环球律师事务所
GLOBAL LAW OFFICE
SINCE 1979

2024

数字经济与网络数据安全

TMT
监管合规洞察

环球数字经济与网络数据安全团队编制

目录

我国电信监管与合规 1

1. 开放怀抱的电信市场：增值电信业务扩大对外开放试点启动 2
2. 北京、上海、深圳、海南四地启动增值电信业务扩大对外开放试点工作 10

我国网络数据安全 13

1. 总则：解读《网络数据安全管理条例》：洞悉数字战役背后的护航力量 14
2. 数据分类分级：解读《数据安全技术 数据分类分级规则》：纲举目张，安则有序 43
3. 数据跨境传输：解读《促进和规范数据跨境流动规定》：流动与安全并重 59
4. 数据跨境传输：解读《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同实施指引》：跨境数据流动创新保障性措施的先行先试 72
5. 网络竞争规范：解读《网络反不正当竞争暂行规定》：互联网条款重点关注 132
6. 测绘信息安全：解读《自然资源部关于加强智能网联汽车有关测绘地理信息安全管理的通知》：安全为基，智驭未来 150
7. 平台运营资质：应用程序分发平台对 App 运营者的资质审核机制分析 163

美国网络数据安全 179

1. 美国数据监管新规观察（上）——美国数据跨境传输行政命令的背景与规则 180
2. 美国数据监管新规观察（中）——美国数据监管行政命令的风险分析与企业因应 197
3. 美国数据监管新规观察（下）——美国数据跨境新政的适用场景、应用公式与应对策略 209

欧美中人工智能监管与合规 236

1. 欧盟：《欧盟人工智能法》正式生效 237
2. 美国：联邦和各州的人工智能立法进展 257
3. 中国：《生成式人工智能服务安全基本要求》正式发布 263
4. 欧美中人工智能监管合规关注对比 273

环球律师事务所
GLOBAL LAW OFFICE SINCE 1979

我国电信监管与合规

- 开放怀抱的电信市场：增值电信业务扩大对外开放试点启动
- 北京、上海、深圳、海南四地启动增值电信业务扩大对外开放试点工作

1. 开放怀抱的电信市场：增值电信业务扩大对外开放试点启动[1]

2024 年 10 月 23 日，工业和信息化部正式启动《关于开展增值电信业务扩大对外开放试点工作的通告》（工信部通信函〔2024〕107 号）（以下简称“**107 号文**”）所规定的北京市服务业扩大开放综合示范区、上海自由贸易试验区临港新片区及社会主义现代化建设引领区、海南自由贸易港、深圳中国特色社会主义先行示范区四地增值电信业务扩大对外开放试点工作。回望过去，在 2001 年 12 月 11 日正式入世的同一天，我国发布了《外商投资电信企业管理规定》以履行其入世文件中关于开放电信行业的承诺，其中第六条规定：外国投资者必须获得批准才能在中国投资经营电信服务的企业，这类企业被称为“外商投资电信企业”，由此我国首次打开了增值电信业务市场的大门，并以“小步”+“慢跑”的方式逐渐平稳开放。本文将基于我国目前增值电信业务市场的相关法律法规和我们的服务经验，对 107 号文的规定以及实务中可能出现的问题进行解读，供企业和各界人士参考。

一、本次试点涉及的增值电信业务

我国加入世界贸易组织时，针对电信业务所做出的承诺为“有限承诺”，即允许外商投资的电信业务仅限于“入世”承诺表和后续颁布的《外商投资准入特别管理措施（负面清单）》所列明的电信业务。根据《中华人民共和国电信条例（2016 修订）》《外商投资电信企业管理规定（2022 修订）》等规定，经营基础电信业务的外资出资比例不得超过 49%，经营增值电信业务的外资出资比例不得超过 50%，国家另有规定的除外。

107 号文第二条所规定的“取消……外资股比限制”，正是针对上述规定所做出的出资比例限制所做出的突破性规定。107 号文正式实施后，外方投资者投资（开展试点范围内增值电信业务的）电信企业的，在企业中的出资比例可以突破 50%的限制，甚至实现 100%独资出资。

根据《中华人民共和国外商投资法》，外商投资企业是指全部或者部分由外国投资者（含港澳台地区）投资，依照中国法律在中国境内经登记注册设立的企业。“入世后”，我国一方面针对港澳台地区投资者的投资比例限制推出了宽松政策，一方面在多个自由贸易区率先开展各类电信业务对外开放的试点，各类政策文件交错形成了较为复杂的规则体系。结合 107 号文、《内地与香港关于建立更紧密经贸关系的安排》（以下简称“**CEPA 政策**”）和《国务院关于印发中国（海南）自由贸易试验区总体方案的通知》等各自贸区文件，我们总结目前的各类电信业务的外资投资比例限制情况如下：

[1] 作者：孟洁、赵姝、黎耀琦

增值电信业务类型	《外商投资电信企业管理规定》及负面清单等基本政策（中国大陆范围内）	CEPA 政策（港澳投资者）	自由贸易区政策（各类外资投资者）	107 号文（北上琼深四地）
B11 类互联网数据中心业务（IDC）	禁止	外资比例≤50%	禁止（海南附条件开放[2]）	外资比例≤100%
B12 类内容分发网络业务（CDN）	禁止	外资比例≤50%	禁止（海南附条件开放）	外资比例≤100%
B14 类互联网接入服务业务（ISP）	禁止	为上网用户提供互联网接入服务：外资比例≤100%；其他 B14 类业务：外资比例≤50%	为上网用户提供互联网接入服务：外资比例≤100%；其他 B14 类业务：禁止	外资比例≤100%
B21 类在线数据处理与交易处理业务（EDI）	电商业务：外资比例≤100%；其他 B21 类业务：外资比例≤50%	电商业务：外资比例≤100%；其他 B21 类业务：外资比例≤50%	电商业务：外资比例≤100%；其他 B21 类业务：外资比例≤50%	外资比例≤100%
B25 类信息服务业务（ICP）	外资比例≤50%	应用商店业务：外资比例≤100%；其他 B25 类业务：外资比例≤50%	应用商店业务：外资比例≤100%；其他 B25 类业务：外资比例≤50%	信息发布平台和递送服务（互联网新闻信息、网络出版、网络视听、互联网文化经营除外）、信息保护和处理服务业务：外资比例≤100%

本次扩大对外开放试点涉及的电信业务覆盖了大量的应用场景，相关业务的具体含义及对应的适用场景如下：

[2] 根据《海南自由贸易港建设总体方案》，允许实体注册、服务设施在海南自由贸易港内的企业，面向自由贸易港全域及国际开展在线数据处理与交易处理等业务，并在安全可控的前提下逐步面向全国开展业务。

（一）B11 类互联网数据中心业务（IDC）

互联网数据中心（IDC）业务是指利用相应的机房设施，以外包出租的方式为用户的服务器等互联网或其他网络相关设备提供放置、代理维护、系统配置及管理服务，以及提供数据库系统或服务器等设备的出租及其存储空间的出租、通信线路和出口带宽的代理租用和其他应用服务互联网数据中心业务经营者应提供机房和相应的配套设施，并提供安全保障措施。常见的场景包括：（1）传统 IDC 服务器厂商；（2）算力基础设施和云计算服务厂商，包括亚马逊 AWS、微软 Azure 等。

（二）内容分发网络业务（CDN）

内容分发网络（CDN）业务是指利用分布在不同区域的节点服务器群组成流量分配管理网络平台，为用户提供内容的分散存储和高速缓存，并根据网络动态流量和负载状况，将内容分发到快速、稳定的缓存服务器上，提高用户内容的访问响应速度和服务的可用性服务。常见的场景包括：网站加速，例如为门户网站、电子商务网站、新闻资讯网站、社交媒体平台等提供加速服务；在线视频流媒体服服务，例如腾讯等视频网站、幕课等在线教育平台、网易云等音乐分享网站等。

对比此前的自贸区政策和 CEPA 政策，IDC 业务和 CDN 业务均是是首次向外资（不包括港澳台地区）开放，而且外资出资比例未设限制，开放力度和尺度进一步增强。

（三）互联网接入服务业务（ISP）

互联网接入服务（ISP）业务是指利用接入服务器和相应的软硬件资源建立业务节点，并利用公用通信基础设施将业务节点与互联网骨干网相连接，为各类用户提供接入互联网的服务。常见的场景包括：为互联网信息服务业务（ICP）经营者提供接入服务；提供宽带接入服务等。

在自贸区政策和 CEPA 政策下，为上网用户提供互联网接入服务已向外资开放、其他 ISP 业务向港澳投资者开放（投资比例不超过 50%），本次扩大对外开放试点则将开放范围扩大至所有 ISP 业务。

（四）在线数据处理与交易处理业务（EDI）

在线数据处理与交易处理（EDI）业务是指利用各种与公用通信网或互联网相连的数据与交易/事务处理应用平台，通过公用通信网或互联网为用户提供在线数据处理和交易/事务处理的业务。常见的场景包括：淘宝、京东等电商平台；智能家居、工业互联网、车联网等物联网平台。

就 EDI 业务，我国此前已经取消了电商类业务的外资投资比例，本次扩大对外开放试点则进一步扩大至所有 EDI 业务。

（五）信息服务业务（ICP）

信息服务（ICP）业务是指通过信息采集、开发、处理和信息平台的建设，通过公用通信网或互联网向用户提供信息服务的业务。值得注意的是，本次扩大对外开放试点的 ICP 业务仅包括信息发布平台和递送服务（互联网新闻信息、网络出版、网络视听、互联网文化经营除外）、信息保护和处理服务业务，而信息搜索查询服务、信息社区平台服务、信息即时交互服务仍未开放，属于外资禁止投资和经营的增值电信业务。

二、境外投资者申请增值电信业务的相关实务问题

我们结合《外商投资电信企业管理规定（2022 修订）》、107 号文等文件以及过去的服务经验，总结了以下境外投资者申请增值电信业务时可能面临的实务问题。

（一）本次扩大对外开放试点地区的范围是？

根据 107 号文的规定，本次试点地区对应的行政区域范围如下表：

序号	试点地区	地域范围	注册地、服务设施	服务范围
1	北京市服务业扩大开放综合示范区	北京市	试点开放业务经营主体注册地、服务设施（含租用、购买等设施）放置地须在同一试点区域内，不得购买、租用本试点区域外 CDN 等设施开展加速服务。	ISP 业务服务范围仅限本试点区域，且需通过基础电信企业互联网接入设备对用户提供互联网接入服务；其他业务服务范围可面向全国。
2	上海自由贸易试验区临港新片区及社会主义现代化建设引领区	上海大治河以南、金汇港以东（包括小洋山岛以及浦东国际机场南侧区域）及浦东新区		
3	海南自由贸易港	海南岛全岛		
4	深圳中国特色社会主义先行示范区	深圳市		

（二）境外投资者申请取得的资质为何种形式？

不同于境内企业申请取得的增值电信业务经营许可证，根据 107 号文的规定，外商投资电信企业应按照相关规定向工业和信息化部申请取得**电信业务经营试点批复**，并在电信业务经营活动中遵守相关法律法规及试点批复的规定，接受、配合电信管理机构及有关主管部门的监督管理。

根据已经开展的自贸区实践，“试点批复”与《电信业务经营许可证》具有同等效力。根据《电信业务经营许可管理办法（2017）》的规定，增值电信业务经营许可证的有效期为 5 年，而本次扩大对外开放试点所下发的电信业务经营试点批复有效期仍有待各地主管部门后续进一步明确。

（三）试点申报条件有哪些？

在工业和信息化部答记者问环节[3]中，明确对在试点地区开展前述增值电信业务的外商投资电信企业，遵循**“内外资一致”原则**进行管理。

根据《电信业务经营许可管理办法（2017）》第六条，经营增值电信业务应当具备下列条件：

（一）经营者为依法设立的公司；

（二）有与开展经营活动相适应的资金和专业人员；

（三）有为用户提供长期服务的信誉或者能力；

（四）在省、自治区、直辖市范围内经营的，注册资本最低限额为 100 万元人民币；在全国或者跨省、自治区、直辖市范围经营的，注册资本最低限额为 1000 万元人民币；

（五）有必要的场地、设施及技术方案；

（六）公司及其主要投资者和主要经营管理人员未被列入电信业务经营失信名单；

（七）国家规定的其他条件。

针对外商投资增值电信业务注册资本要求，以数据中心业务为例，如果存在机房所在地不在同一省份的情况，则需要申请全国或跨省市增值电信业务，则注册资本不得低于 1000 万元人民币。

（四）申请试点需要完成什么申报和审批程序？

根据 107 号文及其附件《增值电信业务扩大对外开放试点方案》，目前试点的实施方案流程如下：

[3] 参见 https://www.gov.cn/zhengce/202404/content_6944438.htm?ddtab=true。

（1）试点地区政府组织制定本地区的试点实施方案，报送至工业和信息化部；

（2）工业和信息化部开展专家评估论证、调研等，作出批复后；

（3）获批复地区可开展试点，制定具体的审批和监管方案；

（4）企业根据发布的具体方案，向工业和信息化部/地方通信管理局申请取得电信业务经营试点批复。

目前，107 号文仅概括性地规定了拟在试点地区开展前述增值电信业务的外商投资电信企业，应按照相关规定向工业和信息化部申请取得电信业务经营试点批复，但未规定具体的审批流程。试点正式启动后，预计各地部门会陆续推出落地实施的具体方案，我们也将持续关注后续试点进展。

三、扩大对外开放试点的影响和意义

本次扩大对外开放试点正式启动后，除了信息搜索查询服务、信息社区平台服务、信息即时交互服务等少部分监管较为严格的增值电信业务外，我国的增值电信业务市场已经极大程度地对境外投资者“开放怀抱”，入局电信市场正在迎来新的窗口期。

（一）算力服务与人工智能的快速发展

算力是数字经济时代的核心生产力，数据中心则是数字经济运行的动脉。随着人工智能模型的快速演进和迭代，模型规模的扩大和算法的复杂化对算力提出了更高的要求。国务院、工信部、国家发改委以及国家能源局等多个部门单独或联合出台了一系列政策，旨在支持、指导和规范数据中心的发展。而本次试点对外开放互联网数据中心业务，允许业务服务范围面向全国展开，则意味着外商投资企业在试点地区取得 IDC 试点批复后，可以在中国境内提供算力服务和云服务等。我国的人工智能产业正处于高速发展时期，我国此举一方面是为了引入外资的先进算力和云计算服务，另一方面，对于外商投资企业而言，也有助于企业捕捉市场需求的变化、及时填补需求端缺口，真正抓住和释放政策带来的红利。

（二）低风险的统一网络安全体系

此前，由于外资投资比例限制，在中国大陆开展业务的过程中，外商投资企业通常需要通过租用境内企业的服务器、数据中心等或通过合资成立子公司开展相关业务。本次扩大对外开放试点实施后，由于数据中心的建设和相关业务不再受到投资比例的限制，外商投资企业可以选择自行开展数据中心建设、搭建数据库系统等业务，供企业集团内部、其他子公司使用，从而搭建统一、安全的网络和数据安全系统，保障数据存储、传输和处理过程中的安全，进而将业务扩展至

第三方企业，提高投资回报比率；另一方面，随着外资比例限制的取消，企业提供集团内部网络和数据服务的监管风险也会显著降低。

（三）物联网服务平台

本次扩大对外开放试点实施后，在线数据处理与交易处理（EDI）业务全部向外资开放，其中电子数据交换业务和网络、电子设备数据处理业务两项业务系首次对外开放，这意味着符合条件的外资企业可独资提供物联网平台服务，对于智能家居、工业互联网、车联网等行业领域的外商投资企业属于重大利好。从目前已经申请试点批复的企业中，不乏特斯拉等典型物联网、车联网企业[4]。

（四）降低投资风险、增加交易确定性

取得电信业务经营试点批复，对于境外投资者投资、收购境内企业也存在积极意义。根据《外商投资安全审查办法》第四条，外国投资者或者境内相关当事人投资关系国家安全的重要信息技术和互联网产品与服务、关键技术以及其他重要领域，并取得所投资企业的实际控制权的，应当在实施投资前主动向工作机制办公室申报国家安全审查。

在 107 号文出台前，由于外资出资比例限制的存在，数据中心业务等增值电信业务是否属于需要进行国家安全审查的范围内始终存在一定争议和疑问。107 号文出台和实施后，我们理解如果外商投资企业顺利取得相应的电信业务经营试点批复，则意味着开展相关的增值电信业务涉及国家安全审查的可能性和风险较低，有利于增加了境外投资者投资、交易的确定性和可预期性。

四、结语与建议

鉴于目前试点区域的具体方案和流程尚未正式出台，我们建议各企业持续关注政策的实际落地情况。同时，根据已有的规定，我们给希望申请取得试点批复的企业提供一些对策与建议，具体如下：

（一）完善网络安全和数据保护体系

尽管 107 号文没有明确对于企业开展相关增值电信业务的监管要求，但是其附件《增值电信业务扩大对外开放试点方案》明确工业和信息化部会在评估论证过程中“调研核查安全监管保障体系等”，并在“试点保障措施”一节提出“建立企业信息上报和定期抽查机制，强化网络和数据安全监管能力，督促企业切实履行安全主体责任。”可见，工业和信息化部等部门对于外商投资企业经营电信业务的监管力度并不会因开放而放松。

[4] 参见 https://cnapp.chinadaily.com.cn/a/202410/23/AP67189eb3a3102b24bcb3f411.html。

以开放试点的互联网数据中心（IDC）业务为例，如果外商投资企业通过数据中心提供边缘算力服务、人工智能算力服务等服务，往往会处理多种类型数据、涉及的数据量巨大，且涉及高精尖技术行业。根据《中国人民共和国网络安全法》等法律法规的规定和我们的服务经验，数据中心按照网络安全等级三级或以上进行定级、开展网络安全保护工作较为适宜。作为试点区域之一的深圳，深圳市公安局公共信息网络安全监察分局在《关于落实网络安全等级保护制度要求的通知》中指出，“互联网数据中心和云平台运营方，原则上基础网络定级不得低于三级，且不得低于所承载信息系统的最高级别等[5]。

鉴于网络安全和数据保护的重要性、事后性，企业率先建立和完善网络安全和数据保护体系，一方面既有利于通过监管部门的审核、顺利取得电信业务经营试点批复；另一方面，在取得批复、开展经营后，完善的网络安全和数据保护体系也有助于企业合法合规开展经营，降低发生数据安全事件等风险。

（二）梳理股权关系结构

参考过去申请增值电信业务许可证时，对于外资出资比例的审核需要进行股权穿透，穿透、追溯至国有独资、自然人及外商独资为止，在此基础上加权累计计算外资出资比例。因此，我们理解本次扩大对外开放试点，尽管取消了对于外资出资比例的限制，但是在申请电信业务经营试点批复的过程中，申请人很有可能也需要提供充分、细致的外资结构和成分等相关文件。

[5] 《深圳市公安局：IDC、云平台「信息安全等级保护」不得低于三级，否则从严处罚》，https://www.sohu.com/a/226909680_465914，最后访问于 2020 年 5 月 5 日。

2. 北京、上海、深圳、海南四地启动增值电信业务扩大对外开放试点工作

2024 年 10 月 23 日，工业和信息化部组织召开增值电信业务扩大对外开放试点工作座谈会，正式启动北京、上海、深圳、海南四地增值电信业务扩大对外开放试点工作，在获批开展试点的地区取消互联网数据中心（IDC）、内容分发网络（CDN）、互联网接入服务（ISP）、在线数据处理与交易处理，以及信息服务中信息发布平台和递送服务（互联网新闻信息、网络出版、网络视听、互联网文化经营除外）、信息保护和处理服务业务的外资股比限制。

近期，各试点地区陆续发布相关解读、通告，正式启动增值电信业务扩大对外开放试点。

省/市	申请条件	申请渠道	申请材料	审核时限	联系方式	参考链接
北京	申请增值电信业务，应当符合《电信业务经营许可管理办法》第六条的规定[6]。同时，还需符合《工业和信息化部关于开展增值电信业务扩大对外开放试点工作的通告》（工信部通信函〔2024〕107号）的相关规定。	申请者登录工业和信息化部政务服务一体化平台（https://ythzxfw.miit.gov.cn），在“公共服务”模块中选择并进入“电信业务市场综合管理信息系统”，点击“电信业务经营许可申请”进入“增值电信业务许可”页面，选择“外资试点申请任务栏”中的“试点许可列表”模块，在线提交申请。	（一）公共表单 1、试点经营增值电信业务申请表 2、公司及人员情况表 3、股东情况表 4、依法试点经营电信业务承诺书 5、电信管理机构要求提交的其他证明材料（选填） （二）业务专用表单 1、互联网数据中心业务专用表 2、内容分发网络业务专用表 3、互联网接入服务专用表 4、在线数据处理与交易处理业务专用表 5、信息服务业务（仅限互联网信息服务）业务专用表 6、信息服务业务（不含互联网信息服务）业务专用表	企业在准备好材料后可随时申请，针对材料有问题的情况，在提交后 5 日内一次性退回补正，受理后 15 日内形成初审意见并上报到工信部信管局复审。	010-51938033 010-51938038	https://mp.weixin.qq.com/s/j5RD5ikCwcbeRJbWZjI6oA

[6] （一）经营者为依法设立的公司；（二）有与开展经营活动相适应的资金和专业人员；（三）有为用户提供长期服务的信誉或者能力；（四）在全国或者跨省、自治区、直辖市范围经营的：1、申请跨地区 IDC\CDN\SP 业务的应不低于 1000 万元人民币。2、申请其他业务最低限额均为 100 万元人民币。（外币需换算）（五）有必要的场地、设施及技术方案；（六）公司及其主要投资者和主要经营管理人员未被列入电信业务经营失信名单；（七）国家规定的其他条件。

省/市	申请条件	申请渠道	申请材料	审核时限	联系方式	参考链接
上海	申请增值电信业务，应当符合《电信业务经营许可管理办法》第六条的规定。同时，还需符合《工业和信息化部关于开展增值电信业务扩大对外开放试点工作的通告》（工信部通信函〔2024〕107号）的相关规定。	有意参与试点申请的外资企业可在工业和信息化部政务服务平台（https://ythzxfw.miit.gov.cn “政务服务” - “行政许可” - “电信和互联网业务” - “电信业务经营许可”板块）在线提交申请，自主申报。	（一）公共表单 1、试点经营增值电信业务申请表 2、公司及人员情况表 3、股东情况表 4、依法试点经营电信业务承诺书 5、电信管理机构要求提交的其他证明材料（选填） （二）业务专用表单 1、互联网数据中心业务专用表 2、内容分发网络业务专用表 3、互联网接入服务专用表 4、在线数据处理与交易处理业务专用表 5、信息服务业务（仅限互联网信息服务）业务专用表 6、信息服务业务（不含互联网信息服务）业务专用表	企业在准备好材料后可随时申请，针对材料有问题的情况，在提交后5日内一次性退回补正，受理后15日内形成初审意见并上报到工信部信管局复审。	政策咨询（市经济信息化委）：021-60801129 填报指引（市通信管理局）：021-63905098 项目申报：浦东新区 021-58788388 转 64417 临港新片区 021-68286752	https://mp.weixin.qq.com/s/GxRpr7f5LKMs67jiuLXiwQ
海南	申请增值电信业务，应当符合《电信业务经营许可管理办法》第六条的规定。同时，还需符合《工业和信息化部关于开展增值电信业务扩大对外开放试点工作的通告》（工信部	企业注册账号并登录工业和信息化部政务服务一体化平台（https://ythzxfw.miit.gov.cn），在“公共服务”模块中选择“电信业务市场综合管理信息系统”，点击“电信业务经营许可申请”进入“增值电信业务许可”页面，选择“外资试点申请任务栏”中的	（一）公共表单 1、试点经营增值电信业务申请表 2、公司及人员情况表 3、股东情况表 4、依法试点经营电信业务承诺书 5、电信管理机构要求提交的其他证明材料（选填） （二）业务专用表单 1、互联网数据中心业务专用表 2、内容分发网络业务专用表	企业可通过“电信业务市场综合管理信息系统”申请提交书面申请材料，对于不符合要求的申请材料，于5个工作日内一次性退回补正。自受理之日起15日内形	海南省通信管理局，0898-65203155，66520730	https://mp.weixin.qq.com/s/9VfaZXEF72FaEdLoHRzOAQ

省/市	申请条件	申请渠道	申请材料	审核时限	联系方式	参考链接
	通信函〔2024〕107号）的相关规定。	“试点许可列表”模块，在线提交申请。	3、互联网接入服务专用表 4、在线数据处理与交易处理业务专用表 5、信息服务业务（仅限互联网信息服务）业务专用表 6、信息服务业务（不含互联网信息服务）业务专用表	成初审意见并上报至工业和信息化部进行复审。		
深圳	申请增值电信业务，应当符合《电信业务经营许可管理办法》第六条的规定。同时，还需符合《工业和信息化部关于开展增值电信业务扩大对外开放试点工作的通告》（工信部通信函〔2024〕107号）的相关规定。	登录工业和信息化部政务服务一体化平台（https://ythzxfw.miit.gov.cn），在“公共服务”模块中选择并进入“电信业务市场综合管理信息系统”，点击“电信业务经营许可申请”进入“增值电信业务许可”页面，选择“外资试点申请任务栏”中的“试点许可列表”模块，在线提交申请。	（一）公共表单 1.试点经营增值电信业务申请表 2.公司及人员情况表 3.股东情况表 4.依法试点经营电信业务承诺书 5.电信管理机构要求提交的其他证明材料（选填） （二）业务专用表单 1.互联网数据中心业务专用表 2.内容分发网络业务专用表 3.互联网接入服务专用表 4.在线数据处理与交易处理业务专用表 5.信息服务业务（仅限互联网信息服务）业务专用表 6.信息服务业务（不含互联网信息服务）业务专用表	企业在准备好材料后可在系统提交申请，若企业提交材料不齐全或者不符合法定形式的，在提交申请后5个工作日内一次性告知申请人。自受理申请之日起，15日内形成初审意见并书面报工业和信息化部信息通信管理局。		https://mp.weixin.qq.com/s/8b3NfARMV6t-iGi-cHfjuw

环球律师事务所 GLOBAL LAW OFFICE SINCE 1979

我国网络数据安全

总则

- 解读《网络数据安全管理条例》：洞悉数字战役背后的护航力量

数据分类分级

- 解读《数据安全技术 数据分类分级规则》：纲举目张，安则有序

数据跨境传输

- 解读《促进和规范数据跨境流动规定》：流动与安全并重
- 解读《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同实施指引》：跨境数据流动创新保障性措施的先行先试

网络竞争规范

- 解读《网络反不正当竞争暂行规定》：互联网条款重点关注

测绘信息安全

- 解读《自然资源部关于加强智能网联汽车有关测绘地理信息安全管理的通知》：安全为基，智驭未来

平台运营资质

- 应用程序分发平台对App运营者的资质审核机制分析

1. 总则：解读《网络数据安全管理条例》：洞悉数字战役背后的护航力量[7]

引言

随着信息技术的迅猛发展，网络数据已成为数字经济时代的重要生产要素。然而，网络数据的安全问题日益凸显，对国家安全、公共利益以及个人和组织的合法权益构成了严重威胁。为了应对这些挑战，我国相继出台了《中华人民共和国网络安全法》（以下简称“《网安法》”）《中华人民共和国数据安全法》（以下简称“《数安法》”）《中华人民共和国个人信息保护法》（以下简称“《个保法》”）等法律法规，构建了较为完善的信息安全法律体系。《网络数据安全管理条例》被连续多年被立为国务院工作计划。2021年11月14日，国家互联网信息办公室（以下简称“网信办”）曾发布《网络数据安全管理条例（征求意见稿）》（以下简称“《征求意见稿》”）。时隔近3年，2024年8月30日，国务院第40次常务会议通过《网络数据安全管理条例》（以下简称“《条例》”）。

导读一：《条例》与《征求意见稿》比较，有哪些主要修订和补充？

较此前《征求意见稿》，《条例》从整体上呈现出针对产业创新性、鼓励性与技术中立性等事项的监管态度较之前变得相对柔和放松；而针对容易出现安全事件并导致重大风险的事项、应设置事先预防机制的事项、特定主体开展业务、运用相关技术、提供相关产品或服务且可能对网络数据安全产生较大影响等事宜均收紧了监管；针对上位法涉及的流程性事宜或者遗留的待进一步解释明确的条款，《条例》则通过更加精细化的立法技术使其呈现体系性和规范化。当然，《条例》属于行政法规，因此针对应更加系统性规定进行补充和阐明的规则，交由下位法，如部门规章、地方性法规、规章、司法解释等已进行或者将进行规制，当然，此类规则也可通过国家或者行业标准等进行技术支撑。

《条例》中体现出监管释放某种信号、并将温和、放缓地处理相关事宜的条款，例如：鼓励网络数据在各行业、各领域的创新应用（第四条）；积极参与网络数据相关国际规则和标准的制定、促进国际交流与合作（第六条）；支持相关行业组织按照章程制定网络数据安全行为规范，加强行业自律，指导会员加强网络数据安全保护（第七条）；个人信息保存期限难以确定的，明确保存期限的确定方法（第二十一条第一款第三项）；与此同时，《条例》删除了必须于十五个工作日内删除个人信息或者进行匿名化处理的规定；也删除了若技术上难以实现或者因业务复杂等原因，在十五个工作日内删除个人信息确有困难的，数据处理者不得开展除存储和采取必要安全保护措施之外的处理并向个人做出合理解释的条款（《征求意见稿》第二十二条）。

在重要数据处理规定方面，《条例》规定了网络数据安全负责人由网络数据处理者的管理层成员担任，修改了《征求意见稿》要求决策层担任的规定，并且网络数据安全负责人有权直接向有关主管部门报告网络数据安全情况（第三十条第二款），修订了《征

[7] 作者：孟洁、殷坤、田梓仪、朱含章

求意见稿》要求向网信部门和主管、监管部门反映数据安全情况的要求，减轻了企业在网络数据安全负责人任命和报告义务上的负担；此外，《条例》规定重要数据处理者应当定期组织宣传教育培训等活动（第三十条第一款第二项），取消了《征求意见稿》要求对相关技术和管理人员每年教育培训时间不得少于二十小时的强制性规定；《条例》只要求重要数据处理者每年度对其网络数据处理活动开展风险评估，并向省级以上有关主管部门报送风险评估报告（第三十三条），没有采取《征求意见稿》对年度风险评估的开展设定前提条件、频率、报送时间等详细要求；针对处理特定人数个人信息的网络数据处理者需要同时履行重要数据处理者的部分义务，《条例》将此数量从《征求意见稿》中的 100 万人提高至 1000 万人，同时也提高了符合门槛的条件，另外还将《征求意见稿》中要求遵守重要数据处理者的全部义务限定到只需要遵守关键性和关联性最强的两项义务（即第三十条、第三十二条），降低了相关企业的一部分合规成本。

除上述放缓措施以外，《条例》取消了《征求意见稿》要求数据处理者对评估报告留存至少三年的规定，只规定当出现数据处理者向其他网络数据处理者提供、委托处理个人信息和重要数据的情况时，须将记录至少保存三年（第十二条）；删除了《征求意见稿》第四十一条第三款规定的境内用户访问境内网络的，其流量不得被路由至境外的规定，对 CDN 等网络加速产业的发展起到了支持和推动的作用；删除了《征求意见稿》第四十三条针对平台规则、隐私政策或对用户权益有重大影响的条款修订前，要求互联网平台运营者在该互联网平台或者行业协会平台面向社会公开征求意见不少于三十日、向用户提供充分表达意见、以易于访问的方式公布意见采纳情况、说明未采纳的理由、接受社会监督的条款；同时，还删除了《征求意见稿》中针对日活用户超过一亿的大型互联网平台在其平台规则、隐私政策的制定或者对用户权益有重大影响的条款修订前，要求大型互联网平台经过国家网信部门认定的第三方机构评估，并报省级及以上网信部门和电信主管部门同意的条款。因为实践中互联网平台产品/功能更迭变化之快需要平台规则随之迅速更新，并于上线前获取用户的同意，但是一般很少有用户会在三十日的等待期内提供有效且有价值的意见反馈，并且国家网信部门也未曾认定哪些第三方评估机构可以作为指导部门对平台更新的用户规则和隐私政策进行确认，因此《征求意见稿》的初衷虽好，但落实起来难度较大，因此《条例》对此类条款也进行了删减。此举措体现了在当前形势下，对相关互联网平台的保护与促进，同时，执法的步伐应当相对放宽和放缓。与之相关的条款还有：删除《征求意见稿》中涉及第三方产品和服务对用户造成损害的，用户有权要求平台运营者先行赔偿的条款（《征求意见稿》第四十四条）；鼓励保险公司开发网络数据损害赔偿责任险种，鼓励网络平台服务提供者、预装应用程序的智能终端等设备生产者投保（第四十条）等。

《条例》相较于《征求意见稿》，部分呈现收紧且加强监管态势的条款有：《条例》第八条、第九条针对网络数据处理者的基本义务和保障性措施进行了加严规制；第十条针对风险补救措施、危险情况发生后 24 小时内的报告义务、制定数据安全事件应急预案等要求进行了明确，以防止危害事件出现后发生不可控的危害后果并因此影响国家安

全、社会公共利益以及人民群众权益。同时，《条例》要求针对处理网络数据情况的记录须保存至少三年；网络数据处理者开展任何网络数据处理活动（不限于《征求意见稿》针对处理一百万人以上个人信息的数据处理者赴国外上市和赴香港上市的数据处理活动影响或者可能影响国家安全这二类特定情形），如果存在影响或者可能影响国家安全的情况，均应当按照有关规定进行国家安全审查（也已不仅限于《征求意见稿》第十三条中涉及的网络安全审查），审查范围更加广泛，重点维护国家整体安全。此外，《条例》针对“数据可携带权”规定了网络数据处理者在收到转移个人信息次数超出合理范围的请求时，享有根据其所付出的成本收到必要（而非合理）费用的权利（第二十五条）。针对企业掌握重要数据的认定标准，《条例》与《促进与规范数据跨境流动规定》保持一致，即以相关地区、部门告知网络数据处理者或者公开发布重要数据目录或清单为依据，同时要求网络数据处理者、制定并实施网络数据管理制度，采取加密、备份、访问控制、安全认证等技术措施，并且鼓励网络数据处理者使用数据标签标识等技术和产品（第二十九条）、采取添加标签标识的技术措施（第三十三条）来提高重要数据的安全管理水平；此外，《条例》规定对处理特定重要数据的网络数据安全负责人和关键岗位的人员进行安全背景审查，必要时，可以申请公安机关和国家安全机关协助审查（第三十条）。针对一些特殊属性的技术（自动化采集、自动化决策）或产品（如应用分发程序）、平台（大型网络平台）的服务提供方，《条例》对此施加了须履行更加严格的义务和须受社会监督的责任（第四十一至第四十六条），具体规定将在文章正文中逐一展开分析。《条例》不仅针对网络数据处理者的义务在特定情形下作缩紧规定，针对承担监管职责的主管部门也提出了从严管理的要求。例如，要求有关主管部门开展网络数据安全监督检查应当客观公正，不得向被检查单位收取费用、不得访问、收集与网络数据安全无关的业务信息，获取的信息只能用于维护网络数据安全的需要，不得用于其他用途（第五十一条）；多个主管部门开展网络数据安全监督检查时，应当加强协同配合、信息沟通，避免不必要的检查和交叉重复检查。重要数据风险评估和网络安全等级测评的内容有重合的，相关结果可以互相采信。企业可以在开展个人信息保护合规审计、重要数据风险评估、重要数据出境安全评估等各类风险评估工作之间建立一套有效且统一的体系，互相之间进行衔接、切换，避免重复评估、审计（第五十二条），减少企业在人力、财务、物力方面的负担，提升内部合规工作的动力。

针对《征求意见稿》中的某些条款，在历经近三年时间的检验后，《条例》进行了更加细化的处理，起到了对《网安法》《数安法》《个保法》中相关规定更好地支撑与落地的作用。例如，在委托处理场景下，《条例》规定了委托方和受托方应分别履行法定和约定的义务，重点提出了受国家机关委托，建设、运行、维护电子政务系统，存储、加工政务数据的受托方义务（第十五条），以及为国家机关、关键信息基础设施运营者提供服务，或者参与其他公共基础设施、公共服务系统建设、运行、维护等受托方义务的细分场景，这为近期讨论热烈的公共数据授权运营涉及的相关方义务提供立法基础。并且《条例》规定网络数据处理者未经委托方同意，不得访问、获取、留存、使用、泄露或者向他人提供网络数据，不得对网络数据进行关联分析（第十六条）。针对自动化

工具访问、收集网络数据的，分别由第十八条和第二十四条进行细化规定；针对使用自动化决策技术向个人推送信息的，《条例》第四十二条进行了细化；提供生成式人工智能服务（第十九条）和面向社会提供产品、服务（第二十条）的网络数据处理者，也分别由《条例》对其进行了细化约束；针对单独设置《儿童隐私保护声明》、在隐私政策外设置“双清单”（第二十一条）、落实个人信息保护合规审计制度（第二十七条），《条例》也都进行了明确；同时还针对“数据可携带权”的实现条件（第二十五条）、重要数据风险评估的内容（第三十一条）进行了详细规定。在对上位法规定颗粒度的细化方面，还涉及针对重要数据的处理者报送风险评估报告的内容；区别于《征求意见稿》，《条例》还处理重要数据的大型网络平台服务提供者报送风险评估报告时还须充分说明关键业务和供应链网络数据安全等情况（第三十三条）；涉及接入平台的第三方产品和服务提供者违规处理数据对用户造成损害的，《条例》区分了网络平台服务提供者、第三方产品和服务提供者、预装应用程序的智能终端等设备生产者，分别应承担的相应责任（第四十条）。同时，《条例》也针对国家不同监管部门的职责进行了分别明确（第四十七条）；针对主管部门可以采取的网络数据安全监督检查措施进行了具体描述（第五十条）。以上规则均将在文章正文中详细分析。

导读二：《条例》与《网安法》《数安法》《个保法》的联系和区别？

《条例》依托于《网安法》《数安法》《个保法》等上位法，属于国务院发布的行政法规，与上位法共同构成了我国网络数据安全法律体系的主干，又为上位法进行了补充和细化，为上位法的网络和数据安全的相关条款进行具体化、操作化，以便责任主体能够更加有效地执行，也为行政监管提供了具体的执法依据。在整体数据安全管理体系中起到了承上启下、细化落实的关键作用。

《网安法》围绕维护国家网络安全（网络架构、设备和运行安全），对网络运营者提出网络安全保护责任，涵盖了网络基础设施安全、网络产品与服务安全、个人信息保护以及关键信息基础设施运营者（CIIO）保护等内容，强调网络空间的主权和网络运行的安全。《数安法》从国家顶层设计开始，建立了数据安全管理制度，主要聚焦于数据的分类分级管理、数据安全监测和防护、数据跨境传输的管理规则，设定与国家安全、公共利益密切相关数据的保护，以及各类数据处理者的责任与义务。《个保法》主要针对个人信息的收集、存储、使用、处理、传输、提供、公开、删除等环节进行全生命周期的保护，保障个人在个人信息处理活动中的合法权益。

《条例》一方面针对《网安法》中网络运营者处理网络数据时的安全管理措施进行了更加具体和细致的规定，确保其处理的不同类型的数据在网络运营各个方面的安全；另一方面针对《数安法》，《条例》细化了数据处理者的责任、数据处理流程等风险控制措施；进一步细化了数据跨境传输合规机制的条件、明确了不同类型数据的出境要求；针对涉及网络数据处理的组织和个人，特别是网络平台、应用服务提供者等企业，进一步细化了他们在收集、存储、传输、提供、委托处理、删除数据时的具体安全要求。结

合了上述两法，《条例》还提出了更加详细的技术措施和操作细节，例如加密、备份、访问控制、安全认证等，确保数据在不同处理阶段的安全。特别是对网络数据的处理提出了更高的要求，强调网络数据处理者在收集、存储、使用、传输时，必须采取必要技术手段防止数据泄露、篡改等安全事件。明确要求重要数据处理者定期对数据处理活动进行安全风险评估并报送风险评估报告，尤其是当数据处理活动涉及提供、委托处理、共同处理重要数据时，必须对潜在的安全风险进行评估。此外，《条例》也会依据《个保法》中的基本原则进行数据安全管理的细则制定，两者在适用中形成互补。只是《个保法》以个人权益保护为核心，《条例》则更关注整体数据（包括个人信息）的安全性管理和风险防控。两者在实际操作中，需要综合理解和遵守，以确保数据处理活动的合法性和合规性。

相较于上位法，《条例》也存在一些相对独特的内容。例如，《数安法》适用范围广泛，涵盖所有从事数据处理活动的个人、企业和政府机构，无论其是否与网络相关；《条例》进一步明确了适用对象为网络数据处理者，包括网络平台、应用服务提供者和其他涉及网络数据处理的主体。其规定的内容主要集中在对网络环境中的数据处理进行安全管理。并且《条例》明确了多个管理部门（如网信办、工信部、公安机关等）在数据安全管理中的具体职责与分工。《网安法》第五十九条至第七十五条对网络运营者未履行安全义务规定了相应的处罚，包括行政处罚、民事赔偿以及其他法律责任；《数安法》第四十四条至第五十二条对违反数据安全规定的行为也规定了警告、罚款等行政责任、民事责任以及其他法律责任。《条例》虽然也规定了行政处罚、民事赔偿以及其他法律责任，但是对违反网络数据安全规定的处罚措施根据违规行为的性质、影响程度等进行了比较详细的分级规定。详细分析请见正文部分。

《条例》的出台，旨在进一步规范网络数据处理活动，保障数据安全，促进网络数据依法合理有效利用，保护个人、组织的合法权益，维护国家安全和公共利益。本文将基于《条例》的整体框架，对《条例》进行分析解读。

（一）适用范围

《条例》第二条延续《网安法》《数安法》《个保法》等上位法规定，明确其适用于中华人民共和国境内利用网络开展的网络数据处理活动及其安全监督管理。

何为“网络数据”？此处的“网络”需要结合《网安法》进行理解，即由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的系统。另外，根据《条例》第六十二条第一款，网络数据是指通过网络处理和产生的各种电子数据。结合上述定义，网络数据具备两方面要素：一是，它指向于电子数据，相较于《数安法》中对于数据更广的定义（即“任何以电子或者其他方式对信息的记录”），《条例》将其管辖的范围仅限定于以电子方式记录的数据；二是须通过网络处理和产生，此处的网络应既包括互联网也包括局域网。

另外，《条例》还明确适用于境外开展网络数据处理活动的场景。《数安法》第二条规定了特定情形下的域外适用效力，即**以“后果论”为标准**，如果境外的数据活动对我国国家、社会、公民利益造成损害的，相关组织和个人应被追究法律责任。《个保法》第三条第二款规定，以向境内自然人提供产品或者服务为目的，或者分析、评估境内自然人的行为，即使处理活动位于境外，也适用《个保法》。《条例》第二条第二款表明其同样适用《个保法》第三条第二款的情形；倘若不构成《个保法》第三条第二款的情形，但是处理活动（无论是个人信息还是非个人信息）损害国家安全、公共利益或者公民、组织合法权益的，也适用《条例》。这体现出《条例》融合了《数安法》以“后果论”适用的域外长臂管辖的精髓。同时，《条例》第五十四条明确规定，境外的组织、个人从事危害中华人民共和国国家安全、公共利益，或者侵害中华人民共和国公民的个人信息权益的网络数据处理活动的，国家网信部门会同有关主管部门可以依法采取相应的必要措施，这也进一步彰显我国以国家利益为主导掌握数据安全主动权的坚定信念。

此外，《条例》沿袭了《个保法》的规定，同样认为自然人因个人或者家庭事务进行的个人信息处理活动不被适用。《条例》还指出，开展涉及核心数据、国家秘密、工作秘密的网络数据处理活动十分特殊，应当依据国家专门法规或者规定执行，也排除于本《条例》的适用范围。

（二）受规制对象

《条例》的规制对象覆盖面广泛，主要包括境内网络数据处理者、境外网络数据处理者，以及既作为监管主体又作为被约束主体的监督管理机构。《条例》还认为在跨境数据流动背景下，境外数据接收者的合规管理同样不容忽视，特别是在处理涉及国家安全、个人隐私和重要数据时，需满足《条例》的特殊要求。总体来看，这些主体的合规行为将直接影响整个网络数据安全管理的秩序与有效性。《条例》通过对多元主体的规制，为不同场景和角色下的数据处理行为设定了明确的红线。这种全方位、多层次的监管模式，既体现了立法者对保障网络数据安全的决心，也标志着国家在数字安全领域的法治化进程上又迈出了坚实一步。然而，《条例》的实施对企业的合规管理提出了前所未有的挑战，不同类型的主体需要投入更多资源与精力去理解并遵守复杂的法律要求。如何在合规与发展之间找到平衡，将成为企业在未来发展中必须面对的重要课题。

1、一般网络数据处理者

根据《条例》第六十二条，网络数据处理者，是指在网络数据处理活动中自主决定处理目的和处理方式的个人、组织。根据网络数据处理者处理数据的地域，可将其划分在中华人民共和国境内开展网络数据处理活动的处理者与在中华人民共和国境外开展网络数据处理活动的处理者；根据处理数据类型不同，网络数据处理者可分为重要数据处理者以及个人信息处理者。此外，根据网络数据处理者提供的业务类型不同，网络数据处理者涵盖了网络服务提供商、网络平台服务提供者（其中根据平台规模的大小，还

可区分出大型网络平台服务提供者）、预装应用的智能终端设备生产者、应用程序分发平台、网络身份统一认证公共服务平台等广泛群体。

网络数据处理者需要承担一般性的安全、合规义务与主体责任，通常不难理解。但在特殊场景和情形下，其义务及责任还可能提升和加重。具体来说：首先，当网络数据处理者因为处理了某些特殊类型的数据而需要承受比一般性合规义务更重的责任。例如其处理活动涉及重要数据或者敏感个人信息，或者开展委托处理或者共同处理活动但涉及电子政务活动和政务数据、公共服务系统和公共数据，那么网络数据处理者的合规义务将会由此升级。其次，若相关运营主体在开展业务过程中提供了网络产品与服务，或者利用网络数据面向社会提供产品或者服务，那么这些网络数据处理者都因将受保护客体的特殊性而被施加特殊义务。再者，如果网络数据处理者的某些行为较为特殊，例如使用了技术类工具收集或访问网络数据、利用网络数据向公众进行个性化推荐、使用生成式人工智能工具向公众提供服务，那么上述处理者需要遵守更高的合规义务，以保证数据处理的安全性。最后，如果网络数据处理者向境外提供产生或者来源于境内的个人信息或者重要数据，或者由于公司实体结构发生变更（如因合并、分立、解散等）而需要转移网络数据，那么该网络数据处理者也需提前履行相应的合规义务，以避免因处理活动可能产生的风险。

2、重要数据处理者

根据《条例》，重要数据处理者，是指处理特定领域、特定群体、特定区域或者达到一定精度和规模，一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能直接危害国家安全、经济运行、社会稳定、公共健康和安全的数据的个人、组织。重要数据处理者本身也属于网络数据处理者中的一类，其因处理的数据量大、数据敏感性强、潜在风险高，一旦泄露、滥用或破坏，可能会对国家安全、社会稳定或经济秩序产生严重后果，因而受到更加严格的监管。因此《条例》也因此在第四章针对重要数据处理者的义务进行了专章规定，要求内部建立严格的安全管理制度，包括识别与申报重要数据、明确网络数据安全责任人和管理机构、以及针对责任人和关键岗位人员进行背景审查；提供、委托处理、共同处理重要数据前，应当进行风险评估；涉及合并、分立、解散、破产等情形，应当采取措施保障网络数据安全，并向相关主管部门报告重要数据处置方案；定期开展安全风险评估并向相关部门报送风险评估报告等。

3、网络平台服务提供者

《条例》以专章的形式对网络平台服务提供者的责任和义务进行了明确规定。对于网络平台服务提供者，《征求意见稿》使用了“互联网平台运营者”的概念，将“互联网平台运营者”定义为向用户提供信息发布、社交、交易、支付、视听等互联网平台服务的数据处理者。此次《条例》对网络平台服务提供者并未进行明确定义，而是直接沿用了《未成年人网络保护条例》中的描述，同时又为满足全文表述一致性的要求，使用了《条例》网络数据处理者中的“网络”这一概念。结合《条例》第四十条和第四十一

条的规定，预装应用的智能终端等设备生产者、提供应用程序分发的服务提供者，都需要适用网络平台服务提供者的相关规定。

相较于《征求意见稿》，此次《条例》对于网络平台服务提供者的义务和责任有所放宽，例如，前文中所述《征求意见稿》曾要求网络平台在平台规则的重大修订前向社会公开征求意见不少于 30 个工作日，超大型网络平台需要报请主管部门同意等，此次《条例》已不再体现。单设第六章明确网络平台服务提供者义务（取代《征求意见稿》互联网平台运营者义务），通过七个条款，分别规定了一般网络平台服务提供者和大型网络平台服务提供者的责任和义务。

针对一般网络平台服务提供者，《条例》第四十条第一款要求其必须通过平台规则或合同形式明确接入其平台的第三方产品和服务提供者的网络数据安全保护义务。这意味着网络平台需要对第三方产品和服务的网络数据安全履行平台监督义务，确保他们接入平台提供的服务能够采取足够的技术和管理措施来保护数据安全。《条例》第四十条第二款进一步明确了预装应用程序的智能终端设备生产者也同样适用《条例》第四十条第一款，即预装应用程序的智能终端设备生产者需要对预装应用程序的安全性起到整体管理责任，在接入预装应用前应确保预装应用能够符合法律法规的要求。此外，根据《条例》第四十条第三款，第三方产品和服务提供者违反法律、行政法规的规定或者平台规则、合同约定开展数据处理活动，对用户造成损害的，各方应当依法承担相应责任。这里首先应当注意的是，立法者在第三方产品和服务违反法定与约定义务之间用了“或者”而不是“和”和“以及”，代表消费者只要主张平台内的第三方产品和服务提供者违法或者违约，只要二者未遵守其一，相关责任人即应当按照过错承担责任。预装应用程序若违法或违约，也应适用此规则。其次，如前所述，此前《征求意见稿》第四十四条第二款规定，第三方产品和服务提供者对用户造成损害的，用户可以要求平台运营者先行赔偿。此次《条例》第四十条第三款不再要求平台运营者先行赔偿，一定程度上体现了对于网络平台服务提供者责任的放宽，但各方可能需要在损害责任认定以及赔偿比例分担方面进行举证和主张。最后，值得注意的是，《条例》第四十条最后一款还鼓励保险公司开发网络数据损害赔偿责任险种，以增强网络平台服务提供者、第三方产品和服务提供者、预装应用程序的智能终端设备生产厂商的风险抵御能力，为义务方积极履行损害赔偿责任、为用户提出正当救济权利均提供了保障。

除上述三类网络平台服务提供者以外，《条例》第四十一条还对应用程序分发服务这一类网络平台服务提供者（例如苹果的 App Store、安卓的 Google Play、华为应用市场等）提出了相关要求。首先，应用程序分发平台应当建立应用程序核验规则并开展网络数据安全相关核验。其次，当该类平台发现待分发或者已分发的应用程序不符合法律、行政法规的规定或者国家标准的强制性要求的，应当及时采取警示、不予分发、暂停分发或者终止分发等措施。以上规定意味着，应用分发服务的网络平台服务提供者需要制定一套针对应用程序的审核标准，确保这些应用程序在上架前和运营中不会存在危害用户隐私、数据安全或影响网络安全的风险，特别是涉及用户数据的收集、存储、传输等

方面的安全措施。除发布规则外，在应用程序上架到应用商店或在运营过程中，应用商店还需要对这些应用进行定期或不定期的安全检查。例如，应用程序在首次运行时，是否弹出符合规范的隐私政策，是否告知用户其将收集哪些个人信息。如果应用程序涉及跨境数据传输，是否符合相关的跨境数据传输规定。应用程序是否明确规定了数据的保存期限、删除机制、用户对其个人数据的控制权等内容，如果隐私政策不清晰或不符合要求，应用商店应拒绝该应用上架。此外，还应核查应用程序在与其服务器通信时，是否使用了安全的加密协议（如 HTTPS），如果应用程序通过明文传输用户的聊天记录或照片，应当拒绝上架。当应用程序请求了过多的系统权限，平台应进一步核查这些权限是否合理，例如，当一个社交应用程序要求访问用户的通话记录，且未能给出合理的解释或无法向用户解释其用途，应用程序分发平台应要求该应用修改或拒绝其上线。如果涉及金融类应用，应用程序分发平台还应检查应用程序是否对用户的账户信息、交易记录等进行了端到端加密、是否采取了有效的账户保护措施，例如多因素身份验证（MFA）、密码强度要求、是否安装了防止身份盗用、异常交易监控等功能，以减少网络诈骗和数据泄露的风险。并且，应用程序分发平台还应使用自动化安全工具检测应用是否存在已知的安全漏洞或风险，譬如是否有被恶意代码注入的可能。如果相关应用程序存在能够被恶意攻击者利用的安全漏洞，应用程序分发平台应要求开发者修复后再重新提交。

《条例》第四十三条明确国家推进网络身份认证公共服务建设，按照政府引导、用户自愿原则，鼓励网络平台服务提供者支持用户使用国家网络身份认证公共服务登记、核验真实身份。2024 年 7 月 26 日，公安部和网信办曾发布《国家网络身份认证公共服务管理办法（征求意见稿）》并提出了“网号”“网证”的概念，以规范网络空间中的身份认证服务，确保在网络活动中的真实身份可追溯，防止虚假身份、匿名使用网络服务所带来的网络安全风险。此次《条例》以《个保法》《网安法》中关于网络实名制认证的要求为基础，从行政法规层级上明确了立法态度，为未来《国家网络身份认证公共服务管理办法》的正式出台明确了方向，以便推动国家级的网络身份认证平台的建设。目前《条例》对用户使用国家网络身份认证公共服务登记、核验真实身份信息持鼓励支持的政策，实则当用户在使用特定网络服务（例如社交媒体注册、在线支付、网络购物、网络游戏、网络评论等）时，通过国家认证平台的统一技术标准进行真实身份信息，包括姓名、身份证号码等内容的校验，能确保所验证的身份信息准确、真实。因此，身份认证服务网络平台提供者在提供此服务的过程中需要承担用户实名制认证中的管理责任，若发生信息泄露或违规行为，相关方需要承担法律后果。

《条例》在本章中还提到了另一类网络平台服务提供者，即大型网络平台服务提供者。关于如何认定“大型”的门槛，根据《条例》第六十二条定义，大型网络平台是指注册用户 5000 万以上或者月活用户 1000 万以上，业务类型复杂，网络数据处理活动对国家安全、经济运行、国计民生等具有重要影响的网络平台。相比于此前《征求意见稿》对于大型互联网平台运营者的定义（用户超过五千万、处理大量个人信息和重要数据、具有强大社会动员能力和市场支配地位的互联网平台运营者），《条例》将用户规模大分

成两个维度理解，其一为用户注册数量多，其二为用户月活程度高。此次设定的数量门槛并没有采取此前讨论过的《互联网平台分类分级指南（征求意见稿）》和《互联网平台落实主体责任指南（征求意见稿）》中对大型、超大型平台以年活跃用户的计数标准，也未纳入市值（估值）作为衡量规模的尺度。《条例》虽然保留了“业务类型复杂”这一考量因素，但使用“网络数据处理活动对国家安全、经济运行、国计民生等具有重要影响”取代了《征求意见稿》中“具有强大社会动员能力和市场支配地位”这一要素，主要是从受影响主体的广度和潜在风险的严重程度出发进行考量，而不仅看平台的规模和其在市场上的垄断和支配能力，确保对用户数据和公共利益产生重大影响的平台能够承担更严格的合规要求。因此，符合前述条件的网络平台提供者应当遵守《条例》第四十四条至四十六条的要求，包括每年度发布社会责任报告、不得实施差别待遇、不得无正当理由限制用户访问和使用网络数据、不得以误导、欺诈、胁迫等方式处理用户在平台上产生的网络数据等。这也与《个保法》对大型互联网平台责任加重的规定一脉相承，其中对涉及处理大量个人信息的运营者，要求其建立独立的个人信息保护机构，并定期进行外部审计。特别地，《条例》第四十六条还兼容了《反垄断指南——关于平台经济领域的反垄断指南》《平台经济反垄断指南（草案）》《国务院关于促进平台经济规范健康发展的指导意见》《关于推动平台经济健康发展的实施意见》等立法精神，对用户基数庞大的平台，明确要求其承担更多的社会责任，以消除这些平台可能利用网络数据、算法、平台规则等从事对用户产生不合理差别待遇等反竞争行为。并且，企业也应结合《互联网信息服务算法推荐管理规定》《关于加强互联网信息服务算法综合治理的指导意见》等规定理解《条例》内容，主管机构有可能依据《条例》及其他法规进一步加强对算法治理和公开透明实践的监管，规范大型网络平台服务提供者在使用算法进行信息推送、个性化推荐等服务时的合规义务。

4、承担网络数据安全和相关监督管理工作的机构

虽然政府部门本身不是被直接规制的对象，但它们在执行条例、进行数据监管和执法过程中也受到相应的约束和监督。《条例》第七章主要围绕网络数据安全监督管理的职责划分、监督检查机制、衔接和互认等方面进行了详细规定。虽然从文章体系角度，应当将监管机构的监督管理放置于责任章节之前，但由于监管机构本身也是条例的受监督对象，从避免赘述的角度，我们统一放在此处进行梳理和解读。

从职责分工来看，根据《条例》第四十七条、第四十九条以及第三十七条，国家网信部门负责统筹协调数据安全和相关监督管理工作；统筹协调主管部门及时汇总、研判、共享、发布数据安全风险相关信息；统筹协调网络数据安全信息共享、风险和威胁监测预警、安全事件应急处置；同时统筹协调有关部门建立国家数据出境安全管理专项工作机制，研究制定国家网络数据出境安全管理相关政策，协调处理网络数据出境安全重大事项。公安机关、国家安全机关在各自职责范围内承担数据安全监管职责，依法防范、查处、打击危害国家安全、公共利益的网络数据安全违法行为和犯罪活动。各地区和行业主管部门承担所在区域、行业和领域的数据安全监管职责，明确本领域、本行业网络

数据安全保护工作机构的设定、统筹制定并组织本行业、本领域网络数据安全事件应急预案、定期组织开展本行业、本领域网络数据安全风险评估，并对网络数据处理者履行网络数据安全保护义务的情况进行监督、检查（包括《条例》第五十条要求数据处理者出具情况说明、查阅文件和记录、检查设备物品和数据安全措施的运行情况等）并指导、督促其整改相关风险隐患。

值得注意的是，《条例》第四十七条第三款还提及了国家数据管理部门在具体承担数据管理工作中履行相应的网络数据安全职责。对此，可结合 2023 年中共中央、国务院发布的《国务院关于提请审议国务院机构改革方案的议案》和《国务院机构改革方案》中对国家数据局在安全管理职能方面的描述进行理解，文件特别提及国家数据局将承担“数据安全和数据开发利用的统筹监管职责”，为全国范围的数据管理和安全工作提供指导和规范。

《条例》第七章通过四个条款说明了各监管机构之间的职责分工，而后通过第五十一条、第五十二条和第五十三条对监管机构执法工作提出了管理要求。首先，第五十条第二款、第五十二条第二款，强调了各类监管机构工作之间应当配合、衔接和互认，包括个人信息保护合规审计、重要数据风险评估、数据出境安全评估等，避免企业对于此类评估或审计工作存在重复作业的情况。同时，针对重要数据风险评估和网络安全等级测评涉及内容重合的部分，认可相关结果之间互相采信的方式，降低企业合规成本和人力、物力的重复铺设。除此以外，针对监管机构在开展执法监督过程中的行为与措施提出严格要求，譬如，有关主管部门开展网络数据安全监督检查，应当客观公正，不得向被检查单位收取费用；在网络数据安全监督检查中不得访问、收集与网络数据安全无关的业务信息，获取的信息只能用于维护网络数据安全的需要，不得用于其他用途；不得将知悉的个人隐私、个人信息、商业秘密、保密商务信息等网络数据泄露或者非法向他人提供，应当依法予以保密。未履行《条例》中规定的上述要求，相关主管机关会被根据《条例》第六十条的规定依法追究法律责任。

（三）网络数据安全总体框架下的细化规定（一般规定）

《条例》第二章“一般规定”作为本法规的核心章节，为我国网络数据处理活动提供了系统的规范框架。该章从多个维度对网络数据的处理、保护和管理进行了详细规定，涵盖了非法活动的禁止性要求、网络数据处理者的责任、产品和服务的安全性要求、应急预案的制定、国家安全审查、自动化工具使用限制以及针对生成式人工智能服务安全管理等方面内容。在充分吸收《征求意见稿》及公众意见的基础上，相较于之前的《个保法》《数安法》和《网安法》，本章呈现出一系列值得关注的要点。具体分析如下：

1. 详细规定了网络数据非法处理活动的具体类型

相较于《征求意见稿》，《条例》第八条释明了何为利用网络数据从事非法活动的行为，具体涵盖窃取、以非法方式获取、非法出售及非法提供网络数据。同时，《条例》特别强调，任何个人和组织都不得提供专门用于非法活动的程序、工具；如果明知他人

从事此类非法活动，也不得为其提供任何形式的技术支持或帮助，具体包括互联网接入、服务器托管、网络存储、通讯传输以及广告推广和支付结算等技术支持和服务类型。这一修订对《网安法》第二十七条、《数安法》第三十二条中所禁止的危害网络安全行为和从事非法网络数据处理活动又进行了细化，提高了法律法规的可操作性和对非法从事网络数据处理活动的打击精度。

与现行《数安法》相比，虽然《数安法》第四章规定了数据处理者的安全保护义务，但未详细列明非法技术支持和服务提供的具体内容，而“非法网络数据活动”的背后往往涉及多种技术支持，包括互联网接入、服务器托管、网络存储和通讯传输等。《条例》新增规定对此进行了补充，若相关网络数据处理者及其相关技术支持者在明知是非法活动的情况下仍然予以协助或者提供支持的，则都可能会被认为违反本《条例》规定。例如，某个网络服务提供商明知其客户（如“丝绸之路”）从事非法活动，仍继续为其提供互联网接入服务，那么该服务提供商可能面临法律责任；如果某托管公司为一个非法运营的网站（例如销售非法商品的暗网市场）提供服务器支持，并且在知晓该网站从事非法活动后未能及时切断服务，这类行为也可能违反《条例》；类似的，提供云存储服务的公司如果已经知道存储了非法平台的数据或内容（例如非法交易记录或用户信息），而没有采取行动进行切断和报告，也可能触犯该法规；又如，平台之间或用户与平台之间的非法通讯，如果得到了技术层面的帮助，例如通过加密传输系统或私有通讯网络帮助非法活动规避监管，对被协助事宜事先知悉的技术提供方也可能受到法律追责。

2. 强化网络数据处理者的主体责任

《条例》第九条要求网络数据处理者在网络安全等级保护的基础上，建立健全网络数据安全管理制度，加强网络数据安全防护手段，处置网络数据安全事件，防范针对和利用网络数据实施的违法犯罪活动，这说明国家希望通过技术手段和管理制度相结合的方式，提升网络数据的安全防护水平。并且，该条强调了网络数据处理者对其所处理的网络数据安全承担主体责任，一旦发生数据泄露、篡改或非法获取等安全事件，网络数据处理者将直接面临法律责任。这不仅迫使企业在遵守《信息安全等级保护管理办法》《信息安全技术 网络安全等级保护基本要求（GB/T 22239-2019）》等法律法规和标准的基础上，根据不同数据的特点和风险程度，加强安全投入，采取动态的网络数据安全保障措施，防止网络数据被违法犯罪分子利用，也反映出国家在应对日益复杂的网络安全威胁时，采取了更为系统、全面的治理思路，对企业提出了更高的安全管理要求。

3. 明确网络产品和服务的安全性要求与应急预案

《条例》第十条对网络数据处理者提供网络产品和服务提出了安全性要求。相较于《征求意见稿》及此前发布的《网络产品安全漏洞管理规定》，《条例》第十条更加注重提升整体网络安全水平、保护用户权益，不仅与《数安法》保持了一致标准，强制性要求网络产品和服务须符合国家标准，而且规定当存在安全缺陷、漏洞等风险时，应立即采取补救措施，并及时告知用户、报告主管部门。相比之下，《网络产品安全漏洞管理

规定》仅规定了网络产品提供者在发现或获知安全漏洞后 2 日内向工业和信息化部网络安全威胁和漏洞信息共享平台报送相关信息。此外，《条例》还要求在涉及国家安全和公共利益时，网络数据处理者应具备快速响应能力，当安全缺陷、漏洞等风险涉及危害国家安全、公共利益时，网络数据处理者须在 24 小时内向有关主管部门报告。这与 2023 年 12 月 8 日网信办发布的《网络安全事件报告管理办法（征求意见稿）》要求对较大、重大或特别重大网络安全事件在 24 小时内补报相关情况和《计算机信息系统安全保护条例》要求在 24 小时内向当地县级以上人民政府公安机关报告计算机系统中发生的案件存在异曲同工之处。实践中，对无任何风险应对经验的企业来说，履行 24 小时内的网络风险报告义务存在一定的压力，因此建议相关企业在日常管理中做好充分的准备和演练。

针对网络安全事件的报告和通知，《网安法》第二十五条中已明确要求网络运营者应当事前制定网络安全事件应急预案，并在发生网络安全事件时立即启动该应急预案，防止危害扩大，并按照规定向有关主管部门报告。《数安法》也提及了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。相较于《征求意见稿》，《条例》删除了安全事件报告的具体时间要求（如“在发生安全事件的八小时内”和“在事件处置完毕后五个工作日内”），而是采用了更为原则性的表述，这可能是为了给予网络数据处理者根据事件的具体情况灵活处理的空间，这种灵活性也意味着关于报告程序的具体要求将依赖于《网络安全事件报告管理办法》正式稿的出台。除了制定应急预案和向主管部门报告、通知受影响主体，《条例》第十一条还增加了网络数据处理者在处置网络数据安全事件过程中发现涉嫌违法犯罪线索时的报案、配合侦查、调查和处置工作的义务。

除此以外，《条例》第二十条还要求面向社会提供产品、服务的网络数据处理者应当接受社会监督，建立便捷的网络数据安全投诉、举报渠道，公布投诉、举报方式等信息，及时受理并处理网络数据安全投诉、举报。通过强化社会监督，鼓励公众积极举报潜在的网络数据安全问题，不仅能够及时发现和解决潜在的网络数据安全风险，还能有效地保障公众在网络数据安全保护中的知情权和参与权。这种双重监督模式有助于提高网络数据安全问题处理的透明度，形成一种更广泛的监督体系，增强网络数据处理者的安全意识和自律性，进而促使其在网络数据安全管理中更加严谨和负责。

4. 界定数据处理具体场景下的管理要求

首先，《条例》第六十二条对委托处理和共同处理的概念进行了明确。虽然基本定义与《个保法》中的概念如出一辙，但《条例》将处理重要数据也纳入定义范围。针对对外提供或委托处理个人信息和重要数据，《条例》第十二条规定了网络数据处理者必须通过合同等形式与网络数据接收方明确约定处理目的、方式、范围及安全保护义务，并由网络数据处理者对网络数据接收方的履行情况进行监督。同时，相较于《征求意见稿》，《条例》将相关数据处理情况记录的保存期限从“至少五年”缩短为“至少三年”。

我们理解，这种调整可能是为了减轻网络数据处理者的合规负担，同时也考虑到了实际操作的可行性和数据安全保护的基本需求。

此外，在电子政务系统以及公共服务系统的委外承建事宜方面，相较于《征求意见稿》，《条例》加强了对政务数据处理的监管和保护要求。第十五条和第十六条明确，一方面国家机关在委托他人建设、运行、维护电子政务系统时，必须经过严格的依法批准程序，国家机关需要监督受托方履行网络数据安全保护义务，确保政务数据的安全。另一方面，国家机关应当通过合同约定，明确受托方的网络数据处理权限、履行网络数据安全保护义务和保护责任，不得在未经委托方同意的情况下对网络数据进行关联分析。这主要是针对许多企业受国家机关委托处理数据的现状进行了更加明确的规制，可结合导读一相关内容进行参考。

5. 公司结构发生变化时的网络数据管理要求

《条例》第十四条规定了当网络数据处理者发生因合并、分立、解散、破产等原因需要转移网络数据的情形，其与《个保法》第二十二条的规定类似，都要求接收方继续履行网络数据安全保护义务或者个人信息保护义务。当前，随着资产收购、股权转让和企业破产等商业行为日益频繁，网络数据作为企业的一项重要资产，往往成为交易中不可忽视的部分。然而，在这些商业活动中，数据的安全转移和后续保护往往面临巨大挑战。首先，如果交易仍处于保密状态，若被交易的网络数据涉及个人信息，需要考虑是否对个人进行告知，这取决于交易双方针对原先处理目的、处理方式是否发生变更的商议。其次，针对提供方，需要按照交易条件进行交割，不得擅自留存数据，且在交易前妥善存储被交易的网络数据；针对接收方，则需严格遵循相关法律规定和安全标准，确保在转移过程中的传输安全和最小范围的人员接触，否则交易前或者交易中一旦发生交易数据泄露或遭到非法利用，将可能对交易双方产生重大且无法挽回的影响。特别是在企业破产清算或解散的情况下，很多公司易忽视对剩余数据的安全处理，或未对数据的去向做出明确交代，导致用户个人信息、商业机密，甚至破产企业涉及处理的重要数据泄露风险增大。《条例》第十四条明确要求了公司主体结构产生特殊情况下，数据接收方仍须承担保护责任，从而避免数据因企业破产、分立、解散等而被非法获取或被滥用。

重要数据处理者因合并、分立、解散、破产等可能影响重要数据安全的，《条例》第三十二条另有规定，我们将在下文进一步分析。

6. 回应新兴技术处理网络数据的监管要求

与《生成式人工智能服务管理暂行办法》第七条中的规定相衔接，《条例》第十九条要求提供生成式人工智能服务的网络数据处理者加强针对训练数据的安全管理。数据质量和安全直接决定了模型的表现和风险，因此《生成式人工智能服务管理暂行办法》要求服务提供者使用具有合法来源的数据和基础模型，且在涉及处理个人信息时，应当事先取得个人同意或者符合法律法规的其他情形。在实际操作中，生成式人工智能的应用已渗透到各个行业，如自动化文本生成、图像生成、聊天机器人等。一旦训练数据包

