3]	■ 涉及众多用户、处理大量个人信息的大型平台和超级平台； ■ 相关单位、组织基于公益目的的驱使。	■ 人民检察院、法律规定的消费者组织和由国家网信部门确定的组织依法提起公益诉讼。
高管[4]责任	■ 企业违法处理个人信息或未履行个人信息保护义务，直接负责的主管人员和其他直接责任人员应承担相应责任； ■ 个人信息保护负责人未履行对企业个人信息处理活动以及采取的保护措施的监督职责。	■ 直接负责的主管人员和其他直接责任人员对于企业个人信息保护合规的管理职责。 ■ 特定企业的个人信息保护负责人的监督职责。	■ 直接负责的主管人员和其他直接责任人员面临一万元以上十万元以下罚款； ■ 情节严重的，直接负责的主管人员和其他直接责任人员面临十万元以上一百万元以下罚款；还可能在一定期限内被禁止担任相关企业的董事、监事、高级管理人员和个人信息保护负责人。
媒体舆情及协会组织的质疑	■ 企业违法违规处理个人信息或未履行个人信息保护义务。	■《个保法》生效后，相关投诉增多、舆情升温； ■ 对企业合规实践水平的对比报道。	■ 企业声誉损失，上市公司还可能面临股价下跌等损失； ■ 引发监管部门的重点关注。

3.关于个人信息检察公益诉讼从严把握的重点方面具体见最高人民检察院《关于贯彻执行个人信息保护法推进个人信息保护公益诉讼检察工作的通知》。
4.在我国个人信息保护法律框架下，对高管人员作了扩张解释，例如，除传统意义上的董监高外，企业个人信息保护负责人或直接责任人员亦将承担相应的法律责任。

在实务过程中，全面梳理个人信息处理活动，并合理论证其法律基础一直是企业的痛点和难点之一。

除上述风险外，企业还可能面临因个人信息保护层面的合规程度低而受到合作伙伴质疑，进而失去商业机会；此外，企业如违法出售、非法提供、非法获取公民个人信息且情节严重的，**还将面临构成侵犯公民个人信息罪的刑事风险。**

我们认为，企业可结合自身的业务特点，评估适用性和影响程度，同时结合监管关注热点和行业实践的情形，采取风险导向的合规思路，适当确定合规任务优先级。基于此，我们根据实务经验，梳理企业面临的六大合规难点问题，涵盖法律基础、单独同意、对外提供、跨境传输、自动化决策及重要互联网平台合规义务，以期帮助企业从内到外、由点及面地展开合规工作，满足法律法规的要求。

PART 002

六项合规难点

1.难点一：法律基础的判断及边界

法律基础是各项个人信息处理活动开展的前提，也决定着个人信息处理全生命周期的策略。区别于既往《中华人民共和国网络安全法》（以下称“**《网络安全法》**”）框架下仅以同意作为个人信息处理活动的法律基础，《个保法》明确列举了除同意外的六项法律基础。其中，不乏独具特色的中国式立法方案，如按照依法制定的劳动规章制度和依法签订的集体合同实施人力资源管理所必需，为应对公共卫生事件，及依照本法规定在合理的范围内处理个人自行公开或者其他已经合法公开的个人信息。在实务过程中，全面梳理个人信息处理活动，并合理论证其法律基础一直是企业的痛点和难点之一。例如：

– 如何判断订立或履行合同所必需的范围？企业内人力资源管理所必需的限度？公开个人信息合理使用的边界？哪些典型场景仅能通过同意的法律基础才能得以实施？在开展个人信息处理活动之前如何获得法律基础？

– 是否需要在处理活动的同时将对应的法律基础向用户告知？能否通过隐私政策等规则性说明文件获得相应的法律基础？

为解决法律基础判断这一难点问题，企业需在清晰梳理所涉个人信息处理活动的

单独同意即对本质上可能对用户个人信息权益带来显著影响的场景，施加给企业更严格的注意及告知义务。

基础上，按照以下的**四步法确定合法基础：**

首先，厘清是否存在个人信息收集的法定义务及职责要求，是否存在紧急情况、突发公共卫生事件、公共利益等事项。

如不涉及，继而从用户选择、使用所提供产品或服务的根本期待和最主要的需求出发，明确产品或服务的业务功能及特性，再对法律基础是订立或履行合同的必要抑或是同意加以区分。

第三，如企业以同意作为个人信息处理活动的合法基础，则需特别注意在实践中是否满足同意**“充分知情、自愿明确、随时撤回”**的标准。

第四，特别地，对于前述创新型法律基础，如人力资源管理及公开个人信息使用，企业在实践中难以比照其他国家或地区的典型做法或判例加以佐证，需严格遵守法律法规的要求，密切关注配套法规的进展及相关执法活动，以及时调整应对。

在法律基础的告知义务层面，除同意需以明确的方式告知用户，使用户充分知情后作出决定外，其他法律基础尚无明确规定需一一向用户说明。但是，我们建议企业在内部梳理法律基础后及时做好记录工作，并以适当方式通过隐私政策等文件对外部披露相关数据处理活动的规则以满足《个保法》第十七条项下的透明性要求，如外部对个人信息处理活动存在疑问或质询，可以以合理理由在第一时间进行解释并作出回复。

2.难点二：单独同意的适用及标准

《个保法》在敏感个人信息处理、对外提供个人信息、个人信息公开、公共场所图像采集及身份识别、个人信息跨境传输场景下首次提出了单独同意的概念。单独同意从文义解释来看，进一步加强了同意的告知义务，形式上更为分别和独立。从风险控制的角度考虑，单独同意即对本质上可能对用户个人信息权益带来显著影响的场景，施加给企业更严格的注意及告知义务。企业为满足此项要求，将着重分析论证相关场景的必要性及合理性，进而在最小必要的限度内开展此类高风险活动，并向用户告知。但在实践中，企业也面临着单独同意相关的种种困扰。例如：

– 单独同意是否仅基于以同意作为个人信息处理活动的法律基础？

在企业实务中，基于透明性要求，企业对于《个保法》第二十三条的适用及其与委托处理、共同处理的关系产生诸多难点。

一单独同意的内容和形式标准?如何处理单独同意可能造成的对用户的打扰与个人信息权益保护之间的平衡?

就单独同意的适用，我们理解，企业既然需在上述场景赋予用户单独同意的权利，那必然需要允许用户拒绝同意并随时撤回。然而，除同意外的其他法律基础，其必要性及不可撤回性将使单独同意的作出形同虚设。另外，企业虽然开展上述高风险场景的活动，但是基于非同意的其他法律基础，如订立或履行合同的必要、履行法定义务或职责、公共利益等，该个人信息处理活动亦属于企业不得不承担的责任或履行的义务，如此时予以用户拒绝的权利，对企业而言也并不合理。据此，我们倾向于认为，单独同意仅适用于以同意作为合法基础的处理场景。

对于单独同意的标准而言，如企业确定在某一场景下需获取单独同意，我们理解，企业无需机械地理解法条规定，完全以牺牲用户体验的代价去实现。企业仅需以达到单独提示用户、赋予用户单独选择机会的效果标准出发，从形式和内容两方面加强高风险场景的告知和提示，确保用户充分知悉该个人信息处理活动的目的、方式和范围。

3.难点三：对外提供、委托处理和共同处理的透明性要求

《个保法》第二十三条规定了个人信息处理者对外提供个人信息的合规要求，其中在透明性要求方面规定了对外提供的增强告知义务，即“告知接收方的名称或者姓名、联系方式、处理目的、处理方式和个人信息的种类”；与此同时，《个保法》第二十条、第二十一条则未对共同处理、委托处理场景提出告知第三方具体信息的要求。在企业实务中，基于此等透明性要求，企业对于《个保法》第二十三条的适用及其与委托处理、共同处理的关系产生诸多难点。例如：

一如何理解对外提供的含义，委托处理是否属于对外提供的范围?

一是否需在隐私政策中对所有涉及第三方的情形均明确告知第三方的名称或者姓名、联系方式?就委托处理而言，是否需要披露具体的处理场景?

目前，实务界和理论界对于对外提供

企业应梳理个人信息处理活动中涉及的第三方，从事实和法律两个层面共同厘清与第三方的关系，并在此基础上分别通过隐私政策履行告知义务。

和委托处理、共同处理的含义已展开较为充分的探讨，其中不乏认为“对外提供包括委托处理，进而在委托处理的场景下也需履行《个保法》第二十三条的告知要求，并获得单独同意”的观点。我们理解，从区分对外提供和委托处理的立法目的角度分析，对外提供意味着提供方和接收方系独立的个人信息处理者，需各自对个人信息处理活动承担责任，个人信息主体亦可自行选择向哪一方处理者行权；而委托处理场景下受托人需完全在委托人指示下基于委托人的处理目的、处理方式来处理个人信息，并由委托人对外承担责任，个人信息主体原则上仅与委托人直接交互并向其行权。因此，我们倾向于认定对外提供和委托处理系并列而非包含关系。

进一步，隐私政策向用户披露个人信息处理规则的核心在于充分保障用户的知情权，而区分不同信息处理者类型的效果之一亦在于便于用户行使个人信息主体权利。同上分析，对外提供和委托处理对于个人信息主体行权存在不同的制度效果和立法意旨，据此，就是否披露第三方的姓名或者姓名、联系方式等信息，在委托处理场景下既无法律强制性要求，亦无扩张适用《个保法》关于对外提供条文予以规制的必要。但需提示企业注意，委托处理作为一种处理方式，应构成《个保法》第十七条第一款第（二）项规定的法定告知事项，因此最合规的做法仍为对每一项委托处理的场景均对处理目的、方式、种类、保存期限予以充分告知。

企业应梳理个人信息处理活动中涉及的第三方，从事实[5]和法律两个层面共同厘清与第三方的关系，并在此基础上分别通过隐私政策履行《个保法》第十七条和第二十一条的告知义务；其中，对于委托处理尽管无需告知受托人的名称或者姓名、联系方式，但原则上仍需逐项告知委托处理的具体场景如受托业务类型等，同时，对于第三方供应商提供数据存储、处理、技术支持支持等外部风险较低的委托处理行为，企业可在评估风险的前提下适当放宽要求。

5.例如，在实务中存在接收方企业希望通过主张自身构成法律层面的受委托处理者，进而降低承担法律责任的风险，但其事实上对于接收的个人信息实施了数据融合等超出原委托协议范围的个人信息处理活动，则其在事实层面已不再属于委托处理，也难以通过主张委托处理而规避监管和责任。

由于相关配套机制尚不完善，企业的本地化存储义务和个人信息跨境传输的路径可谓迷雾重重。

4.难点四：本地化存储义务及跨境传输

《个保法》在第三章对中国式个人信息跨境传输规则作出规定，提出关键信息基础设施运营者和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的本地化存储义务。然而，由于相关配套机制尚不完善，企业的本地化存储义务和个人信息跨境传输的路径可谓迷雾重重。例如：

－关键信息基础设施运营者的判定？国家网信部门规定的个人信息处理数量的判定？是基于个人信息主体数量，或个人信息条数？统计时间从何时开始？企业如包含多个产品或服务条线，应单独计算或整体计算？

－个人信息跨境传输安全评估的适用及流程？个人信息保护认证的适用及流程？与境外接收方签订的标准合同的格式，或需至少包含何种内容？

所幸，2022年7月7日，国家互联网信息办公室（以下称**“国家网信办”**）发布了《数据出境安全评估办法》（以下称**“《评估办法》”**），并于2022年9月1日施行，对部分问题进行了初步解答。

就本地化存储的义务主体而言，除《网络安全法》第三十七条[6]所规制的收集和产生个人信息和重要数据的关键信息基础设施运营者，《中华人民共和国数据安全法》第三十一条[7]规定的收集和产生重要数据的其他数据处理者外，还包括《个保法》第三十六条规定的处理个人信息的国家机关和第四十条规定的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。此外，《汽车数据安全管理若干规定（试行）》等特定行业规范也对构成重要数据的汽车数据、金融数据、医疗健康数据、测绘数据等规定了相应的本地化存储要求。

《评估办法》在第四条中明确：①处理个人信息达到100万人以上的个人信息处理者；或②自上年1月1日起累计向境外提供超过10万人个人信息或1万人敏感个人信息的个人信息处理者，需申报网信办组织的安全评估。我们理解此处是指单个的

6.《网络安全法》第三十七条：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。

7.《数据安全法》第三十一条：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重要数据的出境安全管理，适用《中华人民共和国网络安全法》的规定；其他数据处理者在中华人民共和国境内运营中收集和产生的重要数据的出境安全管理办法，由国家网信部门会同国务院有关部门制定。

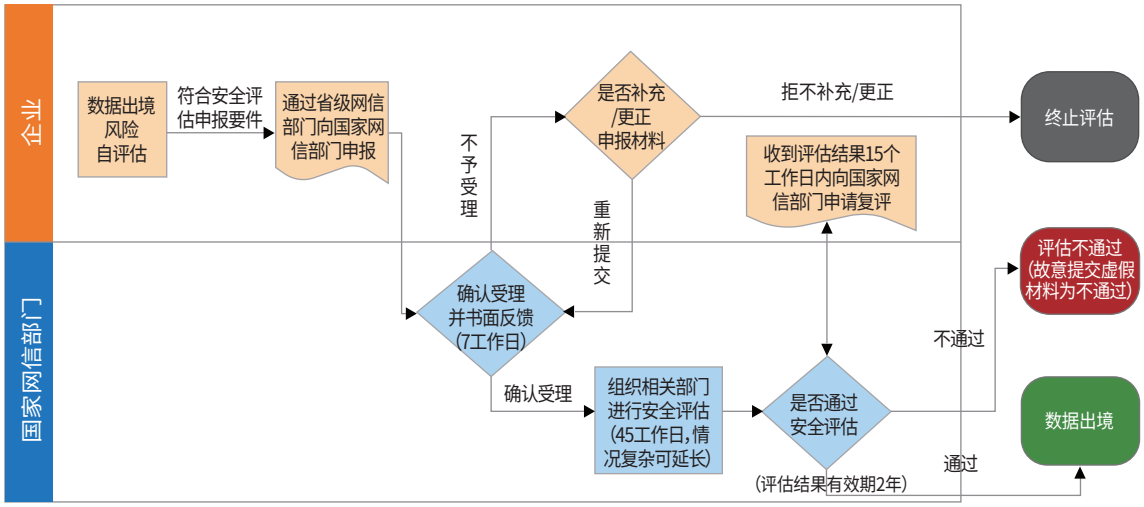
《评估办法》系统性地说明了安全评估的相关细则，包括数据出境风险自评估事项、安全评估的流程、申报材料等。

个人信息处理者，如果某集团公司内涉及的多个实体之间没有数据混同或融合的情况，我们认为应按照不同实体分别计算。同时，计算范围应是个人信息处理者范围内所有个人信息处理场景所涉及主体的总量，既包括外部客户、用户等，也包括内部员工。

虽然法律暂未明确《评估办法》规定的需要申报安全评估的情形，是否一定会触发数据本地存储的义务，但我们倾向于认为本地存储和跨境安全评估是保障数据安全的一体两面。同时，结合《个保法》第四十条的规定，《评估办法》所规定的100万、10万和1万的门槛，构成《个保法》第四十条所指的“国家网信部门规定数量”，因此《办法》规定的需要申报安全评估的情形将触发数据本地存储的义务。

另外，针对个人信息跨境传输的路径，《个保法》设置了国家网信部门组织的安全评估、按照国家网信部门的规定经专业机构进行的个人信息保护认证、按照国家网信部门制定的标准合同与境外接收方订立合同、或其他法律法规规定四种路径。

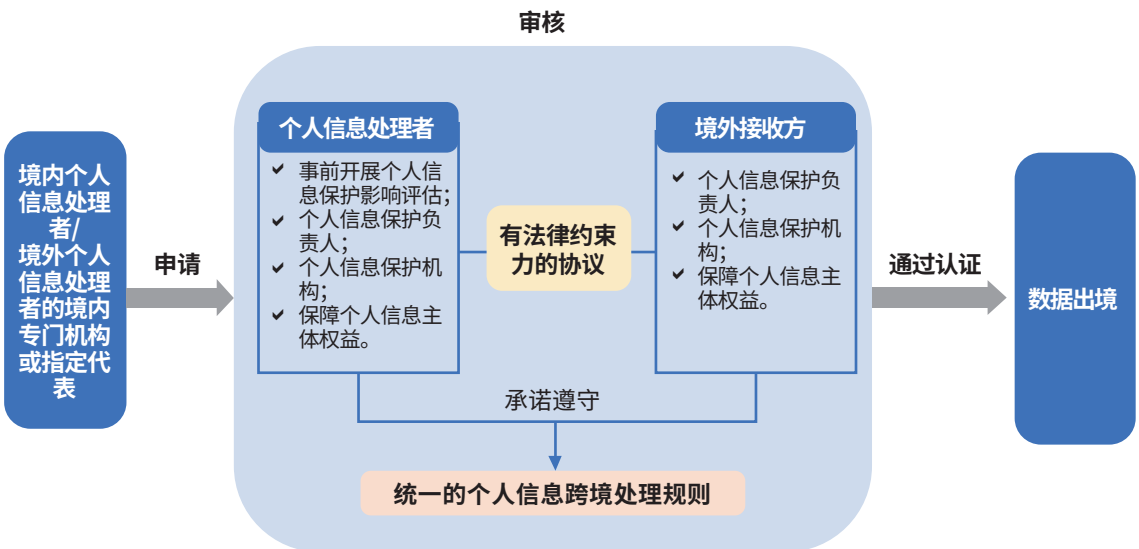
《评估办法》系统性地说明了安全评估的相关细则，包括数据出境风险自评估事项、安全评估的流程、申报材料等（具体见下图）。



（数据出境安全评估流程图）

《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》对个人信息跨境认证的流程与具体要求等进行了规定。

2022年6月24日，全国信息安全标准化技术委员会发布《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》（以下称“**《认证规范》**”），明确个人信息跨境认证适用于：①跨国公司或者同一经济、事业实体下属子公司或关联公司之间的个人信息跨境处理活动，或②《个保法》第三条第二款适用的个人信息处理活动，并对个人信息跨境认证的流程与具体要求等进行了规定（具体见下图），使得个人信息跨境认证机制进入有章可循的局面。但《认证规范》仅为推荐性实践指南，且仍余留部分不明确之处待强制性规范进一步细化或待国家网信部门进一步解释，如未明确具体的认证机构。



（个人信息跨境认证流程图）

此外，国家网信办于2022年6月30日公布《个人信息出境标准合同规定（征求意见稿）》，初步确定了《个人信息出境标准合同》的内容，并提出个人信息处理者应当在标准合同生效之日起10个工作日内，向所在地省级网信部门备案，备案时应当提交所签署的标准合同及个人信息保护影响评估报告。

从数据治理到算法治理层面的透明性要求对于互联网企业提出了巨大挑战。

我们理解，一旦触发数据出境安全评估的法定条件，则相关主体必须向网信办申报安全评估；如未触发，则可选择进行个人信息跨境认证或签订《个人信息出境标准合同》。相对而言，跨国公司及同一实体下的子公司间的处理活动，具有内部性，且各方的关系稳定、公司管理架构一致，容易达成认证所需要的协议、组织设置、统一数据处理规则等要求，比较适合于认证机制；个人信息出境标准合同则具有灵活性，可广泛、便捷应用于各种场景，可能会成为个人信息跨境处理活动中最基础和最为普遍采用的一种合法路径。

5.难点五：数据和算法双重治理下的自动化决策

人工智能、大数据、机器学习蓬勃发展的当下，人类已逐渐进入“算法社会”。算法带来便利的同时，大数据杀熟、信息茧房、价格歧视等问题也体现了算法的负面效应。《个保法》第二十四条对于自动化决策进行规制，并分别提出了三个层面的合规要求。其中《个保法》关于自动化决策的透明度，以及通过自动化决策作出对个人权益有重大影响的决定时的说明义务，均体现出《个保法》在数据治理层面对于公开、透明的重视；与此同时，近期《关于加强互联网信息服务算法综合治理的指导意见》《互联网信息服务算法推荐管理规定》等规定的出台，则从算法治理层面提出了“以显著方式告知用户其提供算法推荐服务的情况，并以适当方式公示算法推荐服务的基本原理、目的意图、运行机制”[8]的告知和公示要求。然而，此等从数据治理到算法治理层面的透明性要求对于互联网企业提出了巨大挑战。例如：

— 算法应当以何种形式披露，是否需包含技术细节，是否应确保用户充分理解？

— 企业如何保证自身商业秘密、经营模式不被泄露的前提下履行算法透明性义务？

— 对于算法的披露需要达到何种程度，标准如何界定？

事实上，无论是《个保法》还是《互联网信息服务算法推荐管理规定》等规定，其对

8.《互联网信息服务算法推荐管理规定》第十六条：算法推荐服务提供者应当以显著方式告知用户其提供算法推荐服务的情况，并以适当方式公示算法推荐服务的基本原理、目的意图和主要运行机制等。

《个保法》从个人信息保护层面对重要互联网平台提出了特殊合规义务，此等合规义务在实务的落实过程中也出现了障碍。

于算法透明性的规定中均未要求披露技术细节，因此，企业不必过于担心因对代码、技术方案等细节的披露不充分而受到监管处罚，也避免企业自身商业秘密、核心经营模式被强制要求公开披露的商业风险。但同时，数据治理和算法治理共同目标在于保护个体的知情权、自决权等权利，据此，企业所披露的算法规则应尽可能便于确保用户理解和作出选择，例如以示例、流程图等方式予以告知。至于算法所披露的详尽程度，从上述规定来看，至少应当包括“基本原理、目的意图、运行机制”等算法的决定性因素。

例如，国内某头部外卖平台即在2021年9月首次公开骑手配送中“预估到达时间”的算法规则，其中并未披露技术细节，但对于基本原理（四层算法模型）、目的意图（为骑手提供充裕送餐时间）、运行机制（在模型预估时间的基础上增加三层保护时间）均予以告知。2022年8月12日，网信办官网公布首批境内互联网信息服务算法备案信息，包括公开了各算法的公示内容，涵盖基本原理、运行机制、应用场景、目的意图四大方面。

尽管相关规定和监管尺度尚属观察阶段，我们理解关于自动化决策透明度要求的监管红线将始终聚焦于用户，企业可结合网信办公布的各互联网信息服务算法备案信息表述，参考行业实践水位，据此部署显著明确、易于用户理解的自动化决策规则公开机制。

6.难点六：重要互联网平台的义务主体定位

平台治理一直是近期的监管重点和难点，除《中华人民共和国反垄断法》《关于平台经济领域的反垄断指南》等规定从反垄断的层面提供规制思路外，《个保法》第五十八条则从个人信息保护层面对提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者提出了特殊合规义务。然而，此等合规义务在实务的落实过程中也出现了障碍，核心问题在于：

- 企业对于自身是否构成《个保法》第五十八条项下的义务主体的判断，即如何准确界定企业是否构成《个保法》规制的重要互联网平台？是单纯以用户数量？还是同时需要考虑其他因素？

值得关注的是，在《个保法》正式生效

的三天前，国家市场监督管理总局于2021年10月29日发布了《互联网平台分类分级指南（征求意见稿）》（以下简称**“《分类分级指南》”**）《互联网平台落实主体责任指南（征求意见稿）》，其中《分类分级指南》明确了平台的分级依据，即“综合考虑用户规模、业务种类以及限制能力”。其中，用户规模即平台在中国的年活跃用户数量，业务种类即平台分类涉及的平台业务，限制能力即平台具有的限制或阻碍商户接触消费者的能力。而就企业最为关心也是最易被量化的判断标准——用户规模而言，《分类分级指南》提出“超级平台”的标准为在中国的年活跃用户**不低于5亿**，“大型平台”的年活跃用户**不低于5000万**。

尽管该《分类分级指南》系由市场监管总局而非网信办等个人信息专门主管部门发布，且其未明确指出适用于《个保法》第五十八条的判断。但我们理解此等关于“大型平台”和“超级平台”用户规模的具体标准可作为企业判断自身是否构成第五十八条义务主体的参考，并据此尽快开展相关合规义务的部署和准备。例如，部分企业均于近期表示将成立“个人信息保护外部监督委员会”，并公开招募隐私保护监督员，此即履行《个保法》第五十八条第一款第（一）项“成立主要由外部成员组成的独立机构对个人信息保护情况进行监督”的合规要求。

针对目前关于《个保法》理解和适用中的前述重难点问题，企业应当尽快做好准备，迎接我国个人信息保护新纪元。

PART 003

七条合规指引

企业在开展个人信息保护合规部署过程中出现的合规难点问题有赖于行业的共同探索，也有待于监管执法的进一步明确。针对目前关于《个保法》理解和适用中的前述重难点问题，我们提出如下合规路径，企业应当尽快做好准备，迎接我国个人信息保护新纪元。

— 企业需首先关注2C端网络产品等易受用户投诉及监管关注的高风险场景，并进行集中治理，积极采取有效措施尽快取得阶段性合规成果，避免直接触发相应民事、行政、甚至刑事责任。

— 企业需在梳理内部所有个人信息处理活动的基础上，首先厘清是否存在同意及合同之外的其他法律基础，其次明确产品或服务的基本业务功能和扩展业务功能，再对法律基础是订立或履行合同的必要抑或是同意加以区分，同时在内部及时做好记录工作。

— 单独同意仅基于以同意作为个人信息处理活动的法律基础，企业仅需以达到单独提示用户、用户单独选择的效果标准出发，确保用户充分知悉该个人信息处理活动的目的、方式和范围。

— 对外提供、委托处理和共同处理系三种并列而非隶属的模式，企业可依据《个保法》履行不同程度的告知义务；对于委托处理不必告知第三方具体信息，但原则上仍应逐项告知委托处理的具体场景。

— 本地化存储及跨境传输相关细则仍有待进一步明确，企业可根据《评估办法》对自身用户量及个人信息处理量级进行统计，及时履行数据出境安全评估相关义务；若未触发数据出境安全评估义务情形，则可参照《认证规范》与《个人信息出境标准合同规定（征求意见稿）》，与境外接收方签署标准合同或进行个人信息出境认证；同时关注法律法规进展，以提前准备应对措施。

— 企业对于自动化决策规则的告知不必披露技术细节，但应以显著明确、易于用户理解作为核心，并包括“基本原理、目的意图、运行机制”等算法的决定性因素。

— 企业可结合《分类分级指南》，从用户规模、业务种类、限制能力等层面综合认

企业应当理性处理，积极应对，明确数据合规道阻且长，在风险导向的方法论指导下，及时转化外部法律要求为内部合规规范。

定自身是否构成《个保法》第五十八条的义务主体，并据此履行重要互联网平台在个人信息保护层面的合规要求。

面对纷繁复杂的《个保法》及配套法规的法定要求以及日趋严格的监管态势，企业应当理性处理，积极应对，明确数据合规道阻且长，在风险导向的方法论指导下，及时转化外部法律要求为内部合规规范，建立数据合规风险长效识别与治理机制，从而能够在控制风险的前提下为数字化业务发展保驾护航。

（焦雅婷对此文亦有贡献）

陈际红
合伙人
知识产权部
北京办公室
+86 10 5957 2003
chenjihong@zhonglun.com

中国版《标准合同条款》揭开面纱，能否成为个人信息出境的通途？

陈际红 吴佳蔚 陈煜烺

我们理解，标准合同条款可能会成为个人信息跨境处理活动中最基础和最为普遍采用的一种合法路径。

国家互联网信息办公室于6月30日公布《个人信息出境标准合同规定（征求意见稿）》（“**标准合同规定**”），并公开征求意见，中国版的标准合同条款揭开面纱。自2021年11月1日《个人信息保护法》（“**个保法**”）生效，关于第三章所确立的个人信息跨境提供的规则的落地细则，即成为社会关注的焦点。在个保法第三章所确立的三项个人信息跨境传输机制中，数据出境安全评估属于法定适用，只要达到法律规定的条件，就必须申报数据出境安全评估；对于认证机制，属于国家推荐的自愿性的认证，主要适用于具有稳定管理或业务关系的跨国公司或关联公司间的个人信息跨境处理；而对于标准合同条款，由于其适用场景的广泛性和应用的便捷性，成为企业最为关注的一种机制。我们理解，标准合同条款可能会成为个人信息跨境处理活动中最基础和最为普遍采用的一种合法路径。

本文也将聚焦网信办发布的《个人信息出境标准合同》（“**标准合同条款**”）中为个人信息处理者和境外接收方设定的责任和义务，以及为个人信息主体作为第三方受益人所设定的权利，并对标准合同条款中关于个人信息保护影响评估、境外接收方再转移以及双方责任分配等重点进行探讨，以期为立法及企业实践提供借鉴和参考。

PART 001

合同目标：实现同等保护原则

在网信办公布的标准合同条款的起始段落，就开宗明义地阐明了标准合同条款的目标追求，即“为了确保境外接收方处理个人信息的活动达到中华人民共和国相关法律法规规定的个人信息保护标准”，标准合同条款实质上是实施个保法所确立的同等保护原则的一种手段或机制。即，考虑到境外接收方所在国家或地区在个人信息保护立法或执法保护水平上存在的不足，通过标准合同条款，把个保法等法律法规所确立的个人信息保护基准要求转化为对境外接收方具有法律约束力和可执行的合同条款。

标准合同条款是一种纳入强监管的合同，为了达到同等保护的目标，在标准合同条款的实施机制中，极大地限缩了合同意

标准合同条款机制与安全评估机制构成了两个层次的个人信息跨境处理的规则：标准合同条款的适用场景、安全评估适用的场景。

思自治的空间。比如，标准合同规定第二条规定，个人信息处理者与境外接收方签订与个人信息出境活动相关的其他合同，不得与标准合同条款相冲突；标准合同条款第九条第（一）项规定，如果本合同在达成或签订时与合同双方已存在的任何其他协议发生冲突，本合同的条款优先适用。虽然标准合同条款看似也预留了一块“自留地”，即附件二双方约定的其他条款，供双方在标准合同条款之外进行额外的约定，但是，附件二的条款不能与标准合同条款本身冲突，也不能规避标准合同条款的实施，更不能限缩个人信息主体所享有的权益。

尽管以上，标准合同条款仍属于合同性质，对于合同双方的争议解决仍采用了民事争议惯用的解决机制：仲裁或者诉讼。考虑到标准合同条款的履行与中国具有最直接的关联性，标准合同条款规定诉讼必须在中国法院开展，仲裁可以选择中国国际经济贸易仲裁委员会、中国海事仲裁委员会或北京仲裁委员会，亦或选择《承认及执行外国仲裁裁决公约》成员的仲裁机构。如此规定仲裁方式，一方面是给予双方一定的意思自治空间，增加合同双方利益的平衡性，另一方面也保证仲裁解决能通过公约加以执行，进而确保标准合同条款的可执行性。当然，标准合同条款要适用中国法。

PART 002

适用场景：与安全评估构成两层次适用规则

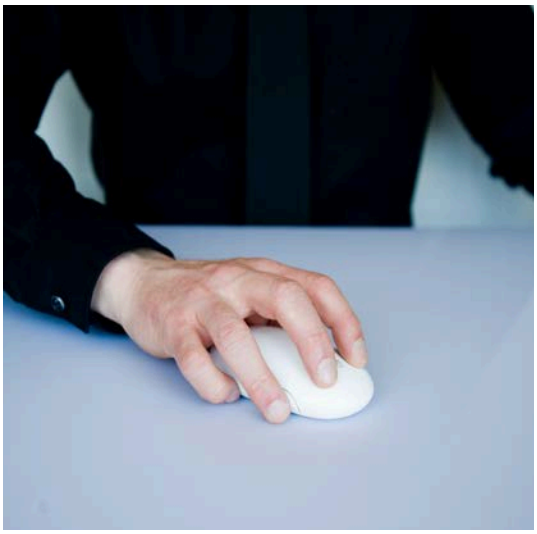
依照标准合同规定的要求，我们可以理解，标准合同条款机制与安全评估机制构成了两个层次的个人信息跨境处理的规则：

第一层次，即标准合同条款的适用场景：（一）非关键信息基础设施运营者；（二）处理个人信息不满100万人的；（三）自上年1月1日起累计向境外提供未达到10万人个人信息的；（四）自上年1月1日起累计向境外提供未达到1万人敏感个人信息的。以上四个条件要同时满足，一旦任一条件不满足，就会强制性地触发安全评估机制的适用。因此，标准合同条款适用于非特殊身份（**CIIO**）的个人信息处理者，且数据处理数量不超标（分别对应100万、10万和1万）的场景。

第二层次，即安全评估适用的场景。简

单理解，对于除标准合同条款可适用的场景，就会强制性触发安全评估要求。与标准合同规定的首要立法宗旨（保护个人信息权益）不同，《数据出境安全评估办法》的立法宗旨还增加了“维护国家安全和社会公共利益”，即数据出境安全评估将重点评估数据出境活动可能对国家安全、公共利益、个人或者组织合法权益带来的风险。可见，安全评估既评估个人信息主体权益的保障，更重要地，还要评估国家安全和公共利益风险。当然，安全评估机制的监管要比标准合同条款更为严格。

关于标准合同条款适用标准的数量的计算，我们理解如下：



关于“处理个人信息不满100万人”，指的是境内个人信息处理者目前所处理个人信息包含的总人数不足100万，而非指个人信息的条数。另外，100万总数的计算，不是按照业务线或产品线来计算，而是按照个人信息处理者的实体来计算。若涉及集团公司或关联公司的，如果各个公司是独立法人，且各个关联公司处理数据活动没有数据混同或融合的情形，我们倾向于认为应当按照独立实体各自的数量来计算，而非整个集团来计算。

关于“自上年1月1日起累计向境外提供未达到10万人个人信息”，指的是出境个人信息所涉总人数的累计计算，且累计期限为两年。此种累计计算的方式，有一种定期清零的效果，对很多中小企业来讲是个利好的安排。关于1万人敏感个人信息的计算，逻辑一致。

如果在标准合同条款有效期间，个人信息处理者所处理的个人信息或跨境累计的个人信息超过规定数量应如何处理呢？比如，境内的个人信息处理者业务得到发展，处理的个人信息量超过了100万人，或者在两年期间，累计向境外传输的个人信

标准合同条款虽是合同性质，但涉及到个保法同等保护原则的适用，因此，个人信息监管机构对标准合同条款的实施也设定了若干监管手段。

息超过了10万人或1万人（敏感个人信息）。我们理解，此种情形下，标准合同条款适用的前提条件已经不复存在，标准合同条款需要转化为安全评估机制，如此，个人信息跨境处理才可以继续。我们也期待在后续的修改中，网信办能够对此问题进一步明确。

PART 003

监管抓手：合同备案与设定接受监管的合同义务

标准合同条款虽是合同性质，但涉及到个保法同等保护原则的适用，因此，个人信息监管机构对标准合同条款的实施也设定了若干监管手段：

一是标准合同条款的备案。按照标准合同规定第七条规定，个人信息处理者应当在标准合同生效之日起10个工作日内，向所在地省级网信部门备案。备案应当提交所签署的标准合同及个人信息保护影响评估（**PIA**）报告。个人信息处理者对所备案材料的真实性负责。根据标准合同规定第十二条规定，未履行备案程序或者提交虚假材料进行备案的，会导致相应的法律责任。备案程序不影响合同的效力，标准合同条款一旦签署即生效并可以开始执行。我们理解，标准合同规定所要求的备案程序，是为了将跨境个人信息处理活动纳入监管机构的视野，并对监管机构保持透明性，这也是监管机构开展监管执法的依据。

二是标准合同条款设定了境外接收方接受监管的义务。标准合同条款第三条规定了境外接收方的义务，第一款第（十二）项规定，（境外接收方）同意在监督本合同实施的相关程序中接受监管机构的监督管理，包括但不限于答复监管机构询问，配合监管机构检查，服从监管机构采取的措施或作出的决定，并提供已采取必要行动的书面证明。我们理解，标准合同条款通过合同条款设定了境外接收方接受监管的义务，等同于把个保法规定的监管权力通过合同义务延伸到境外。

另外，标准合同条款亦设定了个人信息处理者应配合监管的义务。毫无疑问，个人信息处理者在境内处理个人信息，适用个保法，必须依法接受监管机构的监管，此乃法定义务。标准合同条款规定，个人信息

关于监管程序中的举证义务，标准合同条款要求个人信息处理者承担证明本合同义务已经履行的举证责任。

处理者亦有义务答复来自监管机构关于境外接收方的个人信息处理活动的询问。也就是说，个人信息处理者仍是监管机构进行标准合同条款监管的主要抓手。

关于监管程序中的举证义务，标准合同条款要求个人信息处理者承担证明本合同义务已经履行的举证责任。反过来讲，如果个人信息处理者举证不能，就可能要承担监管处罚的后果。这一举证责任的安排，要求个人信息处理者在个人信息处理过程中，要配备必要的评估、记录程序，做到合规看得见。而对于境外的接收方，标准合同条款也要求其对开展的个人信息处理活动进行客观记录，保存记录至少三年；按相关法律法规要求直接或通过个人信息处理者向监管机构提供相关记录文件。

PART 004

国际视野：标准合同条款与GDPR SCCs的横向比较

对个人数据跨境传输的监管一直是欧盟数据保护立法框架下的重点，相关监管制度体系早于1995年颁布的《第95/46/EC号保护个人在数据处理和此类数据自动流动中权利的指令》（以下简称为“**95指令**”）中就已确立。欧盟《通用数据保护条例》（*General Data Protection Regulation*，以下简称为“**GDPR**”）又在此基础上进行了完善。GDPR项下常用的个人数据跨境传输保障机制主要包括充分性决定（Adequacy Decision）、具有约束力的公司规则（Binding Corporate Rules，**BCRs**）和标准合同条款（Standard Contractual Clauses，**SCCs**）。充分性决定适用于欧盟委员会认定某一国家/地区等具备充分的个人数据保护水平的情形，个人数据可以向此类国家/地区传输且无需特别授权；具有约束力的公司规则适用于集团内部之间的个人数据传输，但须经监管机构批准；签订欧盟委员会制定的向第三国转移个人数据的标准合同条款是当前企业广为采用的传输保障机制。

考虑到很多国际企业和在欧盟市场开展业务的中国公司多采用SCCs作为跨境传输机制以满足GDPR的要求，我们对比了中国版标准合同条款与GDPR SCCs的主要异同，以期为国内立法及企业实践提供借鉴和参考。

中国版标准合同条款与GDPR SCCs在适用场景、前置条件、责任分配方式、对目标国建的监管关注度规定有所不同。

	个人信息出境标准合同	GDPR SCCs
适用场景不同	(1)不区分个人信息处理者与境外接收方的数据处理关系; (2)不论境外接收方是否会适用个保法[1]。	(1)根据数据传输方(data exporter)与数据接收方(data importer)关系的不同,共有四种不同的模式(module); (2)若数据接收方适用GDPR,则无法适用此SCCs作为数据跨境传输保障机制[2],可能需签署监管机构将来针对此场景发布的其他文本[3]。
前置条件不同	(1)需**同时满足**四项条件(即不需要进行安全评估):①非CIIO;②处理个人信息不满100万人;③自上年1月1日起累计向境外提供未达到10万人个人信息;④自上年1月1日起累计向境外提供未达到1万人敏感个人信息。 (2)个人信息处理者需事先进行PIA。	(1)适用SCCs作为数据传输保障机制并无严格意义上前置条件的要求; (2)数据跨境传输并不属于必须进行数据保护影响评估(DPIA)的场景; (3)欧盟监管机构也在强调对于数据跨境传输活动进行风险评估及采取有效措施降低跨境传输风险的思路[4]。
责任分配方式不同	不论个人信息处理者与境外接收方的数据处理关系,在不同场景下个人信息处理者与境外接收方承担的义务相同(委托处理场景下略有不同[5])。	根据数据传输方与数据接收方关系的不同,实际意味着数据传输对于数据接收方控制力的不同,在不同的模式下双方所需承担的义务存在差异。
对目标国家的监管关注度不同	在评估境外接收方所在国家/地区当地个人信息保护政策法规对合同条款的影响时,需考虑境外接收方是否曾收到其所在国家/地区公共机关要求其提供个人信息请求及境外接收方应对的情况。	(1)同我国,需考虑数据接收方应对其所在国家/地区公共机关要求其提供个人信息请求的情况; (2)特别地,SCCs第三节规定了在公共当局提出查阅数据请求的情况下当地的法律和义务(local laws and obligations in case of access by public authorities)。当数据接收方收到公共当局具有法律约束力的请求时,应当立即通知数据传输方,并在可能的情况下通知数据主体。

1.此处由于目前征求意见稿的适用条件并未明确此点,有可能会导致境外已适用《个保法》的处理者受到重复的义务约束。
2.EU Commission THE NEW STANDARD CONTRACTUAL CLAUSES – QUESTIONS AND ANSWERS, Q23
3.EDPB Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR (version for public consultation)
4.然而,由于近年来"Schrems II"相关案例争议的影响,实质性达成充分性保护水平成为EDPB监管的重点,具体体现在: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 Adopted on 18 June 2021
5.第三条 境外接收方的义务(八)

中国版标准合同条款与GDPR SCCs在法律管辖、适用范围、监管要求等方面规定有所不同。

	个人信息出境标准合同	GDPR SCCs
法律管辖不同	适用中华人民共和国相关法律法规。	根据适用模式的不同，适用法律可能存在差异[6]： (1)在controller-controller，controller-processor，processor-processor模式下，所适用的法律须为EU/EEA成员国的法律。尤其是在controller-processor以及processor-processor模式下，所适用的法律应当是数据传输方所在国的法律； (2)在processor-controller模式下，所适用的法律有可能不是EU/EEA成员国的法律。
适用范围不同	(1)原则上应只适用于签署标准合同的双方。 (2)如果境外接受方再向境外第三方提供个人信息，必须获得单独同意且要达成新的书面协议。	(1)原则上应只适用于签署SCCs的双方； (2)通过对接条款(docking clause)可以使第三方后续以数据传输方或接收方的身份加入SCCs。
监管要求不同	(1)备案要求：生效后10个工作日内需向所在地省级网信部门备案； (2)日常监管：在合同履行期内，如果省级网信部门发现实际个人信息出境活动不再符合个人信息出境要求，会要求个人信息处理者终止个人信息出境活动。 (3)可以对境外接收方进行询问、检查，境外接收方要服从监管措施或决定。	暂无。 需要注意的是，Schrems II案后，对于适用SCCs作为数据传输保障机制的情形可能需要进行个案评估[7]。
其他	(1)其他合同不得与标准合同条款相冲突；发生冲突，标准合同条款优先适用。 (2)附件二可以进行不与标准合同条款冲突的增补约定。	(1)原则上不可以对SCCs文本进行修改(适当合理的调整除外)； (2)可以将SCCs纳入一个范围更广的商业合同进行签署，前提是合同条款不可与SCCs相冲突[8]。

6.EU Commission THE NEW STANDARD CONTRACTUAL CLAUSES – QUESTIONS AND ANSWERS, Q33
7.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 Adopted on 18 June 2021)
8.EU Commission THE NEW STANDARD CONTRACTUAL CLAUSES – QUESTIONS AND ANSWERS, Q7 & 8

标准合同条款是一种纳入强监管的合同，个人信息处理者和接收方必须履行标准合同条款的约定义务。

PART 005

个人信息处理者和境外接收方的义务设定

根据标准合同规定，标准合同条款具有优先适用性[9]，个人信息处理者还应将标准合同向所在地省级网信部门备案，而省级网信部门且有权在跨境传输过程中进行监督，并有权要求终止个人信息出境活动。据此，标准合同条款是一种纳入强监管的合同，**个人信息处理者和接收方必须履行**标准合同条款的约定**义务**，否则将不仅面临违约责任，更将面临民事侵权或行政监管责任。

（一）个人信息处理者：适用个保法基础上的责任强化

标准合同条款第一条第（四）款即明确，“个人信息处理者”与《个保法》所规定的含义相同，个人信息处理者首先适用个保法并需遵循个保法所设定的一系列合规义务，且标准合同条款针对跨境活动所设定的各种义务亦适用。

针对标准合同条款为个人信息处理者设定的各项合同义务，我们梳理如下表。

序号	义务要点	义务内容
（一）	合法必要	－个人信息需按照相关法律法规进行收集、使用等处理； －出境个人信息范围仅限于实现处理目的所需的最小范围。
（二）	告知； 合法性基础	－向个人信息主体告知境外接收方的基本情况以及其他跨境处理个人信息的规则； －依法取得个人信息主体（或14周岁以下未成年人父母/监护人）单独同意/书面同意（法律法规另有规定除外）。

9.即标准合同规定第二条规定，个人信息处理者与境外接收方签订与个人信息出境活动相关的其他合同，不得与标准合同条款相冲突；标准合同条款第九条第（一）项规定，如果本合同在达成或签订时与合同双方已存在的任何其他协议发生冲突，本合同的条款优先适用。

序号	义务要点	义务内容
（三）	特殊告知要求	告知个人信息主体作为第三方受益人：未在30天内明确拒绝，则推定其同意。
（四）	监督义务	－监督境外接收方履行义务； －监督境外接收方采取相应技术、管理措施。
（五）	提供规范副本	应境外接收方要求，向其提供相关法律规定和技术标准副本。
（六）	配合监管	答复监管机构（关于境外接收方）询问（另有约定除外）。
		应监管要求，依法提供境外接收方的相关信息，包括审计结果。
（七）	个人信息保护影响评估	－提前依法开展个人信息保护影响评估； －保存报告至少3年。
（八）	提供合同副本	经个人信息主体要求，提供个人信息出境合同副本（机密信息可适当遮蔽，但须提供有效摘要帮助理解）。
（九）	承担举证责任	承担证明个人信息出境合同义务已履行的举证责任。

由于个人信息处理者需直接适用个保法，针对上述合同义务中与个保法相一致的部分，本文不再赘述；关于其他部分，我们认为需重点关注的问题如下：

1. 合法性基础：明确单独同意要求

标准合同条款第二条第（二）款规定，个人信息处理者向境外提供个人信息应当取得个人单独同意，但相关法律法规规定不需要取得个人单独同意的除外。个保法第十三条设定了处理个人信息的七项合法性基础，其中即包括履行合同所必需等同意之外的其他合法性基础。然而，个保法第

企业或可在选用标准合同机制后，通过更新隐私政策等形式以实现告知义务。

三十九条规定跨境提供个人信息应取得单独同意，且未设定例外情形。

个保法第三十九条的现有表述直接导致了法律适用和理解上的争议，即，如果企业已具备其他合法性基础，是否在跨境个人传输中还必须履行单独同意的要求?对于这一点，标准合同条款第二条第（二）款的规定或许在一定程度上已给出答案，即：如果个人信息处理者已具备“法律法规规定的例外情形”，那么无需取得个人单独同意。标准合同条款的上述规定是否已实质蕴含了“如已具备同意之外的合法性基础，则无需就跨境再获单独同意”，目前还有待进一步明确。

2.透明性要求：告知个人信息主体为第三方受益人

标准合同条款第二条第（三）款规定，个人信息处理者应当向个人信息主体告知其与境外接收方通过标准合同条款约定个人信息主体为第三方受益人，此乃标准合同条款就透明性要求层面在个保法第十七条和第三十九条基础上的进一步增强告知。

实践中，企业往往通过隐私政策等形式向用户告知关于跨境处理个人信息的规则，考虑到标准合同条款未来可能会成为个人信息跨境处理活动中最基础和最为普遍采用的一种合法路径，**企业或可在选用标准合同机制后，通过更新隐私政策等形式以实现此等告知义务。**

3.举证责任：个人信息处理者应证明合同义务已履行

标准合同条款第二条第（九）款规定由个人信息处理者承担标准合同条款已履行的举证责任。如上文所述，根据该规定，如果个人信息处理者举证不能，就可能要承担监管处罚的后果，而这一举证责任的安排，要求个人信息处理者在个人信息处理过程中，要配备必要的评估、记录程序，做到合规看得见。

具体而言，企业如作为个人信息处理者，一方面自身应依法就跨境活动开展个人信息保护影响评估并记录相关个人信息处理活动，并保留相关材料；另一方面，可充分利用标准合同条款为境外接收方所设定的义务，并确保义务履行全过程的可追溯、可记录。例如：

- 监督境外接收方是否履行义务，是否采取技术和管理措施【标准合同条

由于境外接收方所处的政策法律环境不同，标准合同条款据此也从形式上为境外接收方设定了更多、更严苛的合同义务。

款第二条第(四)款】；

- 查阅境外接收方的数据文件和文档，并对其数据处理活动开展合规审计，要求其提供已获资质认证情况【标准合同条款第三条第(十)款】；
- 要求境外接收方对个人信息处理活动进行记录并保存至少3年，并根据法律法规规定要求其提供相关记录文件【标准合同条款第三条(十一)款】。

(二)境外接收方：通过合同实现同等保护原则

相比个人信息处理者，由于境外接收方所处的政策法律环境不同，标准合同条款据此也从形式上为境外接收方设定了更多、更严苛的合同义务(例如自动化决策)，进而从实质上使境外接收方达到个保法规定的同等保护水平。

针对标准合同条款为个人信息处理者设定的各项合同义务，我们梳理如下表。

序号	义务要点	义务内容
(一)	依约处理个人信息	依照约定处理个人信息，除非另行取得个人信息主体事先同意。
(二)	提供合同副本	应个人信息主体要求，提供个人信息出境合同副本(机密信息可适当遮蔽，但须提供有效摘要帮助理解)。
(三)	最小必要	出境个人信息范围仅限于实现处理目的所需的最小范围。
(四)		- 存储个人信息的期限为实现处理目的所必要的最短时间； - 删除/匿名化超期存储个人信息及其备份(取得个人信息主体单独同意除外)； - 向个人信息处理者提供删除/匿名化相关审计报告(如为受托处理)。
(五)	安全	采取有效技术、管理措施，最小授权访问、操作控制策略等保障个人信息安全。

序号	义务要点	义务内容
（六）	个人信息泄露事件处置	－及时采取补救措施； －立即通知个人信息处理者，并依法报告监管机构； －依法通知个人信息主体（受托处理者除外）； －记录并留存事件事实、影响与补救措施。
（七）	跨境再传输限制	原则上不应将个人信息提供至第三国，除非同时满足： ①业务必要； ②已履行个保法的告知要求，并具备合法性基础； ③与第三方达成书面协议，确保其第三方满足同等保护原则； ④承担再提供导致的连带责任； ⑤向个人信息处理者提供与第三方书面协议副本。
（八）	转委托限制	－事先取得个人信息处理者同意； －确保转委托方在约定范围内处理个人信息； －监督转委托方。
（九）	自动化决策	满足个保法关于自动化决策的要求。
（十）	接受监管	－向个人信息处理者提供必要的信息以证明已遵循合同义务； －允许并协助个人信息处理者查阅相关资料、进行审计； －应个人信息处理者要求提供资质认证情况。
（十一）		－记录并保存个人信息处理活动至少3年； －依法直接或间接向监管机构提供记录文件。
（十二）		同意接受中国监管机构监督管理。

关于境外接收方的义务，主要有如下问题可重点关注：

1. 改变合同范围处理个人信息

标准合同规定第三条第（一）款和第（四）款规定，境外接收方应当在标准合同条款约定范围内处理个人信息，除非已取得个人信息主体的事先同意；并且应当在实现处理目的所必要的最短时间内存储个

标准合同条款对最具特殊性——无法决定数据处目的、方式的境外接收方受托处理情形作进一步明确。

人信息，除非已取得个人信息主体关于存储期限的单独同意。

从个人信息权利保护的角度分析，二者在同意的方式上存在差别。针对个人信息处理行为，如果境外接收方需改变处理活动，则应取得事先的同意，我们理解此种情形下境外接收方将就改变部分的处理活动构成单独的个人信息处理者，因此就该部分的合法性基础应由境外接收方取得；而就处理活动中的存储行为，实践中往往可能出于其他业务目的而需在本合同约定的必要存储时间之外继续存储，则应就此部分取得单独同意。

从民事合同法律关系的角度考虑，如果境外接收方超过标准合同条款约定的范围处理和存储个人信息，但已获得个人信息主体的有效同意，对于这部分合同之外的处理活动是否可能构成违约？从目前标准合同条款的设计来看，**如果境外接收方对这部分合同之外的处理活动已取得同意，那么也应当属于本合同执行的预期范围内；但如果其未履行上述要求，则可能构成违约，而个人信息处理者亦可能对其行为向个人信息处理承担民事责任**（具体见下文“九、责任分配”部分）。

2. 受托处理个人信息的特殊要求

相较GDPR SCCs根据数据出境方与境外接收方所形成的不同数据处理关系划分为四种个人信息跨境传输模式（C-C,C-P,P-P,P-C）[10]，标准合同条款未就缔约双方的数据处理关系做进一步划分。根据我国个保法关于共同处理、委托处理、向第三方提供（有可能构成较为独立的处理关系）的数据处理关系设定及责任承担机制，不同处理关系下的权利义务应当有不同。尽管未作上述区分，标准合同条款仍对其中最具特殊性——无法决定数据处理目的、方式的境外接收方受托处理情形作进一步明确。包括：

- 在删除或匿名化个人信息后，向个人信息处理者提供审计报告【标准合同条款第三条第（四）款】；
- 如境外接收方受托处理时发生个人信息泄露事件，应由个人信息处理者通知个人信息主体【标准合同条款

10.具体包括：1）控制者向控制者传输的“C-C模式”；2）控制者向处理者传输的“C-P模式”；3）处理者向处理者传输的“P-P模式”以及4）处理者向控制者传输的“P-C模式”。

个人信息主体可以向个人信息处理者或境外接收方中的任意一方行使权利，而不论缔约双方的数据处理关系。

第三条第（六）款】；

- 如欲转委托第三方处理个人信息，则应事先获得个人信息处理者同意，同时应确保第三方的处理活动在本合同约定范围内，并对其进行监督【标准合同条款第三条第（八）款】。

3. 域外监管效力的设定

除上述面向个人信息处理者和个人信息主体的义务外，标准合同条款第三条第（十二）款还设定了境外接收方同意接受中国监管机构监督的承诺，包括但不限于答复监管机构询问，配合监管机构检查，服从监管机构采取的措施或作出的决定，并提已采取必要行动的书面证明，我们理解上述规定实际上是对境外类似长臂管辖要求的回应。

PART 006

个人信息主体权利：法定权利基础上增设第三方受益人

结合标准合同条款，个人信息主体可以要求获得签署的标准合同条款的副本【第二条第（八）款】，亦有权（在未表示拒绝的情况下）向缔约双方行使如下权利：

- 执行标准合同条款中关于个人信息保护义务【第五条第（一）款】；
- 提供标准合同副本【第二条第（八）款；第三条第（二）款】；
- 确认境外接收方所在国有关个人信息保护的政策法规对履行标准合同的影响（第四条）；
- 通过投诉、诉讼等方式获得救济【第六条第（三）款】；
- 在法定要件发生时主张解除标准合同【第七条第（三）款】。

就行权/追责对象，根据标准合同条款第五条第（二）款，个人信息主体可以**向个人信息处理者或境外接收方中的任意一方行使权利，而不论缔约双方的数据处理关系。**

就救济途径，标准合同条款第六条第

标准合同条款要求个人信息处理者应当针对跨境活动开展个人信息保护影响评估，并增加了评估境外接收方当地个人信息保护政策对遵守标准合同条款可能造成的影响。

（一）款要求境外接收方在**组织内部确定联系人**以答复并及时处理个人信息主体的询问或投诉，并**通过单独通知或在官网公告的形式告知个人**信息主体该联系人信息。

PART 007

个人信息保护影响评估（PIA）

与《个保法》第五十五条、《数据出境评估办法》一脉相承，标准合同条款第二条第（七）款要求个人信息处理者应当针对跨境活动开展个人信息保护影响评估（personal information protection impact assessment，**PIA**），并在《数据出境评估办法》第五条的基础上增加了评估境外接收方当地个人信息保护政策对遵守标准合同条款可能造成的影响。结合个保法，参考《数据出境评估办法》等，总的来说，针对个人信息出境活动进行PIA主要需评估以下内容：1）个人信息出境活动的具体情况及相应的合法性、正当性、必要性；2）个人信息出境活动对个人信息主体权益的影响；3）个人信息处理者的数据安全保障能力；以及4）境外接收方的数据安全能力情况，包括所在国家/地区所在地的法律环境。

这一规定与Schrems II案后欧盟数据保护委员会（**EDPB**）所发布的建议[11]，及据此更新的GDPR SCCs中要求在依据SCCs作为数据跨境传输保障机制时对数据跨境传输进行评估（transfer impact assessment，**TIA**）的要求十分类似，尤其强调要评估第三国的数据保护法律或实践，以保证数据接收方可以达到与传输方所在国家/地区的同等保护水平。需要注意的是，数据跨境传输并不属于GDPR项下必须进行数据保护影响评估（data protection impact assessment，**DPIA**）的场景[12]，但TIA同样运用了DPIA的基本原理和方法论。

对于如何评估境外接收方当地个人信息保护政策法规对履行合同的影响，标准合同第四条规定需考虑出境的具体情况、境外接收方所在国家/地区的个人信息保护政策法规以及境外接收方的安全管理制

11.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
12.GDPR Art 35
WP 29 Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679

标准合同在第三条境外接收方的义务中规定，境外接收方仅在同时满足特定条件时方可将个人信息提供给相关境外第三方。

度和技术手段保障能力。结合第四条的规定，参考EDPB相关建议[13]及其生效后部分实践，在评估境外接收方所在国家/地区个人信息保护相关法律环境时，至少需要考虑以下因素：1）当地现行的个人信息保护法律法规；2）加入区域或全球个人信息保护组织或做出相关国际承诺的情况；3）当地落实个人信息保护的机制；4）当地行政、监管或司法程序等要求调取个人信息的情况；5）个人信息主体在当地寻求司法救济的可行性等。

PART 008

境外再转移

对于境外接收方可能将个人信息提供给位于中华人民共和国境外第三方的情形，标准合同在第三条境外接收方的义务中规定，境外接收方仅在同时满足以下条件时方可将个人信息提供给相关境外第三方：1）确有业务必要；2）满足个保法等相关法律法规对于告知及同意的要求；3）与第三方达成书面协议，确保第三方具备同等的保护水平，与第三方承担连带责任；4）向个人信息处理者提供协议副本；以及5）事先征得个人信息处理者同意（仅在受个人信息处理者委托处理个人信息时转委托第三方处理的情形下）。

对比GDPR SCCs对于境外再转移的规定，二者间具有相似性：

1）再转移的第三方位于中华人民共和国或EU/EEA境外；

2）本质上是要求再转移的第三方可以保证同等的保护水平。

但与GDPR SCCs不同的是：

1）由于标准合同的适用并不区分个人信息处理者与境外接收方之间的数据处理关系，导致无论在何种情形下，境外接收方向第三方转移个人数据均遵循一致的条件，即要求该第三方满足同等保护水平（通过SCCs或充分性认定等机制），并且数据接收方需保证跨境再转移需要满足标准合同条款中其他合规保障措施，特别是目的限制的规定（仅在受个人信息处理者委托

13.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
EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures
此外，UK ICO International transfer risk assessment and tool (draft)也具有较高的参考意义。

欧盟委员会在更新SCCs时加入对接条款，在一定程度上便利数据处理过程中第三方的加入，同时也可以保证第三方的数据保护水平。

处理个人信息时转委托第三方处理的情形下要求事先征得个人信息处理者的同意）；

2）标准合同明确规定境外接收方与第三方承担连带责任，而GDPR SCCs仅在Clause 9:Use of Sub-processors中对于模式二（控制者-处理者）及模式三（处理者-处理者）下要求数据接收方须确保次级处理者（sub-processor）承担数据接收方根据SCCs所须承担的责任并就次级处理者对数据传输方义务的履行负全责；

