数据合规时事速递
NEWSLETTERS

2022 第一期 /总第三十五期

环球律师事务所
GLOBAL LAW OFFICE

2022 年 02 月 21 日

精彩导读

新规速递/ 工信部就《工业和信息化领域数据安全管理办法》再次公开征求意见

监管动态/ 网信办等部门联合印发《关于加强互联网信息服务算法综合治理的指导意见》

环球评论/《重要数据识别指南》新版草案出台，兼议十二项企业合规义务

环球律师事务所
GLOBAL LAW OFFICE

前　言

随着《网络安全法》、《数据安全法》、《个人信息保护法》及相关配套法律法规等文件的出台，中国正日益加强对个人信息安全的保护和对网络安全监管。我国对个人信息保护和网络数据安全越来越重视，监管趋势也越来越严。

环球律师事务所数据合规团队收集了国内外最新出台的重要法律法规、市场监管动向以及相关处罚案例，旨在为本期刊的读者提供最实时的法律动态，帮助读者第一时间了解网络治理、信息安全相关信息。

环球律师事务所数据合规团队专注于网络安全与数据合规、个人信息隐私保护等领域。我们在企业数据合规体系建设等方面具备丰富的经验，为多家大型互联网公司、全球企业提供法律服务。

我们为客户提供在网络安全与数据合规、个人信息隐私保护、跨境数据传输、电子商务与广告法领域的法律咨询及相关方案设计，帮助客户迎接数据时代的机遇与挑战。

孟洁 | 合伙人律师
直线：86-10-6584-6768
总机：86-10-6584-6688
邮箱：mengjie@glo.com.cn

孟洁律师为环球律师事务所常驻北京的合伙人，主要执业领域为网络安全、个人信息保护、互联网、电商合规、反腐败反商业贿赂合规。孟律师曾在诺基亚等世界五百强跨国公司和知名律师事务所工作超过十余年，担任知名人工智能独角兽公司总法律顾问、DPO。孟洁律师曾经及目前服务于大型跨国公司及知名互联网企业、车企、IoT、电信、云服务、AI、金融、医疗领域企业进行境内/境外的数据合规体系建设与数据合规专项，总结出不少可落地的实操方法论，颇受客户好评。

她荣登钱伯斯大中华区 2022 年法律指南“数据隐私保护”榜单、“科技、媒体、电信”榜单；被 Legal 500 评为 2020 年“TMT 领域特别推荐律师”；2021 年“TMT 领域领军人物”、“数据保护领域领军人物”、“Fintech 领域头部律师”，被 LEGALBAND 评为“2021 年中国律师特别推荐榜：消费与零售”、“2021 年中国律师特别推荐榜：汽车与新能源”、“网络安全与数据合规特别推荐 15 强”、“2020 年度 LEGALBAND 中国律师特别推荐榜 15 强：网络安全与数据合规”，被北京市律协评为全国千名涉外专家律师。在各大期刊、公号发表过数百篇专业文章、著作，例如有《SDK 安全与合规白皮书》，《个性化展示安全与合规报告》、《Cookie 合规指引报告（2021）》、《国内外标准兼容下的个人信息合规体系构建》等。

许国盛 | 资深顾问
直线：86-010-6584-9306
手机：86-185-1085-6288
邮箱：xuguosheng@glo.com.cn

许国盛律师在金融服务与电信领域与合规官以及企业高管有丰富的合作经验。作为迪堡与诺基亚中国的前区域合规总监，许律师在数据保护规制以及中国监管事项方面有着多年经验。除此之外，他也经常协助跨国企业进行敏感的内部调查、监管检查、数据完整性问题检查以及应对政府执法。许律师曾负责管理整合来自不同国家的合规项目，并熟悉美国、欧盟以及亚洲国家的复杂法律法规。

许律师对如何运行合规项目有着极其深入的了解。在环球，许律师曾为客户的海外扩张提供数据合规方面的建议，包括国际数据隐私政策的本地化，员工或客户数据出境和共享，以及数据泄露的管理与向监管机构的自我报告等。许律师亦是《全球化与隐私保护指南（2020）》以及《GB/T 35273 与 ISO/IEC 27701 比较报告（2020）》的合著者。

本团队专门致力于为客户提供全面且专业的法律服务，包括以下业务领域：

- 网络安全与数据合规
- 互联网与电商合规
- 个人信息保护
- 反腐败/反商业贿赂合规

目录

环球律师事务所
GLOBAL LAW OFFICE

新规速递

1. 工信部就《关于进一步规范移动智能终端应用软件预置行为的通告》公开征求意见

2022 年 2 月 17 日，工业和信息化部发布了《关于进一步规范移动智能终端应用软件预置行为的通告（征求意见稿）》（以下简称《征求意见稿》），并向社会征求意见，意见反馈截止日期为 2022 年 2 月 28 日。

《征求意见稿》指出，移动智能终端预置应用软件应遵循依法合规、用户至上、安全便捷、最小必要的原则，按“谁预置、谁负责”的要求落实企业主体责任，依法维护用户知情权、选择权，保障用户合法权益。

同时，《征求意见稿》强调，生产企业应确保除基本功能软件外的预置应用软件均可卸载，并提供安全便捷的卸载方式供用户选择。基本功能软件限于“操作系统基本组件：系统设置、文件管理”等四类范围。实现同一基本功能的预置应用软件，至多有一个可设置为不可卸载。

《关于进一步规范移动智能终端应用软件预置行为的通告（征求意见稿）》全文请参见：

https://www.miit.gov.cn/cms_files/filemanager/1226211233/attach/202112/707e36b243fd4c3f905184413c453f70.doc

2. 八部门发布《关于加强网络预约出租汽车行业事前事中事后全链条联合监管有关工作的通知》，加强网络预约出租汽车监管

2022 年 2 月 15 日，为深入贯彻落实党中央、国务院关于推动平台经济规范健康持续发展的决策部署和《国务院办公厅关于深化改革推进出租汽车行业健康发展的指导意见》（国办发〔2016〕58 号），加强网络预约出租汽车（以下简称“网约车”）行业事前事中事后全链条联合监管，维护市场公平竞争秩序，保障乘客和驾驶员合法权益，

促进网约车行业规范健康持续发展，更好满足人民群众出行需求，交通运输部办公厅、工业和信息化部办公厅、公安部办公厅、人力资源社会保障部办公厅、中国人民银行办公厅、国家税务总局办公厅、国家市场监督管理总局办公厅、国家网信办秘书局等六部门发布了修订后《关于加强网络预约出租汽车行业事前事中事后全链条联合监管有关工作的通知》（以下简称《通知》）。

《通知》的主要修订包括，一是增加了事前联合监管要求。二是完善了全链条联合监管事项。三是细化了全链条联合监管流程。根据《通知》，网约车平台公司存在以下违法违规行为的，可开展事前事中事后全链条联合监管，主要包括“未取得网约车经营许可，擅自从事或者变相从事网约车经营活动”等八类行为。

同时，《通知》将事中事后监管流程细分为发起、上报、处置等环节。经依法依规处理后仍拒不改正的，地级及以上城市相关部门报经当地人民政府同意后，可组织发起联合监管，逐级上报提请采取责令暂停区域内经营服务、暂停发布或下架 App 等处置措施。

《关于加强网络预约出租汽车行业事前事中事后全链条联合监管有关工作的通知》全文请参见：

https://xxgk.mot.gov.cn/2020/jigou/ysfws/202202/t20220215_3641452.html

3. 工信部就《工业和信息化领域数据安全管理办法》再次公开征求意见

近期，工信部根据此前《工业和信息化领域数据安全管理办法（试行）》（征求意见稿）收到的公开意见，进行了修改完善，并于 2022 年 2 月 10 日再次面向社会征求意见。

其中，《征求意见稿》规定，工业和信息化领域数据处理者应当对数据处理活动负安全主体责任，对各类数据实行分级防护，不同级别数据同时被处理且难以分别采取保护措施的，应当按照其中级别最高的要求实施保护，确保数据持续处于有效保护和合法利用的状态。

同时，《征求意见稿》指出，数据处理者在中华人民共和国境内收集和产生的重要数据和核心数据，法律、行政法规有境内存储要求的，应当在境内存储，确需向境外提供的，应当依法依规进行数据出境安全评估。

《工业和信息化领域数据安全管理办法》全文请参见：

https://www.miit.gov.cn/api-gateway/jpaas-web-server/front/document/file-download?fileUrl=/cms_files/filemanager/1226211233/attach/202112/4ca3dd7c3acd48c0b4ab490dcbc31cbb.pdf&fileName=附件 1-《工业和信息化领域数据安全管理办法（试行）》公开征求意见稿.pdf

4. 网信办就《互联网信息服务深度合成管理规定（征求意见稿）》公开征求意见

为了规范互联网信息服务深度合成活动，弘扬社会主义核心价值观，维护国家安全和社会公共利益，保护公民、法人和其他组织的合法权益，网信办起草了《互联网信息服务深度合成管理规定（征求意见稿）》，并向社会公开征求意见。意见反馈截止日期为 2022 年 2 月 28 日。

《征求意见稿》共二十五条，主要规定了以下五个方面的内容：

（一）明确了制定目的依据、适用范围和总体要求。明确在中华人民共和国境内应用深度合成技术提供互联网信息服务，以及为深度合成服务提供技术支持的活动，适用本规定明确深度合成技术、深度合成服务提供者和深度合成服务使用者等概念的含义。明确国家网信部门、地方网信部门的统筹协调和监督管理职责以及深度合成服务提供者、使用者的基本要求。鼓励相关行业组织加强行业自律。强调不得利用深度合成服务从事法律法规禁止的活动，不得制作、复制、发布、传播含有法律法规禁止内容的信息。（第一条至第六条）

（二）明确了深度合成服务提供者主体责任。要求建立健全算法机制机理审核、信息内容管理、从业人员教育培训等管理制度，具有

与新技术新应用发展相适应的安全可控的技术保障措施。应当制定并公开管理规则和平台公约，并对使用者依法进行真实身份信息认证。加强内容管理，采取技术或者人工方式对输入数据和合成结果进行审核，并建立健全相关特征库。加强技术管理，定期审核、评估、验证算法机制机理。提供涉及生物识别信息或者可能涉及国家安全、社会公共利益的模型、模板等工具的，应当自行开展安全评估，预防信息安全风险。加强训练数据管理，确保数据处理正当、合法，采取必要措施保障数据和个人信息安全。（第七条至第十二条）

（三）明确了深度合成信息内容标识管理制度。要求深度合成服务提供者对使用其服务所制作的深度合成信息内容，通过有效技术措施添加不影响用户使用的标识，依法保存日志信息，使深度合成信息内容可被自身识别、追溯。对生成或者显著改变信息内容的深度合成信息内容，应当使用显著方式进行标识，向社会公众有效提示信息内容的合成情况；对其他深度合成信息内容，应当提供进行显著标识的功能，并提示使用者可以自行标识。发现应该进行显著标识而未显著标识的，应当立即停止传输该信息，按规定作出显著标识后，方可继续传输。（第十三条至第十五条）

（四）明确了监督管理相关要求。互联网应用商店服务提供者应当对深度合成应用程序履行安全管理责任，依法依约核验安全评估、备案等情况，对违反国家有关规定的，及时采取不予上架、暂停上架或者下架等处置措施。深度合成服务提供者应当建立健全辟谣机制，设置便捷有效的用户申诉和公众投诉、举报入口；应当按照有关规定履行备案手续、标明备案编号；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；对网信部门依法实施的监督检查，应当予以配合，并提供必要的技术、数据等支持和协助。（第十六条至第二十一条）

（五）明确了法律责任、解释部门和施行日期。违反《规定》相关规定的，由国家和省、自治区、直辖市网信部门依据职责，按照《规定》和有关法律法规规章的规定予以处理。《规定》由国家互联网信息办公室负责解释。（第二十二条至第二十五条）[1]

[1] 网信办官网。

《互联网信息服务深度合成管理规定（征求意见稿）》全文请参见：

http://www.cac.gov.cn/2022-01/28/c_1644970458520968.htm

5. 网信办就《移动互联网应用程序信息服务管理规定（征求意见稿）》公开征求意见

为了进一步规范移动互联网应用程序信息服务管理，促进行业健康有序发展，保障公民、法人和其他组织的合法权益，营造清朗网络空间，根据《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》《互联网信息服务管理办法》《网络信息内容生态治理规定》等法律规定，国家互联网信息办公室对 2016 年 8 月 1 日正式施行的《移动互联网应用程序信息服务管理规定》（以下简称《2016 版管理规定》）进行了修订，并于 2022 年 1 月 5 日向社会公开征求意见。[2]