含有害、不合规信息，或者处理不当，生成的内容便有可能出现偏见、错误，甚至侵犯个人隐私、侵犯他人权益。因此，网络数据处理者有责任从源头上加强数据安全管理，通过严格筛选、清理和监管训练数据，降低生成内容的潜在风险。《条例》进一步强调了防范和处置网络数据安全风险的必要性，要求网络数据处理者采取有效措施，对训练数据采取严格的安全措施，如加密存储、访问控制、去标识化等，以防止数据泄露或被不法分子利用。同时，处理者还需要制定完善的应急预案，及时处置因数据不当使用引发的网络安全事件或数据合规风险，防范各种安全隐患。

此外，《条例》第十八条明确地规范了网络数据处理者在使用自动化工具访问和收集网络数据时的行为。根据该条规定，《条例》间接承认了自动化采集工具本身的技术中立性，因此要求网络数据处理者在使用自动化工具前应当进行风险影响评估，此外，《条例》明确要求不得利用爬虫等自动化采集工具非法侵入他人的网络或干扰第三方网络服务的正常运行。《数据安全管理办法（征求意见稿）》第十六条规定，当采用爬虫技术访问收集流量超过网站日均流量三分之一时，可能会被认为“严重影响网站运行”。但《条例》没有纠结究竟多大流量构成干扰网络正常运行，实践中网络数据处理者也往往没有能力测试到被爬网站的流量数量，原有规定反而造成不少网络数据处理者的困惑，甚至权利人凭借此条寻求救济的也寥寥无几。与《条例》第十八条相媲美的还有《网络反不正当竞争暂行规定》，其明确规定利用技术手段，非法获取、使用其他经营者合法持有的数据，妨碍、破坏其他经营者合法提供的网络产品或者服务的正常运行的行为，可能构成不正当竞争，从反不正当竞争的角度规范爬虫等自动化采集数据的行为。

然而，自动化工具和生成式人工智能服务的技术复杂性较高，如何科学合理地评估其影响并进行有效的监管，有赖于实践层面进不断探索和总结。此外，《条例》还进一步规定了利用自动化采集技术采集非必要个人信息的影响和相关处置措施，我们将在下一章节中进一步分析。

（四）数据的特殊类型之一：个人信息保护细化规定

《条例》第三章在《个保法》及其他个人信息保护相关法律法规和标准的基础上，进一步细化了个人信息处理活动中的告知义务、同意的获取、主体权利的保障以及跨境数据流动等方面的要求。特别地，《条例》针对自动化采集技术的应用和“数据可携带权”，提出明确具体的执行路径。此外，相较于《征求意见稿》，本章内容在个人信息保护规则上进行了优化，更加注重实践中的可行性，体现了我国在数字经济背景下对个人信息保护的重视和对国际立法趋势的积极回应，具体关注要点如下：

1. 强化个人信息处理规则中的告知义务

首先，《个保法》第十七条规定了处理个人信息时，个人信息处理者应当以显著方式、清晰易懂的语言真实、准确、完整地向个人告知相关事项，《条例》第二十一条进一步细化了上述规则。在告知上，《条例》明确了个人信息处理规则的展示方式，即“集中公开展示”“易于访问”“置于醒目位置”。同时，对于网络数据处理者向其他网络数

据处理者提供个人信息的情况，《条例》要求以清单等形式予以列明，这一规定与 2021 年 11 月工业和信息化部发布的《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”制度相呼应。上述通知要求相关企业建立“已收集个人信息清单”和“与第三方共享个人信息清单”，以增强用户对个人信息处理活动的感知和控制。而《条例》的出台，标志着来源于工信部规范性文件的“双清单”制度已经正式上升到了行政法规层面规范的内容。在告知内容上，除《个保法》中提到的基本信息外，《条例》还特别指出需包含处理敏感个人信息的必要性及对个人权益的影响、个人信息保存期限及其确定方法等内容。我们理解，这一调整有利于提高个人信息主体对自身合法权益被侵犯风险的认知水平，同时也促使网络数据处理者在设计产品时应充分考虑隐私保护的因素。

值得注意的是，相较于《征求意见稿》，《条例》第二十一条中对于个人信息保存期限的规定更加灵活。针对难以事先确定保存期限的情况，允许网络数据处理者根据实际情况制定具体的确定方法，这种灵活性既保证了个人信息主体的信息安全，又给予了网络数据处理者一定的操作空间。从落地角度，企业可基于内部数据存储策略，在个人信息处理规则中明确具体的存储期限，也可将确定存储期限的流程和要求向用户进行告知。

最后，《条例》第二十一条沿袭了《儿童个人信息网络保护规定》的规定，特别指出对于不满十四周岁未成年人的信息处理需要具备专门的个人信息处理规则。考虑到儿童作为特殊群体，在使用互联网服务时往往缺乏足够的判断力和自我保护能力，因此给予他们额外的关注具有必要性。

2. 强化用户隐私保护与增强透明度

《条例》第二十二条建立在《个保法》第十三条合法性基础上，但特别针对“同意”这项合法性基础进行了重申并细化了具体要求，包括同意的表达应当“自愿”、同意的范围应该符合必要性、当个人信息的处理目的、方式、种类发生变更的，应当重新取得个人同意。该条第一款第五项还规定“不得在个人明确表示不同意处理其个人信息后，频繁征求同意”。在实践中，一些应用程序或网络数据处理者可能会采用不断弹出请求窗口的方式，试图改变用户的决定，这种行为不仅干扰了用户体验，也违背了用户的真实意愿，即使用户无奈最后按了“同意”键，但这样的同意应当属于“无效”的同意。与《信息安全技术 个人信息安全规范（GB/T 35273-2020）》第 5.3 条 d) 项规定相呼应，这个规定有利于减少网络数据处理者利用模糊规则进行反复请求的机会，从而避免相关用户受到不必要的打扰，能够有效提升整体用户体验。针对处理除儿童个人信息以外的敏感个人信息，《条例》还规定应当取得个人的单独同意或者法律、行政法规规定的书面同意；针对处理儿童个人信息，《条例》要求网络数据处理者应当取得未成年人的父母或者其他监护人的同意。以上规定连同《条例》第二十三条个人行权要求，均未超出《个保法》的相关规定。

3. 细化“数据可携带权”的实现途径

“数据可携带权”作为一类新型权利，在借鉴欧盟《通用数据保护条例》（GDPR）立法经验的基础上，《个保法》第四十五条第三款仅对其做出原则性的界定，即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。然而，何为“国家网信部门规定的条件”，《个保法》并未公布其解。并且，《个保法》实施后，由于缺乏实施细则，实践中，要实现此条的操作技术难度也较高，因此企业目前仅实现了“数据可携带权”的一半含义，即“副本下载”，尚未能充分实现另一半立法本意，即数据向第三方产品和服务提供方实现完全移送。

《条例》第二十五条首次以立法形式细化了个人信息转移请求的实现途径，使得个人信息转移请求不再是抽象的原则。这不仅提高了法律条文的可执行性，还减少了因解释模糊而产生的争议。具体而言，该条明确规定个人信息转移请求的条件，须涵盖请求人的真实身份验证、待转移个人信息的范围（仅限于本人同意或基于合同约定部分）、具备可转移此个人信息的技术可行性及保护其他相关方合法权益的要求，这一规定为网络数据处理者提供了清晰的操作指南，对《个保法》第四十五条第三款预留的伏笔进行了填补。此外，为平衡转移方与转入方的利益，例如由于用户请求多次转移，使网络数据处理者发生了额外的运营和技术成本，法规允许网络数据处理者在评估后向提出请求的用户主张超出合理范围的必要费用。在评估前述问题的过程中，网络数据处理者可以引入个人信息保护影响评估等流程，以便评估与平衡转移行为对个人信息主体权利和他人合法权益可能造成的影响。

4. 自动化采集技术的应用限制

即使前文已经针对《条例》第十八条关于使用自动化工具访问、收集网络数据的规定进行了分析，《条例》第二十四条又针对使用自动化采集技术等手段无法避免采集到非必要个人信息或者采集了未依法取得个人同意的个人信息等情况提出了解决方案——即删除或匿名化处理此类不合规信息。此外，《条例》还特别考虑了实践中的复杂性和多样性，对于法律、行政法规规定的保存期限未届满或者凭借网络数据处理者当时的技术手段和经验难以实现删除的，允许网络数据处理者停止除存储和必要的安全保护措施之外的处理活动。这种灵活的处理方式既为网络数据处理者提供了在特定条件下合理的应对策略，从而避免了过于僵化的法律规定给实际操作带来的困难，又敦促网络数据处理者仍然有义务采取必要措施妥善管理和保护个人信息，并且更加谨慎地对待自动化采集过程中可能产生的非必要信息，防止用户个人信息被滥用或泄露。

5. 落实对境外网络数据处理者处理境内个人信息的监管

《条例》第二十六条主要适用于境外网络数据处理者处理中国境内自然人个人信息的情形，特别强调个人信息保护层面的责任落实。这体现了中国对境外数据处理活动的监管力度不断加强，并释放出明确的信号：境外网络数据处理者不仅要符合当地法律，还必须遵守中国的数据保护法律法规，这也为国际企业在华运营（特别是在中国境内未

设立法人实体、办事机构，且服务器部署于境外但收集中国境内个人信息的企业）提供了清晰的合规指引。该条首先要求境外网络数据处理者按照《个保法》第五十三条的要求，在境内设立专门机构或指定代表，并向所在地的市级网信部门报送相关信息，如机构名称、代表姓名及联系方式。这一要求旨在确保境外企业处理中国境内用户个人信息时有具体的责任主体可以追溯和监管，防止出现个人信息管理的“真空地带”，确保数据保护法律法规能够得到有效执行。其次，该条明确了具体的报送对象为“设区的市级网信部门”，增加了信息共享和协同监管的机制，规定接收到信息的网信部门应当及时通报同级有关主管部门，从而增强信息透明度，便于各监管部门在发现数据泄露、滥用等安全事件时，能够迅速采取应对措施，对违规行为进行及时查处。

6. 网络数据处理者处理 1000 万以上个人信息的特殊合规义务

关于重要数据的识别和认定，《信息安全技术 重要数据识别指南（征求意见稿）》《数据安全技术 数据分类分级规则（GB/T 43697-2024）》及特定行业的法律规范和标准已提供了一定的指导，但是其中对于特定数量的个人信息能否构成重要数据尚未形成统一标准。《条例》第二十八条明确规定，处理 1000 万人以上个人信息的网络数据处理者，还应当遵守《条例》第三十条（任命数据安全负责人及管理机构）和第三十二条（合并、分立、解散、破产时的报送义务）中对于重要数据的处理者的规定。相较于《征求意见稿》中 100 万的量级规定，本次《条例》放宽了认定门槛，这意味着对于处理个人信息数量在 100 万到 1000 万之间的企业，可以免于按重要数据处理者的合规要求和监管措施予以执行；同时，《条例》也缩小了适用条款的范围，要求符合条件的网络数据处理者仅遵守《条例》第三十条和第三十二条的规定，而非遵守《征求意见稿》第四章中针对重要数据处理者的所有规定。这反映了立法者在平衡监管力度与企业运营成本之间进行了成熟考虑，避免对部分百万级企业造成过大的合规负担。

（五）数据的特殊类型之二：重要数据的细化规定

《条例》第四章规定了针对重要数据的安全管理要求，重点包括如下方面：

1. 重要数据目录与重要数据的识别、申报和确认

《条例》第六十二条明确，重要数据是指特定领域、特定群体、特定区域或者达到一定精度和规模，一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能直接危害国家安全、经济运行、社会稳定、公共健康和安全的数据。相比于《征求意见稿》的列举式定义，《条例》的定义进行了提炼和精简，并基于《数据出境安全评估办法》《数据安全技术 数据分类分级规则（GB/T 43697-2024）》等相关法规标准中对于重要数据的定义[8]进一步优化和更新了表述。

[8] 《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。
《数据安全技术 数据分类分级规则（GB/T 43697-2024）》3.2 重要数据：特定领域、特定群体、特定区域或者达到一定精度和规模，一旦遭到篡改、破坏、泄露，可能直接危害国家安全、经济运行、社会稳定、公共健康和安全的

为了保障重要数据安全，《条例》第二十九条第一款首先基于《数安法》的原则性要求[9]，明确国家数据安全工作协调机制，统筹协调有关部门制定重要数据目录，加强对重要数据的保护。同时敦促各地区、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，对列入目录的网络数据进行重点保护。

《条例》第二十九条第二款重点规定了网络数据处理者对重要数据的识别、申报义务与相关地区、部门的确认和告知、公开要求，具体可包括如下步骤：

首先，网络数据处理者应当按照国家有关规定识别重要数据。即企业应当首先自行判断是否涉及处理重要数据。具体而言，企业需要对于所持有的数据资产进行梳理，参考行业相关法律法规、各地区发布的重要数据目录和/或《数据安全技术 数据分类分级规则（GB/T 43697-2024）》等国家标准所列举的重要数据识别因素进行判断，明确企业收集的数据类型，识别数据资产清单中各类数据的用途、面临的主要安全威胁，判断数据安全性（保密性、完整性、可用性等）遭破坏后可能对国家安全及公共利益造成的影响，形成本企业的重要数据目录。

其次，在识别企业内部的重要数据后，该网络数据处理者还需要履行申报义务。但《条例》尚未明确申报重要数据的具体流程、时限和申报监管机构，因此实践中企业如何进行申报还有待未来相关监管机构的进一步明确。另外，《条例》未采纳《征求意见稿》中要求数据处理者在识别重要数据后的十五个工作日内向设区的市级网信部门备案的义务[10]。

最后，待企业完成自主申报后，根据《条例》的规定，最终是否属于重要数据的判定结果应当由相关地区、部门进行确认。对确认为重要数据的，相关地区、部门应当及时向企业告知或者公开发布重要数据目录、清单，企业应当履行网络数据安全保护责任。

此外，《条例》第二十九条第三款还鼓励性地建议企业使用数据标签标识等技术和产品。根据属性、用途、敏感度等信息给特定数据打上相应的标签或标识，不仅能够帮助企业实现对数据的分类分级，以此清晰地知道某一数据的类型、重要性、访问权限以及处理方式，还能提高本企业对重要数据安全管理水平，以及帮助企业在出现数据合规

数据。

[9] 《数据安全法》第二十一条　国家建立数据分类分级保护制度，根据数据在经济社会发展中的重要程度，以及一旦遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者个人、组织合法权益造成的危害程度，对数据实行分类分级保护。国家数据安全工作协调机制统筹协调有关部门制定重要数据目录，加强对重要数据的保护。…… 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，对列入目录的数据进行重点保护。

[10] 《网络数据安全管理条例（征求意见稿）》第二十九条 重要数据的处理者，应当在识别其重要数据后的十五个工作日内向设区的市级网信部门备案，备案内容包括：
（一）数据处理者基本信息，数据安全管理机构信息、数据安全负责人姓名和联系方式等；
（二）处理数据的目的、规模、方式、范围、类型、存储期限、存储地点等，不包括数据内容本身；
（三）国家网信部门和主管、监管部门规定的其他备案内容。
处理数据的目的、范围、类型及数据安全防护措施等有重大变化的，应当重新备案。
依据部门职责分工，网信部门与有关部门共享备案信息。

问题时更容易追踪数据的来源、流动情况和处理过程，以便有效应对潜在的数据泄露和风险事件，并提升审计效率。

2. 网络数据安全责任人与安全管理机构

《条例》第三十条第一款要求重要数据的处理者应当明确网络数据安全负责人和网络数据安全管理机构。网络数据安全管理机构应当履行下列网络数据安全保护责任：

1) 制定实施网络数据安全管理制度、操作规程和网络数据安全事件应急预案；

2) 定期组织开展网络数据安全风险监测、风险评估、应急演练、宣传教育培训等活动，及时处置网络数据安全风险和事件；

3) 受理并处理网络数据安全投诉、举报。

在网络数据安全负责人的任职方面，《条例》第三十条第二款要求网络数据安全负责人应当具备网络数据安全专业知识和相关管理工作经历，由网络数据处理者管理层成员担任，有权直接向有关主管部门报告网络数据安全情况。

值得注意的是，《条例》第三十条第三款还明确要求“掌握有关主管部门规定的特定种类、特定规模重要数据的网络数据处理者，应当对网络数据安全负责人和关键岗位的人员进行安全背景审查，加强相关人员培训”。因此，建议企业应当特别关注所在行业主管部门是否已经发布过针对特定种类、规模的重要数据认定清单或者应当专项咨询监管。例如，虽然《汽车数据安全管理若干规定（试行）》明确规定了汽车领域特定种类（如车辆流量、物流等反映经济运行情况的数据、包含人脸信息、车牌信息等的车外视频、图像数据等）、规模（涉及个人信息主体超过 10 万人的个人信息）属于重要数据[11]，但交通部仍然需要对掌握哪些种类和规模重要数据的企业应当对网络数据安全负责人和关键岗位人员进行严格意义的背景审查做出明确指示。在主管部门尚未给出明确指引前，若已经有相关部门规章规定了某行业特定类型数据为重要数据的，建议该处理重要数据的网络数据处理者对聘用的网络数据安全负责人和关键岗位人员在入职前或者启动专项前均宜启动背景审查。针对背景审查的具体内容，企业可以参考《信息安全技术 个人信息安全规范（GB/T 35273-2020）》第 11.6（a）条的规定，包括审查相关人员的犯罪记录、诚信状况等情况。《条例》规定，符合上述条件进行背景审查时，可以申

[11] 《汽车数据安全管理若干规定（试行）》第三条明确在汽车领域下的重要数据包括：
（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；
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。

请公安机关、国家安全机关协助。具体如何申请公安机关和国家公安机关的协助，可能有赖于实践中的进一步观察。

3. 重要数据提供、委托处理或共同处理的风险评估

根据《条例》第三十一条，如果企业作为重要数据处理者，涉及向外部第三方提供、委托处理或者共同处理重要数据的，应当依据《条例》的规定就该处理活动开展风险评估；但如果是企业为了履行法定职责或者相关法定义务的，则可以豁免该风险评估的要求。相比于《征求意见稿》，《条例》未将“交易”“向境外提供”两种场景纳入风险评估范畴，原因是“交易”的范围太大，可能涉及第三十二条（合并、分立、解散、破产等）中的某些场景，也可能被第十二条向其他网络数据处理者提供所包含；如果未得到合法授权的，还可能落入第八条规定的非法向他人提供的情况。企业“向境外提供重要数据”前必须经过数据出境安全评估，而企业向网信部门提出安全评估申请前还会进行数据出境风险自评估。这些都已经在在《数据出境安全评估办法》中进行了规定且评估内容比较特殊，因此无需包括在《条例》第三十一条中。此外，《条例》还删除了在共享、交易、委托处理重要数据前获取主管部门或网信部门同意的前置审批要求[12]。这一变化体现了立法层面从强调事前的行政审批向企业履行自主合规管理和风险管理的转变，不仅提高了企业的自主性和灵活性，也更加符合国际数据安全管理的趋势。同时，这种自主评估机制并不意味着放松监管。企业的风险评估结果可能需要在后续监管中接受检查，一旦被发现未能进行适当评估或未采取足够的安全措施，相关网络数据处理者仍将面临严厉处罚。这种事后监督的方式也增强了监管的弹性，优化了监管资源的配置，使得监管部门可以根据实际情况调整监管力度。

根据《条例》，在涉及提供、委托处理、共同处理场景下的风险评估应当重点评估下列内容：

1) **合法正当必要性：**提供、委托处理、共同处理网络数据，以及网络数据接收方处理网络数据的目的、方式、范围等是否合法、正当、必要；

2) **数据泄露的风险：**提供、委托处理、共同处理的网络数据遭到篡改、破坏、泄露或者非法获取、非法利用的风险，以及对国家安全、公共利益或者个人、组织合法权益带来的风险；

3) **数据接收方背景：**网络数据接收方的诚信、守法等情况；

4) **合同义务约定：**与网络数据接收方订立或者拟订立的相关合同中关于网络数据安全的要求能否有效约束网络数据接收方履行网络数据安全保护义务；

5) **技术管理措施有效性：**采取或者拟采取的技术和管理措施等能否有效防范网络

[12] 《征求意见稿》第三十三条 数据处理者共享、交易、委托处理重要数据的，应当征得设区的市级及以上主管部门同意，主管部门不明确的，应当征得设区的市级及以上网信部门同意。

数据遭到篡改、破坏、泄露或者非法获取、非法利用等风险；

6) **其他内容：**有关主管部门规定的其他评估内容。

与《征求意见稿》相比，《条例》虽然未明确评估风险为高的后果，但从合规实践来看，如果企业经过评估认为重要数据的共享、委托处理或共同处理可能危害国家安全、经济发展和公共利益，则企业应当避免共享、委托处理或共同处理数据，以免引发监管部门的关注和相关处罚后果。

4. 重要数据处理者合并、分立、解散、破产时的报告义务

《条例》第三十二条规定了重要数据处理者发生合并、分立、分散、破产等情况且经过评估认为可能影响重要数据安全的，重要数据处理者应采取措施履行网络安全保障与上报义务。不难理解，企业在合并、分立、解散、破产等情况下，可能会涉及数据资产的转移或处置，而重要数据的特殊性决定了其处理不当会对国家安全、公共利益、个人隐私等产生重大影响。因此，《条例》要求重要数据处理者上报处置方案、接收方信息等，旨在确保数据处理过程经过充分的安全考量，防止数据的滥用、泄露或非法转移。同时，通过上报处置方案，主管部门能够全面了解重要数据的处置过程，从而在需要时进行指导、干预或采取措施，以保证网络数据的安全和合规性。由于重要数据涉及到国家安全、经济运行、社会稳定等重大利益，因此需要受到较高层级的监管，以确保各级政府能够有足够的权限和能力来应对潜在风险。省级以上的主管部门通常具备更高的资源和权威，能够处理更复杂和重大的数据安全事件，因此相比于《征求意见稿》[13]，《条例》提高了上报部门的级别、细化了需要上报的内容，要求重要数据的处理企业需要向省级以上有关主管部门报告重要数据处置方案、接收方的名称或者姓名和联系方式等；主管部门不明确的，应当向省级以上数据安全工作协调机制报告。“省级以上数据安全工作协调机制”是指由中央网信办及相关部委组成的跨部门协调机构，负责跨行业、跨领域的网络数据安全监管。对于很多企业来说，在合并、分立或解散时，可能不清楚具体应该向哪个主管部门报告，尤其是在数据涉及多个行业或跨区域的情况下，不同部门之间的管辖权还可能不明确。如果行业主管部门或网信部门没有清晰界定的，对重要数据的处置需要由更高行政级别的行政机关进行综合协调。省级以上的主管部门或协调机制能够跨部门、跨地区进行监督管理，避免地方保护主义或部门壁垒，确保跨部门和区域下的的数据安全措施在全国统一实施。

5. 重要数据处理者的年度风险评估

《数安法》第三十条提出，重要数据的处理者应当按照规定对其数据处理活动定期开展风险评估，并向有关主管部门报送风险评估报告。风险评估报告应当包括网络数据处理者所处理的重要数据的种类、数量、开展数据处理活动的情况、面临的数据安全风

[13] 根据《征求意见稿》第十四条，企业发生合并、重组、分立等情况的，数据接收方应当继续履行数据安全保护义务，涉及重要数据的，应当向设区的市级主管部门报告。若企业发生解散、被宣告破产等情况的，应当向设区的市级主管部门报告，按照相关要求移交或删除数据，主管部门不明确的，应当向设区的市级网信部门报告。

险及其应对措施等。部分行业（例如汽车行业）也在部门规章中明确了年度风险评估报告报送的要求。《条例》第三十三条进一步细化规定了重要数据年度风险评估的频率与报告应涉及的内容等。首先，重要数据的处理者应当每年度对其网络数据处理活动开展风险评估；其次，重要数据处理者需要向省级以上有关主管部门报送风险评估报告；再次，由于网络数据安全涉及网信部门、公安机关等多个监管和执法机构的共同管理，形成合力提前准备提升风险预警和应对能力，防范潜在的网络安全事件，因此有关主管部门在接收到重要数据处理者提交的年度风险评估报告后，还应当及时通报同级网信部门、公安机关。最后，年度风险评估报告应当包括下列内容：

1) 网络数据处理者基本信息、网络数据安全管理机构信息、网络数据安全负责人姓名和联系方式等；

2) 处理重要数据的目的、种类、数量、方式、范围、存储期限、存储地点等，开展网络数据处理活动的情况，不包括网络数据内容本身；

3) 网络数据安全管理制度及实施情况，加密、备份、标签标识、访问控制、安全认证等技术措施和其他必要措施及其有效性；

4) 发现的网络数据安全风险，发生的网络数据安全事件及处置情况；

5) 提供、委托处理、共同处理重要数据的风险评估情况；

6) 网络数据出境情况；

7) 有关主管部门规定的其他报告内容。

《条例》特别指出，处理重要数据的大型网络平台服务提供者（定义详见本文第二章第 3 点的内容）报送的风险评估报告，除包括前款规定的内容外，还应当充分说明关键业务和供应链网络数据安全等情况。

如前所述，首先，大型网络平台涉及到的用户数量巨大，且业务类型通常涵盖电子商务、支付服务、社交媒体、云服务等，业务流程极其复杂，其处理网络数据的影响力远远超过一般的网络数据处理者。一旦这些平台的关键业务或供应链受到攻击，可能产生系统性风险，不仅关乎企业本身，也可能影响多个行业和领域的稳定性，乃至对国家安全产生重大影响。

大型网络平台的关键业务往往涉及大量的数据交互和共享，存在多种多样的数据风险，例如涉及用户数据、支付信息、交易记录等敏感数据。因此，在评估报告中详细说明关键业务的数据安全状况，有助于主管机构提前了解并识别该平台的哪些业务节点可能出现数据泄露或滥用的风险，有可能帮助该大型网络平台采取针对性的保护措施进行事先防范。同时，大型网络平台往往也依赖复杂的供应链，包括硬件提供商、软件供应商、外包服务等，某些合作伙伴或外包商倘若存在较低的安全保障措施，链条中的任何一方出现任何漏洞都可能成为攻击者的突破口，进而波及整个平台。况且，有些大型网

络平台的供应链中还可能涉及到海外的软硬件供应商，特别是网络平台在使用国外服务器、数据存储设备或软件的时候，还存在潜在的供应链攻击或服务断供的风险。这类平台的数据安全问题一旦被利用，可能对国家经济、公共服务以及社会稳定造成巨大影响。因此，要求充分说明供应链的安全情况，有助于主管部门识别和控制这种外部安全威胁，提前掌握企业是否存在过度依赖国外供应链的情况，评估可能的地缘政治风险带来的安全威胁。

大型网络平台的关键业务与供应链的安全性，往往直接或间接地与国家安全和公共利益挂钩，但由于其规模和业务复杂性，网络数据安全的管理需要差异化的措施，不可能一刀切。因此，要求大型平台报告中详细说明关键业务和供应链安全情况，有助于主管部门针对具体的业务场景制定更精细化的监管要求。

《条例》还要求，如果重要数据的处理者存在可能危害国家安全的重要数据处理活动的，省级以上有关主管部门应当责令其采取整改或者停止处理重要数据等措施，重要数据的处理者应当按照有关要求立即采取措施。此外，相比于《征求意见稿》第三十二条，《条例》删除了赴境外上市的数据处理者进行年度风险评估的要求，因为现在香港联交所在聆讯前会要求发行人提供数据合规相关的专业法律意见，而律师出具专业法律意见前，一般都会要求企业进行严格的由第三方中介机构主导的全面风险评估或审计；而赴境外上市的数据处理者如果涉及处理重要数据的，则仍然需要遵守《条例》第三十三条的规定，因此《征求意见稿》的考虑之意，实践中都有在被执行。立法者从抓主要矛盾解决问题的视角，取消赴境外上市的数据处理者进行年度风险评估是合理的，也是进一步对企业合规义务减负的表现。同时，《条例》也删除了须“在每年 1 月 31 日前”提交报告的时间要求以及评估报告“应当至少保留三年”的要求，而留给企业很多自主、灵活处理的权利。

（六）网络数据处理活动之特殊行为规定：网络数据跨境安全管理

《条例》第五章规定了涉及数据跨境传输的安全管理要求，重点包括如下方面：

1. 向境外提供个人信息的合规机制

在总结《数据出境安全评估办法》《个人信息出境标准合同办法》《促进和规范数据跨境流动规定》等部门规章制定实施经验基础上，《条例》第三十四条进一步明确了国家网信部门在网络数据出境活动中的功能与作用，同时优化了数据跨境流动的合规机制。《条例》第三十五条规定了七种向境外提供个人信息的条件以及一项兜底条款，既融合了《个保法》的三大数据跨境传输合规机制，也包括《促进和规范数据跨境流动规定》中规定的豁免情形（*相关解读可参考*《流动与安全并重：《促进和规范数据跨境流动规定》来了，企业应当如何应对？》）。并且，结合《条例》第三十六条规定的依据中国加入的国际条约、协定向境外提供个人信息的特殊情形，我国合规地向境外传输个人信息的条件总共有以下八项：

1) **通过数据出境安全评估：**通过国家网信部门组织的数据出境安全评估；

2) **取得个保认证：**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；

3) **签订标准合同：**符合国家网信部门制定的关于个人信息出境标准合同的规定；

4) **履行合同所必需：**为订立、履行个人作为一方当事人的合同，确需向境外提供个人信息；

5) **人力资源管理所必需：**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跨境人力资源管理，确需向境外提供员工个人信息；

6) **履行法定义务所必需：**为履行法定职责或者法定义务，确需向境外提供个人信息；

7) **紧急情况：**紧急情况下为保护自然人的生命健康和财产安全，确需向境外提供个人信息；

8) 法律、行政法规或者国家网信部门规定的**其他条件**。

9) **国际条约规定：**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。

2. 向境外提供重要数据的合规机制

《条例》第三十七条基于《数据出境安全评估办法》的规定，要求网络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**确需**向境外提供的，应当通过国家网信部门组织的数据出境安全评估。

首先还是要明确重要数据的认定标准，具体可详见本文第四章的分析。《条例》第三十七条重申了二点：其一，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需要具有十足的必要性，故相关企业需要自行评估论证，并提供相关证明材料以支撑“确需”提供之说；其次，根据《促进和规范数据跨境流动规定》的要求，重要数据的认定以地方和行业主管部门的通知或公开发布为标准。若相关企业未被相关部门、地区通知处理了重要数据，或者相关部门、地区公开发布的重要数据目录清单中暂未包括本企业所处理的数据的，则企业无需将某类数据作为重要数据申报数据出境安全评估。

此外，企业还应当关注，我国各地区正在积极探索建立数据分级分类保护制度，制定数据跨境流动的正面/负面清单，明确“重要数据”的类型。例如，天津自由贸易试验区于今年 2 月 5 日率先发布了《中国（天津）自由贸易试验区企业数据分类分级标准规范》[14]将数据分为 13 大类 40 子类，核心、重要、一般三个级别；上海临港新片区于今年 2 月 8 日发布《中国（上海）自由贸易试验区临港新片区数据跨境流动分类分级管理

[14] 参见天津市商务局官网：
https://shangwuju.tj.gov.cn/tjsswjzz/zwgk/zcfg_48995/swjwj/202402/t20240207_6534807.html

办法（试行）》[15]，提出对跨境数据进行分类分级管理，并提出重要数据目录制定、应用与更新机制的管理要求；北京市网信办等三部门也于 8 月 26 日印发《中国（北京）自由贸易试验区数据出境负面清单管理办法（试行）》《中国（北京）自由贸易试验区数据出境管理清单（负面清单）（2024 版）》[16]，首批选择汽车、医药、零售、民航、人工智能等 5 个领域率先制定，详细列明了各领域需要通过数据出境安全评估的重要数据清单，涉及 18 个数据子类及其基本特征与描述。

3. 向境外提供数据时的其他合规义务

《数据出境安全评估办法》第八条[17]要求数据出境安全评估时应当对数据出境的目的、范围、方式的合法性、正当性与必要性进行评估；第九条[18]要求数据处理者应当在与境外接收方订立的法律文件中明确约定数据安全保护责任，包括数据出境的目的、方式和数据范围，境外接收方处理数据的用途、方式等。《条例》第三十八条明确提出，网络数据处理者通过数据出境安全评估后向境外提供个人信息和重要数据的，不得超出评估时明确的数据出境目的、方式、范围和种类、规模等。因此，企业在通过数据出境安全评估后，应当严格按照评估材料以及与境外接收方合同约定的内容开展数据跨境传输活动。如果实际的跨境传输活动超过评估时申报的内容，则企业可能被国家网信部门认定为“数据出境活动在实际处理过程中不再符合数据出境的安全管理要求”，因此国家网信部门可能会依据《数据出境安全评估办法》，要求企业终止数据出境活动；如企业需要继续开展的，则应当按照要求整改后重新申请评估[19]。

---

[15] 参见：https://www.lingang.gov.cn/upload/1/dm/1708483614845.pdf

[16] 参见：https://www.beijing.gov.cn/zhengce/zhengcefagui/202409/W020240902597001758234.pdf

[17] 《数据出境安全评估办法》第八条 数据出境安全评估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，主要包括以下事项：
（一）数据出境的目的、范围、方式等的合法性、正当性、必要性；
（二）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；境外接收方的数据保护水平是否达到中华人民共和国法律、行政法规的规定和强制性国家标准的要求；
（三）出境数据的规模、范围、种类、敏感程度，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；
（四）数据安全和个人信息权益是否能够得到充分有效保障；
（五）数据处理者与境外接收方拟订立的法律文件中是否充分约定了数据安全保护责任义务；
（六）遵守中国法律、行政法规、部门规章情况；
（七）国家网信部门认为需要评估的其他事项。

[18] 《数据出境安全评估办法》第九条 数据处理者应当在与境外接收方订立的法律文件中明确约定数据安全保护责任义务，至少包括以下内容：
（一）数据出境的目的、方式和数据范围，境外接收方处理数据的用途、方式等；
（二）数据在境外保存地点、期限，以及达到保存期限、完成约定目的或者法律文件终止后出境数据的处理措施；
（三）对于境外接收方将出境数据再转移给其他组织、个人的约束性要求；
（四）境外接收方在实际控制权或者经营范围发生实质性变化，或者所在国家、地区数据安全保护政策法规和网络安全环境发生变化以及发生其他不可抗力情形导致难以保障数据安全时，应当采取的安全措施；
（五）违反法律文件约定的数据安全保护义务的补救措施、违约责任和争议解决方式；
（六）出境数据遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等风险时，妥善开展应急处置的要求和保障个人维护其个人信息权益的途径和方式。

[19] 《数据出境安全评估办法》第十七条 国家网信部门发现已经通过评估的数据出境活动在实际处理过程中不再符合数据出境安全管理要求的，应当书面通知数据处理者终止数据出境活动。数据处理者需要继续开展数据出境活动的，应当按照要求整改，整改完成后重新申报评估。

如果是个人信息出境的，除了需要确定适用哪项前述提到的出境合规机制，以及评估是否适用自贸区新政以外，还需要向相关个人进行告知，并取得个人的单独同意。与向第三方提供网络数据需要获取单独同意一样，此处的单独同意，仍然采取《条例》第六十二条给出的定义，即指个人针对其个人信息出境的特定处理活动而专门作出具体、明确的同意。同时，出境方还需要开展个人信息保护影响评估、建立个人信息主体权利响应渠道、采取必要的技术保障措施以使出境活动的安全水平达到国家法律法规的保护标准，并对跨境活动进行记录并保存。

此外，《条例》第三十九条一再强调了数据跨境传输过程中，网络数据处理者对安全风险的防范责任。从具体实施的角度，既包括国家将采取措施，防范、处置网络数据跨境安全风险和威胁，也包括任何个人、组织不得提供专门用于破坏、避开技术措施的程序、工具等，以此遏制黑客等组织在社会上扩散犯罪工具；也不得在明知他人从事破坏、避开技术措施等活动，仍为其提供技术支持或者帮助。本条明确，即使个人或组织本身没有直接参与破坏、规避技术措施，只要存在上述行为，同样需要承担法律责任，以此有效减少“共犯”行为，进一步遏制犯罪发生。

（七）法律责任

《条例》第八章规定了违反《条例》的法律责任，与《征求意见稿》相比，《条例》有较大的修改。一方面针对特定违法行为明确了罚则，另一方面也更加突出上位法和《条例》的衔接关系，特别是在认定不同违法行为的处罚力度时，《条例》体现出与现行法律框架保持一致的特点，这有利于当出现跨领域的复杂案件、可能涉及到适用多部法律法规的情形，执法部门能够妥善处理不同法律和不同效力等级法规之间的关系。同时，《条例》在归责处理上又有以下新的亮点：

首先，《条例》针对特定违法行为，规定了违反数据安全义务（第五十五条）、未按照有关规定进行安全审查的（第五十六条）、违反重要数据相关义务（第五十七条）等情况下的罚则；而针对违反《条例》规定的其他义务的情况，具体行政处罚由上位法补足，即由监管部门直接按照《网安法》《数安法》《个保法》等法律追究责任。

其次，在罚则上引入了分级处罚机制，罚款额度总体上较《征求意见稿》有了更明确的规定，依据违法行为的情节轻重、整改情况等设置了不同层次的罚款和制裁，特别是在处罚下限和上限上做了更细化的划分。例如，《条例》规定了初次违法并及时改正或轻微违法的行为可以从轻处罚（第五十九条），而对于拒不改正或情节严重的行为，则可能面临更严厉的罚款、停业整顿、吊销执照等处罚（第五十五条、第五十六条、第五十七条）。这种分级处置机制不仅增强了执法的灵活性，还体现了“宽严相济”的立法思路。但是，《条例》对于一些特定行为的处罚力度有所提升，例如，第五十六条规定情节严重者可处 100 万元以上、1000 万元以下罚款，反映了国家对网络数据安全的日益重视。但需要注意的是，《条例》的罚款力度仍需与企业规模、违法行为的具体后果等因素相匹配，以免出现过度处罚的风险。

再次，相较于《网安法》和《数安法》，《条例》进一步明确了对“直接负责的主管人员”和“其他直接责任人员”的法律责任，不仅规定了罚款额度，还特别强调了在情节严重的情况下，这些责任人员可能面临不同程度的个人罚款（第五十五条至第五十七条）。这反映出《条例》对管理层和一线直接责任人员的归责更加具体、明确，从内部流程和管理上要求强化管理者的个人责任意识。继承《网安法》《数安法》《个保法》的传统，《条例》第六十一条也同样明确了违法行为不仅需承担行政责任，还可能涉及民事甚至刑事责任。这表明《条例》的法律责任与上位法多层次、多维度的责任规定保持一致，企业不仅需要应对监管部门的行政处罚，还可能面临受害者的民事违约或者侵权的索赔或国家控诉机关的刑事追责。因此，企业在遵守《条例》时，需要特别关注潜在的多重责任风险，并进行全面的法律合规风险评估。

此外，《条例》中多次提到“网信、电信、公安、国家安全”等多个部门联合执法（第五十五条、第五十六条），反映了监管的协调性。这种联动机制不仅呼应了第七章中要求监管机构执法上采取协调配合的机制，也确保了不同类型的数据安全问题能够在专业化的背景下得到处理，特别是对于重要数据跨境传输、关键信息基础设施保护等敏感领域，以保证执法的全面性和权威性。通过明确的监管职责划分、严格且协作的监督检查机制以及严厉的法律责任追究制度，为网络数据的安全与秩序提供了有力保障。

最后，《条例》第六十条强调了国家机关不履行数据安全保护义务时的法律责任，这是与《数安法》和《个保法》的一个重要区别。通过对国家机关责任的明确规定，《条例》避免了公权力机关在网络数据安全管理职责中的责任缺位或互相推诿，强化了对公共机构的监督与问责。

（八）结论与展望

《条例》的出台，标志着我国网络数据安全立法体系的进一步完善，成为了数字经济时代下的护航力量。立足当前数字经济发展的需求，《条例》作为应对日益复杂的网络安全挑战的重要法律支撑，不仅回应了社会对网络数据安全的呼声，还为网络数据安全管理提供了更加具体、全面的操作指南。通过动态风险评估、分级责任追究、严明执法机制，《条例》展现了“宽严相济”的立法理念，既强调了对违法行为的惩治力度，也首次为轻微违规提供了纠错的空间。这种兼具严密与灵活的规则设计，为数字经济的可持续、高质量发展奠定了坚实的法律基石。

未来，随着前沿科技的不断发展和应用场景的持续拓展，数据的流动性、复杂性将持续增加，网络数据安全将面临更多新的挑战和机遇。《条例》作为护航数字经济的重要法律保障，将在应对更加复杂的网络安全风险中发挥更加不可或缺的作用。无论是对于国家安全，还是企业的持续发展，数据安全都将成为长期决胜的关键因素。而在这场没有硝烟的数字战役中，法规的完善与执行，正是确保数字经济健康发展的重要防线。

因此，洞悉《网络数据安全管理条例》背后的立法精神，不仅仅是认识到其对于违法行为的惩戒意义，更是要理解它在当前阶段促进数字生态系统健康运转中的长远作用。

未来，企业唯有将网络数据安全视作核心竞争力的一部分，真正融入到日常运营与战略规划中，才能在这个不断演化的数字战役中立于不败之地。而《条例》的实施，正是国家为全新的数字时代保驾护航提供的重要举措和关键力量，其将进一步推动网络数据安全与数字经济的共生繁荣。

2. 数据分类分级：解读《数据安全技术 数据分类分级规则》：纲举目张，安则有序[20]

引言

2024 年 3 月 21 日，全国网络安全标准化技术委员会（原全国信息安全标准化技术委员会）发布《数据安全技术 数据分类分级规则》报批稿（正式标准编号为 GB/T 43697-2024）（以下简称“《规则》”）。此次发布的《规则》是全国网络安全标准化技术委员会更名后，正式发布的第一部以“数据安全技术”命名的国家标准。《规则》有效衔接了《中华人民共和国数据安全法》（以下简称“《数据安全法》”）的原则性规定，提供了数据分类分级的统一通用规则，同时延续和更新了此前发布的《信息安全技术 重要数据识别指南》（征求意见稿）（以下简称“《重要数据识别指南》”）关于重要数据的相关规定，正式确定重要数据的识别标准，即将结束长期以来重要数据识别“无法可依”的局面。《规则》的发布既回应了社会各行各业的期待，也是实现国务院办公厅《扎实推进高水平对外开放更大力度吸引和利用外资行动方案》（国办发〔2024〕9 号）提出的“健全数据跨境流动规则，科学界定重要数据的范围”目标的重要举措。该国家标准将于 2024 年 10 月 1 日正式实施。

一、我国数据分类分级和重要数据立法现状

（一）《数据安全法》的原则性规定

国家“十四五”规划明确提出要建立健全数据要素市场规则和完善适用于大数据环境下的数据分类分级保护制度。2021 年 9 月 1 日实施的《数据安全法》第二十一条明确规定国家建立数据分类分级保护制度，对数据实行分类分级保护。《数据安全法》在法律层面确立了数据划分为“国家核心数据”、“重要数据”以及“一般数据”并实行不同程度的管理、保护制度这一基本原则。同年 11 月 1 日实施的《中华人民共和国个人信息保护法》也在其第五条中指出个人信息处理者应对个人信息实行分类管理。《数据安全法》等法律虽规定了数据分类分级保护的原则，但并未就数据分类和分级方法提供具体的落地指导，也未明确定义何为“国家核心数据”“重要数据”；配套的行政法规、部门规章和国家标准等也迟迟未能正式出台，数据处理者在实际工作开展过程中缺乏相对有效的明确指导。

（二）各行业分类分级标准

随着《数据安全法》等上位法的颁布和推进，各个行业领域的数据分类分级相关标准规范的制定也快马加鞭进入快车道。以金融领域为例，三项数据分类分级相关的标准《金融数据安全 数据安全分级指南》(JR/T0197-2020)《证券期货业数据分类分级指引》(JR/T 0158-2018)《个人金融信息保护技术规范》(JR/T0171-2020)，分别从金融业数据、

[20] 作者：孟洁、钱星辰、黎耀琦

证券期货业数据和个人金融信息的维度对金融数据分类分级做出了规定。电信、工业、医疗健康、智能网联车、政务等行业和领域也纷纷制定了相应的数据分类分级相关标准或政策，以规范行业发展、指引数据合规实践的落地。

在地方层面，各地也根据数据分类分级实践情况积极探索相应的规范治理规则和模式。2016 年，贵州省质量技术监督局发布《政府数据 数据分类分级指南》（DB52/T1123-2016），从主题、行业和服务三个维度对政府数据进行分类，作为贵州省政府数据分类和分级的顶层标准。除贵州省外，浙江省、上海市、山东省青岛市等也曾发布《数字化改革 公共数据分类分级指南》（DB33/T 2351-2021）《上海市公共数据开放分级分类指南(试行)》《青岛市公共数据分类分级指南》等标准或文件，指导当地的政府与公共数据分类分级。

由于国家统一的数据分类分级标准和相应实施细则长期缺位，各行业、各地方的数据分类分级标准往往呈现较为明显的区别：不同行业的业务类型、业务范围、数据处理活动特征差别明显，导致不同行业间的分类分级标准存在一定差异；各地方的数据分类分级侧重点和产业发展着力点有所区别，致使数据分类分级的地方性文件也呈现出一定的地方特色。由于各行业、各地区数据分类分级标准之间存在衔接适用的问题，数据处理者在实际开展分类分级工作过程中会面临诸多困惑，数据分类分级保护机制的整体落地具备一定的挑战。

本次《规则》的发布，一方面落实了《数据安全法》等上位法所规定的原则，在理论上与现行法律法规相衔接，完善了数据分类分级制度体系；另一方面，有助于解决因缺乏国家统一的数据分类分级指导性规则而导致相关国家数据安全制度、数据分类分级保护要求难以整体落地的问题，具有重要的意义。

二、数据分级分类的框架与规则

就具体内容而言，《规则》包含“数据分类分级规范标准”和“重要数据识别标准”两大重要组成部分。《规则》提供了数据分类分级的原则、框架、方法、规则和流程，并在其前身《信息安全技术 网络数据分类分级要求》（征求意见稿）（以下简称“《网络数据分类分级要求》”）的基础上提供了重要数据识别指南，指引数据处理者在行业领域主管部门的引导下进一步准确识别和划分核心数据、重要数据和一般数据，妥善落实数据分级分类保护工作。

（一）分类分级基本原则

根据《规则》第 4 条，数据处理者应遵循如下五项基本原则对数据进行分类分级：

1. 科学实用原则：从便于数据管理和使用的角度，科学选择常见、稳定的属性或特征作为数据分类的依据，并结合实际需要对数据进行细化分类。

2. 边界清晰原则：数据分级的各级别应边界清晰，对不同级别的数据采取相应的保护措施。

3. 就高从严原则：采用就高不就低的原则确定数据级别，当多个因素可能影响数据分级时，按照可能造成的各个影响对象的最高影响程度确定数据级别。

4. 点面结合原则：数据分级既要考虑单项数据分级，也要充分考虑多个领域、群体或区域的数据汇聚融合后的安全影响，综合确定数据级别。

5. 动态更新原则：根据数据的业务属性、重要性和可能造成的危害程度的变化，对数据分类分级、重要数据目录等进行定期审核更新。

《规则》发布前的各类政策文件和国家标准，仅有部分文件对数据分类分级原则做出了相应的规定，多数文件规定了合法合规、可执行性、就高从严、时效性、差异性和客观性原则，少数标准和文件还提出了自主性、合理性、关联叠加效应原则。此次《规则》在完全吸收《网络数据分类分级要求》中发布的五项基本原则的基础上，对不同行业领域的数据分类分级原则进行了一定的统合和增减，为行业领域主管部门和数据处理者明确了工作方向。

（二）数据分类规则

根据《规则》第 5 条，数据分类的框架为先按照**行业领域**分类、再根据**业务属性**分类的思路进行，并提出个人信息等法律法规有专门管理要求的数据类别应按照有关规定和标准进行识别和分类，其中：

- 行业领域包括：工业、电信、金融、能源、交通运输、自然资源、卫生健 康、教育、科学等；
- 业务属性包括：业务领域、责任部门、描述对象、流程环节、数据主体、内容主题、数据用途、数据处理和数据来源等。

《规则》在提供分类框架和分类方法的基础上，在其附录 A 中就描述对象和数据主体两个业务属性的分类提供了如下示例：

数据类别	类别定义	示例
用户数据	在开展业务服务过程中从个人用户或组织用户收集的数据，以及在业务服务过程中产生的归属于用户的数据	如个人信息、组织用户信息(如组织基本信息、组织账号信息、组织信用信息等)
业务数据	在业务的研发、生产、运营过程中收集和产生的非用户类数据	参考业务所属的行业数据分类分级，结合自身业务特点进行细分，如产品数据、合同协议等

数据类别	类别定义	示例
经营管理数据	数据处理者在单位经营和内部管理过程中收集和产生的数据	如经营战略、财务数据、并购融资信息、人力资源数据、市场营销数据等
系统运维数据	网络和信息系统运行维护、日志记录及网络安全数据	如网络设备和信息系统的配置数据、日志数据、安全监测数据、安全漏洞数据、安全事件数据等

表 1 基于描述对象的数据分类参考示例

数据分类	类别定义	示例
公共数据	各级政务部门、具有公共管理和服务职能的组织及其技术支撑单位，在依法履行公共事务管理职责或提供公共服务过程中收集、产生的数据	如政务数据，在供水、供电、供气等公共服务运营过程中收集和产生的数据等
组织数据	组织在自身生产经营活动中收集、产生的不涉及个人信息和公共利益的数据	如不涉及个人信息和公共利益的业务数据、经营管理数据、系统运维数据等
个人信息	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	如个人身份信息、个人生物识别信息、个人财产信息、个人通信信息、个人位置信息、个人健康生理信息等

表 2 基于数据主体的数据分类参考示例

其中，表 1 完全吸收了《网络数据分类分级要求》所作的描述对象方面的示例，采用面分类法，从行业内组织经营维度，将用户数据和经营中的其他数据进行区分，再依据生产经营的各个环节对其他数据进行分类。

表 2 提供的分类参考示例则与中共中央、国务院发布的《关于构建数据基础制度更好发挥数据要素作用的意见》（以下简称“数据二十条”）规定相衔接，明确参照“数据二十条”将数据分为公共数据、企业/组织数据和个人信息数据的基本分类，同时结合了《信息安全技术 个人信息安全规范》（GB/T 35273-2020）（以下简称“《个人信息安全规范》”）对个人信息所作的定义和示例，并在《规则》附录 B 中就个人信息提供了更为细致的分类示例。

根据上述分类框架，《规则》提供了行业领域数据分类的具体步骤和方法，**数据分类工作主要涉及以下四个阶段：**

1. 明确数据范围：按照行业领域主管（监管）部门职责，明确本行业本领域管理的数据范围。**2. 细化业务分类：**对本行业本领域业务进行细化分类，包括：

a) 结合部门职责分工，明确行业领域或业务条线的分类；

b) 按照业务范围、运营模式、业务流程等，细化行业领域或明确各业务条线的关键业务分类。

3. 业务属性分类：选择合适的业务属性，对关键业务的数据进行细化分类。**4. 确定分类规则**：梳理分析各关键业务的数据分类结果，根据行业领域数据管理和使用需求，确定行业领域数据分类规则，例如：a) 可采取“业务条线—关键业务—业务属性分类”的方式给出数据分类规则；

b) 对关键业务的数据分类结果进行归类分析，将具有相似主题的数据子类进行归类。

由于不同行业领域的自身特性，主管部门应结合本行业领域具体的数据管理和使用需求，以及已经具备的数据分类基础，灵活指导本行业的数据分类工作，使得数据处理者能够将所掌握的数据科学分类至合适的数据大类与子类中。

（三）数据分级规则

根据《规则》第 6 条，数据分级的基本框架为根据数据在经济社会发展中的重要程度，以及一旦遭到泄露、篡改、损毁或者非法获取、非法使用、非法共享，对国家运行、经济运行、社会秩序、公共利益、组织权益、个人权益等不同影响对象所造成影响的危害程度，将数据从高到低分为核心数据、重要数据、一般数据三个级别。

根据《规则》，**数据分级工作主要包括如下四个步骤**：

1. 确定分级对象：确定数据项、数据集、衍生数据、跨行业领域数据等待分级数据。

2. 分级要素识别：识别数据的领域、群体、区域、精度、规模、深度、覆盖度、重要性等识别要素（具体请参见《规则》附录 C）。

3. 影响分析：分析数据一旦遭到风险可能影响的对象和影响程度（具体请参见《规则》附录 D、附录 E 及附录 F）。

4. 综合确定级别：结合上述分析综合确定数据级别。《规则》在其第 6.5 条中，指出了结合上述分级要素形成的如下规则表：

影响对象	影响程度		
	特别严重危害	严重危害	一般危害
国家安全	核心数据	核心数据	重要数据
经济运行	核心数据	重要数据	一般数据
社会秩序	核心数据	重要数据	一般数据

影响对象	影响程度		
	特别严重危害	严重危害	一般危害
公共利益	核心数据	重要数据	一般数据
组织权益 个人权益	一般数据	一般数据	一般数据
注：如果影响大规模的个人或组织权益，影响对象可能不只包括个人权益或组织权益，也可能对国家安全、经济运行、社会秩序或公共利益造成影响。			

表 3 数据级别确定规则表

根据上表，影响对象的确定对于数据级别的明确有非常显著的作用。对于关系到国家安全的数据，不论其造成的影响程度如何，一律属于重要数据或核心数据，需要采取更为全面的保护措施、受到更为严格的监管。如果数据仅影响到组织或个人，则其重要性显著下降。对于关系到经济、社会秩序和公共利益的数据，其重要性则依据其影响程度而定。在此基础上，可总结出核心数据、重要数据、一般数据的的级别确定情况：

级别	核心数据	重要数据	一般数据
识别标准	1) 数据一旦遭到泄露、篡改、损毁或者非法获取、非法使用、非法共享，直接对国家安全造成特别严重危害（如直接影响政治安全）或严重危害（如关系其他国家安全重点领域）；2) 数据一旦遭到泄露、篡改、损毁或者非法获取、非法使用、非法共享，直接对经济运行造成特别严重危害（如关系国民经济命脉）；3) 数据一旦遭到泄露、篡改、损毁或者非法获取、非法使用、非法共享，直接对社会秩序 造成特别严重危害（如关系重要民生）；4) 数据一旦遭到泄露、篡改、损毁或者非法获取、非法使用、非法共享，直接对公共利益 造成特别严重危害（如关系重大公共利益）；5) 对领域、群体、区域具有较高覆盖度，直接影响政治安全的重要数据；6) 达到较高精度、较大规模、较高重要性或深度，直接影响政治安全的重要数据；	1) 数据一旦遭到泄露、篡改、损毁或者非法获取、非法使用、非法共享，直接对国家安全造成一般危害；2) 数据一旦遭到泄露、篡改、损毁或者非法获取、非法使用、非法共享，直接对经济运行造成严重危害；3) 数据一旦遭到泄露、篡改、损毁或者非法获取、非法使用、非法共享，直接对社会秩序造成严重危害（如影响社会稳定）；4) 数据一旦遭到泄露、篡改、损毁或者非法获取、非法使用、非法共享，直接对公共利益造成严重危害（如危害公共健康和安全）；5) 数据直接关系国家安全、经济运行、社会稳定、公共健康和安全的特定领域、特定群体或特定区域；6) 数据达到一定精度、规模、深度或重要性，直接影响国家安全、经济运行、社	未识别为核心数据、重要数据的其他数据

级别	核心数据	重要数据	一般数据
	7) 经有关部门评估确定的核心数据。	会稳定、公共健康和安全； 7) 经行业领域主管（监管）部门评估确定的重要数据。	

表 4 核心数据、重要数据与一般数据的级别确定

从上表中不难看出，《规则》中“核心数据”的定义既延续了上位法《数据安全法》第二十一条中“关系国家安全、国民经济命脉、重要民生、重大公共利益”对国家核心数据的识别标准，又充分吸收了《网络数据分类分级要求》和各地方发布的数据分类分级标准规范中[1]“较高覆盖度、较高精度、较大规模、一定深度”等识别要素，定义更为明确和完善。

“重要数据”的定义同样延续了《数据安全法》第二十一条中“一旦遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者个人、组织合法权益造成的危害程度”的原则性规定；新增的“特定领域、特定群体、特定区域或达到一定精度和规模”识别要素一方面与核心数据的定义相衔接，另一方面也吸收和借鉴了《重要数据识别指南》《工业和信息化领域数据安全管理办法（试行）》等文件对于特定敏感行业领域和群体的列示性规定，将相关要求进行浓缩和归纳。

在一般数据的分级方面，此前各个行业领域的政策文件和国家标准对数据分级的规定不一，汇总如下表：

标准	分级标准	分级级别数量
《金融数据安全 数据安全分级指南》（JR/T 0197-2020）	数据安全遭破坏后的影响对象和影响程度	5 级
《基础电信企业数据分类分级方法》（YD/T 3813-2020）	数据对象的重要敏感程度	4 级
《车联网信息服务 数据安全技术要求》（YD/T 3751-2020）	车联网信息服务数据敏感性	2 级
《信息安全技术 健康医疗数据安全指南》（GB/T 39725-2020）	数据重要程度、风险级别可能造成的损害和影响	5 级
《证券期货业数据分类分级指引》（JR/T 0158—2018）	影响对象、影响程度、影响范围	4 级

表 5 各行业领域标准数据分级的级别数量对比

本次《规则》则在其附录 H 中为“一般数据”的分级提供了 4 级、3 级、2 级的灵活分级框架参考，并提供了敏感个人信息、禁止开放/共享的公共数据、组织内部员工个人信息等特定类型一般数据在不同级别框架下的最低参考级别。

《规则》同时按照数据加工程度不同，将数据分为原始数据、脱敏数据、标签数据、统计数据、融合数据，其中脱敏数据、标签数据、统计数据、融合数据均属于衍生数据。根据《规则》中的分级参考，衍生数据的级别需要数据处理者根据实际处理情况确定。脱敏数据因去标识化等处理，数据的敏感性和重要性降低，其数据级别一般较原始数据降低；标签数据、统计数据、融合数据则需要综合数据处理后的相应结果，再次根据分级要素、影响对象和影响程度进行影响分析，进行数据定级，其级别可比原始数据级别降低或升高。

《规则》所建立的"核心数据+重要数据+一般数据（2 级至 4 级）"的分级规则体系，以及关于不同类型衍生数据的分级说明与指引，有助于各行业领域主管部门和数据处理者根据行业领域的特性、具体业务流程和数据的差异性，灵活确定具体的分级规则，并据此制定相应的数据保护措施。

（四）重要数据识别准则

《规则》的另一大亮点是以附录的形式正式发布了规范性质的重要数据识别指南。本次国家标准发布之前，各行业领域主管部门和数据处理者主要参考《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）《重要数据识别指南》等文件自主识别重要数据，但这类文件或仅作原则性规定，或未正式生效，导致有效的重要数据识别准则始终缺位。

国家互联网信息办公室于 2024 年 3 月 22 日正式发布并自公布之日起实施的《促进和规范数据跨境流动规定》，在其第二条中规定了"数据处理者应当按照相关规定识别、申报重要数据。未被相关部门、地区告知或者公开发布为重要数据的，数据处理者不需要作为重要数据申报数据出境安全评估"，即明确了行业主管及监管相关部门、各地区应发布重要数据的识别规则，并按要求指导数据处理者开展重要数据的识别和申报工作。（相关解读可参考团队文章《流动与安全并重：《促进和规范数据跨境流动规定》来了，企业应当如何应对？》；《从源头到结果，从内部到外部：重要数据处理安全要求全景解析》）

在重要数据的识别因素方面，此前发布的《重要数据识别指南》列举了 14 项因素，本次《规则》在附录 G 中将重要数据识别指南所列识别因素则增加至 18 项，具体对比如下：

《重要数据识别指南》（征求意见稿）	《规则》
a)反映国家战略储备、应急动员能力，如战略物资产能、储备量属于重要数据； b)支撑关键基础设施运行或重点领域工业生产，如直接支撑关键基础设施所在行业、	a)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，如未公开的领陆、领水、领空数据；b)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、

《重要数据识别指南》（征求意见稿）	《规则》
领域核心业务运行或重点领域工业生产的数据属于重要数据； c)反映关键信息基础设施网络安全保护情况，可被利用实施对关键信息基础设施的网络攻击，如反映关键信息基础设施网络安全方案、系统配置信息、核心软硬件设计信息、系统拓扑、应急预案等情况的数据属于重要数据； d)关系出口管制物项，如描述出口管制物项的设计原理、工艺流程、制作方法等的信息以及源代码、集成电路布图、技术方案、重要参数、实验数据、检测报告属于重要数据； e)可能被其他国家或组织利用发起对我国的军事打击，如满足一定精度要求的地理信息属于重要数据； f)反映重点目标、重要场所物理安全保护情况或未公开地理目标的位置，可能被恐怖分子、犯罪分子利用实施破坏，如反映重点安保单位、重要生产企业、国家重要资产(如铁路、输油管道)的施工图、内部结构、安防等情况的数据，以及未公开的专用公路、未公开的机场等的信息属于重要数据； g)可能被利用实施对关键设备、系统组件供应链的破坏，以发起高级持续性威胁等网络攻击，如重要客户清单、未公开的关键信息基础运营者采购产品和服务情况、未公开的重大漏洞属于重要数据； 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； i)国家自然资源、环境基础数据，如未公开的水情信息、水文观测数据、气象观测数据、环保监测数据属于重要数据； j)关系科技实力、影响国际竞争力，如描述与国防、国家安全相关的知识产权的数据属于重要数据； k)关系敏感物项生产交易以及重要装备配备、使用，可能被外国政府对我实施制裁，如重点企业金融交易数据、重要装备生产制造信息，以及国家重大工程施工过程中的重	作战等能力，如满足一定精度指标的地理数据或与战略物资产能、储备量有关的数据；**c)直接影响市场经济秩序，**如支撑关键信息基础设施所在行业、领域核心业务运行或重要经济领域生产的数据；**d)反映我国语言文字、历史、风俗习惯、民族价值观念等特质，如记录历史文化遗产的数据；**e)反映重点目标、重要场所物理安全保护情况或未公开地理目标的位置，可被恐怖分子、犯罪分子利用实施破坏，如描述重点安保单位、重要生产企业、国家重要资产(如铁路、输油管道)的施工图、内部结构、安防情况的数据；f)关系我国科技实力、影响我国国际竞争力，或关系出口管制物项，如反映国家科技创新重大成果，或描述我国禁止出口限制出口物项的设计原理、工艺流程、制作方法的数据，以及涉及源代码、集成电路布图、技术方案、重要参数、实验数据、检测报告的数据；g)反映关键信息基础设施总体运行、发展和安全保护情况及其核心软硬件资产信息和供应链管理情况，可被利用实施对关键信息基础设施的网络攻击，如涉及关键信息基础设施系统配置信息、系统拓扑、应急预案、测评、运行维护、审计日志的数据；**h)涉及未公开的攻击方法、攻击工具制作方法或攻击辅助信息，可被用来对重点目标发起供应链攻击、社会工程学攻击等网络攻击，如政府、军工单位等敏感客户清单，以及涉及未公开的产品和服务采购情况、未公开重大漏洞情况的数据；i)反映自然环境、生产生活环境基础情况，或可被利用造成环境安全事件，如未公开的与土壤、气象观测、环保监测有关的数据；j)反映水资源、能源资源、土地资源、矿产资源等资源储备和开发、供给情况，如未公开的描述水文观测结果、耕地面积或质量变化情况的数据；**k)反映核材料、核设施、

《重要数据识别指南》（征求意见稿）	《规则》
要装备配备、使用等生产活动信息属于重要数据； l)在向政府机关、军工企业及其他敏感重要机构提供服务过程中产生的不宜公开的信息，如军工企业较长一段时间内的用车信息； m)未公开的政务数据、工作秘密、情报数据和执法司法数据，如未公开的统计数据； n)其他可能影响国家政治、国土、军事、经济、文化、社会、科技、生态、资源、核设施、海外利益、生物、太空、极地、深海等安全的数据。 具备以上因素之一的，是重要数据。	**核活动情况，或可被利用造成核破坏或其他核安全事件，如涉及核电站设计图、核电站运行情况的数据；l)关系海外能源资源安全、海上战略通道安全、海外公民和法人安全，或可被利用实施对我国参与国际经贸、文化交流活动的破坏或对我国实施歧视性禁止、限制或其他类似措施，如描述国际贸易中特殊物项生产交易以及特殊装备配备、使用和维修情况的数据；m)关系我国在太空、深海、极地等战略新疆域的现实或潜在利益，如未公开的涉及对太空、深海、极地进行科学考察、开发利用的数据，以及影响人员在上述领域安全进出的数据；**n)反映生物技术研究、开发和应用情况，反映族群特征、遗传信息，关系重大突发传染病、动植物疫情，关系生物实验室安全，或可能被利用制造生物武器、实施生物恐怖袭击，关系外来物种入侵和生物多样性，如重要生物资源数据、微生物耐药基础研究数据；o)反映全局性或重点领域经济运行、金融活动状况，关系产业竞争力，可造成公共安全事故或影响公民生命安全，可引发群体性活动或影响群体情感与认知，如未公开的统计数据、重点企业商业秘密；p)反映国家或地区群体健康生理状况，关系疾病传播与防治，关系食品药品安全，如涉及健康医疗资源、批量人口诊疗与健康管理、疾控防疫、健康救援保障、特定药品实验、食品安全溯源的数据；q)其他可能影响国土、军事、经济、文化、社会、科技、**电磁空间、网络**、生态、资源、核、海外利益、太空、极地、深海、生物、**人工智能**等安全的数据；r)其他可能对经济运行、社会秩序或公共利益造成严重危害的数据。具备以上因素之一的数据，可被识别为重要数据。

表 6 重要数据识别指南内容对比

由此可见，在具体内容方面，《规则》在整合《重要数据识别指南》规定的基础上，新增或重点补充了多处重要数据识别因素。补足完善的内容一方面是对我国近年来数据保护实践的归纳总结，另一方面也是为防范诸如涉疆法案等利用数据破坏我国国际合作、影响我国在战略新领域开拓等事件所采取的举措，与我国《数据安全法》《数据出境安全评估办法》和《促进和规范数据跨境流动规定》等法律法规对重要数据跨境流动所作出的规定要求相衔接。

三、《规则》发布的意义与数据分类分级工作开展建议

（一）提供完整规则框架，引导数据处理者建立并完善数据分类分级管理体系

数据分类分级是组织内部数据安全合规处理的基础保障，也是数据安全治理和科学管理的主要措施。结合此次发布的《规则》，数据处理者可以参照如下流程与方式开展内部数据分类分级工作。

数据资产梳理

数据处理者可以首先以盘点的方式划定待开展分类分级工作的数据资源范围，通过技术工具，对结构化和非结构化数据资产进行全量的扫描识别，明确各类数据所涉及的行业领域、所对应的数据处理场景、所涉及的系统、所存储的数据库，以及数据处理的具体方式及结果，并划定原始数据与各类衍生数据的边界，为分类分级工作的实施做好充分准备。

制订内部规则

对于涉及单一行业领域的数据处理者，应根据行业领域主管部门已制定的行业数据分类分级规则指南，结合数据资产梳理情况，确立内部识别核心数据和重要数据的流程，并根据自身的数据掌握情况和管理体系形成适用于本组织的一般数据的分类分级规则。对于尚未形成针对性数据分类分级标准的行业，数据处理者可在《规则》的基础上探索形成自身的分类分级框架体系，并主动与行业领域主管部门开展必要的沟通。对于业务涉及多个行业领域的数据处理者，则可以在参考《规则》的基础上，分别按照各个行业领域的行业规范设定分类分级规则。在此情况下，所处理的同一类型的数据在不同行业领域内可能被确定为不同的数据级别，这需要数据处理者完成内部的协调，实现科学管理。在实践中，数据处理者可参考《规则》的附录 H 和各行业领域制订的数据分类行业标准或指南文件，选择合适的定级框架体系对各行业领域的一般数据进行管理，并将核心数据和重要数据定义为更高级别，形成最高可至 6 级的数据定级体系。此外，对于已经建立内部商业数据保密体系的部分数据处理者，可通过构建数据映射表的方式，将原有的数据保密体系和建设中的数据分类分级规则进行关联映射，方便内部人员理解且合理开展分类分级工作，并进一步对工作成果加以开发利用。

实施数据分类

数据处理者应根据《规则》提供的分类维度，结合自身业务情况，对数据进行大类和子类的划分，并对不同子类进行定义说明，将所含具体数据字段的情况进行列举。在此工作方式下，数据处理者处理的全量原始数据和衍生数据均可以被划入具体的子类中。

实施数据分级

开展数据分级工作时，数据处理者可以根据加工对分级要素、影响对象、影响程度的影响，首先对原始数据进行数据分级，再基于对原始数据的处理活动对通过不同加工方式形成的衍生数据进行定级。在分类分级结果形成后，数据处理者可根据《规则》并参考《金融数据安全 数据安全分级指南》附录 A 等文本的格式，形成组织内部的**数据分类分级清单**（以下为示例，仅供参考）以管理数据分类分级结果：

数据分类分级情况及说明								
一级子类	**二级子类**	**定义说明**	**三级子类**	**定义说明**	**四级子类**	**所含字段**	**数据安全级别**	**备注**
业务数据	合约协议	指合同或协议所包含的所有属性数据	合同通用信息	指合同以及商业银行法所规定的、各种特定业务通用的基本属性	合同信息	合同编号、合同名称、合同种类、合同状态、合同金额、币种等	2 级	一般数据
			存款业务信息	指存款业务所涵盖的相关属性数据	基本信息	贷款类型、贷款用途、保证金金额等	2 级	一般数据
					计息信息	存款业务种类、期限	2 级	一般数据

数据分类分级情况及说明								
						类型等		
		…	…	…	…	…	…	…
	账户信息	账户相关数据	/	/	介质信息	介质号码、卡种类等	3 级	一般数据
		…	…	…	…	…	…	…
	…	…	…	…	…	…	…	…
用户数据	…	…	…	…	…	…	…	…
经营管理数据	…	…	…	…	…	…	…	…
系统运维数据	…	…	…	…	…	…	…	…

表 7 数据分类分级清单示例

在实际数据分级管理工作中，基于数据项（数据库表某一列字段等）将组织内全部的数据以数据字段维度进行管理的难度较大，操作性较低。目前各类组织较为常见的方式是以数据集（由多个数据记录组成的集合，如数据库表、数据文件等）而非数据项为单位进行数据分级的实操管理，从而在保障安全的前提下提升管理工作的便捷性。

在数据集的分级方面，数据处理者可采用《规则》中的原则性建议，依据“就高不就低”的从严定级原则，参考所含数据项的级别对数据集进行定级，并按照数据集的级别确定安全管控措施。