3）标准合同中未提及境外接收方按照行政、监管或司法程序要求须向相关第三方转移个人数据的情况，对于此种情形下境外接收方如何处理仍有待进一步明确。

此外，欧盟委员会在更新SCCs时加入了对接条款（docking clauses），以便于已签署SCCs的各方在复杂的数据处理生命周期中在既有合同中加入新的签约方（既可以是数据传输方也可以是数据接收方）。新的签约方加入后，该签约方将根据其角色承担SCCs下的权利及义务[14]。我们理解，此条款将在一定程度上便利数据处理过程中第三方的加入，同时也可以保证第三方的数据保护水平。目前版本的标准合同中并无类似条款，且仅规定了境外接收方将个人信息再转移给其他第三方的情形，在履行过程中若需加入其他第三方，一方面需要严格满足标准合同所规定的条件，另一方面对于加入新的个人信息处理者（作为数据传输方）可能存在一定阻碍。

14.EU Commission THE NEW STANDARD CONTRACTUAL CLAUSES – QUESTIONS AND ANSWERS, Q11, 12, 13

个人信息处理者或境外接收方除需就自身违法行为依法对个人信息主体承担民事侵权责任或监管责任外，还将依据标准合同条款的约定对个人信息主体承担违约责任。

PART 009

个人信息处理者和境外接收方的责任分配

标准合同条款第八条规定了个人信息处理者与境外接收方之间关于违约责任的分配，值得注意的是，不同于以往“合同责任限于缔约双方”的理论架构，由于本标准合同条款设定了个人信息主体作为第三方受益人，因此，个人信息处理者或境外接收方除需就自身违法行为依法对个人信息主体承担民事侵权责任或监管责任外，还将依据标准合同条款的约定对个人信息主体承担违约责任。

就面向个人信息主体所需承担的责任，主要包括以下情形：

- **原则上，缔约双方应对自身行为承担责任：**标准合同条款第八条第（三）款规定，缔约双方因违反本合同而侵害个人信息主体作为第三方受益人而享有的权利，应当对个人信息主体承担责任；个人信息主体有权获得赔偿。
- **如果共同对损害负责，承担连带责任：**标准合同条款第八条第（四）款规定，缔约双方对因违反本合同而共同对个人信息主体造成的损害负责的，应由缔约双方承担连带责任；我们理解这可能主要是指共同处理的情形，此规定亦与个保法第二十条关于共同处理个人信息的规定相一致。
- **个人信息处理者应承担先行赔偿责任：**标准合同条款第八条第（六）款、第（七）款规定，不论缔约双方是否应最终承担连带责任，个人信息处理者均应就个人信息主体的损害负责人并承担赔偿责任；如损害系境外接收方造成，个人信息处理者有权向境外接收方追偿。

PART 010

结语

自2021年11月个保法生效后，社会即密切关注并期待个人信息跨境处理规则的早日落地。伴随《数据出境安全评估办法》《个人信息出境标准合同规定（征求意见

跨国企业有必要着手落实符合自身特点的跨境合规管理机制，为数据跨境强监管的到来做好准备。

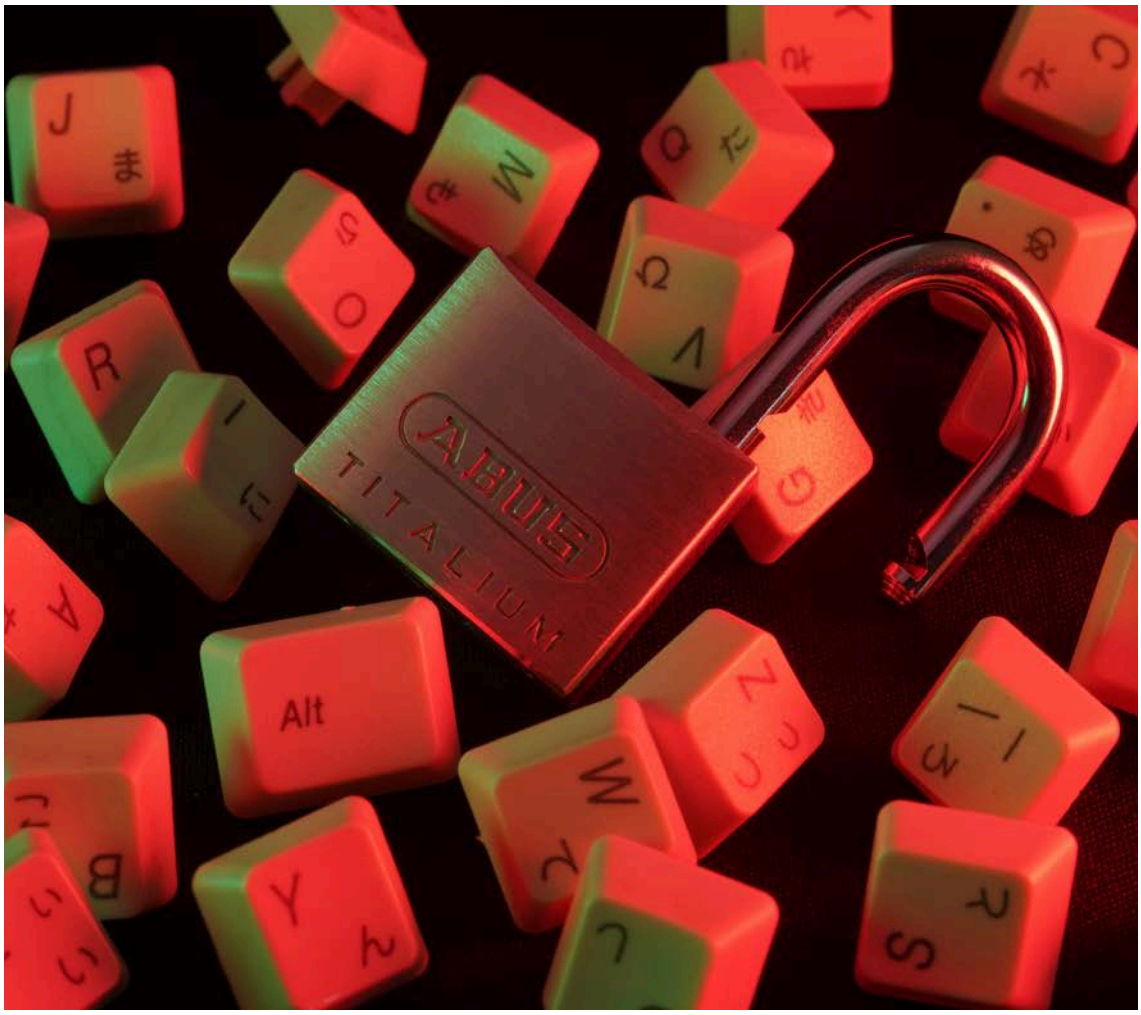
稿）》《个人信息跨境处理活动认证技术规范》的发布，我们理解，尽管部分问题及实施程序仍有待网信办进一步明确，但个保法规定的各项跨境传输机制的配套规则将会在近期逐次落地，以解决跨国企业面临的“数据跨境监管有法律规定但无执行机制”的尴尬局面，跨国企业有必要着手落实符合自身特点的跨境合规管理机制，为数据跨境强监管的到来做好准备。

（杨润对此文亦有贡献）

陈际红
合伙人
知识产权部
北京办公室
+86 10 5957 2003
chenjihong@zhonglun.com

PART TWO

《个保法》合规审计实务



权知轻重，度知长短：如何开展《个人信息保护法》项下的合规审计？

陈际红 刘连炻 韦龙杰

本文结合域外经验，提出企业开展个人信息合规审计的目标、范围、流程和组织等实施路径。

《个人信息保护法》（以下简称“**《个保法》**”）将定期合规审计确立为个人信息处理者的一项法定义务。审计，作为一项风险检视及控制的工具被广泛应用于多个行业领域，但在个人信息保护领域如何开展和实施，仍有诸多不明确之处。目前，业界普遍的困惑包括：

- 什么情况下触发合规审计？
- 审计应按照什么程序开展？
- 审计应包括的必要内容有什么？
- 内审还是外审？
- 谁是《个保法》项下的适格审计机构？
- 审计报告可用于什么目的？

本文对上述问题提出一些思考，以期为个人信息处理者落实《个保法》项下的合规审计提供参考路径。

PART 001

数据合规审计的法定要求

（一）从非强制义务到强制义务

个人信息处理者的合规审计义务并非在《个保法》中首次提出。2020年10月生效的《信息安全技术 个人信息安全规范》（以下简称“**《个人信息安全规范》**”）[1]第11.7条对个人信息处理的安全审计作出规定，将个人信息保护政策、相关规程和安全措施列为审计对象，明确了审计活动记录及留存的相关要求。然而，由于《个人信息安全规范》在效力层面仅为推荐性国家标准，该要求的实际落地情况并不尽如人意。

2021年11月1日《个保法》生效，首次在法律层面规定个人信息处理者应该对其遵守法律、行政法规的情况进行审计。《个保法》项下的审计分为个人信息处理者的自主审计和强制外部审计两种类型。具体而言：

自主审计，《个保法》第五十四条要求个人信息处理者应当定期对其处理个人信息遵守法律、行政法规的情况进行合规审计。对此条款，我们可以理解为一个限定及一个开口。所谓限定，是指审计的法律基准应当属于“法律、行政法规”层级；所谓的开口，是指未对《个保法》下的审计是内审还是外审、审计的频次予以明确。自主审计虽

1.《个人信息安全规范》之前的版本亦有类似的规定。

与《个保法》一脉相承，《网数条例》第五十八条规定了数据处理者的自主审计和强制外部审计义务。

然构成《个保法》项下个人信息处理者的强制性义务，但从立法目的来看，重在强调企业对自身的个人信息处理活动通过审计进行定期自查。因此，审计的频次、以及是否采用外部审计资源，企业可以基于风险导向原则来加以确定。

强制外部审计，《个保法》第六十四条规定，履行个人信息保护职责的部门在履行职责中，发现个人信息处理活动存在较大风险或者发生个人信息安全事件的，可以要求个人信息处理者委托专业机构对其个人信息处理活动进行合规审计。强制外部审计一方面可以利用外部独立机构的专业知识和能力，帮助个人信息处理者更客观、全面地发现、识别合规问题，明确合规差距；另一方面，外部审计机构的审计结果也可以为监管机构开展进一步的执法活动提供依据。

（二）从“个人信息”到“数据”

《个保法》生效之后，国家互联网信息办公室（以下简称“**CAC**”）于2021年11月14日发布《网络数据安全管理条例（征求意见稿）》（以下简称“**《网数条例》**”）。与《个保法》一脉相承，《网数条例》第五十八条规定了数据处理者的自主审计和强制外部审计义务，具体而言：

自主审计，要求数据处理者应当委托数据安全审计专业机构定期对其处理个人信息遵守法律、行政法规的情况进行合规审计。相较于《个保法》中的自主审计，此处的自主审计明确为外部审计；而在审计依据的效力层级上，延续了《个保法》上做出的限定，应为“法律、行政法规”。

强制外部审计，则是主管、监管部门组织开展的对重要数据处理活动的审计，主要聚焦于重要数据处理活动的安全。结合后文将展开介绍的《网数条例》第五十三条，我们也可以看出，《网数条例》将数据合规审计的对象从“个人信息”扩大到“数据”，其中“重要数据”更是监管部门的审计重点。

（三）针对大型互联网平台的特别审计义务

《网数条例》第五十三条对大型互联网平台运营者的合规审计义务做出了特别规定。相较于《个保法》，《网数条例》对大型互联网平台运营者的特别规定之处可以归纳

《网数条例》《分级指南》《平台指南》均对大型互联网平台规定了特别审计义务。

为三个关键词:“第三方审计”、“年度审计”和“审计公开”。据此,《网数条例》项下所规定的合规审计,应该由独立于大型互联网平台运营者的第三方审计机构进行,属于外审;审计的频率是每年一次;审计结果应该对外披露,接受监督。同时,《网数条例》对合规审计范围也作出了规定,应包含平台数据安全情况、平台规则和自身承诺的执行情况、个人信息保护情况、数据开发利用情况等事项。

与此同时,作为部门立法尝试,国家市场监督管理总局(以下简称“**市监总局**”)于2021年10月29日发布的《互联网平台分类分级指南(征求意见稿)》(以下简称“**《分级指南》**”)以及《互联网平台落实主体责任指南(征求意见稿)》(以下简称“**《平台指南》**”)也与此呼应。《平台指南》第八条规定,“超大型平台经营者应定期委托第三方独立机构对本指南所规定的主体责任遵守情况进行审计”,此条指向的对象是“超大型平台”。同时,《平台指南》对审计报告的内容也做出了要求,包括:(一)接受审计的超大型平台的名称、地址和联系方式;(二)开展审计活动的机构组织的名称和地址;(三)审计主要结论;(四)实现合规的操作建议。值得一提的是,《平台指南》项下的审计范围是“对本指南所规定的主体责任遵守情况”,并不限于数据合规,这也是与《个保法》《网数条例》项下的合规审计的主要区别。

(四)关于合规审计义务的总结

基于上述规定,对于我国现行法律框架下不同主体的数据合规审计义务总结如下:

我国现行法律框架规定了不同主体的数据合规审计义务。

法律依据	适用对象	自主审计/强制审计	外审/内审	触发条件	频次	审计内容	审计报告相关要求
《个保法》第五十四条	个人信息处理者	自主审计	N/A	N/A	定期	处理个人信息遵守法律、行政法规的情况。	N/A
《个保法》第六十四条		强制审计	外审	个人信息处理活动存在较大风险或者发生个人信息安全事件。	应监管部门要求	个人信息处理活动。	N/A
《网数条例》第五十三条	大型互联网平台运营者	自主审计	外审	N/A	年度	平台数据安全情况、平台规则和自身承诺的执行情况、个人信息保护情况、数据开发利用情况等。	审计结果应该对外披露。
《网数条例》第五十八条	数据处理者	自主审计	外审	N/A	定期	处理个人信息遵守法律、行政法规的情况。	N/A
	重要数据处理者	强制审计	外审	主管、监管部门组织开展	N/A	履行法律、行政法规规定的义务等情况。	N/A

法律依据	适用对象	自主审计/强制审计	外审/内审	触发条件	频次	审计内容	审计报告相关要求
《平台指南》第八条	超大型平台经营者	自主审计	外审	N/A	定期	主体责任遵守情况。	审计报告应该包括以下内容：（一）接受审计的超大型平台的名称、地址和联系方式；（二）开展审计活动的机构组织的名称和地址；（三）审计主要结论；（四）实现合规的操作建议。

图表 1 我国现行法律框架下数据合规审计义务总结

PART 002

合规审计的国际实践

2018年5月25日生效的《通用数据保护条例》（General Data Protection Regulation，“**GDPR**”）被称为“史上最严格的个人数据保护立法”。GDPR项下的第二十八条（控制者对处理者的审计）、第三十九条（DPO的任务）、第四十七条（BCR应规定数据保护审计等合规机制）及第五十八条（监管机构的审计权力）分别就审计的适用作出规定。GDPR生效至今已接近4年，相关执法标准逐渐明晰，我们也注意到多国数据保护监管机构（Data Protection Author-

各国DPA根据GDPR发布的审计标准，一方面明确了DPA自身开展数据合规审计的具体方式，同时也为相关企业开展GDPR合规工作明确了重点方向。

ity，“**DPA**”）相继发布监管审计标准，同时，数据合规审计也已被应用于GDPR的合规调查中。各国DPA根据GDPR发布的审计标准，一方面明确了DPA自身开展数据合规审计的具体方式，同时也为相关企业开展GDPR合规工作明确了重点方向，对我们开展《个保法》项下的合规审计具有一定的参考价值。

（一）英、法、德DPA发布的数据合规审计指南

1. 英国ICO

英国数据保护执法机构（Information Commissioner’s Office，“**ICO**”）就数据合规审计在官网进行了说明[2]，重点内容包括审计覆盖的范围以及ICO如何进行审计，具体如下：

审计覆盖范围	ICO如何进行审计
－数据保护治理，以及确保数据保护立法有效执行的组织架构、政策、程序； －个人信息记录的管理流程； －响应关于个人数据请求的流程； －确保个人信息记录安全的技术及组织措施； －关于员工数据保护培训及意识提升的规定及监督。	－对制度、流程进行场外审查； －对核心人员进行场外访谈及测试； －审查关于数据保护活动的KPI及管理； －对实际应用的合规流程进行现场审查； －出具报告为企业提供最佳实践及完善建议； －起草执行概要并于ICO官网发布； －在审计完成后6个月进行后续审查。

图表 2 英国ICO数据合规审计核心事项

2. 法国CNIL

法国数据保护监管机构（“**CNIL**”）于2020年9月1日发布了CNIL审计流程指南[3]。在该指南中，重点规定的事项包括：被审计组织的权利、审计覆盖的范围、如何进行审计以及CNIL的职权及义务等事项，主要内容如下：

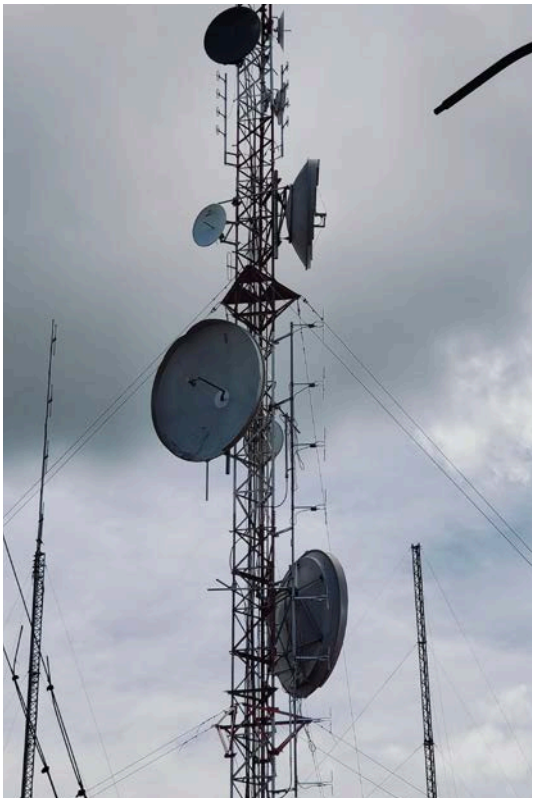
2.参见：https://ico.org.uk/for-organisations/audits/。2022年5月4日最后访问。
3.参见：https://www.cnil.fr/sites/default/files/atoms/files/cnil-charte_des_controles.pdf。2022年5月4日最后访问。

审计覆盖范围	CNIL如何进行审计
－个人数据处理的目的及法律依据； －收集数据的性质； －向数据主体告知的方式，尤其是对于数据主体权利的告知； －数据存储的期限； －数据接收者； －数据安全管控； －数据传输。	CNIL指南中明确了以下四种不同形式的审计活动，审计活动具体开展的方式也相应有所差异： －驻场审计； －线上审计； －通过问询进行审计； －通过文件审查进行审计。

图表 3 法国CNIL数据合规审计核心事项

3. 德国DPA

德国联邦层面的数据保护机构为BfDI (Federal Commissioner for Data Protection and Freedom of Information)，同时在州层面也设有各自的DPA。在GDPR刚生效后的几个月，下萨克森（Lower Saxony）[4]及巴伐利亚（Bavaria）[5]两个州，即宣布开展随机的GDPR合规审计，并面向相关企业发布了审计问卷。以下萨克森州的合规审计问卷为例，主要包括以下事项[6]：



4.参见：https://lfd.niedersachsen.de/startseite/infothek/presseinformationen/fragen-zur-ds-gvo-an-50-unternehmen-166110.html。最后访问日期2022年5月4日。
5.参见：https://www.lda.bayern.de/de/kontrollen.html。最后访问日期2022年5月4日。
6.参见：file:///C:/Users/liulianshi/Downloads/Fragenkatalog_Querschnittsprfung_DSGVO.pdf。最后访问日期2022年5月4日。

在GDPR刚生效后的几个月，德国下萨克森及巴伐利亚两个州即宣布开展随机的GDPR合规审计，并面向相关企业发布了审计问卷。

问题类别	具体问题
GDPR合规准备	—您所在的组织是否为GDPR合规做过准备? —您所在组织的哪个部门参与到了GDPR合规准备? —您所在的组织是否面向员工进行GDPR合规培训?
数据处理活动的记录	—您所在组织如何确保所有数据处理活动都进行了记录? —您所在组织如何确保对相关记录进行更新?
数据处理活动的合法性基础	—您处理个人数据的法律依据是什么? —如果您基于同意的合法性基础处理个人数据，请附上您取得同意的示例。
数据主体的权利	—您所在的组织如何确保数据主体可以主张行使其在GDPR项下的权利? —请特别说明您所在的组织如何履行其告知的义务?
数据安全	—您所在的组织如何确保其已经采取与风险相适应的必要的技术及组织措施? —您所在的组织如何确保上述技术及组织措施的有效性? —您所在的组织如何确保对现有或将来的IT应用程序进行有记录的授权管理; —您所在的组织如何确保设计隐私(Privacy by Design)及默认隐私(Privacy by Default)的理念在产品及服务创建及改造的过程中执行?
数据保护影响评估(DPIA)	—您所在的组织如何识别其需要进行DPIA? —您的组织如何认定DPIA是必要的?
数据处理协议	—您所在的组织是否对数据处理协议进行了更新? —您所在组织的数据处理协议是否满足GDPR的要求?
数据保护官(DPO)	—DPO如何与您所在的组织协作? —您所在的组织任命的DPO是否具有充分的专业知识? —是否向监管机构告知了DPO的信息?
数据泄露的通知	—您所在的组织是否有相应的流程确保在数据泄露发生后在法定期限内及时律师通知义务?

德国多个州的DPA发起了就数据跨境传输的专项合规审计，并面向相关企业发放了审计问卷，要求企业提供信息。

问题类别	具体问题
可问责性（Account-ability）	—您所在的组织如何证明满足上述列举的各项要求？

图表 4 德国下萨克森州数据审计问卷主要内容

（二）数据合规审计在执法中的应用

“Schrems II”案判决[7]做出之后，德国多个州的DPA发起了就数据跨境传输的专项合规审计，并面向相关企业发放了审计问卷，要求企业提供以下信息：

—公司是否向欧盟（**EU**）或欧洲经济区（**EEA**）境外传输个人数据；

—如涉及，公司需说明向EU及EEA境外传输个人数据的合法性基础，如基于SCC进行个人数据跨境传输的应提供SCC文本；

—如数据接收方位于美国，公司需要说明数据接收方是否会被认定为《外国情报监视法》（Foreign Intelligence Surveillance Act）第702节项下的电子通信服务提供者（“electronic communication service provider”）；

—公司是否可以确保接收方能够履行SCC项下的合规义务，并提供相应证据；

—公司就个人数据跨境传输所采取的安全保障措施；

—公司应提供与使用电子邮件服务、网络托管服务、网络跟踪服务、求职者数据管理服务和国际集团内部数据传输有关的处理活动记录的所有相关部分。

上述专项执法活动也为德国企业在数据跨境传输上造成一定的合规压力，由于跨境传输属于个人信息保护的高风险场景，收到问卷的企业对于上述问题的回答，

7.参见：https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=9777234。最后访问时间2022年5月4日。

个人信息的监管机构应考虑发布官方的数据合规审计指引；数据合规审计可作为专项执法检查的工具。

稍有不慎就可能触发行政调查程序。

（三）对完善《个保法》项下合规审计的启示

GDPR项下合规审计的上述实践，对我们完善《个保法》项下的合规审计有以下值得借鉴之处：

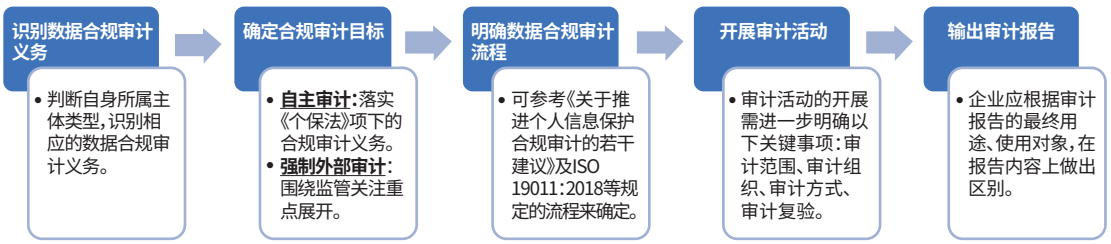
一是，个人信息的监管机构应考虑发布官方的数据合规审计指引：英、法、德数据监管机构分别发布了GDPR项下的专项合规指引、合规审计问卷等，对于企业落实合规审计义务、提升合规管理水平提供了有效参考。有鉴于此，我们也期待我国有关部门可以及时制定、出台个人信息保护合规审计指引或标准，指导个人信息处理者落实《个保法》项下的合规义务，提升合规管控水平。

二是，数据合规审计可作为专项执法检查的工具：根据德国DPA在“Schrems II”案判决做出后的专项执法实践，我们认为将数据合规审计应用于某些高风险合规场景的风险评估，在国家监管层面可以作为一种可借鉴的风险审查和管控措施。

PART 003

如何开展《个保法》的审计合规

基于前文对当前监管要求及国际实践的讨论，对于企业落实《个保法》项下的合规审计义务，我们提出以下建议。



图表 5 开展数据合规审计的关键事项

企业应准确判断自身所属主体类型，在审计目标明确之后，根据确定的审计目标来确定相应的审计流程。

（一）识别数据合规审计义务

根据前述分析，我国《个保法》《网数条例》《平台指南》等分别对个人信息处理者、数据处理者、重要数据处理者、大型互联网平台运营者、超大型平台经营者的数据合规审计义务做出了规定，不同类型的主体在外审/内审、审计频次、审计报告披露、审计内容等方面需要遵循的法律要求有所不同。企业应参考上述法律中对各类主体的定义，准确判断自身所属主体类型，识别相应的数据合规审计义务。

（二）确定合规审计目标

《个保法》项下的合规审计大体分为自主审计和强制审计两种情形，前者主要是企业对于个人信息处理活动的合规自查，后者则是在个人信息处理活动存在较大风险、或发生安全事件后的执法辅助手段，两者的合规审计目标存在较大差异。

对于自主审计，企业应以落实《个保法》项下的审计义务为目标，结合企业实际业务所适用的法律、行政法规的具体要求，从制度建设、组织架构设置、个人信息全生命周期各个环节的合规管控现状等角度，在企业内部开展《个保法》合规审计，或委托外部第三方机构进行。

对于强制外部审计，企业的审计重点应围绕监管机构发现的风险环节及安全事件的处置等方面重点展开。同时，根据合规风险及安全事件影响的大小，监管机构亦可能要求企业进行全面合规审计。

（三）明确数据合规审计流程

在审计目标明确之后，企业应根据确定的审计目标来确定相应的审计流程。2021年12月，由信通院牵头成立的“个人信息保护合规审计推进小组”发布了《关于推进个人信息保护合规审计的若干建议》（以下简称“**《若干建议》**”），其第四章对“审计程序”做出了建议，主要包括计划、准备、实施、报告和后续跟踪等多个阶段，为企业开展《个保法》项下的合规审计提供了有益参考。国际标准化组织发布的《ISO 19011:2018管理体系审计指南》（ISO 19011:2018, Guidelines for auditing management systems）也对管理体系的审计流程作出了规定，在合规审计项目管理层面及合规审计项目实施层面都遵循“计划-实

在审计目标及流程确定后，就审计活动的开展需进一步明确审计范围等关键事项。

施-检查-落实（Plan-Do-Check-Act）”四大步骤，企业在进行《个保法》相关合规审计时可考虑参照执行。具体如下[8]：

	计划（Plan）	实施（Do）	检查（Check）	落实（Act）
项目管理	－确立审计目标 －决定及评估审计项目的风险及机遇 －建立审计项目	－实施审计项目	－监督审计项目	－评估及改进审计项目
项目执行	－启动审计 －准备审计活动	－开展审计活动 －准备并交付审计报告	－完成审计	－审计后续跟进

图表 6 ISO 19011:2018审计流程

（四）开展合规审计活动

在审计目标及流程确定后，就审计活动的开展需进一步明确以下关键事项：

－**审计范围**：审计范围应该根据审计目标确定。具体而言，如为企业的自主审计，审计范围至少应涵盖对现有内部管理制度和操作规程的完备性、执行的有效性的审查；组织架构层面，是否依法设置数据保护机构和个信息保护负责人，其履职是否符合法律要求；个人信息处理活动层面，就个人息的收集、存储、使用、跨境传输、个人信息主体行权响应等环节，是否采取了法律要求的合规措施；安全事件响应机制是否有效运转等事项。《若干意见》第三章也对审计重点给出了有益的参考，包括：1.个人信息处理者义务合规审计；2.个人权利实现方式合规审计；3.个人信息处理活动合规审计（包括

8.参见ISO 19011:2018 (E)，第8页。

在输出审计报告时，我们建议企业应根据审计报告的最终用途、使用对象，在报告内容上作出区别。

收集、存储、使用、加工、提供、传输、公开、删除等各个环节）；4.个人信息跨境提供合规审计等。如为外部强制审计，则重点应该根据监管机构关注的合规问题确定企业的数据合规审计范围。

- **审计组织：**如企业拟开展内部审计，应结合审计目标、审计范围等确定内部审计小组成员。为确保合规审计执行的有效性，需确立审计开展的领导部门，并考虑由合规、法务、IT、业务、HR等多个部门负责人作为审计小组成员来推进审计的实施。在审计小组成立后，审计小组应将审计的目标、实施流程、相关部门需要提供的支持等事项通知到公司内部各个相关部门，为审计的实施做好准备。如企业委托第三方机构开展审计，则企业应该在第三方机构的协助下，确定审计的目标、范围、流程等事项，由第三方机构在审计活动开始之前面向公司内部相关人员召开项目启动会，说明审计的工作计划及相关部门需要提供的支持，以确保后续审计工作的顺利推进。
- **审计方式：**在具体进行审计时，审计机构可以通过审阅制度文件、访谈、进行产品及服务合规测试等方式对现有合规措施的完备性和有效性进行审查，发现并记录问题，生成审计报告。参考英国ICO的审计执法经验，我们建议在审计报告中应考虑就合规审计中发现的问题，根据《个保法》的规定，参考行业最佳实践，提出整改建议，由相关业务部门予以落实。
- **审计复验：**数据合规审计并非一项一劳永逸的工作，考虑到当前国内数据合规立法不断完善，执法活动不断趋严的监管态势，企业应结合国内立法、执法实践，在审计完成后定期复验，确保数据审计中发现的问题能得到有效的解决。

（五）输出审计报告

在输出审计报告时，我们建议企业应根据审计报告的最终用途、使用对象，在报告内容上作出区别。如审计报告拟向监管

审计工作的法律基准确立、企业行为的合规性判断，仍主要是法律工作。

部门提交，则需重点回应监管机构关注的风险问题，并对企业遵守相关法律法规的情况予以说明。但在作为企业合规的支持性文件面向客户提交时，则应就客户对企业在个人信息保护方面的主要关切予以审计说明。值得注意的是，当企业进行定期审计时，建议企业对上一次审计中发现的问题以及合规整改落实情况予以回应，以此作为企业积极落实《个保法》项下的合规义务的有力证明。

PART 004

结语

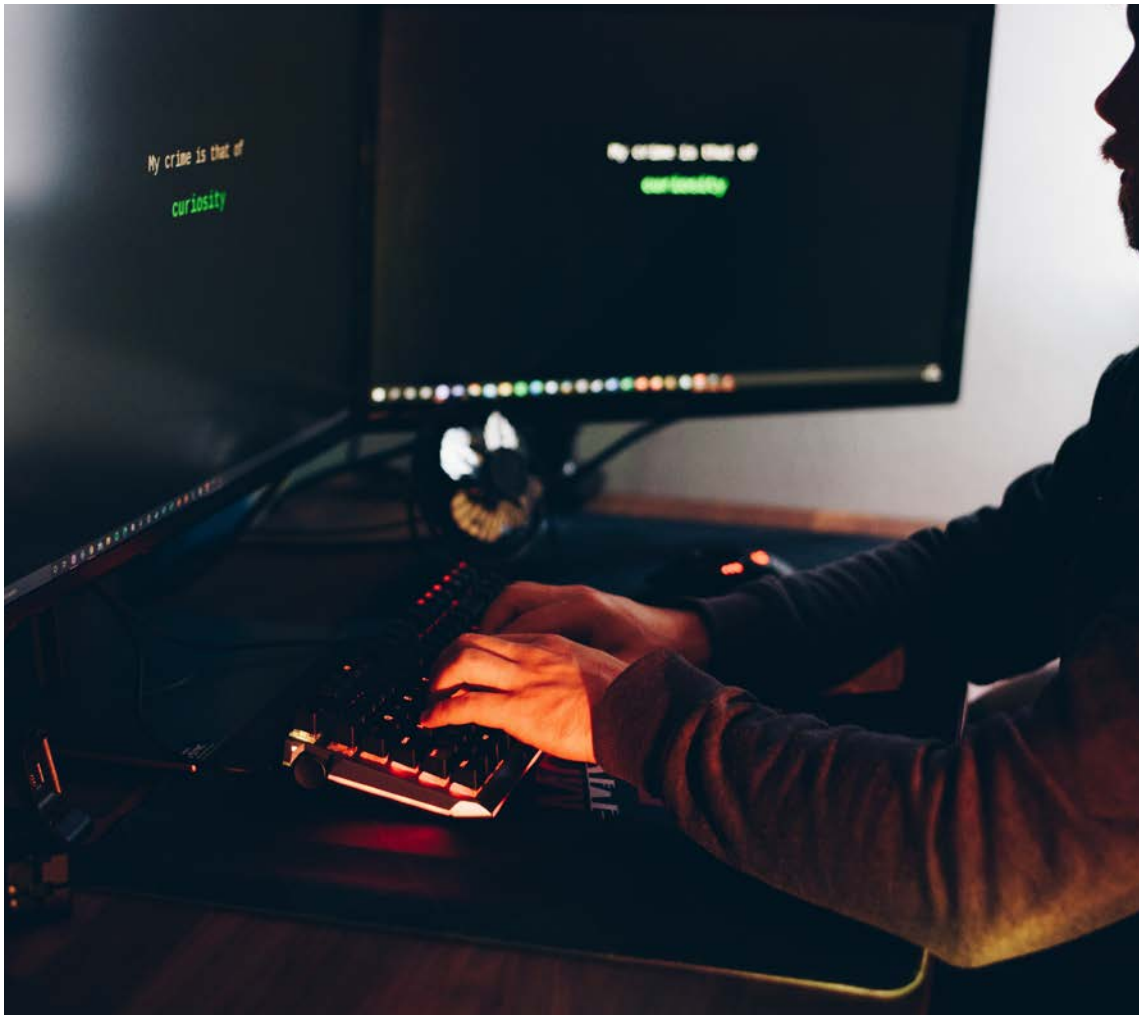
《个保法》自颁布实施以来，企业围绕《个保法》开展的合规整改工作仍在持续进行。对于已经完成初步合规整改工作的企业而言，前期的合规整改工作是否已经落实到位，是否与《个保法》及其他法定要求仍存在合规差距，需要进一步检视。《个保法》项下合规审计的法定要求，既是企业作为个人信息处理者的法定义务，也是企业识别合规风险、提升数据治理水平的合规管控工具。

实施审计工作既具有法律性也具有技术性，审计机构最好兼具这两方面的能力。但总体来讲，审计工作的法律基准确立、企业行为的合规性判断，仍主要是法律工作，因此，由具有能力的律师所承担这一审计工作属于恰当安排。

陈际红
合伙人
知识产权部
北京办公室
+86 10 5957 2003
chenjihong@zhonglun.com

PART THREE

《个保法》合规重难点场景



跨国公司员工管理数据合规十问十答

蔡鹏 胡云浪 苏阳阳

立足现有法律法规，围绕跨国企业常见员工信息处理场景，
本文回答了十个常见代表性员工管理数据合规问题。

人力资源合规是跨国公司最重要的合规部分。自2021年11月1日《个人信息保护法》施行以来，对跨国公司在人力资源管理的场景下提出了一系列新的合规要求。跨国公司如何在《个人信息保护法》的框架下，既满足自身全球化管理的内在需求，又要符合中国法律的规定，成为当前困扰着许多跨国公司的难题。而随着相关配套立法的完善，特别是数据跨境相关立法的落地，一些问题的答案也逐渐清晰。立足于现有法律法规和有关立法征求意见稿，我们围绕跨国企业常见的员工个人信息处理场景，选取了十个具有代表性的问题提供一些建议。

PART 001

员工个人信息的跨境提供如何理解？

(一) 如何理解“员工个人信息”

依据《个人信息保护法》第四条，个人信息是指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。个人信息的内涵十分丰富，根据国家标准《信息安全技术　个人信息安全规范》，个人信息具体可包括：

1.个人基本资料（姓名、出生、性别、民族、国籍、家庭关系、住址、个人电话号码、电子邮件地址等）；

2.个人身份信息（身份证、护照等）；

3.个人生物识别信息（面部识别特征等）；

4.个人健康生理信息（身高、体重、生育信息、病症等）；

5.个人教育工作信息（学历、学位、教育经历、工作经历、培训记录、成绩单等）；

6.个人财产信息（银行账户、房产信息、征信信息等）；

7.网络身份标识信息、联系人信息、个人上网记录、个人常用设备信息、个人位置信息、其他信息。

实践当中，企业在进行员工招聘时往往会通过收集简历、填写入职登记表等方式获得潜在员工的个人基本资料、联系人信息、个人教育工作信息、个人财产信息

必须根据《个保法》以及相关法律法规及行业标准理解“个人信息”内涵与外延的界定，同时结合企业在招聘、管理员工时的具体应用场景来进行梳理。

等；通过入职体检等方式收集潜在员工的个人健康生理信息；以及通过员工日常管理，可能收集到员工的个人生物识别信息等。

需要指出的是，员工个人信息不仅仅包括“一般个人信息”。部分员工个人信息可能落入“敏感个人信息”的范围内。《个人信息保护法》第二十八条将敏感个人信息定义为一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。员工个人信息当中的入职体检报告、违法犯罪记录、宗教信仰、生育信息、不满十四周岁子女信息、身份证、社保卡或居住证件信息、征信信息、指纹、虹膜、人脸信息、监控行踪轨迹、银行账户和工资支付记录等，较大可能落入“敏感个人信息”。《个人信息保护法》及其相关法律法规对处理此类敏感个人信息亦提出了更高标准的处理要求（例如取得个人信息主体的“单独同意”）。

综上，理解员工个人信息，必须根据《个人信息保护法》以及相关法律法规及行业标准理解“个人信息”内涵与外延的界定，同时结合企业在招聘、管理员工时的具体应用场景来进行梳理。

（二）如何理解“跨境提供”？

《个人信息保护法》并未明确定义何为“跨境提供”，根据目前的法律规定，目前可以从两个角度理解“跨境提供”：（1）指在境外处理境内自然人个人信息的特定活动；（2）指向境外提供境内特定数据的情形。当然，理解跨境提供的具体场景，根据现有实践，我们认为以下情形属于数据出境：

1.向本国境内，但向不属于本国管辖/注册的主体提供个人信息；

2.个人信息未转移存储至本国以外的地方，但被境外的机构、组织、个人访问查看的（公开信息、网页访问除外）；

3.网络运营者集团内部数据由境内转移至境外，涉及其在境内运营中收集和产生的个人信息的。

下列行为不包含在数据出境范畴中：

1.非在境内运营中收集和产生的个人信

境外企业通过API接口等方式访问存储于境内公司的员工个人信息，很有可能构成《个人信息保护法》下的个人信息跨境。

息经由本国出境，未经任何变动或加工处理的，不属于数据出境。

2.非在境内运营中收集和产生的个人信息在境内存储、加工处理后出境，不涉及境内运营中收集和产生的个人信息的，不属于数据出境。

值得注意的是，上述理解基于现有规定做出，不排除未来制定《个人信息保护法》实施细则时，在认定属于“跨境提供”的具体场景时会有所改变。

PART 002

境外公司访问境内公司的员工数据存储系统是否构成中国《个人信息保护法》下的个人信息跨境？

参见第一问，我们认为境外公司在境外访问境内公司位于境内的员工数据存储系统属于《个人信息保护法》下的“个人信息跨境提供”。依据《个人信息保护法》第四条的规定，个人信息的处理包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等。境外公司即便仅访问境内的员工数据系统，其“访问”也很极有可能被法律认定为属于对境内员工数据的处理（“使用”），从而落入《个人信息保护法》下“跨境提供”的范畴。就目前实践当中，境外企业通过API接口等方式访问存储于境内公司的员工个人信息，无论根据《个人信息保护法》的法律文本还是通过现有其他法律法规的辅助释义，都很有可能构成《个人信息保护法》下的个人信息跨境。

PART 003

中国《个人信息保护法》第13条中规定的“按照依法制定的劳动规章制度和依法签订的集体合同实施人力资源管理所必需”这一合法性基础如何理解？

个人信息处理者处理个人信息的，须取得《个人信息保护法》第十三条所列六项“合法性基础”之一，其中：“（二）……**或者**按照依法制定的劳动规章制度和依法签订的集体合同实施人力资源管理所必需……”。结合《劳动合同法》的相关规定，可以从以下两个层次理解该合

企业处理员工个人信息若基于“按照依法制定的劳动规章制度和依法签订的集体合同实施人力资源管理所必需”这一合法性基础，则无需另行取得“同意”，亦无需再取得“单独同意”。

法性基础：

(一)按照依法制定的劳动规章制实施人力资源管理所必须。依照《劳动合同法》第四条的规定，企业在制定有关劳动报酬、工作时间、休息休假、劳动安全卫生、保险福利、职工培训、劳动纪律以及劳动定额管理等直接涉及劳动者切身利益的规章制度或者重大事项时，应当经职工代表大会或者全体职工讨论，提出方案和意见，与工会或者职工代表平等协商确定。用人单位应当将直接涉及劳动者切身利益的规章制度和重大事项决定公示，或者告知劳动者。即：依法制定的劳动规章，应当为企业依法经过民主协商程序，将特定的劳动制度进过公示或告知员工，并经过职代会及员工充分协商、反馈后所订立的劳动规章制度。而理解“为人力资源管理所必须”，则应当关注特定劳动规章制度涉及的具体管理事项，不得随意扩大个人信息的处理范围。例如企业依其制定的有关“劳动报酬”的政策时，需要收集个人信息主体的姓名、职级等信息，但实施相关政策并无需收集年龄、性别等个人信息。

(二)按照依法签订的集体合同实施人力资源管理所必须。依照《劳动合同法》第五章第一节的有关规定，集体合同通常是指由工会代表企业职工一方与用人单位通过平等协商，就劳动报酬、工作时间、休息休假、劳动安全卫生、保险福利等事项订立的合同。依法制定的集体合同，其草案应当提交职工代表大会或全体职工讨论通过。实务当中，集体合同通常见诸于建筑、采矿、餐饮等特定行业。同样，依集体合同实施人力资源管理，必须关注集体合同具体约定事项（如劳动报酬、工作时间、休息休假、劳动安全卫生、保险福利等事项）所需处理的个人信息，不得超范围处理。

值得注意的是，作为“同意”这一合法性基础的特殊表现形式，“单独同意”本身并未被《个人信息保护法》列为独立的合法性基础。因此，依据《个人信息保护法》第十三条的相关规定，企业处理员工个人信息若基于“按照依法制定的劳动规章制度和依法签订的集体合同实施人力资源管理所必需”这一合法性基础，则无需另行取得“同意”，亦无需再取得“单独同意”。

境内公司向境外公司跨境提供员工个人信息的，境内公司首先应当明确该处理场景是否需要取得员工的“单独同意”。

PART 004

境内公司向境外公司跨境提供员工个人信息的，境内公司应当如何取得员工的单独同意？

《个人信息保护法》第三十九条规定，个人信息处理者向中华人民共和国境外提供个人信息的，应当向个人告知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**。我们认为可以从以下几个维度理解单独同意：

(一)取得标准。单独同意的取得标准，应当至少不低于《个人信息保护法》就取得个人“同意”的相关规定。即应当充分告知信息主体个人信息处理的方式、目的、规则等，由个人在充分知情的前提下自愿、明确作出；保障个人信息主体能通过便捷的方式撤回其“同意”；以及在变更使用目的或方式等特定情形下重新获取个人信息主体的“同意”。

(二)取得形式。单独同意的取得形式，应当具有独立性。依据《最高人民法院关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定》第四条的规定，以拒不提供产品或服务相胁迫、捆绑授权、强迫或变相强迫等方式获取的同意不属于“单独同意”。

基于上述分析，境内公司向境外公司跨境提供员工个人信息的，境内公司首先应当明确该处理场景是否需要取得员工的“单独同意”。同时建议公司针对法律法规对单独同意的取得标准及取得形式的要求，制定专门的SOP、设置同意授权通道、并由专人负责保障个人信息主体针对其授权同意的行权。

境内公司在向境外公司提供员工个人信息前应当完成个人信息保护影响评估、完成对应跨境路径的评估工作。

PART 005

境内公司在向境外公司跨境提供员工个人信息前，应当开展哪些评估工作？

结合《个人信息保护法》、《数据出境安全评估办法》等有关规定和实践，境内公司在向境外公司提供员工个人信息前应当开展如下评估工作：

(一)完成个人信息保护影响评估

依据《个人信息保护法》及相关法律法规的的规定，个人信息处理者向境外提供个人信息时，应当事前进行个人信息保护影响评估（以下简称“**PIA**”），并对处理情况进行记录。根据我们的经验，我们认为保护影响评估至少包括：

1.评估应当包括评估个人信息的处理目的、处理方式等是否合法、正当、必要及是否符合诚信原则；

2.评估应当包括评估对个人权益的影响及安全风险，在跨境场景下，需要评估境外国家法律保护环境，以及接收方、相关方的安全措施，是否存在风险；

3.评估应当包括评估所采取的保护措施是否合法、有效并与风险程度相适应；

4.评估的报告和处理情况记录应当至少保存三年。

5.评估应当包括评估数据出境和再转移后泄露、毁损、篡改、滥用等的风险，个人维护个人信息权益的渠道是否通畅等。

(二)完成对应跨境路径的评估工作

《个人信息保护法》第三十八条就员工个人信息出境给出了三条路径。即（1）通过国家网信部门安全评估；（2）获得专业机构的认证办理；或（3）通过签订标准合同办理。总体而言，每条通关路径的适用对象、范围不同，且所需完成的评估工作与《个人信息保护法》要求的PIA存在重叠但又有所不同（下文中将详细介绍）。下文就安全评估及专业机构认证所涉及的评估工作进行介绍。

1.通关路径一 – 完成安全评估。依照《个人信息保护法》第三十八条、第四十条以及《数据出境安全评估办法》第四条，**关**

对于非CIIO或处理员工个人信息或员工个人敏感信息没有超过一定数量的企业，可以在跨境提供前选择完成个人信息安全保护认证。

键信息基础设施的运营者（以下简称“**CIIO**”）在中华人民共和国境内运营中收集和产生的**个人信息**、处理个人信息**达到一百万人**的个人信息处理者向境外提供个人信息、**累计向境外提供超过十万人**以上个人信息或者**一万人以上敏感个人信息**应当完成**安全评估**。安全评估应当坚持风险自评估与风险评估相结合的原则。即：

➢ 进行风险自评估，需要完成解答（一）所列举的PIA评估工作，并在此之外梳理与境外接收方订立的数据出境相关合同是否充分约定了数据安全保护责任义务，同时留存数据出境风险自评估报告。

➢备齐相关材料，按照法定程序通过所在地省级网信部门向国家网信部门申报数据出境安全评估。

值得注意的是，CIIO通常是指涉及公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域的信息基础设施运营者。拟跨境提供员工个人信息的企业若所属行业、业务类型可能落入CIIO的，我们建议企业在跨境提供个人信息前，应当完成安全评估。同时，若企业因其业务类型（如专门提供跨境劳务派遣服务）、规模存在大量传输员工个人信息或员工敏感个人信息的情形的，也应当按照法律法规要求完成安全评估工作。相反，若企业规模较小，且不涉及特殊行业或服务类型的，在跨境提供员工个人信息时则并不一定需要完成安全评估工作。

2.通关路径二 - 完成个人信息保护认证。对于非CIIO或处理员工个人信息或员工个人敏感信息没有超过一定数量的企业，可以在跨境提供前选择完成**个人信息安全保护认证**。企业若选择通过该路径跨境提供员工个人信息的，我们建议完成如下评估工作：

（1）明确主体责任。跨国公司或者同一经济、事业实体下属子公司或关联公司之间的个人信息跨境处理活动，可由境内实体申请认证并承担法律责任。若境内企业与境外企业分属不同实体，则我们建议由境外企业在境内设置专门机构以完成认证。

（2）评估是否符合法定原则。企业跨境提供员工个人信息的，须评估是否符合如

企业跨境提供员工个人信息的，须评估是否满足法律约束要求、组织管理要法语等基本要求。

下要求：

➢合法、正当、必要和诚信原则。企业是否采取了对员工权益影响最小的方式处理其个人信息；

➢公开、透明原则。跨境提供员工信息是否做到处理规则公开、处理过程透明，并及时告知员工跨境提供个人信息的目的、范围和方式；

➢信息质量原则。跨境提供员工信息过程中，各方是否能够保证个人信息的准确及完整；

➢同等保护原则。跨境处理员工信息过程中，各方是否能够确保个人信息的处理符合我国相关法律法规就个人信息保护设置的标准。

（3）评估是否满足基本要求。企业跨境提供员工个人信息的，须评估是否满足如下基本要求：

➢法律约束要求。各方是否签订了具有法律约束力和执行力的文件。同时该文件是否包括：参与跨境处理员工个人信息相关方；处理的目的及类别与范围；采取何种措施保障个人信息主体权益；承诺遵守统一个人信息处理规则并确保其水平不低于我国个人信息保护相关规定；接受认证机构监管及法律管辖。

➢组织管理要求。企业内部是否指派了专门保护员工个人信息的负责人，且该负责人是否为决策层成员且职责明确。各相关方就履行员工个人信息保护义务，防止其泄露、篡改、丢失是否设立了专门保护机构。

➢跨境处理规则要求。境内员工个人信息提供方与境外企业是否设置并遵循统一的个人信息处理规则。规则内容包含：处理员工个人信息的基本情况（类型、敏感程度）；处理的目的、方式及范围；境外存储的起止时间及到期后的处理方式；跨境处理员工个人信息是否需要中转及经哪些地区或国家中转；保障员工个人信息主体权益采取的资源和措施；发生安全事件后的赔偿及处置规则。

➢个人信息影响评估要求。参照《个人信息保护法》及《信息安全技术 个人信息安全影响评估指南》就跨境提供员工个人信息进行评估。针该通关路径，我们建议除PIA外，境内提供方与境外接收方还需要重点评估员工个人信息出境目的国和地区的法律环境是否能够对员工个人信息提供

境内公司在向境外公司跨境提供员工个人信息前，
对员工个人有告知义务。

有效保护，以及境外接收方自身的网络环境是否能够对员工个人信息主体权益提供有效保障。

PART 006

境内公司在向境外公司跨境提供员工个人信息前，应当向员工个人告知哪些事项？

境内公司在向境外公司跨境提供员工个人信息前，应当向员工个人告知如下事项：

（一）告知员工个人其个人信息跨境提供的目的、范围和处理方式，确保员工了解自己个人信息处理的全过程。

（二）告知员工参与跨境处理其个人信息的相关方。告知员工有关的保障措施以及所遵守的个人信息处理规则，同时明确境内承担法律责任的实体等。

（三）告知员工行使其个人信息主体权益的方式与路径，以及企业的响应方式。应员工请求，企业应提供其个人信息跨境中与员工签署的法律文件，并提供员工行权路径和涉及员工权益的副本等。若企业拒绝员工相关请求的，企业应当说明理由和救济途径。

（四）针对员工敏感个人信息的特殊告知义务参见第九问。

PART 007

境内公司与境外公司订立的关于员工个人信息跨境提供的合同，应当对哪些事项进行约定？

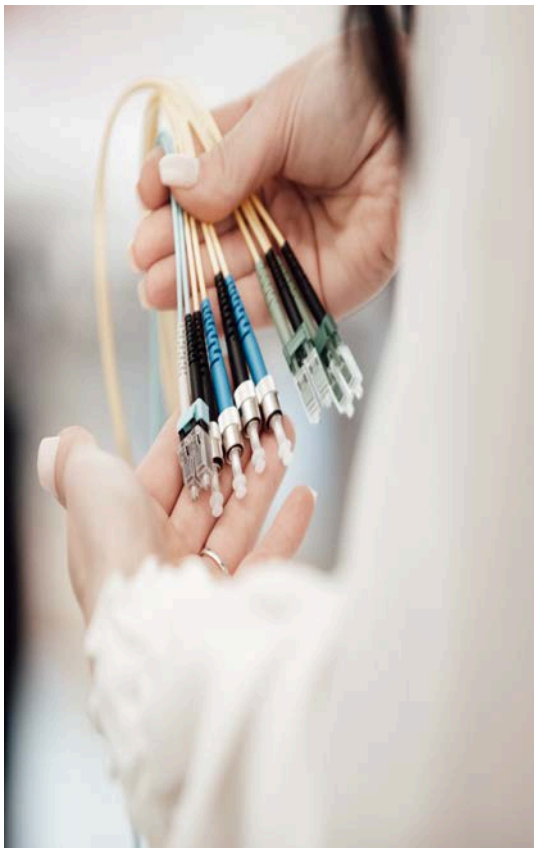
境内公司与境外公司订立的关于员工个人信息跨境提供的合同，我们建议对以下事项进行约定：

（一）境内提供方与境外接收方的具体信息；

（二）跨境的目的、方式以及数据的类别与范围，境外接收方处理数据的用途、方式等；

（三）员工数据在境外的保存地点、期限，以及达到保存期限、完成约定目的或

境内公司与境外公司订立的关于员工个人信息跨境提供的合同，应当对特定事项进行约定。



者合同终止后出境数据的处理措施；

（四）对于员工个人信息主体权益的保护措施；

（五）限制将出境的员工数据再转移给其他组织、个人的约束条款；

（六）在境外接收方的实际控制权或者经营范围发生实质性变化，或者所在国家、地区法律环境发生变化等情况下，导致难以保障员工数据安全时，应当采取的有效安全措施；

（七）境外接收方与境内提供方承诺接受中华人民共和国个人信息保护相关法律、行政法规管辖；

（八）违反员工数据安全保护义务的违约责任，以及具有约束力且可执行的争议解决条款；

（九）境外接收方与境内提供方承诺接受认证机构监督（如进行个人信息跨境活动认证的）；

（十）境外接收方承诺并遵守统一的个人信息处理规则，确保个人信息保护水平不低于中华人民共和国个人信息保护相关法律、行政法规规定的标准。

值得关注的是，《个人信息保护法》第三十八条第（三）款亦明确了“国家网信部门制定的标准合同”这一条件，但目前《个人信息出境标准合同规定》正式稿尚未出台，员工跨境所涉主体也应当保持对于标准合同相应配套规则的关注，待相关规则落地后，亦可结合企业实际对上述约定事项进行针对性调整。

境外公司作为员工个人信息的境外接收方，应当重点从明确《个保法》下的法定权利、建立便捷的员工行权申请受理和处理机制两方面保障员工权利。

PART 008

境外公司作为员工个人信息的境外接收方，如何保障员工在《个人信息保护法》下的法定权利？

根据《个人信息保护法》第三十九条规定："个人信息处理者向中华人民共和国境外提供个人信息的，应当向个人告知……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"。根据该条规定，我们认为，境外公司作为员工个人信息的境外接收方，应当重点从以下两方面保障员工在《个人信息保护法》下的法定权利：

（一）明确《个人信息保护法》下的法定权利：

基于境外公司与境内公司的法律适用性的区别，境外公司往往对于中国《个人信息保护法》下的个人信息主体的法定权利较为陌生。因此，境外公司有必要首先对中国《个人信息保护法》下的个人信息主体的法定权利进行明确。概括而言，在跨境场景下，现有实践中的有关法定权利主要包括以下类别：

1.个人信息主体对其个人信息的处理享有知情权、决定权，有权限制或者拒绝他人对其个人信息进行处理；

2.有权向境外接收方要求查阅、复制、更正、补充、删除其个人信息；

3.有权要求个人信息跨境处理活动相关方对其个人信息处理规则进行解释说明；

4.有权拒绝仅通过自动化决策的方式作出决定；

5.有权向中华人民共和国履行个人信息保护职责的监管机构进行投诉、举报。

根据立法趋势，境外接收方还需要注意以下两点可能的扩张权利（"扩张权利"）：

1.文本获取。个人信息主体是个人信息跨境处理活动相关方签订法律文件中个人信息权益相关条款的受益人，有权要求个人信息跨境处理相关方提供法律文本中涉及个人信息主体权益部分的副本。

2.司法管辖。个人信息主体有权在其经常居住地所在法院向参与个人信息跨境处理的相关方提起司法诉讼。

我们理解，基于目前已生效的《个人信息保护法》，境外接收方应当重点关注前

境内公司向境外公司跨境提供员工的敏感个人信息时，还应当关注特殊合规义务。

五类法定权利，依法保障员工在《个人信息保护法》下的法定权利。至于两类扩张权利，境外接收方可保持关注，待该规则具体落地后，可以结合企业实际，综合考量保障该两类扩张权利的成本，必要的时候可以与监管部门进一步确认。

（二）建立便捷的员工行权申请受理和处理机制

根据《个人信息保护法》第五十条的规定，个人信息处理者应当建立便捷的个人行使权利的申请受理和处理机制。拒绝个人行使权利的请求的，应当说明理由。作为境内员工个人信息的境外接收方，境外公司作为个人信息处理者，亦应当在明确《个人信息保护法》下的法定权利的基础上，建立便捷的员工行权申请受理和处理机制。

在员工个人信息跨境场景下，建议境外公司直接或通过境内公司的协助与相关员工签订《员工隐私政策》，细化各类法定权利的具体行权机制，并依法实际履行该等义务。若进行跨境的员工个人信息亦包含求职者的个人信息，建议境外公司要求境内公司，在招聘环节即前置化要求求职者签订《求职者隐私政策》，以更为全面地保障员工的法定权利。

PART 009

境内公司向境外公司跨境提供员工的敏感个人信息时，应当关注哪些特殊合规义务？

（一）敏感个人信息的识别

识别何类员工个人信息属于敏感员工个人信息参见第一问的回答。

（二）严格限制的处理目的

《个人信息保护法》第二十八条规定：只有在具有特定的目的和充分的必要性，并采取严格保护措施的情形下，个人信息处理者方可处理敏感个人信息。在员工个人信息跨境场景下，境内公司应当首先评估是否满足该等严格限制的处理目的，若不满足，则不应当开展员工敏感个人信息的跨境行为。

（三）特殊的告知义务

《个人信息保护法》第三十条规定："个人信息处理者处理敏感个人信息的，

跨国公司由境内向境外跨境提供员工个人信息前，应当充分论证适用的合法性基础，区分化地判断是否应当取得员工的单独同意。

……还应当向个人告知处理敏感个人信息的必要性以及对个人权益的影响”。境内公司在向境外公司传输员工个人信息前，应当通过协议、文本等留痕方式向员工以其可以充分理解的方式，告知前述必要性以及对员工个人权益的影响。

（四）区分合法性基础下的单独同意义务

基于前述分析，若基于“按照依法制定的劳动规章制度和依法签订的集体合同实施人力资源管理所必需”这一合法性基础处理员工个人信息的，不需取得员工个人的同意；若无法适用前述合法性基础，则需在处理员工个人信息前，谨慎分析处理的合法性基础。