相较于现行有效的《2016 版管理规定》，此次《征求意见稿》着眼于近年来出现的日渐多样化的互联网应用程序形态，并衔接新制定的《网络安全法》《数据安全法》《个人信息保护法》等法律。旨在通过加强对“应用程序提供者”和“应用程序分发平台”的管理，进一步明确“应用程序提供者”和“应用程序分发平台”义务和责任，以期达到规范移动互联网应用程序信息服务的目的。

除进一步压实“应用程序提供者”的相关内容管理主体责任外，此次《征求意见稿》进一步明确了“应用程序分发平台”的范围、义务和责任。为此前《2016 版管理规定》《移动智能终端应用软件预置和分发管理暂行规定》《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）是否能涵盖小程序、快应用等新形态监管提供了有效的监管依据。意见反馈截止时间为 2022 年 1 月 20 日。[3]

[2] 网信办官网。
[3] 网络与数据法律实务：合规责任升级——移动互联网应用程序信息服务管理规定（征求意见稿）解读。

《移动互联网应用程序信息服务管理规定（征求意见稿）》全文请参见：

http://www.cac.gov.cn/2022-01/05/c_1642983962594050.htm

6. 网信办等十三部门修订发布《网络安全审查办法》

近日，国家互联网信息办公室、国家发展和改革委员会、工业和信息化部、公安部、国家安全部、财政部、商务部、中国人民银行、国家市场监督管理总局、国家广播电视总局、中国证券监督管理委员会、国家保密局、国家密码管理局等十三部门联合修订发布《网络安全审查办法》（以下简称《办法》），自 2022 年 2 月 15 日起施行。

国家互联网信息办公室有关负责人表示，网络安全审查是网络安全领域的重要法律制度，原《办法》自 2020 年 6 月 1 日施行以来，对于保障关键信息基础设施供应链安全，维护国家安全发挥了重要作用。为落实《数据安全法》等法律法规要求，国家互联网信息办公室联合相关部门修订了《办法》。

《办法》将网络平台运营者开展数据处理活动影响或者可能影响国家安全等情形纳入网络安全审查，并明确掌握超过 100 万用户个人信息的网络平台运营者赴国外上市必须向网络安全审查办公室申报网络安全审查。根据审查实际需要，增加证监会作为网络安全审查工作机制成员单位，同时完善了国家安全风险评估因素等内容。[4]

《网络安全审查办法》全文请参见：

http://www.cac.gov.cn/2022-01/04/c_1642894602182845.htm

7. 网信办等四部门发布《互联网信息服务算法推荐管理规定》

近日，国家互联网信息办公室、工业和信息化部、公安部、国家市场监督管理总局联合发布《互联网信息服务算法推荐管理规定》（以

[4] 网信办官网。

下简称《规定》)。该《规定》自 2022 年 3 月 1 日起施行。国家互联网信息办公室有关负责人表示，出台《规定》旨在规范互联网信息服务算法推荐活动，维护国家安全和社会公共利益，保护公民、法人和其他组织的合法权益，促进互联网信息服务健康发展。

近年来，算法应用在给政治、经济、社会发展注入新动能的同时，算法歧视、“大数据杀熟”、诱导沉迷等算法不合理应用导致的问题也深刻影响着正常的传播秩序、市场秩序和社会秩序，给维护意识形态安全、社会公平公正和网民合法权益带来挑战。在互联网信息服务领域出台具有针对性的算法推荐规章制度，是防范化解安全风险的需要，也是促进算法推荐服务健康发展、提升监管能力水平的需要。

《规定》明确，应用算法推荐技术，是指利用生成合成类、个性化推送类、排序精选类、检索过滤类、调度决策类等算法技术向用户提供信息。国家网信部门负责统筹协调全国算法推荐服务治理和相关监督管理工作。国务院电信、公安、市场监管等有关部门依据各自职责负责算法推荐服务监督管理工作。地方网信部门负责统筹协调本行政区域内的算法推荐服务治理和相关监督管理工作。地方有关部门依据各自职责负责本行政区域内的算法推荐服务监督管理工作。

《规定》明确了算法推荐服务提供者的信息服务规范，要求算法推荐服务提供者应当坚持主流价值导向，积极传播正能量，不得利用算法推荐服务从事违法活动或者传播违法信息，应当采取措施防范和抵制传播不良信息；建立健全用户注册、信息发布审核、数据安全和个人信息保护、安全事件应急处置等管理制度和技术措施，定期审核、评估、验证算法机制机理、模型、数据和应用结果等；建立健全用于识别违法和不良信息的特征库，发现违法和不良信息的，应当采取相应的处置措施；加强用户模型和用户标签管理，完善记入用户模型的兴趣点规则和用户标签管理规则；加强算法推荐服务版面页面生态管理，建立完善人工干预和用户自主选择机制，在重点环节积极呈现符合主流价值导向的信息；规范开展互联网新闻信息服务，不得生成合成虚假新闻信息或者传播非国家规定范围内的单位发布的新闻信息；不得利用算法实施影响网络舆论、规避监督管理以及垄断和不正当竞争行为。

《规定》明确了算法推荐服务提供者的用户权益保护要求，包括保障算法知情权，要求告知用户其提供算法推荐服务的情况，并公示

服务的基本原理、目的意图和主要运行机制等；保障算法选择权，应当向用户提供不针对其个人特征的选项，或者便捷的关闭算法推荐服务的选项。此外，对向未成年人、老年人、劳动者和消费者等主体提供算法推荐服务的，《规定》明确了具体要求，如不得利用算法推荐服务诱导未成年人沉迷网络，应当便利老年人安全使用算法推荐服务，应当建立完善平台订单分配、报酬构成及支付、工作时间、奖惩等相关算法，以及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。

《规定》要求，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在提供服务之日起十个工作日内通过互联网信息服务算法备案系统填报备案信息，履行备案手续；备案信息发生变更的，应当在规定时间内办理变更手续。算法推荐服务提供者应当依法留存网络日志，配合有关部门开展安全评估和监督检查工作，并提供必要的技术、数据等支持和协助。

国家互联网信息办公室有关负责人指出，算法推荐服务治理需要政府、企业、社会、网民等多方主体共同参与，推动算法推荐服务公正公平、规范透明，促进算法推荐服务向上向善，营造更加清朗的网络空间。[5]

《互联网信息服务算法推荐管理规定》全文请参见：

http://www.cac.gov.cn/2022-01/04/c_1642894606364259.htm

8. 信安标委就《信息安全技术 移动互联网应用程序（App）生命周期安全管理指南》等 4 项国家标准公开征求意见

经信安标委等编制单位的辛勤努力，现已形成以下 4 项国家标准，面向社会广泛征求意见：

[5] 网信办官网。

1）《信息安全技术 移动互联网应用程序（App）生命周期安全管理指南》征求意见稿

全文请参见：

https://www.tc260.org.cn/front/bzzqyjDetail.html?id=20220208192020&norm_id=20201104200032&recode_id=45795

2）《信息安全技术 网络安全服务成本度量指南》征求意见稿

全文请参见：

https://www.tc260.org.cn/front/bzzqyjDetail.html?id=20220117191706&norm_id=20211108000007&recode_id=45645

3）《信息安全技术 网络安全从业人员能力基本要求》征求意见稿

全文请参见：

https://www.tc260.org.cn/front/bzzqyjDetail.html?id=20220117192016&norm_id=20211108000003&recode_id=45649

4）《信息安全技术 重要数据识别指南》征求意见稿

全文请参见：

https://www.tc260.org.cn/front/bzzqyjDetail.html?id=20220113195354&norm_id=20201104200036&recode_id=45625

上述第一项意见征求截止日期为 2022 年 4 月 9 日，第二至三项意见征求截止日期为 2022 年 3 月 18 日，第四项意见征求截止日期为 2022 年 3 月 13 日。[6]

[6] 信安标委官网。

9. 信安标委发布《网络安全标准实践指南——数据分类分级指引》

为贯彻落实《数据安全法》提出的“国家建立数据分类分级保护制度”要求，指导数据处理者开展数据分类分级工作，信安标委秘书处组织编制了《网络安全标准实践指南——网络数据分类分级指引》。

该指南文件依据法律法规和政策标准相关要求，给出了网络数据分类分级的原则、框架和方法。该指南从国家数据安全管理视角对数据分类分级进行研究，给出数据分类分级的原则、框架和规则，可为主管监管部门、数据处理者开展数据分类分级保护工作提供参考。[7]

《网络安全标准实践指南——数据分类分级指引》全文请参见：

https://www.tc260.org.cn/front/postDetail.html?id=20211231160823

10. 欧洲议会表决通过《数字服务法》

当地时间 2022 年 1 月 20 日，欧洲议会以 530 票赞成、78 票反对、80 票弃权的表决结果通过了《数字服务法》。这一法案旨在进一步加强对大型互联网平台的监管，确保平台对其算法负责，并改进内容审核。

投票结束后，领导议会谈判小组的 Christel Schaldemose（S&D，DK）说：“今天的投票表明，欧洲议会议员和欧盟公民希望制定一项面向未来的、加强对数字经济监管的法规。自通过电子商务条令后的 20 年里，情况发生了很多变化。在线平台在我们的日常生活中变得越来越重要，它带来了新的机会，但随之而来也有新的风险。我们有责任确保在线下认定非法的行为，在线上同样认定为非法。我们需要确保我们制定的数字规则对消费者和公民有利。现在我们可以与理事会进行谈判，我相信我们将能够在这些问题上取得进展。”

《数字服务法》明确了数字服务提供者（特别是社交平台和电商平台等在线平台）的责任和问责制。同时，其建立了“通知-行动”机制

[7] 信安标委官网。

和保障措施，以清除网上的非法产品和服务。数字服务提供者在收到此类通知后，应“考虑非法内容的类型和行动的紧迫性，在没有不当延迟的情况下”采取行动。欧洲议会还制订了更有力的保障措施，以确保以非任意和非歧视的方式处理通知，并尊重包括言论自由在内的基本权利。

此外，议会对委员会的提案还进行了如下修改：

（1）豁免小微企业的某些义务。

（2）针对性广告投放：对用户来说，拒绝同意不应当比做出同意更加困难。若同意遭到拒绝或撤回，用户应有权选择其他方式访问平台，包括“基于无跟踪广告的选择”。

（3）禁止为投放广告而使用涉及未成年人数据的定向或放大技术，也禁止根据特定类别的数据对弱势群体进行定向；

（4）赔偿：数据服务的用户与组织应当享有因平台不遵守其调查义务而造成的一切损害请求赔偿的权利。

（5）应当禁止网络平台使用欺骗或诱导技术，通过“算法黑箱”影响用户选择。

（6）基于算法排名上允许更多选择：超大型平台应当至少提供一个不基于数据分析的推荐系统。[8]

欧洲《数字服务法》全文请参见：

https://www.europarl.europa.eu/doceo/document/A-9-2021-0356_EN.html?redirect

[8] 安全内参。

11. 澳大利亚发布《隐私法修订草案（征求意见稿）》

2021 年 10 月 25 日，澳大利亚司法部就《隐私法修订草案》（以下简称“草案”）公开征求意见，拟在现有《隐私法》基础上引入新的在线隐私守则、扩大域外适用范围、强化违规处罚，进一步加强个人信息保护。2021 年 12 月 6 日征求意见结束，2022 年 1 月司法部根据各方意见完成草案修订并提交议会进行了审议。

其中，在监管对象方面，现有《隐私法》的监管对象为在澳大利亚注册或成立的法人团体、合作企业、信托机构以及集中管理的非法人协会，新在线隐私守则拟将监管对象进一步扩大到提供社交媒体服务或数据中介服务的大型在线平台或组织，同时拟要求监管对象履行以下新增义务：

一是按照相关规定停止使用或披露个人信息；

二是严格规范儿童或其他弱势群体的个人信息处理活动；

三是其他非强制性义务，如向隐私专员报送投诉信息等。

此外，在域外适用范围方面，该草案拟将监管范围扩大到不直接在澳大利亚收集或存储公民个人信息的国外组织，以进一步加强对国外组织的数据安全监管。

在违规处罚方面，该草案拟制定更为严格的违规处罚，针对法人组织的罚款金额将从 220 万澳元增加到不超过以下金额中的最大者：一是 10,000 万澳元；二是违法所得收益的 3 倍；三是自违法行为开始 12 个月内所得营业额的 10%。[9]

澳大利亚《隐私法修订法草案（征求意见稿）》全文请参见：

[9] 安全内参。

https://consultations.ag.gov.au/rights-and-protections/online-privacy-bill-exposure-draft/