例如，在总体为 5 级（核心数据设定为 5 级，重要数据设定为 4 级，一般数据分为 1 级、2 级、3 级进行管理）的数据分级框架下，某一数据集中同时含有级别为 1 级、2 级、3 级的一般数据，且该数据集中不含核心数据和重要数据，则此数据集的级别可首先预设为 3 级。但同时，需要判断上述不同级别的数据在该数据集中形成的规模以及可能基于所含有数据形成的衍生数据的影响，从而视情况将数据集的级别调整为 4 级或 5 级进行安全管理。

审核上报目录

数据处理者应根据行业主管监管部门和各地区的要求，落实核心数据和重要数据的记录和报送工作。

此外，数据处理者应根据分类分级结果，在组织内部的数据管理系统、数据库管理平台中将数据的类别、级别进行标识，方便对数据处理行为进行管理和审核。对于业务涉及多个行业领域的数据处理者，则应根据不同业务系统、数据库对应的行业领域情况，对数据的类别、级别等分别进行标识，避免出现矛盾情形。

动态更新管理数据处理者可参考《规则》附录 J，在业务应用场景、数据处理方式和规模发生变化、发生数据安全事件导致数据敏感性发生变化等情形出现时，对数据分类分级的规则和结果进行更新。并在开展内部数据安全审计和个人保护影响评估等工作的过程中，对数据分类分级工作成果进行评估和相应处置。

需要注意的是，分类分级规则的形成和清单的建立仅仅是分类分级管理的先导工作，数据处理者在形成规则和清单的基础上，应进一步制订数据分类分级保护的内部制度，并要求各部门人员根据制度要求对数据进行安全管理。

在分类分级工作规范开展方面，数据处理者可基于已形成的组织内分类分级规则和结果清单制定《数据分类分级管理制度》，明确组织内部不同部门及各岗位人员在数据分类分级识别、记录、维护、更新、报送等方面的职责分工，书面确认分类分级工作的实施流程和细则要求。

而在数据配套安全措施实施方面，数据处理者可在前述工作的基础上，制订《数据分类分级安全保护策略》，在数据访问、存储、对外提供、共享、前端展示等处理环节中采用与其级别、类别相适应的安全控制措施，提升数据处理活动的合规性。对于核心数据、重要数据的安全管理工作，还应参考《信息安全技术 重要数据处理安全要求》（征求意见稿）等文件的正式发布版本严格开展。

（二）明确主管部门的关键作用，加速行业数据标准化管理与数据资源整合

由于不同行业所开展的经营活动性质存在差别，不同行业数据处理者处理活动的典型场景、数据类别、敏感程度等存在较大差别，数据处理者依据统一的《规则》完全自主开展数据分类分级工作仍具备较高难度。因此，行业领域主管机构的组织和引导工作则尤为重要。主管部门需要将分类分级的规则根据行业特性进行明确细化，所提供的不应仅是原则性的要求。

在《规则》提供的框架和附录 G 的基础上，各行业领域的主管部门可结合本行业现行的数据处理活动情况，制定行业数据分类分级标准规范：

- 根据数据的分级要素，明确本行业领域核心数据和重要数据识别的具体细则，明确所涉及的范围，形成本行业领域核心数据、重要数据的推荐性目录，为行业内数据处理者提供划分依据说明；

- 制定本行业领域数据处理者对自身核心数据、重要数据目录的报送和管理要求，明确未按规定开展工作的后果；
- 发布可落地的指南性文件，组织引导本行业本领域的数据分类分级工作，为数据处理者提供必要的支持和指导，引导数据处理者完成有效自查、管理和报送。

结合本次发布的《规则》，各行业领域主管部门亦能够以数据为切入点，加快本行业的数据标准化治理工作，形成行业数据目录资源清单，推动本行业信息化、标准化发展，串联打通行业上下游产业链，从而借助行业内的数据合作提升全行业的生产经营效率。

（三）衔接数据要素价值释放制度，进一步夯实数据要素流通交易的机制基础

本次规则的发布，也与“数据二十条”和《“数据要素×”三年行动计划（2024—2026年）》等数据要素统一市场建设方面的国家政策进行了有效联动，数据处理者在《规则》指引下开展数据分类分级工作有助于其结合自身掌握的数据资源，释放数据要素价值。

数据处理者可在基于已开展分类分级工作的成果，根据《规则》以数据主体为角度的方法对数据进行分类，以呼应“数据二十条”提出的“建立公共数据、企业数据、个人数据的分类分级确权授权制度”要求，并结合数据分级结果明晰组织内部的数据资源结构，从而进一步开展数据资源确权、数据资源入表、数据产品的形成与交易等一系列工作。

数据处理者可以在根据《规则》形成的数据分类分级清单的基础上进一步判断不同类别级别的数据是否由自身“合法拥有或控制”、“是否会给企业带来经济效益”，更为清晰的界定数据生产、流通、使用过程中各方享有的数据资源持有权、数据加工使用权、数据产品经营权等合法权利，并结合分类分级成果对原始数据进行价值复用与充分利用，推动组织内部的数据资本化等数据要素价值释放进程。

行业主管部门后续也有望结合行业数据分类分级标准，发布数据流通方面的行业标准及指南文件，推荐本行业符合流通要求的数据按照类别、级别流通的工作模式，以及不同类别、级别数据流通时应遵循的安全规则。此举既可以提升行业内组织开展数据分类分级工作的积极性，又能够实现有序拓展数据要素应用场景的广度和深度，基于可开发利用的数据资源打造典型的数据应用场景和流通体系，充分发挥数据要素的“乘数效应”。

结语

本次《规则》的发布，与国家“十四五”规划和《数据安全法》所提出的“建立数据分类分级保护制度”的相关要求相呼应，其作为通用性的数据分类分级指导框架，有助于各行业领域主管部门在此基础上制定和更新数据分类分级制度和实施指南，为数据处理者在内部建立和完善数据数据分类分级制度、针对不同类别和级别的数据采取对应的数

据保护技术和管理措施提供指导。《规则》中正式发布的重要数据识别指南也将与《促进和规范数据跨境流动规定》一同帮助数据处理者识别重要数据，妥善进行数据跨境流动，避免合规风险。开展数据分类分级工作本身不是目的，而是应当据此合理配置数据安全管理资源，作为前置程序有序推进各行业各领域的数据治理工作。对在不同行业、不同业务场景下的差异化数据进行系统的梳理，形成标准化、体系化的数据结构，将有助于推进数据分类分级确权授权使用和市场化流通交易，形成符合数字经济发展规律的数据要素市场。

各行业领域的数据处理者需要结合自身所处行业、业务场景等因素，密切关注配套行业标准和文件的出台，并根据《规则》和所处行业的要求建立内部的数据分类分级管理制度，在提升组织数据处理活动安全合规能力、加强对不同类别级别数据安全保护的同时，促进数字经济生态的建设发展，释放自身掌握的数据要素价值，实现数据有序流动。

3. 数据跨境传输：解读《促进和规范数据跨境流动规定》：流动与安全并重[21]

引言

以往，《数据出境安全评估办法》等法律法规，虽搭建出数据出境合规监管框架（简称“旧框架”），但由于细则规定不够明确，企业在数据出境时往往需要结合其主体类型、出境数据类型和累计出境的数量等，综合判断采取何种数据出境制度（即“申报并通过数据出境安全评估、签署并备案个人信息出境标准合同（简称“SCC”）、获得个人信息保护认证”的统称）。自 2023 年 9 月 28 日，国家网信办（简称“网信办”）发布了《规范和促进数据跨境流动规定（征求意见稿）》（简称“《征求意见稿》”）（相关解读可参考文章《构建安全可控、促进发展的数据跨境流动框架：法律与实践的探索》）之日起，社会各界便对数据出境合规措施的选择展开了广泛讨论。

讨论最多的话题，例如“*直接在境外收集境内自然人个人信息应当直接适用个保法但是否属于数据出境的范畴？向境外总部传输员工个人信息、供应商和客户联系人信息是否无需进行 SCC 备案？向境外传输设备运维数据或日志数据等是否需要采取出境制度以及需要采取哪一个具体的合规路径？*”这些均是近半年来客户在数据跨境传输方面最为关注的一些问题。

历经半年，网信办对于各方的反馈意见（例如，建议说明出境个人信息数量时间计算方式、明确是否需要将拟出境敏感个人信息的数量作为申报数据出境安全评估的考虑因素、明确出境时应当取得个人“单独”同意等）进行了细致研判，在 2023 年 11 月 28 日在网信办第 26 次室务会议审议通过后，终于在 2024 年 3 月 22 日正式公布了《促进和规范数据跨境流动规定》（简称“《规定》”），并自颁布之日起施行。《规定》对数据出境监管框架进行了细化（新旧框架的对比详见本文附件表格），相比旧框架，《规定》**进一步放宽了数据跨境流动条件，且相对收窄了数据出境安全评估范围，把“促进”调整到了“规范”前面**，释放出要确保在保障数据安全的前提下，更加关切国家经济发展，通过便利数据跨境流动，降低企业合规成本，促进服务贸易与数字经济的大力开展和实施。

同日，网信办也发布了配套指南《数据出境安全评估申报指南（第二版）》《个人信息出境标准合同备案指南（第二版）》，进一步说明了申报数据出境安全评估、备案个人信息出境标准合同的方式、流程和材料等具体要求。并且，《规定》明确表示，当《数据出境安全评估办法》《个人信息出境标准合同办法》等**相关规定与《规定》有冲突的，以《规定》为准予以适用**。

因《规定》对企业选择数据出境制度有重大影响，本文结合实践需求，通过分析加问答的形式来解答企业关切的重点问题。

[21] 作者：孟洁、赵姝、戴畅、田梓仪

一、新规下什么行为会被认定为“数据出境”？

在讨论如何执行《规定》之前，首先需要明确“数据出境”的定义。网信办最新发布的《数据出境安全评估申报指南（第二版）》《个人信息出境标准合同备案指南（第二版）》对于“数据出境”的认定标准进行了更新，包括如下情形：

（1）数据处理者将在境内运营中收集和产生的数据传输至境外；

（2）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；

（3）符合《中华人民共和国个人信息保护法》（简称《个人信息保护法》）第三条第二款[22]情形（包括以向境内自然人提供产品或者服务为目的；分析、评估境内自然人的行为），在境外处理境内自然人个人信息等其他数据处理活动（新增）。

据此，除了过往熟悉的“境内数据向境外直接传输”、“境内数据被境外访问或调取”两种场景之外，今后**直接在境外处理境内自然人个人信息的行为也已被确定属于数据出境的范畴**。例如，某设立在境外的外国企业面向我国境内用户提供 App 的下载服务，并且直接收集境内用户个人信息并处理，则将被认定为该企业的活动涉及个人信息出境。

二、“重要数据”出境应当申报安全评估，那么究竟如何认定“重要数据”？

一直以来，监管部门明确要求企业对“重要数据”[23]的出境活动在进行安全风险自评估的基础上，向网信部门申报数据出境安全评估。

（一）“识别”与“认定”的义务分配更明确

《规定》第二条首先指出，**企业应当按照相关规定识别、申报重要数据**。就在《规定》公布的前一天，国家标准《数据安全技术 数据分类分级规则（GB/T 43697-2024）》（简称“《数据分类分级规则》”）正式发布，并将于 2024 年 10 月 1 日起正式实施。该规则吸收并细化了《信息安全技术 重要数据识别指南（征求意见稿）》的内容，在附录 G 部分明确列举“重要数据”的 17 项考虑因素以及相应的示例，以供企业参考。

尽管如此，在实践操作过程中，不少企业在自行判断拟出境数据是否属于“重要数据”时，还是存在一定的困难和挑战。对此，《规定》给出了明确指引，即**重要数据的认定以地方和行业主管部门的通知或公开发布为标准。若企业未被相关部门、地区通知处理了重要数据，或者相关部门、地区未公开发布的重要数据目录清单中未包括企业所处理数据的，则企业无需将某类数据作为重要数据申报数据出境安全评估**。一方面，将认定重要数据的艰巨任务从企业身上“移除”，让对自身数据出境的合规风险有了更加明确

[22] 第三条 ……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。

[23] 根据《数据出境安全评估办法》，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。

的可预见性，减轻了企业的合规压力，体现出《规定》促进数据流动的初衷；另一方面，这也反向督促各地区、各部门落实《数据安全法》的规定，按照数据分级分类保护要求，加快制定、确定本地区、本部门以及相关行业、领域的重要数据目录和清单。

各地区也正在积极探索建立数据分级分类的保护制度，以确定“重要数据”为目的，同步促进数据跨境流动管理。例如，天津自由贸易试验区于今年 2 月 5 日率先发布了《中国（天津）自由贸易试验区企业数据分类分级标准规范》[24]，将数据分为 13 大类 40 子类，核心、重要、一般三个级别，以此解决企业数据跨境流动政策诉求；上海市政府也于 2 月 3 日印发了《上海市落实<全面对接国际高标准经贸规则推进中国（上海）自由贸易试验区高水平制度型开放总体方案>的实施方案》，提出率先制定重要数据目录[25]。

（二）企业现阶段的应对措施

在期待各行业、各地区、各部门“重要数据”目录和清单出台的同时，**我们也建议相关企业**：①依据现有法律法规以及《数据分类分级规则》等国家标准进行**企业内部的数据分级分类制度建设**，识别可能涉及的重要数据并采取相应的保护措施。在相关目录和清单出台之前，仍应审慎对待本企业的数据出境活动；②主动**与各地区、行业的主管部门沟通**，及时调整数据跨境策略；③**持续关注“重要数据”目录和清单调整范围**，并对企业拟出境数据的合规性进行阶段性确认，对未来可能发生的政策变化进行提前预防。

三、如何进行“个人信息”和其他普通数据出境的合规工作？

（一）哪些情况下可豁免采取“数据出境制度”？

为促进数据的自由流动，《规定》第三条、第四条、第五条、第六条均规定了免予申报安全评估、订立标准合同、通过个人信息保护认证的特殊场景，如下：

1. 个人信息过境

根据《规定》第四条，**如果企业在境外收集和产生的个人信息传输至境内处理后向境外提供，处理过程中没有引入境内个人信息或者重要数据的（新增），不再需要采取数据出境制度**。这也提示企业，如希望适用该条豁免规定的，则应当注意将从境外收集产生的数据与境内的数据分开存储、进行物理隔离，防止在处理过程中境内外数据发生混同，进而无法被认定为“个人信息过境”导致无法豁免“安全保障性措施”。

2. 为订立、履行个人作为一方当事人的合同所必需

根据《规定》第五条第一项，符合“为订立、履行个人作为一方当事人的合同”的合法性基础，确需向境外提供个人信息的，不需要采取数据出境制度。为“履行合同所必需”的场景包括**跨境购物、跨境寄递（新增）、跨境汇款、跨境支付（新增）、跨境开户**

[24] 参见天津市商务局官网：
https://shangwuju.tj.gov.cn/tjsswjzz/zwgk/zcfg_48995/swjwj/202402/t20240207_6534807.html
[25] 参见上海市人民政府官网：
https://www.shanghai.gov.cn/nw12344/20240205/2af907af61cf4977866b7d377baf5d1d.html

（新增）、机票酒店预订、签证办理、考试服务（新增）等需要向境外提供个人信息的情形。例如，消费者投资国际金融产品时，可能需要向境外提供投资人姓名、身份证信息、联系方式、财务状况等必要个人信息，在此情况下很可能得以豁免。而哪些信息属于“确需”的范畴，仍须进一步通过实践案例进行识别和明确。

3. 基于人力资源管理所必需而出境员工个人信息

根据《规定》第五条第二项，**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，确需向境外提供本企业内部员工个人信息的，不需要采取数据出境制度**。但是，企业依据本场景豁免采取数据出境制度的，还需在实践中进一步评估以下问题：例如，如何确定向境外提供员工个人信息的行为是为实施人力资源管理所“确需”的；如何确定特定字段的出境是为实施人力资源管理所“确需”的。

4. 紧急情况下为保护自然人的生命健康和财产安全

根据《规定》第五条第三项，**紧急情况下为保护自然人的生命健康和财产安全，确需向境外提供个人信息的，不需要采取数据出境制度**。例如，某国家发生了突发性疫情，为了挽救受影响的人民群众的生命安全，某些组织需要将患者的个人信息发送给国际救援机构，以便采取救援措施。但“紧急”到何种程度才可以受豁免，仍然需要通过实践运用而细化明确。

5. 特殊场景下的普通数据出境

企业在实践中常常会问到这一问题：除了个人信息或者重要数据之外的其他数据，例如外贸数据、营销数据、设备运维数据等出境是否需要履行数据出境的相关合规义务。《规定》第三条相对明确地回应了企业的疑虑，**针对下述商业贸易、跨境运输（新增）、生产制造、学术交流等数据跨境流动频繁的领域**对普通数据（不包含个人信息或者重要数据）采取数据出境制度进行了豁免，旨在促进对外开放。以下，我们通过举例的方式，对上述场景中涉及的跨境传输数据情况进行阐释。

国际贸易	例如，当某国内外贸企业向他国出口商品时，需要将关于**商品的数量、规格、重量、价值等信息**发送给进口方，以便帮助各国的海关和贸易伙伴更好地管理和监控这批出口货物的安全交付过程，确保货物能够按时到达目的地，并保证贸易合规性。
跨境运输	例如，在国际贸易过程中，某国内企业在选定国际物流公司后，需要将**运输订单信息、货运线路、运输方式、运输工具、报关信息、在途信息以及费用结算信息等**必要信息传输给货物接收方，以便完成物流运输配送。这一场景往往和上述“国际贸易”紧密相连，故《规定》在《征求意见稿》的基础上加入了“跨境运输”的场景。
学术合作	例如，当国内某研究所与其他国家或机构的研究人员合作进行学术研究时，可能需要共享一些数据，包括**实验结果、调查结论、统计数据等**，以便研究人员更好地共享知识、经验和研究成果，推动国际学术界的合作与交流。但是，需要注意，该场景下的数据出境涉及行业及领域的适

	用性较宽，某些敏感领域中的数据，即使不属于个人信息或重要数据，但是否还可能构成“情报”信息等也有待观察。并且，实践中如何在学术合作场景中鉴别被共享的学术数据不涉及重要数据或者国家秘密，也是一项技术性很强的工作。
跨国生产制造	例如，一家制造型国企在全球多个国家设有生产基地，在进行产品生产制造和装配时，一些数据，例如**物料库存管理信息、零部件生产计划等**，需要从我国出境以支持对生产基地的有效供应链管理，使该企业更好地协调和管理其在全球的供应链，确保物料的及时供应、使当地生产顺利进行。
市场营销	例如，一家跨国消费品企业打算进入我国市场或扩大其在中国市场的业务前，需要对我国市场进行分析调研。在这个过程中，该企业必然需要收集和分析市场数据，包括**我国各线市场调研报告、同行市场占比分析数据、消费者行为数据等**，以了解目标市场的消费者需求、竞争情况、市场趋势等，从而制定相应的市场营销策略和计划。

- **其他普通数据**

《规定》使用了“等活动”是为了对以上举例场景以外的不包含个人信息或者重要数据的普通数据进行兜底。然而，如何确定“等活动”的具体范围？如何确定跨境活动下的数据为普通数据且能够自由跨境流动而无须采取出境制度？这些细节问题均需要在实践中进行精准判断后，逐步形成确定性意见，并由监管机构进一步发布补充性解释说明。

通常一个企业如涉及出境活动的，往往涉及各类业务场景、集团内不同法律实体，并且涉及相关环节、参与方多样，涉及的数据类型和境外接收方也往往很多，数据出境的链条也较为复杂。例如，在市场营销场景下，企业往往会针对特定个人信息主体进行精准营销，也包括利用去标识化处理后的数据对某类人群包进行定向分析和营销，另外还有些不包括个人信息或重要数据的普通数据（例如 aggregative data）。企业若要适用豁免机制，则需要首先准确地判断拟出境的数据是否已经全部达到个人信息匿名化的处理要求。因此，如何识别拟出境的数据是否“不属于个人信息或重要数据”，仍需在实践中进一步探索合规落地标准，也建议企业与监管机构保持沟通或关注其他相关新规出台，或者咨询专业律师以获取对不明确问题的指导与解释。

6. 未列入“自贸区负面清单”的数据

《规定》设计了“自贸区负面清单”的机制——**自由贸易试验区在国家数据分类分级保护制度框架下，可以自行制定区内需要纳入数据出境安全评估、个人信息出境标准合同、个人信息保护认证管理范围的数据清单**（简称“负面清单”），并经省级网络安全和信息化委员会批准后报国家网信部门、国家数据管理部门备案，以简化数据出境机制。

据此，**如果企业位于自贸区内，向境外提供负面清单以外的数据，可以免予申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证**。但需要注意的是，在自贸区负面清单出台前，注册在自贸区内企业的数据出境活动仍需要按照国家数据出境安全管理有关规定执行。

以上海自贸区和临港新片区近期的数据跨境流动管理动态为例。上海市人民政府于2024年2月3日印发了《上海市落实<全面对接国际高标准经贸规则推进中国（上海）自由贸易试验区高水平制度型开放总体方案>的实施方案》，提出制定重要数据目录、探索建立合法安全便利的数据跨境流动机制、在临港新片区建立数据跨境服务中心等措施之后，临港新片区于2024年2月8日编制发布了《中国（上海）自由贸易试验区临港新片区数据跨境流动分类分级管理办法（试行）》，规定了重要数据目录和一般数据清单的管理要求；企业对于**在一般数据清单内的数据，向管委会进行申请备案后，可自由流动[26]。其思路是通过建立"正面清单"，推动《规定》落地和鼓励符合要求的辖区内数据进行自由跨境传输。**

此外，上海自贸区和临港新片区已基本编制完成智能网联汽车车辆远程诊断、公募基金市场投研信息、跨国公司集团管理、生物医药临床试验和研发等20个场景的跨境流动分级分类的首批清单目录，在完成论证后将于近期对外发布。[27]

我们建议设立在自贸区的企业时刻关注自贸区发布数据出境负面清单的最新动向，及时了解自身所在的自贸区是否为企业设置了数据跨境流通的便利通道（例如"白名单"机制），并及时学习并遵守相关规定，由此确保企业既符合数据出境合规性，又享受自贸区内顺畅进行数据跨境流通的优惠待遇，降低数据出境的合规成本和业务压力。

（二）无法豁免的情形下，数据出境应当采取哪种"数据出境制度"？

如果数据出境不属于上文中提及的可以豁免的业务情形，根据《规定》第五条第四项、第七条第二项和第八条，针对拟向境外提供个人信息的一般企业，应当根据如下标准判断自身应当采取的数据出境制度：

1. 自**当年1月1日起累计向境外提供不满10万人个人信息**（不含敏感个人信息）的，免予申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证；

2. 自**当年1月1日起累计向境外提供10万人以上、不满100万人个人信息**（不含敏感个人信息）或者**不满1万人敏感个人信息**的，应当依法与境外接收方订立个人信息出境标准合同或者通过个人信息保护认证；

3. 自**当年1月1日起累计向境外提供100万人以上个人信息**（不含敏感个人信息）或者**1万人以上敏感个人信息**，应通过所在地省级网信部门向国家网信部门申报并通过数据出境安全评估。

关于采取何种数据出境制度的判断标准，此前《数据出境安全评估办法》的着眼点在**自上一年度起已出境的**个人信息主体数据量，以及企业作为个人信息处理者**已处理的**

[26] 参见中国（上海）自由贸易试验区临港新片区管理委员会官网：https://www.lingang.gov.cn/html/website/lg/index/government/file/1756018881550389249.html

[27] 在3月6日十四届全国人大二次会议上海代表团举行开放团组会议上，全国人大代表、临港新片区党工委副书记袁国华接受外媒采访时说明的内容，参见观察者网报道：https://www.guancha.cn/politics/2024_03_06_727487.shtml

数据存量[28]。《征求意见稿》不再谈论“过往”，重点关注**预计未来一年内**拟出境的个人信息主体数据量[29]。相较之下，**《规定》则在“过往”和“未来”之间选择了一条“立足当下”的折中路径--从当年 1 月 1 日起向境外提供的个人信息主体数据量加总作为判断标准**，不再要求企业进行“预判”，从而降低企业与监管各自的工作难度。

《规定》也优化调整了可以采取豁免数据出境制度的人数判定阈值：相较于此前《征求意见稿》提出的“不满 1 万人”，《规定》将这个数字提升到“不满 10 万人”，加大了企业可相对自由地向境外传输个人信息的空间。另一方面，《规定》也将需要申报数据出境安全评估的门槛从《数据出境安全评估办法》项下的“10 万人以上个人信息”提升到“100 万人以上个人信息”，但敏感个人信息数量保持在 1 万人以上需要申请数据出境安全评估不变，但起始点却从去年 1 月 1 日起统一变为自当年 1 月 1 日起。因此也仅为适度收窄了数据出境安全评估的范围，减轻企业一部分负担。

此外，《规定》的出台厘清了《征求意见稿》中有关个人信息出境方面的几个重要问题，为企业判断采取何种数据出境制度提供了更为细化、明确的标准：

- **敏感个人信息出境情况是否需要考虑在内？**

《规定》给出的答案是：需要。并且以当年 1 月 1 日起累计满 1 万人敏感个人信息作为须申请出境安全评估的门槛标准。

《征求意见稿》的文本未对个人信息、敏感个人信息进行了区分只统一讨论个人信息（不管是否包含敏感个人信息）出境人数这种情况。

而《规定》则回归到《数据出境安全评估办法》的思路，将“敏感个人信息”对应的拟出境的自然人数量纳入与个人信息所对应的当年拟出境人数并列关注的范围，**并以自当年 1 月 1 日起累计向境外提供“1 万人以上敏感个人信息”作为须申请数据出境安全评估的阈值标准**。

- **既存在豁免情形，但由于向境外提供个人信息的人数超出 10 万人而需要完成数据出境制度时，该如何处理？**

企业可能会问到，如果其符合《规定》第五条第二项“为实施跨境人力资源管理”的豁免条件，但该企业出境的员工人数超过 10 万人而不满 100 万人的，是否仍需要完成个人信息标准合同备案或通过个人信息保护认证；倘若出境个人信息的人数超过 100 万人时是否仍须申报安全评估？

---

[28] 根据《数据出境安全评估办法》，一般企业向境外提供个人信息时需要申报数据出境安全评估的情形包括：（i）处理 100 万人以上个人信息的；（ii）自上年 1 月 1 日起累计向境外提供 10 万人个人信息的；或（iii）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。

[29] 根据《征求意见稿》第五条、第六条：（i）预计一年内向境外提供 1 万人以下个人信息的一般企业，将豁免数据出境安全评估申报、标准合同备案或个人信息保护认证；（ii）预计一年内向境外提供 1 万人以上不满 100 万人个人信息的一般企业，需要进行标准合同备案或个人信息保护认证，可以不申报数据出境安全评估；（iii）预计一年内向境外提供 100 万人及以上个人信息的一般企业，需要申报数据出境安全评估。

《规定》给出的答案是：否，优先遵从豁免情形。如果存在上文所述豁免数据出境制度的特殊情形（《规定》第三条、第四条、第五条、第六条规定情形的），从其规定。

- **如何计算当年累计向境外提供的个人信息数据量（1 万、10 万、100 万）？**

《规定》颁布后国家网信办答记者问（下称“答记者问”）明确了如何计数的问题：

（1）计算周期为自当年 1 月 1 日起至申报数据出境安全评估之日。

（2）在数量统计上：①需要以自然人为单位进行去重，例如涉及出境一个自然人的多种个人信息的，记一个自然人；并且②属于上文所述豁免采取数据出境制度的情形（《规定》第三条、第四条、第五条第一款第一项至第三项、第六条规定情形的），不计入累计数量。

- **“已处理 100 万人个人信息的个人信息处理者”是否还适用？**

《规定》给出的答案是：不再适用。

过去，根据《数据出境安全评估办法》，如果某企业属于已经处理了 100 万人以上个人信息的个人信息处理者，即使其只出境了 1 个自然人的个人信息，也需申报数据出境安全评估。《规定》已不再强调企业历史上已处理的个人信息主体数据量（即处理 100 万人以上个人信息），而是限定在某一特定时期内（即自当年 1 月 1 日起至申报数据出境安全评估之日）累计出境的个人信息或敏感个人信息的数量。这将极大减轻有出境业务企业的出境负担，只要该企业自当年 1 月 1 日起实际出境的个人信息数量少于 100 万人或敏感个人信息少于 1 万人的，便可以免于申报数据出境安全评估。

（三）数据出境企业应当履行哪些其他合规义务？

应当注意的是，无论是否存在豁免采取数据出境安全保障措施的情形或人数，《规定》第十条强调，**企业作为个人信息处理者都应当履行《个人信息保护法》下的个人信息保护义务以确保数据出境的合规性（新增）**。包括：

1. 告知并取得个人单独同意

除非具有《个人信息保护法》第十三条第二项至第七项规定的不需取得个人同意的情形，根据《个人信息保护法》第三十九条的规定，企业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主体权利的方式和程序等事项，并取得个人的单独同意。

2. 进行个人信息保护影响评估

根据《个人信息保护法》第五十五条的规定，企业应当在个人信息出境前进行个人信息保护影响评估。如果企业在《规定》出台前已开展了部分数据出境合规工作（例如出境数据情况摸排和个人信息保护影响评估）的，则建议应继续进行，并将个人信息保护影响评估报告至少留存三年以备检查、确保合规。

3. 履行数据安全保护义务

根据《规定》第十一条，企业还需要采取技术措施和其他必要措施，保障数据出境的安全，包括通过合同、组织和技术等措施确保境外接收方达到适当的数据安全保护水平[30]。如果发生或者可能发生数据安全事件的，企业应当采取补救措施，及时向省级以上网信部门和其他有关主管部门报告。

四、关键信息基础设施运营者向境外提供重要数据或个人信息需要满足什么合规要求？

《规定》答记者问重申，**关键信息基础设施运营者（简称“CIIO”）的认定仍以“是否被通知”作为标准**。涉及的重要行业和领域的主管部门、监督管理部门负责制定本行业、本领域关键信息基础设施（简称“CII”）的认定规则，并由其组织认定本行业、本领域的 CII，且及时将认定结果通知 CIIO。

由于 CIIO 数据的泄露、损毁与灭失将对国家安全、社会稳定和个人隐私等产生重大影响，因此《规定》第七条第一项与《网络安全法》第三十七条、《个人信息保护法》第四十条和《数据出境安全评估办法》的相关规定保持一致。如果 CIIO 向境外提供个人信息或重要数据，应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。属于《规定》第三条、第四条、第五条、第六条规定情形的，从其规定。

虽然目前大多数企业并未被认定为 CIIO，但这些企业需要关注其客户或合作方是否有可能属于 CIIO，以及企业在与 CIIO 客户进行业务活动时，需要特别遵守与对方在跨境数据交互过程中的合规义务。

五、违反相关规定会面临什么处罚？

相较于《数据出境安全评估办法》和《个人信息出境标准合同办法》，《规定》第十二条规定的罚则相对缓和，给予了数据处理者接受监督、及时整改、消除隐患的机会，对于拟开展数据出境的企业是一大利好消息。

针对“拒不改正或者导致严重后果的”情况，《规定》第十二条明确规定将“依法追究法律责任”，即主要追究行政责任（例如 5000 万元以下或者上一年度营业额 5%以下罚款，直接负责的主管人员和其他直接责任人员担责等），也可能涉及民事责任甚至刑事责任。《征求意见稿》中规定的“依法责令其停止数据出境活动，保障数据安全”也必然会在企业受到法律责任的同时被要求。因此，企业应当引起重视，尽早依法依规完成合规工作。

六、还有哪些需要注意的程序性事项？

[30] 《个人信息保护法》第三十八条第三款：个人信息处理者应当采取必要措施，保障境外接收方处理个人信息的活动达到本法规定的个人信息保护标准。

相比于《征求意见稿》,《规定》以及配套发布的《数据出境安全评估申报指南（第二版）》、《个人信息出境标准合同备案指南（第二版）》明确了相关程序性事项，在此一并提示企业注意。

（一）数据出境安全评估结果有效期是多长？

《规定》给出的答案是：首次通过有效期 3 年，期满后可以再延 3 年。

《规定》将通过数据出境安全评估结果的有效期由《数据出境安全评估办法》中规定的 2 年延长至 3 年（自评估结果出具之日起计算）。

同时，增加企业可以申请延长评估结果有效期的规定。有效期届满，需要继续开展数据出境活动且未发生需要重新申报数据出境安全评估情形的，企业可以在有效期届满前 60 个工作日内通过所在地省级网信部门向国家网信部门提出延长评估结果有效期申请。经国家网信部门批准，可以延长评估结果有效期 3 年。

这意味着，如果企业在首次申报并通过数据出境安全评估后的 3 年内，该企业的数据出境活动仍未触发需要再次申报数据出境安全评估的情形，则企业数据出境安全评估结果有效期可以延长至 6 年。至于 6 年届满后，是否还能继续延长，《规定》和答记者问均未给出明确的答复，我们相信后续监管会给出具体标准。

（二）已经完成或者正在进行的数据出境安全评估与个人信息出境标准合同备案怎么办？

《规定》答记者问给出的答案是：《规定》施行前已经通过数据出境安全评估的数据出境活动，数据处理者可以根据申报事项继续开展。

《规定》施行前未通过或者部分未通过数据出境安全评估，根据《规定》免予申报数据出境安全评估的数据出境活动，数据处理者可以依法通过订立个人信息出境标准合同、通过个人信息保护认证等其他途径向境外提供个人信息。

《规定》施行前已经申报数据出境安全评估、提交个人信息出境标准合同备案，根据《规定》无需开展上述程序的，数据处理者可以按照原程序进行，也可以向所在地省级网信部门撤回申报、备案。

由上可见，在新旧规定两者的衔接问题上，监管部门采用的是“有利于企业开展数据出境”为原则的监管思路。随着近年来各省级网信部门咨询窗口实践水平的提升，以及《规定》第十二条明确提出各地网信部门应当加强对数据处理者数据出境活动的指导监督，强化事前事中事后全链条全领域监管，如果企业有任何疑问，也可咨询监管。

（三）申报与备案提交途径有无变化？

随着《规定》的出台，网信部门也在不断优化申报和备案的流程。根据《数据出境安全评估申报指南（第二版）》的新规定，申报数据出境安全评估、备案个人信息出境

标准合同的企业可以登录专设的数据出境申报系统（网址为 https://sjcj.cac.gov.cn）进行操作。根据《规定》答记者问，申请个人信息保护认证可以登录个人信息保护认证管理系统（网址为 https://data.isccc.gov.cn）。

CIIO 或者其他不适合通过数据出境申报系统申报数据出境安全评估的（目前指南中暂未明确“其他”不适合线上申报的范围），采用线下方式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。指南在《数据出境安全评估申报表》中设置了勾选重要数据情况一栏，因此我们理解涉及重要数据出境的企业可填写该申报表进行申报。

七、结语

千呼万唤始出来的《规定》坚定地拉开了数据跨境流动规范的新篇章。它确立了旨在促进和规范数据跨境自由流动的全面框架体系，通过多种“豁免场景”的设置以及对“数据出境制度”门槛与流程的优化，释放出为企业减负的友好信号。

（一）非 CIIO 企业应当根据《规定》及时评估对现有数据出境合规工作的影响：

1. 针对重要数据出境的：

- 未收到通知属于重要数据的非个人信息，也不属于国家秘密或者其他规章规定的特殊类型数据的，则按普通数据跨境规则处理。同时，应当关注行业、地区“重要数据”目录清单发布情况，并且企业应在内部建立健全数据分级分类制度，识别是否存在重要数据出境的情况。

- 如自行评估后发现可能存在处理重要数据的情况，则应及时向主管部门申报或进行主动沟通确认。若被认定为是重要数据的，则任何一条数据出境均应通过数据出境安全评估。

2. 针对个人信息出境的：

- 企业应先判断是否存在五类豁免场景，包括为订立、履行个人作为一方当事人的合同；实施跨境人力资源管理，确需向境外提供员工个人信息；紧急情况下为保护自然人的生命健康和财产安全，确需向境外提供个人信息；以及，拟出境数据未列入“自贸区负面清单”内。

- 企业应分别统计向境外传输个人信息或敏感个人信息当年的总人数，判断应当采取何种数据出境制度。是否存在少量人数出境的豁免情形，即自当年 1 月 1 日起累计向境外提供不满 10 万人个人信息（不含敏感个人信息）。

- 对于不需要实施数据出境安全评估、标准合同备案和个人信息保护认证三类数据出境制度的企业，也需要根据《个人信息保护法》等法律法规，继续完成“告知-同意”、事前个人信息保护影响评估等合规要求。

- 对于仍需要遵循安全评估、标准合同备案或个人信息保护认证路径的企业，则应继续按时完成相应的申报、备案或认证工作，准确了解每类数据出境制度的具体要求和流程，并按照相关规定进行操作。

3. 针对普通数据（非重要数据或个人信息）出境的：

- 针对国际贸易、跨境运输、跨国生产制造、学术合作、市场营销等活动中收集和产生的数据跨境流动豁免采取出境制度。

- 其他普通数据仍需在实践中进一步探索合规落地标准，但均属于能自由跨境流动而无须采取出境制度。

（二）被通知为 CIIO 的企业涉及个人信息或重要数据出境的，应依法依规完成数据出境安全评估。

同时，也建议企业密切关注监管部门后续对于《规定》的进一步解释与适用，特别是《规定》的豁免场景在实践中的认定情况（包括注册在自贸区的企业应关注自贸区数据出境负面清单或正面清单），以判断自身的数据出境情况是否满足豁免条件，并据此及时调整合规策略，确保企业在数据出境方面符合法规要求。

附件：数据出境合规框架的主要变化对比

对比项		旧框架	《征求意见稿》	《规定》
重要数据出境		企业拟出境的数据为重要数据的，则应当申报数据出境安全评估。	未被相关部门、地区通知或者公开发布为重要数据的，不需要作为重要数据申报数据出境安全评估。	企业应当按照相关规定识别、申报重要数据。未被相关部门、地区告知或者公开发布为重要数据的，不需要作为重要数据申报数据出境安全评估。
个人信息出境	数据出境安全评估	如果拟出境的数据为个人信息的，满足以下任一条件时，应当申报数据出境安全评估： （i）处理 100 万人以上个人信息的； （ii）自上年 1 月 1 日起累计向境外提供 10 万人个人信息的；或 （iii）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。	预计一年内向境外提供 100 万人及以上个人信息的，应当申报数据出境安全评估。	自当年 1 月 1 日起累计向境外提供 100 万人以上个人信息（不含敏感个人信息）或者 1 万人以上敏感个人信息，应当申报数据出境安全评估。

对比项		旧框架	《征求意见稿》	《规定》
	标准合同或认证	如果未满足上述任一情形的，则可以选择（i）订立并备案个人信息保护标准合同，或（ii）通过个人信息安全保护认证后出境个人信息。	预计一年内向境外提供1万人以上、不满100万人个人信息，需要进行标准合同备案或个人信息保护认证，可以不申报数据出境安全评估。	自当年1月1日起累计向境外提供10万人以上、不满100万人个人信息（不含敏感个人信息）或者不满1万人敏感个人信息的，应当订立个人信息出境标准合同或者通过个人信息保护认证。
	豁免情形	N/A	预计一年内向境外提供不满1万人个人信息的，不需要申报数据出境安全评估、订立个人信息保护标准合同、通过个人信息保护认证。	自当年1月1日起累计向境外提供不满10万人个人信息（不含敏感个人信息）的，免予申报数据出境安全评估、订立个人信息保护标准合同、通过个人信息保护认证。
豁免的特殊场景		N/A	a. 个人信息过境； b. 为订立、履行个人作为一方当事人的合同所必需； c. 基于人力资源管理所必需的出境员工个人信息； d. 紧急情况下为保护自然人的生命健康和财产安全； e. 国际贸易、学术合作、跨国生产制造和市场营销等活动（不包含个人信息或重要数据）； f. 未列入“自贸区负面清单”的数据。	a. 个人信息过境； b. 为订立、履行个人作为一方当事人的合同所必需； c. 基于人力资源管理所必需的出境员工个人信息； d. 紧急情况下为保护自然人的生命健康和财产安全； e. 国际贸易、跨境运输、学术合作、跨国生产制造和市场营销等活动（不包含个人信息或重要数据）； f. 未列入“自贸区负面清单”的数据。
CIIO		CIIO向境外提供个人信息或重要数据的，应当依法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。		

4. 数据跨境传输：解读《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同实施指引》：跨境数据流动创新保障性措施的先行先试[31]

引言

2023 年 12 月 13 日，国家互联网信息办公室（下称“国家网信办”）与香港创新科技及工业局为落实《关于促进粤港澳大湾区数据跨境流动的合作备忘录》（下称“《合作备忘录》”）中提出的组织实施粤港澳大湾区（下称“大湾区”）个人信息跨境标准合同的要求，共同制定了《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同实施指引》（下称“《实施指引》”），并以附件的形式提供了《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同》（下称“《大湾区标准合同》”）与《承诺书（模板）》供相关主体使用。

在 2023 年 6 月 29 日签署的《合作备忘录》公告中，国家网信办与香港特区政府创新科技及工业局共同提出将在国家数据跨境安全管理制度框架下，建立大湾区数据跨境流动安全规则。本次《实施指引》适用注册于/位于大湾区内地部分（**广东省广州市、深圳市、珠海市、佛山市、惠州市、东莞市、中山市、江门市、肇庆市**）或者香港特别行政区（下称“香港特区”）的个人信息处理者及接收方。作为《合作备忘录》核心思路的落地举措，《实施指引》可以进一步促进大湾区的数据有序高效流动，促进数据作为生产要素在大湾区城市群内充分释放价值，为大湾区产业发展赋能。

一、中国数据出境政策现状

1. 内地

在《中华人民共和国网络安全法》《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》（下称“《个保法》”）三部法律相继施行后，内地数据出境的基础合规框架已初步形成。在个人信息跨境流动方面，《个保法》第三十八条列明了个人信息处理者应采取的三项安全保障措施，即“通过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，约定双方的权利和义务”（上述三点合称为“数据出境保障性措施”）。随后，为帮助三种出境保障性措施落地，国家网信办及相关行业监管部门也陆续出台了一系列部门规章和指南性文件。

就“订立个人信息出境标准合同”而言，根据国家网信办于 2023 年 2 月 22 日发布的《个人信息出境标准合同办法》（下称“《标准合同办法》”）第四条，当个人信息处理者同时符合以下情形时，可以通过订立标准合同的方式向境外提供个人信息：

（一）非关键信息基础设施运营者；

[31] 作者：孟洁、王程、钱星辰、杜畅

（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个人信息不满 10 万人的；

（四）自上年 1 月 1 日起累计向境外提供敏感个人信息不满 1 万人的。

《标准合同办法》以附件的方式提供了《个人信息出境标准合同》（下称“《内地标准合同》”）的文本，且配套出台了《个人信息出境标准合同备案指南（第一版）》，进一步为标准合同的签订和备案提供了指引。

顺应 2022 年发布的《中共中央 国务院关于构建数据基础制度更好发挥数据要素作用的意见》（下称“数据二十条”），国家网信办在 2023 年 9 月 28 日发布了《规范和促进数据跨境流动规定（征求意见稿）》（下称“《跨境流动规定（征意稿）》”），旨在确保数据有序跨境流动的同时降低企业的合规负担。《跨境流动规定（征意稿）》虽未正式生效，但对三种数据出境保障性措施的适用逻辑进行了较大的调整更新，同时还提出了豁免采取安全保障措施的十大重点场景，较大程度地降低了个人信息出境合规要求的门槛。

2. 香港特区

在个人信息出境的立法方面，中国香港特区颁布的《个人资料（私隐）条例》（下称“《私隐条例》”）在其第 33 条中作出了专门规定。根据该条款，在香港进行或受主要营业地在香港的资料使用者[32]控制而收集、持有、处理[33]或使用[34]的个人资料[35]将原则上被禁止传输至香港以外的地方，除非满足以下条件：

- 转移目的地存在与《私隐条例》相似或已经生效的与本条例目的相同的法律；
- 使用者有合理理由认为该目的地存在上述法律；
- 有关的资料当事人[36]已通过书面方式同意该转移活动；
- 该使用者有合理理由相信：（i）该项转移是为避免针对资料当事人的不利行动或减轻该行动的影响而作出的；（ii）获取资料当事人的书面同意不是切实可行的；及（iii）如获取书面同意是切实可行的，且资料当事人会给予上述同意；

---

[32] **《私隐条例》项下的“资料使用者”：**就个人资料而言，指独自或联同其他人或与其他人共同控制该资料的收集、持有、处理或使用的人（具体请参见《私隐条例》第一部分）。

[33] **《私隐条例》项下的“个人资料的处理”：**个人资料的修改、新增、删除或重新排列（无论是否采用自动化或其他方法）（具体请参见《私隐条例》第一部分）。

[34] **《私隐条例》项下的“使用”：**包括个人资料的披露或转移（具体请参见《私隐条例》第一部分）。

[35] **《私隐条例》项下的“个人资料”：**指符合以下说明的任何资料（数据）：（a）直接或间接与一名在世的个人有关的；（b）从该资料直接或间接地确定有关的个人身份是切实可行的；及（c）该资料的存在形式使得查阅及处理均是切实可行的（具体请参见《私隐条例》第一部分）。

[36] **《私隐条例》项下的资料当事人：**就个人资料而言，指该资料隶属的个人（具体请参见《私隐条例》第一部分）。

- 该资料凭借《私隐条例》第 8 条的规定获得豁免，包括执行司法职能、个人事务、雇佣等事由；或
- 该使用者已采取所有合理的预防措施并已作出所有应尽的努力，以确保该资料不会以违反转移目的地《条例》的方式被收集、持有、处理或使用。

虽然《私隐条例》第 33 条“限制”个人资料向香港以外的地区进行转移且迄今已进行了数次修订更新，但时至今日该条款仍未实施。香港目前也尚未规定数据处理活动达到一定条件时必须采取的数据出境保障性措施，而更多是通过发布推荐性的指引来规范香港个人资料跨境转移的活动，具体而言：

- 2014 年 12 月，私隐公署发布了《保障个人资料：跨境资料转移指引》》（简称“《2014 年指引》”），初次提供了用于指导资料跨境转移的建议合约条文范本，以建议性的方式鼓励资料使用者采用该指引内的推荐操作模式来保护个人资料。
- 2022 年 5 月，私隐公署发布了《跨境资料转移指引：建议合约条文范本》（下称“《2022 年指引》”），进一步提供了两套用于资料跨境传输的范本，分别适用两种不同的跨境数据转移的情况，即（1）由一名资料使用者转移予另一个资料使用者，及（2）由一名资料使用者转移予一名资料处理者，旨在应对愈加严格的全球数据保护监管与新型的通信科技对资料跨境转移带来的新挑战。

尽管《私隐条例》第 33 条至今尚未生效，由《2014 年指引》和《2022 年指引》构成的建议合约条文范本体系可以帮助香港企业及相关组织更好地开展数据使用和处理活动，使之在日常的经营活动及与其他机构的合作中逐渐调整和适应，在满足合规要求的同时促进数据自由流动。

3. 粤港澳大湾区

基于内地和香港分别就个人信息跨境流动实践的探索，两地政府在 2023 年 6 月 29 日共同签署了《合作备忘录》，以在国家数据跨境安全管理框架下建立大湾区数据跨境流动的安全规则，推动该区域数字经济产业的高质量发展。在《合作备忘录》签署后，大湾区也在数据出境保障性措施的优化方面开展了部分探索性工作。

2023 年 10 月，香港特区行政长官李家超发表《行政长官 2023 年施政报告》时提到，将在大湾区以先行先试方式，简化内地个人资料流动到香港的合规安排。2023 年 11 月 1 日，全国信息安全标准化技术委员会进一步制定了《网络安全标准实践指南—粤港澳大湾区跨境个人信息保护要求（征求意见稿）》，规定了大湾区跨境处理个人信息应遵循的基本原则和保护要求。该标准文件作为实践指南，虽不具有

法律强制性，但仍然为“个人信息保护认证”这一数据出境保障性措施在大湾区的弹性落地提供了实操性指引。

本次发布的《实施指引》则进一步完善了大湾区的数据流动合规实施路径，有助于将数据作为推动经济增长的新引擎，促进区域性数字经济的发展。

二、《实施指引》的七大亮点

本次发布的《实施指引》及其附件《大湾区标准合同》，在《标准合同办法》及《内地标准合同》的基础上，充分考虑了内地和香港两个不同法域出境政策的要求和大湾区在数字经济发展方面的重要战略角色，其创新重点体现在以下七个方面。

1. 结合政策定位明确适用范围

根据香港特区政府资讯科技总监办公室的说明，《大湾区标准合同》是一项简化大湾区中内地地区与香港之间的个人信息跨境[37]流动合规安排的措施，属自愿性质，让两地的个人及机构按统一范本订立标准合同，规范合同双方在个人信息保护方面的责任和义务[38]。依据《实施指引》第二条，可以订立《大湾区标准合同》的情形包括两种：由大湾区中的内地地区向香港传输个人信息、或由香港向大湾区中的内地地区传输个人信息。《实施指引》同时明确，如果跨境流动的个人信息被其他相关法律文件认定为重要数据时，个人信息出境方无法通过与入境方签署《大湾区标准合同》的方式作为数据合规保障路径实施出境活动。

在跨境个人信息数量或出境时间的要求方面，《实施指引》则没有具体说明。根据《实施指引》第四条，通过订立《大湾区标准合同》方式跨境提供个人信息的，应当履行标准合同列明的义务责任，并确保在个人信息处理者跨境提供个人信息前，按照个人信息处理者属地法律法规要求告知个人信息主体或者取得个人信息主体的同意，且不得向大湾区以外的组织、个人提供（包括不得从香港地区再传输到其他国家地区）。

2. 因地制宜明确出境适用要求

《实施指引》和《大湾区标准合同》在法律法规的适用方面，充分考虑了内地和香港的数据保护法律体系的差异。

《大湾区标准合同》在第一条中，基于内地《个保法》和香港《私隐条例》，对“个人信息处理者”“个人信息主体”“监管机构”等不同的术语进行了区分解

[37] 此处“跨境”指的是跨关境：关境以内即适用《中华人民共和国海关法》及相关关税制度的区域，也即除港澳台地区以外的中华人民共和国领土；关境以外，包括中华人民共和国拥有主权的港澳台地区，和中华人民共和国行使主权的领土范围以外的国家或地区。

[38] https://www.ogcio.gov.hk/sc/our_work/business/cross-boundary_data_flow/index.html，最后访问于 2024 年 1 月 11 日。

释。而在个人信息识别和合规基础义务的履行方面，《大湾区标准合同》也提出了应当按照两地的法规进行分别确认。

在争议解决方面，《大湾区标准合同》第八条第四项列明了仲裁机构，在保留了中国国际经济贸易仲裁委员会、中国海事仲裁委员会的基础上，更新补充了中国广州国际仲裁委员会、粤港澳大湾区国际仲裁中心、香港国际仲裁中心三个机构，并将诉讼涉及的管辖机构明确为“内地或者香港”有管辖权的人民法院。在该条第五项也明确了合同的解释应当按照个人信息处理者属地相关法律法规的规定进行解释，且不得与个人信息处理者的权利、义务相抵触，降低了因合同产生争议或纠纷而裁判依据不明确造成的解释不准确性。

3. 结合实践要求增加监管主体

在《大湾区标准合同》适用的监管部门方面，《实施指引》第十条及第十一条列明了国家互联网信息办公室、广东省互联网信息办公室或者香港特区政府创新科技及工业局、政府资讯科技总监办公室、香港个人资料私隐专员公署有开展监管活动的权利、责任及义务，明确了内地与香港政府部门有序监管大湾区数据流动活动的监管框架。

4. 平衡个人信息处理者责任义务

虽然个人信息转移双方订立的合同必须严格依据《大湾区标准合同》订立，不得随意修改，但个人信息转移双方可在不与《大湾区标准合同》的内容相冲突的前提下就商业行为另定商业合同[39]。同时，在内地组织或个人作为个人信息处理者时，《大湾区标准合同》规制的内容与《内地标准合同》需要履行的义务和应承担的责任相比之下较少。以订立标准合同前需要开展的个人信息保护影响评估工作为例，《实施指引》将重点评估的内容缩减为三项，仅保留：

（一）个人信息处理者和接收方处理个人信息的目的、方式等的合法性、正当性、必要性；

（二）对个人信息主体权益的影响及安全风险；

（三）接收方承诺承担的义务，以及履行义务的管理和技术措施、能力等能否保障跨境提供的个人信息安全。

对照内地《标准合同办法》，个人信息处理者根据《大湾区标准合同》开展个人信息保护影响评估时不再需要重点评估：跨境流动个人信息的规模、范围、种类、敏感程度；个人信息跨境流动后遭到篡改、破坏、泄露、丢失、非法利用等的

[39] https://www.ogcio.gov.hk/sc/our_work/business/cross-boundary_data_flow/index.html，最后访问于 2024 年 1 月 11 日。

风险，个人信息权益维护的渠道是否通畅等；接收方所在地区的个人信息保护政策和法规对标准合同履行的影响。

上述评估维度的缩减可视作两地对彼此数据保护立法政策方面的认同，并对两地在合作机制下对《实施指南》与《大湾区标准合同》的灵活更新与调整具备充分的信心。

需要注意的是，当位于香港的组织或个人作为个人信息处理者通过签署《大湾区标准合同》的方式向内地传输个人信息时，因为《大湾区标准合同》的规定在较多维度上与内地的要求保持一致，因此香港的组织或个人也应重点关注《个保法》等内地法律法规的要求和合同约定以履行合规义务。

5. 合理减轻接收方合规责任义务

在接收方的合规责任义务方面，《大湾区标准合同》较《内地标准合同》不仅移除了接收方利用个人信息进行自动化决策时需要履行的责任义务，还移除了接收方应允许个人信息处理者对必要数据文件和文档进行查阅等方面的相关表述，在保障必要的责任义务的同时完成了合理减负。

值得注意的是，与《内地标准合同》相比，《大湾区标准合同》在第三条第八项中明确，接收方向同一辖区内的第三方提供个人信息时，仅需满足确有业务需要、履行告知义务、以及依法征得有效同意并符合合同附录所列约定的要求，极大提升了个人信息在大湾区内部流通的便捷性。

虽然《大湾区标准合同》相较《内地标准合同》移除了多项合规要求，值得注意的是，《大湾区标准合同》在第三条第七项和第八项中，明确了不得向大湾区以外的组织、个人提供根据此合同接收的个人信息（包括个人信息向境外第三方的再传输行为），将个人信息跨境流转的范围限定在了大湾区。

6. 强调个人信息主体权利行使保障

《大湾区标准合同》虽免除了个人信息处理者出境安全保障措施中的部分义务，但依据《实施指引》第四条第一项的要求，处理者在跨境提供个人信息前仍然应当按照个人信息处理者属地法律法规要求告知个人信息主体或者取得个人信息主体的同意，保障了个人信息主体知情同意的权利。《大湾区标准合同》除了强调须同时基于属地法律法规要求和合同约定保护个人信息主体的相关权利外，其第四条第一项也明确了个人信息主体享有知情权、决定权，有权限制或者拒绝他人对其个人信息进行处理，有权要求查阅、复制、更正、补充、删除其个人信息，有权要求对其个人信息处理规则进行解释说明，并可以选择向个人信息处理者或接收方提出行权请求，同时要求被请求方根据属地法律要求在合理期限内完成响应。

7. 基于合同相关方承诺简化备案手续

依据《实施指南》第八条，签署《大湾区标准合同》的个人信息处理者及接收方应在标准合同生效之日起 10 个工作日内按照属地向广东省互联网信息办公室或者香港特区政府资讯科技总监办公室进行标准合同备案，并提交如下材料：

（一）法定代表人身份证件影印件；

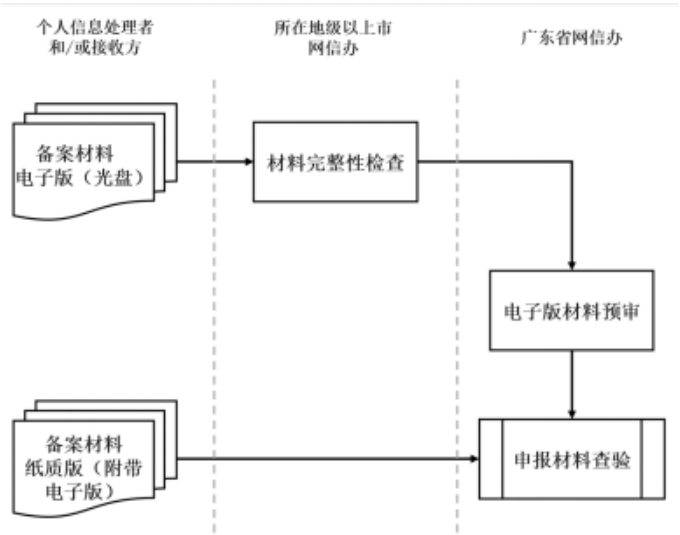
（二）承诺书（模板见附件 2）；

（三）标准合同。

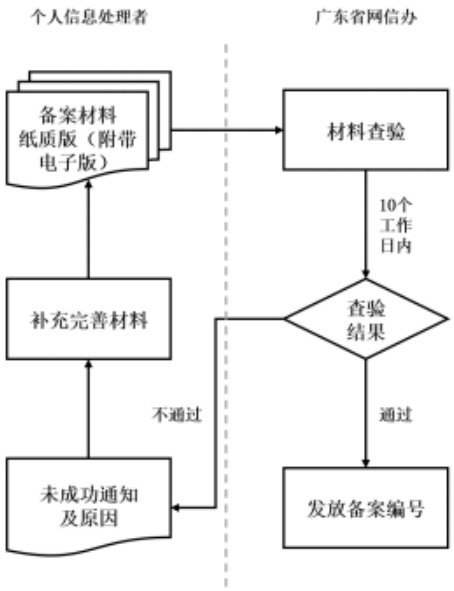
与《内地标准合同》的备案要求相比，**《大湾区标准合同》备案虽然免除了提交个人信息保护影响评估报告的义务**，但仍要求企业根据《实施指南》自主开展个人信息保护影响评估工作并基于评估结果作出合规承诺，因此对于签订《大湾区标准合同》的个人信息处理者来说，开展个人信息保护影响评估更多的是作为加强企业自身风险管理能力的有效工具。《大湾区标准合同》对于备案程序的简化一方面为大湾区组织及个人的个人信息跨境流动提供了便利，另一方面也没有完全放松对相关组织及个人开展个人信息保护影响评估工作的要求。

2024 年 1 月 4 日，广东省互联网信息办公室（下称“广东省网信办”）相应发布了《关于落实〈粤港澳大湾区（内地、香港）个人信息跨境流动标准合同实施指引〉的通知》（下称“《落实通知》”），适用于粤港澳大湾区内地个人信息处理者及接收方针对《大湾区标准合同》开展备案工作。

在备案材料提交方面，《落实通知》规定备案工作采取电子版预审与纸质版查验相结合的方式，并要求企业提供与纸质版材料一致的 PDF 扫描件和 WORD 版电子版材料。具体如下所示：



在材料查验、反馈及后续流程处理方面，《落实通知》规定《大湾区标准合同》备案流程包括材料提交、材料查验及反馈备案结果、补充或者重新备案等环节，具体如下所示：



此外，2023 年 12 月 14 日，香港特区发布了《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同备案指南（适用于香港特区）》及备案表格[40]，适用于《大湾区标准合同》下位于香港的合同方（不论作为《大湾区标准合同》下的个人信息处理者或接收方），为香港的组织或个人在备案的实践开展方面提供了清晰的指引和参考。

三、《实施指引》出台的意义

在全球数字经济蓬勃发展和中国“数据二十条”等政策的有力支撑下，尽管《跨境流动规定（征意稿）》的正式稿尚未发布，但促进数字经济发展和加速数据要素价值释放的相关工作已经处于高速推进中。本次《实施指引》与《跨境流动规定（征意稿）》第七条的规定遥相呼应，进一步完善了数据跨境传输的体系。

数据作为基础生产要素，是推动科技创新和经济高质量发展的重要动力，大湾区内各城市之间经济合作开展紧密，城市间的数据跨境流动需求与日俱增。在具有标志性意义的《合作备忘录》签署后，本次发布的《实施指引》及配套的《大湾区标准合同》将为大湾区中的内地地区与香港之间的跨境数据流动带来便利。通过简化流程和降低合规成本，上述文件有力地推动大湾区内跨境贸易和服务。香港特区政府资讯科技总监办公室提出，为有序开展《大湾区标准合同》的落地工作，其将会同广东省互联网信息办公室共同推出配套的便利措施，惠及大湾区内地城市和香港的各行各业。香港地区将组织进行《大湾区标准合同》便利措施的先行先试，在首阶段邀请银行业、征信业及医疗业企业参与。

根据香港特区政府资讯科技总监办公室的说明，企业参与《大湾区标准合同》的签署与备案完全基于自愿原则。若大湾区企业作为个人信息处理者及接收方采

[40] https://www.ogcio.gov.hk/sc/our_work/business/cross-boundary_data_flow/doc/gbascc02_fg_sc.pdf，最后访问于 2024 年 1 月 11 日。

用《大湾区标准合同》，须根据《实施指引》的要求及相关数据保护法律法规开展合规工作。

综上所述，大湾区企业在开展数据跨境流动活动的过程中应密切关注《跨境流动规定（征意稿）》的发布情况，并可以在满足《实施指引》规定的前提下考虑与区域内的相关方签署《大湾区标准合同》以增强出境活动的合规性和便利性，但同时企业也应当注意履行相关的个人信息保护合规义务以避免触碰监管红线。

附录：

附录一：标准合同涉及政策文件对比

比较维度/政策文件	内地 《个人信息出境标准合同办法》	粤港澳大湾区 《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同实施指引》	香港 2022 年《跨境资料转移指引：建议合约条文范本》
制定原则及背景	**第一条** 为了保护个人信息权益，规范个人信息出境活动，根据《中华人民共和国个人信息保护法》等法律法规，制定本办法。	**第一条** 为促进粤港澳大湾区个人信息跨境安全有序流动，推动粤港澳大湾区高质量发展，落实《中华人民共和国国家互联网信息办公室与香港特别行政区政府创新科技及工业局关于促进粤港澳大湾区数据跨境流动的合作备忘录》（以下简称备忘录），国家互联网信息办公室、香港特别行政区政府创新科技及工业局共同制定本实施指引。	**第一部 引言** 鉴于近年处理个人资料日趋数字化及商业全球化，本地企业（尤其中小企业）在拟定合适的合约条款以实行跨境资料转移并确保有关资料得到《个人资料（隐私）条例》（第 486 章）（《私隐条例》）下要求的相等保障时可能遇到实际困难。同时，随着信息及通讯科技（包括大资料、云端运算、资料分析）的发展及演进，国际间进行资料转移所面临的挑战和复杂性将会与日俱增。
适用范围	**第二条** 个人信息处理者通过与境外接收方订立个人信息出境标准合同（以下简称标准合同）的方式向中华人民共和国	**第二条** 《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同》（以下简称标准合同，见附件 1）为备忘录下有关促进粤港澳大湾区个人信息跨境流动的便利措施。粤港澳大湾区个人信息处理者及接收	**第一部 引言** 个人资料隐私专员公署（隐私公署）拟备了两套跨境资料转移建议合约条文模板（建议条文模板），分别供两种不同的跨境资料转移的情况应用，即（i）由一名

比较维度/政策文件	内地 《个人信息出境标准合同办法》	粤港澳大湾区 《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同实施指引》	香港 2022 年《跨境资料转移指引：建议合约条文范本》
	境外提供个人信息，适用本办法。	方可以按照本实施指引要求，通过订立标准合同的方式进行粤港澳大湾区内内地和香港之间的个人信息跨境流动。被相关部门、地区告知或者公开发布为重要数据的个人信息除外。 个人信息处理者及接收方应注册于（适用于组织）/位于（适用于个人）粤港澳大湾区内地部分，即广东省广州市、深圳市、珠海市、佛山市、惠州市、东莞市、中山市、江门市、肇庆市，或者香港特别行政区。	资料使用者转移予另一名资料使用者；及（ii）由一名资料使用者转移予一名资料处理者。建议条文模板列举一般的条款及细则，适用于由一香港机构转移个人资料至另一境外机构；或两个均属香港境外的机构之间的转移而有关转移由一名香港资料使用者所控制，借以让跨境资料转移的各方能考虑《隐私条例》就此的相关规管要求，包括附表 1 的保障资料原则（保障资料原则）。
通过订立标准合同的方式开展个人信息出境活动时应遵循的原则	**第三条** 通过订立标准合同的方式开展个人信息出境活动，应当坚持自主缔约与备案管理相结合、保护权益与防范风险相结合，保障个人信息跨境安全、自由流动。	**第三条** 通过订立标准合同的方式开展个人信息跨境提供的，应当坚持自主缔约与备案管理相结合、保护个人信息权益与防范风险相结合，保障个人信息跨境安全、自由流动。	**第一部 引言** 资料使用者在转移资料到香港境外的同时亦需要确保符合《隐私条例》的规定，因此资料使用者宜在跨境资料转移中引入建议条文模板。采用建议条文模板有助显示资料使用者已采取所有合理的预防措施及作出所有应作出的努

比较维度/政策文件	内地 《个人信息出境标准合同办法》	粤港澳大湾区 《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同实施指引》	香港 2022 年《跨境资料转移指引：建议合约条文范本》
			力，以确保有关资料不会在获转移资料一方所属的司法管辖区以违反《私隐条例》规定的方式（假如该些活动在香港发生）收集、持有、处理或使用（参见《私隐条例》第33（2）（f）条下的尽职努力的规定）。当有怀疑或声称违反《隐私条例》要求（包括保障资料原则）的情况出现时，该等因素将会全被纳入考虑当中。
通过订立标准合同方式开展个人信息出境活动的条件	**第四条** 个人信息处理者通过订立标准合同的方式向境外提供个人信息的，应当同时符合下列情形： （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；	**第四条** 按照本实施指引，通过订立标准合同跨境提供个人信息的，应当履行标准合同列明的义务和责任，包括满足以下条件： （一）个人信息处理者跨境提供个人信息前，应当按照个人信息处理者属地法律法规要求告知个人信息主体或者取得个人信息主体的同意；	**第一部 引言** 本指引的附表所载列的建议条文范本是供资料使用者（尤其中小企业）使用的建议合约条文，是一个在跨境转移个人资料方面确保相关个人资料获足够的保障的实用方法。 建议条文范本分为两套： A） 第一套适用于由一个资料使用者转移个人资料予另一个资料

比较维度/政策文件	内地 《个人信息出境标准合同办法》	粤港澳大湾区 《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同实施指引》	香港 2022 年《跨境资料转移指引：建议合约条文范本》
	（三）自上年 1 月 1 日起累计向境外提供个人信息不满 10 万人的； （四）自上年 1 月 1 日起累计向境外提供敏感个人信息不满 1 万人的。 法律、行政法规或者国家网信部门另有规定的，从其规定。 个人信息处理者不得采取数量拆分等手段，将依法应当通过出境安全评估的个人信息通过订立标准合同的方式向境外提供。	（二）不得向粤港澳大湾区以外的组织、个人提供。	使用者的情况，当中资料转移者和资料接收者均分别使用有关个人资料作其业务用途（例如，为它们各自的商业活动合作共享资料）（资料使用者转移资料予资料使用者的建议合约条文范本）。 B） 第二套适用于由资料使用者转移个人资料予资料处理者的情况，当中资料接收者只会为资料转移者指定的用途处理个人资料（例如，一间香港公司订立使用境外的云端服务的安排）（资料使用者转移资料予资料处理者的建议合约条文范本）。
标准合同订立前的个人信息保护影响评估内容	**第五条** 个人信息处理者向境外提供个人信息前，应当开展个人信息保护影响评估，重点评估以下内容：	**第五条** 个人信息处理者按照本实施指引，通过订立标准合同跨境提供个人信息前，应当开展个人信息保护影响评估，重点评估以下内容：	/

比较维度/政策文件	内地 《个人信息出境标准合同办法》	粤港澳大湾区 《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同实施指引》	香港 2022 年《跨境资料转移指引：建议合约条文范本》
	（一）个人信息处理者和境外接收方处理个人信息的目的、范围、方式等的合法性、正当性、必要性； （二）出境个人信息的规模、范围、种类、敏感程度，个人信息出境可能对个人信息权益带来的风险； （三）境外接收方承诺承担的义务，以及履行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； （四）个人信息出境后遭到篡改、破坏、泄露、丢失、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）境外接收方所在国家或者地区的个人信息保护政策和法规对标准合同履行的影响；	（一）个人信息处理者和接收方处理个人信息的目的、方式等的合法性、正当性、必要性； （二）对个人信息主体权益的影响及安全风险； （三）接收方承诺承担的义务，以及履行义务的管理和技术措施、能力等能否保障跨境提供的个人信息安全。	

比较维度/政策文件	内地 《个人信息出境标准合同办法》	粤港澳大湾区 《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同实施指引》	香港 2022 年《跨境资料转移指引：建议合约条文范本》
	（六）其他可能影响个人信息出境安全的事项。		
标准合同的订立	**第六条** 标准合同应当严格按照本办法附件订立。国家网信部门可以根据实际情况对附件进行调整。 个人信息处理者可以与境外接收方约定其他条款，但不得与标准合同相冲突。 标准合同生效后方可开展个人信息出境活动。	**第六条** 标准合同应当严格按照本实施指引附件订立，合同生效后方可开展个人信息跨境提供。 个人信息处理者可以与接收方约定其他条款，但不得与标准合同相冲突。	**第二部 采用建议合约条文范本** 私隐公署并不预期建议条文范本是转移及接收资料双方所采纳的协议之全部。双方在转移个人资料前，可能在合约安排上需要顾及商业上的考虑。此外，资料使用者通常宜就资料接收者如何处理转移给它们的个人资料向资料接收者寻求额外及更具体的保证。这些额外保证的例子将会在下文“额外合约措施”中阐述。 建议条文范本旨在列举一般的条款及细则，适用于（i）由一香港机构转移个人资料至另一境外机构，或（ii）两个均属香港境外的机构之间的转移而有关转移由一名香港资料使用者所控制，借以考虑《私隐条

比较维度/政策文件	内地 《个人信息出境标准合同办法》	粤港澳大湾区 《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同实施指引》	香港 2022 年《跨境资料转移指引：建议合约条文范本》
			例》的相关规管要求，尤其附表 1 的保障资料原则。建议条文范本可作为实用的基础，从而便利由香港转移个人资料至境外地方，使机构能订立清晰的协议以订明转移甚麼个人资料、转移资料的目的，以及双方在符合《私隐条例》规定的前提下于不同范畴的具体责任分配，例如资料保安、管理查阅及改正资料的权利，以及资料接收者向其他司法管辖区或其他接收者继续转移有关资料的范围。 机构（尤其中小企业）可在自行制定转移资料协议时采纳建议条文范本，或把这些条文纳入更广泛的服务协议中。机构可自由使用其他在实质上符合《私隐条例》规定的字词。建议条文范本是具独立性 的条文，只要建议条文范本继续达到其