跨国公司由境内向境外跨境提供员工个人信息前，应当充分论证适用的合法性基础，区分化地判断是否应当取得员工的单独同意。根据2021年11月发布的《网络数据安全管理条例（征求意见稿）》第七十三条的规定，“单独同意是指数据处理者在开展具体数据处理活动时，对每项个人信息取得个人同意，不包括一次性针对多项个人信息、多种处理活动的同意。”因此，“单独

同意”的核心在于就要求个人信息处理者将特定个人信息处理事项单独列出，给予该个人就某一事项单独判断的权利与便利。具体到跨国公司在人事管理的场景下，建议公司可以将单独同意事项列出，由员工逐项确认。

（五）个人信息保护影响评估义务

根据《个人信息保护法》第五十五条的规定，处理敏感个人信息，个人信息处理者应当事前进行个人信息保护影响评估，并对处理情况进行记录。境内公司在向境外提供员工敏感个人信息前，应当依法履行个人信息保护影响评估义务，并做好留痕工作。

境外公司违反员工个人信息保护合规义务，主要面临民事、行政、刑事三类法律责任。

PART 010

境外公司违反员工个人信息保护合规义务，将会承担何种法律责任？

境外公司虽然地理位置位于中国境外，但作为境内员工个人信息跨境提供的境外接收方，其对于员工个人信息的处理行为，仍受中国《个人信息保护法》的管辖，其违反员工个人信息保护合规义务，主要面临三类法律责任：

（一）民事责任

处理个人信息侵害个人信息权益造成损害，个人信息处理者不能证明自己没有过错的，应当承担损害赔偿等侵权责任。该损害赔偿责任按照个人因此受到的损失或者个人信息处理者因此获得的利益确定;个人因此受到的损失和个人信息处理者因此获得的利益难以确定的，根据实际情况确定赔偿数额。

（二）行政责任

对个人信息处理者:根据《个人信息保护法》规定，最高可以对违法的个人信息处理者处以上一年度营业额百分之五以下的罚款。

对直接负责的主管人员和其他直接责任人员《个人信息保护法》规定最高可罚款一百万元，并可以决定禁止其在一定期限内担任相关企业的董事、监事、高级管理人员和个人信息保护负责人。

（三）刑事责任

个人信息处理者违反《个人信息保护法》《刑法》等的规定，构成犯罪的，依法追究刑事责任。如构成侵犯公民个人信息罪、拒不履行信息网络安全管理义务罪等犯罪的，最高可处七年以下有期徒刑，并处罚金。

PART 011

结语

所谓正本清源，企业在向中国境外提供员工个人信息时，应当回归《个人信息保护法》等法律法规的相关文本以及立法目的，厘清重点概念并加深对各项法定合规义务的理解，才能在运营管理过程中制定、实施更为有效且具有针对性的合规策

跨国企业做好有关的必备合规动作，确保自身的员工管理行为不会产生法律风险。

略。考虑到《数据出境安全评估办法》《个人信息出境标准合同规定（征求意见稿）》等针对个人信息跨境的法律法规相继发布，我们建议跨国企业做好有关的必备合规动作，确保自身的员工管理行为不会产生法律风险。

蔡鹏
合伙人
知识产权部
北京办公室
+86 10 5087 2786
caipeng@zhonglun.com

医药企业个人信息合规常见问题及应对措施

刘新宇 冯中杰

本文将结合实践经验，简述医药企业在个人信息合规领域的常见问题及应对措施，供相关企业参考。

在被称为“个人信息保护元年”的2021年中，《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》（以下简称“**《个人信息保护法》**”）等规定先后出台，为我国的个人信息保护法律体系搭建了基础的框架。而在进入2022年之后，立法者并未停下完善我国法律体系的脚步，包括《数据出境安全评估办法》《个人信息出境标准合同规定（征求意见稿）》（以下简称“**《标准合同规定（征求意见稿）》**”）在内的各类法律文件相继发布。在这一趋势下，各类企业都面临着愈发严峻的合规压力，而医药行业作为一个本就会接触大量个人信息，尤其是敏感个人信息的行业，更是首当其冲。以下，笔者将结合实践经验，简述医药企业在个人信息合规领域的常见问题及应对措施，供相关企业参考。

PART 001

医药企业应当关注“敏感个人信息”的合规义务

在个人信息中，有一个相对特殊的类别，即“敏感个人信息”。根据《个人信息保护法》第二十八条的规定：“敏感个人信息是一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息。”而包括“医疗健康”信息在内的多项信息均被《个人信息保护法》明确列举为敏感个人信息，故医药企业不可避免地需要在业务中对于处理“敏感个人信息”时的合规义务予以特别的关注。根据《个人信息保护法》，笔者建议医药企业作为敏感个人信息的处理者应当特别注意履行以下的义务。

首先，根据《个人信息保护法》第二十九条的规定，在处理敏感个人信息前，医药企业作为个人信息处理者应当取得个人的单独同意作为处理个人信息的合法性基础。这意味着医药企业不能将敏感个人信息与一般个人信息混同，仅获得个人的概括性授权，而应当就敏感个人信息出具单

医疗健康信息被《个保法》明确列举为敏感个人信息，故医药企业不可避免地需要在业务中对于处理“敏感个人信息”时的合规义务予以特别的关注。

独的《告知同意书》，允许个人仅拒绝其对敏感个人信息的处理行为。需要特别注意的是，敏感个人信息还包括“不满十四周岁未成年人的个人信息”，《个人信息保护法》对于这类信息亦作出了特别规定，即处理前必须获得“未成年人的父母或者其他监护人”的单独同意。在实践中，亦可能存在个别较难获取单独同意的场景，对于这一问题，笔者建议医药企业可以考虑以其他合法性基础代替个人或未成年人监护人的单独同意。《个人信息保护法》第十三条在第二至七项规定了包括“为订立、履行个人作为一方当事人的合同所必需”在内的多项合法性基础，并明确有这些规定情形的，“不需取得个人同意”。故在实践中，如果存在一些较难直接获取个人单独同意的场景，医药企业亦可以考虑仅处理向个人提供服务所必需的个人信息，以“为订立、履行个人作为一方当事人的合同所必需”作为未能取得单独同意时的替代合法性基础。

其次，根据《个人信息保护法》第五十五条的规定，“处理敏感个人信息”属于应当开展“个人信息保护影响评估”的情形之一。医药企业在开展个人信息保护影响评估时，应当特别注意法律法规的以下几点要求：第一，作为一项事前预警机制，个人信息保护影响评估必须在特定个人信息处理活动开展之前完成，因此个人信息处理者有必要提前制定关于个人信息保护影响评估的内部制度、流程，摸排医药企业内部各部门的个人信息处理活动，确定需要开展个人信息保护影响评估的场景，并规划相应的评估方案。第二，虽然原则上可以聘请外部的团队协助医药企业开展个人信息保护影响评估，但是根据《个人信息保护法》第五十五条的规定，开展评估仍然是个人信息处理者，即医药企业自身的义务。同时，参考《信息安全技术　个人信息安全影响评估指南》（GB/T　39335-2020）第5.2.1条的要求，个人信息处理者亦需要“任命负责进行个人信息安全影响评估的人员（评估人）”，并“指定人员负责签署评估报告”。故综合上述规定，笔者建议医药企业亦应当在内部确定负责个人信息保护影响评估的部门或人员，以主导或配合外部团队完成个人信息保护影响评估。第三，根据《个人信息保护法》第五十六条的规定，在完成

医药企业向其他主体传输个人信息主要有三种模式：向其他个人信息处理者提供个人信息，委托处理个人信息，以及作为共同处理者传输个人信息。

评估后，个人信息保护影响评估报告和处理情况记录都应当至少保存三年。故个人信息保护影响评估并非一劳永逸的工作，而是需要持续进行保存与记录，笔者建议医药企业建立起个人信息处理活动的档案管理制度，将历次风险评估报告及处理结果进行保存留档，以应对监管部门可能的不定期抽查，降低自身的合规风险。

PART 002

合理确定与其他主体的个人信息传输模式

除关注与敏感个人信息有关的合规义务外，医药企业在日常经营中可能面临的另一项常见合规问题，就是如何向其他主体传输个人信息。在实践中，新品研发、线上销售等环节都可能涉及医药企业与外部合作方（例如合作研发机构、CRO、医药代理公司等）或关联主体传输个人信息的场景，因此合理确定个人信息的传输模式，妥善约定各方的权利义务关系，就成为了医药企业必须处理的合规问题。在目前《个人信息保护法》的体系下，医药企业向其他主体传输个人信息主要有三种模式：向其他个人信息处理者提供个人信息（以下简称“**对外提供个人信息**”），委托处理个人信息，以及作为共同处理者传输个人信息。

前两种模式，“对外提供个人信息”与“委托处理个人信息”的一项重要区别在于，接收方能否自主决定如何使用个人信息。在医药企业“对外提供个人信息”的模式下，接收方也是独立的个人信息处理者，故只要具备相应的合法性基础，就可以自主决定如何使用接收的个人信息，无需再次征得医药企业的同意。而在“委托处理个人信息”的模式下，接收方则属于医药企业的“受托人”，仅能根据医药企业的指示处理个人信息，无权将个人信息用于未经医药企业许可的目的。相应的，医药企业在两种模式下亦需要承担不同的义务，在“对外提供个人信息”的模式下，根据《个人信息保护法》第二十三条的规定，医药企业需要向个人告知“接收方的名称或者姓名、联系方式、处理目的、处理方式和个人信息的种类”并取得单独同意（除非已经有其他的合法性基础）。而在“委托处理个人信息”的模式下，医药企业可以选择不向个人披露接

收方，但是必须对接收方的个人信息处理活动进行监督。综合上述的分析，“对外提供个人信息”与“委托处理个人信息”作为两种传输个人信息的模式各有优劣，前者无法直接干预接收方的处理行为，还需要承担向个人告知与取得单独同意义务，但是可以免除监督接收方的责任，而后者则恰好相反。

而第三种模式，即“作为共同处理者传输个人信息”，则与“对外提供个人信息”相对更为类似，接收方亦有权自主决定个人信息的处理行为，但区别在于，如果医药企业或接收方在处理个人信息的过程中侵害了个人信息权益，那么应当对个人承担连带责任，而非各自独立承担责任。由于这一特点可能导致风险在主体之间的传递，故在实践中，这一模式较多被应用于医药企业与关联主体之间的个人信息传输场景。

如前所述，医药企业就个人信息传输行为可能根据不同模式而需要面临不同的

医药企业根据商务需要、对于接收方的控制能力以及可能的风险因素，综合选择最适合自身实际情况的方案。

合规义务，但是依据《个人信息保护法》第四条的规定，个人信息不包括“匿名化处理后的信息”，故实务中亦有不少医药企业客户曾计划通过将个人信息进行匿名化处理以避免相应的合规义务。关于这一点，笔者理解要完成“匿名化处理”本身可能存在一定的难度。根据《个人信息保护法》第七十三条的规定：“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。”《个人信息保护法》在该条规定中并未限定“不能复原”是指哪些主体不能对处理后的信息进行复原，故依据文义解释，包括对个人信息进行匿名化处理的医药企业自身亦应当不能复原个人信息。然而，如需要满足该项标准，则相关信息的商用价值可能会明显降低，此时再进行信息传输是否还能实现商业目的就需要企业结合具体情况加以考量。

综上所述，在向其他主体传输个人信息时，采取不同的模式或方案会导致不同的权利义务关系，故笔者建议医药企业根据商务需要、对于接收方的控制能力以及可能的风险因素，综合选择最适合自身实际情况的方案。

PART 003

个人信息出境合规

《个人信息保护法》第三十八条规定了个人信息出境的若干前提条件，但由于该条并未对于如何落实这些前提条件作出细化规定，故在《个人信息保护法》出台后，个人信息出境合规并未立刻成为行业的热点。但进入2022年后，《标准合同规定（征求意见稿）》和《数据出境安全评估办法》相继发布，在个人信息出境领域，相关的操作细节亦逐步得到了填补，故个人信息出境合规也成为了必须引起重视的问题。

在实务中，不少医药企业可能有跨国背景或存在跨境合作的实际需求（例如，境外总部可能需要获取境内子公司员工的个人信息以实现全球统一管理，或为研发药物的目的需要与境外科研机构合作分享信息等），因此，对于如何实现个人信息出境合规亦有必要予以规划。根据《个人信息保护法》第三十八条的规定，除法律、行政法规或者国家网信部门规定的特殊出境条件外，通常的个人信息出境需要满足以下三种条件之一：通过出境安全评估、按照国家

不少医药企业可能有跨国背景或存在跨境合作的实际需求，因此，对于如何实现个人信息出境合规亦有必要予以规划。

网信部门的规定经专业机构进行个人信息保护认证，以及与境外接收方签订标准合同。

首先，关于申报出境安全评估的具体流程可以参照2022年9月1日生效的《数据出境安全评估办法》。就适用范围而言，如果医药企业存在被认定为关键信息基础设施运营者、处理100万人以上个人信息、两年内累计向境外提供10万人个人信息或者1万人敏感个人信息等情形之一的，则有义务在个人信息出境前申报出境安全评估。实践中亦可能存在不少在《数据出境安全评估办法》公布前已经跨境传输个人信息且符合前述情形的主体，对于这类主体，则应当在《数据出境安全评估办法》施行之日起6个月内，即2023年2月28日前完成申报并通过出境安全评估。鉴于这一时间相对紧迫，故笔者建议此类医药企业可以提前予以准备。特别是根据《数据出境安全评估办法》第5条的规定，企业在申报出境安全评估前还应当首先开展数据出境风险自评估，鉴于数据出境风险自评估的事项与个人信息保护影响评估的事项类似，且个人信息出境本就属于应当开展个人信息保护影响评估的情形之一，故笔者建议医药企业尽早梳理自身的个人信息出境行为，并开展个人信息保护影响评估，以个人信息保护影响评估的结论作为后续起草数据出境风险自评估报告的依据。

其次，对于不符合上述情形的医药企业，则可以考虑将个人信息保护认证或签订标准合同作为出境的前提条件。其中，对于个人信息保护认证的流程和细节，网信部门尚未作出明确的规定，但关于签订标准合同的流程，目前网信部门已经发布了《标准合同规定（征求意见稿）》，虽然该规定还不是最终的正式稿，但是考虑到签订标准合同亦需要与境外接收方进行沟通，故该规定亦可以作为医药企业提前与境外接收方协商的参考。

此外，医药企业在研发、试验等环节，还可能接触到一类特殊的个人信息，即“人类遗传资源”。就这一类信息，我国已经制定了包括《中华人民共和国人类遗传资源管理条例》在内的特殊管理规定，2022年3月22日，科学技术部还发布了《人类遗传资源管理条例实施细则（征求意见稿）》（以下简称“**《实施细则（征求意见稿）》**”），并明

不能简单地将《个人信息保护法》中个人信息出境的适用范围套用到人类遗传资源的国际合作中。

确人类遗传资源具体包括人类遗传资源材料和人类遗传资源信息两类。其中，人类遗传资源材料是指含有人体基因组、基因等遗传物质的器官、组织、细胞等遗传材料，而人类遗传资源信息则是指利用人类遗传资源材料产生的人类基因、基因组数据等信息资料。就人类遗传资源能否向境外传输的问题，《实施细则（征求意见稿）》在第11条明确提出："在我国境内采集、保藏和对外提供我国人类遗传资源必须由我国科研机构、高等学校、医疗机构和企业开展。境外组织、个人及其设立或者实际控制的机构不得在我国境内采集、保藏我国人类遗传资源，不得向境外提供我国人类遗传资源。"如需开展基于人类遗传资源的国际合作，需要遵循《实施细则（征求意见稿）》其他规定项下的特殊要求。

需要特别注意的是，不同于《个人信息保护法》，《实施细则（征求意见稿）》并非仅对于"境外主体"接收人类遗传资源进行限制，而是涵盖了"境外组织、个人及其设立或者实际控制的机构"。故外资控股超过50%的外商投资企业、或以VIE等方式被境外主体实际控制的境内企业都可能落入受限的范围内，故从规制对象的角度，《实施细则（征求意见稿）》比《个人信息保护法》的限制范围更宽。笔者提示医药企业亦应当注意该项差异，不能简单地将《个人信息保护法》中个人信息出境的适用范围简单地套用到人类遗传资源的国际合作中。

最后，由于医药本身就是一个强监管的行业，因此政府的执法机构或是司法部门可能存在需要访问医药企业数据并进行监管的情况。而一旦涉及外国司法或者执法机构请求访问中国境内个人信息的情形，就可能产生相应的合规问题。根据《个人信息保护法》第四十一条："非经中华人民共和国主管机关批准，个人信息处理者不得向外国司法或者执法机构提供存储于中华人民共和国境内的个人信息。"故在实践中，如果医药企业在收到外国司法或者执法机构请求后即向其提供个人信息，则可能违反上述规定。故对于如何应对外国司法或者执法机构的调取请求，企业亦应当提前制定处置预案。

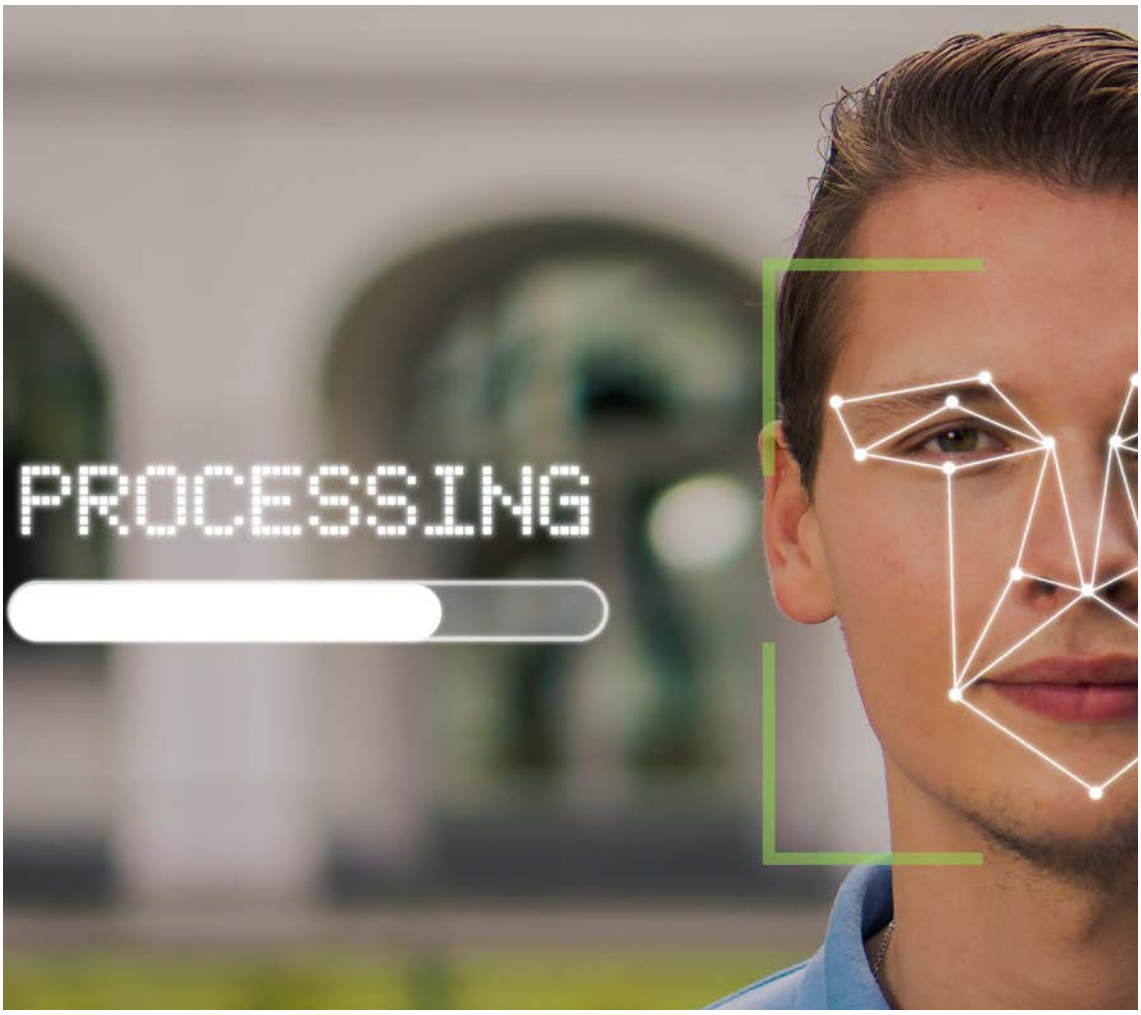
医药企业应当时刻关注最新的立法与执法动态，及时进行调整，以符合法律法规的要求，降低自身的合规风险。

PART 004

结语

综上所述，由于行业本身的特殊性，医药企业在日常经营中可能遇到较多涉及个人信息合规的场景。尤其随着各类个人信息保护的细则不断完善，未来或许会有更多适用于医药企业的个人信息保护要求，笔者建议医药企业应当时刻关注最新的立法与执法动态，及时进行调整，以符合法律法规的要求，降低自身的合规风险。

刘新宇
合伙人
私募基金与资管部
上海办公室
+86 21 6061 3700
jeffreyliu@zhonglun.com



人脸识别场景下的监管要求和合规要点分析

蔡荣伟

本篇文章将从人脸图像涉及的场景的分类出发，分析人脸图像涉及的数据信息类型，并借此厘清人脸识别场景下的监管要求和合规要点。

2021年12月，上海市徐汇区市场监督管理局（“**市监部门**”）对某公司做出行政处罚。处罚事由为，某公司在其门店装有人脸识别摄像头，收集人脸照片数十万余张，用于客流统计和客流分析（比如男女比例和年龄分析等）。但某公司收集人脸数据并未经消费者的同意，也没有告知消费者收集人脸数据的使用目的。

上述事件再次引发了公众对于“隐形”的人脸识别设备随意采集和使用人脸图像的担忧。究其根本在于，人脸图像不仅具有高度敏感的属性，又具有极易被采集的属性。一方面，人脸图像所包含的面部生物识别特征与个人密不可分。面部生物识别特征通常作为个人的生物通行证，用于身份验证。但是面部生物特征又不能被视为一般的用户密码，因为密码可以在泄露的时候进行更改，但面部生物特征却在一定程度上具有永久、不可变更和不可撤销的属性[1]。另一方面，如上述案件所述，现有的人脸识别设备能够以不易察觉甚至“无感”的方式采集人脸信息。这种非接触的、无感的采集方式，使得人脸信息相较于其他生物识别信息（如指纹、耳廓、虹膜、掌纹、DNA）更容易被采集[2]。

本篇文章将从人脸图像涉及的场景的分类出发，分析人脸图像涉及的数据信息类型，并借此厘清人脸识别场景下的监管要求和合规要点。

PART 001

对人脸图像进行处理的场景分类

根据2021年4月发布的国家标准《信息安全技术 人脸识别数据安全要求（征求意见稿）》，涉及人脸图像处理的场景可以分为三类：

1.**人脸验证**：将采集的人脸识别数据与存储的特定自然人的人脸识别数据进行比对（1：1比对），以确认特定自然人是否为其所声明的身份。典型的应用场景包括，机场、火车站的人证比对。在此场景下，人脸识别设备会将实时抓取的人脸信息与身份证所关联的人脸信息进行比对，以识别身份证所关联的身份是否与进站人一致。

1.参考《法国CNIL关于人脸识别报告》。
2.参考《法国CNIL关于人脸识别报告》。

收集使用人脸图像的个人或组织首先需要判断所收集的人脸图像涉及的数据信息类型是什么，其次则需要根据判断结果遵守相应的监管要求。

2.**人脸辨识**：将采集的人脸识别数据与已存储的指定范围内的人脸识别数据进行比对（1：N比对），以识别特定自然人。如公司的考勤打卡软件会将实时获取的人脸图片与库中存储的所有员工人脸图片进行比对后，识别“刷脸”人员的身份。

3.**人脸分析**：不开展人脸验证或人脸辨识，仅对采集的人脸图像进行统计、检测或特征分析。例如统计数量，分析年龄、性别、皮肤状态、微表情等。在上述某公司被处罚案件中，该公司使用算法对面部数据分析进店人员的年龄、性别构成等。也有智能汽车安装摄像头用于判断车主的驾驶行为是否适当，比如判断是否疲劳驾驶。

此外需要注意的是，我们在生活中经常看到的监控摄像头，虽然可能不具备上述三类对人脸图像进行特殊处理的功能，但也可能会收集人脸图像。

PART 002

人脸图像涉及的数据信息类型

相较于普通的个人信息，《个人信息保护法》（“**《个保法》**”）对**敏感个人信息**的处理与保护提出了更为严格的要求。《最高人民法院关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定》（“**《最高院人脸识别案件规定》**”）对于**面部生物识别信息**的使用亦提出了特殊的要求。此外，人脸图像还可能涉及到自然人的隐私和肖像，因此也是人格权的一部分，受到《民法典》的保护。根据《民法典》的规定，私密信息属于**隐私**，自然人的隐私权受到法律的保护。此外，在一定载体上所反映的特定自然人可以被识别的外部形象属于**肖像**，自然人的肖像权受到法律的保护。

因此，收集使用人脸图像的个人或组织首先需要判断所收集的人脸图像涉及的数据信息类型是什么，其次则需要根据判断结果遵守相应的监管要求。

1.个人信息

人脸图像属于个人信息。根据《个保法》第四条，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。上文的场景举例中，用于人脸验证、人脸辨识、人脸分析和监控摄像头摄取的人脸图像均是与已识别或可识别的

对于人脸图像是否属于敏感个人信息需要结合具体图像类型和特定的使用场景来判断。

自然人有关的各种信息。收集人脸图像需要遵守《个保法》、《消费者权益保护法》及《电子商务法》等法律法规中关于处理和保护个人信息的规定。

2.敏感个人信息

1）从人脸图像中提取的面部生物识别信息属于敏感个人信息

(i) 根据《个保法》第二十八条，敏感个人信息是一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息；(ii) 敏感个人信息包含生物识别信息。(iii) 另根据《信息安全技术　个人信息安全规范》，生物识别信息包括面部识别特征。

2）此外，一些人脸图像也可能被认定为敏感个人信息

例如，包含人脸图像的私密照片，一旦被泄露或者非法使用将会导致自身的人格尊严受到侵害，因此具有了敏感属性。

需要注意的是，对于人脸图像是否属于敏感个人信息需要结合具体图像类型和特定的使用场景来判断。例如，很多人都会使用自己的面部照片作为社交媒体（如微信、微博、脉脉等）的“头像”。由于这些人脸图像照片已经在一定范围内被公开，并不具备敏感性。因此，在一般的使用情形下，对这些“头像”的使用和处理行为遵守处理公开个人信息的要求即可。但如果处理者使用一些先进的技术手段从原本较为模糊、像素比较低的“头像”照片中提取面部识别特征，则有可能涉及到对于敏感个人信息的处理，需要遵守《个保法》对于敏感个人信息的处理要求。

3.个人隐私

根据《民法典》，隐私是自然人的私人生活安宁和不愿为他人知晓的私密空间、私密活动、私密信息。如同上文中的举例，**包含人脸图像的私密照片也会被认定为私密信息，被列入隐私权的保护范畴。**与处理个人信息相同，除法律另有规定外，处理私密信息需要取得个人的明确同意。

4.肖像

根据《民法典》，肖像是通过影像、雕塑、绘画等方式在一定载体上所反映的特定自然人可以被识别的外部形象，因此，**人**

目前对使用人脸识别设备收集、处理面部生物识别信息的监管规定最为严格，也相对完备。

脸图像可能会被认定为肖像，被列入肖像权的保护范畴。根据《民法典》的规定，除法律另有规定外，制作、使用或公开肖像，需要取得个人的同意。

PART 003

使用人脸识别的监管要求与合规要点

在对于上述数据类型使用的监管中，目前对使用人脸识别设备收集、处理面部生物识别信息的监管规定最为严格，也相对完备。人脸识别设备需要收集的面部生物识别信息属于敏感个人信息，除遵守一般的个人信息处理和保护规定外，还需要遵守《个保法》关于敏感个人信息方面的特殊规定。此外，也有部分文件对使用人脸识别设备本身提出了要求。我们梳理了相关法律法规文件，对使用人脸识别设备的监管要求和合规要点总结如下：

1. 监管要求

相关法律法规文件对使用人脸识别设备提出了详细的监管要求。

敏感个人信息、面部生物识别信息处理要求	前提	1）必须具有特定的目的和充分的必要性，并采取严格的保护措施[3]。 2）进行个人信息保护影响评估。个人信息保护影响评估应当包括下列内容[4]： a.个人信息的处理目的、处理方式等是否合法、正当、必要； b.对个人权益的影响及安全风险； c.所采取的保护措施是否合法、有效并与风险程度相适应。
	告知的事项	需告知个人如下事项： 1）个人信息处理者的名称和联系方式； 2）处理目的、处理方式，处理的个人信息种类、保存期限； 3）个人权利（如查阅、复制、更正、补充其个人信息，请求删除个人信息，撤回授权同意）的方式和程序； 4）处理的必要性； 5）对个人权益的影响；以及 6）法律、行政法规规定应当告知的其他事项。[5]
	取得同意	1）取得个人的**单独同意**，或者根据法律或行政法规的要求取得书面同意[6]。 2）**不得以如下形式取得同意：** a.信息处理者要求个人同意处理其人脸信息才提供产品或者服务的，但是处理人脸信息属于提供产品或者服务所必需的除外； b.信息处理者以与其他授权捆绑等方式要求个人同意处理其人脸信息的；以及 c.强迫或者变相强迫自然人同意处理其人脸信息的其他情形[7]。

3.《个人信息保护法》第二十八条
4.《个人信息保护法》第五十六条
5.《个人信息保护法》第十七条、第三十条
6.《个人信息保护法》第二十九条
7.《最高人民法院关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定》第四条

在线上或线下场景中使用人脸识别技术时，我们建议人脸信息的收集者和使用者关注合规要点。

使用人脸识别技术的要求	**1）人脸识别不能作为唯一的身份验证方式：** a.根据2021年8月1日生效的《最高院人脸识别案件规定》，物业服务企业或者其他建筑物管理人，不得以人脸识别作为业主或者物业使用人出入物业服务区域的唯一验证方式。 b.于2022年1月1日生效的《上海市数据条例》明确要求，在公共场所、居住小区、商务楼宇等区域不得将图像采集、个人身份识别技术作为出入该场所或区域的唯一验证方式。 c.2021年11月公布的《网络数据安全管理条例（征求意见稿）》进一步要求，不得将人脸等生物特征作为唯一的身份认证方式。 需要注意，当前生效的规定主要限制线下场景将图像采集、个人身份识别作为唯一的验证身份的方式。如《网络数据安全管理条例（征求意见稿）》相关条款生效的，还将进一步限制线上场景中将生物识别验证作为唯一的身份认证方式。 **2）公共场所安装人脸识别设备的特殊要求：** a.应当为维护公共安全所必需，并设置显著的提示标识[8]。 b.所收集的个人图像、身份识别信息只能用于维护公共安全的目的，除取得个人单独同意外，不得用于其他目的[9]。

2. 合规要点

根据上述监管要求，在线上或线下场景中使用人脸识别技术时，我们建议人脸信息的收集者和使用者对以下合规要点加以关注。

1）根据《个保法》及《最高院人脸识别案件规定》对“**取得同意**”的要求，我们建议：

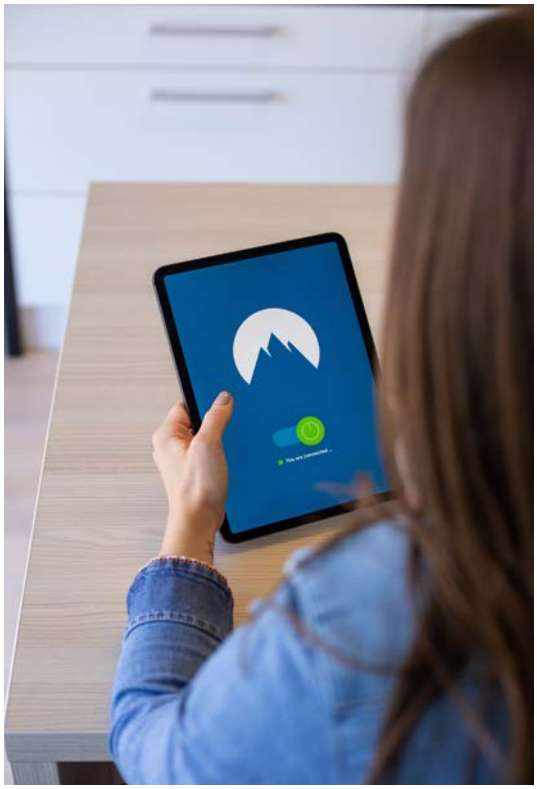
a.应避免与其他授权绑定取得个人对人脸识别的授权，也即关于人脸识别功能的授权需要提供单独的同意选项。

b.建议提供多种身份验证的方式，当个人拒绝使用人脸识别验证时，允许个人通过其他方式进行身份验证，以降低被认定为强迫或变相强迫获取面部生物识别信息的风险。

c.如果获得长期允许（如“始终允许”、“使用APP时允许”）人脸识别的同意

8.《个人信息保护法》第二十六条
9.《个人信息保护法》第二十六条

不同于线上场景中处理者与个人之间有天然的交互介质，线下场景中使用人脸识别，还需要注意获取同意的方法。



的，还需要向个人提供可以改变此种授权的途径。

2）根据《个保法》对于“告知事项”的要求，在进行人脸识别前告知个人处理者对面部生物识别信息的处理目的、处理方式、保存期限等信息，并向个人提供是否同意的选项。

此外，在线下场景中使用人脸识别技术时，一方面需要特别注意“不得将人脸识别作为唯一的验证方式”的监管要求。另一方面，不同于线上场景中处理者与个人之间有天然的交互介质（如APP的交互界面），线下场景中使用人脸识别，还需要注意获取同意的方法。我们结合实务操作经验，提供了一些**线下人脸识别场景的合规建议**：

1）优先选用非自动采集人脸图像的人脸识别设备。比如使用人脸识别屏幕，仅在个人主动点击同意或站在指定区域后，开启人脸识别。

2）对于使用自动采集人脸图的人脸识别设备（“**自动识别设备**”）的，为遵守《个保法》及《最高院人脸识别案件规定》关于“告知事项”和“取得同意”的规定，我们建议：

a.设置警示标志（如语音提示、警示线等），确保个人充分感知到特定区域使用了人脸识别设备，防止个人在不知情的情况下步入自动识别设备覆盖区域；

b.通过书面告知等形式，确保使用个人在步入自动识别设备覆盖区域前，获知处理者对面部生物识别信息的处理目的、处理方式、保存期限等信息；

c.通过书面等形式，确保取得个人的同意；

d.在行人必经的区域和通道上，应控制自动识别设备的覆盖区域，避免全覆盖；以及

e.应向个人提供除人脸识别外其他身份验证的方式，且保证当个人选择其他身份验证方式时不被自动识别设备采集人脸图像。

（陈坤亦对本文有所贡献）

蔡荣伟
合伙人
公司业务部
上海办公室
+86 21 6061 3175
roncai@zhonglun.com

自动驾驶领域的个人信息保护合规

郭建华

实践中层出不穷的汽车行业用户个人信息滥采滥用、数据泄露等事件则引起了用户对隐私安全的担忧，如何保护用户个人信息安全，成为监管与实践所需关注的一大焦点。

新一代网络通信技术与汽车、电子、道路交通系统的深度融合推动着汽车行业向车联网发展，汽车被智能化、网联化、自动化等全新概念重塑。通过搭载先进的车载传感器、控制器、执行器等装置，并融合现代通信与网络技术，智能网联汽车能够从“云-管-端”三方面实现车与X（人、车、路、云端等）智能信息交换、共享，具备复杂环境感知、智能决策、协同控制等功能，达到安全、高效、舒适、节能行驶目的，并最终可实现替代人来自动操作。自动驾驶是未来智能网联汽车发展的目标，而要实现自动驾驶，依赖于汽车的感知、决策、控制三大核心系统，这三个不同层次的系统实现其功能，都基于海量数据及个人信息的采集与处理，如何在保障安全的基础上合法地促进数据利用，是发展自动驾驶及车联网必须解决的问题。实践中层出不穷的汽车行业用户个人信息滥采滥用、数据泄露等事件则引起了用户对隐私安全的担忧，如何保护用户个人信息安全，成为监管与实践所需关注的一大焦点。

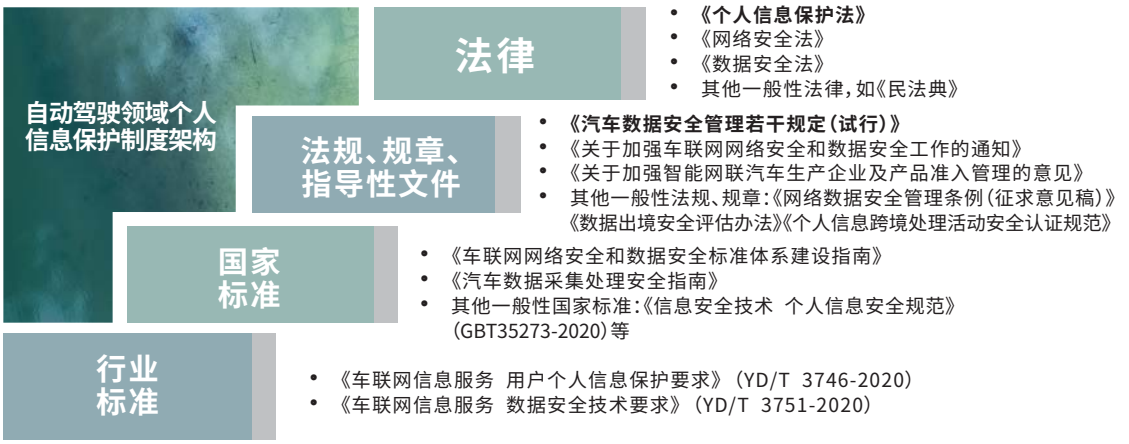
PART 001

我国自动驾驶领域有关个人信息保护的立法与标准化

作为车联网的核心要素，智能网联汽车是车联网终端用户最直接的接触对象，也是汽车数据采集和分析的硬件基础之一，其汇聚了平台层的车辆操作控制系统和终端车辆服务应用与生态，是用户个人信息采集的入口和其他数据的重要来源。随着自动驾驶技术商用化的推进，以及市场主流辅助驾驶技术的应用，我国也加强了相关领域内的数据安全和个人信息保护制度建设，除《网络安全法》《数据安全法》《个人信息保护法》等基础性法律规范以外，汽车行业数据安全相关的规章和指导性文件也逐步出台，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》等；同时，在政府引导基础上，标准委员会、产业联盟积极开展汽车数据安全与个人信息保护的相关标准制定，到目前为止行业内已发布了《车联网信息服务 用户个

汽车数据处理的四大原则：车内处理原则、默认不收集原则、精度范围适用原则和脱敏处理原则。

人信息保护要求》(YD/T 3746-2020)、《车联网信息服务 数据安全技术要求》(YD/T 3751-2020)、《汽车数据采集处理安全指南》等标准和技术文件。



《汽车数据安全管理若干规定（试行）》（下称“**《若干规定》**”）。《若干规定》已于2021年10月1日正式施行。《若干规定》以部门规章的形式将汽车设计、生产、销售、使用、运维过程中的个人信息和重要数据纳入规制范围，涵盖了包括汽车制造商、零部件及软件供应商、经销商、维修等售后服务机构以及出行服务企业等在内的所有车联网信息服务的提供者，同时明确了汽车数据处理的四大原则：**车内处理原则、默认不收集原则、精度范围适用原则和脱敏处理原则**。随着《若干规定》的实施，未来对于车联网产业数据处理行为的规制和安全管理将会更严格。

《车联网信息服务 用户个人信息保护要求》（下称“**《车联网用户个人信息保护要求》**”）是汽车行业内一个重要的个人信息保护实践标准。在车联网及自动驾驶场景下，车辆的的智能感知系统通过车外摄像头、雷达、5G及V2X等技术实现与外部环境

《汽车数据安全要求》将车联网信息服务场景下的相关数据分为了六大类；《车联网指南》明确提出了车联网数据安全的监管逻辑框架及个人信息保护的具体要求。

的交互，车辆的远程控制系统通过对外部环境数据的识别与分析、车内摄像头等对驾驶员状态、习惯等的分析来实现决策以及对车辆的操作和协同控制，车内的多媒体系统则通过收集用户数据来为其提供多样的车内应用与生态。[1]界定和明确这些过程中收集的个人信息种类和范围，是自动驾驶系统开发者以及车联网产业参与者在数据合规中面临的首要问题，《车联网用户个人信息保护要求》为此提供了较为明确的操作指引，从用户身份证明类信息、车联网信息服务内容类用户数据信息和用户服务相关信息三个方面对车联网用户个人信息进行具体描述列举，并按照敏感程度和发生泄露时对用户个人的影响分为个人一般信息、个人重要信息、个人敏感信息三个级别，在《个人信息保护法》《个人信息安全规范》的基础上做出了车联网产业内更有指导性的分级示例。

《车联网信息服务　数据安全技术要求》（下称“**《汽车数据安全要求》**”），将车联网信息服务场景下的相关数据分为了基础属性数据、车辆工况数据、环境感知数据、车控类数据、应用服务类数据以及用户个人信息六大类。对比《车联网用户个人信息保护要求》，两项标准分类维度并不一样，但其中具体的数据项目可能存在重叠，例如应用服务类数据中与用户驾驶行为、出行行为密切相关的数据以及系统应用使用行为数据，能够与其他数据的结合识别到具体的个人或分析出个人的出行习惯、常去地点、偏好等信息，从而可能落入个人信息的范畴。但二者都强调授权验证、访问控制、保密存储等安全手段的运用以保证数据的安全、完整和可用。

2022年3月7日，工信部印发了**《车联网网络安全和数据安全标准体系建设指南》**（下称“**《车联网指南》**”），明确提出了车联网数据安全的监管逻辑框架及个人信息保护的具体要求，通过规划数据全流程的监管方案，就车联网整个环节中数据收集的类型、精度、质量，数据共享和传输的操作要求和评估规范等关键问题指明了方向，强调对汽车数据过度采集和滥用问题的监管，并加强对个人信息的全方位保护。

1.吴卫明、赵彬吟：《智能网联汽车数据的归属——个人信息保护的视角》，2021年4月30日发布于律商视点。

自动驾驶系统开发者及车联网产业参与者必须充分考虑不同场景下如何确保数据来源的合法性。

PART 002

重要数据环节、典型场景下的个人信息合规要点提示

1.个人信息的收集和使用

智能网联汽车及自动驾驶个人信息的收集行为发生在物联网场景下，收集个人信息的介质和用户来源更加多元化，不仅仅包括车载的终端服务应用和生态应用，还包括车内外摄像头、传感器、激光雷达等，所收集的个人信息所属的主体也不仅限于车主、驾驶员、乘客，还包括了行人等非驾驶活动参与者。[2]这也使得在个人信息收集环节，自动驾驶系统开发者及车联网产业参与者无法完全通过“告知-同意”的途径取得个人信息主体的明示同意，必须充分考虑不同场景下如何确保数据来源的合法性。

（1）通过车外摄像头采集包含人脸、车牌等个人信息的环境数据

在自动驾驶以及现阶段的辅助驾驶场景下，通过车外摄像头、雷达等收集外部环境数据是实现自动驾驶、辅助驾驶功能的前提和关键，但却无法向行人履行告知义务，取得其明示授权同意。《个人信息保护法》第13条规定了“紧急情况下为保护自然人的生命健康和财产安全所必需”的，可以不取得个人同意。《若干规定》从目的解释的角度，对该条款进行了细化：出于保证行车安全的需要，无法征得车外个人同意的，可以适用授权同意的例外规定，但《若干规定》同时对数据处理行为做出限制，即：采集的个人信息必须为车外个人信息，传输方向为向车外传输，并且应当进行匿名化处理[3]，包括但不限于删除含有能够识别自然人的画面，或者对画面中的人脸信息进行局部轮廓化处理等，这也符合最小必要原则的要求。

因此在通过车外摄像头采集车外环境数据时，自动驾驶系统开发者以及汽车摄像头、雷达等零部件供应商，应当注意：

1)区分车外环境数据中的行人人脸信息、过往车辆车牌信息，并对画面中的人脸信息进行局部轮廓化处理，含有能够识别

2.参见王源：《自动驾驶场景下的数据安全标准体系建设》，2020年6月20日载于数据法盟。
3.根据《个人信息安全规范》第3.14条的界定，匿名化是指通过对个人信息的技术处理，使得个人信息主体无法被识别或者关联，且处理后的信息不能被复原的过程。个人信息经匿名化处理后所得的信息不再属于个人信息。

自然人的画面应当即用即删，不存储和向云端、远程控制系统传输；

2)根据车外环境数据监测需求及安全驾驶的需要，合理确定车外摄像头、雷达等设备的覆盖范围和分辨率。

(2)生物识别系统/应用

通过指纹或面部解锁的生物识别系统已经在手机、在线支付、门禁等场景和领域中广泛使用，现阶段很多智能网联汽车也将生物识别系统作为亮点之一，并且通常与智能座舱的基础功能相关联，例如某品牌汽车智能视觉系统可通过人脸识别登录账户，同步座椅、后视镜、导航、音乐等个性化设置，同时支持多个账号切换[4]。除此之外，自动驾驶或辅助驾驶系统还会通过车内摄像头对驾驶员的人脸、虹膜等个人信息进行收集，以检测驾驶员的疲惫状态，调整自动驾驶或辅助驾驶的指令，或唤起警示。

根据《个人信息安全规范》，生物识别信息属于个人敏感信息[5]。收集个人敏感信息应当取得个人的单独同意，还应当向个人告知处理敏感个人信息的必要性以及对

4.https://www.pcauto.com.cn/nation/1583/15837168.html，最后访问日期：2022年8月19日。
5.详见《信息安全技术 个人信息安全规范》(GBT 35273-2020)附录B。

自动驾驶系统开发者在利用生物识别系统完成无钥匙进入、智能座舱、自动或辅助驾驶等功能时，应当注意特定合规义务。

个人权益的影响。《若干规定》同样遵循了《个人信息保护法》所确定对个人敏感信息予以特殊保护的要求。因此，自动驾驶系统的开发者在利用生物识别系统完成无钥匙进入、智能座舱、自动或辅助驾驶等功能时，应当注意：

1）以显著方式履行告知说明义务，包括但不限于通过用户说明、车载显示面板、智能语音提示、汽车使用相关应用程序等，充分说明收集个人生物识别信息的种类、范围、具体应用场景、目的、保护措施等，允许用户自行设定同意的期限，并通过用户勾选、点击、口头确认等方式取得其明示同意，在收集过程中应当在车载显示面板提示状态；

2）评估个人生物识别信息收集的必要性，生物识别信息的收集应当直接服务于个人的目的，包括增强行车安全、智能驾驶等；

3）欧盟数据保护委员会（EDPB）在GDPR个人数据保护框架下发布了《在联网车辆和出行相关应用环境下处理个人数据的指南，第1/2020号》，其中第2.1.2条提出，为了保证个人对其信息的完全控制权，在收集用户个人信息生物识别信息以实现登录时，应当同时提供不基于生物识别信息的替代方案，例如物理钥匙或密码，并且不得对个人信息主体施加额外的限制。[6]虽然我国相关法律规范及标准并未明确提及，但考虑到强化个人信息保护的监管趋势以及在自动化决策程序的规制中已有类似的规定，自动驾驶系统开发者及智能汽车厂商应重视并保留非基于生物识别信息的替代方案；

4）根据《个人信息安全规范》第6.3条的要求，自动驾驶系统开发者及智能汽车厂商、相应汽车使用软件提供商原则上不能储存个人生物识别信息，如果确有必要，应在车辆终端采集中实现身份识别、认证等功能，或仅存储个人生物识别信息的摘要信息，在使用面部识别特征、指纹、掌纹、虹膜等实现识别身份、认证等功能后删除可提取个人生物识别信息的原始图像。

（3）智能语音识别系统

通过自动语音识别指令对人声进行分

6.Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications, Adopted on 9 March 2021, European Data Protection Board, PP. 19-20.

声纹属于生物识别信息，因此自动驾驶系统开发者及智能汽车厂商同样需要履行收集个人敏感信息时的特别义务。

析，进而进行协同控制的智能语音识别系统，能够帮助自动驾驶汽车实现车内功能和场景的多样化，也能真正解放驾驶者，实现这一功能可能需要收集用户的语音、声纹信息，声纹同指纹、人脸信息一样，属于生物识别信息，因此自动驾驶系统开发者及智能汽车厂商同样需要履行收集个人敏感信息时的特别义务。

通常来说，用户可以通过预先设置唤醒词，唤醒车辆智能语音系统，并通过发出进一步的指示，来实现具体的场景功能，如拨打电话、播放音乐等。而为了能够随时接收用户的指令，车载麦克风等组件实际上随时处于保持打开的状态。因此在智能语音识别功能中，应当注意：

1)以用户说明、车载显示面板、智能语音提示、汽车使用相关应用程序等显著方式向用户履行告知说明义务，并通过用户勾选、点击、口头确认等方式取得其明示同意；

2)在收集过程中应当在车载显示面板提示麦克风的开启状态，开启录音时应以显著方式提示；

3)根据《若干规定》确立的默认不收集原则，智能语音识别功能模块不应设置为默认开启，应当由用户主动开启，并且在用户发出指令前，应默认不收集用户的语音、声纹信息；我们理解，该功能的实现重点在于听懂指令/口令内容，而与身份识别没有直接关联，并不依赖于发出指令者的身份，因此或可以对声音进行模糊化、匿名化、不进行身份识别的处理。

(4)导航功能

导航功能是自动驾驶汽车的基础功能之一，开启导航需要收集并使用用户的位置信息，包括实时定位；连续的地理位置信息还能形成用户的行踪轨迹信息。对位置信息、车辆轨迹信息进行分析，能够推知用户个人的生活习惯、性格特征、兴趣爱好、工作和居住地址以及宗教信仰、性取向等个人私密信息，[7]根据《个人信息安全规范》，位置信息，尤其是精准定位信息和行踪轨迹属于个人敏感信息。根据《车联网用户个人信息保护要求》第5.2条对车联网数据收集行为的界定，当用户使用离线地图

7.Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications, Adopted on 9 March 2021, European Data Protection Board., PP. 18-19.

自动驾驶技术的开发可能涉及跨境合作和数据的跨境提供，汽车数据作为强监管的对象之一，其出境问题显得更加敏感。

功能时，由于自动驾驶系统开发者及智能汽车厂商，或导航应用的提供者并未收集和访问用户的位置信息，并回传至远程操作系统，因此此时并不构成数据收集行为。除此之外，自动驾驶系统开发者及智能汽车厂商在收集和访问地理位置信息时应当注意：

1)位置信息的收集应当不以默认开启的方式进行，只有当用户启用导航功能时才能收集用户的位置信息，在导航期间，应当在车载显示面板提示GPS开启及车辆实时位置收集的状态；

2)以用户说明、车载显示面板、智能语音提示、汽车使用相关应用程序等显著方式向用户履行告知说明义务，并通过用户勾选、点击、口头确认等方式取得其明示同意；

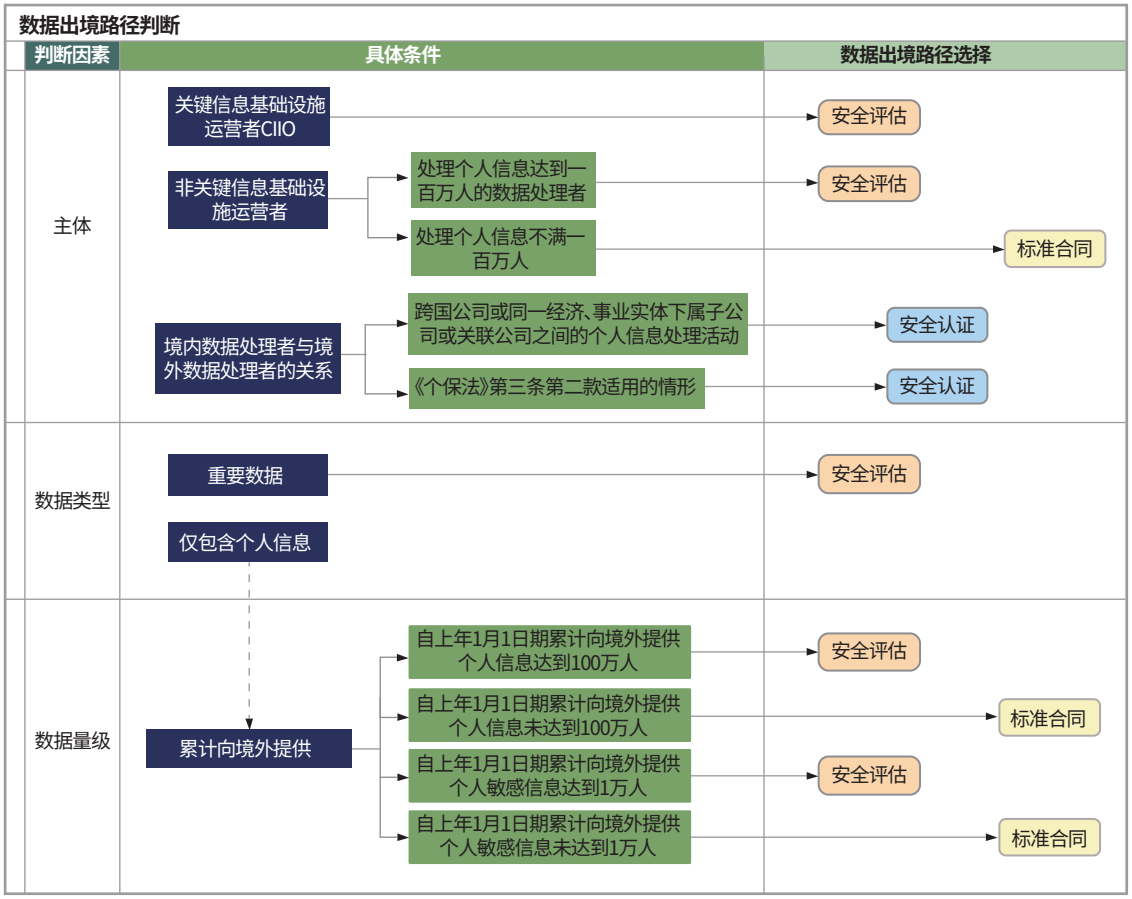
3)《若干规定》明确要求汽车数据除非确有必要，不向车外提供的原则。因此对于自动驾驶系统开发者及智能汽车厂商而言，要加强车载芯片计算能力开发和智能汽车的本地储存能力的提升，对于行踪轨迹数据、常用地点数据，应当存储在车内，尽量避免向云端及远程操作系统中传输。

2.个人信息的出境

汽车行业是一个高度全球化的行业，自动驾驶技术的开发可能涉及跨境合作和数据的跨境提供，汽车数据作为强监管的对象之一，其出境问题显得更加敏感。

2022年6月，国家互联网信息办公室（下称“**国家网信部门**”）发布了《个人信息出境标准合同规定（征求意见稿）》及其附件；7月又发布了《数据出境安全评估办法》，该办法将于2022年9月1日正式生效。加上此前全国信安标委发布的《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》，我国的数据出境管理基本形成“安全评估”“安全认证”“标准合同”三条路径，每条路径都有不同的适用范围和条件（如下图所示），企业无法完全自主选择。

自动驾驶系统开发者及智能汽车厂商应当及时梳理所掌握的数据规模。



其中，根据《数据出境安全评估办法》的规定，1)数据处理者向境外提供重要数据，或2)处理个人信息达到一百万人的数据处理者向境外提供个人信息，或3)自上年1月1日起累计向境外提供10万人个人信息或1万人敏感个人信息的数据处理者，应当进行数据出境安全评估。“100万”、“10万”、“1万”的单位是人，因此是指对应个人信息主体的人数，而不是个人信息的条数。自动驾驶系统开发者及智能汽车厂商应当及时梳理所掌握的数据规模。

自动驾驶系统开发者或智能汽车厂商

应当对自动驾驶与车内应用场景中的个人信息处理活动进行全面梳理，确定是否涉及敏感个人信息，并评估个人信息的收集是否符合最小必要原则。

还需要注意的是，《若干规定》第3条将涉及个人信息主体超过10万人的个人信息，以及包含人脸信息、车牌信息等的车外视频、图像数据定义为重要数据，这意味着当自动驾驶系统开发者或智能汽车厂商向境外提供的数据包含这两类数据时，其构成“向境外提供重要数据”，将直接触发数据出境安全评估要求，汽车企业开展数据跨境活动和申报安全评估前，进行风险自评估是必备的前置程序，因此自动驾驶系统开发者及智能汽车厂商如有数据出境的需求，应当提早做好准备。

PART 003

智能汽车企业如何做好合规准备

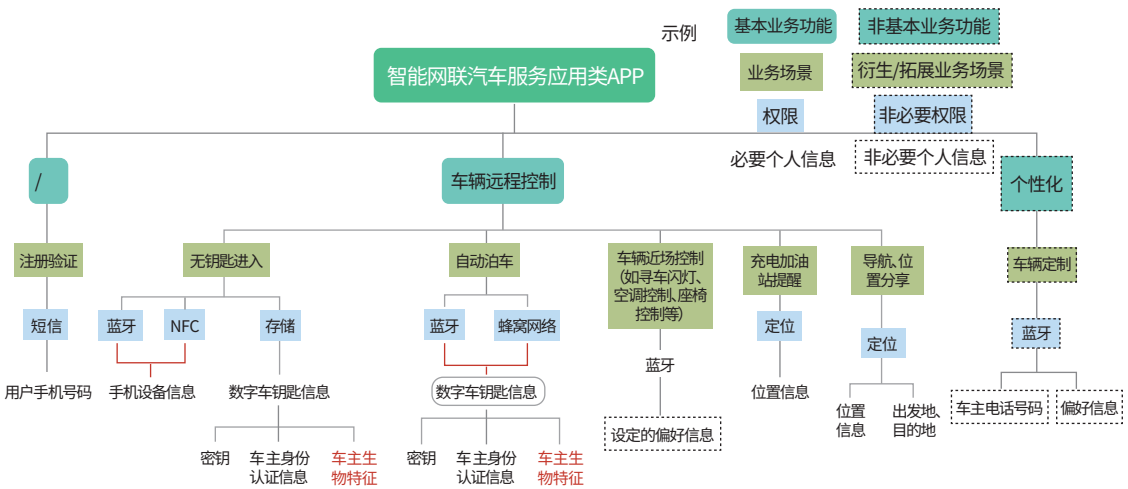
从智能网联汽车及自动驾驶技术的发展现状和实践，我们建议可以从以下两个方面做好合规准备：

1. 短期规划：以业务为导向

（1）智能网联汽车作为车联网终端用户最直接的接触对象和车辆操作控制系统的载体，是用户个人信息采集的入口，自动驾驶系统的开发者及智能汽车厂商应当对自动驾驶与车内应用场景中的个人信息处理活动进行全面梳理，包括各场景下可能涉及的个人信息的类型、范围，形成个人信息目录/清单，确定是否涉及敏感个人信息，并评估个人信息的收集是否符合最小必要原则。根据此前曝出多个案例以及7月21日网信办对某移动出行平台企业做出的处罚决定显示，违法收集、过度收集用户个人信息，过度、频繁索取权限和未准确、清晰履行告知义务仍是智能网联汽车行业存在的普遍问题以及合规监管的重点。

由于智能网联汽车与用户的交互过程往往通过车载智能模块、汽车预置软件平台上相关服务应用和生态应用程序完成，有的还可以通过驾驶者/用户个人所持有的手机等智能移动设备完成[8]，在评估这些应用收集个人信息的必要性时，智能汽车厂商可参考《常见类型移动互联网应用程序必要个人信息范围规定》进行；