12. 美澳签署 CLOUD 法案双边协议，将跨境获取数据

2021 年 12 月 15 日，澳大利亚和美国签署了一项具有里程碑意义的 CLOUD 法案协议，该协议旨在在防止严重犯罪、恐怖主义、勒索软件攻击、关键基础设施破坏和儿童性虐待方面作出努力。该协议是第二个在《澄清境外合法使用数据法案》（CLOUD Act）框架下达成的双边协议。

从主权国家的角度来说，出于执法目的跨境访问数据由两个场景构成：一是执法所需的数据存储在国外；二是外国执法机构需要访问存储在本国的数据。《澄清境外合法使用数据法案》（CLOUD Act）主要针对这两个场景提出了解决方案。[10]

据报道，此前向美国寻求电子证据法律互助请求的数量急剧增加，这使得资源紧张且美国当局的响应时间也被延长。外国当局也表示需要提高获得相关证据的速度。同时，美国收到的许多援助请求是寻求位于其他国家的个人或实体电子信息，但证据恰好由位于美国的全球供应商持有。CLOUD 法案确保外国伙伴与美国通过签订双边协议来获得对相关电子证据的直接访问，无论其位于何处。

《澄清境外合法使用数据法案》（CLOUD Act）全文请参见：https://www.justice.gov/dag/cloudact#:~:text=The%20United%20States%20enacted%20the%20Clarifying%20Lawful%20Overseas,crime%20to%20sexual%20exploitation%20of%20children%20and%20cybercrime

[10] 安全内参。

环球律师事务所
GLOBAL LAW OFFICE

监管动态

1. 网信办发布开展“清朗·2022 年春节网络环境整治”专项行动的通知

为营造文明健康、喜庆祥和的春节网上舆论氛围，中央网信办决定自 2022 年 1 月 24 日至 2 月 24 日开展“清朗·2022 年春节网络环境整治”专项行动。具体行动安排如下：

一、工作目标

聚焦春节期间网民使用频率较高的平台环节和服务类型，聚焦解决影响上网观感、群众反映强烈的网络生态问题，坚决清理一批违法违规信息，处置一批账号和平台，整治网络不良行为乱象，遏制不良文化传播势头，大力净化网络生态，为广大网民尤其是未成年人营造健康、喜庆、祥和的春节网络环境。

二、工作任务

此次专项行动开展时间为 2022 年 1 月 24 日至 2 月 24 日，重点包括以下五方面整治任务：

1. 集中整治网络暴力、散播谣言等问题，切实维护网民利益。一是重点整治借疫情、社会热点事件等挑动网民对立，进行人肉搜索、辱骂攻击等网络暴力行为。二是集中处置公众账号为吸引流量恶意蹭炒春节话题，编造传播谣言、拼接翻炒旧闻、误导公众认知、误导老年人群体等问题。三是严肃查处春节期间以“抢红包”“免费送”等方式，诱导网民点击实施网络诈骗等问题。四是集中查处低俗弹窗广告，清理评论环节不良链接，深入核查问题线索，从严处置一批从事色情、赌博交易的网站平台。

2. 持续开展整治，严防“饭圈”乱象反弹反复。一是及时清理借春节相关话题炒作娱乐明星低俗绯闻丑闻等信息，严防违法失德明星艺人利用晚会、直播等转移阵地复出。二是加强春节期间娱乐明星网上信息呈现规范管理，严格对标相关信息呈现标准，防止过度占用公共平台资源。三是重点关注明星、经纪公司（工作室）、粉丝团（后援

会）、娱乐类账号，加强正向沟通引导，集中查处挑唆粉丝群体互撕谩骂、诱导应援打榜等信息。

3. 加大炫富拜金、封建迷信等问题治理力度，遏制不良网络文化传播扩散。一是严格管控炫富拜金、卖惨审丑等问题，集中清理宣扬拜金主义、攀比享乐信息，打击编造悲惨经历、渲染悲观情绪、故作丑态表演等行为。二是严肃处置猎奇恶搞问题，排查清理涉及暴饮暴食、猎奇伦理剧情信息，关停含有不良 PK 内容的直播间。三是从严查处宣扬封建迷信等问题，排查清理打着高科技名义宣扬迷信思想的不良信息，严厉打击以自动算命、网络占卜等方式，违规获取个人信息或实施诈骗等行为。

4. 从严整治“网红儿童”“软色情”等问题，保障未成年人合法权益。一是严控春节期间借“网红儿童”牟利行为，不得利用未成年人发布低俗不良短视频信息，禁止未成年人出镜直播，防止未成年人以声音、肢体等方式变相出镜。二是聚焦春节期间未成年人使用频率较高的服务应用，大力整治涉未成年人“软色情”、自杀约死、祖安黑界等突出问题。三是进一步完善青少年模式，严格时间限制和功能限制，不得诱导未成年人“氪金”打赏，防止未成年人沉迷网络。

5. 加强重点页面版面生态问题治理，营造良好春节氛围。聚焦网站平台首页首屏、热搜榜单、热门话题、PUSH 弹窗和重要新闻信息内容页面等重点位置版块，积极呈现正能量信息，及时清理淫秽色情、低俗庸俗、血腥暴力、恐怖惊悚等违法和不良信息，维护良好页面版面生态，营造积极向上的春节网络氛围。

三、工作要求

1. 抓好组织实施。各地网信部门要结合本地实际，细化专项行动实施方案，明确目标任务，找准关键环节，配齐工作力量，深入开展清理整治，确保专项行动取得实效。

2. 压实平台责任。督促重点网站平台成立工作专班，预先梳理风险点，排查问题漏洞，加强春节期间值班值守，强化技术手段，完善工作机制，切实加强内容审核管理，及时清理违法和不良信息。

3. 强化处置曝光。处置一批违法违规网站平台和账号，查办一批典型案例，认真总结专项行动工作成效，组织新闻媒体适时开展宣传曝光，形成震慑效应。[11]

2. 网信办等部门联合印发《关于加强互联网信息服务算法综合治理的指导意见》

近年来，互联网信息服务算法（以下简称“算法”）在加速互联网信息传播、繁荣数字经济、促进社会发展等方面发挥了重要作用。与此同时，算法的不合理应用也影响了正常的传播秩序、市场秩序和社会秩序，给维护意识形态安全、社会公平公正和网民合法权益带来挑战。为深入贯彻落实党中央、国务院决策部署，管理好使用好发展好算法应用，全面提升网络综合治理能力，网信办等部门联合发布了《关于加强互联网信息服务算法综合治理的指导意见》，就加强互联网信息服务算法安全治理提出了意见。

一、总体要求

（一）指导思想

坚持以习近平新时代中国特色社会主义思想特别是习近平总书记关于网络强国的重要思想为指导，深入贯彻党的十九大和十九届二中、三中、四中、五中全会精神，坚持正能量是总要求、管得住是硬道理、用得好是真本事，以算法安全可信、高质量、创新性发展为导向，建立健全算法安全治理机制，构建完善算法安全监管体系，推进算法自主创新，促进算法健康、有序、繁荣发展，为建设网络强国提供有力支撑。

（二）基本原则

坚持正确导向，强化科技伦理意识、安全意识和底线思维，充分发挥算法服务正能量传播作用，营造风清气正的网络空间；坚持依法治理，加强法律法规建设，创新技术监管模式，打击违法违规行为，

[11] 网信办官网。

建立健全多方参与的算法安全治理机制；坚持风险防控，推进算法分级分类安全管理，有效识别高风险类算法，实施精准治理；坚持权益保障，引导算法应用公平公正、透明可释，充分保障网民合法权益；坚持技术创新，大力推进我国算法创新研究工作，保护算法知识产权，强化自研算法的部署和推广，提升我国算法的核心竞争力。

（三）主要目标

利用三年左右时间，逐步建立治理机制健全、监管体系完善、算法生态规范的算法安全综合治理格局。

——治理机制健全。制定完善互联网信息服务算法安全治理政策法规，算法安全治理的主体权责明确，治理结构高效运行，形成有法可依、多元协同、多方参与的治理机制。

——监管体系完善。创新性地构建形成算法安全风险监测、算法安全评估、科技伦理审查、算法备案管理和涉算法违法违规行为处置等多维一体的监管体系。

——算法生态规范。算法导向正确、正能量充沛，算法应用公平公正、公开透明，算法发展安全可控、自主创新，有效防范算法滥用带来的风险隐患。

二、健全算法安全治理机制

加强算法治理规范。健全算法安全治理政策法规，加快制定算法管理规定，明确算法管理主体、管理范围、管理要求和法律责任等，完善算法安全治理措施，制定标准、指南等配套文件。

优化算法治理结构。进一步明确政府、企业、行业组织和网民在算法安全治理中的权利、义务和责任，科学合理布局治理组织结构，规范运作、相互衔接，打造形成政府监管、企业履责、行业自律、社会监督的算法安全多元共治局面。

强化统筹协同治理。网信部门会同宣传、教育、科技、工信、公安、文化和旅游、市场监管、广电等部门，建立部门协同联动长效机制，履行监管职责，共同开展算法安全治理工作。

强化企业主体责任。企业应建立算法安全责任制度和科技伦理审查制度，健全算法安全管理组织机构，加强风险防控和隐患排查治理，提升应对算法安全突发事件的能力和水平。企业应强化责任意识，对算法应用产生的结果负主体责任。

强化行业组织自律。互联网信息服务行业应当加强行业自律，积极开展算法科学技术普及工作，逐步组建算法安全治理力量，吸引专业人才队伍，汇聚多方资源投入，承担算法安全治理社会责任，为算法安全治理提供有力支撑。

倡导网民监督参与。鼓励广大网民积极参与算法安全治理工作，切实加强政府、企业、行业组织和网民间的信息交流和有效沟通。政府积极受理网民举报投诉，企业自觉接受社会监督并及时做好结果反馈。

三、构建算法安全监管体系

有效监测算法安全风险。对算法的数据使用、应用场景、影响效果等开展日常监测工作，感知算法应用带来的网络传播趋势、市场规则变化、网民行为等信息，预警算法应用可能产生的不规范、不公平、不公正等隐患，发现算法应用安全问题。

积极开展算法安全评估。组织建立专业技术评估队伍，深入分析算法机制机理，评估算法设计、部署和使用等应用环节的缺陷和漏洞，研判算法应用产生的意识形态、社会公平、道德伦理等安全风险，提出针对性应对措施。

有序推进算法备案工作。建立算法备案制度，梳理算法备案基本情况，健全算法分级分类体系，明确算法备案范围，有序开展备案工作。积极做好备案指导帮助，主动公布备案情况，接受社会监督。

持续推进监管模式创新。持续研判算法领域技术发展新形势，推进监管模式与算法技术协同发展，不断完善、升级、创新监管的方式方法和治理举措，防范监管模式落后导致的算法安全风险。

严厉打击违法违规行为。着力解决网民反映强烈的算法安全问题，对算法监测、评估、备案等工作中发现的、以及网民举报并查实的涉算法违法违规行为，予以严厉打击，坚决维护互联网信息服务算法安全。

四、促进算法生态规范发展

树立算法正确导向。弘扬社会主义核心价值观，在算法应用中坚持正确政治方向、舆论导向、价值取向。提高正能量传播的精准性和有效性，规范信息分发行为和秩序，推动企业借助算法加强正能量传播，引导算法应用向上向善。

推动算法公开透明。规范企业算法应用行为，保护网民合理权益，秉持公平、公正原则，促进算法公开透明。督促企业及时、合理、有效地公开算法基本原理、优化目标、决策标准等信息，做好算法结果解释，畅通投诉通道，消除社会疑虑，推动算法健康发展。

鼓励算法创新发展。提升算法创新能力，积极开展算法研发工作，支持算法与社会、经济各领域深度结合。提高算法自主可控能力，加强知识产权保护，提高自研算法产品的推广和使用，增强算法核心竞争力。

防范算法滥用风险。维护网络空间传播秩序、市场秩序和社会秩序，防止利用算法干扰社会舆论、打压竞争对手、侵害网民权益等行为，防范算法滥用带来意识形态、经济发展和社会管理等方面的风险隐患。[12]

[12] 网信办官网。

3. 欧洲数据保护委员会宣布启动首次联合执法行动

2022 年 2 月 15 日，欧洲数据保护委员会（European Data Protection Board）宣布启动首次联合执法行动，在接下来的几个月时间里，协调欧洲经济区的 22 个国家的监管部门对公共机构使用云服务的情况展开调查。在此之前，欧洲数据保护委员会已建立了协调执法框架（Coordinated Enforcement Framework）和专家支持库（Support Pool of Experts）。这两项措施旨在简化监管机构之间合作执法的流程。