比较维度/政策文件	内地 《个人信息出境标准合同办法》	粤港澳大湾区 《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同实施指引》	香港 2022 年《跨境资料转移指引：建议合约条文范本》
			实质效果（提供予个人资料的保障与《私隐条例》所规定的相同，尤如有关个人资料没有被转移至香港境外），也可被纳入资料转移者与资料接收者之间较一般性的商业协议中。本指引内的建议条文范本不应被视为符合欧洲联盟的《通用数据保护条例》之规定及/或由欧盟委员会颁佈的标准合约条款之替代条文。资料使用者应确保在转移个人资料至香港以外的其他司法管辖区时，相关个人资料获足够的保障。
标准合同的备案要求	**第七条** 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。备案应当提交以下材料： （一）标准合同； （二）个人信息保护影响评估报告。	**第八条** 个人信息处理者及接收方应在标准合同生效之日起 10 个工作日内按照属地向广东省互联网信息办公室或者香港特别行政区政府政府资讯科技总监办公室进行标准合同备案，提交如下材料： （一）法定代表人身份证件影印件； （二）承诺书（模板见附件 2）；	/

比较维度/政策文件	内地 《个人信息出境标准合同办法》	粤港澳大湾区 《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同实施指引》	香港 2022 年《跨境资料转移指引：建议合约条文范本》
	个人信息处理者应当对所备案材料的真实性负责。	（三）标准合同。 个人信息处理者及接收方应当对所备案材料的真实性负责。	
标准合同的订立及备案材料	**第八条** 在标准合同有效期内出现下列情形之一的，个人信息处理者应当重新开展个人信息保护影响评估，补充或者重新订立标准合同，并履行相应备案手续： （一）向境外提供个人信息的目的、范围、种类、敏感程度、方式、保存地点或者境外接收方处理个人信息的用途、方式发生变化，或者延长个人信息境外保存期限的； （二）境外接收方所在国家或者地区的个人信息保护政策和法规发生变化等可能影响个人信息权益的；	**第七条** 跨境提供个人信息的目的、范围、种类、方式，或者接收方处理个人信息的用途、方式发生变化，延长保存期限，以及发生影响或者可能影响个人信息权益其他情况的，个人信息处理者应当重新开展个人信息保护影响评估，补充或者重新订立标准合同，并履行相应备案手续。	/

比较维度/政策文件	内地 《个人信息出境标准合同办法》	粤港澳大湾区 《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同实施指引》	香港 2022 年《跨境资料转移指引：建议合约条文范本》
	（三）可能影响个人信息权益的其他情形。		
监管部门的履职要求	**第九条** 网信部门及其工作人员对在履行职责中知悉的个人隐私、个人信息、商业秘密、保密商务信息等应当依法予以保密，不得泄露或者非法向他人提供、非法使用。	**第十三条** 有关部门及其工作人员对在履行职责中知悉的个人隐私、个人信息、商业秘密、保密商务信息等应当依法予以保密，不得泄露或者非法向他人提供、非法使用。	/
违规行为的处置机制	**第十条** 任何组织和个人发现个人信息处理者违反本办法向境外提供个人信息的，可以向省级以上网信部门举报。	**第十条** 任何组织和个人发现个人信息处理者或接收方按照本实施指引进行粤港澳大湾区内的个人信息跨境流动，但不履行本实施指引及标准合同要求的义务和责任的，可以向国家互联网信息办公室、广东省互联网信息办公室或者香港特别行政区政府创新科技及工业局、政府资讯科技总监办公室、香港个人资料私隐专员公署投诉、举报。 收到投诉、举报的部门发现个人信息跨境活动存在较大安全风险或者发生个人信息	**第二部 采用建议合约条文范本** 如资料使用者不能证明它已实施良好的资料保障措施，例如包括采纳建议条文范本，它们可能要面对潜在的法律责任及声誉受损。

比较维度/政策文件	内地 《个人信息出境标准合同办法》	粤港澳大湾区 《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同实施指引》	香港 2022 年《跨境资料转移指引：建议合约条文范本》
		安全事件的，可以要求个人信息处理者或者接收方整改；需要交由其他执法部门处置的，交由相关部门依法处置。 **第十一条** 个人信息处理者或接收方在处理个人信息时发生个人信息泄露等安全事件的，应立即采取补救措施，按照属地通知国家互联网信息办公室、广东省互联网信息办公室，或者香港特别行政区政府创新科技及工业局、政府资讯科技总监办公室、香港个人资料私隐专员公署。	
监督管理及执法	**第十一条** 省级以上网信部门发现个人信息出境活动存在较大风险或者发生个人信息安全事件的，可以依法对个人信息处理者进行约谈。个人信息处理者应当按照要求整改，消除隐患。	**第九条** 个人信息处理者及接收方接受属地监管机构的监督管理，包括但不限于： （一）根据标准合同第二条第七项及第十项，个人信息处理者答复监管机构的询问及对合同的义务和责任的履行承担举证责任； （二）根据标准合同第三条第十二项，接收方应接受监管机构的监督管理，包括服	/

比较维度/政策文件	内地 《个人信息出境标准合同办法》	粤港澳大湾区 《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同实施指引》	香港 2022 年《跨境资料转移指引：建议合约条文范本》
	第十二条 违反本办法规定的，依据《中华人民共和国个人信息保护法》等法律法规处理；构成犯罪的，依法追究刑事责任。	从监管机构作出的决定以及提供已采取必要行动的证明等； （三）根据标准合同第六条第二项，个人信息处理者解除标准合同时，通知监管机构。 **第十二条** 以上规定并不影响内地履行个人信息保护职责的部门和香港个人资料私隐专员公署在职责范围内依法加强个人信息保护和监督管理工作，包括处理与个人信息保护有关的投诉、举报，调查、处理违法个人信息处理活动等。	
生效及实施	**第十三条** 本办法自 2023 年 6 月 1 日起施行。本办法施行前已经开展的个人信息出境活动，不符合本办法规定的，应当自本办法施行之日起 6 个月内完成整改。	**第十四条** 国家互联网信息办公室和香港特别行政区政府创新科技及工业局可以根据实际情况，经协商一致后对本实施指引及附件进行修订。 **第十五条** 本实施指引自发布之日起生效。	**第一部 引言** 建议条文范本是可自由组合的独立性条文，也可被纳入资料转移者与资料接收者之间的一般性商业协议中。本指引就建议条文范本的实际效果提供详细说明，及阐述如何借遵从建议条文范本以提供《私隐条例》要求的足够保障

比较维度/政策文件	内地 《个人信息出境标准合同办法》	粤港澳大湾区 《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同实施指引》	香港 2022 年《跨境资料转移指引：建议合约条文范本》
			予个人资料，尤如相关个人资料没有被转移至香港境外。 即使就跨境资料转移施加规限的《私隐条例》第 33 条尚未生效，本指引建议资料使用者（尤其中小企业）采取最佳行事方式作为其资料管治责任的一部份，以保障及尊重资料当事人的个人资料。

附录二：标准合同的内容对比

比较维度/ 政策文件	《个人信息出境标准合同》	《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同》	香港-《资料使用者转移资料予资料使用者的建议合约条文模板》	香港《-资料使用者转移资料予资料处理者的建议合约条文模板》
订立基本信息	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，明确个人信息处理者和境外接收方个人信息保护的权利和义务，经双方协商一致，订立本合同。 个人信息处理者： 地址： 联系方式： 联系人：　　职务： 境外接收方： 地址： 联系方式： 联系人：　　职务：	为促进粤港澳大湾区个人信息跨境安全有序流动，明确个人信息处理者和接收方个人信息保护的权利、义务和责任，经双方协商一致，订立本合同。 个人信息处理者: 地址: 联系方式: 联系人：职务: 接收方: 地址: 联系方式: 联系人：职务:	/	/

比较维度/ 政策文件	《个人信息出境标准合同》	《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同》	香港-《资料使用者转移资料予资料使用者的建议合约条文模板》	香港《-资料使用者转移资料予资料处理者的建议合约条文模板》
	个人信息处理者与境外接收方依据本合同约定开展个人信息出境活动，与此活动相关的商业行为，双方【已】/【约定】于 年 月 日订立（商业合同，如有）。 本合同正文根据《个人信息出境标准合同办法》的要求拟定，在不与本合同正文内容相冲突的前提下，双方如有其他约定可在附录二中详述，附录构成本合同的组成部分。	（注:个人信息处理者及接收方应注册于（适用于组织）/位于（适用于个人）粤港澳大湾区内地部分，即广东省广州市、深圳市、珠海市、佛山市、惠州市、东莞市、中山市、江门市、肇庆市，或者香港特别行政区） 个人信息处理者与接收方依据本合同约定开展个人信息跨境活动，与此活动相关的商业行为，双方【已】/【约定】于 年 月 日订立（商业合同，如有）。 本合同正文根据《中华人民共和国国家互联网信息办公室与香港特别行政区政府创新科技		

比较维度/ 政策文件	《个人信息出境标准合同》	《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同》	香港-《资料使用者转移资料予资料使用者的建议合约条文模板》	香港《-资料使用者转移资料予资料处理者的建议合约条文模板》
		及工业局关于促进粤港澳大湾区数据跨境流动的合作备忘录》而拟定，在不与本合同正文内容相冲突的前提下，双方如有其他约定可在附录二中详述，附录构成本合同的组成部分。		
定义及释义	**第一条 定义** 在本合同中，除上下文另有规定外： （一）“个人信息处理者”是指在个人信息处理活动中自主决定处理目的、处理方式的，向中华人民共和国境外提供个人信息的组织、个人。 （二）“境外接收方”是指在中华人民共和国境外自个人信息	**第一条 定义** 在本合同中，除上下文另有规定外: （一）“个人信息处理者”，就内地而言，是指在个人信息处理活动中自主决定处理目的、处理方式的组织、个人;就香港特别行政区而言，亦涵盖“资料使用者”，即就个人资料而言，指独自或联同其他人或与其他	**1.定义** 1.1 就这些条文，包括资料转移一览表（统称「条文」）而言： 「继续转移的接收者」的意思载于第4.9 条； 「《隐私条例》」指《个人资料（隐私）条例》（第	**1.定义** 1.1就这些条文，包括资料转移一览表（统称「条文」）而言： 「《隐私条例》」指《个人资料（隐私）条例》（第486章），或会不时修订；

比较维度/政策文件	《个人信息出境标准合同》	《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同》	香港-《资料使用者转移资料予资料使用者的建议合约条文模板》	香港《-资料使用者转移资料予资料处理者的建议合约条文模板》
	处理者处接收个人信息的组织、个人。 （三）个人信息处理者或者境外接收方单称“一方”，合称“双方”。 （四）“个人信息主体”是指个人信息所识别或者关联的自然人。 （五）“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。 （六）“敏感个人信息”是指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、	人共同控制该资料的收集、持有、处理或使用的人。 本合同所称个人信息处理者为个人信息跨境提供方。 （二）“接收方”是指自个人信息处理者处跨境接收个人信息的组织、个人。 （三）个人信息处理者或者接收方单称“一方”，合称“双方”。 （四）粤港澳大湾区内地个人信息处理者处理的个人信息，按照《中华人民共和国个人信息保护法》确定;香港特别行政区内个人信息处理者处理的个人信息，按照香港特别行政区《个人资料（私隐）条例》的“个人资料”确定。	486 章），或会不时修订； 「准许司法管辖区」指资料转移一览表所列的地方或转移的个人资料不时根据这些条文而被使用或处理或持有的任何其他地方； 「转移的个人资料」指资料转移一览表所列的个人资料种类或类别； 「转移目的」指资料转移一览表所列的使用转移的个人	「准许司法管辖区」指资料转移一览表所列的地方或转移的个人资料不时根据这些条文而被处理或持有的任何其他地方； 「转移的个人资料」指资料转移一览表所列的个人资料种类或类别； 「转移目的」指资料转移一览表所列的处理转移的个人资料的目的或直接有关的目的；

比较维度/政策文件	《个人信息出境标准合同》	《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同》	香港-《资料使用者转移资料予资料使用者的建议合约条文模板》	香港《-资料使用者转移资料予资料处理者的建议合约条文模板》
	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。 （七）“监管机构”是指中华人民共和国省级以上网信部门。 （八）“相关法律法规”是指《中华人民共和国网络安全法》《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》《中华人民共和国民法典》《中华人民共和国民事诉讼法》《个人信息出境标准合同办法》等中华人民共和国法律法规。 （九）本合同其他未定义术语的含义与相关法律法规规定的含义一致。	（五）“个人信息主体”，就内地而言，是指个人信息所识别或者关联的自然人;就香港特别行政区而言，亦涵盖“资料当事人”，即就个人资料而言，指属该资料的当事人的个人。 （六）“监管机构”，就内地而言，是指国家互联网信息办公室及广东省互联网信息办公室;就香港特别行政区而言，是指香港特别行政区政府创新科技及工业局、政府资讯科技总监办公室及香港个人资 料私隐专员公署。 （七）“相关法律法规”，就内地而言，是指《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和	资料的目的或直接有关的目的; 「建议资料处理条文模板」指专员不时就资料使用者跨境转移个人资料予资料处理者而发出的建议合约条文模板；及 「保留时期」指资料转移一览表指明的保留时期。 1.2「专员」、「资料处理者」、「资料当事人」、「资料使用者」、「直接促销」、「个人资料」、「处理」	「保留时期」指资料转移一览表指明的保留时期；及 「分判处理者」的意思载于第3.8条。 1.2「个人资料」及「处理」的意思与《隐私条例》赋予这些词语的意思相同。 **2.释义** 就条文的理解和解释应按照《隐私条例》的条文而作出。有关条文的解释不应存有与《隐私条例》的相关规定抵触的可能性。

比较维度/ 政策文件	《个人信息出境标准合同》	《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同》	香港-《资料使用者转移资料予资料使用者的建议合约条文模板》	香港《-资料使用者转移资料予资料处理者的建议合约条文模板》
		国个人信息保护法》等法律法规;就香港特别行政区而言，是指《个人资料（私隐）条例》等法律法规。	及「使用」的意思与《隐私条例》赋予这些词语的意思相同。 **2.释义** 就条文的理解和解释应按照《隐私条例》的条文而作出。有关条文的解释不应存有与《私隐条例》的相关规定抵触的可能性。	
个人信息处理者的义务	**第二条 个人信息处理者的义务** 个人信息处理者应当履行下列义务： （一）按照相关法律法规规定处理个人信息，向境外提供的	**第二条 个人信息处理者的义务和责任** 个人信息处理者应当履行下列义务和责任: （一）按照属地相关法律法规及本合同要求处理个人信息，	**3.资料转移者的责任** 资料转移者向资料接收者保证及承诺会根据《隐私条例》为转移目的把转移的个人资料转移予准许司法	/

比较维度/政策文件	《个人信息出境标准合同》	《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同》	香港-《资料使用者转移资料予资料使用者的建议合约条文模板》	香港《-资料使用者转移资料予资料处理者的建议合约条文模板》
	个人信息仅限于实现处理目的所需的最小范围。 （二）向个人信息主体告知境外接收方的名称或者姓名、联系方式、附录一“个人信息出境说明”中处理目的、处理方式、个人信息的种类、保存期限，以及行使个人信息主体权利的方式和程序等事项。向境外提供敏感个人信息的，还应当向个人信息主体告知提供敏感个人信息的必要性以及对个人权益的影响。但是法律、行政法规规定不需要告知的除外。 （三）基于个人同意向境外提供个人信息的，应当取得个人信息主体的单独同意。涉及不	向接收方提供的个人信息仅限于实现处理目的所需的最小范围。 （二）向个人信息主体告知接收方的名称或者姓名、联系方式，附录一“个人信息跨境提供说明”中处理目的、处理方式、个人信息的种类、保存期限、个人信息向同辖区第三方提供的情况，以及行使个人信息主体权利的方式和程序等事项。属地相关法律法规要求不需要告知的，从其规定。 （三）向接收方跨境提供个人信息前，应当按照属地法律法规要求取得个人信息主体同意。	管辖区的资料接收者，唯资料接收者须履行它在这些条文下的责任。	

比较维度/政策文件	《个人信息出境标准合同》	《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同》	香港-《资料使用者转移资料予资料使用者的建议合约条文模板》	香港《-资料使用者转移资料予资料处理者的建议合约条文模板》
	满十四周岁未成年人个人信息的，应当取得未成年人的父母或者其他监护人的单独同意。法律、行政法规规定应当取得书面同意的，应当取得书面同意。 （四）向个人信息主体告知其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，如个人信息主体未在30日内明确拒绝，则可以依据本合同享有第三方受益人的权利。 （五）尽合理地努力确保境外接收方采取如下技术和管理措施（综合考虑个人信息处理目的、个人信息的种类、规模、范围及敏感程度、传输的数量和频率、个人信息传输及境外	（四）向个人信息主体告知其与接收方通过本合同约定个人信息主体为第三方受益人，如个人信息主体未在30日内明确拒绝，则可以依据本合同享有第三方受益人的权利。 （五）尽合理的努力确保接收方采取如下技术和管理措施（综合考虑个人信息处理目的、个人信息的种类、规模、范围、传输的数量 和频率、个人信息传输及接收方的保存期限等可能带来的个人信息安全风险），以履行本合同约定的义务和责任。 （如加密、匿名化、去标识化、访问控制等技术和管理措施）		

比较维度/政策文件	《个人信息出境标准合同》	《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同》	香港-《资料使用者转移资料予资料使用者的建议合约条文模板》	香港《-资料使用者转移资料予资料处理者的建议合约条文模板》
	接收方的保存期限等可能带来的个人信息安全风险），以履行本合同约定的义务： （如加密、匿名化、去标识化、访问控制等技术和管理措施） （六）根据境外接收方的要求向境外接收方提供相关法律规定和技术标准的副本。 （七）答复监管机构关于境外接收方的个人信息处理活动的询问。 （八）按照相关法律法规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。重点评估以下内容： 1.个人信息处理者和境外接收方处理个人信息的目的、范围、	（六）根据接收方的要求向接收方提供属地相关法律法规规定和技术标准的副本。 （七）答复属地监管机构关于接收方的个人信息处理活动的询问。 （八）对拟向接收方提供个人信息的活动开展个人信息保护影响评估。重点评估以下内容: 1.个人信息处理者和接收方处理个人信息的目的、方式等的合法性、正当性、必要性; 2.对个人信息主体权益的影响及安全风险; 3.接收方承诺承担的义务，以及履行义务的管理和技术措施、能力等能否保障跨境提供的个人信息安全。		

比较维度/政策文件	《个人信息出境标准合同》	《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同》	香港-《资料使用者转移资料予资料使用者的建议合约条文模板》	香港《-资料使用者转移资料予资料处理者的建议合约条文模板》
	方式等的合法性、正当性、必要性。 2.出境个人信息的规模、范围、种类、敏感程度，个人信息出境可能对个人信息权益带来的风险。 3.境外接收方承诺承担的义务，以及履行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。 4.个人信息出境后遭到篡改、破坏、泄露、丢失、非法利用等的风险，个人信息权益维护的渠道是否通畅等。 5.按照本合同第四条评估当地个人信息保护政策和法规对合同履行的影响。	保存个人信息保护影响评估报告至少 3 年。 （九）根据个人信息主体的要求向个人信息主体提供本合同的副本。如涉及商业秘密或者保密商务信息，在不影响个人信息主体理解的前提下，可对本合同副本相关内容进行适当处理。 （十）对本合同义务和责任的履行承担举证责任。 （十一）根据属地相关法律法规及本合同要求，向属地监管机构 提供本合同第三条第十项所述的信息，包括所有合规审计结果。		

比较维度/ 政策文件	《个人信息出境标准合同》	《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同》	香港-《资料使用者转移资料予资料使用者的建议合约条文模板》	香港《-资料使用者转移资料予资料处理者的建议合约条文模板》
	6.其他可能影响个人信息出境安全的事项。保存个人信息保护影响评估报告至少 3 年。 （九）根据个人信息主体的要求向个人信息主体提供本合同的副本。如涉及商业秘密或者保密商务信息，在不影响个人信息主体理解的前提下，可对本合同副本相关内容进行适当处理。 （十）对本合同义务的履行承担举证责任。 （十一）根据相关法律法规要求，向监管机构提供本合同第三条第十一项所述的信息，包括所有合规审计结果。			
境外接收方的义务	**第三条 境外接收方的义务**	**第三条 接收方的义务和责任**	**4.资料接收者的责任**	**3.资料接收者的责任**

比较维度/政策文件	《个人信息出境标准合同》	《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同》	香港-《资料使用者转移资料予资料使用者的建议合约条文模板》	香港《-资料使用者转移资料予资料处理者的建议合约条文模板》
	境外接收方应当履行下列义务： （一）按照附录一“个人信息出境说明”所列约定处理个人信息。如超出约定的处理目的、处理方式和处理的个人信息种类，基于个人同意处理个人信息的，应当事先取得个人信息主体的单独同意；涉及不满十四周岁未成年人个人信息的，应当取得未成年人的父母或者其他监护人的单独同意。 （二）受个人信息处理者委托处理个人信息的，应当按照与个人信息处理者的约定处理个人信息，不得超出与个人信息处理者约定的处理目的、处理方式等处理个人信息。	接收方应当履行下列义务和责任: （一）按照附录一“个人信息跨境提供说明”所列约定处理个人信息。如超出约定的处理目的、处理方式和处理的个人信息种类，应当事先告知个人信息处理者，补充或者重新订立标准合同，并履行相应备案手续。个人信息处理者属地相关法律法规要求不需要告知的，从其规定。 （二）根据个人信息主体的要求向个人信息主体提供本合同的副本。如涉及商业秘密或者保密商务信息，在不影响个人信息主体理解的前提下，可对	资料接收者向资料转移者保证及承诺： 4.1除非《隐私条例》另有准许，否则只会为转移目的使用转移的个人资料； 4.2确保就转移目的而言，转移的个人资料属足够但不超乎适度； 4.3采用资料转移一览表所列的保安措施使用、持有及传送转移的个人资料； 4.4不会保留转移的个人资料超过达致转移目的所需的时间，及无论如何，不会超	资料接收者向资料转移者保证及承诺： 3.1只会为转移目的处理转移的个人资料； 3.2确保就转移目的而言，转移的个人资料属足够但不超乎适度； 3.3采用资料转移一览表所列的保安措施处理、持有及传送转移的个人资料； 3.4不会保留转移的个人资料超过进行资料转移者指示的处理所需的时间，及无论

比较维度/政策文件	《个人信息出境标准合同》	《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同》	香港-《资料使用者转移资料予资料使用者的建议合约条文模板》	香港《-资料使用者转移资料予资料处理者的建议合约条文模板》
	（三）根据个人信息主体的要求向个人信息主体提供本合同的副本。如涉及商业秘密或者保密商务信息，在不影响个人信息主体理解的前提下，可对本合同副本相关内容进行适当处理。 （四）采取对个人权益影响最小的方式处理个人信息。 （五）个人信息的保存期限为实现处理目的所必要的最短时间，保存期限届满的，应当删除个人信息（包括所有备份）。受个人信息处理者委托处理个人信息，委托合同未生效、无效、被撤销或者终止的，应当将个人信息返还个人信息处理者或者予以删除，并向个人信	本合同副本相关内容进行适当处理。 （三）采取对个人权益影响最小的方式处理个人信息。 （四）个人信息的保存期限为实现处理目的所必要的最短时间，保存期限届满的，应当删除个人信息（包括所有备份）。受个人信息处理者委托处理个人信息，委托合同未生效、无效、被撤销、终止或者按个人信息处理者要求，应当将个人信息予以删除，并向个人信息处理者提供书面说明。删除个人信息从技术上难以实现的，应当停止除存储和采取必要的安全保护措施之外的处理。	过任何适用的保留时期； 4.5采取所有切实可行的步骤，当转移的个人资料不再需要用于达致转移目的，或无论如何，当任何适用的保留时期届满后，即删除有关资料； 4.6采取所有切实可行的步骤，以确保在顾及转移目的下，转移的个人资料是准确的； 4.7采取所有切实可行的步骤，以确保任何不准确的转移的个	如何，不会超过任何适用的保留时期； 3.5采取所有切实可行的步骤，在下述情况删除转移的个人资料：（i）不再需要根据第3.4条保留；或（ii）按资料转移者的指示； 3.6采取所有切实可行的步骤，以确保在顾及转移目的下，转移的个人资料是准确的； 3.7采取所有切实可行的步骤，以确保任何不准确的转移的个人资料（i）在更正

比较维度/政策文件	《个人信息出境标准合同》	《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同》	香港-《资料使用者转移资料予资料使用者的建议合约条文模板》	香港《-资料使用者转移资料予资料处理者的建议合约条文模板》
	息处理者提供书面说明。删除个人信息从技术上难以实现的，应当停止除存储和采取必要的安全保护措施之外的处理。 （六）按下列方式保障个人信息处理安全： 1.采取包括但不限于本合同第二条第五项的技术和管理措施，并定期进行检查，确保个人信息安全。 2.确保授权处理个人信息的人员履行保密义务，并建立最小授权的访问控制权限。 （七）如处理的个人信息发生或者可能发生篡改、破坏、泄露、丢失、非法利用、未经授	（五）按下列方式保障个人信息处理安全: 1.采取包括但不限于本合同第二条第五项的技术和管理措施，并定期进行检查，确保个人信息安全。 2.确保授权处理个人信息的人员履行保密义务和责任，并建立最小授权的访问控制权限。 （六）如处理的个人信息发生或者可能发生篡改、破坏、泄露、丢失、非法利用、未经授权提供或者访问、查阅，应当开展下列工作: 1.及时采取适当补救措施，减轻对个人信息主体造成的不利影响。	人资料（i）在更正前不会被使用或（ii）会被删除； 4.8采取所有切实可行的步骤，以确保资料当事人能查阅其有关转移的个人资料的政策及做法； 4.9不会把转移的个人资料转移予任何人或容许任何人查阅有关资料，例外情况：（i）资料转移一览表准许；或（ii）每个情况均有资料转移者的事前书面同意（在任何一种情况	前不会被处理或（ii）会被删除； 3.8不会把转移的个人资料转移予任何人或容许任何人查阅有关资料，例外情况：（i）资料转移一览表准许；或（ii）每个情况均有资料转移者的事前书面同意（在任何一种情况下，即「分判处理者」）； 3.9确保每个分判处理者会与资料接收者签订具约束力的书面合约，该合约所施加的资料保障责任与这

比较维度/政策文件	《个人信息出境标准合同》	《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同》	香港-《资料使用者转移资料予资料使用者的建议合约条文模板》	香港《-资料使用者转移资料予资料处理者的建议合约条文模板》
	权提供或者访问，应当开展下列工作： 1.及时采取适当补救措施，减轻对个人信息主体造成的不利影响。 2.立即通知个人信息处理者，并根据相关法律法规要求报告监管机构。通知应当包含下列事项： （1）发生或者可能发生篡改、破坏、泄露、丢失、非法利用、未经授权提供或者访问的个人信息种类、原因和可能造成的危害。 （2）已采取的补救措施。 （3）个人信息主体可以采取的减轻危害的措施。	2.立即通知个人信息处理者，并报告属地监管机构。通知应当包含下列事项: （1）发生或者可能发生篡改、破坏、泄露、丢失、非法利用、未经授权提供或者访问、查阅的个人信息种类、原因和可能造成的危害。 （2）已采取的补救措施。 （3）个人信息主体可以采取的减轻危害的措施。 （4）负责处理相关情况的负责人或者负责团队的联系方式。 3.相关法律法规要求通知个人信息主体的，通知的内容包含本项第 2 目的事项。 4.记录并留存所有与发生或者可能发生篡改、破坏、泄露、	下，即「继续转移的接收者」）； 4.10确保每个继续转移的接收者作为： （a）控制使用或处理转移的个人资料的资料使用者（不论是单独或联同其他人）会与资料接收者签订具约束力的书面合约，该合约所施加的资料保障责任与这些条文所载的相同或大体上相似；及／或 （b）代资料接收者（非为继续转移的接收者的个人目的）处理转移的个人资料的	些条文所载的相同或大体上相似；及 3.10如没有资料转移者事前的书面同意，除了准许司法管辖区外，不会（i）在香港境外处理或持有转移的个人资料；或（ii）容许任何分判处理者在香港境外处理或持有转移的个人资料。

比较维度/政策文件	《个人信息出境标准合同》	《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同》	香港-《资料使用者转移资料予资料使用者的建议合约条文模板》	香港《-资料使用者转移资料予资料处理者的建议合约条文模板》
	（4）负责处理相关情况的负责人或者负责团队的联系方式。 3.相关法律法规要求通知个人信息主体的，通知的内容包含本项第2目的事项。受个人信息处理者委托处理个人信息的，由个人信息处理者通知个人信息主体。 4.记录并留存所有与发生或者可能发生篡改、破坏、泄露、丢失、非法利用、未经授权提供或者访问有关的情况，包括采取的所有补救措施。 （八）同时符合下列条件的，方可向中华人民共和国境外的第三方提供个人信息： 1.确有业务需要。	丢失、非法利用、未经授权提供或者访问、查阅有关的情况，包括采取的所有补救措施。 （七）不得向粤港澳大湾区以外的组织、个人提供据此合同接收的个人信息。 （八）同时符合下列条件的，方可向粤港澳大湾区内地或香港特别行政区同辖区内的第三方提供个人信息: 1.确有业务需要。 2.已告知个人信息主体该第三方的名称或者姓名、联系方式、处理目的、处理方式、个人信息种类、保存期限以及行使个人信息主体权利的方式和程序等事项。个人信息处理者	资料处理者会与资料接收者签订具约束力的书面合约，该合约所施加的资料保障责任与建议资料处理条文范本所载的相同或大体上相似；及 4.11在各情况，除了准许司法管辖区外，不会（i）在香港境外使用或持有转移的个人资料；或（ii）容许任何继续转移的接收者在香港境外使用、处理或持有转移的个人资料，除非［它已取得资料转移者事前的书面同意］	

比较维度/政策文件	《个人信息出境标准合同》	《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同》	香港-《资料使用者转移资料予资料使用者的建议合约条文模板》	香港《-资料使用者转移资料予资料处理者的建议合约条文模板》
	2.已告知个人信息主体该第三方的名称或者姓名、联系方式、处理目的、处理方式、个人信息种类、保存期限以及行使个人信息主体权利的方式和程序等事项。向第三方提供敏感个人信息的，还应当向个人信息主体告知提供敏感个人信息的必要性以及对个人权益的影响。但是法律、行政法规规定不需要告知的除外。 3.基于个人同意处理个人信息的，应当取得个人信息主体的单独同意。涉及不满十四周岁未成年人个人信息的，应当取得未成年人的父母或者其他监护人的单独同意。法律、行政	属地相关法律法规要求不 需要告知的，从其规定。 3.基于个人同意处理个人信息的，应当按照个人信息处理者属地法律法规要求取得个人信息主体同意。 4.按照附录一“个人信息跨境提供说明”所列约定向同辖区内的第三方提供个人信息。 （九）受个人信息处理者委托处理个人信息，转委托第三方处理的，应当事先征得个人信息处理者同意，要求该第三方不得超出本合同附录一“个人信息跨境提供说明”中约定的处理目的、处理方式等处理个人信息，并对该第三方的个人信息处理活动进行监督。	或［它已通知资料转移者及： （a）已采取所有合理的预防措施及作出所有应作出的努力，以确保转移的个人资料在该地方不会被人以违反《隐私条例》的方式收集、持有、处理或使用； （b）每个与转移的个人资料有关的资料当事人已书面同意在该地方使用或处理或持有转移的个人资料（有关同意并无被撤回）；	

比较维度/政策文件	《个人信息出境标准合同》	《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同》	香港-《资料使用者转移资料予资料使用者的建议合约条文模板》	香港《-资料使用者转移资料予资料处理者的建议合约条文模板》
	法规规定应当取得书面同意的，应当取得书面同意。 4.与第三方达成书面协议，确保第三方的个人信息处理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，并承担因向中华人民共和国境外的第三方提供个人信息而侵害个人信息主体享有权利的法律责任。 5.根据个人信息主体的要求向个人信息主体提供该书面协议的副本。如涉及商业秘密或者保密商务信息，在不影响个人信息主体理解的前提下，可对该书面协议相关内容进行适当处理。	（十）承诺向个人信息处理者提供已遵守本合同义务和责任所需的必要信息，允许个人信息处理者对本合同涵盖的处理活动进行合规审计，并为个人信息处理者开展合规审计提供便利。 （十一）对开展的个人信息处理活动进行客观记录，保存记录至少 3 年。 （十二）同意在本合同实施的相关监督程序中接受属地监管机构的监督管理，包括但不限于答复属地监管机构询问、配合属地监管机构检查、服从属地监管机构采取的措施或者作出的决定、提供已采取必要行动的书面证明等。	（c）资料接收者有合理理由相信在使用或处理或持有资料的地方有与《隐私条例》大体上相似或达致与《隐私条例》的目的相同的目的之法律正在生效；或 （d）有关使用或处理或持有是获《隐私条例》准许。 **6.有关直接促销的条文** 如转移目的包括由资料接收者使用转移的个人资料作直接促销用途，而资料转移者	

比较维度/政策文件	《个人信息出境标准合同》	《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同》	香港-《资料使用者转移资料予资料使用者的建议合约条文模板》	香港《-资料使用者转移资料予资料处理者的建议合约条文模板》
	（九）受个人信息处理者委托处理个人信息，转委托第三方处理的，应当事先征得个人信息处理者同意，要求该第三方不得超出本合同附录一“个人信息出境说明”中约定的处理目的、处理方式等处理个人信息，并对该第三方的个人信息处理活动进行监督。 （十）利用个人信息进行自动化决策的，应当保证决策的透明度和结果公平、公正，不得对个人信息主体在交易价格等交易条件上实行不合理的差别待遇。通过自动化决策方式向个人信息主体进行信息推送、商业营销的，应当同时提供不针对其个人特征的选项，或者	（十三）接收方所在地的政府部门、司法机构要求接收方提供本合同项下的个人信息的，应当立即通知个人信息处理者。	以书面通知资料接收者停止为这目的使用任何转移的个人资料，除非《隐私条例》另有准许，否则资料接收者须立即停止为直接促销目的而使用转移的个人资料。	

比较维度/政策文件	《个人信息出境标准合同》	《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同》	香港-《资料使用者转移资料予资料使用者的建议合约条文模板》	香港《-资料使用者转移资料予资料处理者的建议合约条文模板》
	向个人信息主体提供便捷的拒绝方式。 （十一）承诺向个人信息处理者提供已遵守本合同义务所需的必要信息，允许个人信息处理者对必要数据文件和文档进行查阅，或者对本合同涵盖的处理活动进行合规审计，并为个人信息处理者开展合规审计提供便利。 （十二）对开展的个人信息处理活动进行客观记录，保存记录至少3年，并按照相关法律法规要求直接或者通过个人信息处理者向监管机构提供相关记录文件。 （十三）同意在监督本合同实施的相关程序中接受监管机构			

比较维度/ 政策文件	《个人信息出境标准合同》	《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同》	香港-《资料使用者转移资料予资料使用者的建议合约条文模板》	香港《-资料使用者转移资料予资料处理者的建议合约条文模板》
	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者作出的决定、提供已采取必要行动的书面证明等。			
接收方所在国家或者地区个人信息保护政策和法规对合同履行的影响	**第四条 境外接收方所在国家或者地区个人信息保护政策和法规对合同履行的影响** （一）双方应当保证在本合同订立时已尽到合理注意义务，未发现境外接收方所在国家或者地区的个人信息保护政策和法规（包括任何提供个人信息的要求或者授权公共机关访问个人信息的规定）影响境外接收方履行本合同约定的义务。	/	/	/

比较维度/政策文件	《个人信息出境标准合同》	《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同》	香港-《资料使用者转移资料予资料使用者的建议合约条文模板》	香港《-资料使用者转移资料予资料处理者的建议合约条文模板》
	（二）双方声明，在作出本条第一项的保证时，已经结合下列情形进行评估： 1.出境的具体情况，包括个人信息处理目的、传输个人信息的种类、规模、范围及敏感程度、传输的规模和频率、个人信息传输及境外接收方的保存期限、境外接收方此前类似的个人信息跨境传输和处理相关经验、境外接收方是否曾发生个人信息安全相关事件及是否进行了及时有效地处置、境外接收方是否曾收到其所在国家或者地区公共机关要求其提供个人信息的请求及境外接收方应对的情况。			

比较维度/政策文件	《个人信息出境标准合同》	《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同》	香港-《资料使用者转移资料予资料使用者的建议合约条文模板》	香港《-资料使用者转移资料予资料处理者的建议合约条文模板》
	2.境外接收方所在国家或者地区的个人信息保护政策和法规，包括下列要素： （1）该国家或者地区现行的个人信息保护法律法规及普遍适用的标准。 （2）该国家或者地区加入的区域性或者全球性的个人信息保护方面的组织，以及所作出的具有约束力的国际承诺。 （3）该国家或者地区落实个人信息保护的机制，如是否具备个人信息保护的监督执法机构和相关司法机构等。 3.境外接收方安全管理制度和技术手段保障能力。 （三）境外接收方保证，在根据本条第二项进行评估时，已			

比较维度/政策文件	《个人信息出境标准合同》	《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同》	香港-《资料使用者转移资料予资料使用者的建议合约条文模板》	香港《-资料使用者转移资料予资料处理者的建议合约条文模板》
	尽最大努力为个人信息处理者提供了必要的相关信息。 （四）双方应当记录根据本条第二项进行评估的过程和结果。 （五）因境外接收方所在国家或者地区的个人信息保护政策和法规发生变化（包括境外接收方所在国家或者地区更改法律，或者采取强制性措施）导致境外接收方无法履行本合同的，境外接收方应当在知道该变化后立即通知个人信息处理者。 （六）境外接收方接到所在国家或者地区的政府部门、司法机构关于提供本合同项下的个			

比较维度/ 政策文件	《个人信息出境标准合同》	《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同》	香港-《资料使用者转移资料予资料使用者的建议合约条文模板》	香港《-资料使用者转移资料予资料处理者的建议合约条文模板》
	人信息要求的，应当立即通知个人信息处理者。			
个人信息主体的权利	**第五条 个人信息主体的权利** 双方约定个人信息主体作为本合同第三方受益人享有以下权利： （一）个人信息主体依据相关法律法规，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，有权要求查阅、复制、更正、补充、删除其个人信息，有权要求对其个人信息处理规则进行解释说明。 （二）当个人信息主体要求对已经出境的个人信息行使上述权利时，个人信息主体可以请求个人信息处理者采取适当措	**第四条 个人信息主体的权利** 双方约定个人信息主体作为本合同第三方受益人享有以下权利: （一）个人信息主体依据个人信息处理者属地相关法律法规及本合同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，有权要求查阅、复制、更正、补充、删除其个人信息，有权要求对其个人信息处理规则进行解释说明。 （二）当个人信息主体要求对依据本合同传输的个人信息行使上述权利时，个人信息主体	**5.资料当事人的查阅及改正资料权利** 资料转移者与资料接收者会就收取及处理转移的个人资料的资料当事人或其代表所提出的查阅及改正资料要求而各自履行其相关责任，正如资料转移一览表所指明。	/

比较维度/政策文件	《个人信息出境标准合同》	《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同》	香港-《资料使用者转移资料予资料使用者的建议合约条文模板》	香港《-资料使用者转移资料予资料处理者的建议合约条文模板》
	施实现，或者直接向境外接收方提出请求。个人信息处理者无法实现的，应当通知并要求境外接收方协助实现。 （三）境外接收方应当按照个人信息处理者的通知，或者根据个人信息主体的请求，在合理期限内实现个人信息主体依照相关法律法规所享有的权利。 境外接收方应当以显著的方式、清晰易懂的语言真实、准确、完整地告知个人信息主体相关信息。 （四）境外接收方拒绝个人信息主体的请求的，应当告知个人信息主体其拒绝的原因，以及个人信息主体向相关监管机	可以请求个人信息处理者采取适当措施实现，或者直接向接收方提出请求。个人信息处理者无法实现的，应当通知并要求接收方协助实现。 （三）接收方应当按照个人信息处理者的通知，或者根据个人信息主体的请求，在合理期限内实现个人信息主体依照个人信息处理者属地相关法律法规及本合同所享有的权利。 接收方应当以显著的方式、清晰易懂的语言真实、准确、完整地告知个人信息主体相关信息。 （四）接收方拒绝个人信息主体的请求的，应当告知个人信息主体其拒绝的原因，以及个		

比较维度/政策文件	《个人信息出境标准合同》	《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同》	香港-《资料使用者转移资料予资料使用者的建议合约条文模板》	香港《-资料使用者转移资料予资料处理者的建议合约条文模板》
	构提出投诉和寻求司法救济的途径。 （五）个人信息主体作为本合同第三方受益人有权根据本合同条款向个人信息处理者和境外接收方的一方或者双方主张并要求履行本合同项下与个人信息主体权利相关的下列条款： 第二条，但第二条第五项、第六项、第七项、第十一项除外。 第三条，但第三条第七项第 2 目和第 4 目、第九项、第十一项、第十二项、第十三项除外。 第四条，但第四条第五项、第六项除外。	人信息主体向个人信息处理者或者接收方属地相关监管机构提出投诉和寻求司法救济的途径。 （五）个人信息主体作为本合同第三方受益人有权根据本合同条款向个人信息处理者和接收方的一方或者双方主张要求履行本合同项下与个人信息主体权利相关的下列条款: 1.第二条，但第二条第五项、第六项、第七项、第十一项除外。 2.第三条，但第三条第六项第 2 目和第 4 目、第九项、第十项、第十一项、第十二项、第十三项除外。		

比较维度/ 政策文件	《个人信息出境标准合同》	《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同》	香港-《资料使用者转移资料予资料使用者的建议合约条文模板》	香港《-资料使用者转移资料予资料处理者的建议合约条文模板》
	第五条。 第六条。 第八条第二项、第三项。 第九条第五项。 上述约定不影响个人信息主体依据《中华人民共和国个人信息保护法》享有的权益。	3.第四条。 4.第五条。 5.第七条第二项、第三项。 6.第八条第五项。 上述约定不影响个人信息主体依据个人信息处理者或者接收方属地相关法律法规享有的权益。		
救济	**第六条 救济** （一）境外接收方应当确定一个联系人，授权其答复有关个人信息处理的询问或者投诉，并应当及时处理个人信息主体的询问或者投诉。境外接收方应当将联系人信息告知个人信息处理者，并以简洁易懂的方式，通过单独通知或者在其网	**第五条 救济** （一）接收方应当确定一个联系人，授权其答复有关个人信息处理的询问或者投诉，并应当及时处理个人信息主体的询问或者投诉。接收方应当将联系人信息告知个人信息处理者，并以简洁易懂的方式，通过单独通知或者在其网站公	/	/

比较维度/政策文件	《个人信息出境标准合同》	《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同》	香港-《资料使用者转移资料予资料使用者的建议合约条文模板》	香港《-资料使用者转移资料予资料处理者的建议合约条文模板》
	站公告，告知个人信息主体该联系人信息，具体为： 联系人及联系方式（办公电话或电子邮箱） （二）一方因履行本合同与个人信息主体发生争议的，应当通知另一方，双方应当合作解决争议。 （三）争议未能友好解决，个人信息主体根据第五条行使第三方受益人的权利的，境外接收方接受个人信息主体通过下列形式维护权利： 1.向监管机构投诉。 2.向本条第五项约定的法院提起诉讼。 （四）双方同意个人信息主体就本合同争议行使第三方受益	告，告知个人信息主体该联系人信息，具体为: 联系人及联系方式（办公电话或电子邮箱） （二）一方因履行本合同与个人信息主体发生争议的，应当通知另一方，双方应当合作解决争议。 （三）争议未能友好解决，个人信息主体根据第四条行使第三方受益人的权利的，接收方接受个人信息主体通过下列形式维护权利: 1.向相关监管机构投诉。 2.向本条第五项约定的法院提起诉讼。 （四）双方同意个人信息主体就本合同争议行使第三方受益		

比较维度/ 政策文件	《个人信息出境标准合同》	《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同》	香港-《资料使用者转移资料予资料使用者的建议合约条文模板》	香港《-资料使用者转移资料予资料处理者的建议合约条文模板》
	人权利，个人信息主体选择适用中华人民共和国相关法律法规的，从其选择。 （五）双方同意个人信息主体就本合同争议行使第三方受益人权利的，个人信息主体可以依据《中华人民共和国民事诉讼法》向有管辖权的人民法院提起诉讼。 （六）双方同意个人信息主体所作的维权选择不会减损个人信息主体根据其他法律法规寻求救济的权利。	人权利，个人信息主体选择适用个人信息处理者属地相关法律法规的，从其选择。 （五）双方同意个人信息主体就本合同争议行使第三方受益人权利的，个人信息主体可以依据《中华人民共和国民事诉讼法》《最高人民法院关于内地与香港特别行政区法院相互认可和执行当事人协议管辖的民商事案件判决的安排》或香港法律法规向内地或者香港有管辖权的法院提起诉讼。 （六）双方同意个人信息主体所作的维权选择不会减损个人信息主体根据其他法律法规寻求救济的权利。		
合同解除	**第七条 合同解除**	**第六条 合同解除**	/	/

比较维度/政策文件	《个人信息出境标准合同》	《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同》	香港-《资料使用者转移资料予资料使用者的建议合约条文模板》	香港《-资料使用者转移资料予资料处理者的建议合约条文模板》
	（一）境外接收方违反本合同约定的义务，或者境外接收方所在国家或者地区的个人信息保护政策和法规发生变化（包括境外接收方所在国家或者地区更改法律，或者采取强制性措施）导致境外接收方无法履行本合同的，个人信息处理者可以暂停向境外接收方提供个人信息，直到违约行为被改正或者合同被解除。 （二）有下列情形之一的，个人信息处理者有权解除本合同，并在必要时通知监管机构： 1.个人信息处理者根据本条第一项的规定暂停向境外接收方提	（一）接收方违反本合同约定的义务和责任，或者被采取强制性措施导致无法履行本合同的，个人信息处理者可以暂停向接收方提供个人信息，直到违约行为被改正或者合同被解除。 （二）有下列情形之一的，个人信息处理者有权解除本合同，并通知个人信息处理者属地监管机构: 1.个人信息处理者根据本条第一项的规定暂停向接收方提供个 人信息的时间超过 1 个月。 2.接收方严重或者持续违反本合同约定的义务和责任。 3.根据主管法院或者监管机构作出的终局决定，接收方或者		

比较维度/政策文件	《个人信息出境标准合同》	《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同》	香港-《资料使用者转移资料予资料使用者的建议合约条文模板》	香港《-资料使用者转移资料予资料处理者的建议合约条文模板》
	供个人信息的时间超过 1 个月。 2.境外接收方遵守本合同将违反其所在国家或者地区的法律规定。 3.境外接收方严重或者持续违反本合同约定的义务。 4.根据境外接收方的主管法院或者监管机构作出的终局决定，境外接收方或者个人信息处理者违反了本合同约定的义务。 在本项第 1 目、第 2 目、第 4 目的情况下，境外接收方可以解除本合同。 （三）经双方同意解除本合同的，合同解除不免除其在个人信息处理过程中的个人信息保护义务。	个人信息处理者违反了本合同约定的义务和责任。 在本项第 3 目的情况下，接收方可以解除本合同。 （三）合同解除不免除双方在个人信息处理过程中的个人信息保 护义务和责任。 （四）合同解除时，接收方应当及时返还或者删除其根据本合同所接收到的个人信息（包括所有备份），并向个人信息处理者提供书面说明。删除个人信息从技术上难以实现的，应当停止除存储和采取必要的安全保护措施之外的处理。		

比较维度/政策文件	《个人信息出境标准合同》	《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同》	香港-《资料使用者转移资料予资料使用者的建议合约条文模板》	香港《-资料使用者转移资料予资料处理者的建议合约条文模板》
	（四）合同解除时，境外接收方应当及时返还或者删除其根据本合同所接收到的个人信息（包括所有备份），并向个人信息处理者提供书面说明。删除个人信息从技术上难以实现的，应当停止除存储和采取必要的安全保护措施之外的处理。			
违约责任	**第八条 违约责任** （一）双方应就其违反本合同而给对方造成的损失承担责任。 （二）任何一方因违反本合同而侵害个人信息主体享有的权利，应当对个人信息主体承担民事法律责任，且不影响相关法律法规规定个人信息处理者应	**第七条 违约责任** （一）双方应就其违反本合同而给对方造成的损失承担责任。 （二）任何一方因违反本合同而侵害个人信息主体享有的权利，应当对个人信息主体承担民事法律责任，且不影响相关法律法规规定个人信息处理者	/	/

比较维度/政策文件	《个人信息出境标准合同》	《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同》	香港-《资料使用者转移资料予资料使用者的建议合约条文模板》	香港《-资料使用者转移资料予资料处理者的建议合约条文模板》
	当承担的行政、刑事等法律责任。 （三）双方依法承担连带责任的，个人信息主体有权请求任何一方或者双方承担责任。一方承担的责任超过其应当承担的责任份额时，有权向另一方追偿。	应当承担的行政、刑事等法律责任。 （三）双方依法承担连带责任的，个人信息主体有权请求任何一方或者双方承担责任。一方承担的责任超过其应当承担的责任份额时，有权向另一方追偿。		
其他约定	**第九条 其他** （一）如本合同与双方订立的任何其他法律文件发生冲突，本合同的条款优先适用。 （二）本合同的成立、效力、履行、解释、因本合同引起的双方间的任何争议，适用中华人民共和国相关法律法规。 （三）发出的通知应当以电子邮件、电报、电传、传真（以	**第八条 其他** （一）如本合同与双方订立的任何其他法律文件发生冲突，本合同的条款优先适用。 （二）本合同的成立、效力、履行、解释、因本合同引起的双方间的任何争议，适用个人信息处理者属地相关法律法规。	/	/

比较维度/政策文件	《个人信息出境标准合同》	《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同》	香港-《资料使用者转移资料予资料使用者的建议合约条文模板》	香港《-资料使用者转移资料予资料处理者的建议合约条文模板》
	航空信件寄送确认副本）或者航空挂号信发往（具体地址）或者书面通知取代该地址的其它地址。如以航空挂号信寄出本合同项下的通知，在邮戳日期后的 天应当视为收讫；如以电子邮件、电报、电传或者传真发出，在发出以后的 个工作日应当视为收讫。 （四）双方因本合同产生的争议以及任何一方因先行赔偿个人信息主体损害赔偿责任而向另一方的追偿，双方应当协商解决；协商解决不成的，任何一方可以采取下列第 种方式加以解决（如选择仲裁，请勾选仲裁机构）： 仲裁。将该争议提交	（三）发出的通知应当以电子邮件、电报、电传、传真（以航空信件寄送确认副本）或者航空挂号信发往（具体地址）或者书面通知取代该地址的其它地址。如以航空挂号信寄出本合同项下的通知，在邮戳日期后的 天应当视为收讫;如以电子邮件、电报、电传或者传真发出，在发出以后的 个工作日应当视为收讫。 （四）双方因本合同产生的争议以及任何一方因先行赔偿个人信息主体损害赔偿责任而向另一方的追偿，双方应当协商解决;协商解决不成的，任何一方可以采取下列第 种方式加以		

比较维度/政策文件	《个人信息出境标准合同》	《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同》	香港-《资料使用者转移资料予资料使用者的建议合约条文模板》	香港《-资料使用者转移资料予资料处理者的建议合约条文模板》
	☐中国国际经济贸易仲裁委员会 ☐中国海事仲裁委员会 ☐北京仲裁委员会（北京国际仲裁中心） ☐上海国际仲裁中心 ☐其他《承认及执行外国仲裁裁决公约》成员的仲裁机构 按其届时有效的仲裁规则在（仲裁地点） 进行仲裁； 诉讼。依法向中华人民共和国有管辖权的人民法院提起诉讼。 （五）本合同应当按照相关法律法规的规定进行解释，不得以与相关法律法规规定的权	解决（如选择仲裁，请勾选仲裁机构）： 1.仲裁。将该争议提交 □中国国际经济贸易仲裁委员会 □中国海事仲裁委员会 □中国广州国际仲裁委员会 □粤港澳大湾区国际仲裁中心 □香港国际仲裁中心 按其届时有效的仲裁规则在（仲裁地点）2.诉讼。依法向内地或者香港有管辖权的法院提起诉讼。 （五）本合同应当按照个人信息处理者属地相关法律法规适用的规定进行解释，不得以与个人信息处理者属地相关法律法规适用的规定的权利、义务		

比较维度/ 政策文件	《个人信息出境标准合同》	《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同》	香港-《资料使用者转移资料予资料使用者的建议合约条文模板》	香港《-资料使用者转移资料予资料处理者的建议合约条文模板》
	利、义务相抵触的方式解释本合同。 （六）本合同正本一式 份，双方各执 份，其法律效力相同。 本合同在（地点） 签订 本合同在（地点）签订 个人信息处理者：年月日 境外接收方：年月日	和责任相抵触的方式解释本合同。 （六）本合同正本一式 份，双方各执 份，其法律效力相同。 本合同在（地点）签订 个人信息处理者：年月日 接收方：年月日		
出境情况说明	**附录一 个人信息出境说明** 根据本合同向境外提供个人信息的详情约定如下： （一）处理目的： （二）处理方式： （三）出境个人信息的规模： （四）出境个人信息种类（参考 GB/T 35273《信息安全技术 个人信息安全规范》和相关标准）：	**附录一 个人信息跨境提供说明** 根据本合同向接收方提供个人信息的详情约定如下： （一）处理目的： （二）处理方式： （三）跨境提供个人信息的规模： （四）跨境提供个人信息的种类（参考 GB/T 35273《信息安全技术 个人信息安全规范》或	**资料转移一览表** 1.转移的描述 转移的个人资料的类别 转移目的 准许司法管辖区 保留时期 2.继续转移 转移的个人资料的类别	**资料转移一览表** 1.转移的描述 转移的个人资料的类别 转移目的 准许司法管辖区 保留时期 2.分判处理 分判处理的个人资料的类别

比较维度/ 政策文件	《个人信息出境标准合同》	《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同》	香港-《资料使用者转移资料予资料使用者的建议合约条文模板》	香港《-资料使用者转移资料予资料处理者的建议合约条文模板》
	（五）出境敏感个人信息种类（如适用，参考 GB/T 35273《信息安全技术 个人信息安全规范》和相关标准）： （六）境外接收方只向以下中华人民共和国境外第三方提供个人信息（如适用）； （七）传输方式： （八）出境后保存期限：（ 年 月 日至 年 月 日） （九）出境后保存地点： （十）其他事项（视情况填写）： **附录二 双方约定的其他条款（如需要）**	个人信息处理者属地相关标准）： （五）接收方只向注册于（适用于组织）/位于（适用于个人）粤港澳大湾区内地或香港特别行政区同辖区内的第三方提供个人信息（如适用）： （六）传输方式: （七）跨境提供后保存期限:（ 年 月 日至 年 月 日） （八）跨境提供后保存地点: （九）其他事项（视情况填写）： **附录二 双方约定的其他条款（如需要）**	继续转移的接收者（具体说明或以类别标示） 继续转移的目的 准许司法管辖区 保留时期 3.保安措施 ［列出资料接收者须对转移的个人资料采取的保安措施。］ 4.资料当事人的查阅及改正资料要求 ［描述收取及处理资料当事人的查阅及改正资料要求的安排。］	分判处理者（具体说明或以类别标示） 准许司法管辖区 保留时期 3.保安措施 ［列出资料接收者须对转移的个人资料采取的保安措施。］

5. 网络竞争规范：解读《网络反不正当竞争暂行规定》：互联网条款重点关注[41]

引言

随着数字经济与互联网的迅猛发展，网络环境中的不正当竞争行为日益凸显，成为扰乱市场秩序、侵害消费者权益、阻碍创新发展的棘手问题。为应对和遏制各类新型不正当竞争行为，我国《中华人民共和国反不正当竞争法》（2019 年修订）（以下简称“《反法》”）第十二条对扰乱互联网领域竞争秩序的行为进行了规制，该条款也通常被称为“互联网专项”条款。2022 年发布的《中华人民共和国反不正当竞争法（修订草案征求意见稿）》（以下简称“《反法草案》”）对《反法》互联网专项条款进行了扩充和细化，采用“一般条款+具体举例”的立法模式，即一般条款作为总则（第十五条）明确了经营者不得利用技术手段实施不正当竞争行为，分则部分（第十六条至第二十二条）列举了互联网不正当竞争行为的具体类型。

2024 年 5 月 6 日，国家市场监管总局发布了《网络反不正当竞争暂行规定》（以下简称“《暂行规定》”），该规定自 2024 年 9 月 1 日起正式施行。对于互联网专项条款，《暂行规定》沿用了《反法草案》互联网专项条款的立法框架，即以第十二条作为总领性条款、第十三条至第二十一条列举具体不正当竞争行为，并将第二十二条作为兜底条款的模式，旨在全面构建互联网领域反不正当竞争行为的规制体系。其中，《暂行规定》除了对《反法》《反法草案》已经规定的“流量劫持”“恶意不兼容”“恶意干扰”等妨害或破坏其他经营者合法提供的网络产品或者服务等行为进行了细化规定外，还首次针对一些新的网络不正当竞争行为（如反向刷单、非法数据获取、恶意拦截、歧视待遇等）提供了认定标准。

顺接《网络反不正当竞争暂行规定》系列解读丨之一：新规亮点解读》的详细解读，本文将专门针对《暂行规定》第十二条至二十二条所规定的“互联网条款”展开进一步介绍分析，以期与感兴趣的读者进行更多探讨和互动。

一、具体条款解读

《反法》	《反法草案》	《暂行规定》
第十二条 经营者利用网络从事生产经营活动，应当遵守本法的各项规定。	**第十五条** 经营者利用网络从事生产经营活动，应当遵守本法的各项规定。	**第十二条** 经营者不得利用互联网、大数据、算法等技术手段，通过影响用户选择或者其他方式，实施流量劫

[41] 作者：孟洁、王程、董杰睿、尹童晖

《反法》	《反法草案》	《暂行规定》
经营者不得利用技术手段，通过影响用户选择或者其他方式，实施下列妨碍、破坏其他经营者合法提供的网络产品或者服务正常运行的行为: ……	经营者不得利用数据和算法、技术以及平台规则等，通过影响用户选择或者其他方式，扰乱市场公平竞争秩序。 前款所称影响用户选择，包括违背用户意愿和选择权、增加操作复杂性、破坏使用连贯性等。	持、干扰、恶意不兼容等行为，妨碍、破坏其他经营者合法提供的网络产品或者服务正常运行。 前款所称的影响用户选择，包括违背用户意愿和选择权、增加操作复杂性、破坏使用连贯性等。 判定是否构成第一款规定的不正当竞争行为，应当充分考虑是否有利于技术创新和行业发展等因素。

首先我们应当关注《暂行规定》第十二条。第十二条作为互联网条款的总括性条款明确了经营者在网络经营活动中扰乱市场公平竞争秩序所利用的各类手段，如**互联网、大数据、算法**等。同时，《暂行规定》第十二条第二款点明了网络不正当竞争行为扰乱市场公平竞争秩序的主要方式——影响用户选择，既包括**违背用户意愿和选择权**的直接方式，又包括通过**增加操作复杂性、破坏使用连贯性等**间接方式来干扰用户使用并最终影响其正常选择。此外，《暂行规定》第十二条第三款新增了判定构成网络不正当竞争行为的因素，即“**是否有利于技术创新和行业发展**”，为判断互联网不正当竞争行为提供了原则性参考依据。这一因素也与此前某高校毕业生就业数据非法使用案中法院的观点相呼应[42]。在该案中，法院认为被告以不正当手段使用和售卖原告收集、加工的“662 所高校学生毕业十年就业薪酬和就业行业分析”数据，不仅损害了原告对涉案数据享有的竞争利益，还不利于技术创新和投入的积极性，破坏竞争秩序，阻碍大数据行业的正常、有序发展，并最终造成消费者基于大数据产品和服务所享有的社会福利的减损，构成不正当竞争行为。

《暂行规定》第十三条至第二十二条紧接第十二条的总领性要求，分别列举了互联网条款所规制的不正当竞争行为的具体表现形式。其中，《暂行规定》第十三条、第十四条、第十五、第二十一条实际上是对《反法》第十二条所规定的流量劫持、干扰、恶意不兼容行为的细化，进一步拓展说明了每种行为的表现形式，与《反法草案》第十六条相呼应。而《暂行规定》第十六条、第十七条、第十八条、第十九条、第二十条为首次增加的新型不正当竞争行为。

[42] 参考北京知识产权法院（2020）京 73 民终 3422 号判决书。

下文中我们将通过对每一类网络不正当竞争行为的阐释，以帮助读者理解每类行为的差异性，并识别认定标准和执法尺度。

（一）流量劫持（第十三条）

《反法》	《反法草案》	《暂行规定》
第十二条 经营者不得利用技术手段，通过影响用户选择或者其他方式，实施下列妨碍、破坏其他经营者合法提供的网络产品或者服务正常运行的行为： （一）未经其他经营者同意，在其合法提供的网络产品或者服务中，插入链接、强制进行目标跳转； …… 	**第十六条** 经营者不得利用技术手段，实施下列流量劫持、不当干扰、恶意不兼容等行为，影响用户选择，妨碍、破坏其他经营者合法提供的网络产品或者服务正常运行： （一）未经其他经营者同意，在其合法提供的网络产品或者服务中，插入链接、强制进行目标跳转、嵌入自己或者他人的产品或者服务； （二）利用关键词联想、设置虚假操作选项等方式，设置指向自身产品或者服务的链接，欺骗或者误导用户点击； ……	**第十三条** 未经其他经营者同意，经营者不得利用技术手段，实施下列插入链接或者强制进行目标跳转等行为，妨碍、破坏其他经营者合法提供的网络产品或者服务正常运行： （一）在其他经营者合法提供的网络产品或者服务中，插入跳转链接、嵌入自己或者他人的产品或者服务； （二）利用关键词联想、设置虚假操作选项等方式，设置指向自身产品或者服务的链接，欺骗或者误导用户点击； （三）其他插入链接或者强制进行目标跳转的行为。

《暂行规定》第十三条将“**流量劫持**”行为细分为三类情形，与《反法草案》第十六条第一款第一项规定的“插入链接、嵌入自己或者他人的产品或者服务”和第二项规定的“利用关键词联想、设置虚假操作选项”相呼应，并新增兜底条款—“其他插入链接或者强制进行目标跳转的行为”，完善了对“流量劫持”不正当竞争行为的规制框架。

首先，当移动智能手机成为大众日常生活消费的主流场景时，原先通过“插入链接”进行的非法跳转行为也“更新换代”为“**嵌入产品或服务**”。在某起浙江省杭州市中级人民法院审理的案件中[43]，被告通过修改 App 客户端的协议，使得用

[43] 参考浙江省杭州市中级人民法院（2020）浙 01 民终 8743 号判决书。

户在打开原告应用程序的时候会被强制跳转到被告的程序。在这种情况下，法院认为被告的行为剥夺了用户的知情权和自由选择权，违背了诚实信用原则和公认的商业道德，导致原告的交易机会流失，扰乱了公平的网络市场竞争秩序，因此该行为应当被认定为不正当竞争行为。

其次，从某种意义上讲，流量的本质代表用户对经营者所提供产品/服务的关注程度，经营者拥有的流量越多，可能获得的商业机会越多，其自身经营力也会随之增强，因此互联网经营者会通过各种手段去争夺用户流量，进一步实现商业变现。常见的非法竞争手段包括通过产品界面设置虚假、隐蔽操作（如用户按点击关闭、翻页按钮反而发生目标跳转等）、模糊关键词联想（如“你有一个红包待领取”“点我减一元”等）、利用技术手段影响、篡改原本的数据传输路径（如通过某些手段修改域名解析，使对特定域名的访问由目标 IP 地址转接到被篡改后的指定 IP，强迫用户接收广告信息）等，从而导致用户无法执行原本希望的操作，反而触发本无访问意图的链接[44]。相关典型案例为 2019 年某搜索引擎公司诉某输入法公司搜索导流的不正当竞争纠纷案[45]。在该案中，被告公司通过自家输入法将搜索候选词排列在输入法界面的输入候选词上方，此时用户点击搜索候选词即直接跳转进入被告公司的搜索结果页面。对此，法院认为被告公司通过搜索候选词将用户引导至同样没有明显标识的、被告公司自己的搜索结果页面，劫持本属于原告的搜索用户流量，应当被认定为利用技术手段，通过影响用户选择的方式，妨碍了原告经营活动的正常运行，构成不正当竞争。

（二）恶意干扰（第十四条、第二十一条）

《反法》	《反法草案》	《暂行规定》
第十二条 经营者不得利用技术手段，通过影响用户选择或者其他方式，实施下列妨碍、破坏其他经营者合法提供的网络产品或者服务正常运行的行为： …… （二）误导、欺骗、强迫用户修改、关闭、卸载其	**第十六条** 经营者不得利用技术手段，实施下列流量劫持、不当干扰、恶意不兼容等行为，影响用户选择，妨碍、破坏其他经营者合法提供的网络产品或者服务正常运行： …… （三）误导、欺骗、强迫用户修改、关闭、卸载其	**第十四条** 经营者不得利用技术手段，误导、欺骗、强迫用户修改、关闭、卸载其他经营者合法提供的设备、功能或者其他程序等网络产品或者服务。

[44] 参考黄武双，谭宇航，《<反不正当竞争法>第十二条类型化条款适用研究》，《科技与法律（中英文）》，2023 年第 2 期。
[45] 参考北京市海淀区人民法院（2017）京 0108 民初 7967 号判决书。

《反法》	《反法草案》	《暂行规定》
他经营者合法提供的网络产品或者服务； …… 	他经营者合法提供的网络产品或者服务； …… 	
/	**第十六条** 经营者不得利用技术手段，实施下列流量劫持、不当干扰、恶意不兼容等行为，影响用户选择，妨碍、破坏其他经营者合法提供的网络产品或者服务正常运行： …… （五）无正当理由，对其他经营者合法提供的产品或者服务的内容、页面实施拦截、屏蔽等； ……	**第二十一条** 经营者不得利用技术手段，通过下列方式，实施妨碍、破坏其他经营者合法提供的网络产品或者服务正常运行的行为： （一）违背用户意愿下载、安装、运行应用程序； （二）无正当理由，对其他经营者合法提供的网络产品或者服务实施拦截、拖延审查、下架，以及其他干扰下载、安装、运行、更新、传播等行为； （三）对相关设备运行非必需的应用程序不提供卸载功能或者对应用程序卸载设置不合理障碍； （四）无正当理由，对其他经营者合法提供的网络产品或者服务，实施搜索降权、限制服务内容、调整搜索结果的自然排序等行为； （五）其他妨碍、破坏其他经营者合法提供的网络产品或者服务正常运行的行为。

《最高人民法院关于适用<中华人民共和国反不正当竞争法>若干问题的解释》第二十二条规定“误导、欺骗、强迫用户修改、关闭、卸载其他经营者合法

提供的网络产品或者服务”属于“恶意干扰”类不正当竞争行为。《暂行规定》第十四条对“恶意干扰”行为原有规定的修改不大，仅是结合互联网产品的发展形态将“干扰”行为所指向的客体扩展到**设备、功能、程序**等网络产品或者服务。涉及经营者实施“恶意干扰”行为的典型案例为某输入法公司 A 与某输入法公司 B 的不正当竞争纠纷案[46]。在该案中，被告 B 公司输入法采用定时和不定时弹出窗口，反复提示用户删除 A 公司输入法在语言栏的快捷方式，造成用户无法再行选择使用 A 公司输入法。虽然被告辩称用户可以点击该窗口右上角的关闭键，但法院考虑到该窗口的对话框没有按照一般规则设置“取消”按钮，本身就会对消费者产生误导；加之该窗口会定时或不定时的多次自动弹出，用户在反复诱导之下按照提示删除 A 公司输入法在语言栏的快捷方式的可能性很大，违反了市场交易中应当遵循的自愿、平等、公平、诚实信用的原则，构成不正当竞争。

此外，《暂行规定》第二十一条还对可被认定为“恶意干扰”行为的两种聚焦于应用程序的表现形式进行了补充细化，分别为**①不得违背用户意愿下载、安装、运行应用程序，②对相关设备运行非必需的应用程序不提供卸载功能或者对应用程序卸载设置不合理障碍。**针对前者，《暂行规定》回应了当下信息资讯网站、网络社区等频繁弹窗推荐 App，要求“下载 App 才能查看全文”“不用 App 不能看评论”等妨碍用户浏览网页信息的热点问题。针对后者，虽然《暂行规定》并未给出“运行非必需的应用程序”的明确定义，但参考《移动智能终端应用软件预置和分发管理暂行规定》《关于进一步规范移动智能终端应用软件预置行为的通告》对“基本功能软件”的相关定义，可理解为保障移动智能终端硬件和操作系统正常运行的移动智能终端应用软件，主要包括操作系统基本组件（如系统设置、文件管理）、保证智能终端硬件正常运行的应用软件（如多媒体摄录）、基本通信应用软件（如接打电话、收发短信、通讯录、浏览器）、应用软件下载通道（如应用商店）这四类。对于移动智能终端以外其他终端产品也可参考上述规定进行综合判断。

（三）恶意不兼容（第十五条）

《反法》	《反法草案》	《暂行规定》
第十二条 经营者不得利用技术手段，通过影响用户选择或者其他方式，实施下列妨碍、破坏其他经营者合法提供的网络产品或者服务正常运行的行为:	**第十六条** 经营者不得利用技术手段，实施下列流量劫持、不当干扰、恶意不兼容等行为，影响用户选择，妨碍、破坏其他经营者合法	**第十五条** 经营者不得利用技术手段，恶意对其他经营者合法提供的网络产品或者服务实施不兼容。 判定经营者是否恶意对其他经营者合法提供的

[46] 参考北京市第一中级人民法院(2009)一中民初字第 16849 号。

《反法》	《反法草案》	《暂行规定》
…… （四）恶意对其他经营者合法提供的网络产品或者服务实施不兼容； ……	提供的网络产品或者服务正常运行： …… （四）恶意对其他经营者合法提供的网络产品或者服务实施不兼容； ……	网络产品或者服务实施不兼容，可以综合考虑以下因素： （一）是否知道或者应当知道不兼容行为会妨碍、破坏其他经营者合法提供的网络产品或者服务正常运行； （二）不兼容行为是否影响其他经营者合法提供的网络产品或者服务正常运行，是否影响网络生态开放共享； （三）不兼容行为是否针对特定对象，是否违反公平、合理、无歧视原则； （四）不兼容行为对消费者、使用该网络产品或者服务的第三方经营者合法权益以及社会公共利益的影响； （五）不兼容行为是否符合行业惯例、从业规范、自律公约等； （六）不兼容行为是否导致其他经营者合法提供的网络产品或者服务成本不合理增加； （七）是否有正当理由。