8.参见全国汽车标准化技术委员会、智能网联汽车分技术委员会：《智能网联汽车与移动终端信息交互功能标准化需求研究报告》，2020年9月。



(2) 量身定制符合企业实际业务产品需求和个人信息处理活动的隐私政策，并将其嵌入用户手册或用户协议中，并在智能网联汽车终端以格式化文本形式展示，在履行告知义务基础上合理区分不同车联网场景下的个人信息收集活动，设计“告知-同意”规则及用户交互界面，避免一揽子授权；

(3) 根据个人信息的分类分级标准确定包括存储、使用、销毁、安全保护等全流程的、符合不同等级安全要求的个人信息保护策略和具体措施，对生物识别信息、位置信息和行踪轨迹等敏感个人信息做好匿名化处理；

(4) 对数据出境活动进行梳理和盘点，根据数据出境路径的适用范围及条件，合理规划数据出境数量，同时，对不再具备利用价值的数据以及无需保留精度的数据及时进行删除或匿名化、模糊化的处理，避免因达到“处理100万人以上个人信息”这一主体身份标准而直接触发安全评估路径适用条件。

2. 长期规划：以组织管理为维度

(1) 指定个人信息保护负责人，完善数据及个人信息保护合规管理组织体系与制度规则，建立常态化人信息保护影响评估

车联网和自动驾驶技术的发展给工业时代的汽车行业带来了巨大变革和商机，也带来了巨大的合规压力。

制度与流程、以数据出境风险自评估为抓手的数据安全保护评估机制（包括组织人员、工作方式等），定期对个人信息处理的合法合规性进行安全评估；

（2）加强智能汽车车载芯片计算能力开发和智能汽车的本地储存能力提升，除《网络安全法》外，工信部2021年发布的《关于加强智能网联汽车生产企业及产品准入管理的意见》要求企业在中国境内运营中收集和产生的个人信息和重要数据在境内存储，因此自动驾驶系统的开发者及智能汽车厂商应尽早规划境内数据存储中心。

车联网和自动驾驶技术的发展给工业时代的汽车行业带来了巨大变革和商机，也带来了巨大的合规压力。随着我国个人信息保护制度框架的形成以及实践中针对互联网行业的个人信息保护执法活动越来越频繁和细致，自动驾驶系统的开发者及智能汽车厂商，除了关注汽车行业内的法律法规更新外，更应该尽早开启个人信息保护合规实践工作。

郭建华
非权益合伙人
知识产权部
南京办公室
+86 25 6951 1898
guojianhua@zhonglun.com

个人金融信息保护的合规要点解读

李瑞 贾申 钟俊鹏 姚远

本文梳理了涉及个人金融信息处理的重要业务场景下的核心合规义务，并为如何展开个人金融信息的全流程的生命周期保护提供更具可操作性的合规建议，以供金融业机构参考。

个人金融信息保护属于个人信息保护领域、消费者权益保护领域及金融监管领域共同关注的议题，可能涉及的监管部门包括央行、银保监会、证监会等金融行业主管部门，网信办、工信部等网络与数据安全主管部门以及市场监督管理局等消费者权益保护主管部门；触及的合规义务主体包括传统金融持牌机构以及各类金融科技公司；具有业务场景复杂、合规要求交错综合等特点，是金融数据合规工作中的难点和重中之重。

在金融数字化不断驱动行业转型的趋势下，如何确保金融业机构在对个人金融信息进行共享利用、价值挖掘的同时，能够将相关生命周期保护的合规要求有针对性地落地，还需要深入金融业机构展业运营的各业务场景当中。为了帮助金融业机构进一步落实《个人信息保护法》（“**《个保法》**”）、《金融消费者权益保护实施办法》（“**《金融消保实施办法》**”）等相关规定中的个人金融信息保护要求、提升个人金融信息全流程处理的规范性，本篇将结合《个人金融信息保护技术规范》（“**《个金技术规范》**”）[1]介绍个人金融信息合规工作中的要点，为金融业机构梳理个人金融信息的定义及范围、分类分级规则。我们也选取了金融业机构日常业务开展中的外部合作管理、跨境传输、App运维、营销宣传及自动化推广等四个涉及个人金融信息处理的重要业务场景，梳理了各场景下的核心合规义务，并为如何展开个人金融信息的全流程的生命周期保护提供更具可操作性的合规建议，以供金融业机构参考。

PART 001

个人金融信息的资产梳理

1.个人金融信息的定义

在展开个人金融信息保护工作之前，首先需要明确何为个人金融信息。根据个金技术规范第3.2条，“个人金融信息”是指“金融业机构[2]通过提供金融产品和服务或

1.根据我们的经验，个金技术规范虽然仅是推荐性标准，但是其内容为金融机构处理个人金融信息过程中涉及的安全核查及评估提供了详尽的规范指引，是金融监管实务中的重要参考依据。
2.金融业机构的具体定义，可以参见作者此前金融数据合规系列文章《举一纲而万目张——金融数据的分类分级与全生命周期保护》。具体而言，其不仅指传统的持牌金融机构，还包括其他提供金融产品/服务从而涉及个人金融信息处理的新型金融业机构。

金融业机构进行个人金融信息资产梳理的核心是建立完善的、动态可调的分类分级体系。

者其他渠道获取、加工和保存的个人信息”，具体包括账户信息、鉴别信息、金融交易信息、个人身份信息、财产信息、借贷信息及其他反映特定个人某些情况的信息。据此，个人金融信息不等同于个保法所提及的金融账户信息，个人金融信息范围显然要更加广泛。另外，根据个保法第28条敏感个人信息的定义及示例[3]，个人金融信息也并不完全落入敏感个人信息的范畴，而需结合相关信息泄露的影响做综合判断。

2.个人金融信息的分类分级

金融业机构进行个人金融信息资产梳理的核心是建立完善的、动态可调的分类分级体系。个人金融信息的分类规则较为明确，参考个金技术规范，金融业机构可以从“账户信息、鉴别信息、金融交易信息、个人身份信息、财产信息、借贷信息及其他信息”将个人金融信息粗分为7大子类，再进一步根据自身组织经营情况向下细分。在明确个人金融信息的分类后，金融业机构应当搭建个人金融信息的分级框架。依据信息遭到未经授权的查看或未经授权的变更后所产生的影响和危害，个金技术规范将个人金融信息按敏感程度从高到低分为为C3、C2、C1三个等级，并示例了具体的个人金融信息等级供参考（如下表1所示）：

3.根据个保法第28条，金融账户属于敏感个人信息。

个金技术规范将个人金融信息按敏感程度从高到低分为C3、C2、C1三个等级。

表1 个人金融信息级判断规则

级	描述	具体信息范围
C3	一旦遭到未经授权的查看或未经授权的变更，会对个人金融信息主体的信息安全与财产安全造成严重危害。	主要为用户鉴别信息，包括但不限于： • 支付敏感信息； • 账户（包括但不限于支付账号、证券账户、保险账户）登录密码、交易密码、查询密码； • 用于用户鉴别的个人生物识别信息。
C2	一旦遭到未经授权的查看或未经授权的变更，会对个人金融信息主体的信息安全与财产安全造成一定危害。	主要为可识别特定个人金融信息主体身份与金融状况的个人金融信息，以及用于金融产品与服务的关键信息，包括但不限于： • 支付账号及其等效信息，如支付账号、证件类识别标识与证件信息（身份证、护照等）、手机号码； • 账户（包括但不限于支付账号、证券账户、保险账户）登录的用户名； • 用户鉴别辅助信息，如动态口令、短信验证码、密码提示问题答案、动态声纹密码；若用户鉴别辅助信息与账号结合使用可直接完成用户鉴别，则属于C3级信息； • 直接反映个人金融信息主体金融状况的信息，如个人财产信息（包括网络支付账号余额）、借贷信息； • 用于金融产品与服务的关键信息，如交易信息（如交易指令、交易流水、证券委托、保险理赔）等； • 用于履行了解客户要求，以及按行业主管部门存证、保全等需要，在提供产品和服务过程中收集的个人金融信息主体照片、音视频等影像信息； • 其他能够识别出特定主体的信息，如家庭地址等。
C1	一旦遭到未经授权的查看或未经授权的变更，可能会对个人金融信息主体的信息安全与财产安全造成一定影响。	主要为机构内部的信息资产，指供金融业机构内部使用的个人金融信息，包括但不限于： • 账户开立时间、开户机构； • 基于账户信息产生的支付标记信息； • C2 和C3 级信息中未包含的其他个人金融信息。

分级标准有助于厘清个人金融信息与个保法下的敏感个人信息的关系。

我们理解，上述分级标准有助于厘清个人金融信息与个保法下的敏感个人信息的关系：首先，个金技术规范对于C2、C3等级信息的描述与个保法下个人敏感信息“一旦泄露或者非法使用，容易导致自然人的财产安全受到危害的个人信息”的属性基本一致，因此，宜将C2、C3级信息归入敏感个人信息，提高其保护合规标准，在处理此类信息时还需要注意遵循单独同意、进行个人信息保护影响评估等特殊处理规则。其次，对于C1级信息，由于其一旦遭到未经授权的查看或未经授权的变更，可能会对个人金融信息主体的信息安全与财产安全造成一定影响，但这种影响是否达到个保法上侵害自然人的人格或危害人身、财产安全的程度从而构成个人敏感信息，则需结合具体场景下判定。

最后，金融业机构在进行个人金融信息资产梳理和等级判定时还应当注意：

- 鉴于《金融数据安全 数据安全分级指南》（“**金融数据分级指南**”）提供了与个金技术规范具有融合性的金融数据的分类分级框架，而个人金融信息又属于金融数据，并且金融数据分级指南中提供的分级框架下的2至4级与C1、C2、C3级信息存在一一对应的关系，因此我们建议，金融业机构可以在金融数据资产清单对应的金融数据等级中嵌入个人金融信息模块，将个人金融信息融合进金融数据分级框架中进行一体化统筹管理，从而减轻需要分别管理多个数据资产清单的工作压力；
- 若干低敏感程度信息经过组合、关联和分析后可能产生高敏感程度信息，例如账户登录的用户名和动态口令均为C2级别信息，但如果两者经过组合、关联后可完成用户鉴别和登录，则产生的信息属于C3级的用户鉴别信息。金融业机构在从事此类行为后，应注意对相关个人金融信息重新进行分级；
- 同一信息在不同的服务场景中可能处于不同的级别，应依据服务场景以及信息在该场景下的作用，对信息等级进行场景化识别。

基于不同的个人金融信息级别，个金技术规范提供了相应的技术和管理要求的参考。

PART 002

个人金融信息生命周期式保护的技术要求

从收集、传输、存储、使用再到删除和销毁，个人金融信息的生命周期的各环节设置与个保法、《金融数据安全　数据生命周期安全规范》等规定基本一致。基于不同的个人金融信息级别，个金技术规范提供了相应的技术和管理要求的参考，金融业机构可以参照相关要求，设计并实施覆盖个人金融信息全生命周期的安全保护策略。篇幅所限，我们仅在下表2中归纳了主要环节中的典型合规义务：

金融业机构可以参照相关要求，设计并实施覆盖个人金融信息全生命周期的安全保护策略。

表2 个人金融信息生命周期保护技术及管理要求示例

处理环节及场景	个金技术规范中的3级个人金融信息适用规则	合规义务示例
收集	一般性规则	• 确保收集信息来源的可追溯性； • 采取技术措施引导个人金融信息主体查阅隐私政策，并获得其明示同意后方可收集； • 应采取屏蔽措施防止用户银行卡、网络支付密码等密码类信息明文显示。
	C2、C3级信息特殊规则	• 不应委托授权无金融业相关资质机构收集C2、C3级信息； • 对于C3级信息，通过受理终端、客户端应用软件、浏览器等方式收集时，应使用加密等技术措施。
传输	一般性规则	• 建立相应的个人金融信息传输安全策略和规程，采用安全通道、数据加密等安全控制措施； • 传输前通信双方应通过技术手段进行身份鉴别认证； • 接收方应对接收的信息进行完整性校验。
	C2、C3级信息特殊规则	• 通过公共网络传输时，C2、C3级信息应使用加密通道或数据加密的方式进行传输。
存储	一般性规则	• 不应留存非本机构的C3级信息，若确有必要留存，则应取得个人金融信息主体及账户管理机构的授权； • 符合个人金融信息主体授权使用的目的所必需的最短时间要求； • 将去标识化、匿名化后的数据与可用于恢复识别个人的信息采取逻辑隔离的方式进行存储。
	C2、C3级信息特殊规则	• C3 级信息应采用加密措施确保数据存储的保密性

处理环节及场景		个金技术规范中的3级个人金融信息适用规则	合规义务示例
使用	共享和转让	一般性规则	• 共享和转让前，开展个人金融信息安全影响评估、接收方信息安全保障能力评估，并签署数据保护责任承诺； • 因收购、兼并、重组、破产等情况而发生共享和转让的，应使用逐一传达（或公告）的方式通知个人金融信息主体。（注：但如果在上述过程中个人金融信息处理的目的发生变化的，应根据个保法要求重新取得信息主体的明示同意）。
		C2、C3级信息特殊规则	• C3 级信息以及 C2 级信息中的用户鉴别辅助信息不应共享、转让。
	公开披露	一般性规则	• 事先开展个人金融信息安全影响评估； • 未经个人金融信息主体同意，不应公开披露个人生物识别信息。
		C2、C3级信息特殊规则	• C3 级信息以及 C2 级信息中的用户鉴别辅助信息不应公开披露；
	委托处理	一般性规则	• 不应超出已征得个人金融信息主体授权同意的范围； • 对委托行为进行个人金融信息安全影响评估； • 对第三方机构等受委托者进行监督，签署合同并进行安全检查和评估； • 未经书面授权，受委托者不得转委托处理； • 委托关系解除时（或外包服务终止后），受委托者应按照金融业机构的要求销毁其处理的个人金融信息，并承担后续保密责任； • 对外部嵌入或接入的SDK等自动化工具应展开技术检测，对其收集的个人金融信息进行审计，发现超范围的及时断开。
		C2、C3级信息特殊规则	• C3级信息以及C2级信息中的用户鉴别辅助信息，不应委托给第三方机构进行处理。

处理环节及场景		个金技术规范中的3级个人金融信息适用规则	合规义务示例
	加工处理	一般性规则	• 清洗和转换过程中对个人金融信息进行保护； • 对匿名化或去标识化处理的数据集或其他数据集汇聚后重新识别出个人金融信息主体的风险进行识别和评价。
		C2、C3级信息特殊规则	• 清洗和转换过程中对C2、C3级信息采取更加严格的保护措施。
	汇聚融合	一般性规则	• 超出收集时所声明的使用范围使用的，应再次征得个人金融信息主体明示同意； • 开展个人金融信息安全影响评估。
删除		一般性规则	• 采取技术手段在金融产品和服务所涉及的系统中去除个人金融信息，使其保持不可被检索和访问； • 依法依规响应个人金融信息主体删除其个人金融信息的要求。
销毁		一般性规则	• 建立个人金融信息销毁策略和管理制度，明确销毁对象、流程、方式和要求； • 对个人金融信息存储介质销毁过程进行监督与控制； • 销毁过程应保留有关记录； • 采用不可恢复的方式（如消磁、焚烧、粉碎等）对不再使用的存储个人金融信息的介质进行销毁处理。

个金技术规范还特别关注支付敏感信息，并在部分环节中针对性地设置了特殊合规义务。

此外，个金技术规范还特别关注支付敏感信息，并在部分环节中针对性地设置了特殊合规义务。根据个金技术规范，“支付敏感信息”是指“支付信息中涉及支付主体隐私和身份识别的重要信息，具体包括银行卡磁道数据（或芯片等效信息）、卡片验证码（CVN和CVN2）、卡片有效期、银行卡密码、网络支付交易密码等用于支付鉴权的个人金融信息。”由于其敏感性，支付敏感信息一般属于C3级别的个人金融信息，因此，除适用上述C3级别信息处理的一般合规要求外，处理支付敏感信息时还需履行以下的特殊合规义务：

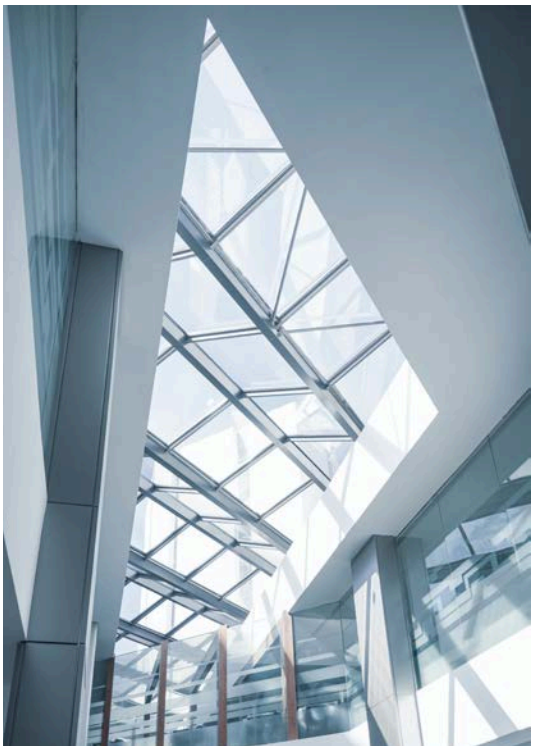


表3 C3级中支付敏感信息的特殊合规义务

处理环节	合规义务示例
收集	网络支付业务系统中，应采取具有信息输入安全防护、即时数据加密功能的安全控件对支付敏感信息的输入进行安全保护，并采取有效措施防止合作机构获取、留存支付敏感信息。
传输	支付敏感信息的安全传输技术控制措施应符合有关行业技术标准与行业主管部门有关规定要求。
存储	受理终端、个人终端及客户端应用软件均不应存储支付敏感信息及个人生物识别信息的样本数据、模板，仅可保存完成当前交易所必需的基本信息要素，并在完成交易后及时予以清除。

金融业机构与外部机构合作开展个人金融信息处理活动已然成为业内常态，合作内容通常涉及收集端和使用端两个环节。

PART 003

个人金融信息外部合作管理

金融业机构与外部机构合作开展个人金融信息处理活动已然成为业内常态，合作内容通常涉及以下两个环节：一是在收集端，即通过数据提供商、互联网平台等外部渠道间接收集个人金融信息；二是使用端，主要是对已收集的信息委托外部机构进行分析、加工等处理活动，或向其他关联和非关联合作方共享以合作开展相关业务。

就收集端而言，金融业机构需要重点对第三方个人信息来源的合法性进行审核，形成规范性审核流程，并且应要求外部合作机构确保其将个人信息提供给金融业机构的情形已经明确为个人信息主体所知晓并同意。如果相关收集行为是为了对相关用户信用状况进行判断，涉及从事个人征信业务，金融业机构还必须核实该个人金融信息提供方是否为个人征信持牌机构。[4]此外，在外部机构主要通过爬虫技术获取信息的情形下，金融业机构需要注意核实信息来源是否确为公开网站等渠道、是否为个人信息主体同意并主动公开，例如爬取用户通讯录中第三人联系信息的行为，就往往因缺乏相应信息主体的同意，不具有合法性基础。

就使用端而言，根据个金技术规范的要求，金融业机构在其个人金融信息保护制度体系的管理范畴中，除了本机构，还应涵盖相关外包服务机构与外部合作机构，确保相关制度传达至外部合作方，并且在委托处理或与外部机构共享前对上述机构进行审查评估。在此基础之上，金融业机构在就个人金融信息开展外部合作时还应当特别注意以下合规义务：

- **妥善签署合作协议，**协议应明确双方个人金融信息保护责任、保密义务、监督、处罚、合同终止和突发情况下的应急处置，并要求外部机构不留存C2、C3级信息；如因业务需要（清分清算、差错处理）确需留存的C2级信息（如支付账号），应明确合作方保密义务与保密责任，并落实相应的安全控制措施、将有关

4.《征信业务管理办法》第3条："本办法所称征信业务，是指对企业和个人的信用信息进行采集、整理、保存、加工，并向信息使用者提供的活动。本办法所称信用信息，是指依法采集，为金融等活动提供服务，用于识别判断企业和个人信用状况的基本信息、借贷信息、其他相关信息，以及基于前述信息形成的分析评价信息。"

个金技术规范确立了个人金融信息本地化存储原则下的跨境传输制度。

资料留档备查；

- **访问权限与控制：**对于可能访问个人金融信息的外部机构及其人员，应要求外部机构同时向有关人员传达个人金融信息保护安全要求，并与其签署保密协议、对协议履行情况进行监督；
- **数据库的运维主体：**除委托外包服务机构处理个人金融信息的情形之外，对于其他外部合作机构，不应将存储个人金融信息的数据库交由其运维；
- **监督与检查：**定期以信息安全评估、现场检查等方式对外部机构个人金融信息保护措施落实情况进行确认；
- **数据分析中的信息脱敏：**开展数据分析等方面的合作时，应确保使用的是脱敏后的个人金融信息；
- **合作方为互联网平台企业时的特殊义务：**如外部机构为互联网平台企业，则未经个人授权同意，应要求其不得跨平台传递个人金融信息。

另外，当出现个人金融信息泄露事件时，如果还因此产生了一定经济损失或社会影响，金融业机构还应及时委托外部的安全评估机构，重新进行相关安全评估与检查活动，同时将相关结果报送行业主管部门。

PART 004

个人金融信息跨境传输

在跨国金融业机构进行用户研究，或境内外金融机构在处理跨境支付、对外联络等业务场景时，通常会产生个人信息跨境传输的需求。需要注意的是，个金技术规范确立了个人金融信息本地化存储原则下的跨境传输制度。[5]如因业务需要，金融业机构确需向境外机构（含总公司、母公司或分公司、子公司及其他为完成该业务所必需的关联机构）提供个人金融信息时，需满足以下要求：

5.2011年央行《关于银行业金融机构做好个人金融信息保护工作的通知》就已经要求银行业金融机构在中国境内收集的个人金融信息的储存、处理和分析应当在中国境内进行，而个金技术规范第7.1.3条则进一步将该义务扩大至所有金融业机构涉及个人金融信息的处理活动。

目前，《数据出境安全评估办法》已经落地，相关实践问题有待在执法中进一步确定。

- 符合国家法律法规及行业主管部门有关规定；
- 获得个人金融信息主体明示同意；
- 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；
- 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。
- 值得注意的是，就上述的“信息出境安全评估”义务，结合《数据出境安全评估办法》，可能存在以下几种触发情形：(i) 数据处理者向境外提供重要数据，(ii) 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；(iii) 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的数据处理者向境外提供个人信息，或 (iv) 国家网信部门规定的其他需要申报数据出境安全评估的情形。就上述的与境外机构签订的数据传输协议，《个保法》《数据出境安全评估办法》里也提出了同样要求，但网信部门当前尚未公布该协议的标准范本。

除上述要求外，如果境外司法或执法机构为跨境调查取证，而请求调取存储在中国境内的个人金融信息的，金融业机构还必须确保在获得境内相关主管机关的批准后方可响应该等请求、对境外提供个人金融信息。需要特别注意的是，数据出境安全评估结果的有效期为二年，有效期届满或在一些情形下，数据处理者需要重新申报评估。目前，《数据出境安全评估办法》已经落地，相关实践问题有待在执法中进一步确定。

个人金融信息收集是当前金融类App监管执法的重点领域。

PART 005

金融类App运维中的个人金融信息收集

在金融产品数字化背景下，App成为当下金融业机构采集用户个人金融信息的主要工具，但同时也是个人信息处理违法违规的重灾区。根据我们的统计，在网信部门及工信部门自2019年以来的App治理通报中，已经有300余款金融类App被监管部门通报或下架处理，其中，隐私政策提示及收集使用规则公开问题，以及违规或超范围收集问题，各占到通报比例的30%以上。此外，第三方SDK披露问题也日趋成为通报重点，并已占到通报比例的25%。由此可见，个人金融信息收集是当前金融类App监管执法的重点领域。我们在此列出以下App收集端须遵循的合规义务要点以供参考：

- 严守最小必要原则，要求用户必须提供的个人信息，不得超过必要个人信息范围，同时避免收集超出业务实际需要、与业务无关的个人信息。金融业机构可参考《常见类型移动互联网应用程序必要个人信息范围规定》对于网络支付、网络借贷、手机银行、投资理财类App的要求，来确定自身的必要个人信息范围；
- 在通过弹窗、明显位置的URL链接等方式收集信息时，需要引导用户查阅隐私政策，并在获得其明示同意后，方可开展有关个人金融信息的收集活动；
- 在隐私政策等公示文本中，必须逐项列明信息收集和共享的内容、目的及范围，以及所嵌入的SDK等第三方共享对象；
- 当用户明确表示不同意收集某项非业务必要的个人信息后，避免继续频繁地征求用户同意、干扰用户正常使用；
- 使用人脸、指纹等个人生物识别信息作为用户登录的验证方式时，应通过弹窗、即时提示等方式征得用户的单独同意，并避免将生物识别作为唯一的验证方式。

在个保法及金融消保实施办法等监管要求下，金融业机构在进行营销宣传活动时还应确保遵守规义务。

PART 006

金融营销宣传及自动化推广

金融产品和服务的营销宣传在当下是金融业机构引流变现的重要渠道。在个保法及金融消保实施办法等监管要求下，金融业机构在进行营销宣传活动时还应确保遵守如下合规义务：

- 收集个人金融信息用于营销宣传、用户体验改进、市场调查等目的时，需要确保通过适当方式供用户自主选择是否同意将自身的个人金融信息用于以上目的，如果用户不同意，金融业机构也不得因此拒绝提供相关产品或服务；
- 向用户通过电话呼叫、信息群发、网络推送发送营销信息时，金融业机构应当同时提供拒绝继续接收或退订的选择，避免短时间内对相同用户的重复呼叫、短信和高频推送；
- 在根据用户兴趣爱好、消费习惯等开展个性化精准营销时，金融业机构应当同时提供不针对用户个人特征推送的选项，或是界面关闭按钮等便捷的拒绝方式；
- 通过书面合作协议约定及采取相应的技术安全措施等方式，防止互联网平台等外部合作机构利用痕迹数据对用户个人开展未经授权的金融营销活动。

PART 007

结语

数字化时代，金融业机构全面提高个人金融信息的保护能力不仅仅是更严监管态势下的必然要求，更是实现数字化金融转型的关键之处。金融业机构应当以网络数据安全及个人信息保护等法律为根基，以行业主管部门的相关规定为枝干，以国家标准为叶，落实个人金融信息的分类分级，并建立涵盖个人金融信息收集、传输、存储、使用、删除、销毁等各个环节的全生命周期的内控合规制度。在网络安全与数据保护方面，金融作为重点行业在相关制度配套方面走在了前列，既有的标准、规范已对金融数据合规提出了诸多要求，但金

金融业机构的金融数据合规应当乘上“三驾马车”，在对数据合规的全局性理解下，全面而具有针对性地从重难点问题入手，展开主动合规工作。

融业机构的金融数据合规应当乘上“三驾马车”，在对数据合规的全局性理解下，全面而具有针对性地从重难点问题入手，展开主动合规工作。本文以个人金融信息保护为基础议题，在搭建好金融数据的分类分级框架，梳理了对金融数据进行全生命周期保护与个人金融信息保护的合规要点后，至此暂告一段落，我们会持续关注重点行业领域的数据合规问题，以期为企业提供具有前瞻性和可操性的合规建议。

（罗仪涵亦对本文有所贡献）

李瑞
合伙人
公司业务部
北京办公室
+86 10 5957 2143
lirui@zhonglun.com

贾申
顾问
合规与政府监管部
北京办公室
+86 10 5957 2263
jiashen@zhonglun.com

钟俊鹏
非权益合伙人
公司业务部
北京办公室
+86 10 5957 2122
zhongjunpeng@zhonglun.com

App“如影随形”，经营者如何把控个人信息保护合规要点?

刘新宇 卢佳宏

随着App的发展，各类App收集的个人信息规模逐渐增大，
相应的个人信息安全隐患也逐渐显现。

根据国家计算机网络应急技术处理协调中心与中国网络空间安全协会于2021年12月发布的《App违法违规收集使用个人信息监测分析报告》（以下简称“**《报告》**”），目前我国主流安卓应用商店在架App去重后总数为112万款。应用安装商城的信息展示界面显示多款头部App安装次数超过100亿次，可见，移动应用App已经成为人们日常生活中获取移动互联网服务的重要载体之一。

随着App的发展，各类App收集的个人信息规模逐渐增大，相应的个人信息安全隐患也逐渐显现。网信办、工信部等各类监管机构关于违法违规收集个人信息App的通报接踵而至，App运营者不仅面临被相关部门约谈、其所运营的App被下架等监管措施，还可能需要处理潜在负面舆情所带来的麻烦。故App运营者有必要提高对App个人信息保护问题的重视程度。结合《中华人民共和国个人信息保护法》（以下简称“**《个人信息保护法》**”）《App违法违规收集使用个人信息行为认定方法》（以下简称“**《认定方法》**”）等相关法律法规规定，及监管部门在开展App个人信息保护合规工作的过程中发现的主要问题，笔者建议App运营者着重关注以下合规要点，以保证App合法合规。

PART 001

告知个人信息主体处理行为并取得同意

《个人信息保护法》第十七条规定个人信息处理者在处理个人信息前，应当以显著方式、清晰易懂的语言真实、准确、完整地向个人信息主体告知个人信息处理者的名称或者姓名和联系方式；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；个人信息主体行使本法规定权利的方式和程序等内容。就App而言，告知个人信息主体的义务通常是通过个人信息保护政策落实。实践中，仍有个别企业并未制定个人信息保护政策。根据《报告》统计数据，2021年尚有6.7%的App没有隐私政策，结合我国主流安卓应用商店在架App的总量，这一数字仍相当可观，此类App运营者应当及时针对该问

实践中个人信息保护政策设置不规范的问题也是监管部门关注的重点。

题进行整改。

同时，即使已经制定了个人信息保护政策，也不意味着所有问题就都迎刃而解，实践中个人信息保护政策设置不规范的问题也是监管部门关注的重点。例如，《个人信息保护法》第十七条明确“个人信息处理者通过制定个人信息处理规则的方式告知第一款规定事项的，处理规则应当公开，并且便于查阅和保存。”故App运营者不仅应当制定个人信息保护政策，而且还需要将其公开以便查阅，尤其不能设置查阅的障碍，否则可能违反上述规定。就“便于查阅和保存”的具体标准，App运营者可以参考《认定方法》的相关规定。根据《认定方法》，为避免个人信息保护政策难以访问或难以阅读，App运营者至少应当做到两点：第一，个人信息主体进入App主界面后，访问到个人信息保护政策的操作不能多于四次点击；第二，个人信息保护政策的文字不应当过小过密、颜色过淡、模糊不清，或存在未提供简体中文版个人信息保护政策等情况。

除前述形式上的问题外，在内容上，个人信息保护政策亦应当满足《个人信息保护法》第十七条“以显著方式、清晰易懂的语言真实、准确、完整地向个人信息主体告知”的要求。例如，实践中有不少App运营者将其收集的个人信息种类与具体的使用方式及目的分拆进行列举，并未建立起对应的关系。该方式看似同时说明了“个人信息的处理目的、处理方式，处理的个人信息种类”，但是个人信息主体通过阅读这样的个人信息保护政策，很有可能仍然无法知悉每项个人信息的具体用途。此类个人信息保护政策就存在违反前述《个人信息保护法》规定的风险。

在完成告知个人信息主体的义务后，另一项义务就是取得处理个人信息的合法性基础，《个人信息保护法》第十三条规定了包括“取得个人的同意”在内的七项处理个人信息的合法性基础。在实践中，直接获取个人信息主体的同意是各类App最常选择的合法性基础，即通过在个人信息主体首次使用App时主动弹窗提示个人信息主体阅读个人信息保护政策并要求其勾选同意。但需要注意的是，在征求个人信息主体同意时应当避免采用默认勾选同意、登录即代表同意等默示方

App在处理个人信息时不可以超出必要范围，此处的范围不仅是收集个人信息的类型，还包括收集的频率、处理的方式。

式获取个人信息主体同意，而应当确保个人信息主体以主动的行为完成“同意”的意思表示。然而，在部分情况下，App运营者亦可能存在较难获取个人信息主体同意的情形，此时，App运营者可以考虑适用《个人信息保护法》第十三条规定的“为订立、履行个人作为一方当事人的合同所必需”等其他合法性基础作为替代。

PART 002

基于最小必要性处理个人信息

《个人信息保护法》第六条规定“处理个人信息应当具有明确、合理的目的，并应当与处理目的直接相关，采取对个人权益影响最小的方式。收集个人信息，应当限于实现处理目的的最小范围，不得过度收集个人信息。”故App在处理个人信息时不可以超出必要范围，须注意，此处的范围不仅是收集个人信息的类型，还包括收集的频率、处理的方式。详细而言，最小必要性主要体现在两个方面：

其一是种类上的必要性，例如，天气预报软件收集用户的地理位置信息对于实现其预报天气的目的具有一定的必要性，因为只有获取该项信息才能更准确并针对性地提供当地的天气情况预测。但如果天气预报软件（只有单一的天气预报功能）收集用户的通讯录信息就明显不符合《个人信息保护法》的最小必要性原则，因为即使不收集通讯录信息也不影响App为用户提供天气信息的预报服务，App运营者无法说明收集通讯录信息对于实现这一目的有何作用。

第二是程度上的必要性，仍以前述天气预报软件为例，该软件收集位置信息固然具有合理性，但是如果不对收集频率加以控制，仍可能存在收集非必要信息的风险。例如无论用户是否使用该款App，App都在后台采集用户的地理位置信息并不断进行更新，这就明显属于违反最小必要性原则的处理行为。

App运营者须保证处理行为具有“特定的目的和充分的必要性”，且应当采取较之一般个人信息更为严格的保护措施。

PART 003

合规处理敏感个人信息

《个人信息保护法》第二十八条规定“敏感个人信息是一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。”例如，个人信息主体的人脸、指纹等信息都可能被认为是《个人信息保护法》下的敏感个人信息。在处理该部分个人信息时，App运营者须保证处理行为具有“特定的目的和充分的必要性”，且应当采取较之一般个人信息更为严格的保护措施（例如进行去标识化处理、加密存储等）。

同时需要注意，依照《个人信息保护法》的规定，App运营者在处理敏感个人信息时，需要取得个人信息主体的单独同意。实践中，部分App运营者可能会要求个人信息主体通过点击弹窗或者勾选单独的敏感个人信息处理规则等方式作出单独同意。鉴于“单独同意”亦属于“同意”的一种形式，如个别场景下取得单独同意存在困难或对用户体验的影响较大，App运营者亦可以考虑以《个人信息保护法》第十三条规定的其他合法性基础替代“取得单独同意”。

PART 004

设置便捷的受理与处理机制

《个人信息保护法》第五十条规定“个人信息处理者应当建立便捷的个人行使权利的受理和处理机制。拒绝个人行使权利的请求的，应当说明理由。”目前大多数App已经设置了此类机制，亦会公示注销账号的途径。但是仅有纸面上的制度与流程并不能保证App运营者完全符合法律法规的要求，制度与流程本身是否“便捷”，在实践中是否得到了落实与执行亦是值得关注的合规问题。在司法实践中，部分法院亦认为，如果个人信息处理者面对个别用户的权利请求未能及时予以响应，那么即使其已经制订了相对完整的受理与处理规则，也依

App运营者应当按照“双清单”的要求，向个人信息主体展示相关情况，以便个人信息主体了解App运营者对其个人信息的处理内容，及时主张权利。

然无法被认定为履行了《个人信息保护法》第五十条的义务。例如，App运营者以验证个人信息主体身份真实性作为提出权利请求的前提，但是并未告知具体的验证方式或渠道；或者公示了接受请求的电子邮箱，但是未及时查看用户的请求内容等，均可能被法院或监管部门认定为未履行法定义务。

在个人信息主体享有的各项权利中，对个人信息处理行为的知情权是一项相当重要的权利，一定程度上亦是行使其他权利的基础。监管部门对此也颇为重视，2022年7月，上海市通信管理局决定，将重点检查“在国内单一应用市场内下载量/安装量达500万次以上的APP应用（含快应用和小程序等新应用形态）”，其中检查的要点之一就是App是否已经建立“双清单”。“双清单”源于2021年11月1日工信部发布的《关于开展信息通信服务感知提升行动的通知》，该通知要求相关企业建立“已收集个人信息清单”和“第三方共享个人信息清单”，简洁、清晰列出App（包括内嵌第三方软件工具开发包SDK）已经收集到/与第三方共享的用户个人信息基本情况。基于此，笔者理解，App运营者除完成《个人信息保护法》规定的告知义务外，还应当按照“双清单”的要求，向个人信息主体展示相关情况，以便个人信息主体了解App运营者对其个人信息的处理内容，及时主张权利。

PART 005

关注SDK数据合规情况

SDK通常是指Software Development Kit，即软件开发工具包。简单来看，它是辅助开发某一类应用软件的相关文档、范例和工具的集合。对App来说，为了提高开发效率，可以将某项功能交给第三方来开发，第三方服务提供商将服务封装为工具包（即SDK）供开发者使用。《认定方法》明确“未逐一列出App（包括委托的第三方或嵌入的第三方代码、插件）收集使用个人信息的目的、方式、范围等”可被认定为“未明示收集使用个人信息的目的、方式和范围”，属于违规的个人信息处理行为，须承担相应的法律责

应全面梳理App已经接入的全部SDK，将接入的SDK收集使用个人信息的目的、方式、范围写入个人信息保护政策。

任。《移动互联网应用程序个人信息保护管理暂行规定（征求意见稿）》第八条明确“使用第三方服务的，应当制定管理规则，明示App第三方服务提供者的名称、功能、个人信息处理规则等内容；应与第三方服务提供者签订个人信息处理协议，明确双方相关权利义务，并对第三方服务提供者的个人信息处理活动和信息安全风险进行管理监督；App开发运营者未尽到监督义务的，应当依法与第三方服务提供者承担连带责任。”虽然该规定暂时还未正式生效，但是如果App中含有侵害个人信息主体权益的SDK，亦可能使App运营者被由此引发的负面舆情所影响，进而损害商誉。在监管实践中，工信部亦于近期对违规的SDK进行了多次通报，可见该问题亦属于监管部门的关注重点。

故SDK就像一把“双刃剑”，为了保证App运营者的自身权益，笔者建议App运营者全面梳理App已经接入的全部SDK，将接入的SDK收集使用个人信息的目的、方式、范围写入个人信息保护政策，以进行明示，并获得个人信息主体的同意，对于媒体曝光和监管通报的存在问题的SDK，如己方App接入了该等SDK，根据问题的严重程度，及时采取要求该等SDK限期整改、停止使用等措施。

PART 006

儿童个人信息保护

App运营者对儿童个人信息的保护义务亦属重中之重。根据《儿童个人信息网络保护规定》第八条的规定“网络运营者应当设置专门的儿童个人信息保护规则和用户协议，并指定专人负责儿童个人信息保护。”笔者建议App运营者如处理儿童个人信息，则应当为儿童设置单独的个人信息保护规则和用户协议，同时，因《个人信息保护法》第二十八条规定不满十四周岁未成年人的个人信息属于敏感个人信息，因此个人信息处理者在处理该等个人信息前需要取得个人信息主体的监护人对此的单独同意，并且应采取更为严格的保护措施，以保护儿童的个人信息，保障儿童人身安全，保护儿童的合法权益。

App运营者对儿童个人信息的保护义务亦属重中之重。

在App运营过程中，App运营者，尤其是UGC（User Generated Content，用户生成内容）型App运营者通常会对用户发布的内容添加标签，以推荐给可能对某类内容感兴趣的其他用户，虽然此种情况在App运营中非常常见，但是需要注意的是，如果该内容涉及到儿童，则应当提前考虑相关风险，特别是此等方式是否会对儿童人身安全、生活安宁等造成潜在风险，甚至是导致个人信息被不法分子利用后，对儿童实施犯罪行为。

除避免App中的儿童个人信息被“外部”的不法分子获取外，App运营者“内部”的工作人员亦应当成为规范的对象。《儿童个人信息网络保护规定》第十五条规定“网络运营者对其工作人员应当以最小授权为原则，严格设定信息访问权限，控制儿童个人信息知悉范围。工作人员访问儿童个人信息的，应当经过儿童个人信息保护负责人或者其授权的管理人员审批，记录访问情况，并采取技术措施，避免违法复制、下载儿童个人信息。”故App运营者不仅需要对儿童个人信息设置访问控制制度，亦需要设置“儿童个人信息保护负责人”，对相关处理行为进行审批、记录，以避免非必要的访问，进一步降低可能对儿童造成的风险。

PART 007

结语

以上是笔者对App部分合规要点的简单梳理，随着我国个人信息保护相关法规日益完善，监管部门对App的监管亦日益加强，笔者建议App运营者应当时刻关注相关法律法规的发展与变化，提升App个人信息保护合规水平，在保障用户权益的前提下，让App更好地服务于用户。

刘新宇
合伙人
私募基金与资管部
上海办公室
+86 21 6061 3700
jeffreyliu@zhonglun.com

CHAPTER 03

数据合规前沿探讨

PART ONE

数据跨境流通研究

数据出境安全评估的策略与方法

周洋 徐颖蕾

本文就企业开展数据出境安全评估工作可能遇到的一些关键问题进行分析解答，为企业顺利通过出境安全评估提供参考。

自2022年9月1日起，《数据出境安全评估办法》（以下简称“**《评估办法》**”）正式施行。在《评估办法》生效前一日，国家互联网信息办公室（以下简称“**国家网信办**”）发布了《数据出境安全评估申报指南（第一版）》（以下简称“**《申报指南》**”），就数据出境安全评估（以下简称“**出境安全评估**”）的申报方式、流程和申报材料提供了详细的操作指引。此后，江苏、北京等地网信部门陆续出台地方申报指南或提供咨询电话，积极落实数据出境安全评估工作。

企业的数据出境活动在什么情况下会触发出境安全评估？在预判可能或必然触发出境安全评估后，企业应如何开展准备工作才能顺利通过评估？本文将基于相关法律法规、《申报指南》的相关要求，结合实务经验，就企业开展数据出境安全评估工作可能遇到的一些关键问题进行分析解答，为企业顺利通过出境安全评估提供参考。[1]

1.本文不涉及可能触发网络安全审查的情形，后者应单独分析研判。

PART 001

如何理解和判定“数据出境”？

根据《评估办法》，只有在数据出境的情况下才谈得上出境安全评估。因此，首先需要判定是否存在数据出境情形。判定是否构成《评估办法》项下的“数据出境”，需要从“数据出境主体”、“数据出境行为”和“数据出境标的”三个方面进行分析。

1.数据出境主体是“数据处理者”而非“数据主体”或“受委托处理者”

《评估办法》第二条规定：“数据处理者向境外提供在中华人民共和国境内运营中收集和产生的重要数据和个人信息的安全评估，适用本办法。法律、行政法规另有规定的，依照其规定。”从语义上看，《评估办法》项下的数据出境主体仅限于数据处理者。尽管《评估办法》没有给出数据处理者的定义，但是参考《个人信息保护法》中关于“个人信息处理者”以及《网络数据安全管理条例（征求意见稿）》中关于“数据处理者”的定义，“数据处理者”应指在数据处理活动中自主决定处理目的和处理方式的个

在个人信息主体向境外提供个人信息的场景下，自主决定处理目的和处理方式的应是境外数据接收方而非境内个人信息主体。

人和组织。

在个人信息主体向境外提供个人信息的场景下，自主决定处理目的和处理方式的应是境外数据接收方而非境内个人信息主体。因此，个人信息主体向境外提供个人信息应不属于《评估办法》项下的数据出境。例如，境内消费者登录境外网站预定酒店并向境外网站提供个人信息，此种情况下，尽管境外数据处理者跨境收集了境内消费者的个人信息，但由于该等数据是个人信息主体提供而非数据处理者提供，因此，此种数据出境活动不适用《评估办法》。尽管如此，境外数据处理者因跨境收集中国境内个人信息，仍需遵守《个人信息保护法》的规定。

此外，数据出境主体排除了不能自主决定处理目的和处理方式的受委托处理者。例如，某境内企业使用境外供应商提供的客户关系管理（**CRM**）系统处理客户数据，该CRM系统部署在境外服务器上。在此情况下，决定客户数据处理目的和方式的是该企业，而CRM系统供应商只是受企业委托进行跨境数据处理活动。如该等跨境数据处理活动达到出境安全评估申报标准，则应由该企业而不是其CRM系统供应商向网信部门申报。

2.数据出境行为包括向境外提供或从境外访问境内数据，企业应按最小必要原则精细化管理出境数据

《申报指南》第一条列举了数据出境行为，包括：(a)数据处理者将在境内运营中收集和产生的数据传输、存储至境外（“**向境外提供**”）；(b)数据处理者收集和产生的数据存储在境内，境外的机构、组织或者个人可以查询、调取、下载、导出（“**从境外访问**”）；(c)国家网信办规定的其他数据出境行为。

前两种出境情形下，如何判断数据出境规模直接涉及是否触发出境安全评估的问题。例如，某外资企业在中国境内有2万名员工，其中只有占员工总数不到十分之一的高管会被公司将其个人信息提供给境外母公司，其他员工只有在内部调查等特殊情况下才会涉及将其个人信息提供给境外母公司。此种情况下，数据出境规模应仅限于被提供给境外母公司的有关员工的个人信息，而不是可被提供给境外的全体员

企业应仅向境外母公司开放将实际发生从境外访问情形的部分员工数据，而不是开放全体员工数据从而降低数据出境规模。

工的个人信息。企业也应当按照最小必要原则，仅提供相关员工的个人信息以降低数据出境规模。

同样，对于从境外访问境内数据，在计算数据出境规模时，我们理解，应以境外实际查询、调取、下载、导出的数据量计算，而非以境外可访问的数据量计算。原因在于，一方面，如将可从境外访问的数据量纳入数据出境统计口径，则该等数据出境可能不符合《个人信息保护法》项下的最小必要原则。另一方面，数据处理者开展数据出境活动，采用向境外提供还是从境外访问只是方式不同，统计口径理应一致。尽管如此，《申报指南》使用了“境外的机构、组织或者个人可以查询、调取、下载、导出”的表述。为避免疑义，企业应更精细化管理出境数据，仅在最小必要范围内授予境外访问权限。上述示例中，从管理数据出境规模角度，企业应仅向境外母公司开放将实际发生从境外访问情形的部分员工数据，而不是开放全体员工数据从而降低数据出境规模。

3.重要数据和个人信息

根据《评估办法》第二条的规定，只有出境数据为重要数据或个人信息才适用出境安全评估。这意味着企业的业务信息、统计数据（“**一般数据**”）的出境，如不含有重

CII和重要数据的认定对企业来说具有重要意义，企业可参考《国家网络安全检查操作指南》所规定的CII识别与认定“三步法”。

要数据或个人信息，通常将不属于《评估办法》项下的“数据出境”。需要注意的是，尽管一般数据不受制于《评估办法》，但一般数据的处理活动仍受制于《网络安全法》和《数据安全法》。因此，企业对于一般数据的出境活动，可参考个人信息和重要数据出境的合规要求开展数据出境安全自评估，为满足一般性数据合规义务打下基础。

PART 002

企业如何判断是否构成关键信息基础设施（“CII”）运营者或出境数据是否构成“重要数据”？

根据《评估办法》，如出境数据包含重要数据，或CII运营者出境个人信息，则不论出境数据量多少，均触发出境安全评估。因此，CII和重要数据的认定对企业来说具有重要意义。但是，由于CII和重要数据的认定规则和清单/目录尚未发布，因此关于这两项的认定对企业而言存在较大的不确定性。在相关规则出台前，企业如何判断自己是否运营CII、是否处理重要数据？若无法判断，企业是否应申报出境安全评估？

1.关键信息基础设施的认定

根据《关键信息基础设施安全保护条例》，CII的认定规则及清单由各重要行业和领域的主管部门、监管部门制定。目前，尚未有部门公布该等认定规则或清单。2016年6月中央网络安全和信息化领导小组办公室网络安全协调局发布的《国家网络安全检查操作指南》中提供了CII识别与认定的“三步法”，即(a)确定关键业务，(b)确定支撑关键业务的信息系统或工业控制系统，(c)根据关键业务对信息系统或工业控制系统的依赖程度，以及信息系统发生网络安全事件后可能造成的损失认定关键信息基础设施。

因此，在公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域的企业应重点关注CII的认定问题。对处于该等领域的企业，可参考上述《国家网络安全检查操作指南》所规定的CII识别与认定“三步法”，划定本企业所在行业的关键业务及相关的信息系统或工业控制系统，并进一步评估该等系统遭到破坏、丧失功能或者数据泄露可能带来的后果。值得注意的是，在《申

对重要数据的认定需要结合企业所在行业、数据内容、数据量、泄露或篡改、损害的后果等因素，进行个案分析。

报指南》中，地方网信部门没有提到要企业自行判断自身是否构成CII运营者，也没有提到网信部门是否会判断企业是否构成CII运营者。因此，在未被识别为CII运营者的情况下，企业需要斟酌是否主动申报数据出境安全评估。

2.重要数据的认定

《评估办法》将“重要数据”定义为“一旦遭到篡改、破坏、泄露或者非法获取、非法利用等，可能危害国家安全、经济运行、社会稳定、公共健康和安全等的数据。”根据《数据安全法》第二十一条的规定，各地区、各部门确定本地区、本部门以及相关行业、领域的重要数据具体目录，对列入目录的数据进行重点保护。目前，除2021年8月16日国家网信办、发展和改革委员会、工业和信息化部、公安部、交通运输部五部门联合发布的《汽车数据安全管理若干规定（试行）》中对汽车数据中的重要数据[2]进行了明确列举外，尚未有部门发布重要数据目录。因此，对于汽车行业外的其他企业而言，在缺乏重要数据目录的情况下，是否涉及重要数据，往往需要企业根据现有的重要数据识别规则自行判定。

2022年4月，全国信息安全标准化技术委员会发布《信息安全技术 重要数据识别规则（征求意见稿）》（以下简称“**《重要数据识别规则》**”），从国家安全体系涵盖的政治安全、国土安全、军事安全等问题领域，描述了重要数据的识别因素，如“直接影响国家主权，政权安全、政治制度、意识形态安全”、“直接影响领土安全和国家统一，或反映国家自然资源基础情况”、“可被其他国家或组织利用发起对我国的军事打击，或反映我国战略储备、应急动员、作战等能力”等。然而，由于《重要数据识别规则》未列举重要数据的类型，因此对重要数据的认定需要结合企业所在行业、数据内容、数据量、泄露或篡改、损害的后果等因素，进

2.《汽车数据安全管理若干规定（试行）》第三条规定：
重要数据是指一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能危害国家安全、公共利益或者个人、组织合法权益的数据，包括：
（一）军事管理区、国防科工单位以及县级以上党政机关等重要敏感区域的地理信息、人员流量、车辆流量等数据；
（二）车辆流量、物流等反映经济运行情况的数据；
（三）汽车充电网的运行数据；
（四）包含人脸信息、车牌信息等的车外视频、图像数据；
（五）涉及个人信息主体超过10万人的个人信息；
（六）国家网信部门和国务院发展改革、工业和信息化、公安、交通运输等有关部门确定的其他可能危害国家安全、公共利益或者个人、组织合法权益的数据。

企业对重要数据的斟酌与对CII的斟酌应采用不同策略，遵循实质重于形式的原则，自主判断并主动申报。

行个案分析。需要注意的是，虽然单纯的个人信息一般不属于重要数据，但如个人信息数量达到一定规模、一定精度，例如个人信息的内容足以反映一定范围内的人口与健康情况，那么该等个人信息就可能构成重要数据。

我们注意到，已经有地方网信部门在根据《申报指南》发布的本地方申报数据出境安全评估的工作指引中对“重要数据”的范围进行了规定。例如，江苏省网信办于2022年9月1日发布《江苏省数据出境安全评估申报工作指引（第一版）》中规定，数据处理者需根据相关行业标准界定出境数据是否为重要数据，如无行业标准，可参考以下标准。[3]

由此可见，虽然重要数据目录没有出台，但在出境安全评估语境下，网信部门将会对重要数据加以判断或要求企业对是否处理重要数据加以判断。因此，企业对重要数据的斟酌与对CII的斟酌应采用不同策略，遵循实质重于形式的原则，自主判断并主动申报，而不应以有关重要数据目录未出台为由不予判断或不予申报出境安全评估。

3.(a)未公开的政务数据、工作秘密、情报数据和执法司法数据；(b)重点行业和领域安全生产、运行的数据，关键系统组件、设备供应链数据；(c)达到国家有关部门规定规模或者精度的基因、地理、矿产、气象等国家基础数据；(e)影响关键信息基础设施安全稳定运行的数据，国防设施、军事管理区、国防科研生产单位等重要敏感区域的地理位置、安保情况等数据；(f)出口管制物项涉及的核心技术、设计方案、生产工艺等相关数据，密码、生物、电子信息、人工智能等领域对国家安全、经济竞争力有直接影响的科学技术成果数据；(g)国家法律、行政法规、部门规章明确规定需要保护或者限制处理的国家经济运行数据、重要行业和领域业务数据、统计数据等；(h)其他一旦遭到篡改、破坏、泄露或者非法获取、非法利用等，可能危害国家安全、经济运行、社会稳定、公共健康和安全等的数据。上述标准与《网络数据安全管理条例（征求意见稿）》中的标准大致相同。

PART 003

如何满足数据出境的合法性要求？

“合法性”是数据出境安全评估的评估重点之一。与“正当性”、“必要性”缺乏明确“是”与“否”的标准不同，“合法性”的判断往往有明确的法律法规依据。实务中，数据出境的合法性通常需考虑：

1.数据出境标的是否合法？

企业首先应当判断出境数据是否涉及不得出境的数据或需经主管部门单独审批或备案的数据。例如，根据《人类遗传资源管理条例》，将人类遗传资源信息向外国组织、个人及其设立或者实际控制的机构提

除了出境标的的合法性，企业还应关注数据出境方式的合法性。

供或者开放使用，应当向国务院科学技术行政部门备案并提交信息备份；可能影响我国公众健康、国家安全和社会公共利益的，应当通过国务院科学技术行政部门组织的安全审查。

2.数据出境方式是否合法？

除了出境标的的合法性，企业还应关注数据出境方式的合法性。例如，2021年11月14日国家网信办发布的《网络数据安全管理条例（征求意见稿）》第41条规定，境内用户访问境内网络的，其流量不得被路由至境外。实践中，对于一些大型跨国公司或具有海外业务的大型中资企业来说，由于全球业务布局而需要采用全球IT架构，在中国香港、新加坡、爱尔兰、美国等全球多地部署数据中心或灾备中心。这种IT架构可能导致境内用户访问境内网络的流量被路由到境外再返回境内。将境内用户流量路由至境外可能带来额外的数据泄露、流量劫持等安全风险，如果缺乏必要性，则可能不满足数据出境的合法性要求。比如，境内企业在境外建立灾备中心是否具有必要性需要具体情况具体分析，企业

至少应能够说明此种IT架构和数据流动的业务合理性、技术合理性。

又例如，企业通过VPN跨境专线进行数据出境，则根据《工业和信息化部关于清理规范互联网网络接入服务市场的通知》《国际通信出入口局管理办法》等相关规定，企业须向持有相关电信资质的服务商租用跨境专线，且该专线仅供企业内部办公专用。比如，企业通过VPN访问部署在境外服务器上的CRM系统或其他办公系统，将境内客户或员工个人信息存储到境外服务器，企业应使用合法租赁的VPN实现连接。

采用何种同意机制既需考虑同意的有效性，也需顾及具体业务场景中的可操作性和便利性。

PART 004

如何有效获得个人信息主体的单独同意？

对于个人信息出境，还需注意是否有效取得个人的单独同意，以及如何证明已取得个人单独同意的问题。实践中既存在通过APP、小程序、网页等线上形式收集个人信息的场景，也存在通过签署合同、填写表格等线下形式收集个人信息的场景。关于单独同意的实现方式，对于线上收集场景，往往可以通过线上交互式界面的设计，由个人信息主体通过勾选、点击“同意”等方式获得单独同意；但对于线下收集场景，则可能需要通过签署书面声明、签字确认的方式获得个人信息主体的单独同意。由于同意的前提是告知数据处理规则，因此告知内容的文案、告知界面的展示、单独同意的设置、告知的时机和频率等问题也需在设计同意机制时予以考虑。总而言之，采用何种同意机制既需考虑同意的有效性，也需顾及具体业务场景中的可操作性和便利性，往往是综合考量、各方因素权衡下的选择。

此外，对于员工个人信息出境的场景，《个人信息保护法》提供了“按照依法制定的劳动规章制度和依法签订的集体合同实施人力资源管理所必需”这一项取得个人同意的例外。因此，企业可通过将员工个人信息处理活动纳入劳动规章制度的方式替代员工的单独同意。然而，根据《劳动合同法》的相关规定，合法有效的规章制度往往需要满足征求意见、平等协商、公示等法定流程。因此，在适用“劳动规章制度”这一取得个人同意的例外收集员工个人信息时，需兼顾《个人信息保护法》及《劳动合同法》的相关要求。

关于同意的证明材料，企业可参照2020年1月全国信息安全标准化技术委员会发布的《信息安全技术 个人信息告知同意指南（征求意见稿）》，提供其直接收集的或受其委托进行数据处理的第三方收集的材料。可以选择的证据内容包括：(1)企业告知数据处理规则的记录和获取同意的记录，记录的方式包括企业内部的电子或纸质文档或邮件等直接证明材料；或(2)与个人信息处理活动存在逻辑关系的记录，比如用户从登录、注册、使用、退出公司官网、

企业不仅要就数据出境本身的合规情况进行分析判断，还需判断是否符合网络安全、数据安全、电信监管等相关规范体系下的其他合规要求。

APP或内网的先后顺序及相关日志与数据库标记等间接证明材料。

PART 005

如何理解“遵守中国法律、行政法规、部门规章情况”并达到合规要求？

1.“遵守中国法律、行政法规、部门规章情况”是评估重点之一

“遵守中国法律、行政法规、部门规章情况”这一评估事项的表述较为概括，但正是因为概括性的表述，使得其所涵盖的范围可以非常宽泛，实践中对于该事项范围的划定将直接影响企业合规义务的范围。例如，“遵守中国法律、行政法规、部门规章情况”可能不仅局限于与数据出境相关的规范，还可解释为与网络安全、数据安全、电信监管等相关的各项法律法规、部门规章。从而企业不仅要就数据出境本身的合规情况进行分析判断，还需判断是否符合网络安全、数据安全、电信监管等相关规范体系下的其他合规要求。

根据《申报指南》中就《数据出境安全评估申报表》（以下简称“**《申报表》**”）第14项“数据处理者遵守中国法律、行政法规、部门规章情况”的说明，企业在填写这一项时需简述近2年在业务经营活动中受到行政处罚和有关主管监管部门调查及整改情况，重点说明数据和网络安全方面相关情况。可见，“遵守中国法律、行政法规、部门规章情况”重点在于数据和网络安全方面的法律法规及规章的遵守情况。《申报表》中对该事项的填写要求较低，仅需要简述监管部门对企业的执法情况。

2.“遵守中国法律、行政法规、部门规章情况”不限于企业受到行政处罚和被执法或被调查的情况

在《申报指南》提供的《数据出境风险自评估报告》（以下简称“**《自评估报告》**”）模板中，企业需详细说明：(a)数据安全管理能力，包括管理组织体系和制度建设情况，全流程管理、分类分级、应急处置、风险评估、个人信息权益保护等制度及落实情况；(b)数据安全技术能力，包括数据收集、存储、使用、加工、传输、提供、公开、删除等全流程所采取的安全技术措施等；(c)数据安全保障措施有效性证明，例如开展的数

“遵守中国法律、行政法规、部门规章情况”还应包括遵守中国电信法律法规、规章情况。

据安全风险评估、数据安全能力认证、数据安全检查测评、数据安全合规审计、网络安全等级保护测评等情况；(d)遵守数据和网络安全相关法律法规的情况。

企业是否依照《网络安全法》履行相关网络安全保护义务，如开展网络安全等级保护、设置网络安全负责人、制定网络安全内部管理制度和操作规程、制定网络安全事件应急预案等；是否依照《数据安全法》履行相关数据安全保护义务，如建立健全全流程数据安全管理制度、开展数据安全教育培训、采取相应的技术措施和其他必要措施保障数据安全等情况实际上仍需要在《自评估报告》中进行阐明。如果企业做过网络安全等级保护或个人信息保护合规审计或ISO认证工作，将非常有助于说明其数据安全管理和保障能力。

3.“遵守中国法律、行政法规、部门规章情况”还应包括遵守中国电信法律法规、规章情况

企业还应注意电信监管的合规性问题。例如，很多企业的外部个人信息来源于其官网、APP、公众号或小程序，而这些平台有的可能没有做过ICP备案，有的没有取得ICP证或其他相应增值电信业务许可证。那么，通过该等非法网站或平台获取的个人信息或数据则存在先天的合法性问题。或者有的企业虽然做过ICP备案或取得了有关增值电信业务许可证，但没有把数据存储在申请该等备案或许可而报告给电信监管部门的本地服务器上。此种情况下的数据出境或出境数据也存在先天的合法性问题。对于这些问题，需要花费较长时间和较大投入方能解决，企业应尽早发现、尽早整改，以达到申报要求。

PART 006

如何提供境外数据安全保护政策法规资料？

数据出境安全评估的评估重点还包括“境外接收方所在国家或者地区的数据安全保护政策法规和网络安全环境对出境数据安全的影响”。《申报指南》提供的《自评估报告》模板中，也要求企业详细说明境外接收方所在国家或地区数据安全保护政策法规和网络安全环境情况。为达到该项要

数据本地化存储与数据出境密切相关，一旦企业未能通过出境安全评估，数据境外存储的实践将面临挑战。

求，实践中需要引入境外律师参与，即由境外接收方所在地的当地律师出具法律意见。如出境数据存储的境外服务器与境外接收方位于不同法域，则可能还需境外服务器所在地律师出具意见。为增强客观性，该等法律意见应为境外外部律师而非公司法务出具的意见。

PART 007

是否需要对数据进行本地存储?