欧洲经济区（包括欧盟）共有超过 75 个公共机构，涵盖卫生、金融、税收、教育、采购、IT 服务等多个行业部门。协调执法框架将通过实况调查，确定是否需要对之进行正式调查，以及采取后续行动、使用一种或几种方式展开国家层面的调查。特别是，监管部门将探讨公共机构在使用云服务时，面临的来自 GDPR 的挑战，包括获取云服务时实施的流程和保障措施、跨境传输合规等。

根据欧盟统计局的数据，在过去 6 年里，整个欧盟企业的云计算使用量翻了一番。新冠肺炎大流行推动了社会组织的数字化转型，许多公共机构也开始使用云服务，这导致欧盟和欧洲国家的公共机构在获得符合欧盟数据保护规则的信息和通信技术产品和服务时将面临风险。通过各方协调一致的合作与行动，监管部门旨在推行最佳实践，从而确保个人信息得到充分保障。[13]

4. 英国信息专员办公室寻求与 Meta 公司就儿童隐私问题进行会谈

据悉，在研究发现 VRChat 存在多起滥用事件后，英国信息专员办公室表示正计划与 Meta 公司就可能违反儿童准则的行为展开“进一步的讨论”。违反该守则可能会被处以 1750 万英镑的罚款或公司全球营业额 4%的罚款。Meta 公司的某位发言人表示，该公司“确信”其产品符合儿童准则所规定的要求。

英国信息专员办公室希望确定 Meta 的头显和 VR 服务是否足以保护儿童的隐私和数据，担心孩子们能很容易登录 Meta 的平台，并

[13] 安全内参。

存在看到虐待、骚扰和露骨内容的风险。据悉，Meta 的平台需要 Facebook 帐户（用户至少 13 岁）才能使用，但这并不意味着合理的年龄审查，孩子们只需在“我已年满 13 岁”选项上打勾就可以进入。

Meta 发言人称，该公司致力于构建尊重儿童的平台，并“相信”其 VR 硬件符合要求。该发言人强调，服务条款不允许 13 岁以下的儿童使用该产品，但依然存在儿童无视该政策的担忧。该公司现已承诺一项 5000 万美元的计划，以确保其元宇宙开发遵守法律法规。[14]

[14] iapp 官网。

环球律师事务所
GLOBAL LAW OFFICE

相关新闻

1. 工信部通报 107 款侵害用户权益 App（2022 年第 1 批，总第 21 批）

依据《网络安全法》《电信条例》《电信和互联网用户个人信息保护规定》等法律法规，工信部近期组织第三方检测机构对手机应用软件进行检查。截至目前，尚有 107 款 App 未完成整改。同时，检测过程中发现，13 款内嵌第三方软件开发工具包（SDK）存在违规收集用户设备信息的行为。上述 App（SDK）应在 2 月 25 日前完成整改落实工作。逾期不整改的，工信部将依法依规组织开展相关处置工作。[15]

相关 App 的名单请参见：

https://www.miit.gov.cn/cms_files/filemanager/1226211233/attach/20222/b921aacc85df4a179275e955a637cd78.docx

2. 中国信通院联合相关机构发布《人脸信息处理合规操作指南》

为帮助人脸信息处理者落实法律法规的相关要求，中国信通院云计算与大数据研究所联合相关机构和专家，依托“可信人脸应用守护计划”（下称“护脸计划”），牵头编写了国内首份《人脸信息合规操作指南》（下称“《操作指南》”），成果达 60 余页、超过 3 万字，得到了律师事务所、科技企业、互联网公司、金融机构、学术团体、高等院校等 60 余家单位的广泛支持，并于 2022 年 1 月 27 日正式对外发布。

《操作指南》开创性提出了人脸信息处理的场景分类，全面梳理了人脸信息处理的全生命周期合规要点及实践案例，系统地构建了一套人脸信息处理合规体系，旨在为合规处理人脸信息提供全面细致的指引，推动人脸识别产业健康发展。

[15] 工信部官网。

此外，《操作指南》收录了多家企业的实践经验和示例，针对每一个合规要点将法律规范与实践经验相结合，提供了可落地的人脸信息合规实践方案。[16]

《人脸信息处理合规操作指南》全文请参见：

https://www.bita.org.cn/newsinfo/2385521.html

3. 因违反欧盟隐私规定，谷歌与脸书或被罚超 15 亿元

近日，因未允许法国用户便捷地拒绝 Cookie 跟踪，法国数据监管机构 CNIL（法国国家信息与自由委员会）将对谷歌和 Facebook 分别处以 1.5 亿欧元（约合 10.81 亿人民币）和 6000 万欧元（约合 4.32 亿人民币）的罚款。

2022 年 1 月，CNIL 在其官网上公布了罚款的消息。CNIL 表示，通过对 Facebook 和 Google 网站的在线调查发现，虽然两家网站均提供了允许用户“立即接受”Cookie 的按钮，但对于拒绝接受 Cookie 的选择却不是同样的容易——用户需要多次点击才能拒绝所有 Cookie，而用户只需要点击一次就可以接受 Cookie。

CNIL 认为，用户可能因为拒绝机制过于复杂而选择放弃，这相当于“变相强制”用户接受 cookie，影响了互联网用户的同意自由，因而违法《法国数据保护法》（French Data Protection Act）第 82 条规定。

除罚款外，CNIL 还要求，如果谷歌和 Facebook 在决定发布后的三个月内没有完成整改，两家公司还将被处以每天 10 万欧元的罚款。

Facebook 所属 Meta 公司一名新闻发言人表示，正在评估法国当局的决定，并致力于与相关部门合作。“我们的 Cookie 同意控制功能让用户对自己的数据有了更大的控制权，包括 Facebook 和 Instagram

[16] 信通院官网。

上一个新的设置菜单，人们可以随时重新访问和管理自己的决定，我们将继续开发和改进这些控制功能。”对此，谷歌方面未作出回应。

两家公司均非首次因隐私问题被罚款。两年前，因违反《法国数据保护法》，CNIL 向谷歌开出了 1 亿欧元的罚单。CNIL 表示，谷歌在没有提前告知并取得用户同意的情况下，在网页自动放置 Cookies 并用于个性化广告的推荐。

而就在不久前，去年 10 月，爱尔兰数据保护委员会（Irish Data Protection Commission，DPC）也在一份决定草案中向欧盟提议，因其数据处理缺乏清晰度和透明度，要求对 Facebook 处以 2800 万至 3600 万欧元的罚款，并在三个月内整改完成。[17]

4. 新加坡自然协会因个人数据保护不力被罚

2022 年 1 月，非政府组织新加坡自然协会（Nature Society）因违反新加坡《个人数据保护法》（Personal Data Protection Act，以下简称“PDPA”）被新加坡个人数据保护委员会（Personal Data Protection Commission，以下简称“PDPC”）处以 1.4 万新元（约合人民币 6.6 万元）的罚款。

新加坡是全球较早对个人数据进行立法保护的国家之一，早在 2012 年就通过了《个人数据保护法》。该法对各组织收集、使用和披露个人数据的行为进行了较为系统全面的规范。一方面，PDPA 承认个人有权保护其个人数据。另一方面，各组织则需要为一个合理的人在这种情况下认为适当的目的而收集、使用和披露个人数据。在执法层面，新加坡设立了专门机构——个人数据保护委员会（PDPC），对各组织违反 PDPA 的行为进行追责问责。自 PDPA 生效以来，该委员会已对未尽到保护个人数据义务或侵犯个人数据的多家机构作出处罚。

据悉，新加坡自然协会被 PDPC 提出多项违法指控：

[17] 安全内参。

一是其网站数据库未能采取合理措施对个人数据进行保护；

二是未任命个人数据保护官；

三是缺少遵守 PDPA 的书面政策和操作规程。[18]

[18] 安全内参。

环球律师事务所
GLOBAL LAW OFFICE

环球评论

1. 《重要数据识别指南》新版草案出台，兼议十二项企业合规义务

引言

博观而约取，厚积而薄发。在数字化竞争的大背景下，数据已经成为了国家博弈间的重要战略资源，网络安全防护工作也成为了国家安全壁垒的重点要求。2021 年 9 月 1 日生效的《数据安全法》首先提出了建立国家安全观以及数据安全制度体系，要求国家数据安全工作协调机制统筹协调制定国家重要数据目录，加强对重要数据的保护。随后于 2021 年 11 月 14 日《网络数据安全管理条例》（以下简称《网络数安条例（征求意见稿）》）公开向社会征求意见，不仅明确了重要数据的定义，还提出了一系列重要数据安全监管制度，因此，“什么是重要数据”以及“如何识别重要数据”便成为了影响当前国家数据安全工作进展的重大议题。

有鉴于此，国家信息安全标准化委员会于 2022 年 1 月 13 日公布了最新调整后的《信息安全技术 重要数据识别指南（征求意见稿）》（以下简称《指南》）。《指南》划分了重要数据的定义范围，重要数据是指“以电子方式存在的，一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能危害国家、公共利益的数据”。[19]这既说明了重要数据的存在形式，也明确了以造成不利后果为判断重要数据的唯一标准。并且，《指南》指明识别重要数据的基本原则、明确重要数据的识别因素等，不仅为各行业、地区、部门制定本行业、本地区、本部门的重要数据具体目录提供参考，也为企业识别其自身掌握的重要数据提供实践指引，从而进一步为国家重要数据安全保护工作提供支撑。

[19] 《指南》第 3.1 条、《网络数安条例（征求意见稿）》第 73 条。

一、《指南》修改亮点

相比于 2021 年 9 月 23 日发布的第一版《信息安全技术 重要数据识别指南》（征求意见稿）（以下简称《2021 指南》），《指南》是从整体上对《2021 指南》进行了重大修订，具体变化体现在如下几点：

（一）改变了体系思路

相较于《2021 指南》以及再早之前版本中大篇幅对重要数据采取不穷尽列举的方式，《指南》仅对识别重要数据的基本原则和重要数据的识别因素进行了说明，给企业和各主管机构留有更多权衡和商榷的余地。

《指南》明确指出，从原先对各类别数据具体范围的框定到目前只确定原则性的做法，《指南》所确定的基本原则包括：聚焦安全影响、突出保护重点、衔接既有规定、综合考虑风险、定量定性结合、以及动态识别复评这六大原则[20]。

（二）删除了关键信息基础设施、国家秘密和个人信息的定义

虽然《指南》中仍然有提到关键信息基础设施、国家秘密和个人信息这些术语，但是在术语和定义一节中，《指南》删除了此前版本中针对这些术语的定义，一来是将文件重点放在“重要数据”本身，避免了众多文件对同一概念的反复定义、重点不明等问题。二来，能够比较明确地说明，重要数据不包括国家秘密和个人信息。被删除的定义可以直接参考《中华人民共和国保守国家秘密法》《个人信息保护法》等上位法的相关规定。但是基于海量个人信息所形成的统计类数

[20] 《指南》第 4 条。

据（aggregate data）、衍生数据（derived data）是有可能属于重要数据的。

（三）取消了对重要数据的特征进行说明

此前版本中，对重要数据的“特征”说明是文件的一大亮点。《2021指南》从与经济运行相关、与人口与健康相关、与自然资源与环境相关、与科学技术相关、与安全保护相关、与应用服务相关、与政务活动相关、以及其他这八个领域入手，分别介绍了重要数据在该领域下不同角度、不同类别的特征，同时对于各大关键领域下的典型重要数据进行了重点举例说明。如与自然资源与环境相关，涉及地理信息的地图数据、导航数据、特殊测绘数据、重点目标地理信息、未公开的重点目标地理信息等均有可能属于重要数据，并对每类数据进行了解释和说明。

经本次修改，《指南》删除了特定领域的划分和详细的举例说明，改而将所有领域打通，将所有领域对重点数据的识别维度均放在认定因素上，从本质上介绍重要数据的识别因素。在总原则引领下，重要数据识别判断因素主要包括：（1）反映国家战略储备、应急动员能力；（2）支撑关键基础设施运行或重点领域工业生产、运行的数据，关键系统组件、设备供应链数据；（3）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；（4）关系出口管制物项；（5）可能被其他国家或组织利用发起对我国的军事打击；（6）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；（7）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；（8）反映群体健康生理状况、族群特征、遗传信息等的

基础数据；（9）达到国家有关部门规定的规模或者精度的国家自然资源、环境基础数据；（10）关系科技实力、影响国际竞争力；（11）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；（12）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；（13）未公开的政务数据、工作秘密、情报数据和执法司法数据；（14）国家法律、行政法规、部门规章明确规定需要保护或者控制传播的国家经济运行数据、重要行业业务数据、统计数据等；以及（15）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。[21]具备以上因素之一的，可能被认定为重要数据。