随着信息及通信技术的飞速进步，虽然实现兼容的手段日益丰富且成本显著降低，但经营者仍需投入大量的人力、物力、财力去确保相互兼容并保障兼容过程中的数据安全。因此在开展网络经营活动时，产品或者服务之间的不兼容是否

构成不正当竞争行为也一直存在争议。需要明确的是，不兼容行为本身并不必然构成法律意义上的“恶意不兼容”。当不兼容是由于技术原因或合理的商业策略所致，且并未对其他经营者的正常运营造成妨碍或破坏时，不应被简单归类为不正当竞争。例如，若某互联网头部公司研发的算法大模型因技术限制或特定需求等原因而无法搭载其他公司的模型应用，这本身并不构成不正当竞争。只有当该公司出于恶意目的，故意实施不兼容行为，以损害竞争对手利益或破坏市场竞争秩序时，才应被视为“恶意不兼容”，进而受到法律法规的制约。

“恶意不兼容”包括“不兼容”与“恶意”两项构成要求。首先，“不兼容”属于一种客观表现形式，指不同产品或服务之间存在冲突，既包括无法同时使用（即“破坏”），也包括无法顺畅地使用（即“妨碍”）。因此，对“不兼容”的判断较为直观且相对容易。值得关注的是“不兼容”的概念与“数据可携权”存在互联共通之处，但二者的侧重点各有不同。例如，《欧盟通用数据保护条例》第二十条规定数据主体享有数据可携权，有权要求数据控制者将自身数据以特定形式移交给其他数据控制者，原数据控制者不得加以阻拦或不完全转移，并应满足“可互操作（interoperable）”的格式要求。“可互操作”要求各个组织之间的信息和通信技术系统之间的数据能够实现交换和共享。由此可知，实现数据可携权与促进产品兼容的概念存在重叠，但是数据可携权更关注数据的交换和共享，聚焦于数据控制者所提供的数据能够被其他数据控制者读取，而“兼容”关注的范围更广，主要关注的客体为“网络产品或者服务”。目前促进产品相互兼容、“互联互通”已成为国内外共同关注的焦点。例如，欧盟《数字服务法》也要求谷歌、苹果、Facebook、亚马逊（GAFA）等超大型平台，如果已经被欧盟成员国一致认定为守门人，则应当让用户能够实现信息的互联互通，即用户如果在 Facebook 中发布信息，也应能够在其他平台上同步收到相应信息，并且可以进行回复[47]。同时，欧盟在 2023 年年底还通过了《数据法案》，旨在营造欧盟内部及其各个行业数据自由流动的统一市场，规定了从互联产品和服务中获取（非个人）数据的条件，并通过修改合同法规则，确保数据持有者在“公平、合理和无歧视”的条件下提供数据访问，促进了数据共享和处理的互操作性标准的发展。

在国内司法实践中，法院一般将“恶意”与“不兼容”因素结合起来进行判断，对于经营者是否构成“恶意”目前并没有形成统一的标准，通常会结合具体案情分析该经营者实施的不兼容行为是否符合诚信原则和商业道德等要求[48]。例如，明知侵犯其他经营者合法权益而仍从事相关违法行为，以及在被起诉后仍未停止，反而变相进行运营、销售等[49]。

---

[47] 参考孟洁，鲁裕鑫，《环球合规与风控|刍议〈个保法〉第五十八条“守门人处理者”的理解与适用》，于 2024 年 5 月 20 日访问，https://mp.weixin.qq.com/s/-9Wzf5-o57Q-71sM48l37w。

[48] 参考蒋舸，《<反不正当竞争法>网络条款的反思与解释——以类型化原理为中心》，《中外法学》2019 年第 1 期。

[49] 参考广州知识产权法院（2021）粤 73 民终 153 号判决书。

本次《暂行规定》第十五条特别新增了判断是否“**恶意不兼容**”行为的七个因素，主要涉及**行为的主观意图、行为后果、是否针对特定对象、对市场竞争秩序的影响、对其他经营者合法运营、消费者合法权益以及社会公共利益的影响、是否符合行业惯例、自律公约等、是否导致其他经营者的成本不合理增加、是否具有其他抗辩事由等。**这些考量因素遵循了《反法》认定违法行为的基本思路框架，对互联网企业的合规具有较大的指导意义。

（四）反向刷单（第十六条）

《反法》	《反法草案》	《暂行规定》
/	**第十四条** 经营者不得为了牟取不正当利益，实施下列恶意交易行为，妨碍、破坏其他经营者的正常经营： （一）故意通过短期内与其他经营者进行大规模、高频次交易、给予好评等，引发相关惩戒，使其他经营者受到搜索降权、降低信用等级、商品下架、断开链接、停止服务等处置； （二）恶意在短期内拍下大量商品不付款； （三）恶意批量购买后退货或者拒绝收货； （四）其他利用规则实施恶意交易，不当妨碍、破坏其他经营者正常经营的行为。	**第十六条** 经营者不得利用技术手段，直接、组织或者通过第三方实施以下行为，妨碍、破坏其他经营者合法提供的网络产品或者服务正常运行： （一）故意在短期内与其他经营者发生大规模、高频次交易，或者给予好评等，使其他经营者受到搜索降权、降低信用等级、商品下架、断开链接、停止服务等处置； （二）恶意在短期内批量拍下商品不付款； （三）恶意批量购买后退货或者拒绝收货等。

《暂行规定》第十六条与《反法草案》第十四条相呼应，对**恶意刷单、反向刷单**等行为进行了规定。原先《反法草案》第十四条的规定在互联网条款第十五条之前，由此可知《反法草案》未将此类行为纳入互联网条款的范围内，而《暂行规定》第十六条直接将恶意刷单、反向刷单类行为归类为互联网条款的一个分项。

《暂行规定》第十六条第一款的规定可以通俗理解为，经营者既不能故意给其他经营者刷差评、也不能刷好评（即反向刷单），因为短时间内商家好评/差评的不正常变化会导致平台对商家进行降权处理，从而导致商家受到损失。对于反向刷单的规制可以追溯到“反向刷单第一案—董某某破坏生产经营罪案”[50]。2014年4月，被告人董某某为谋取市场竞争优势，雇佣被告人谢某某多次以同一账号大量购买智齿科技南京公司淘宝网店铺的商品，致使该公司店铺被淘宝平台认定为虚假交易刷销量并据此对其搜索降权。因消费者在数日内无法通过淘宝网搜索栏搜索到智齿科技南京公司淘宝网店铺的商品，严重影响该公司正常经营。最终南京市中级人民法院依据生产经营罪这一“口袋罪”兜底条款作出判决。对此，《中华人民共和国电子商务法》（以下简称“《电子商务法》”）第十七条也作出相应规定，明确电子商务经营者不得以虚构交易、编造用户评价等方式进行虚假或者引人误解的商业宣传，从而落实了刷单主体的违法责任。《暂行规定》进一步扩大了《电子商务法》的主体适用范围，将电子商务经营者以外的其他经营者也纳入到了规制范围中。

（五）恶意拦截、屏蔽（第十七条）

《反法》	《反法草案》	《暂行规定》
/	**第十六条** 经营者不得利用技术手段，实施下列流量劫持、不当干扰、恶意不兼容等行为，影响用户选择，妨碍、破坏其他经营者合法提供的网络产品或者服务正常运行： …… （五）无正当理由，对其他经营者合法提供的产品或者服务的内容、页面实施拦截、屏蔽等； ……	**第十七条** 经营者不得针对特定经营者，拦截、屏蔽其合法提供的信息内容以及页面，妨碍、破坏其他经营者合法提供的网络产品或者服务正常运行，扰乱市场公平竞争秩序。拦截、屏蔽非法信息，频繁弹出干扰用户正常使用的信息以及不提供关闭方式的漂浮视窗等除外。

早在2021年，工信部就曾发布《关于开展互联网行业市场秩序专项整治活动的通知》，针对各头部互联网平台间相互屏蔽链接的行为开展专项整治行动，重点治理恶意屏蔽网址链接、干扰其他企业产品和服务运行等问题，促进各互联网平台“互联互通”。针对此类市场不正当竞争现象，《暂行规定》第十七条呼应

[50] 参考浙江省义乌市人民法院（2018）浙0782刑初596号判决书。

了《反法草案》第十六条的规定，禁止经营者针对特定经营者，拦截、屏蔽其合法提供的信息内容以及页面，妨碍、破坏其他经营者合法提供的网络产品或者服务正常运行，扰乱市场公平竞争秩序。与前文中的“恶意干扰”条款及“恶意不兼容”条款针对的客体为“网络产品或者服务”不同，《暂行规定》第十七条规定的“恶意拦截、屏蔽”条款针对的客体为“合法提供的信息内容以及页面”。

此外，《暂行规定》第十七条不仅对平台间相互屏蔽的违法行为起到规制作用，也对此前引起人们热议的“广告拦截行为”作出了回应。互联网广告是平台经营者获取收益的重要途径之一，但部分用户会选择通过安装广告拦截应用或插件来一键跳过广告，提高用户体验感，这在一定程度上会导致平台经营者无法通过投放广告获得正当的广告经营收益。对此，法院曾在“芒果 TV 诉拦精灵案件”明确合法的互联网广告商业模式应受法律保护，广告拦截应用开发者推出的拦截广告功能并不区分所拦截的互联网广告是否为“合法提供的信息内容以及页面”，对他人正当经营的广告商业行为造成破坏，因此构成而不正当竞争行为。但与此同时，《暂行规定》的第十七条在规制广告拦截行为时，也充分考虑到了用户体验和互联网生态环境的平衡，即明确指出“拦截、屏蔽非法信息、频繁弹出干扰用户正常使用的信息以及不提供关闭方式的漂浮视窗等”，不会被认定为恶意拦截、屏蔽行为。这一规定能够促进营造更加清朗的互联网环境，防止用户被过度打扰，同时也为广告拦截插件的合理使用提供了明确的指导。因此，若广告拦截插件的应用场景仅限于拦截上述违法信息内容，则一般不会被认定为构成不正当竞争行为。

在《暂行规定》出台前，以往的司法案例一般通过适用《反法》第十二条第二款第四项的规定来规制此类“恶意拦截、屏蔽”违法行为，法院通过以下三要素来判断是否构成不正当竞争行为：①经营者是否利用了技术手段、②被诉行为的对象是否为其他经营者合法提供的网络产品或服务、③是否对其他经营者合法提供的网络产品或服务产生妨碍或破坏使其无法正常运行。而今后则可以直接适用《暂行规定》第十七条的判断标准，减轻了司法者自由裁量的难度。

（六）“二选一”行为（第十八条）

《反法》	《反法草案》	《暂行规定》
/	/	**第十八条** 经营者不得利用技术手段，通过影响用户选择、限流、屏蔽、搜索降权、商品下架等方式，干扰其他经营者之间的正常交易，妨碍、破坏其他经营者合

《反法》	《反法草案》	《暂行规定》
		法提供的网络产品或者服务的正常运行，扰乱市场公平竞争秩序。 经营者不得利用技术手段，通过限制交易对象、销售区域或者时间、参与促销推广活动等，影响其他经营者的经营选择，妨碍、破坏交易相对方合法提供的网络产品或者服务的正常运行，扰乱市场公平交易秩序。

针对人们重点关注的平台“**二选一**”问题，《暂行规定》第十八条进行了规制。此前《中华人民共和国反垄断法》（以下简称“《反垄断法》”）第二十二条曾明确禁止经营者实施“二选一”行为，即禁止具有市场支配地位的经营者“没有正当理由限定交易相对人只能与其进行交易或者只能与其指定的经营者进行交易”。但是，在利用《反垄断法》对“二选一”行为进行规制的前提为经营者“具有市场支配地位”。

对于尚未取得市场支配地位的情形，目前司法实践依赖于《反法》第十二条第二款第四项进行规制。例如，2021 年 2 月 10 日，国家市场监管总局适用《反法》第十二条对某电商平台实施不正当竞争违法行为进行处罚[51]，指出该平台为获取竞争优势及交易机会，开发并使用巡检系统，获取同时在本公司和其他公司上架销售的品牌经营者信息，利用供应商平台系统、智能化组网引擎、运营中台等提供的技术手段，通过影响用户选择以及限流、屏蔽、商品下架等方式，减少品牌经营者的消费注意、流量和交易机会，限制品牌经营者的销售渠道，妨碍、破坏了品牌经营者及其他经营者合法提供的网络产品和服务正常运行，构成不正当竞争行为。但是，由于《反不正当竞争法》第十二条第二款第四项为原则性规定，适用该条款规制“二选一”行为是否具备充足的上位法基础和学理基础在学术界还存在一定争议[52]。而《暂行规定》第十七条明确对“二选一”行为提出了禁止性要求，并细化了两类“二选一”行为，包括“通过影响用户选择、限流、屏蔽、搜索降权、商品下架等方式，干扰其他经营者之间的正常交易”与“通过限制交易对象、销售区域或者时间、参与促销推广活动等，影响其他经营者的经营选择”。

[51] 参考国市监处[2021]3 号《行政处罚决定书》。
[52] 参考《面对平台“二选一”，反不正当竞争就够了？》，于 2024 年 5 月 17 日访问，https://mp.weixin.qq.com/s/1AvUow0BrtF7U7AJaXnzHQ。

这条规定完善了规制“二选一”行为的法律框架，为执法机构提供了更加全面的法律基础，有助于企业明确界定违法界限。

（七）数据爬虫（第十九条）

《反法》	《反法草案》	《暂行规定》
/	**第十八条** 经营者不得实施下列行为，不正当获取或者使用其他经营者的商业数据，损害其他经营者和消费者的合法权益，扰乱市场公平竞争秩序： （一）以盗窃、胁迫、欺诈、电子侵入等方式，破坏技术管理措施，不正当获取其他经营者的商业数据，不合理地增加其他经营者的运营成本、影响其他经营者的正常经营； （二）违反约定或者合理、正当的数据抓取协议，获取和使用他人商业数据，并足以实质性替代其他经营者提供的相关产品或者服务； （三）披露、转让或者使用以不正当手段获取的其他经营者的商业数据，并足以实质性替代其他经营者提供的相关产品或者服务； （四）以违反诚实信用和商业道德的其他方式不正当获取和使用他人商业数据，严重损害其他经营者和消费者的合法权	**第十九条** 经营者不得利用技术手段，非法获取、使用其他经营者合法持有的数据，妨碍、破坏其他经营者合法提供的网络产品或者服务的正常运行，扰乱市场公平竞争秩序。

《反法》	《反法草案》	《暂行规定》
	益，扰乱市场公平竞争秩序。 本法所称商业数据，是指经营者依法收集、具有商业价值并采取相应技术管理措施的数据。 获取、使用或者披露与公众可以无偿利用的信息相同的数据，不属于本条第一款所称不正当获取或者使用其他经营者商业数据。	

《暂行规定》第十九条可以理解为针对网络爬虫技术做出了限制性规定。在实际操作中，关于是否可以利用“爬虫”工具来搜集网站上的公开信息、用户发布的内容及评论，存在着不同的观点和争议。现行《反法》尚未对使用爬虫技术的行为作出明确规定，因此司法实践通常依据现行《反法》的第二条、第九条和第十二条第二款第四项对爬虫行为进行规制。具体来说，现行《反法》第二条为一般原则性规定；第九条为商业秘密相关条款；而第十二条第二款第四项为互联网专条的兜底性规定。为避免司法裁判过度依赖一般原则性规定来认定具体行为，一些法院在实践中倾向于仅根据《反法》第十二条第二款第四项来进行判断，并排除对第二条的引用。然而，第十二条自出台起就缺乏严格的法律构成要件，因此在解释时常常需要引用第二条的内容来进行补充说明。一般而言，法院会分别判断平台对被爬取数据是否拥有《反法》上可保护的权益、平台之间是否具有竞争关系、被抓取平台是否遭受损害以及抓取行为是否具有不正当性等因素。但在不同案件中，法院对于每个因素的判断标准不尽相同。例如，对于“被爬取数据是否具有《反法》下的权益”这一因素，在“淘宝诉美景生意参谋案”[53]中，法院将数据分为原始数据与衍生数据进行论述，并明确平台对于投入了大量智力劳动的衍生数据享有独立的财产性权益；而在“微博诉蚁坊案”[54]、“微博诉云智联案”[55]中，法院则是将数据分为公开数据与非公开数据两个维度，并明确对非公开数据的抓取行为不具有正当性，但对于公开数据，平台经营者应在一定程度上容忍他人合法的收集或利用。因此，在实际裁判中，数据爬取类的不正当竞争纠纷案件在很

[53] 参考浙江省杭州市中级人民法院[2018]浙 01 民终 7312 号判决书。
[54] 参考北京知识产权法院[2019]京 73 民终 3789 号判决书。
[55] 参考北京市海淀区人民法院[2017]京 0108 民初 24512 号判决书。

大程度上依赖于法官的自由裁量权，导致案件判决缺乏一致性，容易出现“同案不同判”的问题[56]。

为了满足对数据爬虫行为进行规范的实际需求，《反法草案》第十八条对数据爬虫行为进行了规定，并列举了四类典型行为，为司法实践提供法律依据。与之相比，《暂行规定》第十九条未对数据爬虫行为再进行细分列举，而是进行了概括性统一规定，要求经营者不得**“利用技术手段，非法获取、使用其他经营者合法持有的数据，妨碍、破坏其他经营者合法提供的网络产品或者服务的正常运行，扰乱市场公平竞争秩序”**，一定程度上**放宽了认定非法数据爬虫行为的门槛**。同时，根据《暂行规定》第十九条的规定，不再需要讨论被爬取数据的性质（公开或非公开、原始或衍生等），而是重点关注**被爬取数据是否为其他经营者“合法持有”**。根据此前公开的司法判例来看，对于这一点法院一般会从数据来源的合法性来进行论证，关注经营者是否通过平台协议（如隐私政策、用户协议等）获取用户的同意、是否在协议中明确约定数据的使用目的等。

（八）歧视待遇（第二十条）

《反法》	《反法草案》	《暂行规定》
/	**第十九条** 经营者不得利用算法，通过分析用户偏好、交易习惯等特征，在交易条件上对交易相对方实施不合理的差别待遇或者进行不合理限制，损害消费者、其他经营者的合法权益和社会公共利益，扰乱市场公平竞争秩序。	**第二十条** 经营者不得利用技术手段，对条件相同的交易相对方不合理地提供不同的交易条件，侵害交易相对方的选择权、公平交易权等，妨碍、破坏其他经营者合法提供的网络产品或者服务正常运行，扰乱市场公平交易秩序。 以下情形不属于前款规定的不正当竞争行为： （一）根据交易相对人实际需求且符合正当的交易习惯和行业惯例，实行不同交易条件；

[56] 参考孟洁，殷坤，《环球<反不正当竞争法（修订草案征求意见稿）>系列解读|之二：对网络爬虫技术从反法角度的再理解》，于 2024 年 5 月 17 日访问，https://mp.weixin.qq.com/s/vUBkRNJLQx05hNNWCYeuCA。

《反法》	《反法草案》	《暂行规定》
		（二）针对新用户在合理期限内开展的优惠活动； （三）基于公平、合理、无歧视的规则实施的随机性交易。

“大数据杀熟”是广大消费者普遍关注的热门话题。所谓“大数据杀熟”，是指平台企业通过收集、追踪用户数据，在利用数据挖掘技术对用户进行标签分类和分析预测的基础上，对特定用户进行歧视性定价，从而获得差额利润的行为。在2021年年底，浙江省绍兴市中级人民法院对“大数据杀熟第一案”[57]作出二审判决，认为被告某在线票务平台存在虚假宣传、价格欺诈和欺骗行为，支持原告退一赔三，但对于被告行为是否构成“大数据杀熟”并未作出认定；在随后出现的“郑某诉某在线票务平台案”[58]“刘某诉某外卖软件平台”[59]等中，法院也均未对此作出明确认定。

本次《暂行办法》第二十条从反不正当竞争规制的角度对“**大数据杀熟**”“**歧视待遇**”问题做出了正面回应。其实在《暂行办法》将此类行为纳入规制范围内之前，也已经有多部法律规范文件从多个角度尝试对这一现象进行管理和规范。例如，《中华人民共和国消费者权益保护法》第八条和第十条侧重于保护消费者权益，规定经营者必须如实告知商品或服务的真实情况（包括定价情况），同时禁止设置不公或不合理的交易条件；《电子商务法》第十八条则聚焦于信息展示，规定电商经营者应向消费者提供非个性化的搜索结果；《个人信息保护法》第二十四条侧重于保护个人信息主体权利，要求利用个人信息进行自动化决策时需保证决策的透明度和结果公平、公正，不得对个人在交易价格等交易条件上实行不合理的差别待遇；《反法》第十七条第一款第六项要求禁止对条件相同的交易相对人在交易价格等交易条件上实行差别待遇；《反法草案》第十九条第一次从反不正当竞争领域对大数据杀熟问题进行规制，要求经营者不得利用算法，通过分析用户偏好、交易习惯等特征，在交易条件上对交易相对方实施不合理的差别待遇或者进行不合理限制。

与《反法草案》相比，《暂行办法》第二十条额外提出了不得对“条件相同的交易相对方”实施大数据杀熟的限制条件，并新增了豁免条款。对于何为“条件相同的交易相对方”，《暂行办法》第二十条未做明确解释。宽泛而言，由于交易相

[57] 参考浙江省绍兴市中级人民法院（2021）浙06民终3129号判决书。
[58] 参考上海市第一中级人民法院（2020）沪01民终13989号判决书。
[59] 参考湖南省长沙市中级人民法院（2019）湘01民终9501号判决书。

对方在消费偏好、购买能力等各方面都存在差异，实践中几乎不存在条件完全相同的交易相对方。《国务院反垄断委员会关于平台经济领域的反垄断指南》第十七条曾对“条件相同”进行定义，即“条件相同是指交易相对人之间在交易安全、交易成本、信用状况、所处交易环节、交易持续时间等方面不存在实质性影响交易的差别。平台在交易中获取的交易相对人的隐私信息、交易历史、个体偏好、消费习惯等方面存在的差异不影响认定交易相对人条件相同”，一定程度上可以为《暂行办法》第二十条下“条件相同”提供借鉴参考依据。

在实践中，大数据算法作为企业的核心商业秘密，难以实现完全透明化，这种不透明性一定程度上掩盖了算法技术本身潜在的缺陷与问题，比如算法编写者可能带有的个人偏见，以及数据和机器自主学习过程中可能产生的偏见。诸如此类不易察觉的问题在行业内被称为“算法黑箱”。算法黑箱的存在不仅可能催生甚至会加剧算法偏见，进而成为导致“大数据杀熟”现象的一个间接且不容忽视的诱因。因此，近年来颁布的算法相关法律法规也对此进行了规制。例如，《互联网信息服务算法推荐管理规定》第二十一条明确规定，不得根据消费者的偏好、交易习惯等特征，利用算法在交易价格等交易条件上实施不合理的差别待遇等违法行为。《生成式人工智能服务管理暂行办法》第四条规定，在算法设计、训练数据选择、模型生成和优化、提供服务等过程中，采取有效措施防止产生民族、信仰、国别、地域、性别、年龄、职业、健康等歧视。对此，我们也提示企业在涉及提供算法服务时，应注意制定和公开完善的算法推荐服务相关规则，综合运用内容去重、打散干预等策略，并优化检索、排序、选择、推送、展示等规则的透明度和可解释性，避免对用户产生不良影响，预防和减少争议纠纷。

三、结语

《暂行规定》的出台标志着我国对网络不正当竞争行为的规制进入了新的阶段。该规定紧扣互联网领域新态势与新变化，对网络不正当竞争行为进行了较为全面的规制。

对于经营者而言，应高度重视《暂行规定》的互联网条款，在日常运营过程中的各阶段确保做到如下要求：

- 在软件开发和运营阶段，遵循公平竞争原则，避免开发恶意不兼容的产品或者会干扰、破坏或修改其他应用正常运行的功能等；
- 在推广和营销阶段，建立完善的内部合规机制，并定期自查是否履行合规义务，包括但不限于严禁未经其他经营者同意私自通过技术手段在其平台中插入链接或者强制进行目标跳转，以此吸引用户流量；避免采用高频次交易、虚假好评、恶意拍货不付款或恶意退货等手段来干扰市场秩序；实时监控交易行为并不断优化评价系统，以预防反向刷单等不正当行为；不得恶意拦截、屏蔽其他经营者合法提供的信息内容以及页面等；

- 在数据收集和使用阶段，建立完善的数据全流程管理制度，在收集使用数据前确保获得合法授权，避免利用技术手段非法爬取、使用其他经营者合法持有的数据；
- 在消费者权益保障方面，应定期审查定价机制及算法，确保用户在相同条件下享受同等价格和待遇，避免发生大数据杀熟、算法歧视的情况。

此外，平台类经营者还应注意，一方面应加强对内部竞争行为的规范管理，明确平台内竞争行为的规范标准，包括但不限于对平台内经营者的入驻审核、商品信息展示、交易流程等方面进行规范管理，以确保公平竞争和保障消费者权益；另一方面应从自身入手，避免出现对平台内经营者进行交易限制以及不合理收费等行为。

6. 测绘信息安全：解读《自然资源部关于加强智能网联汽车有关测绘地理信息安全管理的通知》：安全为基，智驭未来[60]

近年来，我国出台了智能网联汽车相关的各类测绘地理信息管理地方法规、政策，全国各地纷纷展开探索测绘领域的探索并加强测绘安全管理。2022 年 8 月 30 日，自然资源部发布《自然资源部关于促进智能网联汽车发展维护测绘地理信息安全的通知》（以下简称“自然资规〔2022〕1 号”），对汽车行业的测绘监管问题提出明确要求，对测绘活动的范围等关键问题做出了解答。随着测绘行业的不断发展，2023 年 8 月 22 日，自然资源部发布《自然资源部关于加快测绘地理信息事业转型升级 更好支撑高质量发展的意见》（以下简称“《2023 版意见》”），提出加快推进测绘地理信息事业转型升级和产业发展，在严守测绘地理信息管理底线的前提下，激活测绘地理信息数据要素潜能，大力促进测绘地理信息在智能网联汽车业态发展中的应用。在智能网联汽车“高精度地图应用试点”和“车路云一体化”应用试点蓬勃发展的大背景之下，2024 年 7 月 26 日，结合新能源汽车路测和数据采集技术的发展，自然资源部发布《自然资源部关于加强智能网联汽车有关测绘地理信息安全管理的通知》（自然资发〔2024〕139 号）（以下简称“《通知》”），《通知》共十项内容，对自然资规〔2022〕1 号进行了进一步细化。

此次《通知》虽然仅有十条规定，但解答了近年来困扰智能网联汽车测绘领域的重要问题，一方面，顺应和承接了自然资规〔2022〕1 号以及《2023 版意见》的方向和概念[61]，另一方面，从政策导向上较自然资规〔2022〕1 号体现了从严管理的态势。下文将对此次《通知》的要点内容进行分析和解读，以期能为读者提供助益。

一、关于测绘主体与测绘行为的认定与范围

（一）沿用对测绘主体的定义

《通知》沿用了自然资规〔2022〕1 号对测绘主体的定义，根据自然资规〔2022〕1 号，对智能网联汽车运行、服务和道路测试过程中产生的空间坐标、影像、点云及其属性信息等测绘地理信息数据进行收集、存储、传输和处理者，是测绘活动的行为主体，应遵守相关规定并依法承担相应责任。自然资规〔2022〕1 号也明确了测绘主体的角色，车企、服务商及部分智能驾驶软件提供商是主要的数据的收集、存储、传输和处理者，属于测绘主体，同时，仅获得辅助驾驶等服务的智能网联汽车驾乘人员，则不属于测绘活动的行为人。

---

[60] 作者：孟洁、殷坤、吉文行、田梓仪

[61] 呼应了《2023 版意见》的政策要求，加快推进新型基础测绘体系和实景三维中国建设，夯实公共数据资源，《通知》第八条规定，各地要及时提供北斗卫星导航定位基准站“一张网”位置服务，不断提升天地图在线服务能力，推进“实景三维中国”、地理信息要素等公共数据资源在智能网联汽车发展中的共享应用。

实践中，根据部分地方测绘监管部门的态度，测绘行为主体的认定需要考量多种因素，除符合法律要件的数据获取方会被认定为测绘主体外，测绘活动的最终获利方以及最终提供服务方均有可能会被认定为测绘行为主体，因此可能需要取得相应的测绘资质。例如，车企通过招募车主的方式进行路测数据的采集，最终用于导航电子地图等的制作或更新，在该场景下，虽然车主作为智能网联汽车驾乘人员，按照规定不属于测绘活动的行为人，但鉴于企业依靠用户获取数据并且数据最终汇聚在企业，为企业创造价值，企业实际作为数据采集活动的行为主体，从一定意义上来说，企业作为最终的数据受益方和管理者，仍然需要取得相应的测绘资质。

值得注意的是，由于部分测绘资质限制外资进入，外资企业需委托相应测绘资质单位进行测绘活动。例如，根据《外商投资准入特别管理措施（负面清单）（2021 年版）》的规定，地面移动测量、导航电子地图编制等属外资禁入领域。需要从事相关数据收集、存储、传输和处理的车企、服务商及智能驾驶软件提供商等，属于外商投资企业的，应委托具有相应测绘资质的单位开展测绘活动，由被委托的测绘资质单位承担收集、存储、传输和处理相关空间坐标、影像、点云及其属性信息等业务及提供地理信息服务与支持。

对于未具备相应测绘资质的主体，如需开展测绘相关活动，则需要在特定的范围内并履行相应的审批程序。例如，根据《北京市智能网联汽车高精度地图试点工作指导意见》，非测绘资质单位，在示范区域内，应用智能网联汽车高精度地图开展测试、应用、商业运营服务等活动时，使用的高精度地图应是经依法审核批准的。

（二）进一步厘清测绘活动的范围

《通知》细化了《测绘法》与自然资规〔2022〕1 号对测绘活动的定义。《测绘法》最对测绘活动给出了指导性的定义，即测绘活动指对自然地理要素或者地表人工设施的形状、大小、空间位置及其属性等进行测定、采集、表述，以及对获取的数据、信息、成果进行处理和提供的活动，但该定义较为宽泛和模糊，解释具有较强的不确定性，对企业开展测绘业务的实操层面指导性不强。此后，2022 年发布的自然资规〔2022〕1 号在《测绘法》的基础上对测绘活动给出了解释性的细化规定，明确了数据采集装置的类型（安装或集成了卫星导航定位接收模块、惯性测量单元、摄像头、激光雷达等传感器），数据采集对象的范围（车辆及周边道路设施空间坐标、影像、点云及其属性信息等测绘地理信息数据），并明确了智能网联汽车测绘活动的适用场景（即在运行、服务和道路测试场景下的数据采集、存储、传输和处理活动），并明确了各类车载传感器以及智能网联汽车的制造、集成、销售等行为不属于法定的测绘活动。

随着近几年自动驾驶示范与应用、高精度地图的不断试点、道路测试的持续发展，智能网联汽车对导航电子地图的实时更新需求越发增强，企业对数据采集的需求和采集方式不断创新。在此背景下，《通知》规定智能网联汽车在运行、服务和测试过程中,对车辆及周边道路设施的空间坐标、**实景影像（视频和影像等环境感知数据）**、点云及其属性信息等地理信息数据**（含道路拓扑数据）**进行采集、存储、传输和处理的行为，属于测绘活动。就此，《通知》进一步补充了自然资规〔2022〕1 号中规定的测绘活动类型，将“影像”进一步明确为实景影像（视频和影像等环境感知数据），即智能网联汽车通过摄像头拍摄的车外实景视频和影像等环境感知数据也属于测绘活动。

在此之前，虽然自然资规〔2022〕1 号对测绘活动的定义中包括处理“影像”等测绘地理信息数据，但企业对于拍摄道路周边视频的行为是否属于测绘行为，拍摄视频的精度是否会对测绘行为的性质产生影响，以及企业需要取得何种测绘资质仍存在较多疑惑。此次《通知》对拍摄车外视频行为给出了明确的解答。实践中，基于项目经验，企业如涉及采集视频，应当根据采集的数据精度以及后续使用目的，综合判断是否需要相应测绘资质，例如，如仅涉及视频采集还是可能对视频进行加工处理（例如对视频中人脸和车牌做脱敏处理等），资质类别还应根据实际情况进行判断。

虽然此次《通知》未明确测绘行为的例外情形，但目前有些地方规定也在对非测绘行为的情形进行探索。例如，《北京市自动驾驶汽车条例（征求意见稿）》第三十四条规定了利用自动驾驶汽车开展测绘活动的例外情况，即利用自动驾驶汽车只对车辆及周边道路设施的形状、大小、空间位置及其属性进行测定以用于在车端临时构图，且不在自动驾驶汽车上存储，亦不向车外传输有关地理信息数据的除外。这意味着，如不涉及对地理信息数据进行实际的收集存储活动，则不属于开展测绘活动。但需要注意的是，《北京市自动驾驶汽车条例（征求意见稿）》于 2024 年 6 月 30 日发布，时间早于《2023 版意见》，因此《2023 版意见》对于《北京市自动驾驶汽车条例（征求意见稿）》的影响还有待后续进一步观察。

（三）对众源采集模式的进一步探索

近年来，国家持续探索测绘地理信息的潜能和多元化发展。《2023 版意见》提出将开放基础数据资源，加工和编制多尺度、多类型的公众版测绘成果，推动测绘地理信息数据安全有序开放。2022 年 10 月，上海市规划和自然资源局曾发布《上海市智能网联汽车高精度地图管理试点规定（草案）》征求意见，第七条[62]提出对于具有导航电子地图制作测绘资质的单位，鼓励其探索以“众源”方式采集测绘地理信息数据，制作和更新高精度地图。在此背景下，此次《通知》对

[62] 《上海市智能网联汽车高精度地图管理试点规定（草案）》第七条，鼓励具有导航电子地图制作测绘资质的单位，在确保数据安全、处理好知识产权等关系的前提下，探索以众源方式采集测绘地理信息数据，运用实时加密传输及实时安全审校等技术手段，制作和更新高精度地图。

“众源采集”使用了**“支持探索”**的鼓励态度[63]，虽然未对众源采集的主体给出确定性的指向，但明确了在确保安全合规的前提下对对众源采集方式的支持态度，一定程度上打消了企业对众源采集方式的疑虑。

二、关于测绘数据的类型划分

我国目前的法律法规中尚未对于“测绘数据”这一概念进行明确定义。为便于理解，我们将测绘活动所涉及的数据统称为“测绘数据”。

（一）测绘数据可能涉及的数据类型

根据《通知》的规定，智能网络汽车场景下的测绘数据涉及**智能网联汽车在运行、服务和测试过程中,对车辆及周边道路设施的空间坐标、实景影像（视频和影像等环境感知数据）、点云及其属性信息等地理信息数据（含道路拓扑数据）**。根据测绘活动的业务特点并按照数据属性划分，智能网联汽车场景下的测绘数据还可能涉及以下类型（**下述各数据类型在范围上可能相互重叠**）：

数据类型	具体描述
汽车数据	《汽车数据安全管理若干规定（试行）》：汽车数据包括汽车设计、生产、销售、使用、运维等过程中的涉及个人信息数据[64]和重要数据。
时空数据	《智能网联汽车时空数据安全处理基本要求（征求意见稿）》：具有时间、空间特征的地理信息数据。 时空数据包括以下 5 种数据类型： a)位置类：车端收集到的能确定车辆在地球上绝对位置的坐标数据； b)点云类：时空数据传感器收集到的点云数据； c)影像类：时空数据传感器收集到的图像或视频数据； d)惯导类：时空数据传感器获取到的车辆姿态角(或角速率)、加速度及其衍生数据； e)构图类：对上述数据进行加工生成的含有绝对位置坐标的矢量数据。

63 《通知》明确在确保安全合规的前提下，支持车企、服务单位探索智能网联汽车地理信息数据众源采集、实时更新、在线分发、安全传输等安全合规技术路线。

64 《汽车数据安全管理若干规定（试行）》第三条：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车主、驾驶人、乘车人、车外人员等有关的各种信息，不包括匿名化处理后的信息。
敏感个人信息，是指一旦泄露或者非法使用，可能导致车主、驾驶人、乘车人、车外人员等受到歧视或者人身、财产安全受到严重危害的个人信息，包括车辆行踪轨迹、音频、视频、图像和生物识别特征等信息。

数据类型	具体描述
导航地图数据	《GB 20263-2006 导航电子地图安全处理技术基本要求》：含有空间位置地理坐标，能够与空间定位信息系统结合，准确引导人或交通工具从出发地到达目的地的电子地图或数据集。
基础地理信息数据	《GB 21139-2007 基础地理信息标准数据基本规定》：作为统一的空间定位框架和空间分析基础的地理信息数据,该数据反映和描述了地球表面测量控制点、水系、居民地及设施、交通、管线、境界与政区、地貌、植被与土质、地籍、地名等有关自然和社会要素的位置、形态和属性等信息。
重要地理信息数据	《中华人民共和国测绘成果管理条例》：包括：（一）国界、国家海岸线长度；（二）领土、领海、毗连区、专属经济区面积；（三）国家海岸滩涂面积、岛礁数量和面积；（四）国家版图的重要特征点，地势、地貌分区位置；（五）国务院测绘行政主管部门商国务院其他有关部门确定的其他重要自然和人文地理实体的位置、高程、深度、面积、长度等地理信息数据。

而根据数据的敏感程度划分，智能网联汽车场景下的测绘数据也可分为一般数据、重要数据、涉密数据。其中，《通知》所述“涉密、敏感地理信息数据”可能包括如下类型（**下述各数据类型在范围上可能相互重叠**）：

数据类型	具体描述
涉密测绘成果[65]	《测绘地理信息管理工作国家秘密目录》 • **国家秘密**：军事禁区以外平面精度优于（含）10 米或地物高度相对量测精度优于（含）5%、且连续覆盖范围超过 25 平方千米的三维模型、点云、倾斜影像、实景影像、导航电子地图等实测成果。 • **国家机密**：军事禁区平面精度优于（含）10 米或地物高度相对量测精度优于（含）5%的三维模型、点云、倾斜影像、实景影像、导航电子地图等实测成果。
	《关于加强自动驾驶地图生产测试与应用管理的通知》 • **用于自动驾驶技术试验、道路测试的地图数据（包括在传统导航电子地图基础上增添内容、要素或精度提升的）**，应当按照涉密测绘成果进行管理。

[65] 参见《测绘地理信息管理工作国家秘密范围的规定》（自然资源发〔2020〕95 号）及附件《测绘地理信息管理工作国家秘密目录》。

数据类型	具体描述
重要数据[66]	《GB/T 43697-2024 数据安全技术 数据分类分级规则》附录 G 重要数据识别指南 • 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,如**满足一定精度指标的地理数据**或与战略物资产能、储备最有关的数据。 • **反映重点目标、重要场所物理安全保护情况或未公开地理目标的位置**,可被恐怖分子、犯罪分子利用实施破坏,如描述重点安保单位、重要生产企业、国家重要资产(如铁路、输油管道)的施工图、内部结构、安防情况的数据。
重要数据（汽车数据）[67]	《汽车数据安全管理若干规定（试行）》 • 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； • 包含人脸信息、车牌信息等的**车外视频、图像数据**； • 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。

根据不同数据类型及敏感程度的划分，企业除了需要注意《通知》中的相关规定，还应当注意履行相对应法律法规中的合规义务。例如，测绘阶段所收集的测绘数据如落入《汽车数据安全管理若干规定（试行）》中汽车数据范畴的，则需要履行车内处理、默认不收集等处理原则；另外，根据敏感级别，如构成汽车领域重要数据的，则还需要履行报送风险评估报告、年度汽车安全管理情况等合规义务。

（二）《通知》对测绘数据的安全要求

1、数据传输要求

《通知》第五条明确强调企业应当“确保智能网联汽车采集、收集的**用于导航相关活动以及地图制作、更新的地理信息数据，直接传输**至具备导航电子地图制作测绘资质的单位管理，其他单位或个人不得接触。”因此，在地理信息数据的传输过程中，企业应当进一步审视车企与图商之间的数据传输链路及合作模式，进行人员权限与访问控制，使用安全的传输通道并采取必要的保密措施，以防止任何未获授权单位或个人非法接触。

[66] 参见《GB/T 43697-2024 数据安全技术 数据分类分级规则》，附录 G 重要数据识别指南 b）e)。
[67] 参见《汽车数据安全管理若干规定（试行）》第三条。

2、数据存储和对外提供的要求

《通知》第五条还明确规定，“地理信息数据必须**存储于境内**，所使用的存储设备、网络和云服务等必须符合国家有关安全和保密要求。申请向境外提供地理信息数据的，**必须严格履行对外提供审批或地图审核程序，并落实数据出境安全评估等有关规定**。”具体而言，本条可以理解为如下三个方面的要求：

首先，智能网联汽车场景下收集的地理信息数据，无论是否涉密，均应当存储于我国境内，并使用符合国家安全和保密要求的设备、网络和云服务器进行存储。

其次，企业不得擅自向境外提供地理信息数据，若申请出境的需要履行对外提供审批或地图审核程序。但是在实操中，如何落实具体的审批或审核程序仍有待澄清之处。在“对外提供审批”方面，针对涉密测绘成果的对外提供审批，与《通知》同期发布的《对外提供涉密测绘成果管理办法》（自然资规〔2024〕2 号）详细规定了分级审批制度和对外提供的申请条件（具体内容可参见团队文章“AI助理”解读新法规（四）：自然资源部发布《对外提供涉密测绘成果管理办法》。而对外提供不属于涉密测绘成果的地理信息数据，在“对外提供审批”方面，未来是否会建立专门的审批要求，仍待相关主管部门进一步明确。

在“地图审核”方面，《地图审核管理规定》《关于导航电子地图管理有关规定的通知》等相关法律法规仅规定了地图在出版、展示和使用等环节前的审核要求，未具体到“向境外提供”，这是否参照适用已有法律法规的审核要求，还是将另行适用专门的审核程序，也有待实践中相关主管部门的解答。

最后，如涉密测绘成果一旦落入公开发布的重要数据目录（例如《汽车数据安全管理若干规定（试行）》中规定的重要数据），或者被明确告知属于重要数据的，以及在主管部门进行前述审批过程中告知企业涉及重要数据处理行为的，**企业应当在满足上述对外提供审批或地图审核的同时，另行履行数据出境安全评估等义务**。

3、对涉密、敏感地理信息的特殊安全要求

对于涉密、敏感的地理信息则需要在前述基础上进行更加严格的安全管理。《通知》第三条针对**测绘资质单位**提出了对于涉密、敏感的地理信息安全措施要求，包括：

- **强化涉密、敏感地理信息的安全管理：**强化对属于国家秘密的导航电子地图、实景影像、点云等实测成果，以及智能网联汽车采集、收集、存储、传输和处理的包含涉密、敏感内容的地理信息数据（含场景库）管理，不得擅自提供涉密或敏感地理信息。

- **采用地理信息保密处理技术：**未经国家认定的地理信息保密处理技术进行处理的数据，其秘密等级不低于处理前秘密等级。[68]

而对于智能网联汽车企业，《通知》中虽未明确规定其对于涉密、敏感地理信息的安全义务，但也应当注意履行相关法律法规规定的特殊合规要求，包括但不限于：

- **传输：**根据涉密级别履行相应合规要求，例如，对于国家秘密禁止通过互联网及其他公共信息网络或者未采取保密措施的有线和无线通信中传输[69]；
- **向境外提供：**不得擅自向境外提供涉密测绘成果，应当符合《对外提供涉密测绘成果管理办法》的规定；
- **存储与管理：**企业应当根据《关于加强涉密测绘地理信息安全管理的通知》《关于进一步贯彻落实测绘成果核心涉密人员保密管理制度的通知》等法律法规落实有关存储设施、信息系统建设、组织管理等方面的要求[70]。

三、强调导航电子地图测绘资质的要求与对应的合规义务

（一）扩大导航电子地图范围

《通知》进一步收紧了导航电子地图相关的测绘行为管理要求，《通知》扩大了导航电子地图的范围，智能网联汽车使用的**基础地图**、高级辅助驾驶地图、高精度地图、自动驾驶地图等此次均被纳入导航电子地图的范畴内，从而全面增强了对智能联网汽车的监管态势。导航电子地图是指，含有空间位置地理坐标，能够与空间定位系统结合，准确引导人或交通工具从出发地到达目的地的电子地图或数据集。

根据国家测绘地理信息局 2016 年发布的《关于加强自动驾驶地图生产测试与应用管理的通知》（国测成发〔2016〕2 号），自动驾驶地图因其在精度和属性内容等方面具有不同于传统导航电子地图的特点，将其定义为导航电子地图的新型种类和重要组成部分，其数据采集、编辑加工和生产制作必须由具有导航电子地图制作测绘资质的单位承担，并且，企业用于自动驾驶技术试验、道路测试的地图数据(包括在传统导航电子地图基础上增添内容、要素或精度提升的)，还应当按照涉密测绘成果进行管理。此次规定明确了智能网联车场景下的基础地图属

[68] 自然资源部发布的《自然资源部办公厅关于推进地理信息保密处理技术研发和服务工作的通知》（自然资办发〔2021〕22 号）、《地理信息保密处理技术认定工作程序（试行）》（自然资地信函[2022] 51 号）等相关法律法规对地理信息保密技术的认定进行了规范。

[69] 参见《中华人民共和国测绘成果管理条例》《中华人民共和国保守国家秘密法实施条例》。

[70] 《中华人民共和国测绘成果管理条例》第十一条。

于导航电子地图，相关地图数据的处理需要具备导航电子地图制作资质或委托具备导航电子地图制作资质的图商进行处理。

目前，关于导航电子地图相关规定主要参照 2007 年《国家测绘局关于导航电子地图管理有关规定的通知》，此次《通知》明确强调要“从严审核把关导航电子地图”，因此监管导航审核电子地图相关资质可能将更加严格。

在此次《通知》发布之前，对于智能网联车数据采集和地图编制活动需要具备何种测绘资质主要依据《测绘资质管理办法和测绘资质分类分级标准》（自然资办发[2021]43 号）中《专业标准》所列明的各类测绘资质的业务范围。企业如遇到特殊测绘场景，建议需要与各地方自然资源管理局等测绘主管部门工作人员进行个案咨询，基于所进行的测绘业务所涉数据处理行为的类别和程度，以及采集数据的类型和范围等多重考量因素，综合判断并评定开展业务所需的测绘资质类别和等级。一般而言，企业在测绘领域主要涉及的测绘资质如下表。

序号	专业类别	
	测绘资质名称	业务类型
1	测绘航空摄影	一般航摄、无人飞行器航摄、倾斜航摄
2	摄影测量与遥感	摄影测量与遥感外业、摄影测量与遥感内业、摄影测量与遥感监理
3	地理信息系统工程	地理信息数据采集、地理信息数据处理、地理信息系统及数据库建设、地面移动测量、地理信息软件开发、地理信息系统工程监理
4	地图编制	地形图、教学地图、世界政区地图、全国及地方政区地图、电子地图、真三维地图、其他专用地图
5	导航电子地图制作	导航电子地图制作
6	互联网地图服务	地理位置定位、地理信息上传标注、地图数据库开发

同时，考量到乙级导航电子地图制作资质仅限于在相关政府部门划定的自动驾驶区域内从事导航电子地图制作，因此，未来对于甲级导航电子地图制作资质的需求将会越来越大，鉴于实践中甲导资质取得的难度较大，具备相应资质的图商可能将在与车企的合作中发挥更深入的作用。

（二）加强导航电子地图数据处理要求

《通知》在明确了导航电子地图制作资质范围的基础上，加强了地理信息数据处理全生命周期的处理要求。首先，从企业数据收集源头和数据处理目的出发，要求智能网联汽车**采集、收集的用于导航相关活动**以及**地图制作、更新**的地理信息数据，直接传输至具备导航电子地图制作测绘资质的单位管理，其他单位或个人不得接触。该规定也顺应了《国家测绘局关于导航电子地图管理有关规定的通知》的规定，即除依法取得导航电子地图测绘资质的外，其他单位和个人在使用导航电子地图过程中，不得携带其他带有空间定位系统（如 GPS 等）信号接收、定位功能的仪器开展显示、记录、存储、标注空间坐标、高程、地物属性信息，以及检测、校核、更改导航电子地图相关内容等测绘活动，并进一步强调其他单位和个人不得接触该些数据。这意味着，不具备导航电子地图制作资质的企业不得将收集的该些数据存储在自有数据库中，也不得将数据用于地图标注、地图更新等任何加工活动，必须直接传输给具备资质的单位处理。

并且，《通知》规定对智能网联汽车回传的地理信息数据进行收集、存储、传输、处理以及地图制作等活动应由具有导航电子地图制作等测绘资质的单位承担。如企业作为车企且尚未具备导航电子地图测绘资质的，涉及测绘活动，应当严格审查数据处理供应商资质，并确保在不接触地理信息数据的前提下向有资质的单位回传所有地理信息数据。

（三）强化导航电子地图审核

为适应智能网联汽车导航电子地图测试、应用、商业运营服务等需求，《通知》在从严审核把关导航电子地图基础上，既要求各地要依法实施地图审核，强化对导航电子地图制作测绘资质单位和车企的指导监督，确保地图通过审核后才能提供使用，同时也强调了地图新增地理信息内容必须进行安全审校，并及时备案。

根据《地图管理条例》，向社会公开的地图，应当报送有审核权的测绘地理信息行政主管部门审核。自然资源主管部门在自受理地图审核申请之日起 20 个工作日内作出审核决定。[71]但目前对导航电子地图的备案要求仍有待有关部门进一步明确。后续监管是否可能参照互联网地图的管理规定，就审核通过的互联网地图服务，要求申请人每六个月将新增标注内容及核查校对情况向作出审核批准的自然资源主管部门备案，[72]也将有待于后续的实践观察。随着智能网联汽车及自动驾驶技术的持续发展，《通知》也呼应了各地陆续发布管理高精度地图试点等工作的通知，例如，2023 年，《北京市智能网联汽车高精度地图试点工作指导意见》提出探索审图方式，导航电子地图制作资质单位要建立增量更新内容安全审校制度，对可能涉密或敏感地理信息数据严格进行在线过滤和审查把关。支持企

71 《地图审核管理规定》第二十四条。
72 《地图审核管理规定》第二十八条。

业研发增量更新等快速审图技术，探索快速审核模式，在适当条件下试行企业责任制快速增量审图制度，优化审查系统，提高审图效率。

后续企业可持续关注各地区陆续发布的地图试点工作通知，用于进一步指导审图和备案工作。

四、结语

此次《通知》针对智能网联汽车测绘的关键问题做出了细化说明，回应了近几年困扰车企以及图商等汽车企业的测绘合规操作困境，既明确了智能网联汽车测绘行业的数据合规底线，也提出了在汽车行业快速发展的大背景下确保数据安全的强化要求，确保测绘数据及涉密测绘成果安全，在维护国家安全的前提下，进一步促进智能网联企业行业的有序发展。建议企业尽快审查内部测绘成果管理机制和传输现状，同时关注国家和地方后续陆续发布的相关衔接性规定，严格落实《通知》、自然资规〔2022〕1 号等的合规要求。

附件：

规范名称	发文机关	发布/生效日期
法律		
《中华人民共和国测绘法》（2017 年修订）	全国人大常委会	2017 年 7 月 1 日生效
行政法规/部门规章		
《地图管理条例》	国务院	2016 年 1 月 1 日生效
《地图审核管理规定》	自然资源部	2019 年 7 月 24 日生效
《外国的组织或者个人来华测绘管理暂行办法》（2019 修正）	自然资源部	2019 年 7 月 24 日生效
规范性文件		
《对外提供涉密测绘成果管理办法》	**自然资源部**	**2024 年 7 月 26 日生效**
《自然资源部关于加强智能网联汽车有关测绘地理信息安全管理的通知》	**自然资源部**	**2024 年 7 月 26 日生效**
《自然资源部关于加快测绘地理信息事业转型升级 更好支撑高质量发展的意见》	自然资源部	2023 年 8 月 22 日生效

规范名称	发文机关	发布/生效日期
《关于促进智能网联汽车发展维护测绘地理信息安全的通知》	自然资源部	2022 年 8 月 25 日生效
《关于加强自动驾驶地图生产测试与应用管理的通知》	国家测绘地理信息局（已撤销）	2016 年 2 月 3 日生效
《关于导航电子地图管理有关规定的通知》	国家测绘地理信息局（已撤销）	2007 年 11 月 19 日生效
政策性文件		
《智能汽车创新发展战略》	国家发改委、中央网信办、工信部等	2020 年 2 月 10 日生效
国家标准		
《导航电子地图安全处理技术基本要求》（GB 20263-2006）	国家测绘地理信息局（已撤销）	2012 年 1 月 16 日生效
《基础地理信息标准数据基本规定（征求意见稿）》	自然资源部	2024 年 7 月 5 日发布
《智能网联汽车时空数据安全处理基本要求（征求意见稿）》	自然资源部	2024 年 6 月 25 日发布
《智能网联汽车时空数据传感系统安全基本要求（征求意见稿）》	自然资源部	2024 年 6 月 25 日发布
地方性法规/规范性文件		
《关于开展北京市智能网联汽车高精度地图审图工作的通知》	北京市规划与自然资源委员会	2023 年 3 月 31 日生效
《北京市智能网联汽车高精度地图试点工作指导意见》	北京市规划和自然资源委员会 北京市经济和信息化局	2023 年 3 月 28 日生效
《北京市智能汽车基础地图应用试点暂行规定》	北京市规划和自然资源委员会 北京市经济和信息化局	2020 年 12 月 22 日生效
《上海市智能网联汽车高精度地图管理试点规定》	上海市规划和自然资源局	2022 年 11 月 28 日生效

规范名称	发文机关	发布/生效日期
《上海市加快智能网联汽车创新发展实施方案》	上海市人民政府办公厅	2022 年 8 月 23 日生效
《广州市智能网联汽车创新发展条例（草案修改稿 征求意见稿）》	广州市人大常委会	2024 年 7 月 25 日发布
山东省《强化测绘地理信息要素保障更好支撑全省绿色低碳高质量发展若干措施》	山东省自然资源厅	2024 年 7 月 16 日生效
《宁波市测绘地理信息管理办法》	宁波市人民政府	2024 年 3 月 1 日生效
《湖南省测绘地理信息条例》	湖南省人大常委会	2024 年 1 月 1 日生效
《辽宁省测绘地理信息条例》	辽宁省人大常委会	2020 年 12 月 1 日生效
《安徽省自然资源厅关于加快测绘地理信息事业转型升级更好支撑高质量发展的实施意见》	安徽省自然资源厅	2023 年 12 月 24 日生效
江苏省《关于印发加快推进车联网和智能网联汽车高质量发展指导意见的通知》	江苏省工业和信息化厅	2022 年 6 月 1 日生效
《重庆市智能网联汽车高精度地图管理试行办法》	重庆市规划和自然资源局	2022 年 4 月 25 日生效
四川省《关于推进智能网联汽车产业发展的通知》	四川省经济和信息化厅等	2020 年 5 月 12 日生效

7. 平台运营资质：应用程序分发平台对 App 运营者的资质审核机制分析[73]

在当今数字化时代，应用程序分发平台作为连接开发者与用户的关键枢纽，其审核机制的健全性与有效性直接关乎整个应用生态的健康发展。自 2019 年，中央网信办、工信部、公安部、市场监管总局等部门开展多项执法行动，将监管范围从 App 拓展至 SDK 提供者、应用分发平台、互联网平台等，监管焦点也延伸至算法、推荐机制、平台责任等层面。应用程序分发平台也被要求落实管理责任、对 App 上架进行严格审核。应用程序分发平台作为应用程序分发的把关人，应承担平台治理职责，不仅要提供应用分发服务，更要对平台内的应用程序及开发者进行有效管理。在此背景下，深入探讨分发平台的审核机制、明确其审核义务、剖析潜在风险并提出合规建议显得尤为重要。

本文将围绕应用程序分发平台对 App 运营者的资质审查义务这一主题展开探讨。首先，梳理我国现行规范框架下应用程序分发平台的相关规定，其次，围绕资质审核，为分发平台以及应用程序提供者自身提出具有针对性和可操作性的合规建议，助力双方更好地履行各自的责任与义务。最后，通过对比国内主流应用程序分发平台的资质审查机制，剖析其异同之处，以期为应用程序市场的参与者提供全面且有价值的参考，共同促进应用程序行业的健康、有序发展。

一、我国应用程序分发平台审核机制的监管框架

2016 年 12 月 16 日，工业和信息化部发布《移动智能终端应用软件预置和分发管理暂行规定》，最早明确移动应用分发平台应建立应用软件管理机制，规定了移动应用分发平台承担对应用软件的审核及相关检测责任，开启了对平台监管的要求。此后，国家分别相继出台相关规定，重点围绕个人信息保护、网络数据安全、分类管理、实名认证、资质审核等多维度，对移动分发平台的审核维度进行了规定。其中，国家互联网信息办公室于 2022 年 6 月 14 日发布的《移动互联网应用程序信息服务管理规定》（下称“《规定》”）明确区分了应用程序提供者和应用程序分发平台两类角色，对应用程序分发平台的义务进行了较为全面的规定。现将主要法规所涉的分发平台对应用程序的审核义务梳理如下，以供参考：

[73] 作者：孟洁、殷坤、吉文行

法律法规	相关内容
《网络数据安全管理条例》	第四十一条，**提供应用程序分发服务的网络平台服务提供者，应当建立应用程序核验规则并开展网络数据安全相关核验**。发现待分发或者已分发的应用程序不符合法律、行政法规的规定或者国家标准的强制性要求的，应当采取警示、不予分发、暂停分发或者终止分发等措施。
《移动互联网应用程序信息服务管理规定》	第七条，应用程序提供者通过应用程序提供互联网新闻信息服务的，应当取得互联网新闻信息服务许可，禁止未经许可或者超越许可范围开展互联网新闻信息服务活动。 **应用程序提供者提供其他互联网信息服务，依法须经有关主管部门审核同意或者取得相关许可的，经有关主管部门审核同意或者取得相关许可后方可提供服务**。 第二十条　应用程序分发平台应当建立健全管理机制和技术手段，建立完善上架审核、日常管理、应急处置等管理措施。……**应用程序提供的信息服务属于本规定第七条规定范围的，应用程序分发平台应当对相关许可等情况进行核验**……。
《移动智能终端应用软件预置和分发管理暂行规定》（工信部信管[2016]407号）	第八条　从事应用商店等移动应用分发平台服务的互联网信息服务提供者，以及在移动智能终端中预置了移动应用分发平台的生产企业对所提供的应用软件负有以下管理责任： （一）应登记应用软件提供者、运营者、开发者的真实身份、联系方式等信息。 （二）**应建立应用软件管理机制，对应用软件进行审核及安全、服务等相关检测，对审核和检测中发现的恶意应用软件等违法违规软件，不得向用户提供**；对所提供应用软件进行跟踪监测，及时处理违法违规软件，建立完善用户举报投诉处置措施等。

法律法规	相关内容
《工业和信息化部关于开展 APP 侵害用户权益专项整治工作的通知》（工信部信管函〔2019〕337 号）	二、整治对象 本次专项整治工作主要面向两类对象：一是 APP 服务提供者，主要检查是否存在前述 8 类问题；二是 **APP 分发服务提供者，含应用商店和基础电信企业营业厅等承担 APP 分发功能的各类企业，主要检查是否落实《移动智能终端应用软件预置和分发管理暂行规定》（工信部信管〔2016〕407 号）等有关要求**。
《工业和信息化部关于开展纵深推进 APP 侵害用户权益专项整治行动的通知》（工信部信管函〔2020〕164 号）	10.**应用分发平台管理责任落实不到位。重点整治 APP 上架审核不严格**、**违法违规软件处理不及时**和 APP 提供者、运营者、开发者身份信息不真实、联系方式虚假失效等问题。
《工业和信息化部关于进一步提升移动互联网应用服务能力的通知》（工信部信管函〔2023〕26 号）	（二）强化平台分发管理 4.**严格 APP 上架审核**。5.**强化在架 APP 巡查**。
《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）》	第九条 App 分发平台应当履行以下个人信息保护义务：……（四）**对新上架 App 实行上架前个人信息处理活动规范性审核，对已上架 App 在本规定实施后 1 个月内完成补充审核，并根据审核结果进行更新或者清理**；
《信息安全技术 应用商店的移动互联网应用程序(App)个人信息处理规范性审核与管理指南》（征求意见稿）完成时间：2022 年 6 月 15 日	主要包括 App 进入应用商店前的个人信息处理活动审核和 App 进入应用商店后的个人信息安全管理。**针对新申请上架的 App、存量 App 以及发生版本更新的 App，应用商店运营者需对 App 个人信息处理活动进行审核，并在 App 通过审核后对其进行上架**；在 App 进入应用商店后，应用商店运营者需对 App 个人信息处理活动进行安全管理，并在 App 存在主管、监管部

法律法规	相关内容
	门通报的违法违规个人信息处理 活动问题时对其采取督促整改、下架等措施。
《T/TAF 125—2022 应用分发平台 APP 审核规范》	4.1 应用分发平台应建立针对上传到本平台的应用软件管理机制，对应用软件进行审核及安全、服务等相关检测，对审核和检测中发现的恶意应用软件等违法违规软件，不得向用户提供；对所提供应用软件进行跟踪监测，及时处理违法违规软件，建立完善用户举报投诉处置措施等。
《深圳市移动互联网应用程序分发业务合规指引》	第四章规定了分发平台资质与备案要求。

二、应用程序分发平台的资质审核义务

《规定》第二十条第三款明确提及了应用程序分发平台的资质审核义务，即应用程序提供的信息服务属于《规定》第七条规定范围的，应用程序分发平台应当对相关许可等情况进行核验。根据《规定》第七条，应用程序提供者通过应用程序提供互联网新闻信息服务的，应当取得互联网新闻信息服务许可，禁止未经许可或者超越许可范围开展互联网新闻信息服务活动。应用程序提供者提供其他互联网信息服务，依法须经有关主管部门审核同意或者取得相关许可的，经有关主管部门审核同意或者取得相关许可后方可提供服务。因此，应用程序分发平台应当依法对应用程序的相关资质进行审核。

针对特定行业应用，应用程序分发平台可以在平台管理规则中列明分级分类管理制度，明确不同行业类别所需的特定资质审核要求，指导开发者按照拟申请上架的应用程序类别和属性，上传相应的资质证明材料，以便于履行审核监管义务。《T/TAF 125-2023 应用分发平台 App 审核规范》附录 B 列举了应用分发平台业务类型资质证书示例（示例如下图），用于分发平台在资质审核时参考。例如，针对需获取资质证书审批/备案后方可运营的特定行业类别，应用分发平台应当基于其提供的信息服务的类型和范围、应用程序提供者的主体性质，核验其是否取得相应监管部门颁发的许可和资质证书，以及资质是否与实际业务模式和许可范围相符，针对未依法取得相关资质的，分发平台不得为其提供服务。常见的需取得特定资质的行业包括但不限于：金融、新闻、出版、医疗保健、药品和医疗器械、互联网地图服务、社交、游戏等。例如，针对新闻资讯类应用程序，应用程序分发平台应当核验其 ICP 备案或《增值电信业务经营许可证》《互联网新闻

信息服务许可证》及附页等情况，对违反国家有关规定的，应当及时采取不予上架、警示、暂停服务或者下架等处置措施。

应用内容包含的类型	资质要求
期货 证券 股票	——ICP 备案截图加盖公章 ——《经营证券期货业务许可证》 ——股票类应用需提供交易所行情授权书 ——《计算机软件著作权证书》或《APP 电子版权证书》 ——如涉及经营性信息服务，提供增值电信业务经营许可证
基金	——ICP 备案截图加盖公章 ——《经营证券期货业务许可证》 ——基金的三方销售公司：需提供基金公司与三方公司签订的合作协议 ——《计算机软件著作权证书》或《APP 电子版权证书》 ——如涉及经营性信息服务，提供增值电信业务经营许可证
银行	——ICP 备案截图加盖公章 ——《金融许可证》 ——《计算机软件著作权证书》或《APP 电子版权证书》 ——如涉及经营性信息服务，提供增值电信业务经营许可证
银行理财产品超市	——银保监会认可文件 ——合作银行的《金融许可证》 ——合作银行的授权书（合作协议） ——《增值电信业务经营许可证》 ——《计算机软件著作权证书》或《APP 电子版权证书》
信用卡办理	——ICP 备案截图加盖公章 ——《金融许可证》或银保监会关于该行开办信用卡业务的批复 ——《计算机软件著作权证书》或《APP 电子版权证书》 ——如涉及经营性信息服务，提供增值电信业务经营许可证
信用卡超市	——至少三家对应银行信用卡中心的授权证明 ——《增值电信业务经营许可证》 ——《计算机软件著作权证书》或《APP 电子版权证书》
第三方支付	——ICP 备案截图加盖公章 ——《支付业务许可证》 ——《计算机软件著作权证书》或《APP 电子版权证书》 ——如涉及经营性信息服务，提供增值电信业务经营许可证

应用内容包含的类型	资质要求
金融理财资讯 金融辅助工具	——ICP 备案截图加盖公章 ——如涉及证券投资，需补充提供《经营证券期货业务许可证》 ——《计算机软件著作权证书》或《APP 电子版权证书》 ——如涉及经营性信息服务，提供增值电信业务经营许可证
境外证券、期货、股票	——《经营证券期货业务许可证》且经营范围必须包含相关业务范围 ——《增值电信业务经营许可证》 ——《计算机软件著作权证书》或《APP 电子版权证书》
贵金属	——ICP 备案截图加盖公章 ——金融管理部门批准文件证明或《贵金属交易会员证书》 ——《计算机软件著作权证书》或《APP 电子版权证书》 ——如涉及经营性信息服务，提供增值电信业务经营许可证
外汇	——ICP 备案截图加盖公章 ——《经营外汇业务许可证》或外汇管理机关准许经营外汇业务批准文件 ——《计算机软件著作权证书》或《APP 电子版权证书》 ——如涉及经营性信息服务，提供增值电信业务经营许可证
保险	——ICP 备案截图加盖公章 ——根据业务范围，提供以下相关资质： • 《保险公司法人许可证》 • 《经营保险业务许可证》 • 《经营保险代理业务许可证》 • 《经营保险经纪业务许可证》 • 《保险公估业务备案表》 • 《保险兼业代理业务许可证》 • 《保险资产管理公司法人许可证》 • 《经营保险资产管理业务许可证》 ——《计算机软件著作权证书》或《APP 电子版权证书》 ——如涉及经营性信息服务，提供增值电信业务经营许可证
保险超市	——《经营保险代理业务许可证》或《保险兼业代理业务许可证》 ——《增值电信业务经营许可证》 ——《计算机软件著作权证书》或《APP 电子版权证书》
信托 融资租赁 汽车金融 资产管理/交易 消费金融	——ICP 备案截图加盖公章 ——《金融许可证》或当地政府的金融批文 ——《计算机软件著作权证书》或《APP 电子版权证书》 ——如涉及经营性信息服务，提供增值电信业务经营许可证
征信机构	——ICP 备案截图加盖公章 ——中国人民银行省级分支行出具的《备案证明》或《个人征信业务经营许可证》 ——《计算机软件著作权证书》或《APP 电子版权证书》 ——如涉及经营性信息服务，提供增值电信业务经营许可证

应用内容包含的类型	资质要求
商业保理	——ICP 备案截图加盖公章 ——主管单位同意设立商业保理公司的批文 ——《计算机软件著作权证书》或《APP 电子版权证书》 ——如涉及经营性信息服务，提供增值电信业务经营许可证
典当	——ICP 备案截图加盖公章 ——《典当经营许可证》 ——《特种行业许可证》 ——《计算机软件著作权证书》或《APP 电子版权证书》 ——如涉及经营性信息服务，提供增值电信业务经营许可证
小额贷款	——《小额贷款公司经营许可证》或省政府及以上级别发放的相关批文 ——《增值电信业务经营许可证》 ——《计算机软件著作权证书》或《APP 电子版权证书》
贷款超市	——至少三家合作单位的金融监管部门备案登记文件、授权书 ——《增值电信业务经营许可证》 ——《计算机软件著作权证书》或《APP 电子版权证书》
助贷机构	——至少三家合作单位的合作协议或授权书 ——合作单位的金融监管部门备案登记文件 ——《融资担保业务经营许可证》 ——《增值电信业务经营许可证》 ——《计算机软件著作权证书》或《APP 电子版权证书》
药品	——ICP 备案截图加盖公章 ——《互联网药品信息服务资格证书》或《互联网药品交易服务资格证》 ——在省、自治区、直辖市人民政府药品监督管理部门备案凭证 ——《计算机软件著作权证书》或《APP 电子版权证书》 ——如涉及经营性信息服务，提供增值电信业务经营许可证
医疗器械	——ICP 备案截图加盖公章 ——《互联网药品信息服务资格证书》或《医疗器械经营许可证》或《医疗器械网络销售备案凭证》或《医疗器械网络交易服务第三方平台备案凭证》 ——《计算机软件著作权证书》或《APP 电子版权证书》 ——如涉及经营性信息服务，提供增值电信业务经营许可证
医疗服务	包括医疗美容、医疗问诊、心理健康问诊等，需提供： ——ICP 备案截图加盖公章 ——《医疗机构执业许可证》/《设置医疗机构批准书》 ——《计算机软件著作权证书》或《APP 电子版权证书》 ——如涉及经营性信息服务，提供增值电信业务经营许可证 注 1：涉及线上问诊的，许可证上需注明互联网诊疗或互联网医院； 注 2：涉及与医疗机构合作的，需提供合作机构的合作协议及合作方《医疗机构执业许可证》或《设置医疗机构批准书》。