《评估办法》未就数据出境前是否需进行本地存储进行规定。根据《网络安全法》第37条的规定，CII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。同时，根据《个人信息保护法》第40条和《评估办法》第4条，处理100万人以上个人信息的数据处理者应当将在境内收集和产生的个人信息存储在境内。对于其他达到出境安全评估门槛的数据处理者，例如出境重要数据的数据处理者，以及自上年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的数据处理者，现有规则未明确设置数据本地存储的义务。

但实际上，数据本地化存储与数据出境密切相关。因为一旦企业未能通过出境安全评估，数据境外存储的实践将面临挑战。例如，企业使用服务器位于境外的业务系统并将相关数据存储于境外服务器中，如企业未能通过评估，又未能及时搭建或租赁境内服务器用于本地化存储，则企业可能面临业务中断的严重后果。因此，为了避免因无法通过出境安全评估影响企业的业务运转，企业可能需要在综合考虑出境合规成本、IT架构调整成本及业务调整成

数据出境安全评估工作是一个系统工程，应提前规划、尽早安排。

本的基础上，进行全面筹划。如企业通过经ICP备案或电信许可的线上平台收集个人信息，则意味着企业已经有了本地服务器，而在该平台上收集的数据应首先存储在本地。

PART 008

总结

通过以上对企业开展数据出境安全评估工作中几个关键问题的分析，可以看出，数据出境安全评估工作是一个系统工程，应提前规划、尽早安排。主要的时间和成本应该投入在梳理数据处理活动、梳理IT架构及整改方面。只有达到合规状态，企业才能够通过有关个人信息保护影响评估、自评估和出境安全评估。

周洋
合伙人
知识产权部
上海办公室
+86 21 6061 3658
zhouyang@zhonglun.com

数据跨境传输协议应明确哪些权利义务?

李瑞 贾申 徐晨

本文聚焦《个人信息出境标准合同规定（征求意见稿）》及其附件，对于其条款进行解析与提炼，对其规定的数据跨境传输双方的关键权利与义务进行梳理。

企业在清晰梳理自身涉及的数据跨境传输活动及出境数据类型后，下一步需评估选择适用的跨境传输合规机制。除了部分数据跨境传输不受管制、以及部分特殊数据类型的跨境传输需满足特殊监管要求外，大部分数据跨境传输场景需（视具体情境）适用以下三大监管机制之一：（1）通过数据出境安全评估（“**安全评估机制**”）；（2）通过个人信息跨境处理活动安全认证（“**安全认证机制**”）；（3）签署个人信息出境标准合同（“**标准合同机制**”）。不论适用哪一监管机制，境内数据处理者与境外数据接收方均需签订数据跨境传输的协议（或其他替代性法律文件），以充分约定数据安全保护责任与义务。**值得注意的是，不同监管机制下境内数据处理者和境外数据接收方之间需订立的数据跨境传输协议中所约定的责任与义务强度并不完全相同，完全套用统一标准也未必能实现最佳的商业效果。**

如何起草并签订能够有效防范潜在法律风险的数据跨境传输协议是企业在实务中经常遇到的难题。一个整体原则是，在标准合同机制下，由于双方仅通过履行合同的方式对数据跨境安全进行约束与保障，因此标准合同在合同架构与权责设定上对于数据跨境双方的合规要求都最为严格；而在另外两项机制下，由于还有安全认证或安全评估程序可保障数据出境安全，因而相关数据跨境商务合同的条款和条件的合规强度相对而言可以适当放松。

基于上述原则，本文聚焦国家网信办于2022年6月30日发布的《个人信息出境标准合同规定（征求意见稿）》及其附件（下统称“**标准合同征求意见稿**”），对于其条款进行解析与提炼，对其规定的数据跨境传输双方的关键权利与义务进行梳理。根据“举重以明轻”的原则，对于不采用标准合同机制的数据出境场景的当事方，也可参考这些梳理和提炼的内容，同时参考安全认证机制及安全评估机制项下对于数据跨境合同内容所提出的要求，合理安排相关商务合同的条款和条件。

为了便于企业依据自身数据跨境传输活动细节来映射协议起草谈判所需注意的要点，本文将数据跨境传输协议中应约定的各方责任与义务依据角色进行了区分，即（1）境内数据处理者的责任和义务及（2）境外数据接收方的责任和义务。具体

境内数据处理者的主要义务之一：严格执行告知同意义务，
明释第三方受益人权利，保护个人信息主体权利。

请参见下文的详细解析。

PART 001

境内数据处理者的责任和义务

1.主要义务一：严格执行告知同意义务，明释第三方受益人权利，保护个人信息主体权利

- 境内数据处理者应当告知个人信息主体境外接收方的名称、联系方式等信息，并依据法律法规的要求取得其有效同意。

标准合同征求意见稿中的主要相关条款：第二条第（二）款

- 境内数据处理者应当向个人信息主体告知，其已与境外接收方通过本合同约定个人信息主体为第三方受益人。依据标准合同征求意见稿所载，如果个人信息主体未在三十天内明确拒绝，则可以依合同享有第三方受益人的权利。

标准合同征求意见稿中的主要相关条款：第二条第（三）款

- 境内数据处理者与境外数据接收方应当协同配合，响应个人信息主体权利请求，在遇到相关请求时应互相通知并及时合作，并在合理时限内进行处理。

标准合同征求意见稿中的主要相关条款：第五条

- 应个人信息主体要求，双方应当向个人信息主体提供数据跨境传输协议副本。为保护商业秘密或其他机密信息，可在所必需的范围内对于受保护的商业秘密、知识产权等内容进行脱敏处理，但应确保个人信息主体能够理解相关内容。

标准合同征求意见稿中的主要相关条款：第二条第（八）款

境内数据处理者应采取技术与合规管理措施，开展出境后监督管理；遵守法规要求处理数据，切实履行法定义务。

2.主要义务二：采取技术与合规管理措施，开展出境后监督管理

- 境内数据处理者应当对境外数据接收方的数据处理活动进行监督，比如查阅数据文件和文档，开展数据处理活动的审计等，并根据法律法规要求向监管机构提供相关信息，包括审计结果。

标准合同征求意见稿中的主要相关条款：第二条第（四）款、第十款

- 为了帮助境外数据接收方更好地履行数据安全保护义务，境内数据处理者应当帮助境外数据接收方了解相关法律法规及技术标准要求，并提供相关文件副本。

标准合同征求意见稿中的主要相关条款：第二条第（五）款

3.主要义务三：遵守法规要求处理数据，切实履行法定义务

- 境内数据处理者应与境外数据接收方一同约定并承诺数据跨境传输活动符合《个人信息保护法》等法律法规所规定的数据处理的最小必要原则，出境个人信息范围仅限于实现处理目的所需的最小范围。双方还应当采取有效的技术和管理措施来确保个人信息安全。

标准合同征求意见稿中的主要相关条款：第二条第（一）款;第三条第（三）款

- 境内数据处理者应当对拟向境外接收方提供个人信息的活动开展个人信息保护影响评估，并保存个人信息保护影响评估报告至少3年。

标准合同征求意见稿中的主要相关条款：第二条第（七）款

延伸阅读：

标准合同征求意见稿中明确将开展个人信息保护影响评估作为个人信息处理者义务之一，但由于个人信息保护影响评估本就为《个人信息保护法》中所明确的法定义务之一，在数据跨境传输协议中再次明确，使之成为境内传输方需要向境外接收方承担

境内数据处理者应评估合同履约可行性，
配合监管机构调查问询。

的合同义务，会显著加重境内传输方的责任和义务，我们建议不要保留。具体有待标准合同正式稿进一步澄清、明确。

- 如果收到境外数据接收方有关发生个人信息泄露事件的通知，境内数据处理者应当及时依据法律法规要求进行应对，比如要求境外数据处理者及时同步相关信息，共同及时通知监管机构等。

标准合同征求意见稿中的主要相关条款：第三条第（六）款

4.主要义务四：评估合同履约可行性，配合监管机构调查问询

- 境内数据处理者应与境外数据接收方一同承诺，已尽最大努力了解境外接收方所在地的个人信息保护政策法规。双方已共同评估出境风险，确保境外接收方所在法域的法律法规不会影响本合同项下义务的履行。

标准合同征求意见稿中的主要相关条款：第四条

- 境内数据处理者应与境外数据接收方一同合作，及时答复来自境内监管机构的询问，接受监管机构的监督管理，配合监管机构调查，服从监管机构采取的措施或做出的决定，并提供已采取必要行动的证明文件、审计结果。

标准合同征求意见稿中的主要相关条款：第二条第（六）款、第（十）款；第三条第（十二）款

- 境内数据处理者应当承担证明数据跨境传输合同项下义务已履行的举证责任。

标准合同征求意见稿中的主要相关条款：第二条第（九）款

境外数据接收方应保护个人信息主体权利，
承诺配合第三方受益人权利行使。

PART 002

境外数据接收方的责任和义务

1.主要义务一：保护个人信息主体权利，承诺配合第三方受益人权利行使

- 境外数据接收方部署人员与机制，履行个人信息主体权利的保护义务。

标准合同征求意见稿中的主要相关条款：第三条第（二）款；第五条；第六条第（一）款

具体而言：

- 应当指定联系人，授权其答复并处理与个人信息处理相关的询问或投诉。境外数据接收方应当将该联系人的信息告知境内数据处理者和个人信息处理者。
- 与境内数据处理者一样，境外数据接收方也需应要求，向个人信息主体提供数据跨境传输协议副本。

- 若争议未能友好解决，境外数据接收方应当接受个人信息主体通过以下两种方式进行维权：一是向监管机构投诉，二是向合同所规定的法院提起诉讼，以行使第三方受益人权利。

标准合同征求意见稿中的主要相关条款：第六条第（三）款；第九条第（四）款

2.主要义务二：严守约定处理数据，最小限度存储数据，采取有效技术和管理措施保护数据安全

- 境外数据接收方应当严格按照合同所载“数据出境说明”所列约定处理数据，除非获得个人信息主体的事先同意。处理数据也应符合境内相关法律法规对于该类数据加工活动的合规要求，比如贯彻落实最小必要原则，进行自动化决策时保证透明度和公平性，提供不针对个人特征的选项等。

境外数据接收方应严守约定处理数据，最小限度存储数据，采取有效技术和管理措施保护数据安全。

标准合同征求意见稿中的主要相关条款：第三条第（一）款、第（三）款、第（九）款

- 境外数据接收方应当严格限制再次对外数据传输活动。再次对外提供数据前，应有必要性，获得个人信息主体同意，对第三方进行约束与监督，并且向个人信息处理者提供再次对外数据传输协议的副本。

标准合同征求意见稿中的主要相关条款：第三条第（七）款、第（八）款

- 境外数据接收方应当在为实现数据处理目的所需的最短时间内储存数据，贯彻落实数据存储的最小必要性原则：

标准合同征求意见稿中的主要相关条款：第三条第（四）款

  - 一般而言，超出存储期限后，应对所掌握的个人信息（含备份）进行删除或匿名化处理，除非取得个人信息主体关于存储期限的单独同意。
  - 受境内数据处理者委托的境外数据接收方，删除或匿名化处理所涉个人信息时，还应向个人信息处理者提供审计报告。
- 境外接收方需采取有效的技术措施、管理措施，防止发生数据泄露，并且进行定期检查，以确保这些措施持续维持适当的安全水平。境外数据接收方还需注意落实权限设置与员工管理，确保授权处理个人信息的人员履行保密义务，建立最小授权的访问控制策略，使其只能访问职责所需的最小必要的个人信息，仅具备完成职责所需的最少数据操作权限。

标准合同征求意见稿中的主要相关条款：第三条第（五）款

境外数据接收主应准确记录数据处理活动，积极配合数据处理者的监督，共同响应监管机构立问询。

- 如果发生个人信息泄露事件时，应当及时采取补救措施，并立即通知境内数据处理者及监管机构，同时记录相关事实与影响。

标准合同征求意见稿中的主要相关条款：第三条第（六）款

3.主要义务三：准确记录数据处理活动，积极配合数据处理者的监督，共同响应监管机构问询

- 境外数据接收方应当对开展的个人信息处理活动进行客观记录，并保存记录至少三年，并按法律法规要求向境内数据处理者和/或监管机构提供相关记录文件。

标准合同征求意见稿中的主要相关条款：第三条第（十一）款

- 境外数据接收方应当积极配合境内数据处理者的监督，协助并配合境内数据处理者进行数据跨境传输安全保护工作。

标准合同征求意见稿中的主要相关条款：第三条第（十）款；第四条

具体而言：

- 境外数据接收方应向境内数据处理者提供评估境外数据保护相关法律法规的相关信息。如境外接收方所在地数据保护相关法律法规发生变化可能影响合同履行的，境外数据接收方应及时通知境内数据处理者。
- 境外数据接收方应向提供所有必要信息以证明其履行了合同中的义务，比如其所持有的个人信息保护方面的资质认证情况等。
- 境外数据接收方还应允许其对数据文件和文档进行查阅，配合其对数据处理活动进行审计。

企业需在本文中归纳的主要责任与义务的基础上，针对具体的商业模式与数据跨境传输活动进行量体裁衣，妥善设计交易条款，从而同时满足法律合规及商务合作的需要。

- 如上一章节关注要点四所述，双方应协同合作，积极配合境内监管机构的工作，包括答复询问，配合检查，服从监管机构所做出的决定和所采取的措施等。

标准合同征求意见稿中的主要相关条款：第二条第（六）款、第（十）款；第三条第（十二）款

商业活动及数据交互模式千变万化，除直接适用标准合同机制的场景之外，企业在就涉及数据跨境传输的商务合同条款开展具体起草和谈判工作时，需在本文中归纳的主要责任与义务的基础上，针对具体的商业模式与数据跨境传输活动进行量体裁衣，妥善设计交易条款，从而同时满足法律合规及商务合作的需要。如有必要，可针对具体情境咨询外部专家意见。

李瑞
合伙人
公司业务部
北京办公室
+86 10 5957 2143
lirui@zhonglun.com

贾申
顾问
合规与政府监管部
北京办公室
+86 10 5957 2263
jiashen@zhonglun.com

数据出境安全新规出台：境外财富管理机构业务遭遇中国合规挑战?

龚乐凡 姜璐璐

本文将解答中国法对于境外财富管理机构的影响、未能积极应对调整合规策略的不利影响、境外财富管理机构究竟需要履行哪些合规义务、具体怎么做等几方面问题。

服务中国客户的境外财富管理机构，面临一项新的挑战——来自于中国最新的“数据出境安全”方面的新规定。境外的私人银行、资产管理公司、家族办公室，现在获取、保存、处理来自于中国的客户个人信息，由于该等数据来自于境内，必然遇到“数据跨境”的安全评估与法律合规问题，面对中国个人信息保护与数据出境的新规（“**新规**”），究竟意味着怎样的合规风险和挑战，该如何快速应对?不少机构对之了解甚少，应对起来倍感措手不及。

本文将从新规法律框架和法律责任作为起点（第一部分），站在境外财富管理机构展业、获客的合规的角度分享市场洞察（第二部分），从四大高频疑问（第三部分）解答中国法对于境外财富管理机构的影响、未能积极应对调整合规策略的不利影响、境外财富管理机构究竟需要履行哪些合规义务、具体怎么做等几方面问题，我们将通过几个案例分享一些成功经验（第四部分），帮助客户形成高效的合规路径和方案，化解合规部门无从应对的两难困境，最终帮助业务部门持续合规地推进业务，将合规成本降至最低。

PART 001

个人信息保护和数据出境：立法新动向和法律责任概览

从《个人信息保护法》（“**《个保法》**”，2021年11月1日生效）、到2022年9月1日生效的《数据出境安全评估办法》及其细则《数据出境安全评估申报指南（第一版）》（“**《申报指南（第一版）》**”），随着中国个人信息、数据出境方面陆续颁布新规，由于法规本身处于逐步完善、演进的过程，如何在实践中有效履行法定合规义务，存在没有先例可以参考的困境。

在我们服务高净值客户，或与境内外银行、财富机构的合作过程中，我们注意到，“是否需要按中国法新规的要求收集客户个人信息”，已经引起了一些财富管理机构，尤其是私人银行、保险公司、信托公司、家族办公室、资产管理公司等金融机构的关注和困惑，这些财富管理机构都需要履行客户背景尽职调查（即Know Your Client，“**KYC**”），KYC过程会涉及大量高净值客户个人信息的跨境传输、收集、分析，还涉及个人财产、家庭情况甚至医疗健康

如果境外财富管理机构没有在第一时间根据最新的立法进行调整，及时响应境内客房、合作伙伴的合规需求，可能就会错失一批业务机会。

信息等敏感个人信息。

根据《个保法》，个人信息跨境传输之前需要履行法定程序和义务，否则数据不能出境。违规进行跨境传输的，个人信息处理者将受到处罚，以及“直接负责的主管人员和其他直接责任人员”也将受到处罚，除了罚款以外，情况严重的，个人还会遭遇“任职限制”。

PART 002

措手不及和无所适从：数据新规对跨境KYC及获客带来直接影响

境外的一些财富管理机构合规部已经关注到中国个人信息出境监管的立法和监管动向，但是不清楚作为境外主体究竟有哪些责任和义务，针对个人信息如何处理，由于难以高效决策而导致业务部门无法及时开户、无法推进业务。

还有一种情形，由于境内合作伙伴给境外财富管理机构推介客户的时候，需要根据新规完成信息出境的风险自评估，因此需要针对境外财富管理机构的信息安全能力进行尽调，而有的境外财富管理机构合规部门对此的可能回应是，“我们是大型金融机构，已经遵守GDPR[1]规定，有健全的隐私法和数据安全法监管。”没有积极响应该合规要求。由于境外财富管理机构合规部和数据安全部门无法配合提供资料，导致了业务部迟迟无法与中国的高客签约。随着《数据出境安全评估办法》生效（2022年9月1日），数据出境的监管、执法日趋清晰，如果境外财富管理机构没有在第一时间根据最新的立法进行调整，及时响应境内客户、合作伙伴的合规需求，可能就会错失一批业务机会。

PART 003

合规挑战四大高频疑问

如何解决上述“无从应对”的难题？一方面，要纠正“认知误区”，例如，“我们已经按GDPR要求在处理信息，为何还要受中国法管辖？”另一方面，新法下合规要求和义务不少，需要用底线思维去审视这些合规要求，理清脉络，才能“高性价比”解

1.欧盟《通用数据保护条例（General Data Protection Regulations）》。

境外财富管理机构收集境内个人信息的行为属于《个保法》管辖范围。

决问题。

笔者希望通过对以下四大高频疑问进行解答，站在境外财富管理机构合规视角，帮助这些境外机构了解中国个人信息出境合规的法律要求和边界，能够快速响应客户需求，最大限度降低对业务的不利影响。

1.WHY（为什么）：境外财富管理机构在境外对中国客户个人信息进行KYC调查，为何需要遵守中国《个保法》和相关数据安全法规？（中国法新规对域外机构的影响）

根据《个保法》第三条第二款："在中华人民共和国境外处理中华人民共和国境内自然人个人信息的活动，有下列情形之一的，也适用本法：（一）以向境内自然人提供产品或者服务为目的；（二）分析、评估境内自然人的行为；（三）法律、行政法规规定的其他情形。"中国《个保法》具有域外管辖效力，在境外财富管理机构收集客户个人信息KYC的场景下，最终目的是"向境内自然人提供产品或者服务"。因此，境外财富管理机构收集境内个人信息的行为属于《个保法》管辖范围。

此外，在KYC信息收集、处理过程，通

常信息链路往往涉及跨境传输，因此需要遵守《个保法》第三章"个人信息跨境提供的规则"，例如，根据不同情况选择信息出境路径。如果落入需要向国家网信部门进行出境安全评估申报的数据出境情形，还需要同时按照《数据出境安全评估办法》（国家互联网信息办公室令第11号，已于2022年9月1日生效）准备相关数据出境安全评估资料并进行申报。

在法律责任方面，结合财富管理行业业务特色、数据合规风险严重程度和紧迫性，有三点内容值得关注。

2.RISKS（哪些风险）：如果不遵守中国法，是否会有处罚？会有哪些不利后果？

根据《个保法》《数据出境安全评估办法》等规定，未能遵守相关合规义务，将需要承担行政处罚[2]以及民事损害赔偿侵权责任[3]。如果构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任[4]。

在法律责任方面，结合财富管理行业业务特色、数据合规风险严重程度和紧迫性，有三点内容值得关注：

（1）财富管理机构网站、应用程序可能被叫停：除了罚款以外，如果涉及使用网站、应用程序（APP）违规收集、处理个人信息的，网信办有权要求其暂停或终止提供服务。根据网信办官方发布数据[5]，“全国网信系统上半年累计依法约谈网站平台3491家，警告3052家，罚款处罚283家，暂停功能或更新419家，下架移动应用程序177款。”可见网信办对于网站、应用程序是“重拳出击”，这意味着，一旦受到影响导致业务中断，一方面是经济损失，更重要的是客户体验变差，可能导致客户流失。

（2）境内大客户经理个人责任：除了单位受罚以外，“直接负责的主管人员和其他直接责任人员”也需要承担连带责任，情节严重的情况下，个人最高罚款可达100万元，甚至可能被“禁业”（监管部门“可以决定禁止其在一定期限内担任相关企业的董事、监事、高级管理人员和个人信息保护负责人。”），不少境外财富管理机构为了在境内开拓、维系大客户，通

2.《个人信息保护法》第六十六条：违反本法规定处理个人信息，或者处理个人信息未履行本法规定的个人信息保护义务的，由履行个人信息保护职责的部门责令改正，给予警告，没收违法所得，对违法处理个人信息的应用程序，责令暂停或者终止提供服务；拒不改正的，并处一百万元以下罚款；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

有前款规定的违法行为，情节严重的，由省级以上履行个人信息保护职责的部门责令改正，没收违法所得，并处五千万元以下或者上一年度营业额百分之五以下罚款，并可以责令暂停相关业务或者停业整顿、通报有关主管部门吊销相关业务许可或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款，并可以决定禁止其在一定期限内担任相关企业的董事、监事、高级管理人员和个人信息保护负责人。

3.《个人信息保护法》第六十九条：处理个人信息侵害个人信息权益造成损害，个人信息处理者不能证明自己没有过错的，应当承担损害赔偿等侵权责任。

4.《个人信息保护法》第七十一条：违反本法规定，构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

《刑法》（中华人民共和国主席令第66号，2020年修正）第二百五十三条之一：【侵犯公民个人信息罪】违反国家有关规定，向他人出售或者提供公民个人信息，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。

违反国家有关规定，将在履行职责或者提供服务过程中获得的公民个人信息，出售或者提供给他人的，依照前款的规定从重处罚。

窃取或者以其他方法非法获取公民个人信息的，依照第一款的规定处罚。

单位犯前三款罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，依照各该款的规定处罚。

5.《2022年上半年全国网络执法工作取得明显成效》（2022年7月31日）http://www.cac.gov.cn/2022-07/31/c_1660892422799965.htm

常会在境内设置业务经理团队，这一项处罚对于境内负责向境外财富管理机构传输数据的大客户经理将产生较大负面影响。

（3）境外财富管理机构主体存在受处罚可能性：如前文所分析，《个保法》具有域外管辖效力，《个保法》第六十六条法律责任条款，针对处罚对象亦没有明确将境外主体排除在外，同时根据《个保法》第四十二条："境外的组织、个人从事侵害中华人民共和国公民的个人信息权益，或者危害中华人民共和国国家安全、公共利益的个人信息处理活动的，国家网信部门可以将其**列入限制或者禁止个人信息提供清单**，予以公告，并采取限制或者禁止向其提供个人信息等措施。"从法条层面，境外主体若发生违规行为，中国网信部门有权进行执法。这对于视商誉为生命的金融机构来说，再小的处罚，都会带来极大的负面影响。

根据以上分析，如果境外财富管理机构存在违规收集、传输个人信息的情形，存在潜在法律风险，轻则罚款，重则暂停应用程序、网站。

还有一类**隐形风险更为常见**，但往往容易被忽视，境内信息处理者向境外提供个人信息需要完成风险自评估、甚至可能需要向网信办进行数据出境安全评估申报，在此过程中需要对境外接收方进行数据安全尽职调查，如果未能通过数据出境安全评估的，客户信息将无法出境，对于境外财富管理机构来说，可能意味着丢失重要的客户和商机。

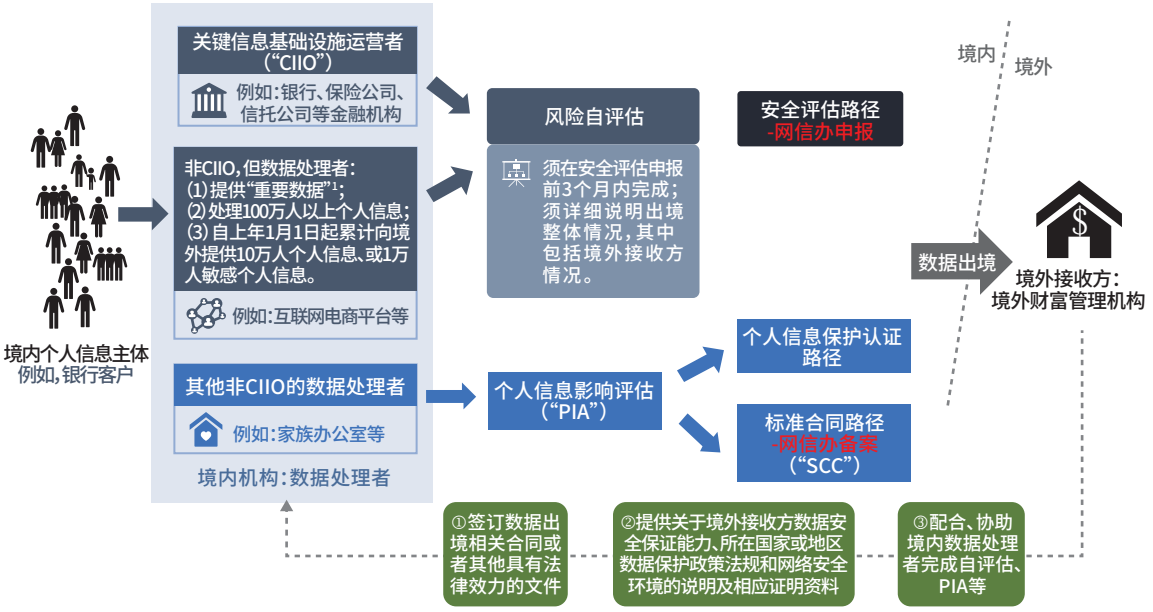
3.WHAT（该做什么）：境外财富管理机构需要履行哪些合规义务？

在回答这个问题之前，需要先厘清一个问题，在数据出境安全评估的情况下，究竟由谁向监管部门提出申报？在存在境内机构向境外财富管理机构转介客户的场景下，境内主体是境内"数据处理者"，由境内信息处理者主导"个人信息保护影响评估"（Privacy Impact Assessment，"**PIA评估**"）、"数据出境风险自评估"、作为申报主体向网信办提交"安全评估申报"。

尽管安全评估由境内主体负责，但这并不意味着境外信息接收方可以"不作为"。以网信办数据出境"安全风险自评估"要求举例，根据《数据出境安全评估办法》以及《申报指南（第一版）》规定，针对

境外接收方需要进行尽调，包括说明处理数据的用途和方式、说明数据安全保障能力、说明境外接收方处理数据的全流程过程描述，而这些内容需要境外接收方提供相关证明文件，除了配合尽调以外，境外接收方还有一些相关的合规义务，例如，与境内主体订立数据处理协议等等。[6]

下图展示了不同境内主体的数据出境合规义务，以及境外金融机构所需要关注的重要内容。



注1：《网络安全法》首次提出"重要数据"的概念，规定关键信息基础设施运营者在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。但对"重要数据"的定义和范围仍有待明确。

6.《数据出境安全评估办法》第五条：数据处理者在申报数据出境安全评估前，应当开展数据出境风险自评估，重点评估以下事项：
（一）数据出境和境外接收方处理数据的目的、范围、方式等的合法性、正当性、必要性；
（二）出境数据的规模、范围、种类、敏感程度，数据出境可能对国家安全、公共利益、个人或者组织合法权益带来的风险；
（三）境外接收方承诺承担的责任义务，以及履行责任义务的管理和技术措施、能力等能否保障出境数据的安全；
（四）数据出境中和出境后遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等的风险，个人信息权益维护的渠道是否通畅等；
（五）与境外接收方拟订立的数据出境相关合同或者其他具有法律效力的文件等（以下统称法律文件）是否充分约定了数据安全保护责任义务；
（六）其他可能影响数据出境安全的事项。

以个人信息跨境传输规则为例，《个保法》主要规定了三种数据出境路径，每条路径所需的程序，难度和耗费时间都有所不同。

4.HOW（怎么做）：拨开迷雾，寻找成本可控的合规策略、方案

（1）误区1：境外机构已按GDPR构建了成熟、健全的个人信息保护、数据安全政策，是否可以默认满足中国法合规要求？

一些境外财富管理机构，尤其是欧盟、新加坡、香港的机构经常会问如上的问题，他们针对隐私法、数据合规意识比较强，也就产生了这样的一种误区，认为自身已经遵循GDPR、PDPA[7]、香港《个人资料（私隐）条例》等当地数据保护法的监管，于是就默认其相关数据处理行为的操作思路和模式也满足了中国法新规要求。这显然是错误的。

实际上，尽管个人信息、数据安全部分立法原则上存在类似的内容，但遵守境外隐私法、数据合规法规，并不能直接等同于已满足中国法合规要求。境外机构必须根据中国法新规重新审视与中国有关的业务产生的信息流，结合新规调整相关合规指引。

（2）误区2：是否所有KYC都需要向中国网信部门进行安全评估申报？是否有统一标准可以遵循？

信息出境路径的合规程序将直接影响信息能否成功出境以及时间表。以个人信息跨境传输规则为例，《个保法》主要规定了三种数据出境路径[8]，包括经网信部门安全评估后的出境路径（“**网信办安全评估路径**”）、经个人信息保护认证后的出境路径、采用订立网信部门指定的标准合同的出境路径。

每条路径所需的程序，难度和耗费时间都有所不同。其中，根据目前法规颁布的情况，相比其他出境路径，按网信办安全评估路径出境规则较为明确，但从程序上看，能否成功并及时通过网信部门审查存在较大不确定性，在网信部门安全评估审批程序，法定至少需要45个工作日，甚

7.指新加坡《个人数据保护法》（Personal Data Protection Act，简称“PDPA”）

8.《个保法》第三十八条：个人信息处理者因业务等需要，确需向中华人民共和国境外提供个人信息的，应当具备下列条件之一：

（一）依照本法第四十条的规定通过国家网信部门组织的安全评估；

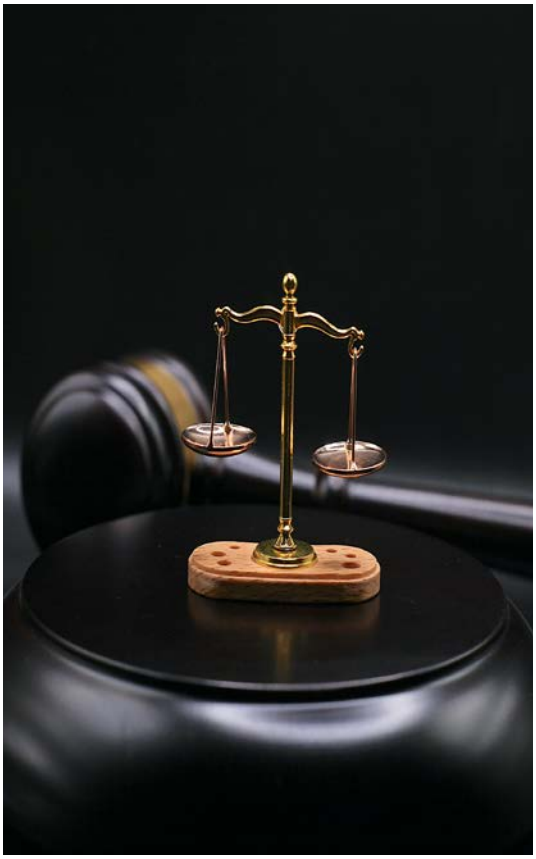
（二）按照国家网信部门的规定经专业机构进行个人信息保护认证；

（三）按照国家网信部门制定的标准合同与境外接收方订立合同，约定双方的权利和义务；

（四）法律、行政法规或者国家网信部门规定的其他条件。

中华人民共和国缔结或者参加的国际条约、协定对向中华人民共和国境外提供个人信息的条件等有规定的，可以按照其规定执行。

境外财富管理机构如果希望避免因前述程序问题耽误客户KYC流程，建议提前规划信息出境链路，高效解决合规问题。



至可能因材料不符合要求导致终止审查。[9]

需要注意的是，如果境外财富管理机构是通过境内金融机构转介客户，或者个人信息跨境传输达到一定量级的，是必须向网信部门进行数据出境安全申报的。因此，境外财富管理机构如果希望避免因前述程序问题耽误客户KYC流程，建议提前规划信息出境链路，高效解决合规问题。

PART 004

我们的方案：境外财富管理机构如何顺势而为，“高效”化解合规困境？

1.来自境外财富管理机构合规部门的“烦恼”：究竟该如何积极应对中国法合规要求？

如上文介绍，境外接收方需要回复尽调清单并提供文件。面对这样一份尽调清单，有些境外财富管理机构会感到不理解，通常会有几类反馈，“我们是XX国银行，已经通过本国的信息安全认证，为何需要提供这么多证明资料？”“集团不允许我们按中国法订立数据处理协议”。“我们合规部门感觉这是你们在对我们进行信息安全审计，我们没有义务配合。”“这属于我们的集团政策、商业秘密，无法提供。”之后，合规部与业务部就陷入了“无解”的僵持。

9.《数据出境安全评估办法》第十二条：国家网信部门应当自向数据处理者发出书面受理通知书之日起45个工作日内完成数据出境安全评估；情况复杂或者需要补充、更正材料的，可以适当延长并告知数据处理者预计延长的时间。

《数据出境安全评估办法》第十一条 安全评估过程中，发现数据处理者提交的申报材料不符合要求的，国家网信部门可以要求其补充或者更正。数据处理者无正当理由不补充或者更正的，国家网信部门可以终止安全评估。

数据处理者对所提交材料的真实性负责，故意提交虚假材料的，按照评估不通过处理，并依法追究相应法律责任。

通过规划最佳实践方案，帮助客户摆脱“纸面合规”，
省“时”省金。

2.我们的解决方案：通过规划最佳实践方案，帮助客户摆脱“纸面合规”，省“时”省金

站在境外财富管理机构获客的立场和角度，当互相竞争的机构因为“合规原因”而卡顿无法为客户开户的时候，你会发现，抢占时间和先机就是抢夺AUM[10]，举一个直观的例子，如果私行KYC长达几个月都没有完成，可能客户就会转而将财富交给其他私行管理了。但是，合规的底线需要守住，那么怎么做才能实现既合规又高效呢？我们通过几个实战案例，分享一些解决思路。

成功案例1：协助境外财富管理机构配合境内风险评估尽调

当境外财富管理机构收到风险评估尽调清单，业务部门被境内合作伙伴催促尽快提交，而合规部门却出于保密风控要求不太配合，怎么办？根据我们处理的经验，如果对资料的颗粒度把控不好，索取资料过多、过少都会产生问题，资料要求过多、过于深入，后果可想而知，要么合规部门需要花费很多时间收集，要么是根本不予配合，资料尽调流于形式可能又会导致无法通过安全评估。那么，此时就需要通过专业沟通，我们基于实操经验，向合规部门、数据安全部门澄清资料的颗粒度，顺利、高效收集这些资料，配合境内的尽调工作。

10.Asset Under Management（资产管理规模）。

答案并非yes or no那么简单，需要结合具体的商业模式、信息链路综合分析才能给出最佳方案。

成功案例2：规划高效、合规数据出境路径

有一家欧洲知名资管公司客户合规意识非常强，主动要求按中国法合规要求操作，但苦于信息链路的其他主体因集团没下达配合的指令而无法推进，到时各方僵持，业务无法开展，客户找到我们希望进行合规风险评估以便内部决策，客户甚至在考虑是否通过集团政策限制欧洲总部接受来自中国的个人信息。我们进行了跨境数据出境映射分析（Cross-border Data Mapping），重新审视了信息处理链路以及各方的职责，成功找到了突破口，帮助客户高性价比地解决了这一困境，使得业务可以重新开展。

我们服务过程中，还会碰到这样的客户问题："如果我给境外机构介绍客户，直接拉个微信群介绍，是否就可以不用进行安全评估了？"诸如此类的客户问题，答案并非yes or no那么简单，需要结合具体的商业模式、信息链路综合分析才能给出最佳方案。

成功案例3：帮助境外机构梳理业务模式，寻找最佳合规路径

我们做大型并购交易、licensing交易、IPO等项目时，通常会使用云储存服务器存储尽调资料。随着中国数据出境法规的陆续生效，这些云储存服务商非常头疼，他们面临着新用户、现有用户的疑问，"你们的服务器系统是否已经根据中国法规定进行了调整？"针对这样的情况，我们为客户设计了可行的业务模式与IT服务器搭建架构，考虑到架构调整需要耗费时间，针对过渡期内用户可能提出的疑问，我们还为客户制备了《用户问答手册》，通过这样的安排，成功地帮助客户在面临法规、监管趋严的情况下，能够与时俱进迅速应变，吸引新用户。

谁能够抢先合规，谁就能抢先避免因为强监管所带来的处罚风险，并且“接住”那些其他机构因为合规问题没有解决而无法接单、开户的客户。

PART 005

启示：如何将挑战变为机遇

F1车手阿尔顿•塞纳说过：“天气晴好的时候，你无法一下子超越15辆车，但是天降大雨的时候，你却可以。”

在面对合规大变局的情况下，谁能够抢先合规，谁就能抢先避免因为强监管所带来的处罚风险，并且“接住”那些其他机构因为合规问题没有解决而无法接单、开户的客户，这就是危机带来的商机。

所以，如果能够快速行动，强占合规先机，就可以避免未来突发事件对业务的冲击，同时掌握合规实践的最佳路径，就能迅速、有效响应，就有机会利用弯道超车，抢占市场。

龚乐凡
合伙人
私募基金与资管部
上海办公室
+86 21 6061 3608
lefangong@zhonglun.com

姜璐璐
非权益合伙人
私募基金与资管部
上海办公室
+86 21 6061 3063
jianglulu@zhonglun.com

数据出境新规下，企业如何应对临床试验数据出境新局面？

严静安 陈方强 叶筝

临床试验数据出境场景将涉及多部门多维度的监管，企业应当如何准备与应对？其中千头万绪，本文试做梳理。

在临床试验数据的安全问题开始逐渐被关注之前，我国在临床试验数据方面的监管主要依靠《药物临床试验质量管理规范》（“**GCP**”）等临床试验相关管理要求进行规范和保护，其中体现的主要是国家药品监督管理局（“**药监局**”）和国家卫生健康委员会（“**卫健委**”）对于临床试验过程中收集到的数据的监管要求，尤其是针对受试者的个人信息的保护。

对于临床试验数据的出境，作为申办方的医药企业此前的主要考量是围绕《中华人民共和国人类遗传资源管理条例》（“**《人遗条例》**”）中规制人类遗传资源信息对外提供行为的要求而展开的。然而，自《中华人民共和国个人信息保护法》（“**《个保法》**”）出台，以及2022年7月7日国家互联网信息办公室（“**网信办**”）颁布《数据出境安全评估办法》以来，网信办对于数据出境的监管思路日益明晰并不断细化。在此背景下，临床试验数据出境场景将涉及多部门多维度的监管，企业应当如何准备与应对？其中千头万绪，本文试做梳理，以期抛砖引玉。

PART 001

哪些常见业务场景会涉及临床试验数据的出境？

（一）跨境申报新药临床试验审批（“IND”）和新药注册申请（“NDA”）

境内企业向境外药品监管机构申请IND时，一般需要就该临床试验申请向境外药品监管机构提交总体研究计划、研究员手册、临床研究方案、化学、生产和质量控制信息、药理和毒理信息、已有人体临床经验、额外信息等。

在NDA阶段，通常需要向境外监管机构（如FDA）提供药品生产信息、非临床药理和毒理数据、临床试验中产生的人体药代动力学和生物利用度数据、微生物数据、临床数据、安全性数据更新报告、统计学数据、病例报告表、有关专利情况、样品、包装及标签等。

（二）国际合作研究涉及的临床试验数据出境

外方单位与中国合作方共同开展国家合作研究，涉及临床试验的，可能会伴随相

使用EDC系统或管理系统服务器将临床数据向境外提供或对外开放、基于科研目的向境外发布临床试验结果就可能构成临床试验数据出境。

关临床试验数据的出境。在该场景下，企业方除了需根据《人遗条例》就国际合作中涉及的人类遗传资源材料及人类遗传资源信息的出境向科学技术行政部门申请相关审批或备案外，其他不属于人类遗传资源信息的临床数据也可能随着研究项目的开展需要向境外提供。

（三）使用EDC系统或管理系统服务器将临床数据向境外提供或对外开放

电子数据采集（Electronic Data Capture，**EDC**）是一种基于计算机网络的用于临床试验数据采集的技术，通过软件、硬件、标准操作程序和人员配置的有机结合，以电子化的形式直接采集和传递临床数据。近年来电子数据采集技术在临床试验中越来越多地被采用，由于其具有数据及时录入、实时发现数据错误、加快研究进度、提高数据质量等优势，各国药品监管部门都鼓励临床试验中采用电子数据采集技术以保证数据质量。若该等采集系统或管理系统的数据传输设置需要将数据传输出境，或将数据向境外主体开放访问权限，或其服务器和运维部署在境外，都可能构成临床试验数据出境。

（四）基于科研目的向境外发布临床试验结果

开展临床试验的研究机构对于其研究发现可能会向境外机构或刊物投稿发布研究成果，在投稿或审稿等过程中可能涉及相关临床试验数据向境外机构提供的情形。

PART 002

个人信息和数据保护法规对临床试验数据出境合规提出了哪些要求？

《个保法》颁布后，其中关于个人信息跨境传输的具体合规路径和门槛要求未同时落地，这导致跨国药企在开展跨国药物研究业务时一直面对着较大的合规不确定性。自2022年6月以来，我国出台了一系列与数据出境相关的法规和征求意见稿，数据出境法规框架正在不断地明确，监管对于实践落地的细节也给出了大幅细化的方向，其中包括2022年6月24日全国信息安全标准化技术委员会（“**信标委**”）发布的《网络安全标准实践指南—个人信息跨境

如果达到安全评估的门槛的，则必须进行安全评估，如果没有达到的，可以选择机构认证或者签署标准合同。

处理活动安全认证规范》（“**《认证规范》**”），2022年6月30日网信办发布的《个人信息出境标准合同规定（征求意见稿）》（“**《标准合同规定》**”，《标准合同规定》附件《个人信息出境标准合同》下称“**中国SCC**”）和2022年7月7日网信办颁布并将于今年9月1日正式生效的《数据出境安全评估办法》。

对于有临床试验数据出境需求的药企来说，这些法规和征求意见稿解答了数据出境活动中的一些基础性问题，明晰了企业数据出境的合规路径，便于药企判断自己是否需要进行安全评估的申报，并且促使药企开始思考其在处理和向境外提供临床数据的实践中，如何履行有关充分同意、单独同意、自评估等合规要求。

《个保法》提供了三条主要的向境外提供个人信息的合规路径，分别为通过国家网信部门组织的数据安全评估（**安全评估**），按照国家网信部门的规定经专业机构进行个人信息保护认证（**机构认证**），或者按照国家网信部门制定的标准合同与境外接收方订立合同，约定双方的权利和义务（**标准合同**）[1]。三者的关系是，如果达到安全评估的门槛的，则必须进行安全评估，如果没有达到的，可以选择机构认证或者签署标准合同。下面对这三条路径在临床试验数据出境的场景下可能面临的问题做一个简单的探讨。

（一）临床试验数据安全评估

数据安全评估的门槛要求在《数据出境安全评估办法》[2]中明确为：

1）数据处理者向境外提供重要数据；

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；

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的数据处理者向境外提供个人信息；

4）国家网信部门规定的其他需要申报数据出境安全评估的情形。

上述第1）条涉及重要数据，第2）和第3）条涉及个人信息。

1.重要数据出境需安全评估

申办者应当考虑受试者个人信息构成

1.《中华人民共和国个人信息保护法》第三十八条。
2.《数据出境安全评估办法》第四条。

后续不同的地区以及不同监管方对于临床试验业务场景下的重要数据也可能会有不同的定义，且该等不同部门对于数据内涵理解不统一的状态可能会长期持续。

重要数据的客观可能性。《中华人民共和国数据安全法》（“**《数安法》**”）、《数据出境安全评估办法》等法律法规判断重要数据的指标是其遭到篡改、破坏、泄露或者非法获取、非法利用后对于国家安全、经济运行、社会稳定、公共健康和安全的危害[3]。虽然《数安法》要求各地区、各部门应当按照数据分类分级保护制度，确定本地区、本部门以及相关行业、领域的重要数据具体目录，但数据主管部门及医疗行业主管部门尚未对医药领域的重要数据制定具体目录。

2022年版本的《信息安全技术重要数据识别指南》（征求意见稿）在重要数据的识别因素中列明：“h）反映群体健康生理状况、族群特征、遗传信息等的基础数据，如人口普查资料、**人类遗传资源信息、基因测序原始数据**属于重要数据”[4]。该版《信息安全技术重要数据识别指南》（征求意见稿）由信标委发布。

而网信办也在2021年11月14日发布的《网络数据安全管理条例（征求意见稿）》中对重要数据进行了定义和列举，其中包括“5.达到国家有关部门规定的规模或者精度的基因、地理、矿产、气象等**人口与健康**、自然资源与环境国家基础数据”[5]。

由以上不同文件中对于重要数据的内涵和外延的解释可以看出，监管部门对于涉及一定量人口基数的，与人口总体健康特征、遗传、基因等方面有关的信息是倾向于加强监管并将其作为较高风险级别的数据进行处理的。同时，上述文件中不尽相同的表述似乎也体现了各监管部门对于重要数据不同角度的理解。

基于《数安法》要求，各地区、各部门应当确定本地区、本部门以及相关行业、领域的重要数据具体目录，我们认为，后续不同地区以及不同监管方对于临床试验业务场景下的重要数据也可能会有不同的定义，且该等不同部门对于数据内涵理解不统一的状态可能会长期持续。在相关的要求被正式明确之前，企业可以（1）从重要数据的定义入手，尝试分析其手中临床试验项目数据一旦遭到篡改、破坏、泄露或者非法

3.《中华人民共和国数据安全法》第二十一条；《数据出境安全评估办法》第十九条。
4.《信息安全技术重要数据识别指南》（征求意见稿）（2022年1月13日颁布）第5条。
5.《网络数据安全管理条例》（征求意见稿）（2021年11月14日颁布）第七十三条第（三）项。

企业需要提前制定应对策略，并判断是否可以避免或减少敏感个人信息的跨境传输，或者如何提高通过安全评估的可能性。

获取、非法利用对于国家安全、经济运行、社会稳定、公共健康和安全可能产生的影响，或者寻求专业法律意见；(2) 注意药监局和卫健委对于医疗行业重要数据划分的监管动态，结合现有的《人遗条例》的监管体系，除履行利用人类遗传资源开展国际合作研究的备案/审批程序、对外提供人遗信息备案、人遗材料出境审批等要求外，对于涉及人类遗传资源信息和基因信息的临床试验数据进行不低于法定的重要数据保护和出境要求的合规处理；(3) 结合自身临床试验项目涉及的个人数量，如自判有临床试验项目涉及受试者数量众多的，则需要提供更高的安全保护措施。

2.敏感个人信息的出境门槛

除了普通的个人信息，药物临床试验中还涉及大量受试者的敏感个人信息。《个保法》将医疗健康信息规定为敏感个人信息，但并未就其外延给出进一步的详细列举。此前，国家标准GB/T 35273-2020《信息安全技术 个人信息安全规范》中将“个人因生病医治等产生的相关记录，如病症、住院志、医嘱单、检验报告、手术及麻醉记录、护理记录、用药记录、药物食物过敏信息、生育信息、以往病史、诊治情况、家族病史、现病史、传染病史等”列为敏感个人信息[6]。

而根据GCP，临床试验阶段所产生的源数据包括如医院病历、医学图像、实验室记录、备忘录、受试者日记或者评估表、发药记录、仪器自动记录的数据、缩微胶片、照相底片、磁介质、X光片、受试者文件，药房、实验室和医技部门保存的临床试验相关的文件和记录，包括核证副本等[7]。可以

6.GB/T 35273-2020《信息安全技术 个人信息安全规范》附录B。
7.《药物临床试验质量管理规范》第十一条第（三十一）项。

在未触发安全评估门槛的情况下，企业可以选择标准合同或机构认证的方式确保向境外传输数据的行为符合中国法律的要求。

看出，临床试验数据中天然地含有各类敏感个人信息。因此，如果将包含敏感个人信息的临床试验数据不加处理地向境外传输，一旦涉及传输超过一万人的敏感个人信息，即需要向网信部门进行出境安全评估的申报。在实践中，临床试验为了保证其结果的准确性和科学性，达到一万人的门槛数量是较为常见的。相关企业需要提前制定应对策略，并判断是否可以避免或减少敏感个人信息的跨境传输，或者如何提高通过安全评估的可能性。

（二）安全评估以外的合规路径：标准合同与机构认证

在未触发安全评估门槛的情况下，企业可以选择标准合同或机构认证的方式确保向境外传输数据的行为符合中国法律的要求。无论是信标委发布的《认证规范》，还是网信办发布的《标准合同规定》，其均要求传输方和境外接收方签署有法律约束力的协议，其中提出了较多具体要求。尤其是《标准合同规定》，除要求境外接收方处理个人信息的目的、范围、方式须具有合法性、正当性、必要性，评估出境个人信息的数量、范围、类型、敏感程度以及个人信息出境可能对个人信息权益带来的风险外，亦要求明确境外接收方承诺承担的责任义务，其履行责任义务的管理和技术措施、能力等能否保障出境个人信息的安全，需要评估个人信息出境后泄露、损毁、篡改、滥用等的风险，个人维护个人信息权益的渠道是否通畅，还需要评估境外接收方所在国家或者地区的个人信息保护政策法规对标准合同履行的影响。该等境外接收方国家或地区的信息保护法规程度可能需要寻求当地专业律师的意见。

《标准合同规定》亦要求境外接收方允许境内个人信息处理者对数据文件和文档进行查阅，或对其涵盖的处理活动进行审计。“中国SCC”附录二部分专门提供了合同当事双方约定的其他条款部分，据此，合同双方可以在附录二中自行协商约定适合自身业务安排的条款。但是，《标准合同规定》第2条第二款规定，境内个人信息处理者与境外接收方签订与个人信息出境活动相关的其他合同，不得与标准合同相冲突。

如临床试验数据境内传输方和境外接收方并非属同一集团公司（譬如直接向境

使用鉴认代码或许可以满足《个保法》中的“去标识化”，但很可能不能满足“匿名化”的要求。

外科研杂志机构提供信息等情况），如要求境外接收方签署“中国SCC”，境外接收方可能会因为标准条款对其施加了较重的义务以及必须接受中国法管辖等原因而有所抵触。目前《标准合同规定》的正式版还有待出台，同时认证工作的实际开展和认可也有待网信办等监管部门一同推动落实，在此之前，相关申报方和科研机构应就跨境方案（包括跨境传输的内容和传输路径的设计等）和跨境合规途径的选择进行消化和充分的探讨，包括与境外接收方进行沟通。

（三）其他合规要求

1.使用鉴认代码的要求与个人信息的匿名化

或许有些申办方会希望GCP要求下的鉴认代码指代方式可以同时满足《个保法》项下对于匿名化的要求，从而使得该等向境外传输的行为不需要被纳入计算安全评估的门槛数量内。虽然GCP要求研究者应在记录不良事件和其他与试验有关的数据时以受试者鉴认代码来代表受试者，但是，由于临床试验中出于研究需要会采集大量特定受试者的生理医疗特征以及病历病史信息，该等临床试验数据若与其他信息结合，未必不能识别出个人信息背后的特定个人。因此，使用鉴认代码或许可以满足《个保法》中的“去标识化”，但很可能不能满足“匿名化”的要求。

敏感个人信息跨境传输安全评估的较低门槛、临床试验数据的出境需求以及《个保法》下匿名化的高标准，使得临床试验数据出境的合规难度有所提高。医药行业亟待有关部门对于包含临床试验数据在内的医疗健康个人信息的分级分类、匿名化或脱敏、出境合规等内容做出具体的指引，以期实现数据的安全共享和并达到科研应用的目的。

2.知情同意、单独同意、另行获取同意

《个保法》下，除明确列出的豁免情形外，对于个人信息的处理要以获取个人在充分知情的前提下自愿、明确的同意为前提[8]。由于临床试验数据涉及数据主体的诊疗记录、用药记录等敏感个人信息，因此，需要向受试者告知有关处理其敏感个人信

8.《中华人民共和国个人信息保护法》第十三条、第十四条。

我们建议申报方或者研究机构至少在同意函中披露当下已知的境外接收方全部的处理目的、范围以及全部可能的后续境外接收方。

息的必要性以及对个人权益的影响[9]。

此外，《个保法》更要求将个人信息提供给其他个人信息处理者以及向境外提供时都需要获取个人信息主体的单独同意[10]。GCP项下亦要求获取受试者的知情同意，受试者被告知可影响其做出参加临床试验决定的各方面情况，确认同意自愿参加临床试验后[11]，研究者方可采集其临床数据进行研究活动。

现阶段，监管部门并未对《个保法》和GCP下的知情同意之间的关系进行释明。我们倾向于认为，《个保法》和GCP保护的法益在临床试验场景下有所交叉，都需要受试者自愿同意；但是，《个保法》和GCP的立法目的和监管范围事实上绝大部分有所不同，因此单纯期望以满足GCP要求的知情同意函来覆盖《个保法》下对于个人信息的种种保护要求，是不充分的。

我们理解，如在已经开始的临床试验项目里为了满足《个保法》的要求而修改知情同意函并另行获取受试者的同意，可能会面临一系列实践中的困难。一方面，可能不是全部受试者都一定会愿意签署，获取全部受试者的签名的可能性较低且成本可能较高。另一方面，《个保法》要求向个人信息主体告知接收方的名称、联系方式、处理目的、处理方式和个人信息的种类，当接收方超越已告知的处理目的、处理方式和个人信息的种类等范围处理个人信息时，需要再次重新取得个人同意。但境内实体在实践中可能难以确保境外接收方在收到临床数据后仅按照其承诺的范围和方式进行处理。

针对以上实践难点，行业的共识亟待达成，目前我们建议申报方或者研究机构至少在同意函中披露当下已知的境外接收方全部的处理目的、范围以及全部可能的后续境外接收方，并尽可能地定期提供境外接收方是否再传输和将临床数据用于其他目的的更新，供受试者自行查阅，并提供便捷的联系方式供受试者撤回或修改同意等。

3.自评估

无论是《个保法》，还是《认证规范》《标准合同规定》或《数据出境安全评估办法》，都要求进行个人信息保护影响评估（“**自评**

9.《中华人民共和国个人信息保护法》第三十条。
10.《中华人民共和国个人信息保护法》第二十三条、第三十九条。
11.《药物临床试验质量管理规范》第十一条第（十一）项。

在个人信息和数据保护法律法规不断完善、细化的大背景下，临床试验数据的出境面临着新的合规挑战。

估”）。鉴于自评估需要全面了解被评估主体的数据流和个人信息保护活动的全貌，并且也涉及对于境外接收方个人信息保护环境的评估，我们建议有出境需求的临床试验参与方应尽早开始进行自评估的工作。

PART 003

小结

在个人信息和数据保护法律法规不断完善、细化的大背景下，临床试验数据的出境面临着新的合规挑战。以往以知情同意函获取受试者同意、使用人遗资源信息对外提供规则约束数据出境的方式已经不能完全满足现有的数据出境法规的要求。《个保法》已于2021年11月1日生效，《数据出境安全评估办法》也将于2022年9月1日正式生效，相关企业宜尽早（1）根据《个保法》的要求开始知情同意函的更新和受试者签署的收集；（2）启动自评估，对所涉重要数据、个人信息和敏感个人信息进行梳理，讨论各类数据出境的必要性；（3）就临床试验数据出境的三条合规路径进行考察，判断是否达到了触发申报安全评估的门槛数量，以及签署标准合同或进行机构认证的可行性。在立法与实践不断接轨的进程中，企业可以根据其自身临床试验项目的特点和业务实际需求，寻求专业的法律意见，把握和落实个人信息和数据保护法律法规提出的新要求，并将其转化为现实可操作的合规建议。