结合上述识别因素，《指南》对如下相关场景包含的重要数据进行举例：战略物资产能、储备量；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；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；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；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；以及描述与国防、国家安全相关的知识产权的数据等等。

同时，《指南》撰写负责人左晓栋院长介绍，在修订《指南》的过程中，标准编制组进一步调研了全球其他国家在网络安全、数据安全

[21] 《指南》第 5 条、《网络数安条例（征求意见稿）》第 73 条。

领域制定类似标准的情况，选择以美国正在使用的《Guideline for Identifying an Information System as a National Security System》（《国家安全系统识别指南》（NIST 800-59））为参照制定本次《指南》。2003 年 8 月，美国国家标准和技术研究院（NIST）与美国国防部联合制定并颁布了 NIST 800-59，提出了判断国家安全系统的方法。NIST 800-59 同样从识别的大方向入手，讨论了识别国家安全系统的基础、识别国家安全系统的方法，并提供了国家安全系统识别列表，通过解答问题的方式协助判断某一系统是否符合国家安全系统的定义。

但值得注意的是，从立项之初乃至 2020 年 5 月，《指南》的重点编制依据均为美国 NIST 发布的《将各类信息与信息系统映射到安全类的指南》（SP 800-60）。SP 800-60 不仅对信息进行了分类，还分别从信息保密性、完整性、可用性角度为信息标明影响级，分别为低、中、高。这与《2021 指南》以及更早期标准的编制思路是一致的—拟以文件形式发布重要数据清单，尽可能做到定性与定量相结合的方式识别重要数据，并重点参考了 SP 800-60 级别为“中”和“高”的信息。此次《指南》的重大修订（甚至改变了编制依据），体现了我国现阶段引导识别重要数据的整体思路的转变，从定性定量描述转化为了对重点原则的把握。这表明，从一定程度上我国逐渐不再框定、限制重要数据的范围，而是改为从数据自身性质出发，给予主管机构更多裁量认定的空间和灵活性，也符合现阶段社会发展的趋势。

总体来说，虽然此次重大修订后的《指南》难以如此前的版本以“手把手”方式来教企业如何核对自身所涉信息是否为重要数据，但是《指南》为企业的自我评估提供了更加灵活的指引思路和识别路径。这种比较开放式的识别方法，为认定重要数据解开了思维约束，但也带来了一定挑战和不确定性风险。下文我们将结合目前的法律动态和

监管趋势，从《指南》的修订点入手，把握重要原则，熟悉识别因素的重要规则，深入分析企业在处理重要数据时应注意的合规义务。

（四）引入了数据分级和数据流动的关联

《指南》提出，在识别重要数据时应遵循的基本原则中，应当突出保护重点。通过对数据分级，可明确安全保护重点，使一般数据充分流动，重要数据在满足安全保护要求的前提下有序流动，释放数据价值。相较于此前版本，《指南》引入了“数据分级”这一制度，与去年九月开始施行的《数据保护法》中国家提出应建立数据分类分级保护制度这一要求前后呼应，顺应政策走向。与此同时，《指南》强调一般数据“充分流动”，相较于《2021 指南》中对于一般数据“自由流动”的态度更加突显出了我国鼓励数据流动、开发数据资产价值的趋势要求。

二、处理重要数据企业的合规提示

（一）梳理数据资产，识别重要数据，形成重要数据目录

我国《数据安全法》《网络安全法》《网络数安条例（征求意见稿）》等法律法规均明确提出了重要数据的概念，企业首先需要做的便是对于企业所持有的数据资产进行梳理，参考《指南》所列举的重要数据的识别因素进行判断，明确企业收集的数据的类型，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、公共利益造成的影响，形成企业的重要数据目录。同时，《数据安全法》第二十一条明确各地区、各部门制定本地区、本部门的重要数据目录。因此，对于在特定领域的企业，则也可以同步参考本领域内行业主管发布的重

要数据识别清单。例如，《汽车数据安全管理若干规定（试行）》明确在汽车领域下的重要数据清单：

- 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；
- 车辆流量、物流等反映经济运行情况的数据；
- 汽车充电网的运行数据；
- 包含人脸信息、车牌信息等的车外视频、图像数据；
- 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。

工业和信息化部通过《工业和信息化领域数据安全管理办法（试行）（征求意见稿）》从危害所造成影响程度为着眼点，对构成重要数据的范围进行了说明。当数据泄露、损毁、丢失所造成的危害和影响程度符合下列条件之一的为重要数据：

- 对政治、国土、军事、经济、文化、社会、科技、网络、生态、资源、核安全等构成威胁，影响海外利益、生物、太空、极地、深海、人工智能等重点领域国家安全相关数据的安全；
- 对工业、电信行业发展、生产、运行和经济利益等造成影响；
- 造成重大数据安全事件或生产安全事故，对公共利益或者个人、组织合法权益造成严重影响，社会负面影响大；

- 引发的级联效应明显，影响范围涉及多个行业、区域或者行业内多个企业，或者影响持续时间长，对行业发展、技术进步和产业生态等造成严重影响；

- 恢复数据或消除负面影响所需付出的代价大；

- 经行业监管部门评估确定的其他重要数据。

在识别完企业内部的重要数据后，根据《网络数安条例（征求意见稿）》第二十二条，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：

- 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；

- 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；

- 国家网信部门和主管、监管部门规定的其他备案内容。

需要注意的是，一旦处理数据的目的、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。

此外，当企业处于运营状态时，其所拥有的数据资产是处于流动状态的，而非仅定格在制作数据资产表的那一刻。因此，企业也需要定期对数据资产梳理表进行复盘与更新，以保持数据状态是最新和完整的，并且符合生产运营情况。

（二）明确数据安全负责人和管理机构，完善内部制度体系

根据《数据安全法》第二十七条，处理重要数据的企业应明确数据安全负责人和管理机构，落实数据安全保护责任。根据《网络数安条例（征求意见稿）》第二十八条，对于年度数据安全管理机构，应在数据安全负责人的领导下，履行以下职责：

- 研究提出数据安全相关重大决策建议；
- 制定实施数据安全保护计划和数据安全事件应急预案；
- 开展数据安全风险监测，及时处置数据安全风险和事件；
- 定期组织开展数据安全宣传教育培训、风险评估、应急演练等活动；
- 受理、处置数据安全投诉、举报；
- 按照要求及时向网信部门和主管、监管部门报告数据安全情况。

对于数据安全负责人，应当具备数据安全专业知识和相关管理工作经历，由数据处理者决策层成员承担，有权直接向网信部门和主管、监管部门反映数据安全情况。

同时，企业应以数据为中心，从制度、规范、流程等角度制定数据安全全生命周期的数据安全制度，包括《数据安全组织架构和安全职责》《重要数据采集规范》《重要数据使用规范》《重要数据安全审计》等。

（三）对于重要数据采取分类分级、加密保护

在第一步识别出重要数据的基础上，对于数据库内的重要数据进行打标，并将其根据企业内部的分类分级制度，从数据处理的全流程角度采取更细致化的保护措施，包括针对数据的访问、分发/复制、传输、存储、文件标签、屏幕显示、销毁、备份等环节均加强保障数据安全。同时，根据《网络数安条例（征求意见稿）》第九条，使用不同类型的加密技术对不同程度的重要数据进行保护。

（四）开展网络安全等级保护，使用可信网络产品和服务

根据《网络数安条例（征求意见稿）》第九条，企业应当按照网络安全等级保护的要求，加强数据处理系统、数据传输网络、数据存储环境等安全防护，处理重要数据的系统原则上应当满足三级以上网络安全等级保护要求。同时，企业在采购网络产品和服务时，应当优先采购可信的网络产品和服务，定期检测并维护信息系统安全。

（五）发生重要数据安全事件时的报告

根据《网络数安条例（征求意见稿）》第十一条，当发生重要数据泄露、毁损、丢失等数据安全事件时，企业应当在发生安全事件的八小时内向设区的市级网信部门和有关主管部门报告事件基本信息，包括涉及的数据数量、类型、可能的影响、已经或拟采取的处置措施等。同时，在事件处置完毕后五个工作日内向设区的市级网信部门和有关主管部门报告包括事件原因、危害后果、责任处理、改进措施等情况的调查评估报告。防患于未然，企业应当提前制定相关的应急预案以及报告流程，以在发生重要数据安全事件时及时尽到报告义务。

（六）共享、交易、委托处理重要数据时审批以及评估要求

当企业共享、交易、委托第三方处理重要数据时，首先，根据《网络数安条例（征求意见稿）》第三十三条规定，应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。其次，根据《网络数安条例（征求意见稿）》第十一条，企业共享、交易、委托处理重要数据时，一方面，应当开展安全评估，评估的角度包括：提供数据以及数据接收方处理数据的目录、方式、范围等是否合法、正当、必要；重要数据被泄露、毁损、篡改、滥用的风险，以及对国家安全、经济发展、公共利益带来的风险；数据接收方的诚信状况、守法情况、承诺承担的责任以及履行责任的能力等是否能够有效保障数据安全；在数据处理过程中的管理和技术措施等是否能够防范数据泄露、毁损等风险；与数据接收方订立的相关合同中关于数据安全的要求能否有效约束数据接收方履行数据安全保护义务等内容。评估认为可能危害国家安全、经济发展和公共利益，企业不应共享、交易、委托第三方处理重要数据。

另一方面，应当与数据接收方约定处理数据的目的、范围、处理方式，数据安全保护措施等，通过合同等形式明确双方的数据安全责任义务，并对数据接收方的数据处理活动进行监督。

同时，留存共享、交易、委托处理重要数据的审批记录、日志记录至少五年。

若企业受第三方委托、接收第三方共享或交易数据时，应当履行约定的义务，不得超出约定的目的、范围、处理方式处理重要数据。

（七）对企业整体处理活动定期开展风险评估并向监管报告

根据《数据安全法》第三十条，企业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，面临的数据安全风险及其应对措施等。在开展评估时，根据《网络数安条例（征求意见稿）》第三十二条，企业可以自行或者委托第三方数据安全服务机构每年开展一次数据安全评估，风险评估报告至少保存三年。同时，企业须在每年 1 月 31 日前将上一年度数据安全评估报告报设区的市级网信部门，年度数据安全评估报告的内容包括：

- 处理重要数据的情况；
- 发现的数据安全风险及处置措施；
- 数据安全管理制度，数据备份、加密、访问控制等安全防护措施，以及管理制度实施情况和防护措施的有效性；
- 落实国家数据安全法律、行政法规和标准情况；
- 发生的数据安全事件及其处置情况；
- 共享、交易、委托处理、向境外提供重要数据的安全评估情况；
- 数据安全相关的投诉及处理情况；
- 国家网信部门和主管、监管部门明确的其他数据安全情况。

（八）发生合并、重组、分立、解散、破产时的报告义务

根据《网络数安条例（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。

（九）在重要数据出境前开展评估

1. 出境前的评估与批准

根据《网络数安条例（征求意见稿）》第三十七条的规定，企业应当在出境重要数据前通过国家网信部门组织的数据出境安全评估。在出境时，企业不得超出网信部门安全评估时明确的出境目的、范围、方式和数据类型、规模等向境外提供重要数据。同时，企业应采取合同等有效措施监督数据接收方按照双方约定的目的、范围、方式使用数据，履行数据安全保护义务，保证数据安全，接受和处理数据出境所涉及的用户投诉，存留相关日志记录和数据出境审批记录三年以上。

数据出境对个人、组织合法权益或者公共利益造成损害的，企业应当依法承担责任，并配合国家网信部门会同国务院有关部门的核验工作以及责令停止数据出境的行为，采取补救措施。

若属于外国司法或者执法机构要求提供数据的情形，则必须经中华人民共和国主管机关批准后方可提供。

2. 出境后的年度报告

企业若向境外提供重要数据，根据《网络数安条例（征求意见稿）》第四十条，应当在每年 1 月 31 日前编制数据出境安全报告，向设区的市级网信部门报告上一年度数据出境情况，内容包括全部数据接收方名称、联系方式；出境数据的类型、数量及目的；数据在境外的存放地点、存储期限、使用范围和方式；涉及向境外提供数据的用户投诉及处理情况；发生的数据安全事件及其处置情况；数据出境后再转移的情况；国家网信部门明确向境外提供数据需要报告的其他事项等内容。

类似的，《工业和信息化领域数据安全管理办法（试行）（征求意见稿）》第二十四条同样强调重要数据出境应当依法依规进行数据出境安全评估，在确保安全的前提下进行数据出境，并加强对数据出境后的跟踪掌握。