应用内容包含的类型	资质要求
门诊预约	——ICP 备案截图加盖公章 ——合作医院的授权书 ——《计算机软件著作权证书》或《APP 电子版权证书》 ——如涉及经营性信息服务，提供增值电信业务经营许可证
运动、健康、养生	——《计算机软件著作权证书》或《APP 电子版权证书》 ——如涉及经营性信息服务，提供增值电信业务经营许可证
音频影视	——ICP 备案截图加盖公章 ——《网络文化经营许可证》 ——《信息网络传播视听节目许可证》 ——若涉及转载内容，需补充提供版权方出具的有效授权证明文件 ——《计算机软件著作权证书》或《APP 电子版权证书》 ——如涉及经营性信息服务，提供增值电信业务经营许可证
直播	——ICP 备案截图加盖公章 ——《网络文化经营许可证》且带有“直播”或“表演”等字样 ——《安全评估报告》加盖公章 ——《安全评估报告》在全国互联网安全服务管理平台的提交结果截图 ——《计算机软件著作权证书》或《APP 电子版权证书》 ——如涉及经营性信息服务，提供增值电信业务经营许可证
阅读	——ICP 备案截图加盖公章 ——《网络出版服务许可证》或《网络文化经营许可证》 ——相关版权方授权书及授权方证明文件 ——阅读类承诺函 ——《计算机软件著作权证书》或《APP 电子版权证书》 ——如涉及经营性信息服务，提供增值电信业务经营许可证
新闻资讯	——ICP 备案截图加盖公章 ——《互联网新闻信息服务许可证》及附页 ——《计算机软件著作权证书》或《APP 电子版权证书》 ——如涉及经营性信息服务，提供增值电信业务经营许可证
互联网宗教信息服务	——ICP 备案截图加盖公章 ——《互联网宗教信息服务许可证》 ——《计算机软件著作权证书》或《APP 电子版权证书》 ——如涉及经营性信息服务，提供增值电信业务经营许可证
聊天 社区 通讯 婚恋	——ICP 备案截图加盖公章 ——《安全评估报告》加盖公章 ——《安全评估报告》在全国互联网安全服务管理平台的提交结果截图 ——《计算机软件著作权证书》或《APP 电子版权证书》 ——如涉及经营性信息服务，提供增值电信业务经营许可证

应用内容包含的类型	资质要求
互联网地图服务	——ICP 备案截图加盖公章 ——《测绘资质证书》并在专业范围中注明互联网地图服务 ——《计算机软件著作权证书》或《APP 电子版权证书》 ——如涉及经营性信息服务，提供增值电信业务经营许可证
加速器 浏览器 网盘/云存储等	——《增值电信业务经营许可证》 ——《计算机软件著作权证书》或《APP 电子版权证书》
游戏	——《网络游戏出版物号（ISBN）核发单》或《关于同意出版运营移动网络游戏的批复》 ——《计算机软件著作权证书》或《APP 电子版权证书》
注1：《计算机软件著作权证书》或《APP电子版权证书》为非必选内容； 注2：行业资质如有更新，以最新法律法规要求为准。	

图 应用分发平台业务类型资质证书示例

《规定》虽规定了应用程序分发平台对应用程序提供者相关资质许可的审核义务，但并未明确此种审核义务属于形式审核还是实质审核。我们理解，分发平台的审核义务存在合理边界，不同于行政监管机关的审核能力，应以分发平台的实际审核能力为限。针对特定行业资质许可审核，通常分发平台对开发者上传的许可证书、备案、授权证明等材料进行形式审核即可视为已尽合理审查强度[74]，如在公开的权威数据库中公示的信息是否与开发者提交的材料一致，申请材料是否存在明显违法内容，以及许可证书是否在有效期内等，如应用程序提供者提供已过期或不具备效用的资质将会被驳回。

在开展形式审核过程中，分发平台应当尤其关注应用程序提供者的资质许可与其提供服务的匹配程度，换言之，应用涉及或包含的全部实际功能和服务内容应与资质许可相匹配，不能仅依据应用程序的分类或主要功能进行判断，而是要通过对应用程序所提供的全部功能或服务进行判断。例如，某应用分类为“聊天社交”，但是某项功能涉及“招聘”，则分发平台也应当核验应用程序提供者是否具备《人力资源服务许可证》等资质，以确保其具备与其所提供应用服务内容相适应的资质。例如，虽然某应用分类不是地图导航类，但是该应用某项功能涉及定位、地图显示、地图搜索、路线规划、导航等互联网地图服务，就需要核验其是否具备互联网地图服务测绘资质或是否具备合作的测绘单位出具的授权证明。例如，结合深圳市人民检察院发布的《深圳市移动互联网应用程序分发业务合规指引》第三十条第（五）款，对于游戏类应用程序，除审查其是否取得国家新闻出版署核发的出版物号，还应一并核验游戏的实质内容是否与取得出版物号的游戏内容相符合。

此外，针对需要进行安全评估核验的特别行业应用程序，分发平台还需要核验相关的评估报告，例如，针对社交通讯、新闻信息类等具有舆论属性或社会动员能力的应用程序，以及涉及使用深度合成等新技术新应用的应用程序，按照有关规定需要开展安全评估，并将评估报告交由网信、公安等有关主管机关审查的，分发平台应当审核应用程序的安全评估报告，并核验主管机关对该应用程序的审查意见。如 oppo 审核规则中说明的，安全评估报告截图中现场检查结果/备案状态必须为“通过”，结果为“待现场检查”、“整改”、“不通过”等情况均为无效上传。

对此，建议分发平台成立专职的资质检测团队，完善资质检测流程，并进一步优化触发资质审核逻辑，高效识别资质真伪，将自动检测与人工检测相结合，以保障应用程序具备合规资质。同时，在监管机构发布实操指引的同时，各大分

[74] 裁判依据可见【广州某网络信息科技有限公司诉被告某软件技术有限公司网络侵权责任纠纷案】，案例来源：“广州互联网法院”微信公众号，链接：
https://mp.weixin.qq.com/s/xx94tFQm9arR4izVvKErFw

发平台厂商已逐步建立自身就应用程序审核的一套规则，具体请见下文第四部分内容。

如分发平台发现待分发或者已分发的应用程序不具备特定行业的相应资质、备案、授权的，或者不符合法律、行政法规的规定或者国家标准的强制性要求的，分发平台应结合违法违规行为的性质、影响、危害等方面因素，依据标准化的处置规则采取相应的处置措施，并向应用程序提供者公示：

- 在App上架审核过程中：如发现其不满足审核要求，可拒绝其上架申请，并要求根据相关规定以及平台审核规范补充材料，并视补充情况作出予以分发、暂停分发或不予分发的决定；
- 在App发布后：如发现存在不满足要求的内容，可采取警示、通知整改、下架、删除、暂停或关闭开发者账号、断开相关应用服务、冻结账号等处理措施；
- 对于存在多次违规的App：如多次通知拒不整改的，或整改后仍存在问题的，或采用技术手段规避审核的，分发平台应酌情采取加严处理措施，如直接下架、冻结账号等。

同时，分发平台还可采取信用管理机制，将违规主体纳入信用管理体系，视情况考虑采取公示黑名单、监督检查、追究应用程序提供者的法律责任等措施，保存处置记录并向有关主管部门报告。

三、应用程序提供者的自查义务

对于应用程序提供者而言，首先，在上架前，应当基于《移动互联网应用程序信息服务管理规定》并结合其提供的服务类型进行自查，若通过应用程序提供互联网新闻信息服务，则必须取得互联网新闻信息服务许可；若提供其他互联网信息服务时，如依法须经有关主管部门审核同意或者取得相关许可，务必在获得有关主管部门审核同意或者取得相关许可之后，才可以开展服务。并且，应严格遵循许可与审核规定开展服务，确保所有服务活动均在合法合规的框架内进行，不得违反规定擅自提供未经许可或未通过审核的信息服务类型。

其次，建立内部数据安全监督检查制度，可考虑建立自动化的动态监测系统或采取清单式检查方法。检查范围包括应用程序的功能、服务内容、应用场景、运营方式等各个方面，检查是否有新增需要许可但未取得许可的服务项目。检查频率可以根据应用程序的风险程度和业务规模来确定，高风险或业务复杂的应用程序可以每季度检查一次或结合发版频率确定，其他应用程序可以每半年检查一次。例如，检查新闻信息服务应用程序是否有未经许可转载的新闻内容，或者其他互联网信息服务应用程序是否在未获得新的许可的情况下增加了需要许可的

服务项目。对于发现的问题，要及时进行整改，并记录在案，作为后续监督的重点。

同时，应积极响应主管部门检查，包括服务资质、内容合法性等方面，如主管部门提出整改意见，应根据意见迅速整改，确保应用程序符合规定。此外，应建立畅通的用户反馈渠道，鼓励用户对应用程序中可能存在的不合规内容或服务进行举报。

四、主流分发平台的落地现状分析及启示

为履行作为分发平台对应用程序提供者进行监督审核的主体责任，且协助其落实不同行业法律法规的要求，目前主流分发平台大多公布了应用程序审核规则，并单独列出了特殊类别应用的审核要求，向应用程序提供者公示常见资质问题及审核指引，管理规则涵盖上架与审核、违规处置、安全隐私、广告投放、投诉处理、消费充值等多方面内容。由于应用内容包含的业务类型繁多以及审核规则不同时期的调整更新，各分发平台均向开发者说明，针对资质的列举和说明并未详尽，如有疑问可咨询客服，以最终审核意见为准，以此引发开发者的特别关注。下文将选取目前几大主流应用程序分发平台，包括华为[75]、oppo[76]、vivo[77]、小米[78]、荣耀[79]、苹果[80]，对目前的现状进行分析。

华为、oppo、vivo、荣耀均制定了特殊行业资质要求清单，苹果主要通过一般性通用授权规则将资质相关要求纳入“知识产权”的说明中，同时也列举了几类特殊行业的资质许可要求[81]，虽然未像其他平台那样明确列出具体业务类型，但通过明确应用程序整体的审核准则，如安全、性能、设计及法律等方面的规定，间接实现对各类业务的规范管理。

关于特殊行业资质要求清单，一般会包括一级、二级业务分类，对应的资质要求和/或备注。其中，各平台对行业类型的分类机制略有不同，例如地图服务类在 oppo 平台中被列入“实用工具”类，在 vivo 平台中则被单独列为“互联网地图服务类”，小米和苹果平台中则通过知识产权规则进行规范，并未专门针对地图服务行业设置相关资质要求。

关于资质要求的文件类型，主要包括开发者自身获取的许可/资质证书、涉及与相关单位合作的需提供合作方的授权证明、主管部门备案证明等。通常来说，所有开发者均需要提供 ICP 备案或《增值电信业务经营许可证》以及《计算机软

[75] https://developer.huawei.com/consumer/cn/doc/app/80301
[76] https://open.oppomobile.com/new/developmentDoc/info?id=12133
[77] https://dev.vivo.com.cn/documentCenter/doc/90
[78] https://dev.mi.com/distribute/doc/details?pId=1139
[79] https://developer.honor.com/cn/doc/guides/101152
[80] https://developer.apple.com/cn/app-store/review/guidelines/
[81] https://developer.apple.com/cn/help/app-store-connect/reference/app-information

件著作权证书》、《APP 电子版权证书》或《软件著作权认证证书》（三者选一）（荣耀作出明确要求）。除此之外，针对金融类、著作权类等强监管类业务功能，还需开发者填写并上传承诺书[82]，要求开发者承诺的事项主要包括：（1）已事先取得审批；且其所提供的内容与许可的内容相符合，未超出行政审批和营业执照经营范围，不进行跨地区使用；（2）资质、审批材料真实、有效；（3）已对资质证件信息进行严格审核，或定期安排专人对应用内的产品巡查巡检，保障产品的合规性。针对通用类承诺函，一般用于确保应用程序所提供的内容均已获得合法授权，不存在任何侵犯第三方合法权益的情形。

总体而言，各主流分发平台对于金融类应用审核严格，涉及银行、证券、基金、保险等细分领域均需相应资质，如银行类应用大多需《金融许可证》，证券类应用需《经营证券期货业务许可证》，医疗应用可能需要医疗机构执业许可证；教育应用则可能要求有办学许可证或教育部门的备案文件。各大应用分发平台基于自身需求，会就应用类型进行明确，现将各大平台的业务类型特点总结如下，具体的资质类别可参见各平台的资质要求清单：

分发平台	关于特殊行业类别
华为	包括全面的金融类、医疗健康类、新闻资讯类、车驾管服务类、互联网地图服务类、深度合成或生成式人工智能服务等较多细分类型
OPPO	金融理财、视听播放、社交聊天、资讯阅读、商城购物、生活服务、教育学习、医疗健康、实用工具、休闲娱乐、深度合成与人工智能、其他
Vivo	金融理财、通讯社交、视频直播、新闻阅读、便捷生活、健康美容、购物优惠、教育学习、实用工具、深度合成类、多方通信类、互联网地图服务类、互联网宗教信息服务、其他类型应用
小米	金融理财、影音视听类、图书阅读类、新闻资讯类、实用工具类、聊天社交类、医疗健康类、学习教育类、宗教类、数字藏品类（展示及首次发售）、深度合成服务类、其他类

[82] 参见金融理财 vivo 承诺函、Oppo 金融类承诺书

分发平台	关于特殊行业类别
荣耀	金融、数字藏品、药品、医疗器械、医疗服务、门诊预约&体检购买、运动健康、影音娱乐、新闻阅读、互联网宗教信息、社交通讯、深度合成服务、互联网地图、网约车、网约车聚合平台、手机话费充值办理手机套餐等业务、上门按摩类、油卡类、出租车、出租车平台、顺风车、加速器/浏览器网盘/云存储等、拍卖、商标代理、求职招聘、法律服务、开锁、营业性演出票务、短信群发、中小学教育、在线办理车驾管业务、多方通信类、其他、游戏
苹果	苹果平台主要在审核指南中强调知识产权相关内容，对 App 中使用的第三方材料、访问第三方服务、显示第三方服务内容、音频/视频下载等涉及知识产权的方面有严格要求，如不得在未经授权情况下使用受保护的第三方材料，访问第三方服务需获得特别许可等。 同时，还针对几类特殊类别行业规定了必须提供相关信息以及一个或多个证明文件（包括相应运营单位的授权协议），如游戏 App 必须取得网络游戏出版物号；图书和报刊杂志 App 必须持有中国国家新闻出版署（NPPA）颁发的《网络出版服务许可证》；包含宗教内容的 App 必须持有中国国家宗教事务局（NRAA）颁发的《互联网宗教信息服务许可证》；新闻 App 必须持有中国国家互联网信息办公室（CAC）颁发的《互联网新闻信息服务许可证》。

五、分发平台的潜在合规风险及法律后果

上方法规要求应用程序提供者和应用程序分发平台严格遵守法律法规，维护应用市场的秩序和用户的合法权益。下文将分析应用程序分发平台可能存在的合规风险，以及若未履行审核义务，将可能面临的法律责任。

（一）合规风险

1. 未制定或公开明确的审核规则和分类规则

虽法律法规未明确规定资质审核规则的具体内容，但从整体政策趋势、行业实践以及监管导向来看，分发平台应具备清晰、合理且透明的审核规则体系，明确审核要素和具体资质要求，公布清晰的审查标准和流程，有助于开发者访问阅读和参考。若缺乏明确的审核标准，可能无法有效筛查和管理应用程序，一旦发生纠纷或违规事件，平台可能因无法证明其已尽合理审核义务而承担不利后果。

2. 资质审查业务流程与核验逻辑缺失的风险

因缺失有效的资质审查业务流程和核验逻辑，分发平台可能无法及时准确判断需要资质许可的触点，进而无法核实开发者的真实身份和合法经营资格，这可能使得非法或无资质的开发者上架应用程序，从事诸如非法金融活动、无资质医疗服务、违规教育业务等行为。这些违规应用可能损害用户权益，扰乱市场秩序，引发行业乱象。一旦发生问题，平台可能因疏于资质审查而成为违法活动的间接推动者，进而面临监管部门的处罚，包括罚款、责令整改、停业整顿甚至吊销相关业务许可证等，同时还可能承担对用户和合法开发者的赔偿责任。

3.缺乏复测检验机制和监督落实不到位的风险

分发平台若缺乏对应用程序上架后的持续巡查和监测机制，将无法及时发现应用程序在运行过程中出现的新问题，如功能变异、恶意更新、用户数据泄露、许可或授权过期等，一旦发生问题，平台内部将难以快速响应和有效解决，增加了平台的运营风险，还可能引发一系列法律问题。此外，若缺乏对已发现问题的应用程序的复测检验机制，违规应用将持续在平台上存在并传播，其危害范围将不断扩大。用户可能在不知情的情况下继续使用违规应用，导致个人信息泄露、遭受诈骗、接触不良内容等风险增加。此外，平台的不作为还将引起监管部门的关注，可能被认定为未履行平台管理责任，面临行政处罚，如警告、罚款、限制业务发展等合规风险。

（二）法律责任

1. 行政责任

《移动互联网应用程序信息服务管理规定（2022）》并未直接规定因未履行主体安全责任的分发平台可能面临的具体的处罚，而是明确了由网信部门和有关主管部门在职责范围内依照相关法律法规处理。根据《移动智能终端应用软件预置和分发管理暂行规定》，通信主管部门有权责令改正，依法进行处罚，并将分发平台违规受到行政处罚的情况记入信誉档案，向社会公布。根据《网络数据安全管理条例》第五十五条，分发平台未履行核验审查义务的，由网信、电信、公安等主管部门依据各自职责责令改正，给予警告，没收违法所得；拒不改正或者情节严重的，处 100 万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员可以处 1 万元以上 10 万元以下罚款。根据《电子商务法》，电子商务平台经营者对平台内经营者未尽到资质资格审核义务，由市场监督管理部门责令限期改正，可能被处五万元以上五十万元以下的罚款；情节严重的，可能被要求责令停业整顿，并处五十万元以上二百万元以下的罚款。

同时，监管部门持续贯彻以平台为抓手的监管思路，如 2020 年 8 月 31 日，部分移动应用分发平台管理主体责任缺位，对上架 App 审核把关不严，被工信部通报并要求限期整改。

2. 民事责任

分发平台本身既非上架应用的实际开发者，也不是应用程序的直接上传主体，且通常情况下分发平台未直接获取经济利益，除分发平台投放推广、搜索广告等会获利的情形，大多情况下不会被径直判定为直接侵权方。然而，从履行网络安全责任义务的层面来看，若其未能尽到相应职责，则有可能被认定为构成帮助侵权，从而需要承担民事赔偿责任。

以北京市首例应用市场因未尽 App 审查义务而被判帮助侵权的案例[83]为例，此案中，分发平台因未尽审查义务，在开发者账户审核和 App 上架申请材料审核中存在失职行为，未注意到伪造的营业执照与国家企业信用信息公示系统中的经营范围部分的内容存在显著差异，并且涉案 App 未取得法律法规要求的电信业务经营许可材料，亦未依法进行标识。由此，因分发平台对 App 上架审核环节未对该材料履行形式真实性审核义务，导致原告遭受了在分发平台中被冒名注册贷款 App 的侵权行为，进而遭受了经济损失。法院判定分发平台未尽到对 App 的审核义务，构成帮助侵权，被判向原告进行赔偿。

3. 刑事责任

分发平台作为网络服务提供者，若未履行对应用程序的审核等安全管理义务，在监管部门责令改正后仍不改正，且导致违法信息大量传播、用户信息泄露等严重后果，将可能触犯拒不履行信息网络安全管理义务罪；分发平台若对应用程序审核不严，致使应用非法获取、出售或提供用户个人信息，如姓名、身份证号、联系方式、银行账号等，且达到情节严重程度，分发平台可能因间接帮助行为而涉嫌侵犯公民个人信息罪。若分发平台明知应用程序存在用于实施犯罪活动的风险却未审核发现，或发现后仍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，情节严重的，将构成帮助信息网络犯罪活动罪。若分发平台明知应用程序存在用于设立违法犯罪活动网站或通讯群组的风险，却未履行审核义务，导致此类应用上架，分发平台可能因间接帮助行为而符合非法利用信息网络罪。

六、结语

应用程序分发平台在应用生态中扮演着至关重要的角色，其对于应用程序提供者的资质审核机制的完善与否直接影响着市场秩序和用户权益保护。通过对监

[83] 参见“北京互联网法院”微信公众号，链接：
https://mp.weixin.qq.com/s/Yyc3VhZ4YrqhDWecxbLFog

管框架、审核要点、应用程序提供者义务、主流平台现状以及分发平台潜在风险的全面分析，我们可以清晰地认识到当前分发平台面临的诸多挑战与责任。为确保平台合规运营，分发平台应积极采取措施实现自治，通过建立健全管理机制和技术手段、严格执行应用程序审核流程，加强对开发者资质和应用安全评估的核验，强化日常管理与巡查复测，切实落实信息内容管理责任。同时，分发平台应制定明确的审核机制和管理协议，并严格执行违规处置措施，确保平台上的应用程序合法合规。对于应用程序提供者而言，应主动加强自身合规建设，获取相应资质、备案或授权等，并积极配合分发平台审核，以确保提供的应用程序符合各项法律法规要求。监管部门也应持续加强对分发平台的监督管理，不断完善相关法规政策，推动行业自律，形成多方协同治理的良好格局。

环球律师事务所 GLOBAL LAW OFFICE SINCE 1979

美国网络数据安全

- 美国数据监管新规观察（上）——美国数据跨境传输行政命令的背景与规则
- 美国数据监管新规观察（中）——美国数据监管行政命令的风险分析与企业因应
- 美国数据监管新规观察（下）——美国数据跨境新政的适用场景、应用公式与应对策略

1. 美国数据监管新规观察（上）——美国数据跨境传输行政命令的背景与规则[84]

前言

当地时间 2024 年 2 月 28 日，美国总统小约瑟夫·罗宾内特·拜登签署并发布了第 14117 号《关于阻止受关注国家获取美国人的大规模敏感个人数据及合众国政府相关数据的行政命令（Executive Order on Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern）》（以下称"**《行政命令》**"）；[85]随后，白宫与美国司法部（Department of Justice）陆续发布了一系列文件。这些以《行政命令》为核心的文件矛头直指所谓"受关注国家（Countries of Concern）"政府（包括**中国、俄罗斯、朝鲜、古巴与委内瑞拉**）以及与其存在关联的实体与个人。此次《行政命令》一定程度上表达出美国联邦政府修改其此前主张的数据跨境自由流动政策的意向，可能对"受关注国家"以及企业带来实质性影响。在本文的上篇中，我们结合目前已公开发布的相关文件，以美国数据跨境流动政策的不变与变化为视角，分析美国在数据跨境政策上的整体方向；在将于后续发布的下篇中，我们将进一步结合企业关注的热点场景为我国企业在相关政策落地前进行风险预判，特别为我国出海企业提供应对参考。

（一）《行政命令》的出台背景：美国数据跨境流动的政策趋势

由于美国联邦层面缺乏数据安全监管法规，且其在各类国际组织与国家间合作中表现踊跃，美国联邦政府对于数据跨境一直持自由流动的态度。但是，仔细考察近几年来美国的国内政策与国际实践可以发现，虽然美国企业在国际市场上仍然保持着强势地位，国与国之间的数据自由流动也持续不断地为美国经济带来正面效益，但一些发展中国家经济的崛起，甚至他们某些行业的企业在全球细分领域的话语权增强，给美国带来了不少竞争压力。与此同时，美国国内保守主义意识形态抬头，令美国联邦政府逐渐倾向于采取具有贸易保护主义色彩的监管政策——这些政策不仅针对特定经济部门、行业产业进行规制，也包括了对网络与数据进行监管。

近几年来，美国在数据跨境流动政策方面表现出较为明显的转向——美国联邦政府出于为境内数据监管政策（尤其是涉及源代码、算法等敏感领域的相关数据）保留空间的目的，倾向于在国际合作中避免在科技监管领域为自身设定具有约束力且可执行的限制——尤其是在进入 2023 年后，美国白宫在促进数据跨境

[84] 作者：孟洁、赵姝、杜畅

[85] https://www.whitehouse.gov/briefing-room/presidential-actions/2024/02/28/executive-order-on-preventing-access-to-americans-bulk-sensitive-personal-data-and-united-states-government-related-data-by-countries-of-concern/ (last visited March 6, 2024).

自由流动方面几近失语，转而制定并落实各类数据监管政策并开展对应的国际实践。

下表针对美国联邦政府在数据跨境流动方面颁布的较为重要的部分国内政策与在国际方面的声明进行了简要梳理：

趋势	国内政策/国际实践	时间
自由流动	【美国国际工商理事会】 世界贸易组织电子商务谈判提案（USCIB Recommendations for the WTO E-Commerce Negotiations）[86]	2019/06/06
	【二十国集团】 “基于信任的数据自由流通”倡议[87]	2019/06/29
	【全球跨境隐私规则论坛】 全球跨境隐私规则声明（Global Cross-Border Privacy Rules (CBPR) Declaration）[88]	2022/04/21
	【经济合作组织】 关于政府调取私营部门实体持有的个人数据的宣言（Declaration on Government Access to Personal Data Held by Private Sector Entities）[89]	2022/12/14
	【美国商务部、欧盟委员会】 欧盟-美国数据隐私框架（EU-US Data Privacy Framework）[90]	2023/07/10
强化监管	【美国白宫】 第 14034 号关于防范外国对立方侵犯美国敏感数据的行政命令（Executive Order on Protecting Americans' Sensitive Data From Foreign Adversaries）[91]	2021/06/09
	【美国贸易代表】 取消 2019 年提出的世界贸易组织电子商务谈判提案[92]	2023/10/26
	【美国商务部】 采取额外措施应对重大恶意网络活动方面的国家紧急情况的拟议规则（Proposed Rules on Taking Additional Steps To Address the National Emergency	2024/01/29

[86] https://www.uscib.org/uscib-content/uploads/2019/06/USCIB-WTO-E-Commerce-Recommendations.pdf (last visited March 6, 2024).
[87] https://www.consilium.europa.eu/media/40124/final_g20_osaka_leaders_declaration.pdf (last visited March 6, 2024).
[88] https://www.globalcbpr.org/wp-content/uploads/Global-CBPR-Declaration-2022.pdf (last visited March 6, 2024).
[89] https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487 (last visited March 6, 2024).
[90] https://www.dataprivacyframework.gov/ (last visited March 6, 2024).
[91] https://www.federalregister.gov/documents/2021/06/11/2021-12506/protecting-americans-sensitive-data-from-foreign-adversaries (last visited March 6, 2024)
[92] https://www.reuters.com/world/us/us-drops-digital-trade-demands-wto-allow-room-stronger-tech-regulation-2023-10-25/ (last visited March 6, 2024).

趋势	国内政策/国际实践	时间
	With Respect to Significant Malicious Cyber-Enabled Activities）[93]	
	【美国白宫】 第 14117 号关于阻止受关注国家获取美国大规模敏感个人数据及合众国政府相关数据的行政命令（Executive Order on Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern）[94]	2024/02/28

表 1 美国联邦数据跨境流动国内政策与国际实践

需要说明的是，《行政命令》的授权依据为《国际紧急经济权力法（International Emergency Economic Powers Act, IEEPA）》以及《国家紧急法（National Emergencies Act, NEA）》——在 IEEPA 与 NEA 中，美国国会对美国总统授予了在紧急状态下较为宽泛的明示授权。总统依据 IEEPA 及 NEA 来宣告国家紧急状态从而使相关紧急权力与授权，从流程上需要依据 NEA 规定立即向国会发送紧急状态命令公告（即下文提及的信函）并发布在联邦公报（Federal Register）上，而紧急状态的宣告多由美国总统通过行政命令的方式进行。

值得注意的是，IEEPA 对紧急状态定义较为模糊并且对总统的授权相对宽泛，这使得美国总统援引 IEEPA 来宣告紧急状态、采取响应措施十分便捷，因此在联邦政府需要强化监管或推动制裁时，通过 IEEPA 宣告紧急状态也成为了多数情况下美国总统的首选项。而由于需要宣告紧急状态以获取授权，国家安全的考量在相关政策文件的首段授权文段，以及序言的正当性说理中，均占据了重要位置。通过观察国家紧急状态宣告的频次变化（1976 年至今 NEA 项下共计发生了 79 次紧急状态宣告，其中有 20 次发生在近 4 年中，宣告频次显著提升[95]），我们也同样能够大致观察到美国联邦政府整体监管强化的蛛丝马迹。

（二）《行政命令》的规则解读：基于风险控制的数据交易监管

除《行政命令》外，2 月 28 日及其后的数日内，美国白宫与美国司法部还陆续发布了如下四份文件：

1) 白宫《事实概况：拜登总统发布行政命令保护美国人的敏感个人数据（Fact Sheet: President Biden Issues Executive Order to Protect Americans' Sensitive

[93] https://www.federalregister.gov/documents/2024/01/29/2024-01580/taking-additional-steps-to-address-the-national-emergency-with-respect-to-significant-malicious (last visited March 6, 2024).
[94] https://www.federalregister.gov/documents/2024/03/01/2024-04573/preventing-access-to-americans-bulk-sensitive-personal-data-and-united-states-government-related (last visited March 6, 2024).
[95] https://www.brennancenter.org/our-work/research-reports/declared-national-emergencies-under-national-emergencies-act (last visited March 6, 2024).

Personal Data)》[96]（以下称“**《白宫概况》**”）；

2) 白宫《就防止受关注国家获取美国人的大规模敏感个人数据和美国政府相关数据致国会的信函（Message to the Congress on Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern)》[97]（以下称“**《致国会信函》**”）；

3) 美国司法部《事实概况：司法部将在即将随突破性的解决受关注国家获取美国人的大规模敏感个人数据问题的行政命令后发布拟议规则制定的预先通知（Fact Sheet: Justice Department Will Issue Advance Notice of Proposed Rulemaking Following Forthcoming Groundbreaking Executive Order Addressing Access to Americans' Bulk Sensitive Personal Data by Countries of Concern)》[98]（以下称“**《司法部概况》**”）；

4) 美国司法部《关于受关注国家获取美国人的大规模敏感个人数据和政府相关数据的规定的拟议规则制定预通知（Advance Notice of Proposed Rulemaking: Provisions Regarding Access to Americans' Bulk Sensitive Personal Data and Government-Related Data by Countries of Concern)》[99]（以下称“**《预通知》**”，美国司法部于当地时间 2024 年 3 月 5 日在《联邦公报（Federal Register)》上公布了《预通知》的正式文本）。

包括《行政命令》自身在内的上述文件，从整体结构上看，包含两层规则内容：（1）白宫在《行政命令》中向各联邦行政部门做出的授权与指令；[100]及（2）联邦行政部门根据《行政命令》中的授权与指令发布的规定与标准。根据《白宫概况》，《行政命令》的授权与指令主要包括六个方面，其中前三个方面与直接要求行政部门制定规则或标准有关，包括要求**美国司法部颁布相关规定**与要求美国国土安全部制定安全要求。

需要明确的是，《行政命令》所指示与授权的监管行动以美国司法部为主导，且美国司法部所颁布的、关于限制与禁止交易的规定在《行政命令》下具有核心地位，因此相关企业应充分关注《预通知》相关的后续规则制定进程。

1. 禁止或限制交易的一般规则

---

[96] https://www.whitehouse.gov/briefing-room/statements-releases/2024/02/28/fact-sheet-president-biden-issues-sweeping-executive-order-to-protect-americans-sensitive-personal-data/ (last visited March 6, 2024).
[97] https://www.whitehouse.gov/briefing-room/presidential-actions/2024/02/28/message-to-the-congress-on-preventing-access-to-americans-bulk-sensitive-personal-data-and-united-states-government-related-data-by-countries-of-concern/ (last visited March 6, 2024).
[98] https://www.justice.gov/opa/media/1340216/dl (last visited March 6, 2024).
[99] https://www.federalregister.gov/documents/2024/03/05/2024-04594/national-security-division-provisions-regarding-access-to-americans-bulk-sensitive-personal-data-and (last visited March 6, 2024).
[100] 基于本文的分析目的，《行政命令》中的授权与指令虽然与受管辖主体所面对的落实规则不直接而相关，但由于其包含对联邦行政部门规则制定行为的限制与指引，在最终落地规则尚未完全明晰，且缺乏任何相关的监管实践与解读的情况下，授权与指令规则为理解政策的倾向、范围与基线提供了支持与证据。

《行政命令》针对性地要求美国司法部颁布**禁止**或**限制**美国主体获取、持有、使用、转让、运输或进出口任何外国（政府）或外国公民在其中拥有任何利益的财产（即，“交易”），如果该交易：①涉及大规模敏感个人数据或与美国政府有关的数据；②属于对美国国家安全构成不可接受风险的交易类别；③在司法部规定的生效日期之后启动、待定或完成；④不符合豁免条件，或未基于许可获得授权；并且⑤不属于提供金融服务（包括银行、资本市场和金融保险服务）的正常相关活动和组成部分，也不是遵守任何联邦法定或监管要求（包括执行这些要求的任何法规、指南或命令）所必需的。

基于《行政命令》的要求，美国司法部在《预通知》中进一步强调：①美国司法部规则禁止美国主体从事“受管辖数据交易（covered data transactions）”类型，因为这些类型的数据交易可能使受关注国家或受管辖主体访问美国的“大规模敏感个人数据（bulk sensitive personal data）”或“政府相关数据（government-related data）”；②一些原本被禁止的交易可能受到限制，并仅在符合某些条件——如，国土安全部发布的“安全要求（security requirements）”——的情况下才被允许开展；③被禁止或受限制的交易可能适用通用或特定“许可（license）”而被允许开展；④任何限制或禁止的要求均不适用于“豁免交易（exempt transactions）”。

不难看出，作为一般适用的基本规则，《行政命令》及相关文件**禁止或限制了美国主体与受关注国家或受管辖主体之间涉及大规模敏感个人数据或政府相关数据的受管辖数据交易，除非该等交易构成豁免交易或基于许可获得了授权；但受限交易可以在满足安全要求的前提下开展**（以下称“**禁止/限制规则**”）。我们从禁止/限制规则中汇总提取了 4 组关键要素：

1) 作为监管目标的数据——大规模敏感个人数据、政府相关数据；

2) 作为监管事项的交易——受管辖数据交易、具体禁令；

3) 开展交易的合规路径——安全要求、许可；

4) 作为监管对象的主体——美国主体、受关注国家与受管辖主体。

以下我们将围绕上述禁止/限制规则中的关键要素及相关概念，基于《行政命令》《司法部概况》与《预通知》等相关文本，对相关政策规则进行进一步解读。

2. 作为监管目标的数据

白宫在《行政命令》中将受管辖的数据类型限定在了“大规模敏感个人数据”与“政府相关数据”两类（在《行政命令》的语境下，二者均为“敏感个人数据”的子类别）并提供了基础的定义，美国司法部则在《司法部概况》与《预通知》为这两类数据提供了更加细致的定义与更加明确的范围。

(1) “敏感个人数据”

《行政命令》语境下的“敏感个人数据”主要被分为了六类，并同时提供了三类不构成敏感个人数据的情形作为对照参考；结合《司法部概况》与《预通知》中的梳理与细化说明，我们将相关定义总结如下表：

定性	类别	定义
构成敏感个人数据	**受管辖的个人识别数据**	具体列明的、与个人有合理关联的个人识别数据类别，这些数据可用于从数据集当中识别特定的个人，并且可以将多个数据集当中的数据与该特定的个人联系起来。 **“受管辖的个人识别数据”包括：** • 相互结合的、列明的个人识别数据； • 与其他敏感个人数据结合的、列明的个人识别数据； • 与交易方根据交易披露的其他数据结合并使个人识别数据可被受关注国家利用的、列明的个人识别数据。 **“受管辖的个人识别数据”不包括：** • **单独的、列明的个人识别数据；** • **未列明的个人识别数据的结合；** • 仅与另一项人口统计或联系数据相关联的人口统计或联系数据（例如姓和名、出生日期、出生地、邮政编码、住宅街道或邮政地址、电话号码和电子邮件地址以及类似的公共账户标识符）； • 仅与提供电信、网络或类似服务的另一网络标识符、账户验证数据或通话详情数据相关联的网络标识符、账户验证数据或通话详情数据。 **“列明的个人识别数据”清单：** • 完整或经过截断处理的政府身份证号或账号——如，社会安全号、驾照或州身份号、护照号或外国人注册号； • 与金融机构或金融服务公司相关的完整金融账号或个人识别码； • 基于设备或硬件的标识符——如，国际移动设备识别码（IMEI）、媒体访问控制（MAC）地址或用户身份模块（SIM）卡号码； • 人口统计或联系数据——如，姓名、出生日期、出生地、邮政编码、住宅街道或邮政地址、电话号码和电子邮件地址以及类似的公共账户标识符； • 广告标识符——如谷歌广告标识符、苹果广告

定性	类别	定义
		标识符或其他移动广告标识符（MAID）； • 账户验证数据——如，账户用户名、账户密码或安全问题答案； • 基于网络的标识符——如，互联网协议（IP）地址或 Cookie 数据； • 呼叫详情数据——如，客户专有网络信息（CPNI）。
		相互结合的、列明的个人识别数据 **定义** 任何与其他列明的个人识别数据相关联的个人识别数据，除了： • 仅与其他人口统计或联系人数据相关联的人口统计或联系人数据；以及 • 仅与其他网络识别符、账户验证数据或通话详情数据相关联的网络识别符、账户验证数据或通话详情数据，且为提供电子通讯、网络或类似服务所必需。 **判断标准** • 在单个受管辖数据交易中，或在相同或相关当事方之间的多个受管辖数据交易/中，所涉及的（各项）个人识别数据能够与同一个特定的人相关联，则该等个人识别数据被视为“相关联的”。 • 如果需要其他与受管辖数据交易不相关的识别数据才能将特定识别数据与同一特定人联系起来，则不认为该等特定识别数据不被视为“相关联的”。 **不包括未列明的数据类型间的相互结合** • 就业经历； • 教育经理； • 组织成员资格； • 犯罪记录；或 • 上网浏览记录。
		与交易方根据交易披露的其他数据结合并使个人识别数据可被受关注国家利用的个人识别数据 **示例** • 连接到位于特定政府建筑中的某一美国快餐餐厅无线网络的所有设备的 MAC 地址（未提供任何其他列明的个人识别数据或敏感个人数据）。 • 具备性少数群体身份的美国现役军官的全名（未提供任何其他列明的个人识别数据或敏感个

定性	类别	定义
		人数据）。
	地理位置数据及相关传感器数据	仅包含精确地理位置数据，即基于电信号或惯性传感单元，识别到特定个人或设备的物理信息在特定距离进度范围（具体精度标准待美国司法部进一步明确）内的实时或历史数据。
	生物识别数据	用于识别或认证特定个人的、可测量的物理特征或行为，包括面部图片、声纹信息、视网膜与虹膜扫描、掌纹与指纹、步态、键盘使用习惯，该等数据在生物识别系统中进行了注册且由该系统生成了数据模板。
	生物组学数据	由人类生成的表征或量化人类生物分子的数据，如人类基因组数据、表观基因组数据、蛋白质组数据、转录物组数据、微生物组数据或代谢组数据，目前阶段仅包含人类基因组数据。 人类基因组数据指代表构成细胞中整套遗传指令或子集的核酸序列的数据，包含了个人基因测试的结果。
	个人健康数据	即“可识别个人身份的健康信息”，指从个人收集的任何信息，包括人口统计信息，这些信息： • 由医疗保健提供者、医疗保险计划、雇主或医疗保健结算中心创建或接收； • 与个人的过去、现在或将来的身体或精神健康或状况、与为个人提供医疗保健服务有关，或与为个人提供医疗保健的过去、现在或将来的支付有关；并且 • 可识别个人身份，或有合理依据认为该信息可以用于识别该个人。
	个人金融数据	• 有关个人信用卡、签账卡或借记卡或银行账户的数据，包括购买和付款记录； • 银行、信贷或其他财务报表中的数据，包括资产、负债和债务以及交易，或信贷或“消费者报告”中的数据。
不构成敏感个人数据	可以合法向公众公开的公共记录数据	如，法庭记录及其他政府记录。
	IEEPA 的个人通信例外所包含的数据	不涉及有价物转让的任何邮政、电报、电话或其他个人通信。（IEEPA 总统授权的个人通信例外，50 U.S. Code § 1702(b)(1)）
	IEEPA 的信息材料例外所包含的数据	任何信息或信息资料，包括但不限于出版物、电影、海报、唱片、照片、缩微胶卷、缩微胶片、磁带、光盘、CD ROM、艺术品和新闻电讯，不论其格式

定性	类别	定义
		或传播媒介如何。（IEEPA 总统授权的信息资料例外 50 U.S. Code § 1702(b)(2)）

表 2 敏感个人数据

(2) “大规模”敏感个人数据的门槛

《预通知》则基于预先风险评估的方式对“大规模”的门槛提供了对应不同个人敏感数据类别的范围（每类数据均包含“低门槛”与“高门槛”两个数值）：

敏感个人数据类型	“大规模”门槛范围	
	低门槛	高门槛
受管辖的个人识别数据	超过 1 万名美国人	超过 100 万名美国人
地理位置数据及相关传感器数据	超过 100 部美国设备	超过 1 万部美国设备
生物识别数据	超过 100 名美国人	超过 1 万名美国人
生物组学数据	超过 100 名美国人	超过 1000 名美国人
个人健康数据	超过 1000 名美国人	超过 100 万名美国人
个人金融数据	超过 1000 名美国人	超过 100 万名美国人

表 3 大规模敏感个人数据的门槛

上述门槛数量中的“美国设备（U.S. device）”被美国司法部定义为“任何与一位美国人关联或存在关联可能性的设备”。需要注意的是，《司法部概况》中强调“大规模”数据的门槛仅适用于敏感个人数据的监管触发；而针对美国政府相关数据，美国司法部会不区分数量地进行全面监管。

美国司法部基于上述门槛范围明确了“大规模敏感个人数据”的定义，即“美国人有关的任何格式的数据集合或数据集，无论这些数据是否是匿名的、假名的、去身份化的还是加密的，且该等数据在过去 12 个月的任一时间点，无论是通过单一的受管辖数据交易，还是以涉及同一外国人或受管辖主体的受管辖数据交易的集合之方式，达到特定门槛”。

(3) “政府相关数据”

《行政命令》将美国政府相关数据定义为“具有被受关注国家利用以损害美国国家安全的高度风险的敏感个人数据，无论其数量多少”。针对政府相关数据的具体规定，我们将相关内容总结如下表：

类别	定义	示例
政府人员关联数据	交易方认为与美国政府（包括军队和情报部门）现任或前任雇	一家美国公司在销售一组敏感个人数据的广告

类别	定义	示例
	员、现任或前任承包商、前任高级官员相关联或存在关联可能性的任何敏感个人数据，无论数量多少。	中称，这些数据属于“现役”人员，“喜欢阅读的军人”，“国防部”人员，“政府雇员”或“与附近军事基地关系密切的社区”。
政府人员识别数据	与可用于识别联邦政府（包括军队和情报部门）现任或前任雇员、现任或前任承包商、前任高级官员身份的数据类别相关联的敏感个人数据，无论数量多少。	一家美国公司在与外国交易方就出售一组敏感个人数据进行讨论时，将这组数据描述为属于一个特定组织的成员，而该组织的成员仅限于现役和退役军人及其家属。
政府精确位置数据	特定地理围栏区域清单中列举的任何区域内，与军事、其他政府或其他敏感设施或地点相关的任何位置的任何精确地理位置数据，无论数量多少。	N/A

表 4 政府相关数据

3. 作为监管事项的交易

《行政命令》将“交易”定义为“获取、持有、使用、转让、运输或进出口任何外国或外国公民在其中拥有任何利益的财产”的行为，并明确了“涉及大规模敏感个人数据或与美国政府有关的数据，对美国国家安全构成不可接受风险的交易”应受限制或禁止。《预通知》则在此基础上将更为具体的“受管辖数据交易”的概念定义为“任何**涉及**美国大规模敏感个人数据或美国政府相关数据的交易，且该交易也涉及：①数据经纪；②供应商协议；③劳动协议；或④投资协议。”

值得注意的是单词“**涉及（involve）**”在此处的多次使用，说明了**《行政命令》相关政策规则体系下的“受管辖数据交易”不仅限于直接进行数据交互的交易活动（如，数据经纪），也包括了可能产生数据访问风险的其他交易活动（如，供应商协议、劳动协议、投资协议）**——这一结论也在《预通知》针对各类受管辖数据交易提供的类型示例中得到了充分的证明——而在《行政命令》的语境下，前述有关风险主要是指受关注国家或受管辖主体访问美国大规模敏感个人数据或政府相关数据的风险。如果使用数据合规实务领域常用的概念来理解，**《行政命令》的“受管辖数据交易”实质上覆盖了各类针对大规模敏感个人数据或政府相关数据的、向受关注国家或受管辖主体进行的共享、转移、委托处理、授权访**

问的行为，以及直接或间接产生受关注国家或受管辖主体访问大规模敏感个人数据或政府相关数据可能性的其他特定交易行为。

受管辖交易行为定义如此宽泛，虽然会受到豁免交易、交易许可及数据范围的三重限制，但仍然可以预期相关规则在具体落实时可能存在较广的灰色地带，给执法机关留下比较大的自由裁量权。

(1) 数据交易的分类监管

针对数据交易的监管，《预通知》中采取了分类监管的策略，将交易分为禁止交易、受限交易与豁免交易。根据《司法部概况》与《预通知》，我们将相关数据交易分类与规则总结如下：

分类	具体情形	分类规则
禁止交易	数据经纪	定义 出售、许可访问或涉及从任何主体（提供者）向任何其他主体（接收者）转移数据的类似商业交易，且接收者并未直接从与所收集或处理的数据有关联或存在关联可能性的个人处收集或处理数据。 示例 • 一家美国公司向总部位于受关注国家的实体出售大规模的美国敏感个人信息。 • 一家美国公司与受管辖主体签署协议并向该主体授权访问美国公司持有的政府相关数据。 • 一家美国组织运营大规模美国敏感个人信息的数据库，并向受管辖主体收费提供年费会员以访问该数据库中的数据。
	基因组数据交易	定义 涉及转让大规模人类基因组数据或可从中提取此类数据的生物样本的基因组数据交易。
受限交易	供应商协议	定义 • 除劳动协议之外的任何协议或安排，根据该等协议或安排任何主体向任何其他主体提供商品或服务（包括云计算服务）以获取付款或其他对价。 • 其中，云计算服务被定义为与提供或使用“云计算”相关的服务，包括基础设施即服务（IaaS）、平台即服务（PaaS）、软件即服务（SaaS）。
	劳动协议	定义 任何协议或安排，根据该等协议或安排除独立承包商外的个人直接为某主体工作或履行工作职能以换取报酬或其他对价，包括在董事会或委员会中的任职、执行级别的安排或服务，以及业务级别的劳动服务。
	投资协议	定义 • 任何协议或安排，根据该等协议或安排任何主体为获

分类	具体情形	分类规则
		取付款或其他对价获取与下列资产有关的直接或间接的所有权益：①位于美国境内的不动产；②美国法律实体。 • 美国司法部正在考虑从作为受限交易的范围中排除：①特定类别的各类被动投资，②对投票权与股权利益的影响低于特定最低门槛的投资行为，以及③未给投资者带来超出合理认定的标准少数股东保护的权利的投资行为。
豁免交易	涉及特定类别数据的交易	• IEEPA 总统授权的个人通信例外——不涉及有价物转让的任何邮政、电报、电话或其他个人通信。（50 U.S. Code § 1702(b)(1)） • IEEPA 总统授权的信息资料例外——任何信息或信息资料，包括但不限于出版物、电影、海报、唱片、照片、缩微胶卷、缩微胶片、磁带、光盘、CD ROM、艺术品和新闻电讯，不论其格式或传播媒介如何。（50 U.S. Code § 1702(b)(2)）
	联邦政府的官方业务交易	定义 由美国政府雇员、资助者或承包商进行的美国政府官方业务的交易，以及根据与美国政府签订的赠款、合同或其他协议进行的交易。具体而言，官方业务交易包含为了以下事项开展的交易： • 美国政府雇员、资助者或承包商进行的美国政府的官方业务； • 任何美国政府部门或机构的授权活动（包括由联邦储蓄机构或信用合作社监管机构以接管人或保守者身份执行的活动）；或 • 根据与美国政府签订的赠款、合同或其他协议进行的交易。
	金融服务、支付处理及监管合规相关的交易	定义 通常作为提供金融服务的一部分，包括银行、资本市场与金融保险服务；或是为了遵守联邦法律或监管要求所必需，包括实施这些要求的任何规定、指导或命令。
	作为业务运营一部分的实体内部的交易	定义 通常与美国跨国公司内部辅助业务运营相关且作为其一部分的交易，具体包括： • 美国主体及其位于受关注国家（或从属于该受关注国家的所有权、指示、管辖或控制）的子公司或附属公司之间的交易， • 通常是跨国公司内部辅助业务运营的一部分（例如，出于人力资源目的共享员工的个人识别数据；薪酬交易，如支付给海外员工或承包商的工资和养老金；支付商业税费；购买商业许可证或执照；以监管合规和风险管理为目的与审计师和律师事务所共享数据）。

分类	具体情形	分类规则
	联邦法律或国际协议要求或授权的交易	示例 • 乘客舱单信息交换 • 国际刑警组织协助请求 • 公共卫生监管

表 5 数据交易的分类

(2) 数据交易的具体禁令

针对具体的禁止措施，美国司法部在《预通知》中提出了针对受管辖数据交易的五类具体禁令，并计划在后续规定中予以进一步落实。我们将相关内容总结如下：

禁令事项	禁令规则
通用数据交易禁令	除非规定中另有授权，美国主体不得在明知的情况下参与同受关注国家或受管辖主体的受管辖数据交易。
数据再传输禁令	除非规定中另有授权，美国主体不得在明知的情况下参与同外国主体间涉及数据经纪活动的受管辖数据交易，除非美国主体通过合同的方式要求该外国主体不得参与同受关注国家或受管辖主体间涉及相同数据的受管辖数据交易。
基因组数据与生物样本禁令	除非规定中另有授权，美国主体不得在明知的情况下参与同受关注国家或受管辖主体的受管辖数据交易，如果该等数据交易使得该等受关注国家或受管辖主体能够访问由人类基因组数据（或可从中获取人类基因组数据的人类生物样本）组成的美国大规模敏感个人数据，且在过去 12 个月的任何时候，无论是在单个受管辖数据交易中还是在各受管辖数据交易的集合中，其所涉及的美国人的数量均超过特定门槛。
不完整及边缘违规禁令	（美国司法部在考虑制定规则以）禁止规避、造成违规、未遂和共谋行为。
规避规定适用禁令	（美国司法部在考虑制定规则以）禁止美国主体在明知的情况下指示境外主体开展特定的受管辖数据交易（包含未遵守安全要求的受限交易），该等交易如果由美国主体参与则会被禁止。 - “指示”指该美国人有权（单独或作为团体的一部分）代表外国实体做出决定，并行使该权力命令、决定或批准某项交易。

表 6 数据交易的具体禁令

值得注意的是，上述禁令中使用的“明知（knowingly）”的措辞将禁令的适用范围限制在了“知道或应当知道交易情况”的美国主体，判断所参考的要素包括①外国主体结构的相对复杂程度，②交易所涉及数据的规模与敏感性，以及③（根据相关事实）交易各方是否以及在何种程度上试图规避规则的适用。根据目

前披露的信息，美国司法部并不要求美国主体在与任何外国主体签订协议或开展其他类别的数据交易时对这些外国主体的背景信息及雇佣行为进行尽职调查，以确定其是否构成受管辖主体；但这一措辞明确禁止了美国主体在明智的情形下逃避或规避禁令的行为，包括以试图规避这些禁令的方式构建交易。

4. 开展交易的合规路径

(1) 受限交易的安全要求

针对受限交易，《行政命令》要求其满足特定的安全要求作为前提，以缓释其所产生的受关注国家及受管辖主体访问大规模敏感个人数据或政府相关数据的风险。《司法部概况》中强调，该等安全要求旨在降低风险，并可能包括网络安全措施，如基本的组织网络安全态势要求、物理和逻辑访问控制、数据屏蔽和最小化，以及隐私保护技术的使用等。

基于上述要求，《预通知》规定了必要的安全要求基本事项，包括：

1) 落实组织网络安全基本态势要求；

2) 在开展受管辖数据交易时遵守下列条件——

① 数据最小化与掩码措施；

② 使用隐私保护技术；

③ 开发用于组织非授权披露的信息技术系统；

④ 落实逻辑与物理访问控制措施；

3) 满足特定合规相关的条件，如设置独立审计人员按以开展对于上述要求落实情况的测试与审计。

(2) 数据交易的许可制度

基于目前美国司法部披露的信息，《行政命令》下的数据交易许可制度可能基于外国资产控制办公室（Office of Foreign Assets Control, OFAC）的许可制度修改而来，并同样会包括“通用许可（general licenses）”与“特定许可（specific licenses）”，用于批准禁止或受限的受管辖数据交易。

通用许可是对于特定类别交易的全面授权，相当于在对于受管辖数据交易的禁止/限制规则下创设一个例外性的授权，为美国司法部提供了灵活的调整空间，以应对政策需求的变化。援引通用许可开展数据交易的美国主体无需自行进行申请，而只需根据美国司法部对于通用许可的相关规定提交报告与声明，并根据相关要求在交易进行过程中进行充分披露；如果未能履行充分披露义务，则给予通

用许可的授权可能面临失效，并同时导致相关交易活动构成对于规定中禁令的违反，相关主体可能面临执法机构制裁的风险。

特定许可是由参与特定受管辖数据交易的特定美国主体主动申请的、一事一议的专项授权，美国主体需要填写并递交各类申请文件以申请特定许可，并可能同样需要遵守通用许可中的持续性披露的义务（如，持续提供有关授权开展的数据交易的报告）。美国司法部目前在针对特定许可考虑要求任何获得特定许可进行大规模敏感个人数据或政府相关数据交易的主体必须在可行的范围内提供保证，确保根据此类交易转移的任何数据都可以恢复、不可逆地删除或以其他方式使其失效。

在上述许可机制外，公司和个人还可以依据法规对特定交易的适用性征求美国司法部（或其他有关部门）的咨询意见。

5. 作为监管对象的主体

上文已提及，《司法部概况》将受关注国家限定在了中国（含中国香港与中国澳门），俄罗斯，伊朗，朝鲜，与委内瑞拉。在此基础上，《行政命令》《司法部概况》及《预通知》对于受管辖主体及美国主体进行了进一步规定，总结如下：

受管辖主体	美国主体
① 被受关注国家直接或间接持股 50%或以上，或在受关注国家组建、注册或设有主要营业地的实体。	• 任何美国公民、国民或合法永久居民； • 任何以难民身份进入美国或获得庇护的人； • 任何仅根据美国法律或美国管辖权范围内的适用法律组建的实体； • 任何位于美国境内的主体。
② 被属于第①类的实体，或属于第③类、第④类、第⑤类的个人，直接或间接持股 50%以上的实体。	
③ 作为受关注国家或属于第①类、第②类、第⑤类的实体的员工或供应商的外国人。	
④ 主要居所地位于受关注国家领土管辖范围内的外国人。	
⑤ 被美国司法部长指认为由某受关注国家拥有或控制，或受其管辖或指示，代表或声称代表某受关注国家或其他受管辖主体行事，或在知情的情况下直接或间接导致或指示违反《行政命令》或用于落实《行政命令》的任何法规的任何人。	

表 7 受管辖主体的范围

三、《行政命令》的管辖分析：与其他监管机制的协调联动

《行政命令》中要求美国司法部在制定规则时考虑与其他联邦政府实体的协调，被提及的联邦政府实体包括美国财政部（the Department of the Treasury）下辖的美国外国投资委员会（Committee on Foreign Investment in the United States, CFIUS）与外国资产控制办公室（Office of Foreign Assets Control, OFAC），美国

商务部（the Department of Commerce）下辖的工业及安全局（Bureau of Industry and Security, BIS），以及负责落实第 13873 号行政命令、第 14034 号行政命令以及第 13913 号行政命令的其他联邦政府实体。根据美国司法部在《预通知》中的判断，在其他相关行政命令下，现有的授权规则尚未针对以下风险提供前瞻性的分类规则：由美国主体与受关注国家或受管辖主体间的交易所带来的国家安全风险，该等风险由于使受关注国家有机会获取美国的大规模敏感个人数据或政府相关数据而构成不可接受的风险。因此，美国司法部目前不认为《行政命令》与《预通知》下的政策会与现有授权规则存在重大重合。

作为以上结论的唯一例外，在《行政命令》下涉及投资协议的受管辖数据交易，由于其可能落入《美国法典（United States Code）》第 50 章第 4565 条定义的“受管辖数据交易”的定义范围，也可能会受到 CFIUS 跨境交易执法权力的管辖。针对这一管辖范围重叠与管辖权冲突的潜在风险，美国司法部在《预通知》中提出了一套管辖礼让的制度设想，即：

1) 在默认状态下，美国司法部对涉及投资协议的受管辖数据交易进行独立监管，适用《行政命令》《预通知》（即后续规定文件）中的规则；

2) 如果 CFIUS 采取了包括临时命令、缓解协议，以及根据命令或缓解协议作出的终止行动决定在内的各类**缓解措施**，以解决由受管辖交易所产生的国家安全风险，则司法部在《预通知》内规划的规则将不再适用于收到 CFIUS 缓释措施影响的相关交易；

3) 即便出现了第 2）项涉及的情形，参与受管辖交易的美国主体仍需完全遵守《预通知》中规划的合规要求。

此外，美国司法部也在《预通知》中列举了部分不会落入 CFIUS 管辖范围的、涉及投资协议的场景，包括：

1) 涉及的数据为低于 CFIUS 的 100 万人门槛的敏感个人数据或无法识别的数据的非控制性投资；

2) 相关风险与 CFIUS 管辖范围内的交易有关但并非作为其结果而产生；

3) 在投资协议签订后，但在相关主体向 CFIUS 申报相关交易前（同时也在相关交易成为 CFIUS 缓解措施的对象之前）可能出现的时间差。

结语

由于对《行政命令》的落实极为重要的美国司法部规则尚处于通过“拟议规则制定预通知（Advance Notice of Proposed Rulemaking, ANPRM）”征集意见的阶段，美国司法部预计会根据公众对于 ANPRM 的意见反馈再行制定更加成熟的“拟议规则制定通知（Notice of Proposed Rulemaking, NPRM）”，并根据公众对于

NPRM 的再次反馈制定最终规则（final rules）并发布在联邦法规汇编（Code of Federal Registration, CFR）上。前述过程往往需要一定的时间来逐步推进，因此我们建议相关从业企业在等待“靴子落地”的过程中密切关注政策内容更新、相关政策变化及行业头部企业的表态，不断强化对相关政策思路与规则的感知，为后续实际合规行动做好准备。

2. 美国数据监管新规观察（中）——美国数据监管行政命令的风险分析与企业因应[101]

前言

当地时间 2024 年 2 月 28 日，美国总统小约瑟夫·罗宾内特·拜登签署并发布了第 14117 号《关于阻止受关注国家获取美国人的大规模敏感个人数据及合众国政府相关数据的行政命令（Executive Order on Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern）》（以下称"**《行政命令》**"）；[102]随后，白宫与美国司法部（Department of Justice）陆续发布了《关于受关注国家获取美国人的大规模敏感个人数据和政府相关数据的规定的拟议规则制定预通知（Advance Notice of Proposed Rulemaking: Provisions Regarding Access to Americans' Bulk Sensitive Personal Data and Government-Related Data by Countries of Concern）》[103]（以下称"**《预通知》**"）等一系列文件。这些以《行政命令》为核心的文件矛头直指所谓"受关注国家（Countries of Concern）"政府（包括**中国、俄罗斯、朝鲜、古巴与委内瑞拉**）以及与其存在关联的实体与个人。此次《行政命令》一定程度上表达出美国联邦政府修改其此前主张的数据跨境自由流动政策与价值取向，这可能对"受关注国家"以及企业带来实质性影响。在此前发布的美国数据监管新规观察（上）丨数据跨境传输行政命令的背景与规则中，我们已结合目前已公开发布的各相关文件，以美国数据跨境流动政策的不变与变化为视角，分析美国在数据跨境政策上的整体方向；在此次发布的下篇中，我们将进一步结合《行政命令》的合规计划与法律责任，基于企业关注的热点场景，为我国企业在相关政策落地前进行风险预判，特别为我国出海企业提供应对参考。

（一）《行政命令》下的合规计划——基于 OFAC 合规计划的分析

《行政命令》向美国司法部长授予了《国际紧急经济权力法（International Emergency Economic Powers Act, IEEPA）》下美国总统的全部授权，并根据 IEEPA 授权条款中的要求，明确且具体地提及了美国司法部的后续规则制定应涉及记录保存与交易报告的需求，为调查、执法和监管工作提供信息。基于这一宽泛的授权，美国司法部目前在《预通知》中表示其考虑针对参与到受监管数据交易中的**美国主体（U.S. person）**施加创设并落实一项合规与执行计划（compliance and enforcement program, CEP），并从四个方面初步阐述了 CEP：①尽职调查与记录保存（due diligence and recordkeeping）；②报告（reporting）；③审计（audits）；

---

101 作者：孟洁、杜畅、赵姝

102 https://www.whitehouse.gov/briefing-room/presidential-actions/2024/02/28/executive-order-on-preventing-access-to-americans-bulk-sensitive-personal-data-and-united-states-government-related-data-by-countries-of-concern/ (last visited March 12, 2024).

103 https://www.federalregister.gov/documents/2024/03/05/2024-04594/national-security-division-provisions-regarding-access-to-americans-bulk-sensitive-personal-data-and (last visited March 6, 2024).

④调查与执行（investigation and enforcement）。我们将《预通知》中对于 CEP 的阐述总结如下表：

事项	内容
尽职调查与记录保存	• 要求受到 CEP 约束的美国主体通过制定、实施和定期更新合规计划的方式落实基于风险的合规方法。 • 适合特定美国主体的合规计划将可能基于下列因素产生变化——主体的规模和复杂性、产品和服务、客户和交易相对方，以及地理位置。 • 不对所有参与同外国主体的受管辖数据交易（covered data transactions）的美国主体规定一般的尽职调查要求或主动的记录保存要求。 • 如果相关美国主体未能制定适当的尽职调查计划，在发生违反规定的行为时该等缺失可能被作为加重因素进行考虑。 • 强制实施的主动尽职调查和记录保存要求仅作为参与限制性的受管辖数据交易的条件，或作为通用或特定许可证的条件。 • 上述主动的尽职调查和记录保存要求包括“了解你的供应商”和“了解你的客户”的要求。 • 要求受尽职调查要求约束的美国主体保存尽职调查记录，以协助司法部的调查与执行。
报告	• CEP 不会为所有与外国主体进行数据交易的美国主体规定一般的报告要求，即便该外国主体为受管辖主体（covered persons）。 • 仅作为某些类别的美国主体从事限制性的受管辖数据交易的条件，或作为通用或特定许可证的条件，或在少数情况下作为识别进行禁止的受管辖数据交易的企图的方式。 • 报告要求的目的是帮助司法部识别对持续合规和执行工作具有最高优先级的受管辖数据交易。 • 获取许可的主体应提供有文件支持的年度认证，以证明该主体遵守了被授予的许可的条款。 • 需要主动履行报告义务的美国主体的类别包括： 1) 该美国主体①参与涉及云计算服务的限制性受管辖数据交易，或涉及数据经纪或云计算服务的、经许可授权的受管辖数据交易，且②其 25%或以上的股权通过任何合同（contract）、安排（arrangement）、谅解（understanding）、关系（relationship）或其他方式，直接或间接地由受关注国家或受管辖主体所持有；或 2) 该美国主体收到并明确拒绝另一主体提出的要约，该要约有关于参与涉及数据经纪的、禁止的受管辖数据交易。
审计	• 为了协助确保遵守限制性覆盖数据交易的安全要求以及根据规则颁发的许可证，美国主体在进行受限交易（无论是否基于许可进行）或基于许可进行的禁止交易时可能被要求遵守某些条件。 • 前述条件可能包括：①指定一个经认可的审计师每年评估安全要求或许可条件的符合性与有效性，以及②将上述审计结果提交给司法部。

事项	内容
	• 审计将需要关注：①美国主体的受管辖数据交易的性质，以及②该交易是否符合适用的安全要求、司法部长颁发的任何许可的条款、司法部规定的任何其他方面。
调查与执行	• 为了协助调查潜在不合规情形，任何美国主体均可能被要求保留交易的完整记录，并以报告或其他形式提供与任何禁止或受限的受管辖数据交易相关的完整信息。 • 《行政命令》与司法部颁布的规定不会为美国政府创造任何新的数据访问权利，以获取美国人的敏感个人数据或政府相关数据，也不会赋予美国政府新的权利来监控美国人的通信。

表 1 合规与执行计划

需要注意的是，《预通知》中对上述四个方面的阐述并未包含 CEP 在最终落实阶段的具体结构与要素，因此 CEP 的具体执行机制仍待后续司法部规定的完善及进一步公示。由于《预通知》中说明了 CEP 的构建将参考外国资产控制办公室（Office of Foreign Assets Control, OFAC）的制裁合规计划（sanctions compliance program, SCP），因此我们根据 OFAC 发布的《OFAC 合规义务承诺框架（A Framework for OFAC Compliance Commitments）》[104]将 SCP 的五个基本部分的相关要求总结如下表，供企业在提前考虑落实 CEP 时进行参考：

必要部分	具体要求
管理层承诺	• 高级管理人员审阅并批准合规计划。 • 高级管理人员确保合规部门的权限和自主，合规计划负责人与高级管理人员之间存在直接汇报关系，包括例行和定期会议。 • 高级管理人员确保合规部门获得充足的资源，包括人力资源、专业知识、信息技术和其他适当资源，且这些资源与企业的业务范围、目标客户和二级市场以及影响其整体风险状况的其他因素相适应。具体包括： 1) 任命一名专职合规人员； 2) 确保企业的合规计划负责人了解并具备与监管规定相关的专业知识，并且拥有将监管要求应用落地的能力。 • 高级管理人员在企业内部推广“合规文化”。具体包括： 1) 允许员工向高级管理人员报告违规行为而不必担心报复； 2) 高级管理人员阻止不当行为与禁止行为，并强调违反监管要求可能受到的影响； 3) 为了遵守监管规定，合规计划有能力监督整个企业的行动，包括但不限于高级管理层。 • 高级管理人员认识到明显违反法律法规及未能遵守合

[104] https://ofac.treasury.gov/media/16331/download?inline (last visited March 12, 2024).