严静安
合伙人
公司业务部
上海办公室
+86 21 6061 3187
yanjingan@zhonglun.com

PART TWO

司法视角下的数据合规

透过Cadence v. Syntronic 看数据出境：企业应对外国司法和行政程序的合规方案

陈际红

本文透过Cadence v. Syntronic案，总结企业在面对外国执法机构或司法机构强制调取数据时的合规方案，供企业面临相关场景时参考。

PART 001

案例评析：Cadence v. Syntronic

美国当地时间2022年6月24日，北加州联邦地区法院（Northern District Court of California，以下简称“**法庭**”）驳回了被告Syntronic北京公司要求法庭重新考虑此前作出的、要求Syntronic将位于中国境内的员工电脑运往美国接受检查的动议。

本案[1]中原告Cadence声称被告Syntronic北京公司未经许可使用其软件，为进行事实认定，法庭命令（order）被告将24台计算机运往美国进行检查。被告因此提出请求法庭重新考虑的动议（Motion for Reconsideration）。在动议中，被告主要依据《个人信息保护法》第39条[2]，声称相关计算机包含使用该等计算机的被告公司员工和前员工的受保护的个人信息，而《个人信息保护法》禁止被告在获得相关员工和前员工的同意前对其个人信息进行跨境提供。被告进一步声称，由于本案中相关员工拒绝同意其个人信息出境，因此法庭应考虑礼让原则，不应要求被告违反中国法律。

法庭在驳回被告的动议时指出，《个人信息保护法》第13条规定，除同意外，处理个人信息可以依据其他的合法性基础。若处理个人信息的合法性基础非同意的，则进行《个人信息保护法》其他条款所规定的需取得个人同意的个人信息处理活动时，不需取得个人同意。法庭进一步认定，本案中法庭的命令对被告产生了一项法律义务，被告基于“为履行法定职责或者法定义务所必需”这一合法性基础，跨境提供员工个人信息时无需取得其同意。

本文暂不对法庭适用的合法性基础如何展开讨论。跨境提供个人信息可以基于除同意外的其他合法性基础已基本成为业内共识，法庭据此驳回被告动议于理有据。被告在面对外国法院证据调取的命令时，虽提出了国际礼让原则，但抗辩所依据的法律条款并未与法庭作出的证据调取命令构成实质上的法律适用冲突，为外国法院

1.Case No.21-cv-03610-SI (JCS)

2.《个人信息保护法》第三十九条　个人信息处理者向中华人民共和国境外提供个人信息的，应当向个人告知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。

“阻断条款”为境内企业应对外国司法、执法机构强制调取数据命令提供了一盏指路明灯，但其并非凭空诞生。

留有了驳回的余地。针对外国法院强制调取位于我国境内的证据这一情形，其实我国立法者已在《数据安全法》与《个人信息保护法》中设立了相关的“阻断条款”，具体如下：

“《数据安全法》第三十六条　中华人民共和国主管机关根据有关法律和中华人民共和国缔结或者参加的国际条约、协定，或者按照平等互惠原则，处理外国司法或者执法机构关于提供数据的请求。非经中华人民共和国主管机关批准，境内的组织、个人不得向外国司法或者执法机构提供存储于中华人民共和国境内的数据。

《个人信息保护法》第四十一条　中华人民共和国主管机关根据有关法律和中华人民共和国缔结或者参加的国际条约、协定，或者按照平等互惠原则，处理外国司法或者执法机构关于提供存储于境内个人信息的请求。非经中华人民共和国主管机关批准，个人信息处理者不得向外国司法或者执法机构提供存储于中华人民共和国境内的个人信息。”

无论需跨境提供的证据属于“个人信息”还是涵盖范围更广的“数据”，我国企业在面对外国司法或者执法机构调取存储于我国境内相关证据的要求时，均可依据上述相关条款（以下简称“**阻断条款**”）提出抗辩：未经我国相关主管机关的批准即向境外提供证据的，将面临罚款、停业整顿、吊销相关业务许可证或吊销营业执照等处罚，与遵守外国司法、执法机构作出的证据调取命令构成实质上的法律冲突。

PART 002

“阻断条款”的出台背景

“阻断条款”为境内企业应对外国司法、执法机构强制调取数据命令提供了一盏指路明灯，但其并非凭空诞生。2018年，美国为解决政府搜查令能否要求通信服务商提供存储在境外服务器上的数据问题，通过了《合法使用域外数据澄清法案》（the Clarifying Lawful Overseas Use of Data Act，以下简称“**CLOUD Act**”）。

CLOUD Act主要分为两部分：一部分致力于构建跨境执法证据调取的新机制。在CLOUD Act的框架下，与美国签署政府间协议的国家将可基于调查严重犯罪的目

“阻断条款”针对的应是本应根据国际条约、协定向我国主管机关申请证据调取协助而绕过我国主管机关直接向证据所属组织、个人直接调取的场景。

的直接向美国境内的组织发出调取数据的命令。目前已与美国签署双边协议的国家有英国与澳大利亚，加快了两国访问总部位于美国的通信服务提供者所持有的电子数据的速度；另一部分则重点澄清依据《电子通信隐私法案》(the Electronic Communications Privacy Act) 出具的数据调取令可以直接访问相关数据而无论数据存储在何地，只要拥有、保管或者控制相关数据的公司实体受美国法律的管辖。但执法机构依据CLOUD Act调取数据的能力并非毫无限制，其仅能在满足以下条件的情况下调取数据：(1) 执法机构必须是出于调查犯罪的目的调取证据；(2) 执法机构已获得法院出具的搜查令；(3) 搜查令中必须就拟调取的数据进行详细说明。

同时，CLOUD Act 给通信服务提供者提供了抗辩的余地：当法案所针对的并非“美国人”且对象不在美国境内时，通信服务提供者可提出法律冲突的抗辩，由美国法院进行礼让分析。基于美国的长臂管辖条款使得与美国有最低限度联系 (minimum contacts) 的企业也落入美国法院管辖的范围，从而使得美国可“自由”访问企业存储在美国域外的数据，企业可向美国法院提出法律冲突的抗辩将是保障数据主权的有效措施之一。基于此，我国“阻断条款”应运而生。

PART 003

“阻断条款”的适用场景

从“阻断条款”的构成角度出发，“阻断条款”起首即是强调我国主管机关将根据有关法律和中华人民共和国缔结或者参加的国际条约、协定，或者按照平等互惠原则，处理外国司法或者执法机构关于提供存储于境内个人信息的请求。结合“阻断条款”的立法目的，由于司法权、行政执法权是国家权力的重要组成部分，无论是本国司法机关、行政执法机关调取存储在国外的数据，又或是外国司法机关、行政执法机关调取存储在本国的数据，均需遵循国家主权原则，通过国际法框架下的司法协助、行政执法协助进行。因此学界有观点认为，“阻断条款”主要针对前文所述一些国家绕开国际司法协助、行政执法协助，通过制定国内法案赋予本国司法机构、行政执法机

在行政审批类别下，主要典型的场景涉及国外上市、境外投资中的国家安全审查、境外并购中的反垄断申报等。

构强制调取海外数据权力的行为，通过设置前置审批的机制，阻断他国的域外管辖能力。

鉴于“阻断条款”针对的应是本应根据国际条约、协定向我国主管机关申请证据调取协助而绕过我国主管机关直接向证据所属组织、个人直接调取的场景，我们总结可能适用的场景如下：

（一）行政审批类

在行政审批类别下，主要典型的场景涉及国外上市、境外投资中的国家安全审查、境外并购中的反垄断申报等。

以国外上市为例，中国公司需向上市地的证券交易所或者监管机关提交财务以及审计资料等。以美国为例，2020年12月美国通过了《外国公司问责法案》（以下简称“**HFCAA**”），2021年12月美国证券交易委员会（以下简称“**SEC**”）宣布通过法规修正案，完善了HFCAA相关的信息披露细则。实施细则要求在美国上市的公司遵守美国上市公司会计师监督委员会（以下简称“**PCAOB**”）的审计标准，接受PCAOB的检查，并需要进一步加强信息披露，其中就包括上市公司的审计工作底稿。而工作底稿作为上市公司财务报表以及审计结论的重要支撑，可能包含涉及企业经营成果和财务状况的敏感商业信息，比如供应商清单、客户清单、成本构成、关联交易等。对于特定行业的公司，审计底稿可能还会包括更为敏感的行业信息，例如反映社会经济运行状况、供应链安全、群体健康生理状况、族群特征、遗传信息等数据。

针对PCAOB直接对上市公司审计底稿进行审查的行为，2022年4月2日证监会发布的《关于加强境内企业境外发行证券和上市相关保密和档案管理工作的规定（征求意见稿）》（以下简称“**《上市保密新规》**”）第九条明确要求为境内企业境外发行证券和上市提供相关证券服务的证券公司、证券服务机构在境内形成的工作底稿等档案应当存放在境内。涉及对国家和社会具有重要保存价值的档案或档案复制件需要出境的，需办理审批手续。同时，第十条说明证监会、财政部、国家保密局和国家档案局等有关部门将建立协作机制，对涉及保密和档案管理的有关事项进行规范和监督检查。《上市保密新规》的相关规定无

行政调查类活动中，最典型的场景涉及出口管制调查、制裁调查、反倾销反补贴调查、外国海关调查等。

疑是对“阻断条款”适用的呼应与支撑，给予了企业可有效实施抗辩的佐证。

再以国家安全审查为例，中国企业收购美国企业或资产还可能面临美国外国投资委员会（以下简称“**CFIUS**”）的国家安全审查。按照美国《外国投资与国家安全法》和《2018年外国投资风险评估现代化法案》等法律规定，外国中央或地方政府持有实质性利益的外国投资人收购美国相关TID[3]企业的实质性利益的交易，以及涉及相关TID企业的将关键技术出口、再出口、（境内）转让或再转让给某些外国公司或个人的交易，都需要向美国CFIUS进行强制性申报。申报材料主要有：包括交易性质、交易主体、交易标的、相关金融服务机构在内的交易基本信息；被收购的美国资产信息；交易标的是否涉及美国出口管制、国防产品和服务等相关信息。尽管CFIUS收集这些信息的目的是维护美国国家安全，但是中国企业对外提交的数据中一般会包括高管个人基本信息、身份信息、任职信息、住址信息，企业战略报告、管理制度、董事会决策内容、党组织作用，对企业本身业务的详细介绍，企业与政府、军队的合作与联系，企业所涉及敏感行业的情况等。此类数据涉及敏感个人信息，亦可能涉及国家秘密或重要数据，擅自对外提供有可能危害国家安全。

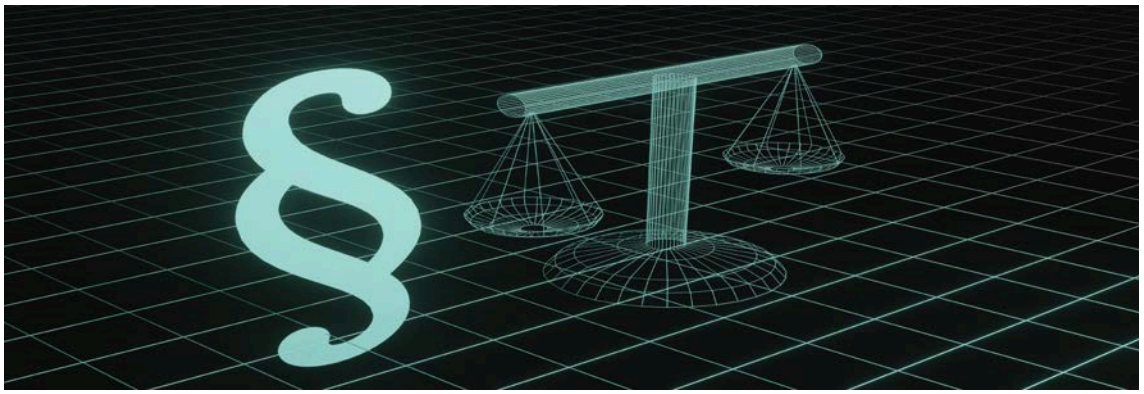
（二）行政调查类

行政调查类活动中，最典型的场景涉及出口管制调查、制裁调查、反倾销反补贴调查、外国海关调查等。

以制裁调查为例，自中美贸易争端以来，美国加强了对中国企业违反其制裁法律法规的调查活动。不少企业接到了来自美国有关部门直接或者间接的调查通知，要求对特定交易提供证据材料。由于美国制裁的领域涉及贸易、金融等各个方面，不同程度的制裁措施涵盖了朝鲜、伊朗、古巴、叙利亚、克里米亚、俄罗斯、白俄罗斯、委内瑞拉等有关国家和地区。受到调查的企业需要披露与被制裁国别、被制裁对象的特定交易，包括中外双方交易主体、交易物项、交流流程和交易渠道的详细信息。

3.TID:“关键技术”（Critical Technology）、“关键基础设施”（Critical Infrastructure）或“敏感个人数据”（Sensitive Personal Data）

仲裁程序属于商事自治行为，不涉及对司法主权的影响，因而“阻断条款”主要适用的应为外国诉讼程序。



再以UFLPA海关执法调查为例，去年12月23日，美国总统签署所谓的《强迫劳动法案》后，美国海关与边境保护局（以下简称“**CBP**”）对来自中国的部分商品签发暂扣令，暂停进口通关，限时要求美国进口商向其提供进口商品的供应链溯源信息。在此过程中，中国出口企业将需要收集、整理其在中国境内供应商的相关信息，向境外提供。需要特别说明的是，在所谓强迫劳动法案项下，CBP要求对输美商品的供应链进行极限溯源，提交的数据中包括产品BOM表、产品成本构成、供应商清单、员工个人信息、薪资水平、日常活动记录等大量敏感信息和个人信息，而中国企业未经相关主管部门批准而直接向美国海关提交涉疆信息或构成对“阻断条款”的直接违反。

（三）司法协助类

中国企业在境外参加民商事诉讼和仲裁程序必然面临对外提供证据的问题。结合前述对“阻断条款”的适用分析，仲裁程序属于商事自治行为，不涉及对司法主权的影响，因而“阻断条款”主要适用的应为外国诉讼程序。

在普通法系国家的诉讼程序中，证据开示（discovery）的范围较广，对抗的双方会尽可能的收集和使用有利于己的证据。以美国为例，根据联邦民诉规则（Federal Rules of Civil Procedure），双方当事人必须主动向对方当事人出示与请求有关的任何信息。即一方当事人利用证据开示制度可以要求对方当事人提供任何信息，除非该方所要求的信息与案件毫不相关，或对

结合民事诉讼程序的证据类型及证据递交方式，在应对外国司法、执法程序中，企业可能存在三种数据出境方式。

另一方造成过分负担，或该等信息属于保密特权信息[4]。

对外提供的证据材料从类型上主要是书证、证人证言、鉴定意见等，这些资料基本都可以通过数据电文的形式对外提供。例如涉及专利权、技术秘密的跨境诉讼中，当事人会对外提交大量证明产品特征、技术指标的书证材料和鉴定意见；再比如涉及管制产品出口的贸易跨境诉讼中，当事人有可能对外提交涉及出口管制方面的敏感信息和数据。这些都有可能详细披露我国在特定行业或领域的技术水平和管制政策。

PART 004

企业的合规指引方案

(一)司法程序中常见的数据出境方式

结合民事诉讼程序的证据类型及证据递交方式，在应对外国司法、执法程序中，企业可能存在以下的数据出境方式：

(1) 外国司法、执法机构通过远程方式直接获得证据材料

该类场景涉及的证据类型通常为证人证言、电子数据、视听资料、书证等。由于该类场景相关证据通常为数据电文形式或可通过数据电文形式进行传输（例如，通过电话、视频方式询问中国境内的证人，通过网络访问境内服务器），当事人可能存在向外国司法、执法机构提交相关证据材料的访问权限，使得外国司法、执法机构取得存储在中国境内的证据材料。

(2) 外国司法、执法机构委托中国境内的律师或机构调取证据材料

在中国民事诉讼程序中，部分省、直辖市高级法院出台了试行律师调查令制度。在律师调查令制度中，法院赋予当事人或其代理人的代理律师代表法院向相关方面调查或调取证据。在一些案件中，外国司法、执法机关可能依据当地法律委托律师或其他机构调取位于中国境内的证据材料，并用于该诉讼案件。

(3) 当事人自行向外国司法、执法机关提交位于境内的证据材料

该类场景为最为常见的场景，即当事人收集案件相关证据后向相关司法、执法

4.Federal Rules of Civil Procedure R26 (b)

针对数据出境的监管，我国采取了双因素监管路径：
特殊类型主体与特殊类型数据。

机构提交。

第一、二种场景明显存在“绕开国际司法协助、行政执法协助”的情形，2022年6月24日司法部公布了《国际民商事司法协助常见问题解答》第6、7条[5]明确指出这些场景的不合法性。对于第三种场景下如何提交证据材料的情况，司法部指出，境内证据材料的出境应当符合《民事诉讼法》《数据安全法》《个人信息保护法》的相关规定。

如上述分析，“阻断条款”虽然为境内企业应对外国司法、执法机构调取相关数据提供了一条规范路径，但其所规范的向外国司法或执法机构提供数据的行为本质仍属于数据跨境传输。这意味着虽然该行为需受“阻断条款”的规制、履行数据出境前向主管机关报批的特殊义务，其亦需受《数据安全法》第三十一条和《个人信息保护法》第三十八条的规制，履行数据出境的一般义务。下文将从数据出境的一般义务起进行介绍，探讨企业向外国司法或执法机构提供数据的合规方案。

5.http://www.moj.gov.cn/pub/sfbgw/jgsz/jgszzsdw/zsdwsfxzjlzx/sfxzjlzxxwdt/202206/t20220624_458335.html

(二)数据出境的一般机制

针对数据出境的监管，我国采取了双因素监管路径：特殊类型主体与特殊类型数据。针对特殊类型主体，《网络安全法》第三十七条规定，“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。”该条确立了关键信息基础设施运营者（以下简称“**CIIO**”）数据本地化、出境需安全评估的基本制度。

除CIIO以外，《数据出境安全评估办法》（以下简称“**《办法》**”）第四条同时规定，达到以下个人信息处理量级的数据处理者也需向国家网信部门申报数据出境安全评估：处理100万人以上个人信息的数据处理者；自上年1月1日起累计向境外提供10万人个人信息的数据处理者；以及自上年1月1日起累计向境外提供1万人敏感个人信息的数据处理者。

除确立了上述特殊类型主体数据出境需履行安全评估义务外，针对不同类型

不论数据处理者采取何种数据跨境传输合规路径，均应遵守《办法》第五条的要求，在向境外提供数据前事先开展数据出境风险自评估。

的数据[6]，我国确立了以下数据出境合规机制：

针对“重要数据[7]”，《办法》第四条规定，数据处理者向境外提供前需申报数据出境安全评估。

针对个人信息，《个人信息保护法》第三章设置了专门的规则。根据《个保法》第三十八条的要求，结合国家部门近期公开征求意见的《个人信息出境标准合同规定（征求意见稿）》相关规定，非上述特殊类型的数据处理者，可通过经专业机构进行个人信息保护认证或按照标准合同与境外接收方订立合同等两种方式进行个人信息合规跨境传输。

值得注意的是，不论数据处理者采取何种数据跨境传输合规路径，均应遵守《办法》第五条的要求，在向境外提供数据前事先开展数据出境风险自评估。自评估要点如下图：

企业风险自评估要点

- ✔ 数据出境和境外接收方处理数据的目的、范围、方式等的合法性、正当性、必要性
- ✔ 出境数据的规模、范围、种类、敏感程度，数据出境可能对国家安全、公共利益、个人或者组织合法权益带来的风险
- ✔ 境外接收方承诺承担的责任义务，以及履行责任义务的管理和技术措施、能力等能否保障出境数所的安全
- ✔ 数据出境中和出境后遭到篡改、破坏、汇露、丢失、转移或者被非法获取、非法利用等的风险，个人信息权益维护的渠道是否通畅等
- ✔ 与境外接收方拟订立的数据出境相关合同或者其他具有法律效力的文件等是否充分约定了数据安全保护责任义务
- ✔ 其他可能影响数据出境安全的事项

图 数据出境风险自评估

(三)数据出境的特殊机制：报请主管部门审批

除需履行上述数据出境的一般合规义务外，企业向外国司法或执法机构提供数据前还需按照“阻断条款”的规定，履行向主管部门报请审批的义务。

以应对外国司法程序为例，司法部在《国际民商事司法协助常见问题解答》第9条明确指出，在国际司法协助场景中，境内

6.本文仅针对一般情况下的重要数据及个人信息出境情况，金融、地图、基因等特殊领域的数据出境时需履行特殊行政审批的问题不在此列。
7.《数据出境安全评估办法》第十九条 本办法所称重要数据，是指一旦遭到篡改、破坏、泄露或者非法获取、非法利用等，可能危害国家安全、经济运行、社会稳定、公共健康和安全等的数据。

组织、个人在获得我国主管机关批准前不得向外国司法或者执法机构提供存储于中国境内的数据或个人信息。根据《关于从国外调取民事或商事证据的公约》，“国际司法协助”是指“缔约国的司法机关可以根据该国的法律规定，通过请求书的方式，请求另一缔约国主管机关调取证据或履行某些其他司法行为。”而“主管机关”，根据《全国人民代表大会常务委员会关于我国加入<关于从国外调取民事或商事证据的公约>的决定》以及《最高人民法院关于依据国际公约和双边司法协助条约办理民商事案件司法文书送达和调查取证司法协助请求的规定》，司法部为负责接收来自另一缔约国司法机关请求书的中央机关，最高人民法院为负责审核与执行司法协助的主管机关，各级有权人民法院为具体执行司法协助的部门。

鉴于上述，结合国际民商事司法协助的流程，企业在向外国司法机构提供数据前，应遵循以下流程：

（1）要求外国司法机构通过请求书的方式，向我国司法部司法协助中心发起协助申请；

（2）若外国司法机构拒绝上述申请流程的，企业应向外国司法机构提出适用“阻断条款”的抗辩，并自行履行向司法部司法协助中心申请审批的义务；

（3）企业向司法部司法协助中心递交如下材料，等待最高人民法院的批示：

- 证据出境申请书，说明案件基本情况（如案由、具体外国法院等）；
- 外国法院关于证据调取的命令；
- 拟出境的具体证据清单；
- 关于拟出境证据的律师评估报告，报告内容涵盖拟出境证据与案件的关联性、出境可能产生的安全影响以及是否应当出境的评估结论等。

(四)企业合规方案小结

结合“（二）数据出境的一般机制”中所述的合规措施，我们总结企业在面对外国执法机构或司法机构强制调取数据时的合规方案如下，供企业面临相关场景时参考：

（1）识别数据传输主体：识别拟证据出境的主体身份，是否属于特殊类型主体（CIIO或个人信息处理量级达到网信办规

我们总结企业在面对外国执法机构或司法机构强制调取数据时的合规方案，供企业面临相关场景时参考。

定的门槛的数据处理者）；

（2）识别证据所属数据类别：识别拟出境证据的数据类别，是否含有重要数据或个人信息；

（3）进行数据出境风险自评估：评估证据出境可能产生的安全影响，并形成评估报告；

（4）根据自评估报告判断是否需要向国家网信部门申报数据出境安全评估；

（5）准备拟递交的材料（含申请书、自评估报告、外国执法机构或司法机构关于证据调取的命令、证据清单等），并向主管部门申请审批。

陈际红
合伙人
知识产权部
北京办公室
+86 10 5957 2003
chenjihong@zhonglun.com

当数据合规遇见刑事追诉——首例数据合规不起诉案件所带来的分析和启示

蔡鹏 葛燕 胡云浪

本文对国内首例数据合规不起诉案件进行分析，探讨数据合规如何能够帮助企业避免刑事责任，并分享企业如何建立完备的数据合规体系。

PART 001

近期一件数据合规不起诉案件要点回顾

1.案件基本情况

2022年5月，上海普陀区检察院公布了全国首例数据合规不起诉案。在该案中，Z网络科技有限公司（以下简称“**Z公司**”）向普陀区检察院提出了合规不起诉申请，普陀区检察院审查后向Z公司制发了合规检察建议，并启动范式合规审查。Z公司在整改期间积极开展数据合规整改工作，最终在普陀区检察院举行的公开审查听证中，参与听证的各方均认为Z公司数据合规整改到位，并一致同意对Z公司及人员作出不起诉决定。

案件基本情况概览

项目	具体内容
涉嫌犯罪事实	2019年至2020年，Z公司在未经授权许可的情况下，为运营需要，由公司首席技术官陈某某指使多名技术人员，通过数据爬虫技术，非法获某外卖平台数据，造成某外卖平台直接经济损失4万余元。
涉案企业、个人	Z公司、首席技术官陈某某及其所指使的多名技术人员
涉案罪名	非法获取计算机信息系统数据罪
适用法律	《中华人民共和国刑法》第285条
案件情节	企业认罪认罚、积极赔偿并取得被害单位谅解
案件处理（合规不起诉）	(1)**提出申请**：Z公司提出合规不起诉申请，普陀区检察院根据Z公司的申请向其制发合规检察建议，并启动范式合规审查。 (2)**整改建议**：普陀区检察院根据Z公司经营现状，从**数据合规管理、数据风险识别、评估与处理、数据合规运行与保障**等方面提出整改建议。 (3)**积极整改**：Z公司收到整改建议后积极整改，并引入外部法律顾问协助整改。 (4)**听证**：整改期结束后，经过听证评议，**各参与听证方认为Z公司数据合规整改到位**，一致同意**对涉案单位及人员作出不起诉决定**。

2.案件涉及的合规流程

合规不起诉流程要点

序号	合规不起诉流程	具体要点
1	Z公司申请合规不起诉	(1)**前提**:Z公司犯罪情节较轻,主观恶性较小,认罪认罚、积极赔偿损失并取得被害单位谅解。 (2)**申请**:Z公司向检察机关申请适用合规整改。
2	检察机关对Z公司制发检察建议	(1)**了解Z公司经营情况**:普陀区检察院实地走访Z公司查看经营现状、会同监管部门研商Z公司运营情况; (2)**提出整改建议**:普陀区检察院从数据合规管理、数据风险识别、评估与处理、数据合规运行与保障等方面提出整改建议,指导Z公司作出合规承诺; (3)**具体的整改意见包括**: ①**构建数据合规管理体系**:设置专门的数据合规管理部门,特别针对数据来源合法性,制定并不断完善数据合规计划,消除内部管理盲区。 ②**提高数据合规风险识别、应对能力**:规范技术汇报审批流程,建立技术应用合规评估制度,避免技术滥用。 ③**稳健数据合规运行**:建立数据合规咨询机制与数据不合规发现机制,建立数据分级分类管理制度及员工数据安全管理制度,填补制度空白。
3	Z公司进行合规整改工作	(1)**整改**:Z公司做出合规承诺,并围绕管理、技术、制度进行自查整改; (2)**聘请外部法律顾问**:Z公司还聘请法律顾问团队制定数据合规整改计划,严格按照合规承诺扎实推进。

序号	合规不起诉流程	具体要点
4	引入第三方组织进行监督考察	(1)**第三方组织成员**:国家互联网信息办公室、某知名互联网安全企业、产业促进社会组织等专家成员; (2)**全程监督**:通过询问谈话、审查资料、召开培训等形式全程监督Z公司数据合规整改工作; (3)**评定整改合格**:考察期满后,第三方组织评定Z公司合规整改合格。
5	检察机关举行不起诉公开听证	(1)**听证参与人**:听证员、侦查人员、企业合规第三方考察员和被害单位等参与不起诉公开听证,四名全国人大代表受邀旁听; (2)**听证内容**:围绕合规评估合格、社会危害性和是否可作不起诉处理进行公开听证。
6	检察机关作出不起诉决定	(1)**听证会意见**:参与听证各方认为Z公司数据合规整改到位一致同意对涉案单位及人员作出不起诉决定; (2)**不起诉决定**:人民检察院根据听证结果作出不起诉决定。

PART 002

涉数据类犯罪案件适用合规不起诉分析

1.检察机关推进三阶段简要回顾

2020年,最高人民检察院对我国企业刑事合规不起诉制度的探索拉开帷幕,同年3月,最高检启动涉案违法犯罪依法不捕、不诉、不判处实刑的企业合规监管试点工作,并确定上海市浦东新区、金山区检察院,广东省深圳市南山区、宝安区检察院,江苏省张家港市检察院,山东省郯城县检察院等6个检察院为试点单位。此次试点在我国刑事司法领域初步确立了合规不起诉的概念。

2021年3月,最高检发布《关于开展企业合规改革试点工作方案》(以下简称"**《试点工作方案》**"),企业合规试点范围进一步扩大至北京、上海、浙江等10个省份的27个市级检察院、165个基层检察院。同年6月3日,最高检联合多部委共同发布《关于建立涉案企业合规第三方监督评估机制的指导

我国《刑法》设立了多项与数据安全密切相关的罪名，
从法益侵害角度，这些罪名大致可分为三大类。

意见（试行）》（以下简称“**《指导意见》**”），明确“涉案企业合规第三方监督评估机制是指人民检察院在办理涉企犯罪案件时，对符合企业合规改革试点适用条件的，交由第三方监督评估机制管理委员会选任组成的第三方监督评估组织，对涉案企业的合规承诺进行调查、评估、监督和考察，考察结果作为人民检察院依法处理案件的重要参考”。

2022年4月19日全国工商联、最高检等九部委发布《涉案企业合规建设、评估和审查办法（试行）》，明确企业合规的本质内涵是改造企业治理结构和重塑企业文化。

2.涉数据类犯罪外延

我国《刑法》设立了多项与数据安全密切相关的罪名，从法益侵害角度，这些罪名大致可分为三大类：一是**危害计算机信息系统安全**的犯罪。包括非法侵入计算机信息系统罪和破坏计算机信息系统罪这两大类犯罪，具体包括非法侵入计算机信息系统罪、非法获取计算机信息系统数据、非法控制计算机信息系统罪、提供侵入、非法控制计算机信息系统程序、工具罪、破坏计算机信息系统罪等五项罪名；二是**侵害具体数据类型安全**的犯罪。**具体**包括侵犯公民信息安全和侵犯商业秘密两大类犯罪，具体包括侵犯公民个人信息罪、侵犯商业秘密罪两项罪名；三是**围绕信息网络**相关罪名。具体包括拒不履行信息网络安全管理义务罪、非法利用信息网络罪以及帮助信息网络犯罪活动罪。

对于公司来说，司法实践中应当关注的罪名当属非法侵入计算机信息系统罪、非法获取计算机信息系统数据、非法控制计算机信息系统罪、侵犯公民个人信息罪、侵犯商业秘密罪、拒不履行信息网络安全管理义务罪以及帮助信息网络犯罪活动罪。

3.涉数据类犯罪特点

我国《刑法》第285条确立了非法侵入计算机信息系统罪、非法获取计算机信息系统数据、非法控制计算机信息系统罪这一类犯罪。

罪名	行为
非法侵入计算机信息系统罪（第285条第一款）	指自然人或者单位违反国家规定，侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统的行为。
非法获取计算机信息系统数据、非法控制计算机信息系统罪（第285条第二款）	指违法国家规定侵入国家事务、国防建设、尖端科学技术领域的计算机系统以外的计算机信息系统或者采用其他技术手段，获取该计算机信息系统中存储、处理或者传输的数据，或者对该计算机信息系统实施非法控制、情节严重的行为。
侵犯公民个人信息罪（第253条之一）	指违反国家有关规定，存在“向他人出售或者提供公民个人信息”，或者“窃取或者以其他方法非法获取公民信息”的行为，达到情节严重的程度。
拒不履行信息网络安全管理义务罪（第286条）	指网络服务者不履行法律、行政法规规定的信息网络安全管理义务，经监管部门责令采取改正措施而拒不改正，致使违法信息大量传播的；或致使用户信息泄露，造成严重后果的；或者致使刑事案件证据灭失，情节严重的；或者具有其他严重情节严重的行为。
侵犯商业秘密罪（第219条）	指以盗窃、贿赂、欺诈、胁迫、电子侵入或者其他不正当手段获取权利人的商业秘密；披露、使用或者允许他人使用以前项手段获取的权利人的商业秘密的；违反保密义务或者违反权利人有关保守商业秘密的要求，披露、使用或者允许他人使用其所掌握的商业秘密。
帮助信息网络犯罪活动罪（第287条之二）	指明知他人利用信息网络实施犯罪，为其犯罪提供互联网接入、服务器托管、网络存储、通讯传输等技术支持，或者提供广告推广、支付结算等帮助的行为。

我国《刑法》第285条确立了**非法侵入计算机信息系统罪、非法获取计算机信息系统数据、非法控制计算机信息系统罪**这一类犯罪。非法侵入计算机信息系统罪（第285条第一款）指自然人或者单位违反国家规定，侵入国家事务、国防建设、尖端科学

我国《刑法》第253条之一确立了侵犯公民个人信息罪。

技术领域的计算机信息系统的行为。主观方面，本罪的成立需要满足故意要件，如果是无意中进入计算机信息系统，但经警示仍不退出的，应当视为故意非法侵入。非法获取计算机信息系统数据、非法控制计算机信息系统罪（第285条第二款）为《刑法修正案（七）》规定的新罪，客观方面指违法国家规定侵入国家事务、国防建设、尖端科学技术领域的计算机系统以外（即第285条第一款规定以外）的计算机信息系统或者采用其他技术手段，获取该计算机信息系统中存储、处理或者传输的数据，或者对该计算机信息系统实施非法控制、情节严重的行为，本罪属于选择性罪名。近日公布的首例数据合规不起诉案中的Z公司的客观行为就表现为利用“爬虫”非法获取其他计算机信息系统中存储、处理或者传输的数据，若其未进行合规整改，则将以此类罪名被追诉。

我国《刑法》第253条之一确立了**侵犯公民个人信息罪**。根据最高法和最高检的司法解释，该罪的违法性组成有：一是违反国家有关规定，二是存在“向他人出售或者提供公民个人信息”，或者“窃取或者以其他方法非法获取公民信息”的行为；三是行为达到情节严重的程度。其中，“两高”司法解释对作为入罪标准的情节严重做出了规定，个人或者单位侵犯公民个人信息，只需要数量或者情节上达到一般标准，例如：非法获取、出售、提供“**重大敏感信息**[1]”50条以上的；非法获取、出售、提供“**一般敏感信息**[2]”500条以上的；非法获取、出售或者提供行踪轨迹信息，被他人用于犯罪的；等等。随着互联网的发展，大数据企业、电子商务企业等都依托网络平台，其业务开展不可避免需要收集大量公民个人信息和数据，2021年，全国公安机关深入推进“净网2021”专项行动，针对人民群众关注的个人信息保护问题，全力组织开展侦查打击工作，共破获侵犯公民个人信息案件9800余起，抓获犯罪嫌疑人1.7万余名，维护了网络空间秩序和人民群众合法权益。2022年1月，公安部公布了侵犯公民个人信息犯罪十大典型案例[3]，其中，典型案例六为公司非法获取个人信息案例，该案例中山东某网

1.重大敏感信息包括：行踪轨迹信息、通信信息、征信信息、财产信息。
2.一般敏感信息包括：住宿信息、通信记录、健康生理信息、交易信息等可能影响人身、财产安全的公民个人信息。
3.打击侵犯公民个人信息犯罪这一年：公安部公布十大典型案例，最后访问时间：2022年6月5日，https://app.mps.gov.cn/gdnps/pc/content.jsp?id=8314457

拒不履行信息网络安全管理义务罪为真正不作为犯，本罪的成立，要求经过监管部门责令采取改正措施而拒不改正。

络科技公司从网上购买公民信息，在辽宁阜新石某团伙的技术支撑下，突破游戏公司验证机制，非法注册实名网络游戏账号1.8万余个，向未成年人出售，非法牟利170余万元。

我国《刑法》第286条确立了**拒不履行信息网络安全管理义务罪**。本罪是指网络服务者不履行法律、行政法规规定的信息网络安全管理义务，经监管部门责令采取改正措施而拒不改正，致使违法信息大量传播的；或致使用户信息泄露，造成严重后果的；或者致使刑事案件证据灭失，情节严重的；或者具有其他严重情节严重的行为。**此罪为真正不作为犯，本罪的成立，要求经过监管部门责令采取改正措施而拒不改正。**2021年4月昆明市盘龙区人民法院判处了全国首例“因运营商拒不履行信息网络安全管理义务”案例，某虚拟运营商xx通信技术有限公司，因拒不履行信息网络安全管理义务，董事长及部分高管被一审判处一年四个月至一年十个月的有期徒刑或拘役。法院认为：虚拟运营商xx通信技术有限公司明知山东某通信代理公司在从事违法行为而拒不履行其网络管理责任者的义务，涉嫌拒不履行信息网络安全管理义务罪被法院依法判决。

我国《刑法》第219条确立了**侵犯商业秘密罪**，《刑法修正案（十一）》对其进行了部分修改。侵犯商业秘密罪的犯罪主体是一般主体，既可以是自然人，也可以是公司、企业等单位。在实务中，触犯该罪的多为企业的中高级管理人员、进行技术研发的核心骨干或者是因合作关系而知悉企业商业秘密的交易第三方。在主观方面，侵犯商业秘密罪需满足故意。在客观方面，侵犯商业秘密罪需要从行为对象、行为方式以及行为结果三方面进行判别：1）侵犯商业秘密罪的行为对象是商业秘密，商业秘密是企业的无形资产，能使企业在激烈的竞争环境中取得竞争优势，商业秘密一旦泄漏，将给企业带来不可估量的损失；2）侵犯商业秘密法定的行为方式包括：以盗窃、贿赂、欺诈、胁迫、电子侵入或者其他不正当手段获取权利人的商业秘密；披露、使用或者允许他人使用以前项手段获取的权利人的商业秘密的；违反保密义务或者违反权利人有关保守商业秘密的要求，披露、使用或者允许他人使用其所掌握的商业秘密；

若案件进入检察院合规审查阶段，那么首先要做的是判断涉数据类犯罪案件是否符合第三方机制的适用条件。

3）成立侵犯商业秘密罪，要求侵犯商业秘密行为给权利人造成了重大损失以上的结果，目前侵犯商业秘密的重大损失数额标准为三十万元[4]。实践中，若企业利用员工跳槽带来的其他企业的机密数据，或者利用其他企业尚未公开的技术相关数据进行业务拓展、新品开发等，则可能面临数据合规风险，甚至构成侵犯商业秘密罪。

我国《刑法》第287条之二确立了**帮助信息网络犯罪活动罪**，本罪是指明知他人利用信息网络实施犯罪，为其犯罪提供互联网接入、服务器托管、网络存储、通讯传输等技术支持，或者提供广告推广、支付结算等帮助的行为。主观方面体现为明知，根据司法实践，目前此罪名客观行为主要表现为两个方面，其一是通过手机卡、银行卡向犯罪行为人提供结算功能，帮助实施信息网络犯罪的人犯罪的行为；其二是**针对提供互联网技术服务从而帮助犯罪行为人实施信息网络犯罪**的行为。根据最高检公布的2021年全国检察机关主要办案数据，2021年，起诉帮助信息网络犯罪活动罪近13万人，同比上升超8倍，位居各类刑事犯罪的第3位；根据最高检公布的2022年1月至3月全国检察机关主要办案数据，帮助信息网络犯罪活动罪仍处高位，上述办案数据引起很多互联网企业高度关注。因此，在日前检察机关正高度关注此罪的大背景下，若互联网企业、大数据企业明知他人利用网络平台实施犯罪仍提供互联网技术服务的，也可能面临数据合规风险，甚至构成帮助信息网络犯罪活动罪。

4.合规不起诉适用于涉数据类犯罪案件的可行性论证

若案件进入检察院合规审查阶段，那么首先要做的是判断涉数据类犯罪案件是否符合第三方机制的适用条件，具体而言：

《指导意见》中明确规定企业合规不起诉适用于经济犯罪和职务犯罪案件。经济犯罪指的是在商品经济的运行领域中，为谋取不法利益，违反国家法律规定，严重侵犯国家管理制度和破坏社会经济秩序，依照刑法应受刑罚处罚的行为。[5]参上文所述，数据合规视阈下企业在生产经营过程中若

4.《最高人民法院、最高人民检察院关于办理侵犯知识产权刑事案件具体应用法律若干问题的解释（三）》第四条。
5.高铭暄,王作富.中国惩治经济犯罪全书(Z).北京:中国政法大学出版社,1995

涉嫌侵犯商业秘密罪，则亦在经济犯罪规制范畴之内；同时，在“互联网+”的技术驱动下，经济犯罪也正在大规模地向网络空间转移，并衍生出一种全新的犯罪形态——**“网络经济犯罪”**，而数据合规领域涉及的非法侵入计算机信息系统罪、非法获取计算机信息系统数据、非法控制计算机信息系统罪、侵犯公民个人信息罪、拒不履行信息网络安全管理义务罪等恰为“经济犯罪”所包含。基于以上，涉数据类犯罪案件属于企业合规不起诉的适用对象。

根据最高检下发的《试点工作方案》、《指导意见》以及当前试点地区的司法实践来看，试点地区的检察机关基本上将合规考察制度的适用对象设定为“相关责任人”可能被判处3年有期徒刑以下刑罚的涉企刑事案件，也有部分检察院将重罪纳入合规不起诉的适用范围，如辽宁省人民检察院出台的《关于建立涉罪企业合规考察制度的意见》，规定“直接负责的主管人员和其他直接责任人员依法应当被判处三年以上十年以下有期徒刑的，具有自首情节或者在共同犯罪中系从犯，或者直接负责的主管人员、其他直接责任人员具有立功表现的，可以适用合规考察制度”。参上文所述，**涉数据类犯罪主要涉及罪名中，非法侵入计算机信息系统罪、拒不履行信息网络安全管理义务罪、帮助信息网络犯罪活动罪法定最高刑为3年、非法获取计算机信息系统数据、非法控制计算机信息系统罪、侵犯商业秘密罪、侵犯公民个人信息罪情节严重的法定最高刑为3年，符合合规不起诉适用刑罚范围规定。**

5.涉案企业启动该程序的相关流程

涉案企业启动该程序的相关流程分为五个阶段。

第一阶段：启动程序	
检察院对企业进行合规审查	(1) 依职权审查：人民检察院在办理涉企犯罪案件时，应当注意审查是否符合企业合规试点以及第三方机制的适用条件，并及时征询涉案企业、个人的意见； (2) 依申请审查：涉案企业、个人及其辩护人、诉讼代理人或者其他相关单位、人员提出适用企业合规试点以及第三方机制申请的，人民检察院应当依法受理并进行审查。
签署认罪认罚具结书和合规承诺书	实践中一般以涉罪企业及其人员在值班律师或辩护律师在场的情况下，签署认罪认罚具结书和合规承诺书为前提。
启动第三方监督评估机制	《指导意见》中明确规定要建立涉案企业合规第三方监督评估机制，人民检察院在办理涉企犯罪案件时，对符合企业合规改革试点适用条件的，交由第三方监督评估机制管理委员会选任组成的第三方监督评估组织（第三方组织），对涉案企业的合规承诺进行调查、评估、监督和考察，考察结果作为人民检察院依法处理案件的重要参考。
第二阶段：合规计划制定与评价	
制定合规计划	涉案企业（可委托的刑事辩护律师或专项合规律师辅助）应当根据第三方组织的要求而提交专项或者多项合规计划。
第三方组织评价合规计划	(1) 第三方组织对涉案企业合规计划的可行性、有效性与全面性进行审查，提出修改完善的意见建议； (2) 根据案件具体情况和涉案企业承诺履行的期限，确定合规考察期限（有试点单位将涉罪企业的合规考察期定为3个月至5个月，也有定为6个月至1年甚至更长）。
第三阶段：合规计划执行	
合规计划执行	(1) 涉案企业应当按照合规计划进行合规整改，定期或者不定期接受第三方组织对合规计划履行情况的检查和评估； (2) 如第三方组织有要求，涉案企业需定期书面报告合规计划的执行情况，同时抄送负责办理案件的人民检察院。

数据合规之于企业的意义，除了通过“数据合规不起诉”帮助涉刑企业完成经营模式整改，将企业从犯罪的边缘重新拉回发展正轨外，更核心的价值在于帮助企业防范于未然。

第四阶段：全面评估考核	
全面评估考核	在合规考察期届满后，第三方组织对涉案企业的合规计划完成情况进行全面检查、评估和考核，并制作合规考察书面报告，报送负责选任第三方组织的第三方机制管委会和负责办理案件的人民检察院。
第五阶段：检察院处理	
听证程序（非必需）	人民检察院对于拟作不批准逮捕、不起诉、变更强制措施等决定的涉企犯罪案件，可以根据《人民检察院审查案件听证工作规定》召开听证会，并邀请第三方组织组成人员到会发表意见。
检察院作出决定	人民检察院结合第三方组织合规考察书面报告、涉案企业合规计划、定期书面报告等合规材料作出批准或者不批准逮捕、起诉或者不起诉以及是否变更强制措施等决定，必要时提出检察建议或检察意见。

PART 003

数据合规为什么能够帮助企业避免刑事责任？

数据合规之于企业的意义，除了通过“数据合规不起诉”帮助涉刑企业完成经营模式整改，将企业从犯罪的边缘重新拉回发展正轨外，更核心的价值在于帮助企业防范于未然：通过评估合规边界、给出贴合企业发展阶段与商业模式的合规解决方案，助力企业将原本刑事责任红线以下的风险，转变为新的商业机会。纵观当前的司法环境，同时立足刑事责任的特性，我们将从以下几个角度分析企业为什么要开展数据合规工作，以及将数据合规工作贯穿企业发展全生命周期的实际意义。

1.刑事责任是企业数据业务面临的终极风险

不同于民事责任或行政责任，刑事责任是指国家依据刑法通过一系列最为严厉

目前我国针对数据类犯罪的判定已逐渐明朗。

的强制措施，对罪犯施以惩戒，使其接受改造的法律责任承担形式，是企业数据业务可能面临的终极风险。我国刑法针对单位犯罪采取双罚制，即单位犯罪的，对单位判处罚金，同时对直接负责的主管人员和其他直接责任人员判处刑罚。被刑事追责的企业的商誉往往会因此遭受重创，难再获得市场行信任，而从此一蹶不振。目前我国针对数据类犯罪的判定已逐渐明朗，主要涉及以下罪名：

刑事罪名
侵犯公民个人信息罪
非法侵入计算机信息系统罪
非法获取计算机信息系统数据、非法控制计算机信息系统罪
提供侵入、非法控制计算机信息系统程序、工具罪
破坏计算机信息系统罪
拒不履行信息网络安全管理义务罪
非法利用信息网络罪
帮助信息网络犯罪活动罪
掩饰、隐瞒犯罪所得罪
非法获取国家秘密罪，为境外窃取、刺探、收买、非法提供国家秘密罪，故意（过失）泄露国家秘密罪，非法获取军事秘密罪，为境外窃取、刺探、收买、非法提供军事秘密罪，故意（过失）泄露军事秘密罪等
侵犯商业秘密；为境外窃取、刺探、收买、非法提供商业秘密罪

近年来，我国数据类的罪名在数量上呈现上升趋势，
在适用范围上亦呈现扩张趋势。

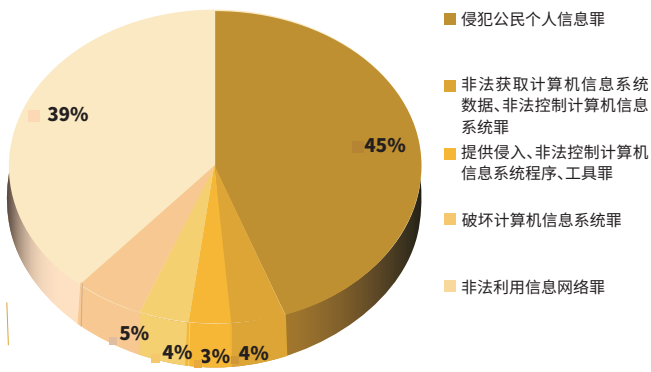
例如（2019）粤0305刑初193号一案中，深圳市某互联科技有限公司的技术总监以及核心技术人员因使用爬虫技术导致深圳市住房系统瘫痪，构成“破坏计算机信息系统罪”。由于核心人员被定罪，该公司如今难以继续展开正常经营，其各项协议先后无法继续履行，法定代表人亦被列入失信名单。

2.数据类罪名增加，刑事案件呈上升趋势

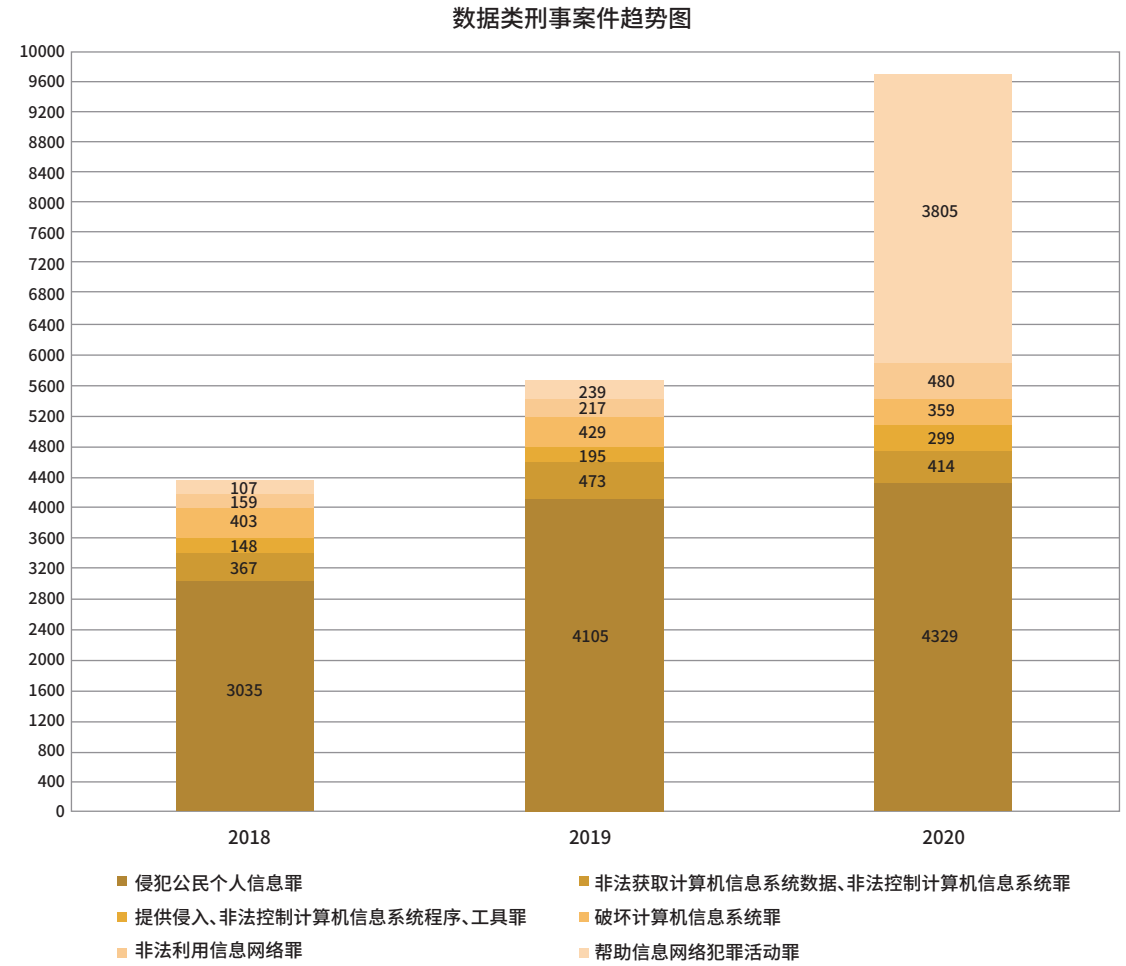
近年来，我国数据类的罪名在数量上呈现上升趋势，在适用范围上亦呈现扩张趋势。例如，《刑法修正案（七）》在《刑法》253条之一增加规定了出售、非法提供公民个人信息罪和非法窃取公民个人信息罪。而随后的《刑法修正案（九）》则将《刑法》253条中出售、非法提供公民个人信息罪和非法获取公民个人信息罪的犯罪主体由原来的特定主体（国家机关或者金融、电信、交通、教育、医疗等单位及其工作人员）改为不特定主体，所有违反本罪的单位与个人皆可被追责。

互联网模式的快速更新和技术迭代，导致网络犯罪呈现复杂化与多元化的趋势。未来可预计的是，随着法律的逐渐落地，实践中各种涉及数据有关的新的犯罪形式将会涌现，国家将在针对数据违法罪名设计上更为专门化、精细化，相关的刑事执法活动也将呈现更加活跃的态势。

图：2020年数据类刑事案件趋势图



该案件代表性地反映出了一类企业在发展过程中长期忽视数据合规而可能产生的后果。



3.监管日趋严格，行为违法界限不清晰

当今互联网行业的营商环境已非“劣币驱逐良币”，而将“技术中立”等同于合法使用的理念也已在日趋严格的监管下多次被证伪。忽视数据合规边界而试错，企业付出的代价可能是被刑事追责。在首例数据合规不起诉案中，正是因为缺乏合规意识，盲目使用爬虫技术抓取第三方平台致使该平台直接经济损失4万多元，Z公司从手握10余项计算机软件著作权，有着光明发展前景的“高新技术企业”最终成为罪犯。技术的发展与企业壮大并不等同于法律意识

企业应当尽早通过合规识别从源头上防范终极刑事风险，
避免刑事“入罪”，免遭刑法的巨大威慑。

的增强，该案件代表性地反映出了一类企业在发展过程中长期忽视数据合规而可能产生的后果。

另外，当前针对数据类犯罪的行为在违法认定上也并非清晰。刑法所规制的是被社会所谴责的，对法益具有严重侵害的犯罪行为。而在一些已知披露的案例中，拨去复杂的技术问题，从造成损害的结果上看，似乎并未有较为严重的法益侵害。因此这些案件是否应当被定性为刑事意义上的、可被谴责的社会危害行为，也在业内形成了诸多讨论。

可以看出，数据类案件往往由于存在较强的技术属性，在定罪和量刑方面会有较多的考虑因素。当下日益凸显的矛盾和难点在于：如何在数据安全和个人隐私日益增强的监管要求下，穿透复杂的技术问题，从而精确的识别犯罪和准确的量刑。

4. 刑法威力极大，存在“溢出效应”

我国刑法对单位犯罪采取双罚制，即对单位判处罚金的同时，还对其直接责任人包括高管以及技术人员等实施限制人身自由刑罚措施。在实践中，因利用职业便利实施犯罪，或者实施违背职业要求的特定义务的犯罪被判处刑罚的，法院可以在刑罚终止后，禁止其从事相关职业。而在刑事案件追诉过程中，侦查机关有权对涉案的财物采取查封冻结等强制措施。前述种种，无不说明刑法本身威力巨大，对罪犯的社会关系形成了“灭顶之灾”。

尽管事后的刑事合规从“出罪”的角度为企业指明了一条救赎路径，但企业还应当尽早通过合规识别从源头上防范终极刑事风险，避免刑事“入罪”，免遭刑法的巨大威慑。

5.数据合规在刑事危机中不同阶段的意义

5.1.事前合规，将危机化为无形

探索新的商业模式往往伴随着未知的风险，故企业至少应当以刑事责任为红线，尽早引入专业人士开展合规评估。例如在首例数据合规不起诉案中，Z公司虽然看到数据抓取本身技术中立且未被禁止，却忽视了就企业应用数据抓取的商业模式进行合规评估的必要性。若Z公司尽早引入专业人士对爬虫技术使用场景进行调查与合规分析，并让Z公司及时知悉利用技术手段绕

在发展过程中，企业应当定期梳理数据资产，同时针对高风险数据处理活动开展专项数据合规专项的评估与整改。

过第三方平台的身份验证系统、访问频率限制，情节严重的则可能会构成非法获取计算机信息系统数据罪，那么企业及其创始人早已将相关风险消融于萌芽阶段。

另外，企业通过非法安装SDK、绕过用户授权默认安装APK的方式向用户手机装载程序非法获取商业利益的，则可能构成非法控制计算机信息系统罪。其他涉及以未授权的方式收集、获取、出售用户个人信息，或通过植入木马、伪装系统等的行为，皆有可能落入刑事责任。而上述行为如何界定罪与非罪的边界，则需要借助法律、技术、安全方面的专业人士，通过详尽的合规评估，才能识别其中的巨大风险。

因此，技术型企业，尤其是处理大量数据的企业，当数据来源或处理方式存在不确定性时，应当尽早引入合规评估，从根源上排查合规风险，避免落入刑事追责的窘境，化危机为无形。

5.2.事中合规-转危为机

在发展过程中，企业应当定期梳理数据资产，同时针对高风险数据处理活动开展专项数据合规专项的评估与整改。只有这样，在日趋严格的国内监管环境以及日趋激烈的以数据为核心的国际竞争大背景下，企业才能具备足够的适应性，领先竞争对手，并将危机转化为机遇。正如业内讨论较多的某食品公司员工侵犯公民个人信息一案中，企业通过在经营中坚持不懈的合规工作，在工作中全流程落地了合规措施并进行专项整改。相关合规成果在刑事追诉的关键时刻起到了积极显著的作用，帮助企业妥善处理了相关风险，不仅为企业发展保驾护航，同时也为企业赢得了赞誉。

5.3.事后合规-最后的救济

当然，若企业在事前、事中环节因合规重视不足而落入刑事追诉的，在现有机制下，还可以通过积极的措施进行补救，通过取得受害人的谅解，与检察院以及第三方机构通力合作，开展数据合规工作，完成指定整改并取得各方谅解而“出罪”。

我们认为，尽管有事后的救济手段，但是在整体合规流程中，事后合规已经是“最后一根稻草”。是否能抓住，取决于行为本身的性质以及社会危害程度等各方面因素，具有一定的“偶然性”。如何把这种“偶然性”转化成不被追诉的“必然性”，还是需要企业紧紧守住合规义务，将合规工作前置。

企业开展数据合规工作是企业履行其法定义务的表现。

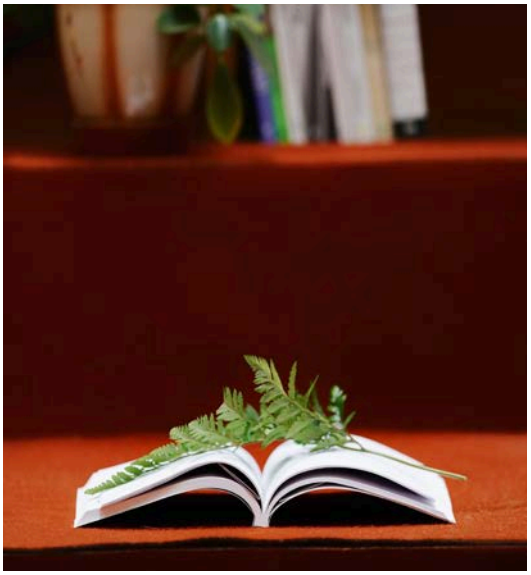
PART 004

企业如何建立数据合规体系

1.建立数据合规体系是法律的要求

我国《个人信息保护法》《数据安全法》等上位法中，明确提出了企业应当建立数据合规体系。例如，《个人信息保护法》第五十一条要求企业："……采取下列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：(一)制定内部管理制度和操作规程……"；《个人信息保护法》第五十八条要求："提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者，应当履行下列义务：(一)按照国家规定建立健全个人信息保护合规制度体系，成立主要由外部成员组成的独立机构对个人信息保护情况进行监督……"；

《数据安全法》要求企业开展数据处理活动的，"……应当依照法律、法规的规定，建立健全全流程数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，保障数据安全。"



因此，企业开展数据合规工作是企业履行其法定义务的表现。

2.重点突出，逐步完善

企业，尤其是处于发展初期的企业往往存在着成本控制的压力。因此，开展合规工作需要与企业的业务场景、发展阶段及监管热点结合，对症下药，突出合规重点，分步骤逐步完善数据合规体系。举例来说，对于互联网企业，可以重点关注爬虫技术的合法性问题，以避免如Z公司一般落入刑事问责的窘境。我们将利用爬虫技术可能触及刑事责任的一般情形总结于下图：