（十）若企业有上市计划，则应审慎评估重要数据相关风险

《网络安全审查办法》除关注掌握超过 100 万用户个人信息的网络平台运营者赴国外上市，必须向网络安全审查办公室申报网络安全审查外，还要求企业重点防控重要数据被窃取、泄露、毁损以及非法利用、非法出境的风险；上市存在重要数据被外国政府影响、控制、恶意利用的风险，以及网络信息安全风险。因此，若企业持有重要数据，则在赴国外上市时需要额外评估重要数据的安全风险以及对国家网络安全的影响，配合国家的网络安全审查。此外，考虑到企业在赴国外上市还会涉及数据出境的情况，因此需要额外关注《数据出境安全评估办法（征求意见稿）》要求所有数据处理者在向境外提供数据前须事先开展数据出境风险自评估。如果出境数据中包括在境内运营

过程中收集和产生的重要数据的，则运营者还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。

同时，根据《网络数安条例（征求意见稿）》第三十二条，企业应当自行或者委托数据安全服务机构每年开展一次数据安全评估，并在每年 1 月 31 日前将上一年度数据安全评估报告报设区的市级网信部门。企业应保存该等风险评估报告至少三年。

（十一）制定培训计划，定期开展培训

根据《网络数安条例（征求意见稿）》第三十条的规定，企业应当制定数据安全培训计划，每年组织开展全员数据安全教育培训，负责处理重要数据安全相关的技术和管理人员每年教育培训时间不得少于二十小时。

（十二）遵循企业本行业对于重要数据的额外要求

《数据安全法》及其配套规则从普适的角度对于处理重要数据企业的合规义务进行了要求，各行业、各地区同样被赋权针对重要数据出具本行业、本地区的要求，因此，企业同样需要关注本行业、本地区的额外规定。

例如，《汽车数据安全管理若干规定（试行）》针对汽车数据处理活动所涉及的重要数据进行了规定，额外要求包括：

汽车重要数据原则在境内存储，因业务需要确需向境外提供的，应当通过国家网信部门会同国务院有关部门组织的安全评估；

每年十二月十五日前向省、自治区、直辖市网信部门和有关部门报送年度汽车数据安全管理情况，内容包括：汽车数据安全管理负责

人、用户权益事务联系人的姓名和联系方式、处理汽车数据的种类、规模、目的和必要性、汽车数据的安全防护和管理措施，包括保存地点、期限等内容；

向境外提供汽车重要数据的，补充报告接收者的基本情况、出境汽车数据的种类、规模、目的和必要性、汽车数据在境外的保存地点、期限、范围和方式、涉及向境外提供汽车数据的用户投诉和处理情况等内容。

三、结语

悬衡而知平，随着《指南》的修订和完善，我们相信在识别重要数据方面最终将会在顺应世界数据资源竞争趋势的同时，形成具有中国特色的可操性的指南。与此同时，我们建议企业首先应当梳理数据资产，识别并形成重要数据目录，并落实数据安全负责人和管理机构、完善内部制度体系、定期开展培训；其次，企业应当在落实网络等级保护要求的同时，对重要数据进行分类分级和加密保护；再次，当企业发生重要数据安全事件、在处理重要数据、涉及重要数据出境，以及赴国外上市等场景时，应当依法履行不同场景下开展自评估、向监管机构报告、向有关机构申报批准等合规流程；最后，企业还需要时刻关注所处行业和领域的特殊规定及行业标准，以便能够有针对性地及早做好准备。如此以来，企业才能在监管新趋势、新要求下不慌不乱，抓住机遇，迎接挑战。[22]

[22] 作者：孟洁、王程、张淑怡，https://mp.weixin.qq.com/s/455HRPeH7VDJqEl4sOu5PQ。

2. 境外上市中的网络安全审查（更新版）

引言

2021 年 12 月 24 日，中国证券监督管理委员会发布《关于就〈国务院关于境内企业境外发行证券和上市的管理规定（草案征求意见稿）〉公开征求意见的通知》[23]，强调境内企业境外发行上市的，应当严格遵守国家法律法规和有关规定，建立健全保密制度，采取必要措施落实保密义务，不得泄露国家秘密，不得损害国家安全和公共利益。**境内企业境外发行上市涉及向境外提供个人信息和重要数据的，应当符合国家法律法规和有关规定。**经国务院有关主管部门依法审查认定，境外发行上市威胁或危害国家安全的，不得境外发行上市。

2022 年 1 月 4 日，国家互联网信息办公室等十三部门发布《网络安全审查办法》。相较于 2021 年 7 月 10 日发布的《网络安全审查办法（修订草案征求意见稿）》，《网络安全审查办法》2022 年修订版整体调整幅度不大，判断企业是否需要主动申报网络安全审查的实质标准仍为：是否掌握了 100 万用户个人信息并赴国外上市、是否影响或者可能影响国家安全。我们结合《网络安全审查办法》终审稿，特更新本文（本文初版发表于 2021 年 12 月 29 日）。

一、我国网络安全审查制度的演进

我国网络安全审查制度可追溯至 2015 年颁布的《中华人民共和国国家安全法》（以下简称《国家安全法》）。其中第五十九条明确，国家建立国家安全审查和监管的制度和机制，对**影响或者可能影响国家安全的外商投资、特定物项和关键技术、网络信息技术产品和服务、**

[23] 原文请参见：http://www.csrc.gov.cn/csrc/c101981/c1662244/content.shtml。

涉及国家安全事项的建设项目，以及其他重大事项和活动，进行国家安全审查，有效预防和化解国家安全风险。

全国人大常委会于2016年通过的《中华人民共和国网络安全法》（以下简称《网络安全法》）第三十五条明确，**关键信息基础设施运营者采购网络产品和服务**，可能影响国家安全的，应当通过国家网信部门会同国务院有关部门组织的国家安全审查。

2020年4月13日，国家互联网信息办公室（以下简称"网信办"）与其他11个国务院直属部门共同发布了《网络安全审查办法》，要求关键信息基础设施运营者采购网络产品和服务，影响或可能影响国家安全的，应当进行网络安全审查，并明确废止了2017年5月2日发布的《网络产品和服务安全审查办法（试行）》（现已失效）。此前《网络产品和服务安全审查办法（试行）》将须进行网络安全审查的对象仅限定于**关系国家安全的网络和信息系统采购的重要网络产品和服务**。

2021年7月2日，网络安全审查办公室发布公告，对某互联网出行平台启动网络安全审查。[24]随后，网信办会同其他六部委联合进驻该平台，开展网络安全审查，以确定其是否符合《国家安全法》《网络安全法》及《网络安全审查办法》。在审查过程中，为配合审查工作，防范风险扩大，该平台被要求暂停新用户注册。同一时期，网信办还启动了对其他三个互联网平台的网络安全审查。

2021年7月10日，网信办发布了《网络安全审查办法（修订草案征求意见稿）》，并向社会公开征求意见（以下简称《审查办法修

[24] 请参见：http://www.cac.gov.cn/2021-07/02/c_1626811521011934.htm。

订意见稿》）。《审查办法修订意见稿》扩大了网络安全审查的范围，将所有在中国大陆境内收集、产生数据，可能影响国家安全的数据处理者纳入了审查范围，由此明确网络安全审查将同时涵盖网络安全与数据处理活动安全两方面内容。此外，《审查办法修订意见稿》第六条规定，掌握超过 100 万用户个人信息的运营者赴国外上市，必须向网络安全审查办公室申报网络安全审查。进一步明确，对于数据处理者开展数据处理活动，影响或可能影响国家安全的，也应进行网络安全审查。审查内容主要包括两类，一类是针对核心数据、重要数据或大量个人信息被窃取、泄露、毁损以及非法利用或出境的风险，另一类则是针对国外上市后关键信息基础设施、核心数据、重要数据或大量个人信息被国外政府影响、控制、恶意利用的风险。

2021 年 9 月 1 日生效并实施的《中华人民共和国数据安全法》（以下简称《数据安全法》）承袭了《审查办法修订意见稿》对网络安全审查适用范围进行扩展的思路。《数据安全法》第二十四条规定，“对影响或者可能影响国家安全的**数据处理活动**进行国家安全审查。”因此，网络安全审查对象以生效法律规定得以确认，其不仅针对《网络安全法》下的关键信息基础设施运营者，而是包括关键信息基础设施运营者在内的开展数据处理活动的所有数据处理者。

2021 年 11 月 14 日，网信办公布《网络数据安全管理条例（征求意见稿）》（以下简称《数安条例意见稿》），对《网络安全法》《数据安全法》《中华人民共和国个人信息保护法》（以下简称《个人信息保护法》）中关于数据安全管理的规定提出了细化要求。其中令人关注的条款是第十三条规定的网络安全审查义务。在如下情况下，数据处理者应当申报网络安全审查：（1）汇聚掌握大量关系国家安全、经济发展、公共利益的数据资源的互联网平台运营者实施合并、

重组、分立，影响或者可能影响国家安全的；（2）**处理一百万人以上个人信息的数据处理者赴国外上市的**；（3）**数据处理者赴香港上市，影响或者可能影响国家安全的**；（4）其他影响或者可能影响国家安全的数据处理活动。

2022 年 1 月 4 日，网信办在内的十三部委联合修订了《网络安全审查办法》（以下简称《审查办法 2022 修订》），该办法自 2022 年 2 月 15 日起施行，并废止了 2020 年 4 月 13 日公布的《网络安全审查办法》。

我们将网络安全审查制度的演进过程制作为如下图示，供读者参阅：

二、对境外上市企业启动网络安全审查的条件

针对境外上市是否涉及网络安全审查，《数安条例意见稿》对此前《审查办法修订意见稿》规定的**审查启动条件**进行了调整和补充，而《审查办法 2022 修订》基本沿用了《审查办法修订意见稿》的规定，具体比较如下：

《审查办法修订意见稿》	《数安条例意见稿》	《审查办法 2022 修订》
第二条：**关键信息基础设施运营者**采购网络产品和服务，**数据处理者**（以下称运营者）开展数据处	第十三条：**数据处理者**开展以下活动，应当按	第二条：**关键信息基础设施运营者**采购网络产品和服务，**网络平台运营者**开展数据处理活动，**影**

理活动，**影响或可能影响国家安全的**，应当按照本办法进行网络安全审查。 第六条：**掌握超过 100 万用户个人信息的运营者**赴**国外上市**，必须向网络安全审查办公室申报网络安全审查。	照国家有关规定，申报网络安全审查： （一）汇聚掌握大量关系国家安全、经济发展、公共利益的数据资源的互联网平台运营者实施合并、重组、分立，影响或者可能影响国家安全的； （二）**处理一百万人以上个人信息**的数据处理者赴**国外上市**的； （三）数据处理者赴**香港上市，影响或者**可能**影响国家安全**的； （四）其他影响或者可能影响国家安全的数据处理活动。	**响或者可能影响**国家**安全的**，应当按照本办法进行网络安全审查。 第五条：**关键信息基础设施运营者**采购网络产品和服务的，应当预判该产品和服务投入使用后可能带来的国家安全风险。影响或者可能影响国家安全的，应当向网络安全审查办公室申报网络安全审查。 关键信息基础设施安全保护工作部门可以制定本行业、本领域预判指南。 第七条：**掌握超过 100 万用户个人信息的网络平台运营者**赴国外上市，必须向网络安全审查办公室申报网络安全审查。

根据《审查办法 2022 修订》，企业境外上市过程中的网络安全审查启动条件要点如下：

1. **掌握超过 100 万用户个人信息的网络平台运营者赴国外上市，必须向网络安全审查办公室申报网络安全审查。**《审查办法 2022 修订》新增了“网络平台运营者”这一概念，但并未对其进行明确定义，可参考《数安条例意见稿》对于“互联网平台运营者”的定义，“互联网

平台运营者是指为用户提供信息发布、社交、交易、支付、视听等互联网平台服务的数据处理者”。假如《数安条例意见稿》最终出台时对现有条款不再调整，那么其所规制的数据处理者范围较《审查办法2022修订》中规定的网络平台运营者实则更大。但从申报条件来说，依然要重点关注“掌握”和“超过100万用户个人信息”这两个标准，对于传统企业，例如钢铁、食品等，在数字经济时代也迈向了数字化平台转型步伐，是否需要申报网络安全审查，依然取决于是否“掌握”及“超过100万用户个人信息”。

2. **《审查办法2022修订》未提及赴香港上市是否承担网络安全审查申报义务**，未提及《数安条例意见稿》中赴香港上市的相关要求。虽然从效力位阶上看，《数安条例意见稿》将由国务院发布，生效后属于行政法规，而《审查办法2022修订》生效后仅为部门规章，但是，从发布时间来看，《审查办法2022修订》现已发布，《数安条例意见稿》的意见反馈截止时间为2021年12月13日，二者均由网信办会同相关部门研究起草。因此，就香港上市是否需要申报网络安全审查的问题，我们认为后续《数安条例意见稿》较大概率会保持和《审查办法2022修订》的统一。根据**《审查办法2022修订》，拟香港上市企业（即便掌握超过100万用户个人信息的网络平台运营者）通常并无网络安全审查主动申报义务，但企业仍应排查其是否落入《审查办法2022修订》第二条需要进行网络安全审查的范畴。**