必要部分	具体要求
	规计划的严重性，并采取必要措施以减少未来发生此类情形；此类措施应解决已发生的违规行为的根本原因，并尽可能采用系统性的解决方案。
风险评估	• 风险评估工作一般应包括对企业的全面审查，并评估其与外部环境的接触，以确定企业可能直接或间接与禁止的人员、当事人、国家或地区接触的潜在领域。 • 合规计划负责人可以对以下方面进行评估： 1) 客户、供应链、中间商和交易相对方； 2) 企业提供的产品和服务，包括这些产品和服务如何以及在何处匹配其他金融或商业产品、服务、网络或系统； 3) 企业及其客户、供应链、中间商和交易相对方的地理位置。 • 企业进行风险评估的方式和频率应充分考虑潜在风险——此类风险可能由其客户、顾客、产品、服务、供应链、中介、相对方、交易和地理位置造成，具体取决于该企业的性质。 • 企业应制定一套用于识别、分析和应对所发现特定风险的方法。 • 风险评估应酌情更新，以说明企业在日常业务过程中发现的任何明显违规行为或系统性缺陷的根本原因。
内部控制	有效的合规计划应包括内部控制（及相关政策与程序），以识别、拦截或报告被禁止的行为，并保存相关记录。具体而言： • 企业应制定并实施书面政策和程序，该等政策和程序与企业相关，反映了企业的日常运作和程序，易于遵循，且旨在防止员工从事不当行为。 • 企业应实施内部控制措施，以充分应对并处置其风险评估结果，并使该企业能够有效地识别、拦截、上报可能被禁止的交易和活动，并向企业内适当人员报告。 • 在信息技术解决方案纳入企业内部控制的范围内，企业应选择并校准适合企业风险状况和合规需求的解决方案，并对解决方案进行例行测试，以确保其有效性。 • 企业应通过内部和/或外部审计审查其为遵守监管部门的内部控制要求而实施的政策和程序。 • 企业应确保其记录保存政策和程序充分考虑并符合监管部门的相关要求。 • 企业应确保在获悉其相关内部控制存在薄弱环节时，立即采取有效措施，确定并实施补偿性控制措施，直至能够确定并纠正导致薄弱环节的根本原因。 • 企业应向所有相关人员明确传达合规计划相关的政策和程序，包括 执行计划的内部人员、相关审核人员、在高风险地区运营的业务部门，以及代表企业履行合规计划职

必要部分	具体要求
	责的第三方。 • 企业应指定专人负责将合规计划相关的政策和程序匹配企业的日常运营，应与相关业务部门协商，并应确认企业员工理解。
测试和审计	企业应进行审计以评估当前合规计划的有效性，并且确定合规计划的薄弱环节和缺陷，以协助改进其合规计划以弥补合规方面的漏洞。 • 改进可以包含更新合规计划的内容以应对变化中的风险评估或监管环境。 • 审计可以对合规计划的特定内容进行测试和审计，也可以在整个企业范围内实施测试和审计。 具体而言： • 企业应确保测试或审计人员直接对高级管理人员负责，独立于被审计的活动和部门，并在企业内拥有足够的授权、技能、专业知识的资源。 • 企业应确保其采用的测试或审计程序与其合规计划的级别和复杂程度相适应，并确保相关人员（无论是内部审计还是外部审计）对企业的风险评估和内部控制进行全面、客观的评价。 • 企业应确保在获悉与合规计划有关的、经确认的负面测试结果或审计发现时，将立即采取有效措施，确定并实施补偿控制措施，直至能够确定并纠正导致薄弱环节的根本原因。
培训	应根据企业风险状况制定培训方案，并确保方案中涵盖适当人员（尤其应针对高风险员工开展）。每年应当至少举办一次相关合规培训，并达成以下目标： • 根据需求提供与工作相关的知识； • 传达每个员工的合规责任；并且 • 通过评估使员工对制裁合规培训负责。 具体而言： • 企业应确保其培训计划向员工及利益相关者（如客户、供应商、业务伙伴和交易相对方）提供充分的信息和指导，以支持企业合规工作。 • 企业应提供与合规要求相关的培训，培训范围应与其提供的产品和服务、用户、客户和合作伙伴关系以及运营所在的地理区域相适应。 • 企业应根据其相关风险评估和风险状况，以适当的频率提供与监管要求相关的培训。 • 企业应在获悉经确认的负面测试结果或审计发现，或与其合规计划有关的其他缺陷时，确保立即采取有效措施，为相关人员提供培训或采取其他纠正措施。 • 企业的培训计划应包括便于所有相关人员使用的资源

必要部分	具体要求
	和材料。

表 2 OFAC 制裁合规计划框架

（二）《行政命令》下的法律责任——基于 OFAC 及 CFIUS 罚款制度的对比

除合规计划外，美国司法部还在考虑针对美国主体建立一套民事处罚程序，包括处罚前通知、答复机会与最终决定机制。是否进行罚款罚金数额可能受到以下要素的影响：①违反规定，②进行重大虚假陈述或遗漏，③提供虚假的证明或文件呈交，或④其他行为或因素。

由于司法部在《预通知》中明确前述处罚程序将与 OFAC 及美国外国投资委员会（Committee on Foreign Investment in the United States, CFIUS）的处罚程序相似，我们将 OFAC 与 CFIUS 的相关机制对比总结如下表，供企业提前评估风险参考：

序号	OFAC 处罚程序 （31 CFR Appendix A to Part 501）	CFIUS 处罚程序 （31 CFR § 800.901）
1	**处罚前通知（Pre-Penalty Notice）** • 如果 OFAC 有理由认为发生了违反制裁的行为，并认为民事处罚是适当的，它将根据规定的程序发出处罚前通知。 • 处罚前通知中列出的拟议处罚金额将反映 OFAC 处根据其当时掌握的信息对适当处罚金额的初步评估；随着 OFAC 了解到更多相关信息，最终处罚金额可能会发生变化。 • 如果在发布处罚前通知后，OFAC 认定处罚金额比处罚前通知中的建议处罚金额增加 10%以上是适当的，或者 OFAC 希望指控更多违规行为，它将发布修订版处罚前通知，列出新的建议处罚金额和/或指控的违规行为。	**处罚通知（Notice of the Penalty）** • CFIUS 会向处罚对象发送处罚通知，包括对处罚行为和罚款金额的书面解释。 • 处罚通知将说明认定该行为构成违规的法律依据，并可能列出委员会考虑的任何加重和减轻处罚的因素。
2	**处罚前通知答复（Response to Pre-Penalty Notice）** • 受处罚人可根据规定的程序，提交对处罚前通知的书面答复。 • 一般情况下，回复要么选择同意《处罚前通知》中提出的处罚建议，要么说明不应处罚的原因（或应当处罚，则说明处罚金额应低于建议金额的原因）。	**复议申请（Petition for Reconsideration）** • 处罚对象可在收到处罚通知后 15 个工作日内，向 CFIUS 主席提交复议申请，包括任何辩护、理由、减轻因素或解释。

序号	OFAC 处罚程序 （31 CFR Appendix A to Part 501）	CFIUS 处罚程序 （31 CFR § 800.901）
	• 答复应包括受处罚人所掌握的支持答复中所述论点的所有文件或其他证据，OFAC 将考虑提交的所有相关材料。	• 如有正当理由，经主席和处罚对象书面同意，可延长前述期限。
3	**处罚通知（Penalty Notice）** • 如果 OFAC 在处罚前通知规定的时间内未收到对处罚前通知的答复，或者在收到对处罚前通知的答复并审查其中所载信息和证据后，OFAC 得出结论认为应处以民事罚款，则一般将根据规定的程序发出处罚通知。 • 处罚通知构成 OFAC 对违规行为发生的最终裁定。 • 处罚通知中规定的处罚金额将考虑到受处罚人在回复处罚前通知时提供的相关补充信息。 • 如果没有对处罚前通知做出回应，处罚通知中规定的处罚金额通常与处罚前通知中规定的建议处罚金额相同。	**最终处罚决定（Final Penalty Determination）** • 如果及时收到复议申请，CFIUS 将在收到申请后 15 个工作日内进行审议，然后发布最终处罚决定，主席和处罚对象可通过书面协议延长该期限。 • 如果没有及时收到复议申请，CFIUS 通常会以通知的形式向当事人发出最终处罚决定。

表 3 民事处罚程序对比

（三）《行政命令》下的合规风险——我国出海企业的合规风险与应对

虽然《行政命令》及相关文件确立的规则直接适用的主体对象仅包括美国主体，但如果作为受监管主体的企业所经营的业务涉及受监管数据交易，则相关业务行为受监管审查乃至被要求停止开展，那么与受监管数据交易中与我国企业有关的风险场景，结合《非正式预通知》中提供的规则与交易示例进行适用性分析，仍可能给我国企业带来较为严重的利益损失。

1. 海外 App 运营的风险分析

目前存在出海业务的企业最为关注的风险之一是在《行政命令》逐步落实的背景下，具有中资背景的 App 在美国境内开展运营活动并收集、存储、使用美国用户的个人数据，是否可能触发《行政命令》体系下的禁止/限制规则？

基于禁止/限制规则的基本结构，对于这一潜在风险项的分析可以基于如下思路进行：

1) 是否涉及受监管数据？

不同类别 App 的运营可能涉及的数据类别也不尽相同；但需要注意《行政命令》与《非正式预通知》对于“受监管的个人识别数据”的定义十分宽泛。

虽然《行政命令》与《非正式预通知》要求复数字段与同一个人相关联以构成受监管数据，由于《非正式预通知》中列明的个人识别数据包含了各类常见设备信息、广告标识符、账户信息、网络协议等 App 运营中难免会收集、存储的数据，因此可以较为容易地通过“相互结合的、列明的个人识别数据”这一细分路径也将构成敏感个人数据。

在大规模敏感个人数据的门槛方面，由于目前对于受监管个人识别数据类别的门槛设置尚未确定，且可能的范围较为宽泛（介于 1 万人至 100 万人之间），企业需要着重关注后续规则制定的进展以判断相关业务是否触发该门槛。

2) 是否涉及受监管交易？

对于这一问题的答案在很大程度上取决于 App 运营方的身份、中国母公司的身份，以及作为投资方/控制方的中国母公司是否可能访问到运营方的数据。

在 App 运营方的身份方面，无论运营方在美国境内注册设立、设有分支机构，还是单纯通过远程方式运营 App，均可能会构成《行政命令》与《非正式预通知》下的“美国主体”，进而适用相关监管规则与合规要求。

在中国母公司的身份方面，由于运营方背后的母公司/集团的中资背景，无论如何安排其股权与控制权结构，都不太可能完全避开作为“受监管主体”判断的兜底情形，即被美国司法部长指认为由某受关注国家拥有或控制，或受其管辖或指示。

在母公司的访问控制方面，如果运营方与母公司之间存在涉及受监管数据的数据交互，则在该等交互的数据方面具有较高可能性符合《非正式预通知》中对于数据经纪活动的定义，并且也符合场景示例中“签署协议并授权访问”的基本事实。因此，**如果希望避免落入监管规则的适用范围，相关企业需要在 App 运营企业与境外母公司之间制定并落实数据隔离与访问控制的策略，避免被认定构成受监管数据交易**。

3) 是否涉及豁免交易？

在豁免交易方面，由于 App 用户个人数据的范围较广，相关从业企业能够潜在依赖的豁免事项仅有“作为业务运营一部分实体内部交易”中的“美国主体及其位于受关注国家（或从属于该受关注国家的所有权、指示、管辖或控制）子公司或分公司之间的交易”这一种类别；而该类豁免事项的适用要求企业调整组织架构，将美国主体作为主要运营实体，令境外实体成为美国主体的子公司或分公司——对于多数公司而言，该等调整在业务与管理层面的可行性不高。

2. 海外实体招聘的风险分析

另一类受到较多关注的场景是中资背景的美国主体在员工招聘方面，基于管理、运维、业务等各方面的考量，实践中经常需要聘用中国境内的技术团队及人员，或聘用中方母公司的管理层人员。

(1) 聘用中国技术团队进行运维

假设一家中资背景且经营消费端业务的美国公司收集并维护来自美国消费者的大规模人类基因组数据、个人健康数据等敏感个人数据，该美国公司在信息技术运维方面归入中方母公司的全球运维规划内，并按照母公司的供应商采购策略雇用了一个主要由中国公民组成的团队提供后端服务——如果该后端运维团队可以访问包含大规模敏感个人数据的系统，则该等劳动协议或聘用安排本身构成受监管数据交易。

(2) 聘用中国公民进行开发/项目管理

假设一家中资背景的美国公司通过从社交媒体平台抓取已公开照片的方式收集美国网民的大规模敏感个人数据（包含包括面部数据扫描），并将这些照片输入其自研的数据库用于训练人脸识别算法；基于项目推进效率的考量，该美国公司计划雇佣一位在中国母公司拥有丰富项目管理经验的员工（中国公民）担任数据库项目经理——如果该员工作为项目经理的工作内容将涉及到访问大规模生物特征识别数据，则该等劳动协议或聘用安排本身构成受监管数据交易。

假设一家中资背景的美国金融服务公司正在开发基于生成式人工智能的个人助理应用，并计划将其作为该公司的独立产品销售给客户；基于中国母公司的商密保护需求，该美国公司需要雇佣一名原本任职于母公司的数据科学家（中国公民）领导产品研发——如果作为受雇工作内容的一部分，该数据科学家所拥有的权限允许其访问、下载和传输大规模的个人金融数据，且这些数据不是通常属于公司向其客户提供的金融服务的一部分，则该等劳动协议或聘用安排本身构成受监管数据交易。

(3) 聘用母公司高管进行组织管理

假设一家中资背景的美国公司开发即时通讯类 App 并通过美国软件应用程序数字发行平台在美国发行，该 App 收集美国用户的大规模敏感个人数据；基于中国母公司实际控制要求，该美国公司需要雇用一名原本任职于母公司的高管（非中国公民，但由于其与母公司的历史沿革被美国司法部长指定为受监管主体）担任首席执行官——如果该高管作为首席执行官的权力和职责涉及访问应用程序收集的所有数据，则该等劳动协议或聘用安排本身构成受监管数据交易。

3. 海外项目投资的风险分析

除了上述出海布局业务外，中国企业在美国开展的投资活动也可能受制于《行政命令》及相关政策规则而受到不利影响。具体而言：

假设一家美国公司计划在美国境内建造一个数据中心，该数据中心将存储美国人的大规模个人健康数据，一家中资背景的私募基金同意为数据中心的建设提供资金，以换取该数据中心的多数权益——此时该等投资协议或安排本身可能被认定为构成受监管数据交易。

假设一家中国科技公司与一家开发即时通讯 App 的美国公司签订了股权转让协议或者增资协议，中国公司根据该协议获得了美国公司的少数股权，而该美国公司的 App 系统性地收集其美国用户的大规模敏感个人数据——此时，无论投资协议是否明确授予该外国科技公司访问该等数据的能力，即便协议中明确禁止该等访问，该等投资协议或安排本身仍可能被认定为构成受监管数据交易。

我们理解，监管机构可能不会只根据书面文件来判断受关注国家的投资人是否有权利访问或接触美国大规模敏感个人数据或美国政府相关数据的权利，而是更加看重受关注国家是否有可能通过该交易访问或接触到美国大规模敏感个人数据或美国政府相关数，因此，对投资人基于协议的数据访问权限的限制并不会被认为降低了风险。而与之相反的是，如果上述接受投资的美国公司客观上不具备访问美国大规模敏感个人数据或美国政府相关数据的能力，则中国企业对于该等美国公司的投资一般不会触发针对包含投资协议的受监管数据交易的禁止/控制。

4. 为海外提供云服务的风险分析

中国云服务企业在近年来也凭借高性价比的优势逐渐打开国际市场。随着《行政命令》及相关政策规则的落地实施，中国云服务企业作为供应商提供的 IaaS/PaaS/SaaS 类云服务也可以预见会受到一定程度的冲击。

假设一家美国公司通过 App 从美国用户处收集大规模精确地理位置数据，并与总部位于中国的云服务公司签署协议以处理并存储该等数据——此时该等供应商协议或安排本身将构成受监管数据交易。

假设一家美国医疗机构与一家总部位于中国的云服务公司签署协议以获取信息技术相关的服务，该医疗机构掌握有预期美国病人相关的大规模个人健康数据，且该协议中涉及访问保存有该等大规模个人健康数据的信息系统——此时该等供应商协议或安排本身仍然构成受监管数据交易。

假设一家美国公司由总部位于中国的公司控股并且指定了受监管主体（中国公民）作为管理人员，该公司在美国境内建立数据中心运营数据托管服务，并作为供应商向其他美国公司提供服务以存储美国公司收集的美国大规模敏感个人数据——此时该等供应商协议或安排本身仍构成受监管数据交易。

5. 现阶段相关企业的合规应对

基于上述潜在风险，建议我国出海企业：

1) 从管理层面禁止中国实体对美国实体持有的敏感个人数据的访问；

2) 确保美国实体针对受监管数据单独落实严格的数据隔离存储策略；

3) 在中国实体与美国实体之间采取数据隔离与访问控制措施，将潜在的数据交互行为限制在最小必要的范围内；

4) 在内部程序与制度中明确《行政命令》及《预通知》的合规要求；

5) 尽可能避免中国实体与美国实体之间任何层面的人员穿插混同；

6) 在开展针对美国公司的投资前谨慎评估标的公司涉及的数据类型与数据量；

7) 在为美国公司提供云服务前谨慎评估客户项目涉及的数据类型与数据量，并在服务器中针对客户数据落实数据隔离与访问控制措施。

《行政命令》和《预通知》标志着一个重要规则制定过程的开始。该命令指示司法部在 180 天内发布拟议规则制定通知（Notice of Proposed Rulemaking, NPRM），随后发布最终规则。通过《预通知》，司法部就其考虑纳入拟议规则的许多关键定义征求了公众意见，这为受监管行业提供了一个与政府合作、制定拟议规则和最终规则的机会。

现阶段，除了为之后的合规措施做出预案外，我们还建议所涉行业的相关企业如果初步判断该行政命令相关的限制可能对自身影响较大，则可以根据自身的情况考虑单独或者联合向司法部提出建议和意见，或通过恰当的渠道表达自身的诉求，最大程度争取利益。

结语

《行政命令》标志着美国总统又一次动用 IEEPA 下的紧急权力，并在实际上建立了一个重要的新监管制度。在此，司法部负责在建立和管理这一监管制度方面发挥重要的新作用。虽然现在的重点是监管程序，但司法部最终将需要建立审查许可证和处理民事执法案件的基础措施，这些措施在很大程度上更类似于 OFAC 在管理制裁制度方面所做的工作。《行政命令》在国家安全的考虑下不可避免地偏离了跨境数据自由流动的政策方向；而对于依赖数据跨境传输开展业务的我国出海企业而言，重新评估和调整业务的潜在需求带来了严峻的挑战。因此，企业如何在加强内部管理、提升数据处理的安全性和透明度的同时，在成本可控的前提下确保出海业务的可持续发展，是长远视角下的重要话题。

但即便面对并不乐观的国际形势，数据跨境流动的自由和安全仍不失为所有国家共同关注的议题；而我国企业在困难环境重所积累的经验和智慧，也势必为全球数据治理体系的完善贡献中国智慧和中国方案。

3. 美国数据监管新规观察（下）——美国数据跨境新政的适用场景、应用公式与应对策略

前言

2024 年 12 月 27 日，美国司法部（Department of Justice, DOJ）制定并发布了**《关于落实 EO 14117 行政命令，以防止俄罗斯、伊朗、中国及其他受关注国家获取美国人的大量敏感个人数据和美国政府相关数据的最终规则（Final Rule Implements Executive Order to Prevent Access to Americans' Bulk Sensitive Personal Data and U.S. Government-Related Data by Russia, Iran, China and Other Countries of Concern）》**[105]（以下称"**《最终规则》**"）。此次发布的**《最终规则》将在刊登于《联邦公报》的 90 日后生效**。

《最终规则》的发布是美国司法部基于 2024 年 2 月 28 日美国总统小约瑟夫·罗宾内特·拜登签署并发布的第 14117 号《关于阻止受关注国家获取美国人的大规模敏感个人数据及合众国政府相关数据的行政命令（Executive Order on Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern）》（以下称"**EO 14117**"）的授权，[106]在美国司法部前序发布的《关于受关注国家获取美国人的大规模敏感个人数据和政府相关数据的规定的拟议规则制定预通知（Advance Notice of Proposed Rulemaking: Provisions Regarding Access to Americans' Bulk Sensitive Personal Data and Government-Related Data by Countries of Concern）》[107]（以下称"**《预通知》**"）和于 2024 年 10 月 21 日制定并发布《防止受关注国家获取美国人大规模敏感个人数据及政府相关数据拟议规则通知（Provisions Pertaining to Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons）》（以下称"**《通知》**"）征询意见期结束后进一步发布的正式规定，是美国司法部基于 EO 14117 制定后续其他规则的先导。

以上这些以 EO 14117 为核心的文件矛头直指有关"受关注国家（Countries of Concern）"政府（包括**中国、俄罗斯、朝鲜、古巴、伊朗与委内瑞拉**）以及与其存在关联的实体与个人。EO 14117 及相关文件的发布，在一定程度上体现出美国联邦政府修改其此前主张的数据跨境自由流动政策的意向，可能对"受关注国家"以及企业带来实质性影响。本文将结合目前已公开发布的相关文件，以美国数据跨境流动政策的不变与变化为视角，分析美国在数据跨境政策

[105] 参见 https://www.justice.gov/nsd/media/1382521/d（最后访问时间：2024 年 12 月 29 日）
[106] 参见 https://www.whitehouse.gov/briefing-room/presidential-actions/2024/02/28/executive-order-on-preventing-access-to-americans-bulk-sensitive-personal-data-and-united-states-government-related-data-by-countries-of-concern/ (最后访问时间：12 月 29 日)
[107] 参见 https://www.federalregister.gov/documents/2024/03/05/2024-04594/national-security-division-provisions-regarding-access-to-americans-bulk-sensitive-personal-data-and（最后访问时间：2024 年 12 月 29 日）

上的整体方向；在此基础上，我们将进一步结合企业关注的热点场景为我国企业在相关政策落地前进行风险预判，特别为我国出海企业提供应对参考。

一、EO 14117 的情景引入：出海企业运营触发监管规制的行为或场景

根据《最终规则》、《通知》及《预通知》中提供的信息，我们提供以下 9 个案例作为导引场景，供读者思考——我国企业出海运营的过程中存在的哪些行为或场景，可能触发美国联邦政府根据 EO 14117 及相关文件开展的监管行动。

案例 1：聘用中国技术团队进行运维

假设一家中资背景且经营消费端业务的美国公司收集并维护来自美国消费者的大规模人类基因组数据、个人健康数据等敏感个人数据，该美国公司在信息技术运维方面归入中方母公司的全球运维规划内，并按照母公司的供应商采购策略雇用了一个主要由中国公民组成的团队提供后端服务。

案例 2：聘用中国公民进行项目管理

假设一家中资背景的美国公司通过从社交媒体平台爬取已公开照片的方式收集美国网民的大规模敏感个人数据（包含包括面部数据扫描），并将这些照片输入其自研的数据库用于训练人脸识别算法；基于项目推进效率的考量，该美国公司计划雇佣一位在中国母公司拥有丰富项目管理经验的员工（中国公民）担任数据库项目经理。

案例 3：聘用中国公民进行产品研发

假设一家中资背景的美国金融服务公司正在开发基于生成式人工智能的个人助理应用，并计划将其作为该公司的独立产品销售给客户；基于中国母公司的商密保护需求，该美国公司需要雇佣一名原本任职于母公司的数据科学家（中国公民）领导产品研发。

案例 4：聘用母公司高管进行组织管理

假设一家中资背景的美国公司开发即时通讯类 App 并通过美国软件应用程序数字发行平台在美国发行，该 App 收集美国用户的大规模敏感个人数据；基于中国母公司实际控制要求，该美国公司需要雇用一名原本任职于母公司的高管（受监管主体）担任首席执行官。

案例 5：中资股权投资美国个人健康数据中心

假设一家美国公司计划在美国境内建造一个数据中心，该数据中心将存储美国人的大规模个人健康数据，一家中资背景的私募基金同意为数据中心的建设提供资金，以换取该数据中心的多数权益。

案例 6：中资收购美国 App 运营公司少数股权

假设一家中国科技公司与一家开发即时通讯 App 的美国公司签订了股权转让协议或者增资协议，中国公司根据该协议获得了美国公司的少数股权，而该美国公司的 App 系统性地收集其美国用户的大规模敏感个人数据。

案例 7：中国云服务商为美国公司存储精确地理位置数据

假设一家美国公司通过 App 从美国用户处收集大规模精确地理位置数据，并与总部位于中国的云服务公司签署协议以处理并存储该等数据。

案例 8：中国云服务商为美国医疗机构存储个人健康数据

假设一家美国医疗机构与一家总部位于中国的云服务公司签署协议以获取信息技术相关的服务，该医疗机构掌握有预期美国病人相关的大规模个人健康数据，且该协议中涉及访问保存有该等大规模个人健康数据的信息系统。

案例 9：中资控股云服务商为美国公司存储敏感个人数据

假设一家美国公司由总部位于中国的公司控股并且指定了受监管主体（中国公民）作为管理人员，该公司在美国境内建立数据中心运营数据托管服务，并作为供应商向其他美国公司提供服务以存储美国公司收集的美国大规模敏感个人数据。

以上导引案例的结论与分析，详见本文第四部分。

二、EO 14117 的规则解读：基于风险控制的数据交易监管

EO 14117 针对性地要求美国司法部颁布**禁止**或**限制**美国主体获取、持有、使用、转让、运输或进出口任何外国（政府）或外国公民在其中拥有任何利益的财产（即，“交易”），如果该交易：①涉及大规模敏感个人数据或与美国政府有关的数据；②属于对美国国家安全构成不可接受风险的交易类别；③在司法部规定的生效日期之后启动、待定或完成；④不符合豁免条件，或未基于许可获得授权；并且⑤不属于提供金融服务（包括银行、资本市场和金融保险服务）的正常相关活动和组成部分，也不是遵守任何联邦法定或监管要求（包括执行这些要求的任何法规、指南或命令）所必需的。

基于 EO 14117 的要求，美国司法部在发布的相关文件中中进一步强调：①美国司法部规则禁止美国主体从事“受管辖数据交易（covered data transactions）”类型，因为这些类型的数据交易可能使受关注国家或受管辖主体访问美国的“大规模敏感个人数据（bulk sensitive personal data）”或“政府相关数据（government-related data）”；②一些原本被禁止的交易可能受到限制，并仅在符合某些条件——如，国土安全部发布的“安全要求（security

requirements）”——的情况下才被允许开展；③被禁止或受限制的交易可能适用通用或特定“许可（license）”而被允许开展；④任何限制或禁止的要求均不适用于“豁免交易（exempt transactions）”。

作为一般适用的基本规则，EO 14117 及相关文件**禁止或限制了美国主体与受关注国家或受管辖主体之间涉及大规模敏感个人数据或政府相关数据的受管辖数据交易，除非该等交易构成豁免交易或基于许可获得了授权；但受限交易可以在满足安全要求的前提下开展**（以下称“**禁止/限制规则**”）。我们从禁止/限制规则中汇总提取了 4 组关键要素：

5) 作为监管目标的数据——大规模敏感个人数据、政府相关数据；

6) 作为监管事项的交易——受管辖数据交易、具体禁令；

7) 开展交易的合规路径——实施安全要求、获得许可；

8) 作为监管对象的主体——美国主体、受关注国家与受管辖主体。

（一）EO 14117 规制的应用公式

在上述一般性规则的基础上，通过梳理 EO 14117 与《最终规则》的最新要求，我们理解，EO 14117 的规制公式可以总结为：

禁止或限制美国主体从事任何获取、持有、使用、转让、运输、进出口或参与任何与其他国家或国民有利益关系的交易（即“交易”），如果该交易：

1) *受关注国家*或*受管辖主体*与*美国主体*间开展的交易；

2) 交易对象涉及*受管辖的数据*；

3) 属于*受监管的交易*；

4) 交易发生于《最终规则》的生效期间；

5) 交易不属于*被豁免的交易*；

6) 交易未采取相关*合规路径*（未取得相关许可且未满足安全要求）。

以下我们将围绕上述规制公式中的关键要素及相关概念，基于 EO 14117 与《最终规则》等相关文本，对相关政策规则进行进一步解读。

（二）受关注国家

根据《最终规则》，“受关注的国家”的定义为符合以下条件的任何外国政府：

1) 从事长期或严重不利于美国国家安全或美国人安全的行为；并且

2) 构成利用政府相关数据或大量美国敏感个人数据损害美国国家安全或美国人安全的重大风险。

具体而言，受关注国家共有六个，分别是：**中国（包括中国香港和澳门）、古巴、伊朗、朝鲜、俄罗斯、委内瑞拉**。

（三）受管辖主体

在受关注国家的基础上，《最终规则》将受管辖主体**定义**为符合以下条件的外国主体：

1) 直接或间接，单独或整体上由一个或多个受关注国家或由符合第（2）款的个人持有 50%或以上股份，根据受关注国家的法律组织或特许而设立，或主要营业地位于受关注国家的实体；

2) 直接或间接，单独或整体上由符合第(1)款、第(3)款、第(4)款或第(5)款所述的主体持有 50%或以上股份的实体；

3) 作为受关注国家的员工或承包商的个人，或作为符合第(1)款、第(2)款或第(5)款所述的实体的员工或承包商的个人；

4) 主要作为受关注国家的领土管辖范围内居民的个人；

5) 由司法部长认定的任何主体，无论其位于何处：

   1) 由、曾由或可能由受关注国家或受管辖主体拥有或控制，或受其管辖或指示；

   2) 为、曾为或意图为受关注国家或受管辖主体行事，或代表受关注国家或受管辖主体行事；

   3) 故意引发或指示违反本规则的行为，或可能故意引发或指示违反本规则的行为。

（四）美国主体

《最终规则》将美国主体**定义**为符合以下条件的主体：

1) 任何美国公民、国民或合法永久居民；

2) 根据《美国法典》第 8 编第 1157 条被接纳为美国难民或根据第 1158 条被授予庇护的任何自然人；

3) 任何仅依据美国或美国辖区内的法律成立的实体（包括外国分支机构）；或

4) 任何位于美国境内的主体。

（五）受管辖的数据

1、“敏感个人数据”

《最终规则》将敏感个人数据定义为受管辖的个人标识符、精确地理位置数据、生物标识符、人类组学数据、个人健康数据、个人金融数据，或任何以上数据的结合；但不包括：

1) 与个人无关的公开或非公开数据，包括符合（18 U.S.C. 1839 (3)中定义）“商业秘密”或符合（50 U.S.C. 1708 (d) (7)中定义）“专有信息”的数据；

2) 在交易发生时，根据联邦、州或地方政府记录（如，法庭记录）或广泛传播的媒介（如，通常通过不受限制和开放获取的存储库向公众提供的来源），可以由公众合法获取的数据；

3) IEEPA 的个人通信例外所包含的数据；

4) IEEPA 的信息材料例外所包含的数据。

具体而言，以及相关的细分定义总结如下：

定性	类别	定义
构成敏感个人数据	**受管辖的个人标识符**	**“受管辖的个人标识符”指的是符合以下任一条件的列明的个人标识符：** • 与任何其他列明的个人标识符结合；或 • 与交易方根据交易披露的其他数据结合，使得列明的个人标识符与其他列明的个人标识符或其他敏感个人数据相关联或可关联。 **但“受管辖的个人标识符”不包括：** • 仅与另一项人口统计或联系数据相关联的人口统计或联系数据（例如姓名、出生日期、出生地、邮政编码、居所街道或邮政地址、电话号码和电子邮件地址，以及类似的公共账户标识符）； • 仅与提供电信、网络或类似服务的另一网络标识符、账户验证数据或通话详情数据相关联的网络标识符、账户验证数据或通话详情数据。 **“列明的个人标识符”清单：**

定性	类别	定义
		• 完整或经过截取处理的政府身份证号或账号； • 与金融机构或金融服务公司相关的完整金融账号或个人识别号码； • 基于设备或硬件的标识符——如，国际移动设备识别码（IMEI）、媒体访问控制（MAC）地址、用户身份模块（SIM）卡号码； • 人口统计或联系数据——如，姓名、出生日期、出生地、邮政编码、居所街道或邮政地址、电话号码和电子邮件地址，以及类似的公共账户标识符； • 广告标识符——如谷歌广告标识符、苹果广告标识符或其他移动广告标识符（MAID）； • 账户验证数据——如，账户用户名、账户密码或安全问题答案； • 基于网络的标识符——如，互联网协议（IP）地址或 Cookie 数据； • 呼叫详情数据——如，客户专有网络信息（CPNI）。
	精确地理位置数据	能够将目标明确在 1,000 米精度范围内的实时或历史数据。
	生物标识符	用于识别或认证特定个人的、可测量的物理特征或行为，包括面部图像、声纹和声波模式、视网膜与虹膜扫描、掌纹与指纹、步态、键盘使用习惯，该等数据在生物识别系统中进行了注册且由该系统生成了数据模板。
	人类组学数据	人类组学数据具体指： • 人类基因组数据。表示核酸序列的数据，这些核酸序列构成人类细胞中全部或部分的遗传指令集，包含了个人（42 U.S.C. 300gg-91(d)(17)中定义的）“基因测试”的结果。

定性	类别	定义
		• 人类表观基因组数据。通过对人类表观遗传修饰进行系统层面分析得出的数据，表观遗传修饰是指不涉及 DNA 序列本身改变的基因表达变化。这些表观遗传修饰包括诸如 DNA 甲基化、组蛋白修饰和非编码 RNA 调控等修饰。出于个性化患者护理目的对表观遗传修饰进行的常规临床测量，根据本规则不被视为表观基因组数据，因为此类测量并不需要对样本中的表观遗传修饰进行系统层面的分析。 • 人类蛋白质组数据。通过对人类基因组、细胞、组织或生物体所表达的蛋白质进行系统层面分析得出的数据。出于个性化患者护理目的对蛋白质进行的常规临床测量，不被视为蛋白质组数据，因为此类测量并不需要对样本中发现的蛋白质进行系统层面的分析。 • 人类转录组数据。通过对在特定条件下或特定细胞类型中由人类基因组产生的 RNA 转录本进行系统层面分析得出的数据。出于个性化患者护理目的对 RNA 转录本进行的常规临床测量，根据本规则不被视为转录组数据，因为此类测量并不需要对样本中的 RNA 转录本进行系统层面的分析。 但人类组学数据不包含嵌入人类组学数据集中的病原体特异性数据。
	个人健康数据	与个人的过去、现在或将来的身体或精神健康或状况有关，与为个人提供医疗保健服务有关，或与为个人提供医疗保健的过去、现在或将来的支付有关的健康信息；包括： • 基本的身体测量和健康属性（如，身体功能、身高和体重、生命体征、症状和过敏情况）； • 社会、心理、行为和医学诊断、干预和治疗历史；

定性	类别	定义
		• 测试结果； • 锻炼习惯的记录； • 免疫数据； • 生殖和性健康数据；以及 • 使用或购买处方药物的数据。
	个人金融数据	• 有关个人信用卡、签账卡或借记卡或银行账户的数据，包括购买和付款记录； • 银行、信贷或其他财务报表中的数据，包括资产、负债和债务以及交易； • 信用报告中的数据，或（15 U.S.C. 1681a(d)中定义的）“消费者报告”中的数据。
不构成敏感个人数据	**与个人无关的公开或非公开数据**	包括符合（18 U.S.C. 1839 (3)中定义）“商业秘密”或符合（50 U.S.C. 1708 (d) (7)中定义）“专有信息”的数据。
	可以由公众合法获取的数据	在交易发生时，根据联邦、州或地方政府记录（如，法庭记录）或广泛传播的媒介（如，通常通过不受限制和开放获取的存储库向公众提供的来源），可以由公众合法获取的数据。
	IEEPA 的个人通信例外所包含的数据	不涉及有价物转让的任何邮政、电报、电话或其他个人通信。（如 50 U.S. Code § 1702(b)(1)中所述）
	IEEPA 的信息或信息材料例外所包含的数据	任何信息或信息资料，包括但不限于出版物、电影、海报、唱片、照片、缩微胶卷、缩微胶片、磁带、光盘、CD ROM、艺术品和新闻电讯，不论其格式或传播媒介如何；但不包括技术性、功能性或其他非表达性的数据。 此外，信息或信息材料不包括： • 在数据交易日期尚未完全创建并存在的信息或信息材料，或对信息或信息材料的实质性或艺

定性	类别	定义
		术性的修改或增强，或提供市场营销和商业咨询服务，包括市场推广、制作或共同制作，或协助创建信息或信息材料； • 截至 1994 年 4 月 30 日，或在该时间之后成为出口管制对象的物品，这种管制是为了促进美国的核武器不扩散或反恐政策，或根据 18 U.S.C. chapter 37 被禁止的行为。

表 1 EO 14117 下的敏感个人数据

2、“大规模”敏感个人数据的门槛

“大规模敏感个人数据”的定义为“与美国敏感个人数据有关的任何格式的大规模数据集合或数据集，无论这些数据是否经匿名化、假名化、去标识化或加密处理”。“大规模”一词是指任何在过去 12 个月的任一时间点达到特定门槛的数据——该等特定门槛可以通过单一的受管辖交易的数据量来满足，也可以通过复数受管辖交易的集合的数据量来满足，但后者要求集合内的交易涉及同一受管辖主体。我们比较了《预通知》《通知》与《最终规则》对于“大规模”含义比规定的区别并总结如下：

《预通知》中的规定			《通知》中的规定		《最终规则》中的规定	
敏感个人数据类型	数量门槛		敏感个人数据类型	数量门槛	敏感个人数据类型	数量门槛
	低门槛	高门槛				
受管辖的个人识别数据	超过 1 万名美国个人	超过 100 万名美国个人	受管辖的个人标识符	超过 10 万名美国个人	受管辖的个人标识符	超过 10 万名美国个人
地理位置数据及相关传感器数据	超过 100 部美国设备	超过 1 万部美国设备	精确地理位置数据	超过 1000 部美国设备	精确地理位置数据	超过 1000 部美国设备

《预通知》中的规定			《通知》中的规定		《最终规则》中的规定		
敏感个人数据类型	数量门槛		敏感个人数据类型	数量门槛	敏感个人数据类型		数量门槛
	低门槛	高门槛					
生物识别数据	超过 100 名美国个人	超过 1 万名美国个人	生物识别数据	超过 1000 名美国个人	生物识别数据		超过 1000 名美国个人
生物组学数据	超过 100 名美国个人	超过 1000 名美国个人	人类基因组数据	超过 100 名美国个人	人类组学数据	人类基因组数据	超过 100 名美国个人
						人类表观基因组数据	超过 1000 名美国个人
						人类蛋白质组数据	超过 1000 名美国个人

《预通知》中的规定			《通知》中的规定		《最终规则》中的规定	
敏感个人数据类型	数量门槛		敏感个人数据类型	数量门槛	敏感个人数据类型	数量门槛
	低门槛	高门槛				
					人类转录组数据	超过1000名美国个人
个人健康数据	超过1000名美国个人	超过100万名美国个人	个人健康数据	超过1万名美国个人	个人健康数据	超过1万名美国个人
个人金融数据	超过1000名美国个人	超过100万名美国个人	个人金融数据	超过1万名美国个人	个人金融数据	超过1万名美国个人

表 2 EO 14117 下大规模敏感个人数据的门槛

此外，美国司法部同时强调其将会持续关注技术和威胁的演变，并在必要情况下对目前《最终规则》设定的相关数量门槛进一步调整。

3、美国“政府相关数据”

EO 14117 将美国政府相关数据定义为“具有被受关注国家利用以损害美国国家安全的高度风险的敏感个人数据，无论其数量多少”。《最终规则》则在此基础上对美国政府相关数据提供了细化定义与相应示例如下：

类别	定义
政府精确位置数据	对于在政府相关位置数据列表（§202.1401）上列出的任何区域内任何位置的任何精确地理位置数据，无论其数量多少。这些位置数

类别	定义
	据由于其自身性质或在其地点工作人员的原因，一旦泄漏后被受关注国家掌握或利用将造成较高风险，从而损害美国国家安全。此类相关数据包括这些具体位置的设施情况、所开展活动和人口等相关数据。
政府人员相关联或可关联数据	交易方认为与美国政府（包括军队和情报部门）现任或前任雇员、现任或前任承包商、前任高级官员相关联或可关联的任何敏感个人数据，无论其数量多少。

表 3 EO 14117 下的美国政府相关数据

（六）受监管的交易

EO 14117 将“交易”定义为“获取、持有、使用、转让、运输或进出口任何外国或外国公民在其中拥有任何利益的财产”的行为，并明确了“涉及大规模敏感个人数据或与美国政府有关的数据，对美国国家安全构成不可接受风险的交易”应受限制或禁止。《预通知》则在此基础上将更为具体的“受管辖数据交易”的概念定义为“任何涉及美国大规模敏感个人数据或美国政府相关数据的交易，且该交易也涉及：①数据经纪[108]；②供应商协议；③劳动协议；或④投资协议”。《最终规则》也进一步肯定了这一定义。

值得注意的是单词“**涉及（involve）**”在此处的多次使用，说明了**EO 14117 相关政策规则体系下的“受管辖数据交易”不仅限于直接进行数据交互的交易活动（如，数据经纪），也包括了可能产生数据访问风险的其他交易活动（如，供应商协议、劳动协议、投资协议）**——而在 EO 14117 的语境下，前述有关风险主要是指受关注国家或受管辖主体访问美国大规模敏感个人数据或政府相关数据的风险。如果使用数据合规实务领域常用的概念来理解，**EO 14117 的“受管辖数据交易”实质上覆盖了各类针对大规模敏感个人数据或政府相关数据的、向受关注国家或受管辖主体进行的共享、转移、委托处理、授权访问的行为，以及直接或间接产生受关注国家或受管辖主体访问大规模敏感个人数据或政府相关数据可能性的其他特定交易行为，且“访问”的性质将不会因为应用安全措施而被影响或改变。**

[108] “数据经纪”（Data Brokerage）：指数据的出售、数据访问授权或类似的商业交易，其中涉及将数据从某一方（提供方）转移到另一方（接收方），且接收方并非直接从与已收集或处理的数据相关联或可关联的个人处收集或处理数据。

此外，受管辖交易行为虽然会受到豁免交易、交易许可及数据范围的三重限制，但由于其定义相对宽泛，可以预期相关规则在具体落实时可能仍然存在较广的灰色地带，给执法机关留下比较大的自由裁量权。

针对数据交易的监管，《最终规则》采取了分类监管的策略，将交易分为禁止交易与受限交易，并进一步提出了交易豁免的类别。根据《预通知》《通知》与《最终规则》，我们将相关禁止交易与受限交易的分类标准与禁止/限制规则总结如下：

分类	具体情形	分类标准
禁止交易	数据经纪交易	定义 数据的出售、数据访问授权或类似的商业交易（不包含劳动协议、投资协议或供应商协议），其中涉及将数据从某一方（提供方）转移到另一方（接收方），且接收方并非直接从与已收集或处理的数据相关联或可关联的个人处收集或处理数据。
	涉及人类基因组数据和人类生物样本的交易	定义 涉及转让大规模人类基因组数据或可从中提取此类数据的生物样本的基因组数据交易。
受限交易	涉及提供商品和服务的供应商协议的交易	定义 除了雇佣协议之外的任何协议或安排，其中任何个人向另一人提供商品或服务，包括云计算服务，以换取报酬或其他报酬。
	涉及劳动协议的交易	定义 “劳动协议”指任何个人（不作为独立承包商）直接为他人工作或执行工作职能以换取报酬或其他报酬的协议或安排，包

分类	具体情形	分类标准
		括在董事会或委员会中的任职、执行级别的安排或服务，以及业务级别的劳动服务。
	涉及投资协议的交易	定义 “投资协议”指任何个人以支付或其他报酬为交换，获得直接或间接的所有权利益或与以下相关的权益的协议或安排：①位于美国境内的不动产；②美国法律实体。“投资协议”不包括同时符合以下条件的被动投资情形： • 如果投资是： o 投入（根据 15 U.S.C. 78c(a)(10)定义的）公开交易的证券，以任何货币计价，在任何司法管辖区的证券交易所或通过 “场外交易”的方法进行交易； o 投入由以下实体提供的证券： - （根据 15 U.S.C. 80a-3(a)(1) 定义的）“投资公司”，并且在美国证券交易委员会注册（如，指数基金、共同基金或交易所交易基金）；或 - 任何被选择受监管或根据 15 U.S.C. 80a-53 作为商业发展公司受监管的公司，或上述任何衍生实体；或 o 作为有限合伙人投入风险投资基金、私募股权基金、基金中的基金或其他集合投资基金，如果有限合伙人的贡献仅为资本，且有限合伙人不能做出管理决策，不对超出其投资的任何债务负责，并且没有正式或非正式的能力影响或参与基金或美国人员的决策或运营； • 给予受管辖主体美国主体总投票权与股权利益不到 10%；并且 • 不给予受管辖主体超出被认为是标准少数股东保护权利之外的权利，包括—— o 在董事会或美国人员的等同管理机构的成员或观察

分类	具体情形	分类标准
		员权利，或提名个人担任董事会或等同管理机构的职位的权利，或 ○ 在投票股份之外，对美国主体的实质性商业决策、管理或战略的任何其他参与。

表 4 EO 14117 下的数据交易的分类

（七）被豁免的交易

在禁止交易与限制交易的基础上，《最终规则》还规定了共计十一项被豁免的数据交易，包括：

1) 适用于《最终规则》全文规定的三项豁免——

a. 涉及任何邮政、电报、电话或其他不涉及任何有价物品转让的个人通信的数据交易。

b. 涉及表达性材料信息的进口或出口。

c. 旅行信息，包括个人行李、生活费用和旅行安排的相关数据。

2) 适用于《最终规则》第 C（禁止交易）、D（受限交易）、J（尽职调查与审计）、K（报告与记录保存）子部分的八项豁免——

a. 美国政府的官方交易活动。

b. 涉及提供金融服务通常附带的交易，金融服务包括银行业务、资本市场或金融保险服务；国家银行授权的金融活动；根据银行控股公司法定义为金融性质或补充金融活动的活动；附带个人财务数据的电子商务转移；以及为补偿提供投资组合或资产投资建议的投资管理服务（包括相关辅助服务）则属于金融服务。

c. 美国人与其外国子公司或关联公司之间的公司集团交易（当这些交易通常属于日常行政或业务运营的一部分时），如人力资源、薪资、税务、许可、合规、风险管理、差旅和客户支持。

d. 联邦法律或国际协议要求或授权的交易，其中包括《国际民用航空公约》（2022 年）、《世界卫生组织章程》（1946 年）等协议。此外，如果交易属于遵守联邦法律法规的正常附带活动。

e. 美国财政部（the Department of the Treasury）下辖的美国外国投资委

员会（Committee on Foreign Investment in the United States, CFIUS）明确指定豁免的投资协议。

f. 提供电信服务（包括国际电话、移动语音和数据漫游）过程中通常涉及的交易。

g. 药品、生物制品和医疗器械授权相关数据交易，当其涉及在相关国家获得或维持监管审批所需的“监管审批数据”。

h. 其他临床研究和上市后监督数据。

三、EO 14117 的合规路径：数据交易许可、合规措施与安全要求

（一）数据交易的许可制度

EO 14117 下的数据交易许可制度主要基于外国资产控制办公室（Office of Foreign Assets Control, OFAC）的许可制度修改而来，且与 OFAC 的许可制度类似，同样包括“通用许可（general licenses）”与“特定许可（specific licenses）”，用于批准禁止或受限的受管辖数据交易。

通用许可是对于特定类别交易的全面授权，相当于在对于受管辖数据交易的禁止/限制规则下创设一个例外性的授权，为美国司法部提供了灵活的调整空间，以应对政策需求的变化。援引通用许可开展数据交易的美国主体无需自行进行申请，而只需根据美国司法部对于通用许可的相关规定提交报告与声明，并根据相关要求在交易进行过程中进行充分披露；如果未能履行充分披露义务，则给予通用许可的授权可能面临失效，并同时导致相关交易活动构成对于规定中禁令的违反，相关主体可能面临执法机构制裁的风险。

特定许可是由参与特定受管辖数据交易的特定美国主体主动申请的、一事一议的专项授权，美国主体需要填写并递交各类申请文件以申请特定许可，并可能同样需要遵守通用许可中的持续性披露的义务（如，持续提供有关授权开展的数据交易的报告）。美国司法部目前在针对特定许可考虑要求任何获得特定许可进行大规模敏感个人数据或政府相关数据交易的主体必须在可行的范围内提供保证，确保根据此类交易转移的任何数据都可以恢复、不可逆地删除或以其他方式使其失效。

在上述许可机制外，公司和个人还可以依据法规对特定交易的适用性征求美国司法部（或其他有关部门）的咨询意见。

（二）数据交易的合规安全措施

《最终规则》充分考虑了《通知》与《预通知》中提出的监管受限制交易的措施，并根据 EO 14117 的授权对受限制交易的行为施加了尽调与审计要求；此外，《最终规则》也提出了相应的报告与记录保存要求。

1、尽职调查与审计要求

1) 规定参与受限制交易的条件是按照要求开展尽职调查，并保存尽职调查的文件材料，以协助检查和执法；

2) 规定参与受限制交易的条件之一是开展第三方年度独立审计，并保存年度审计报告，以核实和改进安全要求的遵守情况；

3) 要求制定并实施数据合规计划，并制定基于风险的程序来核实数据流，包括交易中涉及的数据类型和数量、交易各方的身份以及数据的最终用途。

2、报告与记录保存要求

1) 从事涉及云计算服务的受限制交易时，如果受限制交易的 25%或以上直接或间接由受关注国家或受管辖主体所有，相关美国个人应当按要求提交年度报告 ；

2) 任何收到并明确拒绝他人提出从事禁止交易的要约的美国人必须在拒绝后的 14 个工作日内向司法部提交报告；

3) 从事与外国非受管辖主体进行涉及数据经纪的受关注交易的美国人，在知道或怀疑外国交易对手违反了向受关注国家或受管辖主体转售和转移的限制时，应提交报告；以及

4) 美国个人援引交易豁免以向相关国家提供获得或维持监管审批所需的“监管审批数据”，且当这些交易对于获得或维持在受关注国家针对特定业务获取监管批准是必要时，应提交报告，因为将受监管数据直接传输给关注国家的政府实体会带来更高的国家安全风险。

5) 此外，根据《最终规则》第 202.1101 条，需要记录的内容包括：

a. 描述合规程序的书面政策；

b. 记录实施受限交易安全措施的书面政策；

c. 评估对安全措施遵守情况的任何审计结果；

d. 为验证任何受限交易中涉及的数据流而进行的尽职调查的文件；

e. 与每次交易相关的其他相关信息；

f. 数据传输方式的证明文件；

g. 交易开始与结束日期的证明文件；

h. 与交易相关协议的副本；

i. 与交易相关的许可或咨询意见的副本；

j. 总检查长向其发布的任何原始文件的文件编号；

k. 交易过程中接收或创建的相关文件副本；

l. 对记录尽职调查的完整性和准确性进行的年度证明。

6） **根据《最终规则》第 202.1001-202.1002 条从事受限制交易的美国主体所负担的尽职调查与审计义务，以及第 202.1103-202.1104 条规定的部分报告义务，将于《最终规则》刊登于《联邦公报》270 日后生效。**

（三）受限制交易的安全要求

针对受限制交易，EO 14117 要求其满足特定的安全要求作为前提，以缓释其所产生的受关注国家及受管辖主体访问大规模敏感个人数据或政府相关数据的风险。EO 14117 相关文件中强调，该等安全要求旨在降低风险，并可能包括网络安全措施，如基本的组织网络安全态势要求、物理和逻辑访问控制、数据屏蔽和最小化，以及隐私保护技术的使用等。

2024 年 10 月 24 日，美国国土安全部网络安全与基础设施局（Cybersecurity and Infrastructure Security Agency）（以下称“CISA”）按照 EO 14117 的指示制定了**适用于美国司法部所颁布法规中确定的受限制交易的安全要求**（以下称“**安全要求**”）[109]，并于 2024 年 10 月 29 日刊登于《联邦公报》对外征求意见。**CISA 近期也将基于《最终规则》发布针对受限制交易的正式安全要求。**

在司法部提出的合规要求的基础上，CISA 在安全要求中针对所涉数据、所涉系统和组织整体角度，提出如何结合美国现有的网络安全和隐私保护框架（目前暂无详细规定，但 CISA 已经提出将援引 NIST 框架作为参考）**以符合 EO 14117 的要求。**进一步地，**CISA 从“组织和系统层面”以及“数据层面”区分了针对限制性交易的拟议安全要求的主要内容。**

1、组织和系统层面的安全要求

[109] 参见 https://www.cisa.gov/resources-tools/resources/proposed-security-requirements-restricted-transactions（最后访问时间：2024 年 12 月 29 日）

在组织和系统层面，CISA 针对限制性交易的拟议安全要求可分为三个子项，**即“实施组织网络安全政策、实践和要求”“实施访问控制措施”与“开展数据风险评估”**。

1) 实施组织网络安全政策

a. 识别、记录所涉系统的所有系统及数据资产，并定期更新；

b. 在组织层面指定负责网络安全以及合规职能方面的管理人员；

c. 对所涉系统制定应急事件响应计划，在规定时间内修复漏洞；

d. 记录并维护所涉系统的所有供应商协议；

e. 开发并维护所涉系统准确网络拓扑结构；

f. 配置安装或部署新的硬件、固件或软件前的批准流程。

2) 实施访问控制措施

a. 在所涉系统上实施多因素认证或要求密码具备足够强度；

b. 合理且动态配置个人系统权访问权限；

c. 收集所涉系统中与访问及安全相关事件有关的日志（12 个月）；

d. 确保未经授权的介质和硬件不会连接到所涉资产；

e. 默认情况下拒绝所有连接到所涉系统以及相关网络的连接；

f. 在组织层面管理系统身份标识和凭证。

3) 开展数据风险评估

a. 评估应考量数据对外披露的可能性和危害性；

b. 针对评估的风险确定风险缓释措施，追踪缓释措施实施情况。

2、数据层面的安全要求

1) 在受限制交易过程中应用安全加密技术

a. 全面加密：使用行业标准加密技术对所涉数据在传输和存储过程中进行加密；

b. 保障传输层安全：通过互联网传输所涉数据时仅使用 TLS1.2 或更高版本的协议；

c. 密钥管理：生成并安全管理用于加密所涉数据的加密密钥。

2) 应用数据最小化和数据脱敏策略

a. 制定书面的数据留存和删除政策，并每年进行审查且根据情况适时更新；

b. 通过处理实现数据不再属于“受管辖的个人标识符”范畴，或最大限度降低与美国公民实体的关联性。

3) 应用隐私增强技术

不向参与受限制交易的相关人员透露所涉数据或可合理用于重识别所涉数据的信息。

4) 配置身份管理策略

确保受关注国家相关人员无法访问所涉系统及数据。

四、EO 14117 的风险应对：我国出海企业的合规风险与应对

虽然 EO 14117 及相关文件确立的规则直接适用的主体对象仅包括美国主体，但如果作为受监管主体的企业所经营的业务涉及受监管的数据交易，且涉及业务的开展与我国企业相关，则有关业务行为仍存在受到监管审查乃至被要求停止开展的可能性。因此，结合对《预通知》《通知》与《最终规则》中提供的规则与交易示例进行适用性分析，中国企业如未按照 EO 14117 与《最终规则》的合规要求开展商业活动，仍可能受到较为严重的利益损失和其他负面影响。我们将结合本文第一部分中提供的导引案例进行解释说明。

（一）海外 App 运营的风险分析

目前存在出海业务的企业最为关注的风险之一是在 EO 14117 逐步落实的背景下，具有中资背景的 App 在美国境内开展运营活动并收集、存储、使用美国用户的个人数据，是否可能触发 EO 14117 体系下的禁止/限制规则？

基于禁止/限制规则的基本结构，对于这一潜在风险项的分析可以基于如下思路进行：

1、是否涉及受监管数据？

不同类别 App 的运营可能涉及的数据类别也不尽相同；但需要注意 EO 14117 与《最终规则》对于“受监管的个人识别数据”的定义十分宽泛。

由于《最终规则》中列明的个人识别数据包含了各类常见设备信息、广告标识符、账户信息、网络协议等 App 难免会收集、存储的数据，因此可以较为容易地通过“相互结合的、列明的个人识别数据”这一细分路径也将构成敏感个人数据。

在大规模敏感个人数据的门槛方面，对于企业而言，触发《最终规则》中“大规模”门槛的可能性是相对较高的，企业需要清晰梳理所涉及业务涉及的个人信息主体数量是否会实际触发该门槛。

2、是否涉及受监管的交易？

对于这一问题的答案在很大程度上取决于 App 运营方的身份、中国母公司的身份，以及作为投资方/控制方的中国母公司是否可能访问到运营方的数据。

在 App 运营方的身份方面，无论运营方在美国境内注册设立、设有分支机构，还是单纯通过远程方式运营 App，均可能会构成 EO 14117 与《最终规则》下的“美国主体”，进而适用相关监管规则与合规要求。

在中国母公司的身份方面，由于运营方背后的母公司/集团的中资背景，无论如何安排其股权与控制权结构，都不太可能完全避开作为“受监管主体”判断的兜底情形，即被美国司法部长指认为由某受关注国家拥有或控制，或受其管辖或指示。

在母公司的访问控制方面，如果运营方与母公司之间存在涉及受监管数据的数据交互，则在该等交互的数据方面具有较高可能性符合《最终规则》中对于数据经纪活动的定义，并且也符合场景示例中“签署协议并授权访问”的基本事实。因此，**如果希望避免落入监管规则的适用范围，相关企业需要在 App 运营企业与境外母公司之间制定并落实数据隔离与访问控制的策略，避免被认定构成受监管数据交易**。

3、是否涉及豁免交易？

在豁免交易方面，由于 App 用户个人数据的范围较广，相关从业企业能够潜在依赖的豁免事项仅有“作为业务运营一部分实体内部交易”中的“美国主体及其位于受关注国家（或从属于该受关注国家的所有权、指示、管辖或控制）子公司或分公司之间的交易”这一种类别；而该类豁免事项的适用要求企业调整组织架构，将美国主体作为主要运营实体，令境外实体成为美国主体的子公司或分公司——对于多数公司而言，该等调整在业务与管理层面的可行性不高。

（二）海外实体招聘的风险分析

另一类受到较多关注的场景是中资背景的美国主体在员工招聘方面，基于管理、运维、业务等各方面的考量，实践中经常需要聘用中国境内的技术团队及人员，或聘用中方母公司的管理层人员。

1、聘用中国技术团队进行运维

假设一家中资背景且经营消费端业务的美国公司收集并维护来自美国消费者的大规模人类基因组数据、个人健康数据等敏感个人数据，该美国公司在信息技术运维方面归入中方母公司的全球运维规划内，并按照母公司的供应商采购策略雇用了一个主要由中国公民组成的团队提供后端服务（第一部分“案例1”）。

——如果该后端运维团队可以访问包含大规模敏感个人数据的系统，则该等劳动协议或聘用安排本身构成受监管数据交易，将受到 EO 14117 以及《最终规则》的规制。

2、聘用中国公民进行项目管理

假设一家中资背景的美国公司通过从社交媒体平台抓取已公开照片的方式收集美国网民的大规模敏感个人数据（包含包括面部数据扫描），并将这些照片输入其自研的数据库用于训练人脸识别算法；基于项目推进效率的考量，该美国公司计划雇佣一位在中国母公司拥有丰富项目管理经验的员工（中国公民）担任数据库项目经理（第一部分“案例 2”）。

——如果该员工作为项目经理的工作内容将涉及到访问大规模生物特征识别数据，则该等劳动协议或聘用安排本身构成受监管数据交易，将受到 EO 14117 以及《最终规则》的规制。

3、聘用中国公民进行产品研发

假设一家中资背景的美国金融服务公司正在开发基于生成式人工智能的个人助理应用，并计划将其作为该公司的独立产品销售给客户；基于中国母公司的商密保护需求，该美国公司需要雇佣一名原本任职于母公司的数据科学家（中国公民）领导产品研发（第一部分“案例 3”）。

——如果作为受雇工作内容的一部分，该数据科学家所拥有的权限允许其访问、下载和传输大规模的个人金融数据，且这些数据不是通常属于公司向其客户提供的金融服务的一部分，则该等劳动协议或聘用安排本身构成受监管数据交易，将受到 EO 14117 以及《最终规则》的规制。

4、聘用母公司高管进行组织管理

假设一家中资背景的美国公司开发即时通讯类 App 并通过美国软件应用程序数字发行平台在美国发行，该 App 收集美国用户的大规模敏感个人数据；基于中国母公司实际控制要求，该美国公司需要雇用一名原本任职于母公司的高管（非中国公民，但由于其与母公司的历史沿革被美国司法部长指定为受监管主体）担任首席执行官（第一部分“案例 4”）。

——如果该高管作为首席执行官的权力和职责涉及访问应用程序收集的所有数据，则该等劳动协议或聘用安排本身构成受监管数据交易，将受到 EO 14117 以及《最终规则》的规制。

（三）海外项目投资的风险分析

除了上述出海布局业务外，中国企业在美国开展的投资活动也可能受制于 EO 14117 及相关政策规则而受到不利影响。具体而言：

1、中资股权投资美国个人健康数据中心

假设一家美国公司计划在美国境内建造一个数据中心，该数据中心将存储美国人的大规模个人健康数据，一家中资背景的私募基金同意为数据中心的建设提供资金，以换取该数据中心的多数权益（第一部分“案例 5”）。

——此时该等投资协议或安排本身可能被认定为构成受监管数据交易，将受到 EO 14117 以及《最终规则》的规制。

2、中资收购美国 App 运营公司少数股权

假设一家中国科技公司与一家开发即时通讯 App 的美国公司签订了股权转让协议或者增资协议，中国公司根据该协议获得了美国公司的少数股权，而该美国公司的 App 系统性地收集其美国用户的大规模敏感个人数据（第一部分“案例 6”）

——此时，无论投资协议是否明确授予该外国科技公司访问该等数据的能力，即便协议中明确禁止该等访问，该等投资协议或安排本身仍可能被认定为构成受监管数据交易，将受到 EO 14117 以及《最终规则》的规制。

我们理解，监管机构可能不会只根据书面文件来判断受关注国家的投资人是否有权利访问或接触美国大规模敏感个人数据或美国政府相关数据的权利，而是更加看重受关注国家是否有可能通过该交易访问或接触到美国大规模敏感个人数据或美国政府相关数，因此，对投资人基于协议的数据访问权限的限制并不会被认为降低了风险。而与之相反的是，如果上述接受投资的美国公司客观上不具备访问美国大规模敏感个人数据或美国政府相关数据的能力，则中国企业对于该等美国公司的投资一般不会触发针对包含投资协议的受监管数据交易的禁止/控制。

（四）为海外提供云服务的风险分析

中国云服务企业在近年来也凭借高性价比的优势逐渐打开国际市场。随着 EO 14117 及相关政策规则的落地实施，中国云服务企业作为供应商提供的 IaaS/PaaS/SaaS 类云服务也可以预见会受到一定程度的冲击。

1、中国云服务商为美国公司存储精确地理位置数据

假设一家美国公司通过 App 从美国用户处收集大规模精确地理位置数据，并与总部位于中国的云服务公司签署协议以处理并存储该等数据（第一部分“案例 7”）。

——此时该等供应商协议或安排本身将构成受监管数据交易，将受到 EO 14117 以及《最终规则》的规制。

2、中国云服务商为美国医疗机构存储个人健康数据

假设一家美国医疗机构与一家总部位于中国的云服务公司签署协议以获取信息技术相关的服务，该医疗机构掌握有预期美国病人相关的大规模个人健康数据，且该协议中涉及访问保存有该等大规模个人健康数据的信息系统（第一部分“案例 8”）。

——此时该等供应商协议或安排本身仍然构成受监管数据交易，将受到 EO 14117 以及《最终规则》的规制。

3、中资控股云服务商为美国公司存储敏感个人数据

假设一家美国公司由总部位于中国的公司控股并且指定了受监管主体（中国公民）作为管理人员，该公司在美国境内建立数据中心运营数据托管服务，并作为供应商向其他美国公司提供服务以存储美国公司收集的美国大规模敏感个人数据（第一部分“案例 9”）。

——此时该等供应商协议或安排本身仍构成受监管数据交易，将受到 EO 14117 以及《最终规则》的规制。

（五）现阶段相关企业的合规应对

基于上述潜在风险，我国出海企业可以结合企业内部制度管理、技术保障、数据全生命周期安全等方面的合规落实路径，按照以下思路与流程开展 EO 14117 及相关法规文件下的合规动作：

1、数据梳理与适用判断

1) 梳理公司数据资产中与美国境内业务及美国境内居民存在关联的部分，识别其中的敏感个人数据及政府相关数据；

2) 梳理公司涉及数据处理的业务模式，识别其中受管辖的数据交易类型及场景；

3) 针对 EO 14117 对公司业务活动的适用性进行综合判断。

2、技术与管理措施落实

在专业人士的指导下，参考 CISA 发布的安全指南和 NIST 网络安全及隐私保护相关的合规框架及合规工具，从**所涉数据**、**所涉系统**和**组织整体的**角度出发，实施与本组织相适应的安全技术与管理措施，有效控制合规风险。

3、合规落地的日常咨询

1) 基于对法律法规的深入调研分析与丰富的行业实践经验，提供 EO 14117 的落地合规水位指引；

2) 针对未来潜在的监管合规风险，提供事前、事中、事后的全流程合规建议指引与落实方案；

3) 考虑企业现有数据跨境传输合规管理体系，提供纳入 EO 14117 合规要求的制度流程更新。

以上仅为对于相关合规事项的初步、大致的建议，考虑到 EO 14117、《最终规则》及 CISA 安全指南的复杂性、专业性，我们建议相关企业尽早咨询具备丰富全球合规管理与数据跨境传输合规经验的专业外部法律顾问，对于企业的合规计划落实进行指导与协助。（如需对于 EO 14117 的进一步解读，可以通过文末的联系方式联络本文作者）。

结语

EO 14117 及《最终规则》等相关文件的发布，标志着美国总统又一次动用 IEEPA 下的紧急权力，并在实质层面建立了一个重要的新监管制度。在此，司法部负责在建立和管理这一监管制度方面发挥重要的新作用。虽然目前该机制的重点是监管规则和程序的确立，但司法部最终将需要建立审查许可证和处理民事执法案件的基础措施，这些措施在很大程度上更类似于 OFAC 在管理制裁制度方面所做的工作。EO 14117 在国家安全的考虑下不可避免地偏离了跨境数据自由流动的政策方向；而对于依赖数据跨境传输开展业务的我国出海企业而言，重新评估和调整业务的潜在需求带来了严峻的挑战。因此，企业如何在加强内部管理、提升数据处理的安全性和透明度的同时，在成本可控的前提下确保出海业务的可持续发展，是长远视角下的重要话题。

EO 14117 与《预通知》、《通知》以及《最终规则》在不到一年内的陆续发布，在美国历史上开创性地构建起一套以保护美国国家安全为目的的较为完备的敏感数据跨境流动监管体系。从此，美国长期秉持的“数据跨境自由流动”理念被赋予了清晰的边界条件，即该原则仅在数据出境目的地并非“外国对手”或“受关注”国家等特定国家时适用；而一旦涉及向该等特定国家进行数据出境操作，那么“数据跨境自由流动”的一般性原则将存在适用的例外。

因此，我们建议所涉行业的相关企业如果初步判断 **EO 14117** 相关的规则限制可能对自身产生较大影响，即应尽快引入具有丰富全球合规管理经验的律师等外部专家顾问，协助企业从内部管理、业务运营的实际场景出发，逐步搭建符合 **EO 14117** 与《最终规则》监管要求的合规体系，并在外部顾问的协助下确保企业日常运营中的数据处理与跨境传输活动中落实符合该等监管要求的具体合规预防措施；对于可能已经存在风险敞口的出海企业，也建议在外部专家的支持下尽快落实风险缓释措施，面对全球化的监管风险为企业最大程度地争取利益。

环球律师事务所 GLOBAL LAW OFFICE SINCE 1979

欧美中人工智能监管与合规

- 欧盟：《欧盟人工智能法》正式生效
- 美国：联邦和各州的人工智能立法进展
- 中国：《生成式人工智能服务安全基本要求》正式发布
- 欧美中人工智能监管合规关注对比

1. 欧盟：《欧盟人工智能法》正式生效[110]

2024 年 8 月 1 日，全球首部人工智能领域的综合性法律——《制定人工智能统一规则的条例（Regulation Laying Down Harmonised Rules on Artificial Intelligence）》（以下简称“欧盟《人工智能法》”或“EU AIA”）正式生效。从本期开始，《人工智能合规资讯速递与解读》将不定期辟专章对欧盟《人工智能法》逐步进行全面解读，以帮助企业深入理解这部重要法规的框架、要求与影响。

（一）立法过程与重点关注

2021 年 4 月 21 日，欧盟委员会公布了《关于制定人工智能统一规则的条例的建议（Proposal for a Regulation laying down harmonised rules on artificial intelligence）》，旨在应对人工智能特定用途的风险，将其分为 4 个不同等级：不可接受的风险、高风险、有限风险和最低风险。通过这种方式，该条例将确保欧洲人可以信任他们正在使用的人工智能，并建立人工智能卓越生态系统和加强欧盟全球竞争能力。

2022 年 12 月 6 日，欧盟理事会通过了关于欧盟《人工智能法》的共同立场（common position）（文件名称为《欧洲议会和欧盟理事会关于制定人工智能统一规则（人工智能法）并修订某些欧盟法案的条例提案—总体思路》），以确保投放到欧盟市场并在欧盟内使用的人工智能系统的安全，并尊重有关基本权利和欧盟价值观的现行法律。在此基础上，一旦欧洲议会通过自己的立场，理事会就可以开始与欧洲议会进行谈判（“三方谈判（trilogues）”），以期就拟议的法规达成一致意见。

2023 年 6 月 14 日，欧洲议会通过了其关于欧盟《人工智能法》的谈判立场并提出若干修正案，针对人工智能系统的定义、受禁止的人工智能系统的清单进行了重要修改，要求针对在欧盟境内部署高风险人工智能系统开展基本权利影响评估（FRIA），建议纳入分层方法来规制通用人工智能系统，提出强化各成员国监管部门的权力并允许其访问人工智能系统的训练数据与参数，提出建立人工智能办公室以协调后续实施与跨境协作，并同意研究和开发开源人工智能组件应免于遵守欧盟《人工智能法》下的多数合规要求；当月，欧洲议会、欧盟理事会和欧盟委员会三方谈判启动。

2023 年 11 月 18 日，德国、法国、意大利三国就欧盟人工智能监管达成关于人工智能监管方式的联合文件，支持针对人工智能基础模型“通过行为准则的方式进行强制性自律”，但反对“未经检验的规范”；支持对人工智能供应商实施有约束力的义务要求，但建议将相关义务普遍延伸至所有人工智能提供

[110] 作者：孟洁、杜畅

者；要求重点监管人工智能的应用，反对针对人工智能技术与模型开发进行监管。

2023 年 12 月 9 日，欧盟理事会与欧盟议会就欧盟《人工智能法》达成临时协议（Provisional Agreement）。协议文本旨在确保投放到欧洲市场并在欧盟境内使用的人工智能系统的安全，尊重基本权利和欧盟价值观，并刺激欧洲的人工智能投资和创新。

2024 年 2 月，欧洲议会内部市场和消费者保护（IMCO）委员会以及公民自由、司法和内政（LIBE）委员会批准《人工智能法案》政治协议；欧盟理事会宣布由 27 个欧盟成员国副常驻代表组成的 Coreper I 投票通过欧盟《人工智能法》。

2024 年 5 月 21 日，欧盟理事会正式批准欧盟《人工智能法》；2024 年 7 月 12 日，欧盟公报（OJEU）以文件号 Regulation (EU) 2024/1689 正式发布欧盟《人工智能法》的最终文本；2024 年 8 月 1 日，欧盟《人工智能法》正式生效。

（二）关联法规与治理框架

欧盟的人工智能治理的发展从 2017 年起步，逐步形成了**以“1（条例）+1（指令）+1（公约）”3 份关键文件为核心，以“1（欧洲议会）+1（欧盟委员会）+1（人工智能高级别专家组）”3 组来源的政策文件为方向与路径支撑**的立法与政策体系，整体呈现系统化的趋势。

作为欧盟人工智能治理的核心法规，欧盟《人工智能法》历经 3 年的立法进程，于 2024 年 5 月 21 日被欧盟理事会正式批准，将成为全球首部对人工智能领域进行全面监管的法律。作为欧盟 AIA 最为核心的内容，相关从业企业需要重点关注（1）其覆盖人工智能全价值链的主体适用——包括了人工智能系统提供商（providers）、使用商（deployers）、进口商（importers）、分销商（distributors）和产品制造商（product manufacturers），（2）其与 GDPR 第 3 条一脉相承的域外适用——在人工智能系统所产生的输出成果在欧盟使用的前提下适用于位于欧盟境内外的提供商与使用商，（3）其确认并细化的基于风险分级的监管路径——明确禁止部分人工智能实践并对高风险人工智能系统与通用人工智能模型施加较重的义务。

在对人工智能产业相关主体施加正向合规义务之外，人工智能产生损害时的民事责任判定规则同样亟待确认。基于这一考量，2022 年 9 月 28 日欧盟委员会提出了《关于使非合同民事责任规则适应人工智能的指令提案（Proposal for a Directive on Adapting Non-Contractual Civil Liability Rules to Artificial Intelligence）》（以下简称“欧盟《人工智能责任指令》提案”或“AILD 提

案”），并提交欧盟理事会和欧洲议会审议。AILD 提案主要针对与人工智能相关的过错责任案件中受害人举证困难的现实情况，提出了（1）高风险人工智能系统的提供者或其他相同责任人的证据披露义务，（2）拒绝法庭披露命令的过错推定，以及（3）因果关系推定制度。值得注意的是，由于 AILD 属于欧盟立法中的“指令（directive）”而非“条例（regulation）”类别，AILD 即便在欧盟层面通过后仍需各成员国具体落实才会产生实际影响。

此外，欧洲理事会于 2024 年 5 月 18 日在斯特拉斯堡正式通过了全球首个关于负责任地使用人工智能的具有法律约束力的国际条约《人工智能与人权、民主和法治框架公约（Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law）》（以下简称“《人工智能框架公约》”）。《人工智能框架公约》（1）为缔约方确立了“保护人权”及“民主进程与法治”2 项通用义务，（2）为人工智能生命周期设立了人的尊严和个人自主、透明度和监督、可问责性和责任承担、平等和不歧视、隐私和个人数据保护、可靠性、安全创新 7 项基本原则，（3）要求缔约方在确保对人工智能系统生命周期内的活动所造成的侵犯人权行为提供可获得的有效救济，以及（4）确定了公约实施过程中不歧视、残疾人和儿童的权利、公众咨询、数字扫盲和技能、对现有人权的保障、更广泛的保护 6 项实施原则。

在推进上述“1（条例）+1（指令）+1（公约）”3 份关键文件的过程中，欧洲议会、欧盟委员会与（欧盟委员会于 2018 年 6 月设立的）人工智能高级别专家组（High-Level Expert Group on AI）均提供了大量（虽不具备强制效力但具有重要参考意义的）政策文件与指南。