数据安全管理机构既要有决策权，又要避免沦为“一言堂”。

数据抓取妨碍网站正常运营的

- 以数据抓取的方式造成网站、信息系统瘫痪或暂时瘫痪的，可能构成“破坏计算机信息系统罪”。例如(2019)粤0305刑初193号案件中，被告使用爬虫技术导致“深圳市居住证系统”停止运行两小时，从而被告被认定其爬虫行为构成“破坏计算机信息系统罪”。

数据抓取违反平台技术限制及访问要求的

- 绕过平台技术访问限制、身份限制等爬取个人信息的，将可能如本案Z公司般构成“非法获取计算机信息系统罪”。

抓取特定领域内的非公开信息的

- 利用爬虫技术抓取特定领域内的非公开信息的，将可能被认定为构成“非法侵入计算机系统罪”。

除上图所列情形外，利用爬虫技术，擅自使用其他经营者征得用户同意、依法汇集且具有商业价值的数据，实质性替代其他经营者提供的部分产品或服务，损害公平竞争的市场秩序的，还可能构成不正当竞争，从而被平台方追究侵权责任。

3.建立数据合规体系的几个基本步骤

3.1.明确数据安全管理机构与人员

在建立数据合规体系时，企业首先应当明确数据安全管理机构与人员，以落实数据安全保护职责。我们建议企业结合实际设置该数据安全管理机构与人员：如企业目前暂未涉嫌刑事风险，为了更好地协调组织多部门联动开展数据合规工作，可由决策层成员组成数据安全管理机构；但需要注意的是，数据安全管理机构既要有决策权，又要避免沦为“一言堂”，否则也容易因为某个人的激进决策导致企业出现合规风险，进而成为刑事隐患。

3.2.全流程数据安全管理制度的制定

根据《数据安全法》第二十七条的要

建议企业根据自身情况制定数据分类分级保护制度，
利用数据分类分级工具对数据安全进行差异化管控。

求，企业应当依法制定全流程的数据安全管理制度，通过该制度对本企业的数据收集、存储、使用、加工、传输、提供、公开等全生命周期的安全提出具体合规要求。我们建议企业结合实际制定数据全生命周期的合规管理制度。在企业尚未涉嫌刑事风险，建议企业全面梳理数据处理各个环节的风险与合规薄弱点，通过制度的约束完善企业的数据合规工作；若企业已经面临刑事风险，则建议企业结合检察机关的《检察建议书》等要求以及第三方组织合规评估的重点，针对性地制定本企业的数据安全管理制度，通过制度的制定协助企业尽快“去犯罪化”。此外，为了企业数据安全管理制度的有效落地与执行，建议企业在本制度中明确数据安全合规工作细化的奖惩机制，并严格施行。

3.3.安全与合规的两大工具：数据分类分级+PIA

根据法律的要求以及实践需要，建议企业根据自身情况制定数据分类分级保护制度，利用数据分类分级工具对数据安全进行差异化管控。在制定数据分类分级保护制度时，建议企业首先对数据资产进行梳理，形成数据资产清单；其次，企业应当结合实际需求对数据进行分类与定级：如企业暂未涉嫌刑事风险，则可参考目前的数据分类分级相关指南，如《网络安全标准实践指南——网络数据分类分级指引》，灵活进行数据的分类与定级；若企业已涉嫌刑事风险，则应当对涉嫌刑事风险的相关数据进行特别分类与更高级别的定级管控；最后，建议企业针对不同类别与级别的数据设置区分化的管控措施。

根据《个人信息保护法》第五十五条和第五十六条的要求，建议企业建立个人信息保护影响评估评估机制（**PIA**），对于法定的需要开展个人信息保护影响评估的情形，事前开展评估工作，并依法留存个人信息保护影响评估报告和处理情况记录。企业在应用该工具时，亦可与企业的OA审批等流程相结合，通过自动化的方式将该工具导入企业日常管理中，促进企业数据合规。

以上两类工具的应用，不仅是为了落实《数据安全法》与《个人信息保护法》的要求，更为重要的是，应用上述工具的过程中所产生的众多留痕文件，可以协助企业在事前、事中与事后环节有效识别风险，防范

与应对潜在的刑事问题。

3.4.数据安全事件应急响应机制

根据《数据安全法》第二十七条的要求，企业应当建立数据安全事件应急响应机制，在发生数据安全事件时，应当立即采取处置措施，按照规定及时告知用户并向有关主管部门报告。针对数据安全事件应急预案定期进行演练，以做到对数据安全事件的快速响应。对于已涉嫌刑事风险的企业，建议在设置数据安全事件应急响应机制时，应当重点关注对于可能的犯罪行为已造成的危害后果（如个人信息主体权益严重受损等）的弥补，减轻企业数据类犯罪行为的法益侵害性。

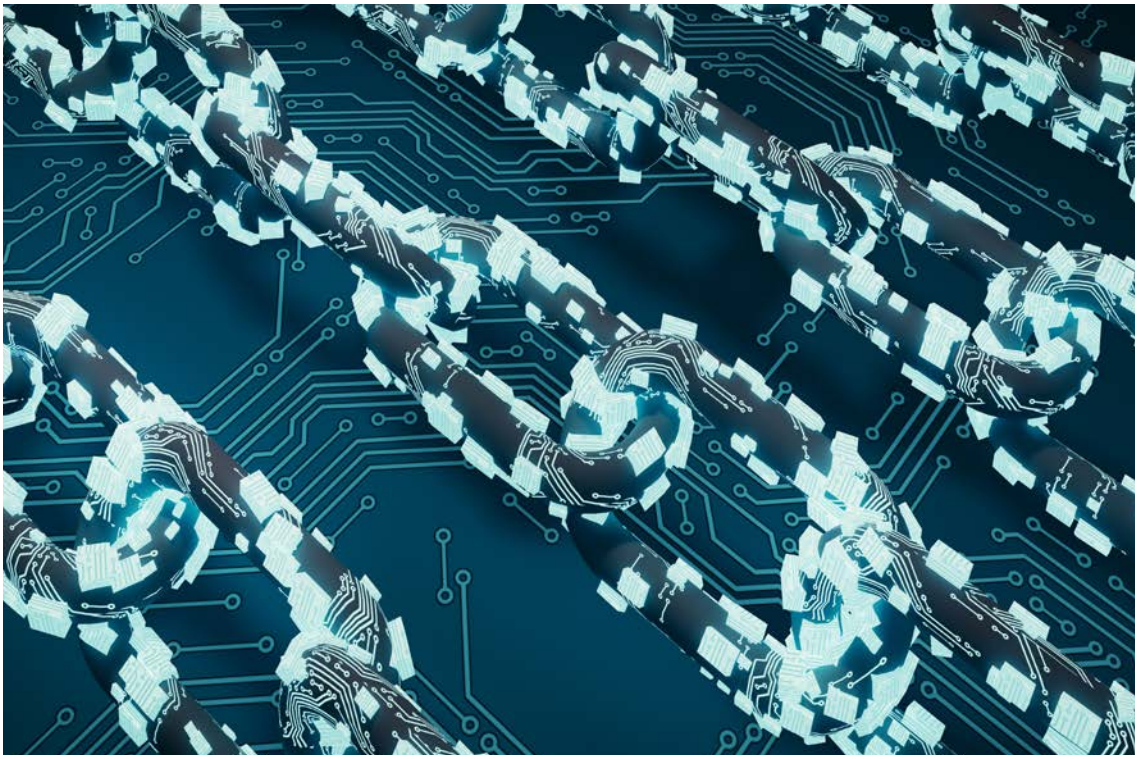
3.5.第三方合作数据合规管理机制

业务运营中，建议企业应当针对上下游严格落实全闭环审核管理，前期审核包括审核服务对象的数据内容、使用范围是否明确，及要求的数据提供方式是否安全等。中期审核包括合同审核，合作伙伴资质审核，明确数据使用范围，同时确保针对个人信息的隐私保护技术切实有效性。后期审核包括通过使用审计或者定期报告等手段，监测整个数据共享链条上的供应商及代理等是否有效履行了合规义务。同时，在第三方合作场景下，建议企业根据与第三方合作的关系，区分化签订不同类型的《数据处理协议》。

在大数据时代，企业的上下游往往是引爆企业刑事风险的“地雷”，诸多案件证明了，由于普遍存在的“数据黑市”，让企业往往存在一定的侥幸心里：“大家都这么干，为什么非要抓我？“。根据我们的经验，很多企业卷入刑事危机，往往是由于一次不经意的”合作“，导致了数年后的刑事风暴。因此，我们建议，对于各类数据处理者，尤其是大数据企业，需要设定特定内部合规机制，在经营中全面、不时地排查与第三方合作的有关风险。

3.6.积极开展数据安全教育与培训

根据《数据安全法》第二十七条的规定，建议企业积极开展数据安全教育与培训工作，增强和提升员工的数据安全保护意识和保护能力。根据近期公布的刑事相关案件，特别是“SDK案”，我们注意到员工个人涉刑事风险亦非常高，且对员工个人的影响极大。因此，企业开展数据安全教育与培训工作的意义，不仅在于防范企业的



合规风险，更在于避免员工个人面临刑事风险。

3.7.定期开展个人信息保护合规审计

根据《个人信息保护法》第五十四条的要求，针对日常运营，尤其是高风险的数据处理活动，建议企业聘请外部专业人员，通过内外部合作定期开展个人信息保护合规审计工作，以审计方式，定期巡查数据合规问题。

3.8.重视数据安全的权限管理工作

在数据安全措施方面，建议企业重点关注权限管理工作。建议企业根据岗位职责设置各级数据处理权限，按照最小必要、职权分离等原则，授予不同员工为完成各自承担任务所需的最小权限，在各账号间形成相互制约的关系。同时，明确数据权限授权审批流程，对数据申请和变更权限严格控制并定期审核，与能够接触重要数据

在数字经济时代，只有在“当数据合规遇到刑事追诉”这种情况发生时，企业和员工不再因终极制裁而担心和焦虑，企业才能因此走向健康、无阻的康庄大道。

或个人信息的员工签订数据保护协议。

PART 005

结语

如果企业做好了数据合规，是否就能依法“脱罪“?尽管很多学者倡导构建事前合规、实体出罪的合规激励机制，但此类机制尚未体现在《刑法》条文中。不过令人欣慰的事，在数据合规和个人信息保护领域，因合规而脱罪的刑事案件已经出现，而且在实践中有关案例也层出不穷。《个人信息保护法》69条设定的”推定过错责任“也证明了在个人信息保护领域，立法者鼓励数据处理者通过搭建实施合规制度，可以证明自己的”无过错“，避免侵权责任。

因此，在数字经济时代，只有在”当数据合规遇到刑事追诉“这种情况发生时，企业和员工不再因终极制裁而担心和焦虑，企业才能因此走向健康、无阻的康庄大道。

（刘颖琪亦对本文作出贡献）

蔡鹏
合伙人
知识产权部
北京办公室
+86 10 5087 2786
caipeng@zhonglun.com

葛燕
非权益合伙人
争议解决部
北京办公室
+86 10 5957 2228
geyan@zhonglun.com

PART THREE

IPO场景下企业数据合规

医疗AI企业IPO数据合规重点问题与应对

陈际红

本文将基于《网络安全法》《数据安全法》《个人信息保护法》及其配套法规，结合健康医疗领域的相关规定，具体介绍医疗AI企业IPO数据合规审查相关重点及应对建议。

人工智能（Artificial Intelligence，简称“**AI**”）概括而言是对人的意识和思维过程的模拟，利用机器学习和数据分析方法赋予机器类人的能力。AI技术发展至今，已经将计算机视觉技术、自然语言处理技术、跨媒体分析推理技术等技术运用到安防、金融、零售、交通、教育、医疗、制造、健康等各个产业与场景，大大提升了社会劳动生产率，降低了劳动成本，优化了产品和服务，为人类的生产和生活带来了巨大的转变。医疗AI是指将AI技术应用到医疗领域中，可以解决医疗资源短缺、分配不均等问题，提升诊疗水平和效率。近年来，随着AI技术的加速成熟，其在医疗健康领域的应用场景不断丰富，为疾病检测、诊断及治疗模式带来深刻变革。

据不完全统计，2019年至今，国内医疗AI企业共发生200多起融资事件，l医疗、东软医疗、T医疗、数坤科技、A科技等医疗AI企业也先后递交招股书，最终A科技（Airdoc）于2021年11月正式于香港联交所主板挂牌上市，成为了医疗AI赛道上成功上市的第一家公司。根据预测分析，全球AI应用市场总值预计在2025年将达到1270亿美元，其中医疗行业将占AI应用市场规模的五分之一[1]，医疗AI行业将集体迎来前所未有的蓝海时代。

为了更好地服务医疗AI企业，尤其是拟上市企业的数据合规落地工作，本文将基于《网络安全法》《数据安全法》《个人信息保护法》及其配套法规，结合健康医疗领域的相关规定，具体介绍医疗AI企业IPO数据合规审查相关重点及应对建议。

PART 001

医疗AI产业政策及监管规范概览

近年来，我国陆续出台利好医疗AI领域的宏观产业政策，大力推广应用人工智能诊疗新模式，从鼓励创新、促进应用以及完善标准等方面支持人工智能医疗体系的创新发展。我们在下表中梳理归纳了国家层面针对医疗AI产业出台的系列支持政策：

1.中国信息通信研究院、工业互联网创新中心（上海）有限公司、36氪研究院：《2020年人工智能医疗产业发展蓝皮书》。

近年来，我国陆续出台利好医疗AI领域的宏观产业政策，从鼓励创新、促进应用以及完善标准等方面支持人工智能医疗体系的创新发展。

文件名称	发布机构	时间	核心要点
《关于加快场景创新以人工智能高水平应用促进经济高质量发展的指导意见》	科技部等六部门	2022.8	在医疗领域积极探索医疗影像智能辅助诊断、临床诊疗辅助决策支持、医用机器人、互联网医院、智能医疗设备管理、智慧医院、智能公共卫生服务等人工智能重大场景。
《“十四五”生物经济发展规划》	发改委	2022.5	鼓励发展人工智能以辅助新药研发和支持疾病诊疗。
《关于推动公立医院高质量发展的意见》	国务院	2021.6	推动手术机器人等智能医疗设备和智能辅助诊疗系统的研发与应用。
《国家新一代人工智能标准体系建设指南》	标准委、网信办、发改委等五部委	2020.8	围绕医疗数据、医疗诊断、医疗服务、医疗监管等，重点规范人工智能医疗应用在数据获取、数据隐身管理等方面内容，包括医疗数据特征表示、人工智能医疗质量评估等标准。
《国家新一代人工智能开放创新平台建设工作指引》	科技部	2019.8	鼓励人工智能细分领域领军企业搭建开源、开放平台，面向公众开放人工智能技术研发资源，向社会输出人工智能技术服务能力，推动人工智能技术的行业应用，培育行业领军企业，助力中小微企业成长。
《关于促进人工智能和实体经济深度融合的指导意见》	深改委	2019.3	稳步推进教育、医疗、能源、公共安全等领域数据的内部整合、共享与对外开放，制定数据资源清单和开放计划，支持相关企事业单位联合人工智能企业围绕应用场景开展人工智能服务，鼓励优质机构人工智能服务能力和资源向地方开放。
《关于深入开展“互联网+医疗健康”便民惠民活动的通知》	卫健委、中医药管理局	2018.7	加快推进智慧医院建设，改造优化诊疗流程。推进智能医学影像识别、病理分型和多学科会诊以及多种医疗健康场景下的智能语音技术应用，提高医疗服务效率。

文件名称	发布机构	时间	核心要点
《关于促进“互联网+医疗健康”发展的意见》	国务院	2018.4	推进“互联网+”人工智能应用服务。开展基于人工智能技术、医疗健康智能设备的移动医疗示范，实现个人健康实时监测与评估、疾病预警、慢病筛查、主动干预。加强临床、科研数据整合共享和应用，支持研发医疗健康相关的人工智能技术、医用机器人、大型医疗设备、应急救援医疗设备、生物三维打印技术和可穿戴设备等。
《关于印发新一代人工智能发展规划的通知》	国务院	2017.7	推广应用人工智能治疗新模式新手段，建立快速精准的智能医疗体系。基于人工智能开发医疗设备、开展研究和新药研发，推进医药监管智能化。计划到2025年，新一代人工智能在智能医疗等领域得到广泛应用。

表1：医疗AI领域宏观产业政策概览

在医疗领域科技创新纵深发展和AI领域重大场景积极布局的背景下，上述利好政策无疑促进了医疗AI企业在资本市场的活跃表现。然而，医疗AI的配套监管措施却较为庞杂，针对医疗AI企业在产品研发、业务开展等过程中使用个人信息及医疗健康数据如何进行规制等问题，暂无体系化的专门立法予以规制。当前，医疗AI监管仍沿用医疗大数据领域、网络安全、数据安全及个人信息保护领域的相关规范。

当前，医疗AI监管仍沿用医疗大数据领域、网络安全、数据安全及个人信息保护领域的相关规范。

文件名称	发布机构	时间	核心要点
《信息安全技术—生物特征识别信息保护基本要求》	市监局、标准委	2022.5	对生物特征识别信息的收集、存储、使用、主体权利、委托处理、共享、转让、公开披露、信息安全事件处置、信息安全管理要求做出规定。明确基于生物特征识别信息的身份识别相关算法，以及开展生物特征识别相关活动时收集的生物特征识别信息原则上不应出境、出口；如有特殊原因需经审批。
《医疗器械网络安全注册审查指导原则（2022年修订版）》	药监局	2022.3	对医疗器械相关数据、网络安全事件应急响应、网络安全更新、网络安全生存周期过程、医疗数据出境和远程维护与升级等方面做出具体规定。
《最高人民法院关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定》	最高法	2021.7	从民事责任角度，规定了处理平等民事主体之间因使用人脸识别技术处理人脸信息所引发纠纷的裁判规则。
《信息安全技术—健康医疗数据安全指南》	市监局、标准委	2021.7	指导健康医疗数据控制者对健康医疗数据进行安全保护，也可供健康医疗、网络安全相关主管部门以及第三方评估机构等组织开展健康医疗数据的安全监督管理与评估等工作时参考。
《互联网医疗健康信息安全管理规范（征求意见稿）》	卫健委	2021.6	互联网医疗健康信息系统应通过网络安全等级保护三级测评和定期复评。互联网医疗健康信息系统集成第三方服务应用时，第三方服务也需要达到相关安全防护水平。
《药物临床试验质量管理规范》	药监局、卫健委	2020.7	针对临床试验不同主体（包括申办者、临床试验机构以及主要研究者）规范临床试验数据的真实性、可靠性和合规性。

无体系化的专门立法会带来当前和未来适用法律法规的不确定性，而人工智能高速发展带来的风险却仍有增加。

文件名称	发布机构	时间	核心要点
《国家健康医疗大数据标准、安全和服务管理办法(试行)》	卫健委	2018.7	明确各级卫生健康部门、医疗卫生机构、相关应用单位及个人在健康医疗大数据标准管理、安全管理、服务管理中的职责权利。
《人口健康信息管理办法(试行)》	卫计委(现卫健委)	2014.5	规范各级各类医疗卫生计生服务机构所涉及的人口健康信息的采集、管理、利用、安全和隐私保护工作。
《医疗机构病历管理规定》	卫计委(现卫健委)、中医药管理局	2013.11	明确医疗机构及其医务人员应当严格保护患者隐私，禁止以非医疗、教学、研究目的泄露患者的病历资料。

表2：医疗AI数据合规核心规范[2]

在遵守数据合规相关法律法规之外，医疗AI企业还应关注其所适用的不同细分领域的法律法规。提供软件的医疗AI企业需关注医疗器械注册、安全技术审评等合规要点[3]；提供互联网诊疗服务的医疗AI企业需关注互联网诊疗及人工智能辅助治疗相关规范，注意AI软件不得冒用、替代医师本人接诊，严禁使用AI自动生成处方等。此外，企业还应特别关注人工智能伦理审查问题，具体包括以人为本、明确问责体系、提升系统透明度和避免算法歧视等。

综上所述，无体系化的专门立法会带来当前和未来适用法律法规的不确定性，而人工智能高速发展带来的风险却仍有增加。这导致近年来监管机构和交易所针对医疗AI企业提起问询的态度愈发严格和审慎，故医疗AI企业在IPO阶段面临的数据合规问询挑战将不断提高。

2.在本文主题下，此处仅聚焦医疗AI企业数据合规特别规范，不含一般数据合规法律法规。
3.可参考《人工智能辅助治疗技术临床应用管理规范(2022年版)》《人工智能医用软件产品分类界定指导原则》《深度学习辅助决策医疗器械软件审评要点》等规范。

我们梳理了四家在问询阶段涉及数据合规问题的企业，以期识别监管部门及交易所在IPO阶段的数据合规审查重点。

PART 002

医疗AI企业IPO数据合规审查重点

当前，虽然医疗AI领域成长为一级市场投融资热门赛道，但已上市企业较少。基于医疗AI企业IPO公开材料，我们梳理了四家在问询阶段涉及数据合规问题的企业，以期识别监管部门及交易所在IPO阶段的数据合规审查重点。具体公司及相关情况如下表所示[4]：

上市板块	公司名称	业务	涉及数据合规问题的问询阶段	上市进程
科创板	浙江太美医疗科技股份有限公司（“太美科技”）	云计算和大数据技术的生命科学产业数字化解决方案	第一轮审核问询	已问询
科创板	J（北京）科技股份有限公司（“J科技”）	医疗信息化软件产品研发、销售及技术服务	第一轮审核问询 第三轮审核问询	2021年12月上市（688246.SH）
联交所	北京A科技发展股份有限公司（“A科技”）	人工智能视网膜影像识别的早期检测、诊断及健康风险评估解决方案	问询及聆讯阶段	2021年10月上市（02251.HK）
联交所	Y科技有限公司（“Y科技”）	大数据和人工智能技术的医疗解决方案	问询及聆讯阶段	2020年12月上市（02158.HK）

表3：医疗AI领域涉及数据合规问询公司

在科创板全公开问询模式下，监管机构的审核问询函可以直接体现其关注重点，故我们梳理了科创板（拟）上市企业于问询阶段被要求回复的数据合规问题，具体内容如下：

4.经检索，部分医疗AI企业在问询阶段未涉及数据合规问题，如上海I医疗科技股份有限公司、北京天智航医疗科技股份有限公司。

在科创板全公开问询模式下，监管机构的审核问询函可以直接体现其关注重点。

类别	被问询企业	问题
数据收集	太美科技	主要产品及核心技术涉及的数据来源及类型、数据获取方式。
	J科技	各项核心技术涉及的数据来源及类型、数据获取方式。(第一轮审核问询)
		共建大数据平台模式下的数据来源，该模式下数据的获取是否合法合规。(第三轮审核问询)
数据存储	太美科技	主要产品及核心技术涉及的数据存储方式。
	J科技	各项核心技术涉及的数据存储方式。(第一轮审核问询)
数据使用	太美科技	在数据使用中是否需取得相关方的许可或授权、相关授权是否完整；是否存在超出授权范围使用数据的情形。
	J科技	共建大数据平台模式下的数据使用是否合法合规。(第三轮审核问询)
第三方管理	J科技	通过科研合作产生数据集或基于真实医疗业务数据开展技术的，在数据使用中是否需取得相关方的许可或授权、相关授权是否完整。(第一轮审核问询)
数据安全	太美科技	是否存在侵犯患者隐私的情形。
		是否建立有效的内部控制制度确保业务开展中涉及的数据合规性。
	J科技	是否存在侵犯患者隐私的情形。(第一轮审核问询)
		是否建立有效的内部控制制度确保业务开展中涉及的数据合规性。(第三轮审核问询)

类别	被问询企业	问题
数据立法和监管	太美科技	符合《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》等相关规定的情况。
	J科技	共建大数据平台模式下，相关数据的获取、管理和使用是否符合《中华人民共和国数据安全法》等相关规定、是否存在法律风险。（第三轮审核问询）
		相关数据在发行人不同产品及技术中的具体作用，发行人的核心技术集中体现在其收集、积累的大量数据，还是对客户数据的加工处理能力，发行人关于数据的采集、存储及使用与同行业可比公司是否存在差异。（第一轮审核问询）

表4：科创板上市医疗AI企业数据合规相关问询问题[5]

赴港上市时，申请人一般在招股书的概要、风险因素、监管概览、业务四个章节披露数据合规情况。由于联交所的问询和聆讯都是以非公开的方式进行，问询和聆讯的结果主要体现在招股书的变化上。故通过梳理发行上市时的招股书相较于A1招股书的更新情况，可以探寻联交所在企业数据合规方面的关注重点。

5.见华泰联合证券有限责任公司：《关于浙江太美医疗科技股份有限公司首次公开发行股票并在科创板上市申请文件的审核问询函的回复》，2022年3月，上海证券交易所。华泰联合证券有限责任公司：《关于J（北京）科技股份有限公司首次公开发行股票并在科创板上市的申请文件的审核问询函之回复报告》，2020年11月，上海证券交易所。华泰联合证券有限责任公司：《关于J（北京）科技股份有限公司首次公开发行股票并在科创板上市的申请文件的第三轮审核问询函之回复报告》，2021年4月，上海证券交易所。

通过梳理发行上市时的招股书相较于A1招股书的更新情况，可以探寻联交所在企业数据合规方面的关注重点。

章节	披露重点	企业	招股书更新情况
概要	披露近期数据合规监管趋势以及在记录期内和截至实际可行日的相关合规情况	A科技	(1)在“与我们的业务合作伙伴展开合作”部分，就第三方的数据收集、存储，与第三方签署协议情况以及内部政策展开描述； (2)新增“数据隐私及保护”板块，披露数据处理合规情况以及采取的合规措施。
		Y科技	(1)新增“数据安排和安全”板块，披露数据处理合规情况以及采取的合规措施。
风险因素	披露运营中与数据合规相关的潜在风险	A科技	(1)更新关于因第三方合作伙伴泄露或滥用用户数据带来的相关风险表述； (2)新增披露网络安全审查可能带来的风险； (3)新增披露监管及执法制度不断完善可能带来的风险。
		Y科技	(1)新增披露第三方数据源准确性可能带来的风险； (2)新增披露去标识化数据集重新标识可能带来的风险。
监管概览	梳理并披露运营中需遵守的重大数据合规相关法律法规（包括现时需遵守的，以及未来预期将对其业务有重大影响的）	A科技	(1)对作为数据处理者如何履行《数据安全法》展开更为详细的描述； (2)更新关于《网络安全审查办法》《国家健康医疗大数据标准、安全和服务管理办法（试行）》《信息安全等级保护管理办法》相关表述； (3)新增对于公司是否以及如何适用《网络产品安全漏洞管理规定》《最高人民法院关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定》《关键信息基础设施安全保护条例》《汽车数据安全管理若干规定（试行）》《个人信息保护法》《互联网信息服务算法推荐管理规定（征求意见稿）》的论述； (4)在《关于依法从严打击证券违法活动的意见》颁布后的中概股严格合规审查背景下，从数据收集、存储、安全管理三方面论述采取何等措施加强数据安全保护； (5)新增披露选择健康医疗大数据服务提供商需遵守的法律法规及标准。

章节	披露重点	企业	招股书更新情况
		Y科技	(1)新增“有关医疗大数据的法规”板块,系统梳理健康医疗大数据相关法律法规及标准; (2)新增披露选择健康医疗大数据服务提供商需遵守的法律法规及标准; (3)更新关于《网络安全审查办法》《信息安全等级保护管理办法》《网络安全等级保护定级指南》相关表述; (4)新增对于公司是否以及如何适用《信息安全技术 个人信息安全规范》《信息安全技术 个人信息去标识化指南》《信息技术　资料品质评价指标》以及其他非强制性国家标准的论述; (5)新增对于公司是否以及如何适用《保守国家秘密法》的论述。
业务	在业务模式和业务运营具体场景下,披露运营中采取的数据合规内控措施	A科技	(1)新增关于数据收集(直接收集、通过业务合作伙伴收集)的业务合规描述; (2)更新数据保护政策、数据保护解决方案、与数据保护有关的其他措施等内容; (3)新增网络安全审查对业务影响的论述; (4)在“与临床试验机构的合作”部分,就第三方的数据收集、存储,与第三方签署协议情况以及内部政策展开描述。
		Y科技	(1)新增“数据安排和安全”板块,披露数据处理合规情况以及采取的合规措施; (2)详细描述等保备案情况; (3)详细描述算法和模型部署情况; (4)详细描述去标识化技术情况; (5)详细描述公司内部针对数据安全和个人信息保护的内部控制系统情况; (6)详细描述公司内部数据合规组织架构情况; (7)新增披露各业务如何经审阅确认后在重大方面符合数据保护和隐私相关中国法律法规。

表5:联交所上市医疗AI企业数据合规相关问询问题[6]

6.见A科技:发行上市时的招股书、A1招股书;Y科技:发行上市时的招股书、A1招股书。

如何保障数据全生命周期处理活动的合法合规将是医疗AI企业需要首要解决的问题。

整体而言，数据采集、存储、使用和安全管理系上市评审机构所重点关注的数据合规问题。特别地，针对医疗AI企业，患者个人信息的安全保障以及与线下医院、科研机构等第三方合作中的数据处理通常受到重点关注。对于赴港上市的医疗AI企业，联交所当前关注一条主线和一个重点，主线即企业是否充分披露在业务开展和内部控制中为确保遵守相关已生效和即将生效的数据合规法律法规而采取的措施；重点即医疗AI企业与第三方合作伙伴之间的数据处理活动。此外，联交所还会对企业是否就网络安全审查采取相应行动展开问询，主要关注医疗AI企业是否构成关键信息基础设施运营者以及相关业务是否会影响国家安全。

PART 003

医疗AI主要应用场景及数据合规要点

数据是人工智能发展的基石，人工智能在深度学习和机器学习领域的突破高度，有赖于高密度、高质量、多种类的数据支撑，数据全生命周期的合规管理要求，应成为人工智能研发、测试、应用过程中纳入考量的合规重点。鉴于医疗AI往往涉及处理患者、医生以及其他医疗AI产品或设备使用者的个人信息，且可能涉及处理诸如敏感个人信息、健康医疗大数据、人类遗传资源信息、重要数据等，医疗AI企业在数据合规层面面临巨大的压力，如何保障数据全生命周期处理活动的合法合规将是医疗AI企业需要首要解决的问题（下图为医疗AI上下游产业链、医疗AI应用场景以及AI相关技术全景图）。

在原始数据收集阶段，医疗AI企业将面临如何确保数据源合法合规等问题。

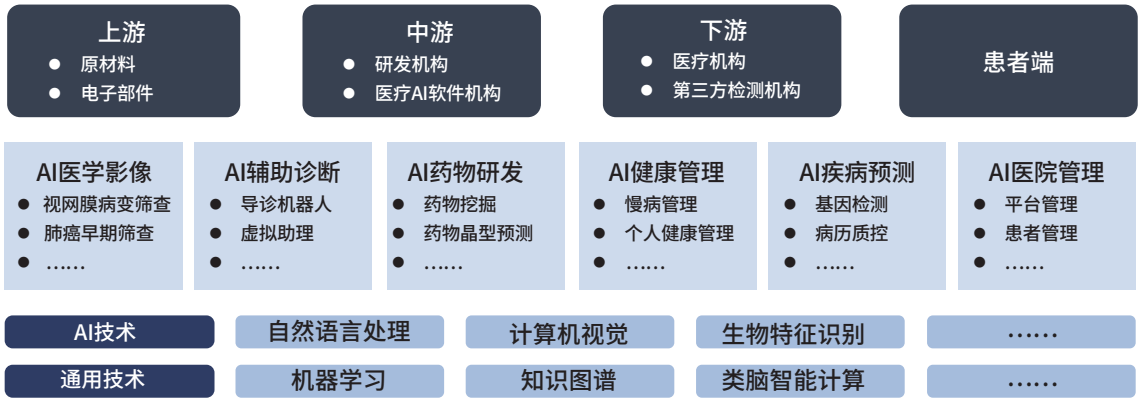


图:医疗AI应用全景图

3.1 数据收集

在原始数据收集阶段，AI系统以模型训练、结果推断预测及输出等目的，通过个人信息主体主动提供、设备自动采集或从第三方间接获取等方式收集大量训练和应用数据。以AI医学影像为例，大部分医疗数据来自于医学影像，这些医学影像数据结构简单，便于用作机器学习的素材，并且具有深度挖掘与研究的价值。AI医学影像一般以计算机视觉技术为核心，通过图像获取、预处理、特征提取、检测/分割和高级处理等过程对医疗影像进行处理，同时还可能运用自然语言处理等人工智能技术，学习、理解和归纳医学书籍文献、诊疗指南、病历信息等，形成“医学知识图谱”[7]，通过深度学习建立诊断模型，并在人类医学专家的校验下，优化诊断模型。由此，在原始数据收集阶段，医疗AI企业将面临如何确保数据源合法合规等问题。

•直接从个人信息主体收集

在从个人信息主体直接收集数据时，医疗AI企业应重点审查，是否具备收集、处理个人信息的合法基础，如基于用户的同意或是履行合同所必要等，在涉及收集、处理敏感个人信息时，以同意为合法基础的，还应该获得用户的单独同意。

7.《2019年人工智能发展白皮书》腾讯觅影AI辅诊开放平台核心能力的技术能力描述。

医疗AI企业应该遵循最小必要原则收集、处理个人信息，避免过度（过量或者过频）采集数据。

医疗AI企业还需要考虑是否设置了隐私政策、知情同意书、告知函（以下统称“**规则告知文本**”），明确个人信息处理的目的、方式、范围，涉及处理敏感个人信息的，还应当向个人信息主体告知处理敏感个人信息的必要性以及对个人权益的影响。在某些敏感程度较高的数据收集场景中，保障个人信息主体的知情同意将尤为重要，如从事基因检测或疾病预测的医疗AI企业，一般会收集并处理人类遗传资源信息（如基因数据），在收集相关人类遗传资源信息前，医疗AI企业应该做到事先全面、完整、真实、准确告知采集目的、人类遗传资源信息的预期用途、对个人健康可能产生的影响以及医疗AI企业采取的隐私保护措施[8]，并征得人类遗传资源信息提供者的书面同意，最后，还需要保障人类遗传资源信息提供者自愿参与和在处理其人遗资源的过程中随时无条件退出的权利。

在数据收集阶段，医疗AI企业应避免超出规则告知文本公示的范围收集、处理个人信息。实际上，基于AI技术的复杂性，可能确实存在AI开发者在使用个人信息时，发现关联到特定自然人，或产生新的个人信息使用的情形，而这些情况可能未在收集时向信息主体披露的规则告知文本中予以穷尽，从而出现超范围收集、处理个人信息的情况。医疗AI企业应该在个人信息处理方式、目的、范围发生变化后，及时通过更新规则告知文本等方式，向用户予以说明，重新获得用户授权同意或具备其他合法基础，避免产生合规风险。

医疗AI企业应该遵循最小必要原则收集、处理个人信息，避免过度（过量或者过频）采集数据。鉴于人工智能模型训练需建立在高数量、多种类的数据的基础上，医疗AI企业需重点关注所收集、处理的数据是否均限于实现所述目的最小必要。例如，医疗AI在个人健康大数据智能分析领域应用过程中，可能通过智能穿戴设备直接收集用户个人信息，从事个人健康大数据智能分析的企业应着重关注通过智能穿戴设备收集用户个人信息的范围、频率的情况，在用户佩戴智能穿戴设备的过程中，企业可能在全方位、随时随地、在用户毫无感知情况下获取和分析用户的血氧饱和度、血压、

8.《人类遗传资源管理条例》第12条。

在国家大力发展数据交易，促进数据要素流通的背景下，数据交易相关的法律法规将更加完善，医疗AI企业可以考虑通过数据交易所等平台获取数据。

血糖、心率、睡眠等信息，无止境的数据收集行为存在超出最小必要收集个人信息的可能，将会给相关企业带来巨大的合规风险。据此，一方面，相关企业在收集、处理个人信息前应进行必要性评估，避免违背最小必要原则收集、处理个人信息；另一方面，相关企业可以通过在智能穿戴设备设置相关功能，保障用户可以自主控制智能穿戴设备，能够自主开启或关闭相关场景数据收集的功能[9]。

•间接从第三方收集

从合作的第三方获取数据时，医疗AI企业首先需要确保数据源合法合规，明确双方数据安全及保护责任。一般而言，应通过补充协议/承诺函等方式，要求合作方对数据来源合法合规性作出承诺，并厘清双方在数据处理层面的角色关系以及各自的权利和义务，如在开展临床研究时，应该明确申办者、临床研究机构、研究者等角色，明确重点安全措施，保障处理数据的安全[10]。此外，通过采购的方式从第三方获取数据时，可能也存在上述无法确保数据源合法合规的问题。目前，在国家大力发展数据交易，促进数据要素流通的背景下，数据交易相关的法律法规将更加完善，医疗AI企业可以考虑通过数据交易所等平台获取数据，一方面，各医疗机构、科研机构可能掌握了大量的患者数据，可以通过数据交易所等平台向医疗AI企业提供研究、测试数据，另一方面，数据交易所将对其挂牌的数据产品进行更严格和完善的审核，以保障数据源合法合规，保障数据产品的质量，提高研发效率。

•通过公开渠道收集

通过公开渠道获取数据时，则应该注重获取数据的手段是否合法合规，尤其通过爬虫技术等手段间接获得数据时，可能存在不正当竞争、侵犯商业秘密甚至刑事责任的风险，通过人工下载等方式获取公开数据的，也可能存在无法保障数据来源合法合规性等风险。医疗AI企业在通过公开渠道获取数据时，应注重使用数据爬取等自动化技术的合法合规性，应评估数据爬取对象的性质、频率、数据量、采取的具体技术措施等，综合评估行为合规性，进而采取风险缓释措施，包括但不限于仅抓取

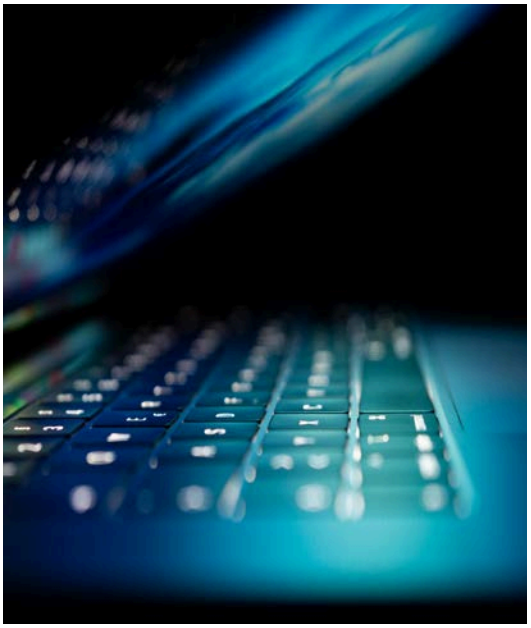
9.《健康医疗数据安全指南》第11.5.2.2，11.5.2.4条
10.《信息安全技术 健康医疗数据安全指南》第11.3条。

医疗AI企业应根据不同应用场景需求设计数据存储策略。

公开的前台数据、遵守Robots协议、抓取行为不应妨碍网站的正常运行[11]、限制抓取内容、避免抓取行为对被抓取方造成直接损害或侵犯其实质商业利益（若数据抓取方和被抓取方的商业模式相同或近似）、不采用违法技术手段（比如破解密码、身份伪装等）等。在使用人工下载等方式获取数据的，也应该尽量选择政府平台或数据公开的官方平台，以降低合规风险。

3.2 数据存储及跨境

对于AI系统收集或产生的数据，通常存储地点分为本地现场存储（前端）、后端数据存储（数仓、底层数据池等）、云端数据库存储等，医疗AI企业应根据不同应用场景需求设计数据存储策略，如在个人健康大数据智能分析应用场景中，在收集、处理智能穿戴设备佩戴者呼吸、心率、脉搏、睡眠等数据时，需要现场对数据进行实时分析、备份、回传、处理等；在电子病历管理过程中，需要进行语音、语义识别时，则可能通过云端处理及存储；在医疗AI影像应用场景中，医疗影像数据一般来自第三方合作伙伴或公开渠道，则需要在后端进行大



量的数据存储并开展深度学习。

•存储期限

在数据存储期限方面，对于涉及处理个人信息的，医疗AI企业需要着重审查是否在满足法律法规要求的最低存储期限的基础上，按照数据存储时间最小化的原则要求，结合业务及技术需要，合理制定数据存储期限，避免数据永久存储带来的合规风险，关于不同类型数据存储要求见下表。

11.《数据安全管理办法（征求意见稿）》第十六条 网络运营者采取自动化手段访问收集网站数据，不得妨碍网站正常运行；此类行为严重影响网站运行，如自动化访问收集流量超过网站日均流量三分之一，网站要求停止自动化访问收集时，应当停止。

按照数据存储时间最小化的原则要求，结合业务及技术需要，合理制定数据存储期限，避免数据永久存储带来的合规风险。

数据类型	存储期限要求	可能涉及医疗AI领域
病历数据（含电子病历）	门（急）诊（电子）病历由医疗机构保管的，保存时间自患者最后一次就诊之日起不少于15年；住院（电子）病历保存时间自患者最后一次住院出院之日起不少于30年。	AI电子病历（语音录入病例）
处方数据	普通处方、急诊处方、儿科处方保存期限为1年，医疗用毒性药品、第二类精神药品处方保存期限为2年，麻醉药品和第一类精神药品处方保存期限为3年。 处方保存期满后，经医疗机构主要负责人批准、登记备案，方可销毁。	AI药物研发等
医疗器械销售数据	从事医疗器械网络销售的企业、医疗器械网络交易服务第三方平台提供者，应当记录医疗器械销售信息，记录应当保存至医疗器械有效期后2年；无有效期的，保存时间不得少于5年；植入类医疗器械的销售信息应当永久保存。	医疗AI产品可能构成医用软件，对外出售相关医疗AI产品可能需要处理医疗器械销售数据[12]。
人类遗传资源信息	人类遗传资源采集、保藏单位，在开展相关行为前，需获取国务院科学技术行政部门批准。采集时需事先告知提供者采集目的、采集用途、对健康可能产生的影响、个人隐私保护措施及其享有的自愿参与和随时无条件退出的权利，并征得其书面同意。保藏应制定应急预案及做好日常保藏记录。	AI疾病预测及基因检测
药品数据	供货企业资质证明文件、购销记录、电子订单、在线药学服务等记录留存应当完整，并保存5年以上。	AI药物研发等

表6:数据存储期限要求

12.医疗AI企业应该注意开展业务是否需要具备相关资质，如从事AI医用软件产品经营的企业可能需要向相关部门申请经营备案或许可，AI医用软件产品线上销售企业可能需要获得经营备案或许可，并可能需要进行医疗器械网络销售信息备案。

医疗AI企业应该梳理企业自身处理数据的类型，履行数据分类分级义务，落实本地化存储的要求。

•存储措施

在数据存储措施方面，医疗AI企业应该根据数据分类分级的结果，明确不同数据的存储要求，如开展AI辅助诊疗应用的企业，可能通过分析虹膜、静脉等生物识别信息，结合深度学习的AI技术达到提示其他疾病风险的目标，而在疾病预测应用中，则可能通过收集、分析人类遗传资源信息达到疾病预测的目标，对于前述敏感程度更高的生物识别信息的存储，除一般加密存储、物理分隔存储、访问权限管控、超期删除等保障措施，还应注意原则上不存储原始数据，仅保留信息摘要，并注重采取匿名化处理等手段保障数据存储安全。

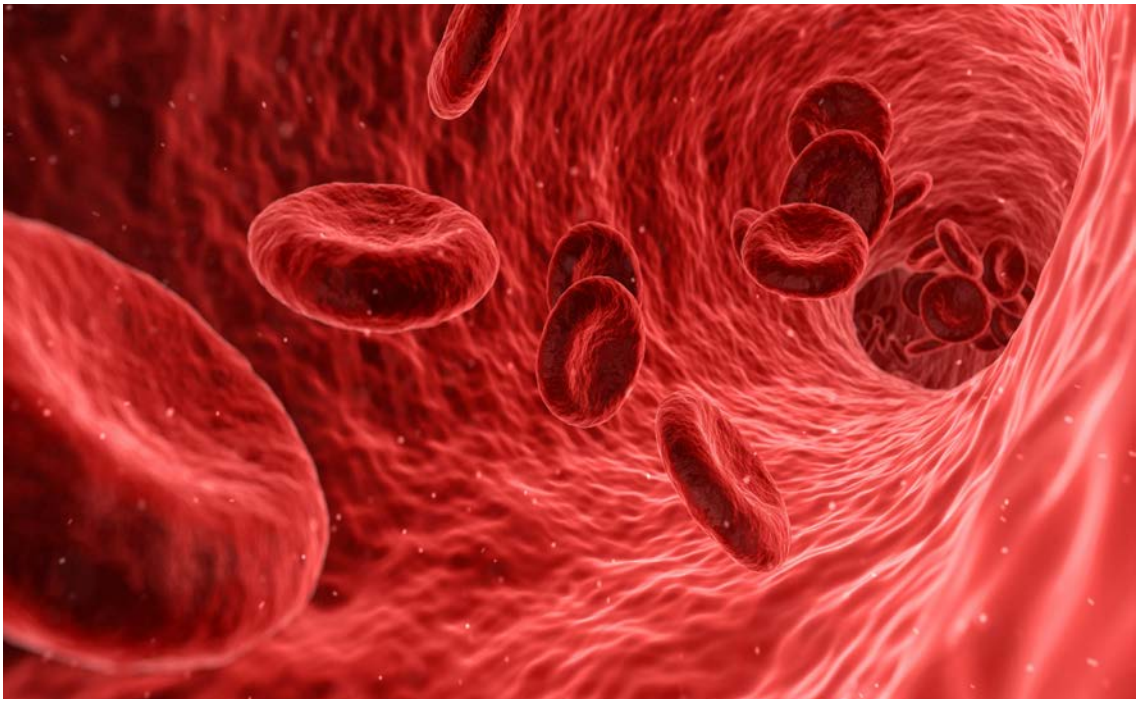
•本地存储及数据跨境要求

医疗AI企业还应该注重不同类型的健康医疗数据本地化存储及跨境传输的监管要求。整体而言，医疗AI企业应该梳理企业自身处理数据的类型，履行数据分类分级义务，落实本地化存储的要求。《网络安全法》《数据安全法》《个人信息保护法》及配套的《数据出境安全评估办法》从整体层面明确了数据本地化存储及跨境传输的要求，关键信息基础设施的运营者（**CIIO**）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[13]，以及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[14]在中华人民共和国境内收集和产生的个人信息，应当存储在境内。

就个人信息跨境传输而言，被认定为CIIO或处理个人信息达到100万的数据处理者（数据处理者身份维度），或自上年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的数据处理者（数据量级维度）向境外提供个人信息的，应当通过网信部门的安全评估[15]。对于其他个人信息跨境传输的场景，企业可以自行选择经专业机构的个人信息保护认证，或与境外接收方订立网信部门制定的跨境传输标准合同，并具备处理个人信息的合法基础，满足透明性要求，开展个人信息保护影响评估，确保境外接收方数据安全能力达到同等保护水平。

13.《网络安全法》第37条，《数据安全法》第31条。
14.《个人信息保护法》第40条，结合《数据出境安全评估办法》第4条，我们理解目前处理个人信息达到100万的，应该履行本地化的存储要求。
15.《数据出境安全评估办法》第4条。

医疗AI企业在处理个人健康医疗数据、人类遗传资源信息、健康医疗大数据、人口健康数据等数据时，应该以本地化存储为原则，跨境传输为例外。



医疗AI企业在关注个人健康医疗相关的数据时，还应该关注企业自身业务开展过程中是否涉及处理重要数据，如反映群体健康生理状况、族群特征、遗传信息等的基础数据，如人口普查资料、人类遗传资源信息、基因测序原始数据均可能属于重要数据[16]，若医疗AI企业因业务需要确需跨境传输重要数据的，应该通过相关部门的安全评估。

除了遵循《数据安全法》《个人信息保护法》等一般性法律法规的要求，医疗AI企业处理各类数据，还应该遵循医疗健康领域特殊要求。医疗AI企业在处理个人健康医疗数据、人类遗传资源信息、健康医疗大数据、人口健康数据等数据时，应该以本地化存储为原则，跨境传输为例外，具体要求如下表：

16.《信息安全技术 重要数据识别指南》（征求意见稿）第5条。

数据类型	本地化存储要求	跨境传输特殊要求	医疗AI领域列举
个人健康医疗数据	健康医疗数据应存储在境内服务器，健康医疗数据控制者不托管、租赁在境外的服务器。	**场景1**：基于**学术研讨需要**的健康医疗数据跨境传输：宜进行必要的去标识化处理；经数据安全委员会讨论审批同意；数量在250条以内；非涉密非重要数据。 **场景2**：一般数据跨境：经**主体授权**同意和数据安全委员会讨论审批同意；数量**累计**在250条以内；非涉密非重要数据非其他禁止或限制向境外提供的数据[17]。	医疗AI影像涉及大量医疗影像，可能涉及个人健康医疗数据。 AI辅助诊断，涉及癌症诊断、电子病历等，可能涉及个人健康医疗数据。 个人健康大数据智能分析可能通过智能穿戴设备收集个人健康医疗数据。
人类遗传资源信息	/	**场景1**：利用我国人类遗传资源开展国际合作科学研究；因其他特殊情况确需将我国人类遗传资源材料运送、邮寄、携带出境：对我国公众健康、国家安全和社会公共利益没有危害，来源合法，出境用途合理；取得人类遗传资源材料出境证明；涉及外方单位，应与中方单位以合作方式开展，经国务院科学技术行政部门批准。 **场景2：【视同跨境】**：向**外国**组织、个人及其设立或者实际控制的机构提供或者开放使用，**可能影响公众健康、国家安全和社会公共利益的**：应当通过国务院科学技术行政部门组织的安全审查；应当向国务院科学技术行政部门备案并提交信息备份[18]。	AI疾病预测及基因检测可能涉及人类遗传资源信息。

17.《信息安全技术 健康医疗数据安全指南》第7 o)、p)条。
18.《人类遗传资源管理条例》第22、28条

医疗AI企业应该注重数据使用过程中涉及的数据质量、数据重识别及算法合规问题。

数据类型	本地化存储要求	跨境传输特殊要求	医疗AI领域列举
健康医疗大数据	健康医疗大数据应当存储在境内安全可信的服务器上，因业务需要确需向境外提供的，应当按照相关法律法规及有关要求进行安全评估审核。	因业务需要确需向境外提供的：安全评估审核[19]。	在研发、测试及应用医疗AI产品过程中收集、产生、衍生的数据，可能属于在人们疾病防治、健康管理等过程中产生的与健康医疗相关的数据，即构成“健康医疗大数据”。
人口健康数据	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。	禁止跨境传输[20]。	在研发、测试医疗AI时，可能与第三方合作伙伴合作，来自各类医疗卫生计生服务机构在服务和管理过程中产生的人口基本信息、医疗卫生服务信息等数据，可能属于人口健康数据。

表7：数据本地化存储及跨境传输要求

3.3 数据使用

在内部数据使用（数据分析和处理）阶段，涉及模型训练和部署运行过程，包括数据准备、数据挖掘、模型训练、测试验证、模型参数部署、预测结果输出等。医疗AI企业应该注重数据使用过程中涉及的数据质量、数据重识别及算法合规问题。

•数据质量

医疗AI企业应该保障数据质量。基于AI技术的特点，用于训练的数据集质量将对AI系统的可靠性和安全性起到至关重

19.《国家健康医疗大数据标准、安全和服务管理办法（试行）》第30条。
20.《人口健康信息管理办法（试行）第10条。

医疗AI企业在开展训练前应做好数据准备，对原始数据进行预处理或标注，从而保障训练数据集质量。

要的作用，若训练数据集数量稀少、缺乏多样性或均衡性不足、标注质量低、存在数据噪声等问题，均将明显影数据训练的结果。医疗AI企业在开展训练前应做好数据准备，对原始数据进行预处理或标注，从而保障训练数据集质量。具体的，企业可以从以下几个方面开展工作：

数据汇集与清洗：针对不同来源的数据进行汇集和清洗，设置质量控制规则，检测数据中的错误的、重复的信息，并进行删除或纠正，以提高数据质量。

结构化和标准化：结合AI技术，如采用计算机视觉技术、自然语言处理技术对数据进行结构化和标准化处理，以便机器可以理解、处理和分析；注重对敏感信息进行校验，避免对个人信息的违法违规使用行为。

全流程管理：建立并完善数据质量全流程管理机制，包括但不限于质量监控、分析、报告、警告等，并匹配相应的数据质量管理负责人，及时发现问题，解决问题。

•数据重识别

医疗AI企业应该重点关注去标识化或匿名化处理后数据的重识别问题。一方面是医疗AI企业可能通过从第三方或公开渠道收集的去标识化[21]或匿名化处理的数据重识别到特定自然人。基于AI技术的特点，医疗AI企业一般会将不同渠道收集的数据进行一定程度的汇聚融合，并通过预处理技术来提升数据质量，在将从外部获取的数据与内部已经完成去标识化或匿名化处理的数据进行合并分析的过程中，海量的数据分析处理结果可能导致已经被去标识化或匿名化处理的数据可再次识别出特定自然人，从而被认定为处理个人信息，此时可能存在欠缺处理个人信息的合法基础，不满足透明性等要求的法律风险；另一方面，医疗AI企业在与其他第三方合作开展数据处理活动过程中，虽然提供的是去标识化或匿名化处理后的数据，但是结合合作伙伴掌握的其他数据资源，仍然存在重识别出特定自然人的可能，从而需要承担未获得个人信息主体授权或不具备其他合法基础的情况下向第三方提供个人信息的风险。

医疗AI企业在对数据进行匿名化处

21.去标识化技术可参考《信息安全技术　个人信息去标识化指南》以及美国的《健康保险可移植性和责任法案》(HIPPA)。

医疗AI企业还应该重点关注AI技术算法合规问题，尤其是与自动化决策相关的影响用户权益的问题。

理时，应平衡数据隐私性和可用性，不同应用场景的匿名化机制有所差别，同时随着技术发展，需要定期对匿名化机制和对个人信息风险影响进行评估和更新，并保障匿名化数据不可以复原和关联数据主体，并匹配相应的保障机制。此外，企业应当通过第三方控制手段（例如合同约束），防止第三方直接识别特定个人，如果去标识化数据经重识别后，重新成为个人信息，则应该按照个人信息保护法律法规及相关标准要求，开展数据合规管理。

•算法合规

医疗AI企业还应该重点关注AI技术算法合规问题，尤其是与自动化决策相关的影响用户权益的问题。医疗AI企业将AI技术应用于辅助诊疗、疾病预测、个人健康管理、医疗保险等场景时，不可避免地涉及对患者或普通用户健康信息的分析，并给出辅助诊断或健康管理的结果，或与第三方合作伙伴共同开展商业活动，如在医疗保险场景，将健康状况信息、医疗应用信息、医疗资金与支付信息关联，通过自动化决策技术对相关群体做出拒保或其他不合理的收取高额保费的决策，影响患者或普通用户的合法权益，由此引发患者或普通用户投诉或监管处罚的风险。因此，医疗AI企业首先应该考虑算法及自动化决策透明性的问题，通过自动化决策方式作出对个人权益有重大影响的决定，个人有权要求个人信息处理者予以说明，并有权拒绝个人信息处理者仅通过自动化决策的方式作出决定。此外，医疗AI企业还应该关注算法偏见的问题，数据样本的偏差、算法逻辑的瑕疵、算法设计者动机等因素均可能导致算法产生偏向性结果，医疗AI且应该考察如何合理设置模型筛选、识别后的结果的自动运用，在保障训练算法及模型的保密性的基础上，高度重视自动化决策机制设置的合理性、规则的透明性及可解释性，以避免其对用户合法权益的直接影响。

3.4 第三方管理

数据对外提供包括数据委托处理、共享、转让等不同情形，医疗AI企业应该基于与第三方合作的不同目的，例如数据收集、数据标注、数据清洗、建模分析及数据测试、算法或者模型训练等，明确与第三

医疗AI企业在隐私保护层面受到严格的监管，近两年异军突起的隐私计算则为这一问题提供了全新的解题思路。

方的数据处理关系。对于医疗AI企业而言，日常运营中涉及与第三方合作处理数据的场景主要包括基于商业合作、科研合作目的共享，从医疗机构、研究机构等获取健康医疗数据，或是基于数据标注、存储、处理、分析等专项服务与外部第三方合作。医疗AI企业首先应该识别自身与第三方之间的数据处理关系，签订数据处理协议明确双方的处理角色和权责，尤其应该事先充分审查合作伙伴的数据安全管理能力，事中通过不定期审计等手段约束合作伙伴在约定的范围内使用数据、承担保密义务，事后及时要求第三方合作伙伴删除相关数据，从而全方面保障数据安全。

•隐私计算

由于医疗AI企业可能涉及大量个人健康数据、人类遗传资源信息及其他敏感程度较高的数据，在隐私保护层面受到严格的监管，近两年异军突起的隐私计算（Privacy Computing）则为这一问题提供了全新的解题思路。隐私计算是一种由两个或多个参与方联合计算的技术和系统，参与方在不泄露各自数据的前提下通过协作对各自的数据进行联合机器学习和联合分析，如联邦学习、安全多方计算等。以联邦学习为例，目前相关技术已经在医学影像分割任务中取得了较理想的效果，其既能避免不同的第三方对原始数据的直接访问，也能达到医疗影像获取、预处理、特征提取、检测/分割和高级处理等结果，很好地解决了健康医疗数据的隐私保护问题。在法律和监管层面，隐私计算技术乃至数据交易流通产业所涉及的合规红线目前仍有待观察，在技术层面，要求隐私计算参与方完全避免技术固有的风险也不具有现实可能性，但可以作为医疗AI企业良好实践的方式。隐私计算能降低医疗AI企业在隐私保护层面的合规风险，但是医疗AI企业在尝试发展、使用隐私计算进行研发、测试时，依然需要满足数据处理的一般性要求，如明确数据处理的合法基础，确保不同渠道数据源合法合规，事先开展个人信息保护影响评估，关注算法及自动化决策等风险。

•数据权属

此外，医疗AI企业在与第三方合作时，还应该注重数据权属问题，若数据权属问题存在瑕疵，可能会影响后续数据处

医疗AI企业应该关注自身数据安全管理能力，保障数据收集、存储、传输、使用等全生命流程的安全。

理一系列行为的合法、有效性，包括衍生数据成果的归属等。目前我国暂未就数据权属进行明确的法律界定，但通过对国家层面相关政策文件的解读，可以知悉各方主体能够享有数据持有权、使用权、经营权，符合数据要素流动的特点和需要，并且能够在尊重数据持有主体控制权的同时，促进数据要素流动、加快数据增值。

针对原始数据，医疗AI企业在法律法规规定及用户授权同意或具备其他合法基础的情况下上享有数据处理的权利，医疗AI企业应该审查自身收集原始数据的合法合规性，从而确保自身具备处理原始数据的权利。此外，关于原始数据的知识产权约定，建议双方在最初的合作协议中，在不违反现行法律法规的基础上进行约定。针对衍生成果（研发数据、算法、模型、核心技术等）权属，医疗AI企业应在上述针对原始数据权属评估的基础上，由双方针对衍生成果在数据控制权、知识产权层面的权益归属进行明确约定。通过上述隐私计算的方式开展合作的，应就模型的源代码、模型结构或参数的权属在合作开始前进行约定，以避免后续争议影响模型使用。