3. 《审查办法2022修订》第二条规定，关键信息基础设施运营者采购网络产品和服务，网络平台运营者开展数据处理活动，影响或者可能影响国家安全的，应当按照本办法进行网络安全审查。结合《审查办法2022修订》第十条，评估国家安全风险时，重点考虑如下因素：

（1）如拟上市企业目前未被认定为关键信息基础设施运营者的（以下简称“非关键信息基础设施运营者”），则应评估：（i）产品和服务的安全性、开放性、透明性、来源的多样性，供应渠道的可靠性以及是否因政治、外交、贸易等因素导致供应链可能中断的风险；（ii）产品和服务提供者遵守中国法律、行政法规、部门规章的情况；（iii）核心数据、重要数据或大量个人信息被窃取、泄露、毁损以及非法利用、非法出境的风险、被国外政府影响、控制、恶意利用的风险等；（iv）其他可能危害网络安全和数据安全的因素等。据此，建议企业赴香港上市前，对网络安全和数据合规情况进行综合评估，并对企业处理数据是否存在影响国家安全的可能性提前进行自评估或者委托专业机构协助评估，综合考虑网络安全的可靠性、所在行业、数据量级、数据敏感程度、是否存在数据出境等情况，尤其重视上市过程中也须同等履行数据安全义务，防止因上市活动可能引发的安全风险。

（2）如拟上市企业已经被主管部门认定为关键信息基础设施运营者的，除上方第（1）点所述内容外，还应评估：（i）企业所采购的产品和服务在使用后是否会产生关键信息基础设施被非法控制、遭受干扰或者破坏的风险；（ii）产品和服务供应一旦中断，是否会对关键信息基础设施业务的连续性造成危害；（iii）上市是否存在关键信息基础设施被国外政府影响、控制、恶意利用的风险，以及网络信息安全风险；（iv）其他可能危害关键信息基础设施安全、网络安全和数据安全的因素。

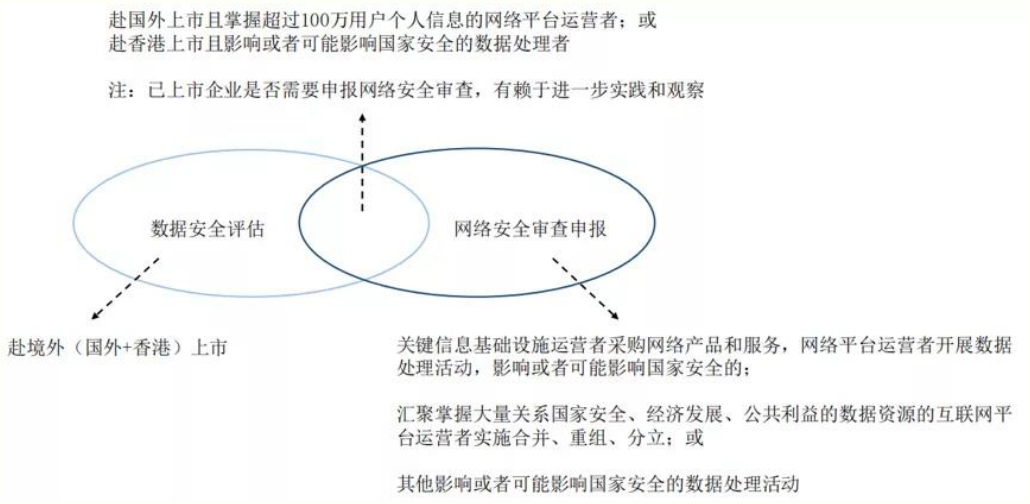
针对“关键信息基础设施运营者”的认定，国务院于 2021 年 7 月 30 日发布的《关键信息基础设施安全保护条例》仅给出原则性指引：关键信息基础设施是指公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域的，以及

其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统等。该条例第九条、第十条进一步规定，由行业主管部门制定具体的认定规则，并对关键信息基础设施进行认定并通知运营者。

4. **网络安全审查可以由网络安全审查办公室依职权发起**。网络安全审查办公室有权对其认为影响或者可能影响国家安全的网络产品和服务以及数据处理活动开展网络安全审查，网络安全审查办公室将委托中国网络安全审查技术与认证中心承担具体工作，由中国网络安全审查技术与认证中心在网络安全审查办公室的指导下，承担接受申报材料和进行形式审查等工作。网络安全审查办公室、网络安全审查工作机制成员单位和/或中央网络安全和信息化委员会依照《审查办法 2022 修订》的规定进行审查。

5. 《数安条例意见稿》除了第十三条规定的网络安全审查外，第三十二条还要求，赴境外上市的数据处理者，应当自行或委托第三方每年开展一次**数据安全评估**，并在每年 1 月 31 日将上一年度数据安全评估报告报送设区的市级网信部门。此处《数安条例意见稿》使用“境外”的表达，意味着无论赴国外上市还是赴香港上市，均需要进行数据安全评估。值得注意的是，《审查办法 2022 修订》增加了第二十二条第二款，提出“国家对数据安全审查、外商投资安全审查另有规定的，应当同时符合其规定。”这意味着，网络安全审查并不完全等同于数据安全审查。

我们将不同上市场景发行人的网络安全审查义务图示如下：



三、网络安全审查流程和时间

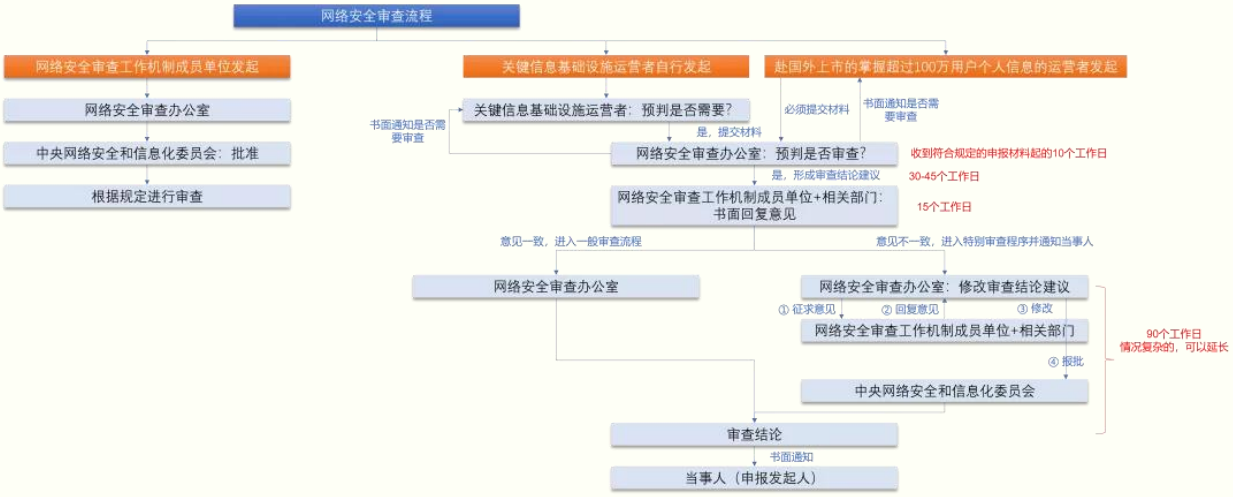
网络平台运营者赴国外上市的网络安全审查(如需)的流程如下：

- 网络平台运营者应当在向国外证券监管机构提出上市申请之前，申报网络安全审查。
- 网络安全审查办公室应当自收到符合《审查办法 2022 修订》第八条规定的审查申报材料起 10 个工作日内，确定是否需要审查并书面通知当事人。
- 网络安全审查办公室认为需要开展网络安全审查的，应当自向当事人发出书面通知之日起 30 个工作日内完成初步审查，包括形成审查结论建议和将审查结论建议发送网络安全审查工作机制成员单位、相关部门征求意见；情况复杂的，可以延长 15 个工作日。
- 网络安全审查工作机制成员单位和相关部门应当自收到审查结论建议之日起 15 个工作日内书面回复意见。

- 网络安全审查工作机制成员单位、相关部门意见一致的，网络安全审查办公室以书面形式将审查结论通知当事人；意见不一致的，按照特别审查程序处理。

- 特别审查程序一般应当在 90 个工作日内完成，情况复杂的可以延长。

具体流程图示如下：



企业申报网络安全审查可能有以下三种情况：一是无需审查；二是启动审查后，经研判不影响国家安全的，可继续赴国外上市程序；三是启动审查后，经研判影响国家安全的，不允许赴国外上市。

四、法律后果

对于违反《审查办法 2022 修订》的行为，《审查办法 2022 修订》仅规定依照《网络安全法》《数据安全法》的规定处理。相关的法律后果包括：

- 关键信息基础设施运营者违反本法第三十五条[25]规定，使用未经安全审查或者安全审查未通过的网络产品或者服务的，由有关主管部门责令停止使用，处采购金额一倍以上十倍以下罚款；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款（《网络安全法》第六十五条）。

- 关键信息基础设施运营者违反本法第三十七条[26]规定，在境外存储网络数据，或者向境外提供网络数据的，由有关主管部门责令改正，给予警告，没收违法所得，处五万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、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处一万元以上十万元以下罚款（《网络安全法》第六十六条）。

- 违反国家核心数据管理制度，危害国家主权、安全和发展利益的，由有关主管部门处二百万元以上一千万元以下罚款，并根据情况责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照；构成犯罪的，依法追究刑事责任（《数据安全法》第四十五条第二款）。

- 如应履行而未申报网络安全审查的，《数安条例意见稿》规定的处罚后果是：由有关主管部门对企业处以责令改正、给予警告、罚款、责令暂停相关业务、停业整顿、吊销相关业务许可

[25] 《网络安全法》第三十五条：关基运营者采购网络产品和服务，可能影响国家安全的，应当通过国家网信部门会同国务院有关部门组织的国家安全审查。

[26] 《网络安全法》第三十七条：关基运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。

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处罚款。

《审查办法 2022 修订》第十六条第二款进一步明确，为防范风险，当事人应当在审查期间按照审查要求采取预防和消减风险的措施。结合 2021 年 7 月网络安全审查办公室发起的审查情况来看，预防和消减风险的措施可能包括配合审查进行产品下架、停止新用户注册等。

《国务院关于境内企业境外发行证券和上市的管理规定（草案征求意见稿）》进一步规定，如企业属于该规定列举的不得境外发行上市的情形（包括经审查境外发行上市威胁或危害国家安全的）进行境外发行上市的，国务院证券监督管理机构、国务院有关主管部门对境内企业给予警告，并处以一百万元以上一千万元以下的罚款，情节严重的，责令暂停相关业务或者停业整顿、吊销相关业务资质许可或者吊销营业执照。对境内企业的控股股东、实际控制人、董事、监事、高级管理人员给予警告，单处或者并处五十万元以上五百万元以下的罚款。

此外，《国务院关于境内企业境外发行证券和上市的管理规定（草案征求意见稿）》还规定证券公司、律师事务所未严格履行职责、督促企业遵守相关规定的，给予警告，并处以五十万元以上五百万元以下的罚款。对有关责任人员给予警告，并处以二十万元以上二百万元以下的罚款。因此，上市中介机构在就网络安全审查相关问题发表意见时，亦应慎重对待。

五、近期港股上市案例中的相关披露

（一）某在线音乐服务企业

某在线音乐服务企业于2021年12月初在香港联交所上市，其招股说明书中与网络安全审查有关的披露如下：[27]