具体而言，“1（欧洲议会）+1（欧盟委员会）+1（人工智能高级别专家组）”3 组来源中值得关注的部分政策文件如下：

主体	政策文件
欧洲议会	2019 年 4 月，《算法问责及透明度监管框架（A Governance Framework for Algorithmic Accountability and Transparency）》 2020 年 10 月，《人工智能、机器人和相关技术的伦理问题框架（Framework of Ethical Aspects of AI, Robotics and Related Technologies）》 2020 年 10 月，《关于发展人工智能技术的知识产权的决议（Resolution on IP Rights for the Development of AI Technologies）》 2020 年 10 月，《人工智能民事责任体系（Civil Liability Regime for AI）》

	2021 年 5 月，《关于教育、文化、视听领域人工智能的决议（Resolution on AI in Education, Culture and the Audiovisual Sector）》 2022 年 5 月，《关于数字时代人工智能的决议（Resolution on AI in a Digital Age）》
欧盟委员会	2018 年 4 月，《欧洲人工智能（Artificial Intelligence for Europe）》 2018 年 12 月，《人工智能协调计划（Coordinated Plan on AI）》 2020 年 2 月，《人工智能白皮书：追求卓越和信任的欧盟路径（White Paper on AI: A European Approach to Excellence and Trust）》 2020 年 7 月，《初始影响评估：人工智能的伦理和法律要求（Inception Impact Assessment: Ethical and Legal Requirements on AI）》 2021 年 4 月，《人工智能法规的影响评估（Impact Assessment of an AI Regulation）》 2021 年 4 月，《更新的人工智能协调计划（Updated Coordinated Plan on AI）》 2024 年 3 月，《关于在研究中负责任地使用生成式人工智能的活动指南（Living Guidelines on the Responsible Use of Generative Artificial Intelligence in Research）》 2024 年 5 月，《生成式人工智能透明度：机器生成内容的识别（Generative AI Transparency: Identification of Machine-Generated content）》
人工智能高级别专家组	2019 年 4 月，《可信赖人工智能的伦理准则（Ethics Guidelines for Trustworthy AI）》 2019 年 6 月，《人工智能的政策和投资建议（Policy and Investment Recommendations of AI）》 2019 年 12 月，《可信赖人工智能评估清单先导（Piloting of Assessment List of Trustweorthy AI）》 2020 年 7 月，《可信赖人工智能最终评估清单（Final Assessment List on Trustworthy AI, ALTAI）》 2020 年 7 月，《可信赖人工智能部门建议（Sectorial Recommendations of Trustworthy AI）》

（三）条款结构与生效安排

根据欧盟《人工智能法》第 113 条的规定，虽然该法规本身将在欧盟公报（OJEU）发布最终文本的 20 天起生效（entry into force），但其实际适用（application）则存在分段适用的详细安排，具体总结如下。

篇章条款	生效日期			
	2025 年 2 月 2 日	2025 年 8 月 2 日	2026 年 8 月 2 日	2027 年 8 月 2 日
第一章：总则				
全文	☑			
第二章：受禁止的人工智能实践				
全文	☑			
第三章：高风险人工智能系统				
第一节：人工智能系统的高风险分类			☑	【基于第 6 条第 1 款及附件一协调产品立法分级为高风险的人工智能系统及相应的主体责任】
第二节：高风险人工智能系统的要求			☑	
第三节：高风险人工智能系统提供者、部署者及其他主体的义务			☑	
第四节：通知当局与被通知机构		☑		
第五节：标准、符合性评估、证书、注册			☑	
第四章：特定人工智能系统的提供商和使用商的透明度义务				
全文			☑	
第五章：通用人工智能模型				
全文		☑		
第六章：支持创新的举措				

篇章条款	生效日期			
	2025 年 2 月 2 日	2025 年 8 月 2 日	2026 年 8 月 2 日	2027 年 8 月 2 日
全文			☑	
第七章：治理				
全文		☑		
第八章：欧盟高风险人工智能系统数据库				
全文			☑	
第九章：进入市场后监测、信息共享、市场监督				
全文		【第 78 条】	☑	
第十章：行为准则和指引				
全文			☑	
第十一章：授权和理事会程序				
全文			☑	
第十二章：罚则				
全文		☑	【第 101 条】	
第十三章：终则				
全文			☑	

（四）主体管辖与适用范围

根据欧盟《人工智能法》第 2 条关于适用范围的规定，其适用于：

- 在欧盟内向市场投放人工智能系统或将其投入使用或向市场投放通用人工智能模型的**提供者（provider）**，无论这些提供者是在欧盟内还是在第三国设立或位于欧盟内；
- 在欧盟内设有机构或者位于欧盟内的人工智能系统**部署者（deployer）**；
- 机构所在地或位于第三国的人工智能系统**提供者（provider）**和**部署者（deployer）**，其人工智能系统的输出用于欧盟；
- 人工智能系统的**进口者（importer）**和**分销者（distributor）**；
- **产品制造商（product manufacturer）**以自己的名义或商标将人工智能系统与其产品一起投放市场或投入使用；
- 未在欧盟境内设立的提供者的**授权代表（authorised representative）**；
- 位于欧盟内的受影响者。

因此，该法案适用主体十分广泛，涵盖人工智能价值链的全流程，包括了与欧盟市场有连接点的人工智能系统提供者、部署者、进口商、分销商和产品

制造商；同时该法案也具有域外适用效力，因此中国企业如涉及向欧盟境内提供包含人工智能的产品或服务，通过经销商间接向欧盟境内提供包含人工智能的产品或服务，或所生产或运营的包含人工智能的产品或服务由于投放行为可以合理预期被欧盟境内用户使用等，则有可能会受到管辖。

此外，欧盟《人工智能法》针对其适用范围还规定了同时基于适用主体与规制客体类别的除外情形，主要包括：

- 专门为军事、国防或国家安全目的而投放市场、投入使用或经修改或不经修改而使用的人工智能系统；
- 属于该法案范围内的第三国公共机关或国际组织；
- 专为科学研究和开发目的而开发和投入使用的人工智能系统和模型。

作为对上述分析的补充，我们将欧盟《人工智能法》对提供者（provider）、部署者（deployer）、进口者（importer）、分销者（distributor）以及授权代表（authorised representative）的定义总结如下：

主体	定义
提供者（provider）	① **开发**人工智能系统或通用人工智能模型的自然人或法人、公共当局、机构或其他团体； ② **开发**了人工智能系统或通用人工智能模型并**将其投放市场**的自然人或法人、公共当局、机构或其他团体； ③ **以自己的名义或商标**（无论以付费还是免费的形式）将人工智能系统**投入运营**的自然人或法人、公共当局、机构或其他团体。
部署者（deployer）	在其自身权利允许范围内（基于其自身目的）使用人工智能系统的自然人或法人、公共当局、机构或其他团体；但在个人非专业活动中使用人工智能系统的情况除外。
进口者（importer）	位于或设立在欧盟境内的自然人或法人，将带有在第三国设立的自然人或法人的名称或商标的人工智能系统投放到欧盟市场。
分销者（distributor）	除提供者或进口者之外，在供应链中将人工智能系统推向欧盟市场的自然人或法人。
授权代表（authorised representative）	位于或设立在欧盟境内的自然人或法人，已收到并接受人工智能系统或通用人工智能模型提供者的书面授权，分别代表其履行和执行欧盟《人工智能法》规定的义务和程序。

（五）领土管辖与域外适用

在上述主体管辖分析的基础上，根据欧盟《人工智能法》第 2 条与第 3 条的规定，涉及域外适用范围的情形及相对应的连接点汇总如下（域外情形使用**加粗标注**，连接点使用下划线标注）：

- 在欧盟内向市场投放（placing on the market）人工智能系统或将其投入运营（putting into service）或向市场投放（placing on the market）通用人工智能模型的提供者，**无论这些提供者是在欧盟内还是在第三国设立或位于欧盟内还是第三国（irrespective of whether those providers are established or located within the Union or in a third country）**；
- 人工智能系统的进口者在欧盟境内向市场投放（placing on the market）**带有在第三国设立的自然人或法人的名称或商标（bears the name or trademark of a natural or legal person established in a third country）的人工智能系统**；
- 人工智能系统的分销者将**带有在第三国设立的自然人或法人的名称或商标（bears the name or trademark of a natural or legal person established in a third country）**的人工智能系统推向（making available）欧盟市场；
- **机构所在地或位于第三国（have their place of establishment or are located in a third country）**的人工智能系统提供者和部署者，其人工智能系统的输出用于欧盟（the output produced by the AI system is used in the Union）；
- **未在欧盟境内设立（not established in the Union）**的提供者的授权代表（authorised representative）。

针对“输出用于欧盟”的情形，欧盟《人工智能法》序言 22 提供了 1 项示例：在欧盟设立的主体将某些人工智能服务承包给在第三国设立的主体，而该第三国主体的人工智能系统所从事的活动属于高风险活动，此时第三国经营者在第三国使用的人工智能系统可以处理在欧盟合法收集并从欧盟转移的数据，并向欧盟境内的主体提供该人工智能系统在处理过程中产生的输出，而无需将该人工智能系统投放市场、投入运营或在欧盟使用。而针对“输出（output）”的范围，欧盟《人工智能法》序言 12 提供的例子包括预测、内容、建议或决定（predictions, content, recommendations, or decisions）。

但上述示例与说明仍未能明确的是，“输出用于欧盟”的连接点是否要求人工智能系统的运营主体意图（intent to）将输出用于欧盟或对于最终输出用于欧盟具有合理可预见性（reasonable foreseeability）；还是在所有输出用于欧盟境内

的情况下，设立在或位于第三国的人工智能系统提供者和/或部署者均受到欧盟《人工智能法》的管辖。对于这一点的相关说明，企业可以理性期待后续欧盟数据保护委员会（EDPB）可能会发布的指南文件。

为便于理解，我们将欧盟《人工智能法》的上述域外适用规则总结如下。

域外适用连接点	价值链主体				
	提供者	部署者	进口者	分销者	授权代表
市场投放	☑		☑		☑
投入运营	☑				☑
推向市场				☑	
输出使用	☑	☑			☑

欧盟《人工智能法》之外，在与数据监管相关的管辖权规则方面，《通用数据保护条例》第 3 条第 2 款同样提供了保护性的域外适用条款。该条以个人数据保护为核心，确立了“经营场所（establishment criterion）”和“处理目的（targeting criterion）”两个平行的判断标准：

- 在“经营场所”标准下，无论数据处理主体的行为是否发生在欧盟内，只要其经营场所位于欧盟境内（an establishment of a controller or a processor in the Union），相关的数据处理行为都会受到《通用数据保护条例》的管辖；
- 在“处理目的”标准下，只要相关主体的行为涉及“向欧盟数据主体提供商品或服务”（the processing activities are related to the offering of goods or services to data subjects who are in the Union）或“对欧盟数据主体在欧盟境内的活动进行监控”（the monitoring of their behaviour as far as their behaviour takes place within the Union），无论该主体是否在欧盟境内有实体存在，相关数据处理行为都会受到《通用数据保护条例》的管辖。

可以看到，欧盟《人工智能法》与《通用数据保护条例》的域外适用条款存在相通之处，但在确认域外适用连接点的路径上也存在一定的不同。

（六）与《通用数据保护条例》的关系

根据欧盟《人工智能法》全文（包含序言与附件）中提及《通用数据保护条例》（即 Regulation (EU) 2016/679）的情况，我们将据文本可知的 2 部法规的关联点总结如下。

事项	欧盟《人工智能法》条款	规定内容
定义	序言 14	欧盟《人工智能法》中使用的“生物特征识别数据”的概念应根据《通用数据保护条例》第 4 条第（14）点所定义的生物特征识别数据的概念来解释。
	第 3 条第（37）项	“特殊类别的个人数据”是指《通用数据保护条例》第 9 条第 1 款中提及的个人数据类别。
	第 3 条第（50）项	“个人数据”是指《通用数据保护条例》第 4 条第（1）点中定义的个人数据。
	第 3 条第（51）项	“非个人数据”是指《通用数据保护条例》第 4 条第（1）点中定义的个人数据以外的数据。
	第 3 条第（52）项	“特征识别分析”是指《通用数据保护条例》第 4 条第（4）点中定义的特征识别分析。
适用范围	第 2 条第 7 款	欧盟关于保护个人数据、隐私和通信保密的法律适用于与欧盟《人工智能法》规定的权利和义务相关的个人数据处理行为。在不影响欧盟《人工智能法》第 10 条第 5 款和第 59 条的情况下，欧盟《人工智能法》的适用不得影响《通用数据保护条例》。
生物特征识别数据的使用限制	序言 39	对于执法以外的目的，《通用数据保护条例》第 9 条第 1 款禁止处理生物识别数据，但欧盟《人工智能法》中规定的有限例外情况除外。 在适用《通用数据保护条例》第 9 条第 1 款时，各国数据保护机关已作出禁止将远程生物特征识别用于执法以外目的的决定。
	序言 54	在欧盟《人工智能法》未禁止的前提下，拟用于根据受《通用数据保护条例》第 9 条保护的敏感属性或特征在

事项	欧盟《人工智能法》条款	规定内容
		生物识别数据基础上进行生物识别分类的人工智能系统应归类为高风险人工智能系统。
	序言 95	在不影响适用的欧盟法律（特别是《通用数据保护条例》）的情况下，考虑到后远程生物识别系统的侵入性，后远程生物识别系统的使用应受到保障措施的约束。
	序言 140	欧盟《人工智能法》应为人工智能监管沙盒中的提供商和潜在提供商提供法律依据，使其仅在特定条件下，根据《通用数据保护条例》第 6 条第 4 款和第 9 条第 2 款第（g）点，使用为其他目的收集的个人数据，在人工智能监管沙盒中开发符合公共利益的某些人工智能系统。
	第 5 条第 1 款	本款第 1 项第（h）点（对于实时远程识别系统的规定）不影响《通用数据保护条例》关于为执法以外目的处理生物识别数据的规定。
	第 26 条第 10 款	本款（对于用于后远程生物识别的高风险人工智能系统的规定）不影响《通用数据保护条例》第 9 条关于生物识别数据处理的规定。
特征识别分析（自动化个人决策）的应用限制	序言 53	在任何情况下，如果本条例附件所列的高风险使用情况下使用的人工智能系统进行了《通用数据保护条例》第 4 条第（4）点意义上的特征分析，其应被视为对健康、安全或基本权利构成重大损害风险。
	序言 140	本条例不应提供《通用数据保护条例》第 22 条第 2 款第（b）点所指的法律依据。
透明性原则	序言 67	为便于遵守欧盟数据保护法，如《通用数据保护条例》，与个人数据相关的

事项	欧盟《人工智能法》条款	规定内容
		数据治理和管理实践应包括确保数据收集初始目的的透明度要求。
偏见识别与纠正	序言 70	为了保护他人的权利免受人工智能系统中的偏见可能导致的歧视，在例外情况下，人工智能系统提供者应在确保自然人的基本权利与自由的适当保障以及《通用数据保护条例》第 9 条第 2 款的前提下，在严格必要的范围内，确保对高风险人工智能系统进行偏见检测和纠正。
开展数据保护影响评估（DPIA）	第 26 条第 9 款	在适用的情况下，高风险人工智能系统的部署者应使用根据欧盟《人工智能法》第 13 条提供的信息，以履行其根据《通用数据保护条例》第 35 条进行数据保护影响评估（DPIA）的义务。
	第 27 条第 4 款	如果欧盟《人工智能法》第 27 条规定的任何义务已通过根据《通用数据保护条例》第 35 条进行的数据保护影响评估（DPIA）得到履行，则本条第 1 款提及的基本权利影响评估（FRIA）应作为该数据保护影响评估的补充。
	第 59 条第 1 款第（c）点	建立有效的监控机制，以确定在沙盒实验过程中是否可能出现《通用数据保护条例》第 35 条所述的数据主体权利和自由方面的任何高风险，并建立响应机制，以迅速降低这些风险，并在必要时停止处理过程。
	附件八第 C 条	对于根据欧盟《人工智能法》第 49 条第 3 款登记的高风险人工智能系统，应提供并不断更新以下信息： …… 5、根据《通用数据保护条例》第 35 条或《数据保护执法指令》（即 Directive (EU) 2016/680）第 27 条进行

事项	欧盟《人工智能法》条款	规定内容
		的数据保护影响评估（如适用）的摘要。
监管机构	第 74 条第 8 款	对于欧盟《人工智能法》附件三第 1 点所列的高风险人工智能系统（限于该等系统用于执法目的、边境管理以及司法和民主的情形），以及附件三第 6 点、第 7 点和第 8 点所列的高风险人工智能系统，成员国应为欧盟《人工智能法》之目的指定以下中的 1 个为市场监督机构： ➢ 《通用数据保护条例》或《数据保护执法指令》项下的数据保护监督机构，或 ➢ 根据《数据保护执法指令》第 41 条至第 44 条规定的相同条件指定的任何其他机构为市场监督机构。

对于欧盟《人工智能法》与《通用数据保护条例》之间在法律适用上的竞合问题中更加整体的事项，目前欧盟层面尚未发布统一的政策或指南；但对于重要的欧盟成员国监管机构对于此问题的态度，则可以从法国数据保护局（CNIL）发布的《欧洲人工智能法规生效：CNIL 的首批问答》中获得部分前瞻，具体内容总结如下。

问题	CNIL 回答
欧盟《人工智能法》是否取代了《通用数据保护条例》的要求？	没有。 欧盟《人工智能法》并不能取代《通用数据保护条例》的要求——这一点非常明确。与此相反，欧盟《人工智能法》旨在通过规定开发和部署可信人工智能系统所需的条件来补充《通用数据保护条例》的要求。 具体来说，《通用数据保护条例》适用于所有个人数据处理，包括： ➢ 在人工智能系统的**开发阶段**：根据欧盟《人工智能法》，人工智能系统或模型的提供者通常被视为《通用数据保护条例》下的数据控制者；

<table>
<tr><th>问题</th><th>CNIL 回答</th></tr>
<tr><td></td><td>➢ 在人工智能系统的使用（或部署）阶段：欧盟《人工智能法》项下的人工智能系统的部署者或用户如涉及处理个人数据，通常会根据《通用数据保护条例》对处理行为负责。
另一方面，欧盟《人工智能法》规定了具体的要求，这些要求有助于遵守 《通用数据保护条例》项下的要求</td></tr>
<tr><td>欧盟《人工智能法》/《通用数据保护条例》：如何判断（哪个）法规适用？</td><td>由于欧盟《人工智能法》仅适用于人工智能系统和模型，而《通用数据保护条例》适用于任何个人数据处理行为，因此有四种可能的情况：
➢ 仅适用欧盟《人工智能法》：这对应特定高风险人工智能系统提供者的情况，该等系统的开发和部署都不需要处理个人数据。
示例：应用于发电厂管理的人工智能系统。
➢ 仅适用《通用数据保护条例》：对于用于开发或使用不受欧盟《人工智能法》约束的人工智能系统的个人数据处理活动，将仅适用《通用数据保护条例》。
示例：用于为广告目的分配利益的人工智能系统，或专门为科学研究目的开发的系统。
➢ 两者都适用：这对应特定高风险人工智能系统，该等系统在开发和/或部署时需要个人数据。
示例：用于简历自动排序的人工智能系统。
➢ 两者都不适用：这对应风险极低且不涉及个人数据处理行为的人工智能系统。
示例：用于电子游戏拟真的人工智能系统。
进一步而言，可以将欧盟《人工智能法》下特定类别客体的《通用数据保护条例》适用情况总结如下表：
<table>
<tr><th>欧盟《人工智能法》的适用规则</th><th>《通用数据保护条例》的适用情况</th></tr>
<tr><td>受禁止的人工智能实践</td><td>系统性适用——所有受禁止的人工智能实践均涉及个人数据处理活动。</td></tr>
<tr><td>（包括具有系统性风险的）通用人工智能模型</td><td>接近于系统性适用——通用人工智能模型常基于使用个人数据进行训练。</td></tr>
</table>
</td></tr>
</table>

问题	CNIL 回答	
	高风险的人工智能系统	在许多情况下（有显著例外，如用于关键基础设施、农用车辆、电梯等的人工智能系统）。
	具有特定透明度风险的人工智能系统	在某些情况下，特别是设计目的包含与自然人直接交互的人工智能系统。
欧盟《人工智能法》对《通用数据保护条例》有何影响？	欧盟《人工智能法》和《通用数据保护条例》所规范的对象并不相同，所要求的方法也不尽相同。 但是，确保欧盟《人工智能法》下的合规有助于（甚至会帮助企业准备）遵守《通用数据保护条例》——例如，**人工智能系统遵守《通用数据保护条例》的情况被纳入欧盟《人工智能法》附件五所规定的欧盟符合性声明的要求中**。 此外，欧盟《人工智能法》还解决了《通用数据保护条例》的某些要求与其自身要求之间的一些矛盾。因此，欧盟《人工智能法》在某些明确界定的问题上延伸并取代了《通用数据保护条例》： ➢ 欧盟《人工智能法》取代了《通用数据保护条例》中**关于执法机构在公共场所使用实时远程生物识别技术的某些规定**，并在某些条件下（第 5 条）例外地允许使用这些技术； ➢ 在特殊情况下，欧盟《人工智能法》**允许处理（《通用数据保护条例》第 9 条定义的）敏感数据，以检测和纠正可能造成伤害的潜在偏差**，但必须在严格必要的情况下并遵守适当的保障措施（第 10 条）； ➢ 欧盟《人工智能法》还**允许在其建立的人工智能监管沙盒中重新使用个人数据（特别是敏感数据）**。监管沙盒旨在促进具有重大公共利益的系统的开发（如，改善卫生健康系统），并由一个专门的机构进行监督，该机构必须事先咨询成员国数据保护机构（如 CNIL），并核实是否符合一系列要求（第 59 条）。	
透明度和文档：如何将欧盟《人工智能法》的这些要求与《通用数据保护条例》	欧盟《人工智能法》和《通用数据保护条例》从不同的角度处理类似的规范（如透明度原则与存档要求），体现了 2 部法规之间的互补性。 **透明度措施**	

<table>
<tr><th>问题</th><th colspan="3">CNIL 回答</th></tr>
<tr><td>的要求联系起来？</td><td colspan="3">《通用数据保护条例》规定了透明度义务，主要包括告知数据被处理的个人数据是如何被处理的（为什么处理、由谁处理、如何处理、处理多长时间等）。这一义务既适用于为开发人工智能系统而进行的数据处理，也适用于对个人或由个人使用人工智能系统（因此导致的个人数据的处理）。
欧盟《人工智能法》规定了非常类似的透明度措施，例如用于训练通用人工智能模型（根据其第 53 条后续将会公布相关模型的清单）的数据或用于与个人互动系统的数据（第 50 条）。

存档要求
欧盟《人工智能法》规定，高风险人工智能系统（根据第 11 和第 13 条）或通用人工智能模型（根据第 53 条）的提供者应向其部署者和用户提供技术文档和信息。这些文档应包括所进行的测试和符合性评估程序的细节。
欧盟《人工智能法》还要求某些高风险人工智能系统的部署者进行基本权利影响评估（FRIA）（第 27 条，主要涉及公共主体和受委托执行公共服务任务的机构）。
《通用数据保护条例》规定的数据保护影响评估（DPIA）的义务补充了欧盟《人工智能法》的这些要求——高风险人工智能系统的提供者和部署者将被推定需要进行 DPIA，且 DPIA 可以为欧盟《人工智能法》所要求的文件提供有用的信息（第 26 条）。
欧盟《人工智能法》还规定，部署者可以依靠提供者已经进行的 DPIA 来进行 FRIA（第 27 条）。由于 DPIA 与 FRIA 共同的目标是采取一切必要措施以针对人工智能系统影响人的健康、安全和基本权利的风险进行缓释，这些分析可以合并成一份文件，以避免过于繁琐的形式主义。

目前，欧盟数据保护委员会（EDPB）正在进行关于个人数据保护规则与欧盟《人工智能法》之间相互作用的工作，以进一步明确衔接点。</td></tr>
<tr><td rowspan="2">欧盟《人工智能法》与《通用数</td><td></td><td>欧盟《人工智能法》</td><td>《通用数据保护条例》</td></tr>
<tr><td>适用范围</td><td>开发（development）、向市场投放（placing on the</td><td>对个人数据的任何处理行为，无论（以及是否）使用</td></tr>
</table>

问题	CNIL 回答		
据保护条例》有哪些不同？		market）与部署（deployment）人工智能系统与模型。	何种技术设备（包括为开发人工智能模型或系统而进行的（训练数据）处理，以及使用人工智能系统过程中进行的处理）。
	目标主体	主要是人工智能系统的提供者与部署者（其次是进口者、分销者与提供者的授权代表）。	数据控制者和处理者（包括欧盟《人工智能法》规制的提供者和部署者）。
	路径	对健康、安全或基本权利采取**基于风险的方法**，包括通过对人工智能系统和模型进行产品安全和市场监督进行落实。	**基于原则的方法**，通过风险评估和问责落实。
	符合性评估的主要模式	内部或第三方符合性评估，包括通过风险管理系统和根据统一标准进行评估。	问责原则（内部文件）和合规工具（认证、行为准则）。
	适用的主要罚则	产品召回或退出市场。 最高可达 **3500 万欧元或全球年营业额 7%**的行政处罚。	正式通知（可要求处理活动进一步符合规定，对处理活动进行暂时或永久限制，包括定期支付罚款）。 最高可达 **2000 万欧元或全球年营业额 4%**的行政处罚。

此外，奥地利数据保护机构（DSB）发布的公告《关于人工智能（AI）条例；数据保护机构就〈通用数据保护条例〉与欧盟〈人工智能法〉之间的关系为私主体提供的信息》以及《关于人工智能与数据保护的问答》中也涉及了对于 2 部法规之间关系的讨论。

在上述文件中，DSB 特别强调：

- 在人工智能系统的开发、运营与使用过程中，当涉及处理个人数据时，《通用数据保护条例》维持并行适用；

- 在开发和使用人工智能系统的过程中处理个人数据时，根据《通用数据保护条例》第 5 条第 2 款，企业负有证明处理行为遵守基本原则的责任；
- 在开发和使用人工智能系统的过程中处理个人数据时，必须具备《通用数据保护条例》第 6 条第 1 款规定的合法性基础；
- 在开发和使用人工智能系统的过程中如涉及处理特殊类别的个人数据，还需要满足《通用数据保护条例》第 9 条的相关要求
- 如果人工智能系统应用于《通用数据保护条例》第 22 条规制的自动化决策系统（如，自动授信或在线招聘），（考虑到欧盟及成员国司法判例该条适用范围的扩张性解释，）相关运营主体需要注意遵守《通用数据保护条例》第 22 条第 2 款、第 3 款以及（如有必要）第 4 款的规定，并参考 WP29 工作组的相关指南。

（七）欧盟及各国已发布的相关指引

随着《人工智能法》的生效落地，欧盟数据保护委员会，以及法国、荷兰、波兰与奥地利等成员国数据保护机构于近期发布了针对该法的配套指导文件，旨在帮助相关人工智能企业理解并落实《人工智能法》的监管要求。相关信息汇总如下。

发布单位	内容	来源
欧盟 EDPB	2024 年 7 月 17 日，EDPB 通过了一份关于数据保护机构（DPA）在《人工智能法》框架中的作用的声明。EDPB 指出，由于 DPA 在处理人工智能法对于基本权利（特别是个人数据保护）的影响方面已经拥有经验和专业知识，因此成员国应尽可能考虑将 DPA 指定为《人工智能法》市场监督机构（MSA），负责《人工智能法》在本国的实施与执行。	https://www.edpb.europa.eu/news/news/2024/edpb-adopts-statement-dpas-role-ai-act-framework-eu-us-data-privacy-framework-faq_en
法国 CNIL	2024 年 7 月 12 日，法国个人信息与自由委员会（CNIL）发布《欧盟<人工智能法>生效：CNIL 的第一个问答》，对《人工智能法》的内容及其与	https://www.cnil.fr/en/entry-force-european-ai-regulation-first-questions-and-answers-cnil

发布单位	内容	来源
	《通用数据保护条例》（GDPR）之间的关系进行了分析解读，明确了《人工智能法》与GDPR的适用关系、《人工智能法案》对于GDPR的影响，以及企业如何结合落实《人工智能法》与GDPR下的透明度义务、基本权利影响评估与数据保护评估等。	
荷兰AP	2024年7月31日，荷兰数据保护局（AP）发布了《<人工智能法案>生效：开发者和部署者需要做的工作》，为人工智能开发者和部署者提供了合规策略指导。AP指出，《人工智能法》对于开发者和部署者提出的各项合规要求将逐步适用，相关企业有必要事先了解该法案的具体内容，识别其所提供或部署的人工智能系统是否落入不可接受风险、高风险、有限风险的范畴，并据以采取相应的合规措施。此外，AP还提示相关企业应当开展人工智能知识培训，确保员工的人工智能知识水平与其人工智能系统的性质和可能影响相适应。	https://www.autoriteitpersoonsgegevens.nl/actueel/ai-verordening-gaat-in-werk-aan-de-winkel-voor-ontwikkelaars-en-gebruikers
波兰UODO	2024年7月17日，波兰数据保护局（UODO）发布了一份声明，就落地《人工智能法》时应当考虑的因素进行了说明。UODO明确，由于人工智能系统可能涉及大规模处理个人数据，包括特殊类别的数	https://uodo.gov.pl/pl/138/3224

发布单位	内容	来源
	据，在波兰法律体系中落地《人工智能法》应当重点考虑与现行个人数据和隐私保护标准相适应。	
奥地利 DSB	2024 年 5 月 31 日，奥地利数据保护局（DSB）发布了一份关于 GDPR 与《人工智能法》的关系的公告。DSB 指出，人工智能系统提供者和部署者在 GDPR 下作为控制者或处理者的义务不受《人工智能法》的影响，并特别提示人工智能系统提供者和部署者应关注 GDPR 第 22 条关于自动化决策的要求。	https://www.dsb.gv.at/dam/jcr:584b2148-2fed-491b-a118-900368bffad2/Informationen%20der%20Datenschutzbeh%C3%B6rde%20zum%20Verh%C3%A4ltnis%20zwischen%20der%20DSGVO%20und%20der%20Verordnung%20(EU)%20%C3%BCber%20k%C3%BCnstliche%20Intelligenz%20(KI-VO)%20f%C3%BCr%20Verantwortliche%20des%20privaten%20Bereichs.pdf
	2024 年 5 月开始，DSB 还发布并持续更新《关于人工智能与数据保护的问答》。	https://www.dsb.gv.at/download-links/FAQ-zum-Thema-KI-und-Datenschutz.html#Frage_3

2. 美国：联邦和各州的人工智能立法进展[111]

2022 年 12 月后，美国针对人工智能技术提出的法律草案数量明显增长。过去的五年里，美国与人工智能相关的法规数量显著增加。2023 年，有 25 项与人工智能相关的法规，而 2016 年仅有 1 项。仅 2023 年一年，人工智能相关法规的总数就增长了 56.3%。全球人工智能调查的一部分显示企业的主要人工智能相关担忧包括隐私、数据安全和可靠性。

（一）美国各部门对于人工智能的定义

美国联邦贸易委员会（FTC）：“究竟什么是‘人工智能’呢？这是一个含义模糊、定义多样的术语。它通常指的是使用计算来执行预测、决策或推荐等各种任务的一系列技术和工具。”（2023 年 2 月）“人工智能有许多定义，往往是非常宽泛的……定义者是谁，谁有权力定义这一点很重要……更重要的是输出和影响。”（2022 年 6 月）。

《加利福尼亚州人工智能透明度法案》California AI Transparency Act：“‘人工智能’或‘AI’是指一个工程或基于机器的系统，其自主程度各不相同，可以根据接收到的输入推断如何生成影响物理或虚拟环境的输出。”

《关于安全、可靠和可信的人工智能开发和使用的行政命令》Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence：“人工智能”是指一个基于机器的系统，可以根据人类定义的目标，做出预测、推荐或决策，影响真实或虚拟环境。人工智能系统使用机器和人类输入来感知真实和虚拟环境；通过自动化分析将这些感知抽象成模型；并通过模型推理来制定信息或行动的选项。（2023 年 10 月 30 日）（平等就业机会委员会（EEOC）也采用了相同的定义。）

（二）美国立法规制人工智能所面临的挑战

防止偏见和歧视——保护人权和公民权利也是一个复杂的非技术问题。

透明度——解释人工智能系统的开发过程是技术性的；解释部署后的人工智能系统如何具体影响个人可能是可能的，也可能不可能，例如，因为人工智能系统会“学习”。

隐私和安全保护——用于开发、部署和改进人工智能的个人数据存在隐私风险；保护数据是一项持久的技术挑战。

有益目的——价值观、目标和上下文的变化意味着有益目的也会演变；人工智能框架中的一个持久目标是保护人类自主权。

---

111 作者：孟洁、黎耀琦

问责制——开发者和/或（组织）用户应对输入、输出和影响负责；开发者的“垃圾输入”会导致部署者的“垃圾输出”。

安全性和可靠性——确保人工智能系统按预期工作并持续如此。

促进创新与抑制创新。

（三）美国联邦层面的立法

1. 美国联邦贸易委员会是目前的主要执法机构：

- 《联邦贸易委员会法》（FTC Act）第 5 节禁止“在商业中或影响商业的不公平或欺骗性行为或做法。”
- 不公平 - 导致或可能对消费者造成重大伤害，这种伤害是消费者无法合理避免的，并且这种伤害没有被对消费者的反向利益所抵消。
- 欺骗性 - 表述、遗漏或行为必须误导（或可能误导）消费者，并且是重要的。
- 与人工智能相关的监管活动：（1）关于人工智能使用和功效的虚假、误导性或未经证实的声明；（2）由滥用人工智能语音克隆技术造成的危害；（3）公司是否考虑了在其产品中使用生成式人工智能的可预见风险；（4）生成式人工智能的训练数据是否包含受版权保护或其他受保护的材料，以及包含的程度。

2.《关于安全、可靠和可信的人工智能开发和使用的行政命令》Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence

- 新的人工智能安全和保障标准 - “随着人工智能能力的增长，它对美国人安全和保障的影响也在增加。”
- 保护美国人的隐私 - “没有保障措施，人工智能可能会进一步威胁美国人的隐私。人工智能不仅使提取、识别和利用个人数据变得更加容易，还增加了这样做的动机，因为公司使用数据来训练人工智能系统。”
- 推进公平和民权 - “不负责任地使用人工智能可能导致并加深司法、医疗保健和住房领域的歧视、偏见和其他滥用行为。”
- 维护消费者、患者和学生的权益 - “联邦政府将……制定适当的保障措施，防止人工智能带来的欺诈、无意的偏见、歧视、侵犯隐私以及其他危害。这些保护措施在医疗保健、金融服务、教育、住房、法律和交通等关键领域尤为重要，因为在这些领域，人工智能的错误或滥用可能会伤害患者、给消费者或小企业带来损失，或危及安全或权利。”

- 支持工人 - “人工智能正在改变美国的工作和工作场所，既带来了提高生产力的希望，也带来了加强工作场所监控、偏见和失业的风险。”
- 促进创新和竞争 - “美国已经在人工智能创新方面领先——去年在美国首次融资的人工智能初创企业数量超过了接下来七个国家的总和。”
- 推动美国在海外的领导地位 - “拜登-哈里斯政府将继续与其他国家合作，支持全球范围内安全、可靠和值得信赖的人工智能部署和使用。”
- 确保政府负责任和有效地使用人工智能 - “人工智能可以帮助政府为美国人民提供更好的结果。它可以扩大机构的监管、治理和发放福利的能力，还可以降低成本并增强政府系统的安全性。然而，使用人工智能也可能带来风险，例如歧视和不安全的决策。”

注意：人工智能行政命令（1）不直接适用于私营部门；（2）指示联邦政府制定某些与人工智能相关的标准，其中一些将适用于人工智能开发者和用户；（3）可被继任总统撤销，但在国会达成全面人工智能立法之前提供了一些结构参考；（4）引发了联邦监管活动的激增。

（四）2024 年美国在人工智能领域的重要进展

2024 年 2 月 22 日，美国司法部长 Merrick B.Garland 宣布 Jonathan Mayer 将担任美国司法部首位首席科技顾问及首席人工智能官（Chief Science and Technology Advisor and Chief Artificial Intelligence (AI) Officer）[112]，协助美国司法部提升在网络安全、人工智能等领域的能力以应对科技发展带来的挑战和机遇。

2024 年 7 月 11 日，美国参议院商务、科学和交通委员会主席 Maria Cantwell 与参议员 Marsha Blackburn、Martin Heinrich，向美国国会提交了《保护内容来源和完整性并防止编辑和深度伪造媒体法》（Content Origin Protection and Integrity from Edited and Deepfaked Media Act, COPIED Act），针对被定义为“完全由算法（包括人工智能）生成的信息，包括图像、视频、音频片段和文本等人类作品”的“合成内容（synthetic content）”，要求 NIST 与美国专利商标局（United States Patent and Trademark Office, USPTO）和美国版权局（United States Copoyright Office, USCO）协商，为以下方面的自愿性、基于共识的标准制定指导方针：（1）合成内容检测；（2）水印和内容出处（content provenance）信息，包括评估、测试和网络安全保护。此外，COPIED Act 还：（1）要求用于生成合成内容的人工智能系统和应用程序的开发者和部署者在 2 年内为用户提供附加内容出处信息的选项；（2）禁止删除、更改、篡改或禁用内容出处信息；（3）禁止在未获得明确知情同意且遵守内容使用条款的情况下，使用具有内容出处的“受管辖内容

[112] https://www.justice.gov/opa/pr/attorney-general-merrick-b-garland-departments-firstesignates-lonathan-maversery，2024 年 12 月 19 日访问。

（即，版权作品的数字表示）”来训练基于人工智能/算法的系统或创建合成内容。

（五）2024 年美国多个州通过人工智能相关法律法规

在州法律层面，科罗拉多州成为美国第一个通过全面人工智能立法的州。科罗拉多 SB205 法案大量借鉴了欧盟《人工智能法》的理念和规定，例如以**“基于风险”的方法**、对“高风险类的人工智能系统”做出特殊规制等。该法案特别强调了人工智能系统在重大决策中引起偏见和歧视的风险，要求避免算法歧视，例如人工智能系统的开发者需要提供材料证明其在算法设计中采取了防歧视措施，部署者则需要建立高风险人工智能系统的风险控制机制、政策和程序，定期开展影响评估以保证人工智能系统的使用符合法律要求和伦理标准。对于消费者而言，该法案规定了透明度义务，要求向消费者清楚地公开其使用的人工智能系统的具体信息，包括系统的功能、限制和可能的风险，向消费者提供选择退出（opt out）的相关信息。

加利福尼亚州也采取了行动，通过了《加州生成人工智能问责法案》（California Generative AI Accountability Act, SB 896）和《生成式人工智能：训练数据透明度法案》（Generative AI: Training Data Transparency Act, AB 2013）等人工智能相关法律法规。其中，SB 896 主要是针对使用生成式人工智能的政府部门，要求每年对生成式人工智能系统的风险进行评估并向立法机关报告调查结果，在人工智能生成的内容中加入清晰醒目的免责声明和提示，并提供人类代表的联系信息等；AB 2013 则要求生成式人工智能系统的开发者（不论规模大小）在 2026 年 1 月 1 日之前公开披露人工智能模型的训练数据的详细信息，包括数据集摘要、数据来源及其所有人、数据类型、是否包含个人或者消费者的信息、受到知识产权保护的信息等。

同期，加利福尼亚州州长却否决了《前沿人工智能模型安全与保障创新法案》（Safe and Secure Innovation for Frontier Artificial Intelligence Models Act, SB 1047），该法案要求开发者必须实施人工智能模型可以完全关闭，严谨记录并持续维护所有安全措施和协议。此外，开发者应每年委托独立审计师审查对相关法案的遵循情况；出现任何涉及人工智能模型的安全问题，都须及时通报给司法部长。否决意见指出，该法案仅针对大规模的基础人工智能模型，未考虑到人工智能模型部署的场景，可能会抑制人工智能产业的发展和创新，也无法有效的解决人工智能技术的潜在风险。

2024 年 3 月 13 日，犹他州州长 Spencer J. Cox 签署了《犹他州人工智能政策法案》（UAIPA）[113]，该法案于 2024 年 5 月 1 日生效。该法案对使用生成式

[113] https://le.utah.gov/~2024/bills/sbillint/SB0149.htm，2024 年 12 月 1 日访问。

人工智能工具与客户打交道的实体提出了信息披露要求，限制了实体就违反消费者保护法的言论指责生成式人工智能的能力，并创建了人工智能政策办公室来管理一个州人工智能项目。

美国佛罗里达州《人工智能法规》则针对广告中的人工智能技术应用做出了特殊规定，从 2024 年 7 月 1 日开始，如果政治广告当中使用了人工智能技术，竞选活动或政治团体将不得不在广告中放置免责声明。一旦该法规生效，佛罗里达州将成为美国最早在政治广告中规范人工智能的州之一[114]。

犹他州人工智能政策法案（Utah Artificial Intelligence Policy Act） - 自 2024 年 5 月 1 日起生效 – 使用、提示或以其他方式导致生成式人工智能与个人互动的企业或个人必须“清楚且显眼地披露”个人正在与生成式人工智能（而非人类）互动“如果个人询问或提示”；从事“受监管职业”（通常需要州许可证或认证）的人员必须“显著”披露消费者在接受监管服务时正在与生成式人工智能互动。

伊利诺伊州人权法和消费者保护法修正案（Amendment to Illinois Human Rights Act and Consumer Protection Law） - 于 2024 年 8 月 9 日通过，自 2026 年 1 月 1 日起生效 – 规定在使用人工智能进行“招聘、雇佣、晋升、续签雇佣、培训或学徒选拔、解雇、纪律处分、任期或雇佣的条款、特权或条件”时，必须通知申请人和员工；明确禁止使用具有“基于受保护类别，包括平等就业机会委员会（Equal Employment Opportunity Commission，EEOC）相关法案所保护的特殊类别人群的歧视效果”的人工智能；并禁止“将邮政编码作为前述受保护类别的代表/代替”。

纽约市地方法律 144：使用自动就业决策工具（NYC Local Law 144: Using Automated Employment Decision Tools）

- 纽约市的雇主在招聘过程中使用任何自动就业决策工具（AEDT）时，必须（除其他要求外）：
  - 在使用 AEDT 之前，每年进行一次由独立审计师进行的偏见审计
  - 公布偏见审计的摘要
- 在使用 AEDT 前至少 10 个工作日通知纽约市的候选人。（雇主可以通过在其网站上、职位发布中或通过邮件或电子邮件发送给候选人来提供通知。）

[114] https://www.wcjb.com/2024/06/19/floridas-ai-regulations-take-effect-july-1/，2024 年 12 月 1 日访问。

AEDT 指的是“任何源自机器学习、统计建模、数据分析或人工智能的计算过程，该过程生成简化输出，包括评分、分类或推荐，用于实质性地协助或替代自由裁量决策，以做出影响自然人的就业决策。”

3. 中国：《生成式人工智能服务安全基本要求》正式发布[115]

生成式人工智能技术是指具有文本、图片、音频、视频等内容生成能力的模型及相关技术[116]。以 ChatGPT、文心一言、通义千问等为代表的生成式人工智能因具备强大的语义理解和文本生成能力，被广泛应用于各行各业。为促进生成式人工智能健康发展和规范应用，2023 年 7 月《生成式人工智能服务管理暂行办法》（以下称“**《暂行办法》**”）正式版发布并于 8 月正式生效，明确提出了企业提供和使用生成式人工智能服务的法律底线。2024 年 3 月 4 日，全国网络安全标准化技术委员会发布了《生成式人工智能服务安全基本要求》（TC260-003）（以下称“**《基本要求》**”），为《暂行办法》的落地提供了国家标准层面上的支撑，提出了生成式人工智能服务提供者在安全方面需遵循的基本要求，包括语料安全、模型安全、安全措施等，并为服务提供者开展安全评估提供了合规参考。

本文从《基本要求》的适用范围、安全基本要求和安全评估要求等方面入手对《基本要求》进行解读，以期为企业在生成式人工智能的使用、运营、研发、接入等全流程提供合规指引。

（一）适用范围

根据《基本要求》第 3.2 条规定，《基本要求》的适用主体为服务提供者，即指以交互界面、可编程接口等形式提供生成式人工智能服务的组织或个人。

值得注意的是，与《互联网信息服务深度合成管理规定》（以下称“**《深度合成规定》**”）将适用主体划分为“技术支持者-服务提供者-服务使用者”不同，《基本要求》沿用了《暂行办法》的主要监管思路，未对“技术支持者”和“服务提供者”进行区分，即无论企业直接面向 C 端用户提供服务（如网页版 ChatGPT 界面），还是通过 API 接口等方式为 B 端用户提供服务（如 OpenAI 面向 B 端用户提供 API 接口），均构成生成式人工智能“服务提供者”。

（二）安全基本要求

生成式人工智能从研发到实际应用涉及模型选择、数据/语料准备、模型训练、模型评估优化和模型部署等多个环节。明确界定生成式人工智能技术从研发到服务不同环节的合规要求，有利于降低生成式人工智能的安全风险，增强“控制”措施的可落地性。

因此，《基本要求》从“语料安全”“模型安全”“安全措施”“内容治理”四个方面提出了服务提供者应承担的基本安全要求，并形成了“研发—服务”的双层安全技术控制体系。特别是第五章“语料安全要求”和第六章“模型安全要求”中，针对

[115] 作者：孟洁、杜畅、尹童晖
[116] 《暂行办法》第二十二条。

生成式人工智能技术的研发提出了合规要求；而第七章“安全措施要求”与第八章“其他要求”则聚焦于向使用者提供生成式人工智能技术服务场景，并在此基础上针对性地提出了一系列合规要求。《基本要求》下安全基本要求的整体结构如下图所示：

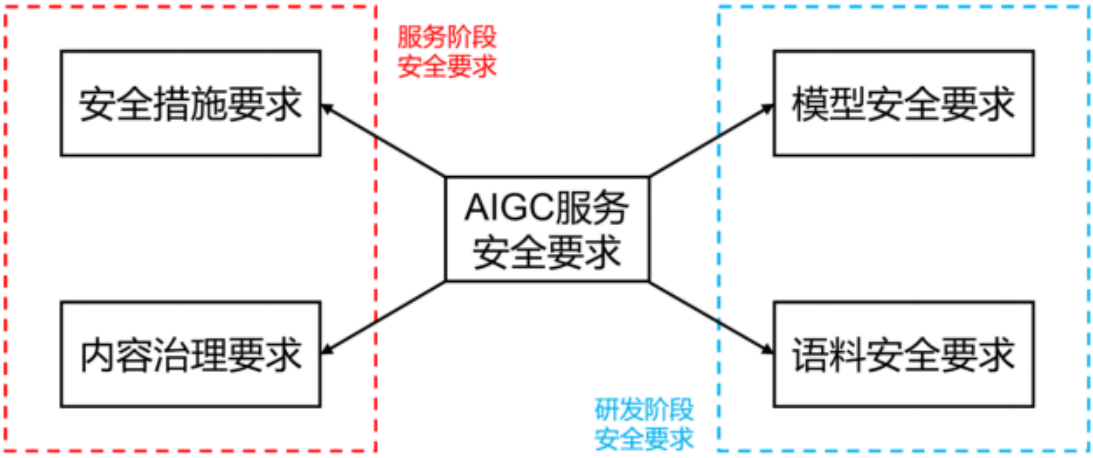


图 1 《基本要求》下的安全基本要求

本章节将对服务提供者在研发阶段和服务阶段分别应遵守的重点合规义务进行解读。

1. 研发阶段安全要求

(1) 语料安全要求

生成式人工智能研发的首要阶段就是处理数据/语料。由于生成式人工智能技术底层模型的训练需要使用已有数据或数据集对算法模型开展训练，并依赖这些数据和相关算法生成用户所需内容，所以语料安全是首要重大风险点，其涉及内容合规、知识产权合规和隐私保护三大方面。例如，在广州互联网法院于 2024 年 2 月 8 日宣判的一起生成式人工智能服务生成的内容侵犯著作权案件中，法院认为由于被告网站生成的案涉图片部分或完全复制了“奥特曼”这一美术形象的独创性表达，并在部分保留了“奥特曼”作品的独创性表达的基础上形成了新的特征，因此被告所提供的服务侵犯了原告对“奥特曼”作品的复制权、改编权；并依据《暂行办法》的有关规定认定涉案平台作为生成式人工智能服务提供者，认为其未能履行应尽的合理注意义务。[117]值得注意的是，法院虽然并未支持原告关于将案涉奥特曼物料从被告训练数据集中删除的主张，但也未支持被告使用该等物料进行训练的合法性，而是以被告并未实际开展模型训练为理由规避了对于该问题的实质判断。该案件触及了训练语料的合规性问题，进一步提醒企业生成式人工智能服务的语料安全是研发阶段必须正视的风险因素。

[117]（2024）粤 0192 民初 113 号。

《基本要求》对于语料合规性的要求从语料来源安全、语料内容安全和语料标注安全三方面进行提出，我们将其中的重点要求总结如下表：

《基本要求》——语料安全要求		
语料来源安全	语料来源管理	采集特定来源语料前应对语料内容进行安全评估，采集特定来源语料后应对语料内容进行核验，不得采集/使用预料内容中含违法不良信息超过5%的来源语料。
	语料搭配管理	提高语料来源的多样性，每种语言及模态的语料均应有多个来源； 如需使用境外语料，应合理搭配境内外来源语料。
	语料来源合法	根据语料的性质（包括开源语料、自采语料、商业语料、使用者输入信息等）确保具备相应的合法证明材料（如具备相关授权协议、具备采集记录等）。
语料内容安全	语料内容过滤	采取关键词、分类模型、人工抽检等方式，充分过滤全部语料中的违法不良信息。
	知识产权保护	设置语料以及生成内容的知识产权负责人，并建立知识产权管理策略； 在训练语料前进行知识产权侵权风险识别与处置； 建立投诉举报渠道； 在用户服务协议中告知使用者可能涉及的知识产权相关风险，并就责任义务进行规定； 根据法律法规与投诉举报情况更新知识产权策略。
	个人信息保护	涉及个人信息的，应取得个人同意或符合法律、行政法规规定； 涉及敏感个人信息的，还需取得个人的单独同意或者符合法律、行政法规规定。
语料标注安全	标注人员管理	对标注人员进行安全培训、考核； 对标注人员的职能进行明确划分，避免一人多责； 预留充足且合理的标注时间。
	标注规则建设	明确标注目标、数据格式、标注方法、质量指标等内容； 应对功能性标注以及安全性标注分别制定标注规则，覆盖数据表述与数据审核等环节。
	标注内容准确	对每一批标注语料进行人工抽检，并对不准确与不良信息进行处置； 对每一条标注语料至少由一名审核人员进行审核并通过。

《基本要求》——语料安全要求		
	存储要求	宜对安全性标注数据进行隔离存储。

表 1 语料安全要求

(2) 模型安全要求

针对模型安全，《基本要求》主要强调模型生成的内容须安全、准确和可靠，重点合规要求请见下表：

《基本要求》——模型安全要求	
使用第三方基础模型	应使用已经主管部门备案的第三方基础模型提供服务。
生成内容安全	训练过程中将生成内容的安全性作为生成结果优劣的主要评价指标； 对每次对话使用者输入的信息进行安全性检测，引导模型生成积极正向内容； 建立常态化检测测评手段，针对发现的安全问题及时整改。
生成内容准确	采取技术措施提高生成内容响应使用者输入意图的能力； 采取技术措施提高生成内容与科学常识和主流认知的符合程度。
生成内容可靠	采取技术措施提高生成内容格式框架的合理性和有效内容含量。

表 2 模型安全要求

综上，服务提供者在落实模型安全相关要求时应结合语料安全的要求尽力做到保证生成的内容积极向上。实践中，服务提供者应首先符合语料来源安全、语料内容安全和语料标注安全的相关要求，而后再进一步落实模型安全的相关要求。

2. 服务阶段安全要求

(1) 安全措施要求

《基本要求》第七章“安全措施要求”重点关注向使用者提供生成式人工智能技术服务场景，我们将其中的重点合规要求总结如下表：

《基本要求》——安全措施要求	
适用人群、场合、用途	充分论证生成式人工智能的必要性、适用性以及安全性； 服务用于关键信息基础设施的，应采取与风险程度以及场景相适应的保护措施； 服务适用未成年人的，应允许监护人设置防沉迷措施、确保仅提供与未成年人民事行为能力相符的付费服务，并展

《基本要求》——安全措施要求	
	示有益于未成年人身心健康的内容； 服务不适用未成年人的，应采取技术或管理措施防止未成年人使用。
服务透明度	在网站首页/说明文档中公开生成式人工智能服务适用的人群、场合、用途信息、生成式人工智能服务的局限性、模型、算法等概要信息、所采集的个人信息和相应用途等内容。
输入信息处理	提供关闭输入信息用于训练的方式（如采用选项方式时使用者从服务主界面开始到达该选项所需操作不超过4次点击）。 将收集使用者输入的状态以及关闭输入信息用于训练的方式显著告知使用者。
内容标识管理	满足国家相关规定以及国家标准的要求（如，《TC260-PG-20233A 网络安全标准实践指南—生成式人工智能服务内容标识方法》）。
计算系统安全	评估供应链的安全性，侧重评估续性、稳定性等方面； 所采用芯片宜支持基于硬件的安全启动、可信启动流程及安全性验证，保障生成式人工智能系统运行在安全可信环境中。
投诉举报处理	提供投诉举报途径及反馈机制； 设定投诉举报处理规则和时限。
服务提供检测	对使用者输入信息进行检测，对于连续三次或一天内累计五次输入违法不良信息采取暂停提供服务等处置措施； 对明显偏激或者诱导生成违法不良信息的问题拒绝回答； 设置监看人员，监看人员数量应与服务规模相匹配。
模型更新升级	制定模型更新、升级的安全管理策略与管理机制； 在模型重要更新、升级后再次自行组织安全评估。
服务稳定持续	将训练环境与推理环境隔离； 对模型输入内容持续监测； 定期对开发框架、代码进行安全审计； 建立备份机制与恢复策略，确保业务连续性。

表 3 安全措施要求

(2) 内容治理要求

《基本要求》第八章对于关键词库、生成内容测试题库和拒绝测试题库进一步提出了具体合规要求，明确各题库应具备全面性和代表性。针对全面性，《基本要求》具体规定了各题库应具备的总规模量。针对代表性，《基本要求》附录A列举了31种语料及生成内容的主要安全风险[118]，基本与《网络信息内容生态

[118] 《基本要求》附录A语料及生成内容的主要安全风险，涉及A1包含违反社会主义核心价值观的内容、A2包含歧视性的内容、A3商业违法违规、A4侵犯他人合法权益、A5无法满足特定服务类型的安全

治理规定》第五条至第七条的规定一一对应。生成式人工智能服务提供者在对语料内容进行过滤时也应充分考虑上述提及的安全风险，摘除违法不良信息。

（三）安全评估要求

1. 安全评估的触发情形

安全评估是确保生成式人工智能服务符合安全基本要求的关键环节。《基本要求》第 4 条明确指出服务提供者在按照有关要求履行备案手续时，须按照该文件的要求进行安全评估，并提交评估报告。该规定为《暂行办法》第十七条规定的落地提供了支撑[119]。

实际上，《暂行办法》并非第一次提出安全评估的监管要求。最早在 2017 年，网信办发布的《互联网新闻信息服务新技术新应用安全评估管理规定》第七条规定，有下列情形之一的，互联网新闻信息服务提供者应当自行组织开展新技术新应用安全评估（即“双新评估”），编制书面安全评估报告，并对评估结果负责：（一）应用新技术、调整增设具有新闻舆论属性或社会动员能力的应用功能的；（二）新技术、新应用功能在用户规模、功能属性、技术实现方式、基础资源配置等方面的改变导致新闻舆论属性或社会动员能力发生重大变化的。

2023 年网信办发布的《具有舆论属性或社会动员能力的互联网信息服务安全评估规定》（以下称“**《评估规定》**”）承接“双新评估”的要求，进一步明确了企业进行安全评估的情形[120]，规定互联网信息服务提供者具有下列情形之一的，应当自行开展安全评估：（一）具有舆论属性或社会动员能力的信息服务上线，或者信息服务增设相关功能的；（二）使用新技术新应用，使信息服务的功能属性、技术实现方式、基础资源配置等发生重大变更，导致舆论属性或者社会动员能力发生重大变化的；（三）用户规模显著增加，导致信息服务的舆论属性或者社会动员能力发生重大变化的；（四）发生违法有害信息传播扩散，表明已有安全措施难以有效防控网络安全风险的。此后，进行安全评估的要求在《互联网信息服务算法推荐管理规定》（以下称“**《算法推荐规定》**”）[121]《深度合成规定》[122]和《暂行办法》中被再次重申，要求具有舆论属性或者社会动员能力的服务提供者，按照国家有关规定开展安全评估。

需求。

119 《暂行办法》第十七条，“提供具有舆论属性或者社会动员能力的生成式人工智能服务的，应当按照国家有关规定开展安全评估，并按照《互联网信息服务算法推荐管理规定》履行算法备案和变更、注销备案手续。”

120 《具有舆论属性或社会动员能力的互联网信息服务安全评估规定》第七条。

121 《互联网信息服务算法推荐管理规定》第二十七条，“具有舆论属性或者社会动员能力的算法推荐服务提供者应当按照国家有关规定开展安全评估。”

122 《互联网信息服务深度合成管理规定》第二十条，“深度合成服务提供者开发上线具有舆论属性或者社会动员能力的新产品、新应用、新功能的，应当按照国家有关规定开展安全评估。”

结合《评估规定》《算法推荐规定》《深度合成规定》与《暂行办法》等文件中的要求，我们将算法业务场景下可能会触发“双新评估”的情形总结如下表：

<table>
<tr><th colspan="3">网信办“双新评估”的算法相关场景</th></tr>
<tr><th>触发情形</th><th>具体情形</th><th>细分场景</th></tr>
<tr><td rowspan="5">具有舆论属性或社会动员能力的信息服务上线，或者信息服务增设相关功能的</td><td colspan="2">具有舆论属性或者社会动员能力的算法推荐服务上线</td></tr>
<tr><td colspan="2">具有舆论属性或者社会动员能力的深度合成服务上线</td></tr>
<tr><td rowspan="2">深度合成服务提供者和技术支持者提供具有右侧功能的模型、模板等工具</td><td>生成或者编辑人脸、人声等生物识别信息</td></tr>
<tr><td>生成或者编辑可能涉及国家安全、国家形象、国家利益和社会公共利益的特殊物体、场景等非生物识别信息的</td></tr>
<tr><td colspan="2">提供具有舆论属性或者社会动员能力的生成式人工智能服务</td></tr>
<tr><td rowspan="2">使用新技术新应用，使信息服务的功能属性、技术实现方式、基础资源配置等发生重大变更，导致舆论属性或者社会动员能力发生重大变化的。</td><td colspan="2">应用新技术、调整增设具有新闻舆论属性或社会动员能力的应用功能</td></tr>
<tr><td colspan="2">新技术、新应用功能在用户规模、功能属性、技术实现方式、基础资源配置等方面的改变导致新闻舆论属性或社会动员能力发生重大变化</td></tr>
<tr><td colspan="3">用户规模显著增加，导致信息服务的舆论属性或者社会动员能力发生重大变化</td></tr>
<tr><td colspan="3">发生违法有害信息传播扩散，表明已有安全措施难以有效防控网络安全风险</td></tr>
<tr><td colspan="3">地市级以上网信部门或者公安机关书面通知需要进行安全评估的其他情形</td></tr>
</table>

表 4 安全评估的触发场景

上述文件虽然提出了适用安全评估的情形，但未就如何进行安全评估作出规定。《基本要求》首次针对安全评估的具体评估内容、评估方法和具体要求进行规定，是对《暂行办法》第十七条的细化，为企业实践提供了参考和指引，具有重要意义。我们将通过下文展开分析。

2. 安全评估的评估内容

根据《评估规定》，开展安全评估，应当对信息服务和新技术新应用的合法性，落实法律、行政法规、部门规章和标准规定的安全措施的有效性，防控安全风险的有效性等情况进行全面评估，并重点评估下列内容：

1) 确定与所提供服务相适应的安全管理负责人、信息审核人员或者建立安全管理机构的情况；

2) 用户真实身份核验以及注册信息留存措施；

3) 对用户的账号、操作时间、操作类型、网络源地址和目标地址、网络源端口、客户端硬件特征等日志信息，以及用户发布信息记录的留存措施；

4) 对用户账号和通讯群组名称、昵称、简介、备注、标识，信息发布、转发、评论和通讯群组等服务功能中违法有害信息的防范处置和有关记录保存措施；

5) 个人信息保护以及防范违法有害信息传播扩散、社会动员功能失控风险的技术措施；

6) 建立投诉、举报制度，公布投诉、举报方式等信息，及时受理并处理有关投诉和举报的情况；

7) 建立为网信部门依法履行互联网信息服务监督管理职责提供技术、数据支持和协助的工作机制的情况；

8) 建立为公安机关、国家安全机关依法维护国家安全和查处违法犯罪提供技术、数据支持和协助的工作机制的情况。

3. 安全评估的评估方法

在上述一般性适用的安全评估要求的基础上，《基本要求》明确要求生成式人工智能的安全评估应对语料安全、模型安全、安全措施、内容治理分别进行评估并形成单独的评估结果。换言之，上述四部分基本安全要求的落地情况将共同构成最终的安全评估报告。因此，服务提供者在日常合规管理措施中必须落实各部分的安全基本要求才能确保后续的安全评估工作顺利推进。

此外，《基本要求》针对评估结果的形成方式进行了具体规定，我们总结如下表：

《基本要求》——安全评估方法			
各条款结果		整体结论	
结果判定	证明要求	结果判定	具体标准
符合	应具有充分的证明材料。	全部符合	各条款的评估结果均为符合或不适用时。
不符合	应说明不符合的原因，有以下特殊情况的应补充说明：采用与本文件不一致的技术或管理借施,但能达到同样安全效果的，应详细说明	部分符合	部分条款评估结果为不符合时。

《基本要求》——安全评估方法			
	并提供借施有效性的证明；已采取技术或管理借施但尚未满足要求的,应详细说明采取的措施和后线满足要求的计划。	全部不符合	全部条款均为不符合时。
不适用	应说明不适用理由。	注：推荐性条款（使用“宜”或“不宜”的条款）的评估结果不影响整体评估结论。	

表 5 安全评估方法

此外，针对安全评估报告，《基本要求》要求：

1) 各条款的评估结果以及相关证明、支撑材料应统一写入评估报告；

2) 因格式原因，部分条款的评估结果和相关情况无法写入正文的，应统一写入附件；

3) 评估报告中应包含整体评估结论；

4) 自行开展安全评估的，评估报告应至少具有三名负责人共同签字——

① 单位法定代表人；

② 安全评估工作整体负责人（应为单位主要管理者或网络安全负责人）；

③ 安全评估合法性部分负责人（应为单位主要管理者或法务负责人）；

④ 如上述相关负责人存在兼任情形时，可由法定代表人同意签字，但应另附说明。

4. 安全评估的具体要求

针对《基本要求》中安全评估的具体要求，我们总结如下表：

《基本要求》——安全评估要求		
语料安全评估	人工抽检	采用人工抽检,从全部语料中随机抽取不少于4000 条语料，合格率不应低于 96%。
	技术抽检	从全部语料中随机抽取不少于总量 10%的语料，抽样合格率不应低于 98%。
	关键词库、分类模型	对采用的关键词库和分类模型进行评估。
生成内容安全评估	人工抽检	从生成内容测试题库中随机抽取不少于 1000 条测试题,模型生成内容的抽样合格率不应低

《基本要求》——安全评估要求		
		于 90%。
	关键词抽检	从生成内容测试题库中随机抽取不少于 1000 条测试题，模型生成内容的抽样合格率不应低于 90%。
	分类模型抽检	从生成内容测试题库中随机抽取不少于 1000 条测试题，模型生成内容的抽样合格率不应低于 90%。
问题拒答评估	**拒答测试题库**	评估是否建设符合要求的拒答测试题库。
	应拒答测试题库	随机抽取不少于 300 条测试题，模型的拒答率不应低于 95%。
	非拒答测试题库	随机抽取不少于 300 条测试题，模型的拒答率不应高于 5%。

表 6 安全评估要求

（四）总结与展望

随着《暂行办法》落实的逐步铺开，生成式人工智能技术研发与服务提供的相关从业企业积极开展算法备案与生成式人工智能服务上线备案的工作，大量获批的模型与服务陆续符合合规上线要求，监管层面对于准入层面的政策落实初见成效。但即便在满足准入门槛的情况下，作为新兴领域的生成式人工智能技术也需要准入后的持续监管措施来避免各类安全风险。在这一背景下，《基本要求》的出台恰逢其时，为推动服务提供者落实生成式人工智能服务安全自评估义务，以及监管部门开展准入后的安全评估与监督检查工作提供了参考。

我们建议生成式人工智能的相关从业企业高度关注《基本要求》中提出的自评估方法与要求，根据《暂行办法》与《评估规定》下规定的触发条件判断是否需要开展生成式人工智能安全自评估。同时，即便在暂时无需开展自评估的情形下，也应在日常管理与业务流程中落实《基本要求》对于研发与服务阶段规定的安全要求，为业务规模扩展等情形下可能面临的安全自评估与监督检查要求提前做好充分准备。

4. 欧美中人工智能监管合规关注对比

	欧盟	美国	中国
立法进展	进度最快，除相关的监管指导性文件之外已通过专门的法案。2024 年 5 月，欧洲议会正式通过《人工智能法案》。	对监管立法比较谨慎，联邦层面暂无统一立法，立法提案大多针对特定问题，州层面呈现分散探索人工智能监管的态势。联邦政府在为市场提供监管参考时通常采用白皮书、指南等形式；地方政府在提供监管参考时则多以立法形式。	2023 年 7 月通过《生成式人工智能服务管理暂行办法》。
政策导向	以基本人权为底层逻辑，侧重保障个人权利。	以促进产业发展为主，在治理时侧重于维护公平和保护隐私。	以社会风险控制为关注点，开展区分价值链主体、技术集中视角的监管方向。
治理模式	通过专门立法实施强监管，基于比例原则的风险分级治理。	多依靠地方法规、行业规则以及倡议等实施监管，虽然近几年监管态势逐渐趋严，但还是着力于“避免妨碍人工智能创新和增长的不必要的监管或非监管活动”。	通过专门立法实施强监管，基于人工智能生命周期主体的风险治理。
监管重点	基于风险预防理念，将风险划分等级；为通用人工智能模型设置专有规则；确立人工智能监管沙盒制度，激励人工智能创新，保护企业发展。	侧重于对人工智能在具体应用场景下的监管，核心是以技术的发展应用为重点，逐步向加强监管靠拢。	侧重于对对具有舆论属性与社会动员能力的相关产品和/或服务的相关风险的关注。

	欧盟	美国	中国
监管机构	欧盟层面成立人工智能委员会、人工智能办公室等机构；成员国应指定一个国家监管机构负责法规的执行，并代表该国参加欧盟人工智能委员。	一般来说，独立的监管机构作为政府权力的延伸与补充，其创建的目的通常是对不公平举措进行预防。目前，美国并未统一设置人工智能监管机构，各政府部门通过发布对现有规则的解释与指引或发布新规则来对人工智能进行监管，监管主体有联邦政府及其相关部门或机构、州政府及其相关部门或机构。	网信办、科技部、发改委、工信部、数据局等多部门均涉及人工智能相关技术、产业的监管职能。
监管机制	欧盟层面与成员国层面采取分级监管、多种监管，并实行高额的行政处罚，且将公私机构一起纳入监管范围。	不是单一的依赖行政监管，强调政府部门与私营部门的协作，同时为了推进人工智能的发展，主张企业进行自我监管。	目前暂时没有成文的监管权职划分，各部门在其现有监管职能与权力清单范围内实施人工智能监管。
伦理	2018 年，欧盟委员会成立了一个独立的人工智能的高级别专家组（High-Level Expert Groupon Artificial Intelligence, AIHLEG），以起草与制定欧盟人工智能伦理准则的初稿。 2019 年 4 月正式发布了《可信的人工智能伦理准则》。 2024 年 3 月通过的《人工智能法案》基于 AI 伦理的基本要求，将具有共识性的关键要素上升	美国《2022 年算法问责法案》要求使用自动化决策系统作出关键决策的企业应研究并报告系统对消费者的影响。 拜登《关于通过联邦政府进一步促进种族平等和支持服务不足社区的行政命令》规定了大模型应避免由于输入训练数据中的歧视信息。 州层面提交算法歧视相关法案等。	《网络安全标准实践指南—人工智能伦理安全风险防范指引》2021.1 《新一代人工智能伦理规范》2021.9

	欧盟	美国	中国
	至法律规则的层面，以此来设定相应的制度设计。		
安全	《人工智能法案》从人工智能的风险分级管理着手，覆盖产业链上的不同责任主体作为规范对象，详细规定各参与者的义务	美国白宫科技政策办公室《人工智能权利法案蓝图》提出了指导人工智能的设计、使用和部署的五项原则，其中有四项均涉及安全保护，即技术的安全性和有效性、保护数据隐私、告知及解释义务、人类参与决策。 美国参众两院《美国数据隐私和保护法案》进一步明确了“覆盖算法”及其规范等说明。	TC260-003《生成式人工智能服务安全基本要求》
治理	欧盟《人工智能法案》成立人工智能办公室。 和各成员国执法监督机构协同合作。	拜登《关于安全、可靠和值得信赖的人工智能的行政命令》	《新一代人工智能治理原则——发展负责任的人工智能》 2019.6 《国家新一代人工智能标准体系建设指南》 2020.8

环球律师事务所 GLOBAL LAW OFFICE SINCE 1979

环球数字经济与网络数据安全团队编制

联系人： 孟洁

邮箱 / E. mengjie@glo.com.cn

电话 / T.（86 10）6584 6768

手机 / M.（86 10）158 1105 0850

订阅/E.

dataprotection@glo.com.cn

请您知悉，本集锦的内容均不构成任何形式的法律意见。

如您欲进一步了解本集锦所涉及的内容，您可以通过上述方式联系我们。

版权声明

本报告每篇文章的版权属于相应作者所有或者共有，并受法律保护。您可以通过转载、摘编的方式使用本报告每篇文章的文字或者观点，但不得对本报告所选取的文章进行改编、汇编、翻译或出版。在使用时应注明每篇文章（包括附件）的“来源”以及作者名字。违反上述声明者，将追究其相关法律责任。