3.5 数据安全保障

鉴于医疗AI企业将处理大量健康医疗数据，其敏感程度较高，还可能构成重要数据或国家核心数据，医疗AI企业应该关注自身数据安全管理能力，保障数据收集、存储、传输、使用等全生命流程的安全。

•机构设置

就组织机构设置而言，医疗AI企业应该设置数据管理机构，设置网络安全负责人，在涉及处理重要数据或处理个人信息达到国家网信部门规定数量的，应该设置数据安全负责人或个人信息保护负责人。医疗AI企业还应该根据数据管理战略安排，设置健康医疗数据管理委员会、健康医疗数据管理工作办公室等负责健康医疗数据决策、管理、执行部门，并明确各部门及人员角色相应的职责。

•制度建设

就制度建设而言，医疗AI企业应该设置健康医疗数据分类分级管理制度，制定健康医疗数据内部管理制度体系，覆盖IT信息安全、数据全生命周期管理等核心管理要求，设置应对信息安全事件应急响应制度体系文件，包括响应流程、演练/培训

医疗AI企业应该注重相关技术人员管理和审查，
避免因此导致的数据安全风险。

方案等，并组织进行应急响应培训/演练等。此外，医疗AI企业可以引入专业的第三方，对信息安全管理体系、质量管理体系和信息技术服务管理体系开展ISO、数据安全管理认证（**DSM**）等标准认证[22]。

•管理措施

就管理措施而言，医疗AI企业应该设定访问权限控制措施和流程制度建设、对数据收集和处理实践进行记录并定期进行安全审计，加强对员工的安全意识培训和安全能力考核等；尤其应该注意，对于能够直接接触原始数据的技术人员，如果内部机构设置、数据安全管理制度体系、技术及管理措施不甚规范，可能存在数据窃取、未授权访问数据、数据投毒、数据污染、泄露及非法利用数据等风险，并将直接对前端产品产生影响，医疗AI企业应该注重相关技术人员管理和审查，避免因此导致的数据安全风险。

•技术措施

就技术措施而言，医疗AI企业作为网络运营者，应认真落实网络安全等级保护的要求，对健康医疗业务开展涉及的核心业务系统，开展等保测评及备案，获取公安机关备案证明，并定期开展信息系统测评审计，其中互联网医院的信息系统应实施第三级网络安全等级保护；在数据全生命周期的管理中，应该通过技术措施及其他必要措施降低数据安全风险，将重要的数据进行备份，防范数据丢失风险；建立监控报警机制、灾难恢复机制等、安全事件应急机制，避免数据泄露；实施日志记录和监控，数据脱敏和加密，进行定期安全审核，保障数据整体安全。

PART 004

合规自检要点

结合医疗AI企业业务特征及企业IPO过程中，上交所在问询阶段重点关注的数据合规问题以及提交联交所上市过程中相关企业重点披露的数据合规问题，医疗AI企业应该从以下整体层面考虑自身业务数据合规要点。

22.国家市场监督管理总局及国家互联网信息办公室联合发布了《关于开展数据安全管理认证工作的公告》，鼓励网络运营者通过数据安全管理认证（DSM）方式规范网络数据处理活动，加强网络数据安全保护。

上交所在问询阶段重点关注的数据合规问题以及提交联交所上市过程中相关企业重点披露的数据合规问题，企业应当关注。

类别	上市板块	问题及重点描述	合规自检要点
整体合规要求	上交所	是否存在侵犯患者隐私的情形；	▪ 进行整体合规评估，完成合规自查和整改。
		数据使用是否符合《中华人民共和国数据安全法》等相关规定、是否存在法律风险；	
	联交所	新增大陆地区相关法律法规的要求，披露监管及执法制度不断完善可能带来的风险；	▪ 明确大陆地区相关法律法规，结合立法、执法动态判断自身合规状态。
		新增网络安全审查对业务影响的论述；	▪ 判断是否触发网络安全审查，一般情况下，赴港上市不属于需要主动申报网络安全审查的范畴。[23]
数据收集	上交所	主要产品及核心技术涉及的数据来源及类型、数据获取方式，数据获取是否合法合规；	▪ 直接收集用户数据应： 具备合法基础； 满足透明性要求； 符合最小必要原则； 避免超范围收集； ▪ 从第三方收集数据应： 审查数据源合法合规性； 签署协议约束双方权责； ▪ 从公开渠道收集数据应： 审查数据源合法合规性； 审查爬虫技术的合法合规性。
		在数据使用中是否需取得相关方的许可或授权、相关授权是否完整；是否存在超出授权范围使用数据的情形；	
	联交所	新增披露第三方数据源准确性可能带来的风险；	
		新增关于数据收集（直接收集、通过业务合作伙伴收集）的业务合规描述；	

23.赴香港上市属于赴境外上市，不太可能被视为“国外上市”，不属于《网络安全审查办法》第7条规定的赴国外上市的情形，且截至目前也没有发生过对港股上市企业的网络安全审查。

类别	上市板块	问题及重点描述	合规自检要点
数据存储	上交所	主要产品及核心技术涉及的数据存储方式；	▪ 满足数据最小必要存储期限； ▪ 满足数据存储安全要求； ▪ 满足数据本地化存储要求（视情形）； ▪ 满足数据跨境传输要求。
		发行人关于数据的采集、存储及使用与同行业可比公司是否存在差异；	
	联交所	更新从数据存储等方面论述采取何等措施加强数据安全保护；	
数据使用	上交所	数据使用是否合法合规；	▪ 保障数据质量； ▪ 保证数据匿名化有效性，避免数据重识别； ▪ 算法合规要求： 满足透明性； 避免算法偏见； 保障用户行权。
		在数据使用中是否需取得相关方的许可或授权、相关授权是否完整；是否存在超出授权范围使用数据的情形；	
	联交所	详细描述去标识化技术情况；新增披露去标识化数据集重新标识可能带来的风险；	
		详细描述算法和模型部署情况；	
第三方管理	上交所	通过科研合作产生数据集或基于真实医疗业务数据开展技术的，在数据使用中是否需取得相关方的许可或授权、相关授权是否完整；	▪ 明确与第三方的数据处理关系； ▪ 与第三方签署协议明确双方权责； ▪ 开发AI新技术，保障数据处理安全及隐私安全； ▪ 注重约定数据和知识产权的权益归属。
	联交所	更新关于因第三方合作伙伴泄露或滥用用户数据带来的相关风险表述；	
		新增关于第三方的数据收集、存储，与第三方签署协议情况以及内部政策的描述；	

类别	上市板块	问题及重点描述	合规自检要点
数据安全	上交所	是否建立有效的内部控制制度确保业务开展中涉及的数据合规性；	▪ 机构设置 审查是否设置有效的数据安全管理机构，是否设置负责健康医疗数据决策、管理、执行的相关部门。 ▪ 制度建设 审查是否设置有效的内部控制制度，包括但不限于数据安全、个人信息保护等； ▪ 管理措施 审查是否实施有效的管理措施，包括但不限于人员管理、权限管理、定期审计等。 ▪ 技术措施 审查是否实施有效的技术措施，包括但不限于完成等保测评及备案、进行安全监测等。
		共建大数据平台模式下，相关数据的获取、管理和使用是否符合《中华人民共和国数据安全法》等相关规定、是否存在法律风险，与同行业可比公司是否存在差异；	
	联交所	更新数据保护政策、数据保护解决方案、与数据保护有关的其他措施等内容；	
		详细描述开展等保备案情况；	
		详细描述公司内部针对数据安全和个人信息保护的内部控制系统情况；	
		详细描述公司内部数据合规组织架构情况；	
		新增披露各业务如何经审阅确认后在重大方面符合数据保护和隐私相关中国法律法规。	

表8：医疗AI企业IPO合规自检要点

陈际红
合伙人
知识产权部
北京办公室
+86 10 5957 2003
chenjihong@zhonglun.com

数字经济时代科技企业上市数据合规指南——基于2021年度(申报)上市案例的分析

张诗伟 蔡鹏 王梦迪[1]

数据合规已成为数字经济时代科技企业申请上市的最重要的法律关口之一。本文从2021年度最新（申报）上市案例出发，在梳理、分析相关证券监管审核和问询等基础上针对数据业务全生命周期的各个环节形成此数据合规指南。

数据被称为二十一世纪的“石油”。而随着互联网、大数据、云计算、人工智能、区块链等技术加速创新，日益融入经济社会发展各领域全过程，[2]更形成所谓数字经济。而数据作为数字经济的核心生产要素，其合规性问题已成为制约数字经济是否能实现良好发展的根本前提，是以对数据保护的重视程度已不亚于前数字经济时代对产权保护的重视程度。数据合规无小事，小则涉及个人信息和隐私，大则涉及国家安全和社会公共利益。中国的相关法制建设也迅速跟上。目前基本法律层面已经形成以《民法典》为核心，《网络安全法》、《数据安全法》、《个人信息保护法》三驾马车并行的数据保护合规立法体系。在行政法规、规章以及规范性文件层面，相关规定更是密集出台，（个人信息）数据合规保护规范体系日益丰满成型。[3]随着监管的逐步深入，相关执法或专项治理行动也不断见诸于报章。[4]强监管背景之下，企业也面临越来越严格细密的数据合规要求和法律责任，包括民事责任、行政责任（主要为被通报、产品被下架、企业及直接责任人被罚款、暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照等）甚至刑事责任。[5]

企业申请IPO上市所需过的最重要的法律关口无疑为合规关。就科技企业而言，无疑数据合规是重要的关口之一。相关拟上市公司在境内外申请上市，被证券监管部门问询的家数和次数也呈逐年上升趋势。[6]而数据合规不过关问题有时更直接成为申请上市的实质性法律障碍。[7]相关拟上市公司务必高度重视数据合规问题。根据我们的相关经验和研究，现有相关企业主要风险主要在数据采集、使用、管理以及共

1.感谢李清仪、严培晏、陈雨婕在本文写作初期的整理和补充。
2.习近平：《不断做强做优做大我国数字经济》，载2022年第2期《求是》，http://www.qstheory.cn/dukan/qs/2022-01/15/c_1128261632.htm。
3.比如自2020年10月1日起实施的《个人信息安全规范》和近日出台、将于2022年2月15日起实施的《网络安全审查办法》，以及国家互联网信息办公室于2021年11月14日发布的《网络数据安全管理条例（征求意见稿）》。
4.2019年起，工信部及各省市通信局持续开展APP侵害用户权益专项整治行动，加大对APP治理的常态化执法力度，并表示对APP违规行为将持续保持高压震慑；2021年7月，在前期APP专项整治的基础上，工信部决定开展互联网行业专项整治行动，主要聚焦扰乱市场秩序、侵害用户权益、威胁数据安全等四方面8类问题，涉及22个具体场景。2021年10月工信部持续开展APP专项整治，坚决下架408款拒不整改的APP。2021年12月9日，工信部在官方网站发布通报，称依据《个人信息保护法》《网络安全法》等相关法律要求，对106款App进行下架，许多知名APP在列。
5.参见《数据安全法》第四十五条、《数据安全法》第四十六条。
6.根据不完全统计，仅就相关企业境内A股IPO而言，受到相关问询的2021年共有32家、2022年共有44家。另外，文章标题为人工智能等行业公司，实际上，随着数据对经济生活越来越深的渗入，越来越多行业的企业业务也都涉及数据处理，因此也都会涉及数据合规问题，比如互联网金融公司、电商公司、快递公司、外卖公司、教育公司、医疗公司等等，更别说专门的数据服务公司或专门的或综合的互联网平台公司。
7.如北京墨迹风云科技股份有限公司。

享(流转)这四个包含在数据全生命周期的环节中。同时,就上市招股说明书等法定文件的信息披露而言,还包括对前述各环节相关情况充分的风险披露。本文选取了2021年度中的9个案例,在梳理、分析相关证券监管问询、拟上市企业的答复以及相关招股说明书等公开披露文件基础上形成该数据合规指南。

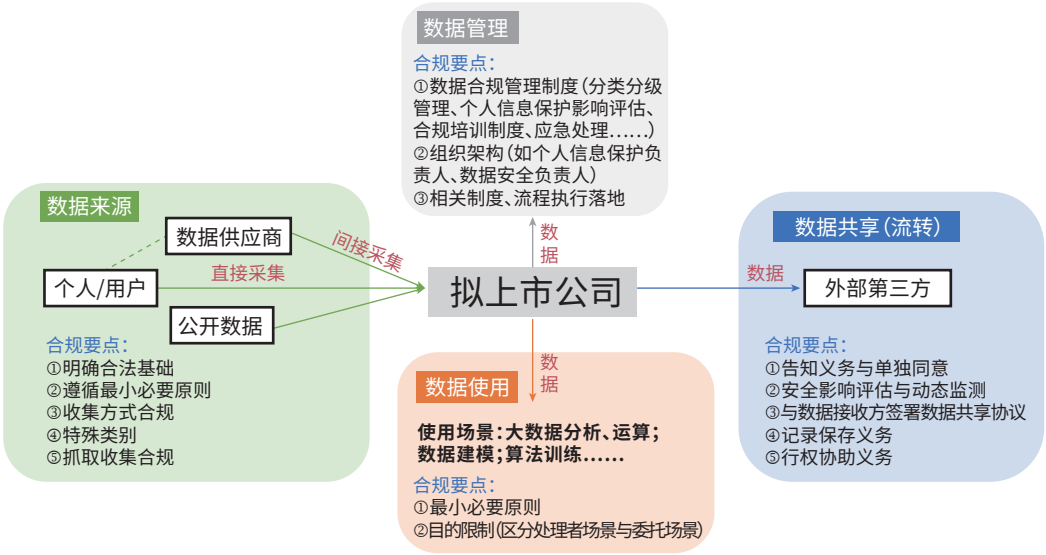


图:企业数据合规全构成图

把好数据来源合规关，确保获取/采集数据的途径、方式均合乎相关法律法规的要求，就把好了数据合规的第一道关口。

PART 001

数据采集合规

数据的获取/采集是数据业务的起点和入口，解决的是数据来源合规性问题，把好数据来源合规关，确保获取/采集数据的途径、方式均合乎相关法律法规的要求，就把好了数据合规的第一道关口。在当前违法违规收集使用个人信息问题仍然突出的态势下[8]，该问题自然也成为上市审核实践中最关注的问题。数据的采集分为直接收集和间接收集。直接收集指拟上市公司直接第一手采集C端信息，而不通过其他方共享或者委托处理的方式获得个人信息。而间接收集与之相对，指拟上市公司不直接对C端，而是一般通过直接收集方共享或者委托处理的方式获得个人信息，相关问询及回复情况如下表：

8.比如根据相关通报，前述2021年12月9日下架的106款App中，有96款存在违规收集个人信息的问题，占比高达90.6%。

在当前违法违规收集使用个人信息问题仍然突出的态势下，数据来源合规性问题自然也成为上市审核实践中最关注的问题。

序号	公司名称	具体问询内容	具体答复内容
1	旷视科技	(2) 发行人**自身**核心技术（如算法的训练、系统的搭建等）是否涉及大量的数据的应用，如是，相关**数据的来源及其合规性**； (3) 发行人**对外**提供的产品（或服务）是否涉及数据的采集运用，如是，说明**数据的来源及其合法合规性**； (5) 发行人的数据来源中是否包含**向供应商采购**，如是，请说明是否在**相关合同中约定数据合规的条款或措施……**	(2) 发行人核心技术研发过程中使用的数据来源的合规管理措施如下：1、配合式采集……2、公开数据集…… (3) 发行人业务及产品（或服务）在消费物联网、城市物联网、供应链物联网三大核心场景下的数据采集运用情况： ①消费物联网、城市物联网 **发行人不参与产品在客户侧的运营**，未经**客户授权及同意**，发行人无权接触客户运营中产生的数据，因此**发行人不涉及数据的采集与运用……** ②消费物联网 **移动终端类解决方案中**，发行人**仅提供技术工具而无法访问移动设备终端上数据；云端SaaS类解决方案中**，发行人在与客户签署的业务合同及线上平台注册服务协议中，均**明确要求客户应确保在合法、正当、必要的前提下使用发行人提供的产品与技术能力，涉及人体相关数据的，客户还应提前取得终端个人用户的明确授权同意**，授权范围至少覆盖：1）**用户知悉并同意客户收集其个人信息**，并由客户将前述信息**提供给发行人**；2）**用户知悉并同意发行人有权从客户获得其个人信息，用于向客户提供相应服务**。按上述要求，由客户在其自有APP与网页的注册流程上，提示隐私政策并获得终端个人用户的授权同意，并据此收集相关数据。 (5) 报告期内，发行人的数据来源中不包含向供应商采购数据的情形。……对于提供配合式采集服务的供应商，发行人会与供应商签订**发行人标准的数据服务协议**，在协议中**供应商承诺确保其向发行人提供的服务符合中国法律法规和/或可能涉及的相关国家/地区法律法规要求；涉及个人数据的，符合适用地法律。供应商提供数据采集服务且需要取得相关数据主体书面授权同意时，均承诺按照法律法规要求，取得数据主体书面签署的授权书**。

序号	公司名称	具体问询内容	具体答复内容
2	云从科技	(2)发行人产品的研发、生产及使用过程中涉及到的**数据获取**、使用情况，**数据获取方式及其合规性**，是否获得相关数据主体的**明确授权许可**，授权许可是否存在**使用范围、主体或期限等方面的限制……**是否存在获取、使用相关数据时**侵犯个人隐私或其他合法权益**的情形……发行人业务开展及**人脸信息收集**等是否符合《个人信息安全规范》等相关法律法规的规定……	发行人研发、测试环境的数据**主要来源于数据供应商或互联网已经公开的开源数据、其他明确授权的自然人、发行人员工**。发行人从数据供应商处取得个人数据时，**要求数据供应商承诺数据来源合法且已获得了个人信息主体的明示的授权并且供应商依据该等授权有权按照协议约定将相关数据提供给发行人用于产品研发**，授权许可一般约定了授权信息的范围、收集目的、信息提供对象的范围等内容，但未约定授权期限；**发行人在从个人信息主体处直接取得相关数据时，通过授权形式依法取得了个人信息主体的明确授权**，授权许可一般约定了**授权信息的范围、信息提供对象的范围、授权期限**等内容。
3	观想科技	(2)补充披露智能数据采集终端、装备离线数据采集终端采集的**数据内容，合同中对于数据收集……的具体约定……**	在**数据收集**功能上……不存在发行人采集客户数据的情形；
4	嘉和美康	请发行人律师对发行人相关数据的**采集**……是否合法合规……并发表明确意见。	①发行人核心技术涉及的数据……来源于医院内部业务系统，由发行人相关产品在医院现场进行生产、获取……**均部署在医院内部服务器上，无医院授权外部无法访问。**②发行人通过科研合作产生的数据集……是一组医疗领域数据元的集合，不涉及真实医疗业务数据。

序号	公司名称	具体问询内容	具体答复内容
			③对于基于真实医疗业务开展涉及的数据……**发行人通过与医院签署合同的方式获得授权**，在**合同约定范围内**提取去隐私的数据样本作为交付系统开发或技术验证的基础数据……④对于基于医学研究项目涉及的数据，经由项目主管单位的医学伦理委员会进行伦理审批后方可启动研究项目。研究项目涉及患者数据的，**将征求患者同意，并签署知情同意书，知情同意书会明确告知患者的数据收集范围以及将来数据的用途**。发行人作为信息系统的提供方，会与项目组签署**保密协议……**
5	零点有数	（2）数据集成及采购的数据中，是否存在**未经授权获取**用户数据的情况，获取个人数据是否对用户有明确提示、收集的数据**是否限制在必要的范围内、是否仅概括性提示**收集用户信息……或存在**未经其他平台的授权直接收取**数据的行为；	1、发行人业务所用数据中，不同数据的取得对于用户授权和提示要求不同：（1）**样本调查数据和交互数据**涉及的个人信息主要包含个人的性别、年龄、收入水平、教育程度等，仅因互动便利和质量复核的需要，才会了解受访者的姓氏/姓名和联系方式，并**严加保密，不作为业务数据使用**。（2）**巡查数据**……无需取得个人信息主体的授权同意。（3）公司采购的大数据为加工处理过的数据集或分析结果，不涉及任何能够识别或关联到特定自然人的个人信息及个人敏感信息……**公司取得大数据无需取得个人主体的授权或对用户进行提示**。 2、**发行人已明确告知收集信息的范围及使用用途而非概括性提示：** 发行人……**明确告知了发行人收集和使用相关个人信息时对应的处理规则……并取得了相关信息主体（及用户）的合法授权**。因此，发行人**有权在相关信息主体（及用户）授权个人信息的使用目的、方式和范围内，对相关数据进行合理的使用和处理……** 3、发行人…**不存在未经其他平台的授权直接收取的行为。**

序号	公司名称	具体问询内容	具体答复内容
6	云天励飞	(2) 视觉人工智能技术的初始训练、迭代更新、模型训练上所需的大量数据的具体来源，发行人在场景应用过程中是否接触、收集、利用**人脸数据信息**，数据采集和使用过程中是否获得被收集者许可，是否存在侵犯个人隐私、肖像权等权益的情形，发行人业务开展过程中涉及到数据获取……是否合法合规……	(1)初始训练、模型训练数据来源……主要包括在经员工授权同意的前提下向员工采集数据、向专业数据供应商采购。 (2)迭代更新数据来源 ……涉及重新训练的情形下，发行人将派技术人员到客户现场直接进行调试，数据来源于客户。调试完毕后，数据无法由发行人的技术人员带走。 (3)具体数据来源:报告期内，发行人获取数据方式主要包括在经员工授权同意的前提下向员工采集数据、向专业数据供应商采购以及使用互联网公开数据集数据，不存在违法 收集数据的情形。 报告期内，发行人与相关供应商签订的数据采购合同均约定了供应商须遵守中国法律关于采集人脸面部信息规定的相关条款，须确保采集方式合法合规(**应征得被采集人同意并告知数据用途**)，因供应商违反法律规定所产生的责任由供应商自行承担。根据上述合同约定及相关法律法规规定，供应商承担数据合法合规性的法律责任，发行人在数据合规性层面没有连带法律责任。
7	合合信息	(1) 发行人各项业务及研发分别获取、存储、使用哪些数据，对应的数据来源、数据权属； (2) 发行人向个人供应商采购数据的主要内容、比例及原因； (3) 发行人自动化访问获取的企业数据如何确保来源合法性，发行人调查供应商及数据来源合法性的具体方式及有效性。	(1) 发行人获取数据方式多元化，C端主要通过APP获取。其大数据业务获取主要有四种途径，分别是向供应商采购的企业数据、数据与数据互换、广告与数据互换、自动化访问获取。 (2) 发行人采取了多重方式确保自动化数据采集的全过程的数据合规性，包括数据采集之前完成合规评估，流程评估以及制落实定有关制度，确保抓取的网站变化不至于影响评估结果。发行人同时制定了有关制度和流程，确保抓取的网站均为访问清单内，并且为公开信息。 (3) 对于外采数据，发行人进行了一系列内控措施和采购流程管理，确保数据的合法合规性。

证券监管部门在问询时，在数据收集环节关注的主要问题在：数据收集合法性基础；最小必要原则；数据收集的具体方式。

序号	公司名称	具体问询内容	具体答复内容
8	金智教育	(1) 发行人是否可以通过向客户提供公司主要产品及服务而直接或间接获得相关学校、师生的具体数据和**个人资料等信息**，如是，请说明**获取条件、获取方式和信息范围；** (2) 上述数据和信息**获取方式**是否**合法合规**，是否**符合相关监管要求或保密约定；**	发行人各项产品及服务涉及的信息获得情况如下……综上所述，报告期内发行人收到的核查整改通知/通报已及时整改完成。发行人上述数据和信息的获得**已征得用户授权**，获取**方式符合《网络安全法》《信息安全技术个人信息安全规范》等法律及国家标准的规定要求，符合网络信息安全的监管要求**，以及发行人与客户之间的**保密约定**。
9	商汤科技	根据《招股书》中所列举的“企业方舟”之开发，公司收集的数据包括面部识别数据、现实世界场景的图像及视频数据、以及特定物体的图像及视频数据三类。其中，就面部识别数据而言，公司**仅在获得授权的情况下自行采集**。而对于其它类型的数据，其来源途径主要包括：自行收集来源（包括手动拍摄的照片及视频、街头风景及公共场所的物品）、第三方供应商、客户、以及公共数据集。[9]	

总结上表可知，证券监管部门在问询时，在数据收集环节关注的主要问题在如下方面：

1）数据收集（数据来源）是否具备合法性基础；

2）数据收集是否遵循最小必要原则；

3）数据收集的具体方式是否满足法律的合规要求；

4）不同类别个人信息的收集是否满足其具体和相应的合规要求。

据此，我们理解，拟上市企业的相关

9.和A股审核不同，香港联交所上市相关问询和回复并不公开，相关内容主要体现为招股书的相关披露。

在我国个人信息保护相关规则几经演变的过程中，最小必要原则一直是个人信息收集和处理的核心要求。

应对解决措施为：

（1）明确合法基础

《个人信息保护法》第十三条规定，处理个人信息应当具备相应的合法性基础；或基于个人信息主体的同意，或基于订立、履行作为一方当事人的合同所必需等。对拟上市公司而言，应根据数据收集场景的不同，梳理匹配对应不同的合法基础，从而进一步履行数据收集环节的相应合规义务。例如，如果拟上市公司是基于个人信息主体的同意收集个人信息，则在数据收集前首先应告知个人信息主体数据处理的目的、方式、范围、保存期限等信息；其次如涉及敏感个人信息的收集，则应获取个人信息主体的单独同意等。

（2）遵循最小必要原则

在我国个人信息保护相关规则几经演变的过程中，最小必要原则一直是个人信息收集和处理的核心要求。《个人信息保护法》第六条规定，收集个人信息，应当限于实现处理目的的最小范围，不得过度收集个人信息。对拟上市公司而言，根据不同的数据收集场景，首先应明确数据收集的目的，进而确定数据收集的范围、类型等。例如，人工智能企业在收集数据用于算法训练过程中，如仅收集一般个人信息或者脱敏后的信息即可满足算法训练的需求，即应避免过度收集其他类型的个人信息。

（3）收集方式应满足合规性要求

结合上述应对策略（1），在确定数据处理的合法基础后，拟上市公司在收集数据时，应根据数据收集方式的不同，履行不同的合规义务。具体而言，如拟上市公司是基于个人信息主体的同意收集数据，则应避免捆绑授权、强制授权等情形发生；如拟上市公司是从数据供应商处购买获得数据，则首先应对数据供应商进行尽职调查，明确其数据来源合法合规；其次在与数据供应商的合作协议中明确双方的数据处理关系，以及各自的权利义务。对数据供应商做到事前到事后的全流程审查，防范数据安全风险和影响。

（4）特殊类别个人信息的收集

基于不同的业务领域，拟上市公司收集的数据类型也存在差异。除一般个人信息（如姓名、性别、年龄等）之外，可能还会涉及面部数据等生物识别信息、医疗健康

法院在考量抓取行为的正当性时，基于既往的认知总体上会偏保守。

信息、公开数据等，前述不同类型的数据会具有相应不同的数据保护要求（如《最高人民法院关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定》、《信息安全技术健康医疗数据安全指南》等）。因此，拟上市公司应结合自身的业务特点，识别业务需求中不同类别的数据，满足数据收集面临的不同监管要求所规定的合规义务。

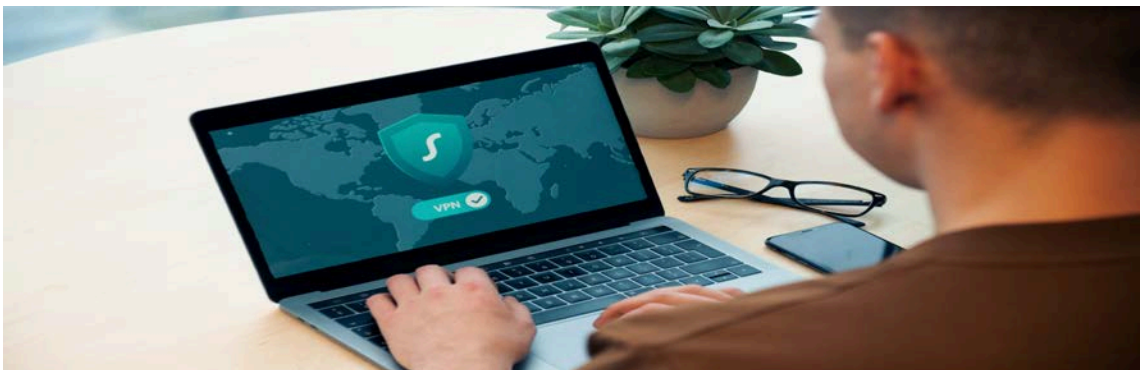
（5）对抓取收集方式的合规要求

数据抓取是一种较为常见的收集方式，人工智能类拟上市公司会采用抓取公开数据的方式，进行结构化处理并以此训练算法和进行深度学习。而数据抓取面临的法律问题和挑战较多，不仅涉及数据权属的问题，而且涉及抓取方式合规性以及被抓网站和ROBOTS协议的限制等问题。近年来，有关此类数据抓取的诉讼数量呈明显上升趋势，有关平台基于各种利益考虑，会主动提起侵权诉讼。而法院在考量抓取行为的正当性时，基于既往的认知总体上会偏保守。因此，拟上市公司需要在开展此类业务时，进行充分的法律论证和风险识别，并进行合规评估和项目监管，防止因抓取行为侵犯平台合法权益，而导致不利诉讼的发生。

PART 002

数据使用合规

就该问题，具体证券监管部门问询内及拟上市公司答复、相关《招股书》披露如下：



序号	公司名称	具体问询内容	具体答复内容
1	佳创视讯	(5)……是否**超出用户授权范围使用**数据……	尚未答复。
2	旷视科技	(6)结合发行人的产品交付及部署模式，说明发行人的产品（或服务）中涉及到用户的**个人数据的情形和场景**，该等数据的**运用……及其合规性**	……②消费物联网：云端SaaS类解决方案中，**客户**作为数据控制者，开发、运营面向个人用户的APP或网页产品，**自行履行相关合规义务并对其中涉及的数据处理活动负责。发行人作为服务提供方，已明确要求客户在合法、正当、必要的前提下使用发行人产品，**涉及个人数据的，客户还应提前取得终端个人用户的明确、完整授权同意。
3	云从科技	(2)发行人产品的研发、生产及使用过程中涉及到的**数据……使用**情况……发行人是否存在**超出上述限制使用**数据的情形，是否存在……**使用**相关数据时**侵犯个人隐私或其他合法权益**的情形……	在数据存储、使用过程中，发行人**按照授权许可以及与数据供应商签订的业务合同中约定的范围使用相关数据，不存在超出约定限制使用数据的情形。**另外，对于发行人自智慧商业业务客户处取得的他人个人信息，均在合同中约定，协议终止后，接受一方应返还或清除对方提供的全部保密信息以及任何形式的备份；**发行人在实现协议目的后，均会依约删除相关数据。**
4	观想科技	(2)**……合同中对于数据……使用……的具体约定**，是否符合相关法律法规，是否存在**侵犯隐私行为……**	(2)在数据使用上：……发行人无法获取、使用相关数据。
5	嘉和美康	请发行人律师对发行人相关数据的……**使用**……是否合法合规、是否存在**超出授权范围使用**数据的情形进行核查，并发表明确意见。	发行人为医院提供的业务系统与大数据应用**仅服务**于医院内部数据收集、质控管理、科研水平提升等，均在获得医患双方授权前提下**按照合同约定使用数据**，不存在侵犯患者隐私的情况。

序号	公司名称	具体问询内容	具体答复内容
6	零点有数	(2).....是否超出用户授权范围使用数据.....	发行人严格按照《零点有数隐私政策》及数据安全相关内控制度使用、处理相关数据，**仅将数据用于**基于数据分析的决策支持服务及相关技术研发.....
7	合合信息	报告期内发行人数据管理不完善的具体情形、影响范围、严重程度，是否存在侵权行为、纠纷、潜在纠纷或可能被处罚的情形，目前发行人针对该等不完善情形的具体整改情况及效果，发行人数据合规纠纷的解决机制。	发行人的数据使用合规措施有： (1) 制定了用户个人信息的使用限制以及数据分析需求的处理流程，制定了访问授权流程，在权限管理中遵循职责分离原则。 (2) 公司通过权限管理对核心触点的应用系统及后台支撑系统的访问权限进行限制，以保护用户个人信息免受未经授权访问、公开披露、使用、修改、损坏或丢失。 (3) 公司制定了数据资源的申请审批流程，并限制了数据库的访问授权。
8	云天励飞	(1)清晰说明发行人业务开展过程中涉及到相关**个人数据、信息**安全的.....利用.....的情况; (2)视觉人工智能技术的初始训练、迭代更新、模型训练上所需的大量数据的具体来源，发行人在场景应用过程中是否.....**利用人脸数据信息**.....发行人业务开展过程中涉及到数据.....**使用**是否合法合规.....	.....商场与发行人在合作协议中明确约定所收集人脸识别信息的权利归属，即由商场对所收集的人脸识别信息享有控制权，发行人仅在商场的授权范围内作为人脸识别信息的受托处理者，**按照商场的指示与安排进行信息处理活动。未经客户授权及许可，发行人无法使用该等数据.....**
9	商汤科技	根据《招股书》，公司按照所收集数据的限制用途及限制储存时间对数据进行标注；**任何数据使用均须事先在数据平台上提交申请，只有在取得该数据相应机密水平的批准才可使用**；任何数据训练或测试将在数据平台上进行，且**不得在平台之外使用该数据**。同时，根据公司内部政策，**公司仅根据需要在授权范围内在公共云服务器上处理包含个人信息的最终用户数据，**而不将有关数据下载至内部数据平台。	

基于收集数据（来源）的不同，在数据使用过程中，
数据处理者需要履行的合规义务也存在差异。

由上表可知，证券监管部门在问询时聚焦于“拟上市公司在使用数据时是否满足最小必要原则，是否超出相应的授权范围使用数据，是否存在侵犯个人隐私或其他合法权益的情形”。基于收集数据（来源）的不同，在数据使用过程中，数据处理者需要履行的合规义务也存在差异。基于此，结合《数据安全法》与《个人信息保护法》，我们总结梳理应对解决策略如下：

（1）直接收集数据使用应遵循最小必要原则

如果拟上市公司直接向用户收集数据，则在数据使用过程中，应当在数据收集时向用户明示数据处理目的，并需要在授权范围内使用数据。数据处理者不得超出处理所必须的授权范围，或者超出数据处理目的去使用数据，否则，则极有可能违反最小必要原则，进而侵犯用户的个人信息权益、隐私等。

举例而言，如个人信息主体同意收集其手机号仅用于账户注册，拟上市企业则不应使用其手机号码开展个性化推荐/精准营销活动；如果拟上市企业基于订立、履行作为一方当事人的合同所必须而处理数据，则仅能使用实现合同目的所需的最小范围内的数据；如拟上市公司使用收货人姓名、联系方式及收货地址即可实现作为线上交易一方当事人合同中的产品交付目的，拟上市企业则不应额外使用银行账号信息、身份证号等信息以完成产品交付；如基于按照依法制定的劳动规章制度和依法签订的集体合同实施人力资源管理所必需处理数据，应仅使用实现实施人力资源管理目的所必需的最小范围的数据。

最小必要原则贯穿于数据处理全生命周期，拟上市公司应当制定有关规范和评估工具，对敏感场景下是否遵循了此项原则，进行针对性和周期性的评估。

（2）间接收集数据的使用应遵循目的限制

在间接收集数据的场景下，又进一步区分处理场景和委托场景的不同做不同应对：

a.在处理场景下，可以进一步区分为单独处理与共同处理。拟上市公司间接收集数据后，可以自行决定数据处理的目的和方式，则其作为独立的数据处理者使用数据；如需与数据提供方共同决定数据处理的目的和方式，则双方作共同数据处理

拟上市公司在与数据提供方订立数据委托处理协议时，应着重关注委托人对受托人数据处理活动的要求和限制。

者使用数据。在前述两种场景下，数据合规义务的相同之处在于，拟上市公司的数据使用活动首先应受制于其与数据提供方之间约定的数据处理目的（数据处理目的将会对拟上市公司数据使用的具体方式、场景等产生重要影响，因此如何限制或者约定不同数据处理者的目的是拟上市公司数据合规中的难点问题，必要时，拟上市企业可以聘请外部专业机构对双方的数据合作进行相应评估与协助，从而明确数据处理目的，避免对业务发展产生限制或者不利影响）；不同之处在于，在单独处理场景下，拟上市公司应自行承担数据处理义务（如保障数据使用的安全等），如数据使用活动侵害个人权益造成损害时的，应依法自行承担责任；而在共同处理场景下，拟上市公司应与数据提供方根据双方的约定承担各自的数据处理义务，如数据使用活动侵害个人权益造成损害时的，各方应依法承担连带责任。

b.在委托处理场景，拟上市公司基于数据提供方的委托而处理数据，数据提供方是委托人，拟上市公司是受托人，双方首先应通过订立数据委托处理协议的方式，对数据处理的目的、期限、处理方式、数据种类、保护措施以及双方的权利义务进行明确约定；在后续的数据使用中，拟上市公司应遵循合同约定的目的使用数据。如违反与委托人的约定，将可能会面临违约等相关风险。如数据使用活动侵害个人权益造成损害时的，委托人应自行承担责任。《个人信息保护法》中也明确委托人对受托人数据处理活动的监督义务。如何实际限制和控制受托人的数据处理活动，将会直接影响拟上市公司数据处理活动的范围和具体场景。因此，拟上市公司在与数据提供方订立数据委托处理协议时，应着重关注委托人对受托人数据处理活动的要求和限制，避免约定不明或者约定过于严苛导致对实际业务开展造成不利影响。

PART 003

数据管理合规

数据管理是保障拟上市公司平台内数据存储、安全防护、防止数据泄漏等方面制度、措施之集合。相关证券监管部门问询内容及答复、相关《招股书》内容披露如下：

数据管理是保障拟上市公司平台内数据存储、安全防护、防止数据泄漏等方面制度、措施之集合。

序号	公司名称	具体问询内容	具体答复内容
1	旷视科技	(4) 发行人**保证数据**采集、清洗、**管理**、运用等各方面的**合规措施**; (6) 结合发行人的产品交付及部署模式,说明发行人的产品(或服务)中涉及到用户的**个人数据的情形和场景**,该等数据的**运用、管理及其合规性**。	根据发行人书面说明,发行人主要从**技术、制度和人员机构三个维度**提升数据采集、清洗、管理、运用的合规性,具体措施如下:1.技术维度……2、制度维度:发行人**制定了不同层级、不同侧重的数据安全与合规相关内部制度体系……**3、人员机构维度:发行人CTO下设安全部……发行人CTO下设信息技术工程部……发行人CFO下设法务部……4、人员管理方面,发行人采取以下措施提升数据合规性:①协议约束:**发行人员工均已签署保密协议**,其中包含个人信息保护相关条款。②培养合规意识:发行人定期、不定期**组织员工进行有关个人数据安全保护的培训及考试,对新员工进行有关数据安全的入职培训;**不定期对关键岗位人员进行**额外的安全培训与交流,**并**补充技术考核与审查。**③**推行奖惩措施**:发行人已制定并实施数据泄露等信息安全事件的奖惩规则,对于违反相关规定的人员进行惩戒。④管控人员权限:发行人**根据员工的工作职责配置必要、最小的系统访问权限,**定期对人员的访问权限进行审核,员工**离职前将进行信息安全核查;外部人员访问**受控区域前**需向对应管理部门提出书面申请,经审批**后,方可授权进入。
2	观想科技	(2)**……合同中对于数据……存储的具体约定,**是否符合相关法律法规,是否存在**侵犯隐私行为……**	(3) 在数据存储上:相关数据均由客户按照我国相关保密法规要求进行存储。

序号	公司名称	具体问询内容	具体答复内容
3	嘉和美康	请发行人律师对发行人相关数据的存储……是否合法合规……并发表明确意见。	发行人核心技术涉及的数据……**均部署在医院内部服务器上，无医院授权外部无法访问……**发行人作为信息系统的提供方，会与项目组签署保密协议，保证在系统运维过程中，对接触的隐私数据执行保密约定。发行人在产品正式上线运行前，都是通过测试数据进行系统验证；一旦产品正式上线，**后台数据库管理密码将交付客户，并确认客户及时修改密码**；后续产品的运维过程中，**如需要进入系统后台，则通过客户授权（最小授权原则）后，并在可实时监控的环境下（如运维堡垒机）进行。**发行人与客户签署的技术服务合同含有**业务保密条款**，发行人员工与发行人签署的保密协议也包含员工对发行人业务对象的保密义务……
4	零点有数	2.发行人针对上述数据使用、隐私及安全方面的**内部控制措施及其有效性，**是否存在泄密及其他数据使用风险	（2）数据传输与存储方面，发行人要求数据传输过程中必须选择**安全的传输渠道……数据存储采取分类分级管理制度**，针对不同级别的信息制定不同等级的安全策略，并对涉及个人信息的敏感数据库加强权限控制和安全审计。（3）网络安全方面，发行人建立了**网络防火墙**，采用**内外网分离措施……针对外网访问建立日志审计及预警机制，**以最大程度避免网络安全事件的发生。（4）数据安全管理制度方面，发行人已制定了包括……与数据安全和隐私保护相关的**内部控制制度，**并已切实定期开展数据使用、隐私及安全方面的**培训**，加强员工数据合规意识，确保上述各项内部控制制度的有效实施。

序号	公司名称	具体问询内容	具体答复内容
5	云天励飞	(2)视觉人工智能技术的初始训练、迭代更新、模型训练上所需的大量数据的具体来源……发行人业务开展过程中涉及到数据……管理……是否合法合规，发行人是否已建立**完善的防泄密和保障网络安全的内部管理制度，该等制度的执行是否有效**，发行人**是否需要取得开展涉密类业务的资质或许可。**	发行人已经在技术层面和制度层面建立完善的防泄密和保障网络安全的**内部管理制度**，具体如下：(1)在技术层面：1.公司储存数据、训练模型等工作全部放在**核心内网，与办公网络及外部的公开互联网实现物理隔离……**2.硬件控制方面，公司研发人员及 IT 人员用户端的电脑装有**防泄密安全软件**……存储服务器有软件快照备份机制。3.在机房的管理方面，非机房管理人员无法进入。在信息获取方面，遵循**信息分级**以及**最小控制权限原则为员工授权。** (2)在制度层面：1.公司内部组建了**信息安全委员会和信息安全管理小组，**并制定了**一整套信息安全管理制度**…… 2.发行人组成了……**信息安全委员会**……报告期内，发行人未出现数据泄露等方面的事故，该等制度的执行有效。3.公司已取得了……信息安全管理体系认证，认证范围包括……
6	合合信息	报告期内发行人数据管理不完善的具体情形以及解决方案	发行人发现了管理漏洞后，采取的主要管理措施包括： (1) 在数据存储与销毁方面，公司定义了个人信息的存储方式、存储期限，以及个人信息的到期删除或匿名化处理标准。公司制定了个人信息的删除流程，在接收用户注销申请后，数据库和后台支持系统对用户个人信息进行物理删除。 (2) 为确保将数据合规管理落到实处，发行人制定了覆盖整个数据生命周期管理的相关制度，包括数据采集、数据使用、数据访问权限控制、数据导出和数据删除相关的制度。并设计了相应的管理流程，实现全数据生命周期的管理。

序号	公司名称	具体问询内容	具体答复内容
			(3) 规定了公司合规与信息安全的组织架构，明确了安全与合规管理委员会在业务合规、网络安全、数据安全和用户个人信息保护等方面的责任以及安全与合规部和各事业部的职责，并规定网络安全、数据安全和个人信息保护等相关责任机构的汇报层级要求。
7	金智教育	(3) 发行人对相关信息的**储存**及使用情况……是否存在相关信息泄露的情况，是否存在侵犯用户隐私及数据的情况…… (4) 发行人关于信息安全与数据保护的**相关内部控制制度及执行情况**，必要时请完善相关风险提示。	发行人关于信息安全与数据保护的相关内部控制制度及执行情况发行人建立了**企业网络信息合规管理体系**，确保数据收集、存储、传输、应用等的安全与合规，基于此制订和执行的主要内部控制制度包括……发行人**已建立的信息安全与数据保护相关内部控制制度**覆盖了……此外，员工入职时即进行《员工手册》及内部控制制度的**教育和培训**，全体员工均签署了**《保密和知识产权协议》**，明确员工应对公司承诺负有保密义务的客户和用户信息承担保密义务。 发行人为增强全员数据安全意识、进一步提升公司的数据合规水平、推动落实上述各项内部控制制度，切实开展了多次**信息安全培训活动**，其中包括……
8	商汤科技	根据《招股书》，待数据收集端提交完整的授权资料后，相关数据才可以上传至公司内部的数据平台，并**按照相关数据的机密级别在平台上进行标识**。同时，未经负责人批准，在数据标识过程中公司不得进行标识之外的数据操作，包括但不限于修改、删除、保存或共享。此外，数据在内部使用期限届满时，相关数据将须销毁，并向数据管理部门提供**数据销毁报告**；在数据授权到期时，相关数据将被销毁，而相关数据的**所有副本也将予以删除**。	

证券监管部门关于数据管理方面的关注问题主要集中在数据安全管理建制是否完善、是否实际落实执行等方面。

总结上表可知，证券监管部门关于数据管理方面的关注问题主要集中在数据安全管理（包括但不限于数据存储制度、权限管理、安全漏洞防控等）建制是否完善、是否实际落实执行等方面。基于此，我们梳理相关应对解决策略如下：

（1）搭建数据安全内部管理制度

根据《数据安全法》与《个人信息保护法》的相关要求，数据处理者应当根据数据的处理目的、处理方式、数据的种类以及对个人权益的影响、可能存在的安全风险等制定全生命周期的数据安全内部管理制度和操作规程，保障数据处理活动的安全。整体而言，数据处理者需要制定的内部管理制度包括但不限于数据安全管理制度、数据分类分级管理制度、个人信息保护影响评估制度、数据合作管理制度、数据合规培训制度、数据安全事件应急预案等。对拟上市公司而言，需要依据自身的业务特点、商业模式、处理数据的类型、具体的数据处理活动等整体布局，科学地搭建数据合规内部管理制度体系。合理的数据安全内部管理制度不仅可以保障外部数据处理行为的秩序和合法合规性，而且也可以实现内部数据处理活动的科学、有效、合规地管理。

（2）完善数据安全人员组织结构

对拟上市公司而言，制度建设是数据管理重要的方面，人员组织架构的完善也是不可或缺的部分。《个人信息保护法》明确：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，《数据安全法》则要求重要数据处理者应当明确数据安全负责人和保护机构。对此，拟上市公司应根据处理数据的数量、种类，确定是否需要指定相应的数据安全负责人。指定负责人的同时，公司还应当明确负责人或者负责机构的职责范围（例如监督、管理、上报等职责）。

（3）确保相关制度、流程的执行落地

拟上市企业欲实现企业内部数据安全，以及数据处理活动的科学有效管理，我们建议拟上市公司制定了数据安全管理制度，明确个人信息保护负责人/数据安全负责人及其相关职责以及日常业务经营活动相关必要的支持与协助措施，同时，建立起数据分类分级管理，根据数据分类分级的结果，制定相配套的数据存储、权限控制、访问限制、展示限制等措施，并且在系统、

数据的流转或共享由于涉及外部第三方，也是最容易造成安全隐患和突破合规底线的薄弱环节。

流程中进行落地和执行。

PART 004

数据共享（流转）合规

数据的价值在于使用，其生命在于流动。数据流转，即拟上市公司授权或分享给外部第三方部分或全部获取本公司所有的数据信息，可见广义的数据流转内含了分享的意蕴。但无论是分享还是流动，其前提无疑也都在于安全合规。而数据的流转或共享由于涉及外部第三方，也是最容易造成安全隐患和突破合规底线的薄弱环节。[10]

相关证券监管部门问询内容及答复、《招股书》内容披露如下：

序号	公司名称	具体问询内容	具体答复内容
1	金智教育	（3）发行人对相关信息的储存及使用情况，是否存在**转授权或流转给第三方**的情况……	2、**转授权或流转**给第三方的情况 “今日校园”APP隐私政策明示，若用户选择一键登录、站内信息通知等功能，同时为监测和防止欺诈行为，**经用户同意后，“今日校园”APP将收集**用户的手机号和手机设备标识符（**IMEI、IDFA、Android ID、MAC、OAID**、应用列表信息等），**并共享给友盟、极光、Mobtech等第三方SDK。该等信息共享系经用户同意，**且仅限于用户手机号（不包括姓名、身份号等身份信息）和手机设备标识符，除此之外，发行人没有共享任何学校、师生的具体数据和个人资料信息。
2	商汤科技	根据《招股书》，在数据标识过程中，公司不得……共享（内部平台上的数据）。任何数据训练或测试……不得在数据平台之外进行。	

10.以SDK为例，开发者可以通过调用SDK的方式，为App嵌入地图、广告、数据统计、支付和第三方登录等功能，而无需从头为这项功能编写代码。由于SDK自身的行为具有较强的隐蔽性，因此存在多种安全隐患：或是其自身有安全漏洞问题，或是存在如流量劫持、资费消耗、隐私窃取等SDK恶意行为，或是由于处理者存在无法控制SDK的处理数据的技术可能性，SDK容易基于其自身利益，超范围收集信息主体的个人信息。

拟上市公司应在实现合同约定目的最小必要范围内共享数据，并要求数据接收方在实现合同目的最小范围内使用数据。

综上，我们梳理拟上市公司数据共享方面的合规应对要点如下：

（1）履行告知义务并征得用户单独同意

针对数据共享行为，拟上市公司应当在隐私政策或用户协议中向个人告知接收方的名称或者姓名、联系方式、处理目的、处理方式和数据种类；如基于个人的同意处理数据的，拟上市公司应就数据共享行为征得个人的单独同意。如涉及敏感个人信息的共享，其应向个人告知共享的敏感个人信息类型、数据接收方的身份和数据安全能力，并征得用户的单独同意。根据工信部2021年11月发布的《关于开展信息通信服务感知提升行动的通知》中提出的“双清单”要求，拟上市公司可以在隐私协议中以列表方式明确APP产品与第三方共享的用户个人信息基本情况，包括与第三方共享的个人信息种类、使用目的、使用场景和共享方式等。

（2）安全影响评估与动态监测

拟上市公司在对外共享数据前，应当根据公司内部制定的个人信息安全影响评估制度事先开展个人信息安全影响评估，并依评估结果采取有效的数据安全与个人信息保护措施。在共享之后，应当就数据接收方的相关数据处理活动进行监测和追踪，并对相应情况进行记录。

（3）与数据接收方签署合作协议

拟上市公司应当与数据接收方签署合作协议，明确约定处理数据的目的、范围、处理方式，在数据安全方面明确自身和第三方应分别承担的责任和义务，以及各自应当采取的数据安全保护措施等内容。拟上市公司应在实现合同约定目的最小必要范围内共享数据，并要求数据接收方在实现合同目的最小范围内使用数据。

（4）记录保存义务

拟上市公司应当准确记录和保存个人信息共享的情况，包括共享的日期、规模、目的，以及数据接收方基本情况等。根据网信办发布的《网络数据安全管理条例（征求意见稿）》，提示拟上市公司注意，进行数据共享应当对个人同意情况进行记录，提供个人信息的日志记录、共享重要数据的审批记录和日志记录保存至少五年时间。

（5）行权协助义务

拟上市公司应当帮助个人信息主体了解数据接收方履行义务的情况（例如对个

对数据合规风险的披露，既包括对既存数据合规风险的揭示，也包括对未来潜在数据合规风险的客观分析。

人信息的保存、使用等情况），以及个人信息主体享有的权利，包括但不限于访问、更正、删除、注销账户等。

PART 005

相关数据合规风险的披露

拟上市公司在上市过程中在招股说明书等相关上市申请文件中对数据合规风险应进行充分的披露，既包括对既存数据合规风险的揭示，也包括对未来潜在数据合规风险的客观分析。相关证券监管部门问询和拟上市公司答复及相关招股说明书披露如下：

序号	公司名称	具体问询内容	具体答复内容
1	旷视科技	（5）……结合**《民法典》《网络安全法》和《个人信息安全规范》《数据安全法》《个人信息保护法》等相关规定**，说明相关措施是否能切实保证发行人不出现数据合规风险或法律纠纷。 （7）发行人产品至今是否面临数据合规方面的**诉讼或纠纷；**并请结合**相关公开报道**，说明发行人数据的合规性。	（5）截至本回复出具日，未发现违反《民法典》《网络安全法》《个人信息安全规范》《数据安全法》《个人信息保护法》关于个人信息采集相关规定的情形或出现法律纠纷，未发现数据合规风险。 （7）①截至本补充法律意见出具日，发行人**未面临数据合规方面的诉讼或纠纷**。②虽然部分媒体报道声称发行人的产品（如安全摄像头）未经授权收集人脸信息，**但该等报道混淆了发行人在相关事件中的角色……**③发行人在数据安全与合规方面，已获得多项国内外权威认证认可……
2	观想科技	2）补充披露……是否存在侵犯隐私行为或**行政处罚**的风险；	发行人产品中数据采集、使用、储存的功能**不存在违反法律法规的情形，不存在侵犯隐私行为或面临行政处罚的风险。**

序号	公司名称	具体问询内容	具体答复内容
3	合合信息	核查并说明**发行人境外业务开展**是否遵守当地个人信息和数据安全保护的相关规定，是否存在被境外主管机构处罚的情况或潜在风险。近年关于数据安全、个人信息保护等立法对发行人研发、采购、销售等的影响，发行人业务开展是否符合该等法律法规规定……	1.境外业务方面，公司的APP已符合APP平台相关规定，并在APP中明示《隐私政策》并按照个人信息及数据安全保护的相关规定开展业务； 2.**发行人律师根据 GDPR 的相关规定进行了核查，**其认为公司在 2021 年 3 月 31 日的数据保护及隐私合规没有整改建议。 3.发行人内部的安全与合规管理委员会根据不断更新的数据行业监管、个人隐私保护政策，统筹规划合规与信息安全管理制度体系的维护与持续运作。**基于持续的研究，对公司相关经营管理制度、流程、方案及计划中的数据安全、隐私保护等方面的合规性进行评估和管理，积极提升公司数据安全与合规管理能力。**
4	云天励飞	招股说明书中提请投资者关注**政策制度风险**：人工智能技术被不当使用或被滥用都可能令潜在客户对人工智能解决方案却步，也可能影响社会对人工智能解决方案的普遍接纳程度，引起负面报道，甚至可能违反中国及其他司法辖区的相关法律法规，面临诉讼风险、来自积极股东及其他组织的压力以及监管机构更严格的监管。请结合发行人主要产品及业务模式具体说明面临的上述政策制度风险的具体体现，并客观分析可能对发行人业务及生产经营的影响。	1.政策风险的具体体现 发行人面临的上述政策制度风险的具体体现如下： (1)发行人面向商业用户的产品可能涉及到获取和使用用户隐私数据，如果商业客户未能恰当获得用户数据授权，有可能存在**数据安全**的风险。 (2)《**个人信息保护法**》等与个人信息保护相关的法规正在立法过程中，如果公司产品的使用方未能恰当遵守相关规定可能招致其存在法律风险，进而影响发行人产品推广和使用。 2.对于发行人业务和生产经营的影响……

对于潜在数据合规风险的评估，证券监管部门在问询中对拟上市公司未来潜在的数据合规风险也尤为关注。

而对于既有数据合规风险的披露，证券监管部门要求拟上市公司一方面应披露现有的诉讼或者行政处罚情况，另一方面应披露现有产品和业务模式下是否有导致诉讼或者行政处罚的风险。对于潜在数据合规风险的评估，证券监管部门在问询中对拟上市公司未来潜在的数据合规风险也尤为关注：其会要求拟上市公司根据主要产品和业务模式对未来的政策制度风险可能对业务及生产经营产生的影响进行客观分析。相应的应对解决方式为：

(1) 已有数据合规风险披露

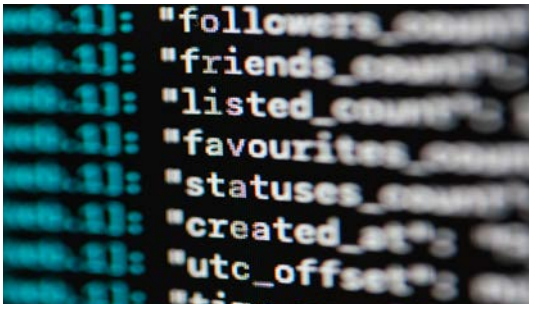
充分评估及披露其是否因数据不合规受过相关的行政处罚、法律纠纷或诉讼以及其对公司业务的影响；对于相关负面舆论报道，也需及时关注与回应，必要时进行进一步相关说明。

(2) 未来潜在数据合规风险评估

未来潜在风险，不仅包括现有商业模式下“灰度”问题如何去解释和改进，也包括由于立法的更新和变化，所带来监管的不确定性考虑。我们认为，拟上市公司应当从持续跟进—积极研判—主动评估—制度落地—意识提升等几个维度去进行建设，形成自身良好的合规闭环体系，以及从上至下的合规意识提升，从而才能有效应对未来的数据合规风险。

(3) 跨境业务下的风险评估

考虑到大多数国内企业产品在国内外均具有市场竞争力，有些拟上市公司产品已经行销海外，因此境外的数据合规问题亦不容忽视。全球主要经济体对于个人隐私和数据安全均十分看重，而每个国家对此的合规要求又有不同。因此拟上市公司必须评估产品和服务跨境场景下的数据合规问题。而根据我们经验，跨境合规评估涉及到不同法域和不同场景，相较于国内合规评估，此类合规工作较为复杂和不可控。因此，我们建议拟上市企业应当未雨绸缪，尽早进行规划，特别是主要产品的主要市场在境外的，更要制定比较详细的评估方案，以应对监管问询。



科技企业的数据合规问题已经成为企业上市所需要关注的核心问题。

PART 006

结语

如本指南所揭示，科技企业的数据合规问题已经成为企业上市所需要关注的核心问题。目前证券监管部门在相关审核和问询中所重点关注的风险不仅涵盖最基础的如数据搜集、数据购买、数据使用和管理等“必答题”，而且对于当前比较有争议的比如用户的行权问题、自动化访问收集等问题均有详细的问询。在有限时间内如何帮助拟上市企业迅速有效应对和解决这些问询，考验着专业律师的经验和智慧。我们的初步建议是相关拟上市企业在上市专业律师之外，同时也尽早引入数据合规专业律师以全面熟悉企业的核心产品和技术方案，并协同公司法务、风控合规、技术、业务等各部门条线和外部技术专家顾问一起，及早核查整改并确保相关措施有效实施。企业甚至应考虑在公司初创及产品设计或早期融资时即开展相关工作，避免拖延到后期积重难返而整改成本代价畸高，甚至直接构成通过上市审核的实质性障碍。

张诗伟
合伙人
资本市场部
北京办公室
+86 10 5957 2022
zhangshiwei@zhonglun.com

蔡鹏
合伙人
知识产权部
北京办公室
+86 10 5087 2786
caipeng@zhonglun.com

主编

陈际红
蔡荣伟
蔡鹏

编委（按姓氏笔画排序）

刘新宇
张诗伟
李瑞
严静安
周洋
钟俊鹏
侯彰慧
姜璐璐
贾申
郭建华
斯响俊
葛燕

总编

龚乐凡
张炯

特别声明：以上所刊登的文章仅代表作者本人观点，不代表北京市中伦律师事务所或其律师出具的任何形式之法律意见或建议。未经本所书面授权，不得转载或使用该等文章中的任何内容，含图片、影像等视听资料。如您有意就相关议题进一步交流或探讨，欢迎与本所联系。

WWW.ZHONGLUN.COM