“概要”章节	于2021年7月10日，网信办就《审查办法修订意见稿》公开征求意见，规定关基运营者采购网络产品和服务，数据处理者（连同关基运营者统称“运营者”）开展数据处理活动，影响或可能影响国家安全的，应当进行网络安全审查。根据《审查办法修订意见稿》，掌握超过一百万用户个人信息的运营者赴国外上市，必须向网络安全审查办公室申报网络安全审查。然而，《审查办法修订意见稿》并无就“国外上市”提供进一步解释或诠释。截至最后实际可行日期，《审查办法修订意见稿》尚未正式施行。根据现有中国网络安全法律，关基运营者拟采购网络产品和服务，可能影响国家安全的，应当进行网络安全审查。如我们的中国法律顾问告知，在《审查办法修订意见稿》下，**“关基运营者”的实际范畴及现有监管机制尚未明确**，而中国政府机关对诠释及执行该等法律可能具广泛的自由裁量权。截至本文件日期，我们并无涉及网信办就网络安全审查作出的任何调查，而我们亦无就此方面接获任何询问、通知、警告或制裁。 2021年11月14日，网信办就《数安条例意见稿》公开征求意见。根据《数安条例意见稿》，数据处理者如进行以下活动：（1）汇聚掌握大量关系国家安全、经济发展、公共利益的数据资源的互联网平台运营者实施合并、重组、分立，影响或者可能影响国家安全的；（2）处理一百万人以上个人信息的数据处理者赴国外上市的；（3）数据处理者赴香港上市，影响或者可能影响国家安全的；（4）其他影响或者可能影响国家安全的数据处理活动，应当按照国家有关规定，申报网络安全审查。然而，**《数安条例意见稿》并无就“影响或可能影响国家安全”提供进**

[27] 请参见：https://www1.hkexnews.hk/listedco/listconews/sehk/2021/1123/2021112300033_c.pdf。为了便于阅读，招股书中的表述与本文其他部分的表述做了统一处理。

	一步解释或诠释。如我们的中国法律顾问所告知，中国政府机关对于“影响或可能影响国家安全”的诠释可能具有广泛的自由裁量权。 假设《审查办法修订意见稿》及《数安条例意见稿》未来以目前的形式生效，视乎《审查办法修订意见稿》及《数安条例意见稿》的进一步实施详情、指引及澄清，我们及中国法律顾问认为将不会对我们截至本文件日期在任何重大方面遵守法律法规或上市构成重大不利影响，原因是（i）如“业务—数据安全”所披露，我们**已实施措施，以确保安全存储和传送数据，以及防止任何未经授权取得或使用数据**；（ii）截至本文件日期，我们并无遭受任何政府机关处以有关违反数据安全法律法规的重大罚款或行政处罚；（iii）截至本文件日期，我们概无将对业务运营有重大不利影响的数据或个人信息重大泄漏或对数据保护和隐私法律法规的违反；（iv）我们已在**采取措施准备遵守《数安条例意见稿》的规定**；及（v）我们将继续关注中国数据安全法规的发展。倘《审查办法修订意见稿》及《数安条例意见稿》生效，我们将向相关监管机构寻求指引，以确保我们采取的措施属适当。然而，本公司中国法律顾问不排除未来颁布的新规则或法规将对本集团造成额外合规要求的可能性。
“风险因素”章节	全国人大常委会于 2021 年 6 月 10 日发布《数据安全法》，规范中国的数据处理活动和安全监管，该法已于 2021 年 9 月 1 日生效。根据《数据安全法》，国家建立数据安全审查制度，对影响或者可能影响国家安全的数据处理活动进行国家安全审查。于 2021 年 7 月 10 日，网信办就《审查办法修订意见稿》公开征求意见，该草案规定运营者开展数据处理活动，影响或可能影响国家安全的，应当进行网络安全审查。根据《审查办法修订意见稿》，掌握超过 1 百万用户个人信息的运营者赴国外上市，必须向网络安全审查办公室申报网络安全审查。此外，于

	2021 年 11 月 14 日，网信办就《数安条例意见稿》公开征求意见，当中要求数据处理者于其日常营运遵守若干规定，并进一步列明若干情况下数据处理者应申报网络安全审查，包括数据处理者赴香港上市，影响或者可能影响国家安全的。然而，**《审查办法修订意见稿》及《数安条例意见稿》均无就"国外上市"或"影响或可能影响国家安全"提供任何进一步解释或诠释**。截至最后实际可行日期，《审查办法修订意见稿》及《数安条例意见稿》均未正式通过。我们无法保证我们在日后的融资活动中会否受网络安全审查的限制，抑或日后新颁布的规则或法规会否对我们构成额外合规要求。

根据上述披露，该公司未进行网络安全审查，其主张的理由如下：一方面，现行有效的《网络安全法》中对于"关键信息基础设施运营者"认定不明；另一方面，因《审查办法修订意见稿》与《数安条例意见稿》暂未生效，即使其按照现行版本生效，鉴于其对"国外上市"与"影响或可能影响国家安全"的定义不明晰，具体影响暂未可知。

（二）某人工智能软件公司

某人工智能软件公司于 2021 年 12 月末在香港联交所上市，其招股说明书中与网络安全审查有关的披露如下：[28]

"概要"章节	最近中国政府机构已颁布（其中包括）《个人信息保护法》及《数据安全法》，以确保网络安全、数据及个人信息保护，表明随着相关监督监管力度不断加大，规管该等领域的相关法律及法规亦在不断完善。具体而言，网信办已提出《审查办法修订意见稿》及《数安条例意见稿》，征求公众意见，当中对潜在网

[28] 请参见：https://www1.hkexnews.hk/listedco/listconews/sehk/2021/1207/2021120700018_c.pdf。为了便于阅读，招股书中的表述与本文其他部分的表述做了统一处理。

	络安全审查范围提出指引……我们及我们的中国法律顾问认为，假设管理条例草案及修订草案以其当前形式生效，其不会对我们的业务经营、全球发售或上市产生重大不利影响，理由如下（i）如“业务—数据隐私及个人信息保护”所披露，我们已经实施全面措施以确保持续遵守相关法律法规；（ii）截至本招股章程日期，我们并未就数据及网络安全受到任何政府机构实施重大罚款、强制整改或其他处罚；（iii）截至本招股章程日期，不存在任何由主管政府部门或第三方针对本集团提起的、未决的或可能提起将对我们的业务营运产生重大不利影响的数据或个人信息泄露、违反数据保护和隐私法律法规的重大事件、或者调查或其他法律程序；及（iv）我们将继续密切关注数据安全方面的法律法规及监管发展，并遵守最新的监管规定。
“风险因素”章节	于 2021 年 7 月 10 日，网信办颁布《审查办法修订意见稿》，进一步重申和扩大了网络安全审查的适用范围。根据办法草案，拟采购网络产品和服务的关基运营者及数据处理者（统称“运营者”）从事影响或可能影响国家安全的数据处理活动的，应当接受网络安全审查。办法草案进一步规定，倘若运营者掌握 100 万以上用户的个人信息并拟“国外”上市，则其必须进行网络安全审查。 然而，办法草案并未对“国外”上市规定进一步解释或阐释。诚如我们的中国法律顾问所告知，办法草案中掌握有 100 万以上个人用户信息的运营者赴国外上市申请网络安全审查的要求在当前形式下不适用于我们，主要乃由于（i）截至本招股章程日期，**本集团尚未从适用中国政府当局收到任何通知或决定，将其确定为关基运营者**，（ii）办法草案下的**“数据处理者”的确切范围尚不明确**，（iii）本集团正在申请于香港上市，而**香港不属于“国外”的范围**。于 2021 年 11 月 14 日，网信办发布了《数安条例意见稿》，重申了数据处理者应当申请网络安全审查的情

	形，其中包括（i）处理一百万人以上个人信息的数据处理者申请赴“国外”上市的；及（ii）数据处理者赴香港上市，影响或者可能影响国家安全的。然而，对于**如何确定什么构成“影响国家安全”，其并无提供进一步的说明或解释**，我们是否会根据该办法草案就全球发售接受网络安全审查仍存在不确定性。截至最后实际可行日期，上述两项办法草案尚未获正式通过。截至本招股章程日期，我们尚未收到适用政府当局有关国家安全的任何调查、通知、警告或制裁。本集团亦确认，截至本招股章程日期，我们并无涉及网信办基于国家安全或其他任何理由进行的有关网络安全审查的调查，且并未就此收到任何询问、通知、警告或制裁。此外，执行条款和预期采纳或生效日期可能会发生很大的不确定性变化。在现阶段，我们无法预测该等办法草案的影响（如有），且我们将密切监测和评价规则制定过程中的任何进展。因此，尚不确定拟议草案是否适用于我们的业务、全球发售，或者未来的监管变化是否会对我们这样的公司施加额外限制。鉴于上述不确定性，截至本招股章程日期，我们尚未申请有关网络安全审查。

基于该公司于招股说明书中的披露，其暂未根据《审查办法修订意见稿》或《数安条例意见稿》向监管部门申请网络安全审查。其主张的理由如下：该公司未被认定为关键信息基础设施运营者；该公司赴港上市不属于国外上市；现阶段《审查办法修订意见稿》与《数安条例意见稿》仍未生效，即使其按照现行版本生效，“数据处理者”、“国家安全”的定义未明确，因此该公司认为其被要求进行网络安全审查的可能性较低。

虽然上述两家公司于香港上市时，《审查办法 2022 修订》尚未颁布，但鉴于《审查办法 2022 修订》未对《审查办法修订意见稿》

中需进行网络安全审查主体的判断标准作出实质性更改，因此以上两个案例仍具有一定的参考意义。

六、可借鉴的应对思路

基于《审查办法 2022 修订》的规定，结合过往案例中发行人于招股说明书中的披露，在香港联交所上市的发行人在招股书中的披露可以采纳以下思路：

发行人应判断其是否属于网络平台运营者，或是否已经被监管部门确认并通知为“关键信息基础设施运营者”（在可行的情况下，建议征求行业主管部门的意见）；如是，则发行人应评估其采购网络产品和服务的行为或者开展数据处理活动的行为是否影响或者可能影响到国家安全；如认为是，则需要及时申报网络安全审查。

1. 在《审查办法 2022 修订》2022 年 2 月 15 日实施后，如发行人属于掌握超过 100 万用户个人信息的网络平台运营者赴国外上市的，则必须申报网络安全审查。但是掌握个人信息的数量并非赴香港上市企业申报网络安全审查的标准，因此赴香港上市是否需要进行网络安全审查的判断重点应落在“影响或者可能影响国家安全”，企业赴香港上市判断是否“影响或者可能影响国家安全”，可以参考本文第二节有关“非关键信息基础设施运营者”考虑的评估因素。

2. 如果发行人不属于影响或者可能影响国家安全的关键信息基础设施运营者或网络平台运营者，一旦因其处理数据的活动或行为影响或者可能影响国家安全，则仍然需要申报网络安

全审查。建议相关企业参考本文有关“非关键信息基础设施运营者”考虑的评估因素。

3. 虽然《审查办法 2022 修订》刚刚发布，我们依然期待《数安条例意见稿》终审稿可以早日出台，两者构成完整规则以指导实践。企业是否需要主动申报网络安全审查，建议可从运营者的主体性质、处理个人信息的人数，以及处理行为本身的影响等维度出发，对影响或者可能影响国家安全进行判断与风险评估。值得一提的是，上文两个港股上市案例中，无论是否申报网络安全审查，发行人均采取了数据安全及合规的相关措施，包括：保障数据的安全存储和传输、防止任何未经授权的数据获取和使用、加强网络与数据安全的内控制度、发挥管理层与董事会的监督管理职责等，以表明发行人对现有数据处理行为合法合规的做法。

七、总结与展望

随着网络安全审查制度体系的逐步落地与完善，企业上市前的数据合规实施工作、评估及审计落实情况，以及确认是否需要依法申报网络安全审查已然成为拟赴境外上市企业所需面临的新课题。一方面，拟境外上市的企业需在上市前搭建较为完整的数据合规体系[29]，以应对上市过程中保荐人、中介机构的询问以及监管部门的审核。另一方面，经自评估，有可能触发网络安全审查申报的企业，应当在上市材

[29] 具体可详见《环球合规与风控 | 面对网络安全审查，中概股企业需做何准备？——下篇：企业数据合规建议》，链接为 https://mp.weixin.qq.com/s/e29tnDhdLBGGWLTgbgmDbg。

料递交前履行网络安全审查申报义务，以符合监管要求。目前网络安全审查的案例有限，网络安全审查的具体实践仍有待观察和总结。[30]

[30] 作者：孟洁、李来祥、殷坤、李楠，https://mp.weixin.qq.com/s/bmJXr-dUeFprJMg4E61yfw。

2022 年 第一期 /总第三十五期

数据合规时事速递
NEWSLETTERS

环球律师事务所数据合规团队专注于网络安全与数据合规、个人信息隐私保护等领域。我们在企业数据合规体系建设等方面具备丰富的经验，为多家大型互联网公司、全球企业提供法律服务。

我们为客户提供在网络安全与数据合规、个人信息隐私保护、跨境数据传输、电子商务与广告法领域的法律咨询及相关方案设计，帮助客户迎接数据时代的机遇与挑战。

若您有任何疑问和建议，欢迎随时与我们联系，联系邮箱：dongjierui@glo.com。您也可以扫描上方二维码，关注我们的公众号“M 姐 数据合规评论”获取更多资讯。