

# 数据合规时事速递

## NEWSLETTERS

2022 第二期/ 总第三十六期



环球律师事务所  
GLOBAL LAW OFFICE



### 精彩导读

新规速递/ 网信办就《互联网弹窗信息推送服务管理规定（征求意见稿）》公开征求意见

监管动态/ 工信部召开行政指导会规范 App 推荐下载行为及改善网页浏览服务体验

环球评论/ 《工业和信息化领域数据安全管理办法（试行）（第二次征求意见稿）》要点解读


2022 年 03 月 15 日



## 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其知名互联网企业、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 LEALBAND 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 LEALBAND 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《B/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:

⑩ 网络安全与数据合规

⑩ 互联网与电商合规

⑩ 个人信息保护

⑩ 反腐败/反商业贿赂合规



## 目录

一、新规速递.....	6
1. 工信部印发《车联网网络安全和数据安全标准体系建设指南》	7
2. 网信办就《互联网弹窗信息推送服务管理规定（征求意见稿）》 公开征求意见.....	7
3. 网信办就《未成年人网络保护条例》再次公开征求意见.....	8
4. 《山东省公共数据开放办法》于 2022 年 4 月 1 日起施行.....	9
5. 美国参议院通过《加强美国网络安全法》.....	10
6. 英国和新加坡签署《数字经济协议》.....	11
二、监管动态.....	13
1. 工信部召开行政指导会规范 APP 推荐下载行为及改善网页浏览 服务体验.....	14
2. 工信部网络安全管理局召开全国会议指导推进车联网卡实名登 记工作.....	15
3. 北京市通管局就网络安全问题约谈两家互联网公司.....	15
4. 美国就儿童隐私保护问题对某知名短视频 APP 企业展开调查..	16
5. 美国证交会拟要求上市公司信息安全事件应在 4 天内披露.....	17
三、相关新闻.....	18
1. 工信部通报 14 款侵害用户权益 APP（2022 年第 2 批，总第 22	

批) .....	19
2. 最高检印发第三十五批指导性案例, 督促保护儿童个人信息权益	
19	
3. 2022 年 2 月全国受理网络违法和不良信息举报 1233.2 万件....	20
4. 浙江省 APP 专项治理工作组通报 38 款违法违规收集使用个人信息 APP .....	21
5. 上海市通管局发布关于通信网络安全防护管理情况的通报.....	21
6. 意大利对 CLEARVIEW AI 罚款 2000 万欧元并令其删除数据 .....	22
7. 美国对 WEIGHT WATCHERS 处以 150 万美元罚款 .....	23
<b>四、环球评论.....</b>	<b>24</b>
1. 《工业和信息化领域数据安全管理办法（试行）（第二次征求意见稿）》要点解读.....	25

---

# 新规速递



## 1. 工信部印发《车联网网络安全和数据安全标准体系建设指南》

2022年3月7日，工业和信息化部发布了《车联网网络安全和数据安全标准体系建设指南》（以下简称《指南》），以指导车联网相关标准研制。

《指南》提出，到2025年形成较为完善的车联网网络安全和数据安全标准体系。完成100项以上标准的研制，提升标准对细分领域的覆盖程度，加强标准服务能力，提高标准应用水平，支撑车联网产业安全健康发展。

《指南》明确，标准体系的建设内容主要涉及总体与基础共性、终端与设施网络安全、网联通信安全、数据安全、应用服务安全、安全保障与支撑等六个部分。

其中，数据安全标准主要规范智能网联汽车、车联网平台、车载应用服务等数据安全和个人信息保护要求，包括通用要求、分类分级、出境安全、个人信息保护、应用数据安全等五类标准。<sup>1</sup>

《车联网网络安全和数据安全标准体系建设指南》全文请参见：

[https://www.miit.gov.cn/zwgk/zcwj/wjfb/tz/art/2022/art\\_e36a55c43a3346c9a4b31e534b92be44.html](https://www.miit.gov.cn/zwgk/zcwj/wjfb/tz/art/2022/art_e36a55c43a3346c9a4b31e534b92be44.html)

## 2. 网信办就《互联网弹窗信息推送服务管理规定（征求意见稿）》公开征求意见

2022年3月2日，国家互联网信息办公室公布了《互联网弹窗信息推送服务管理规定（征求意见稿）》（以下简称《征求意见稿》），并向社会征求意见，意见反馈截至3月17日。

---

<sup>1</sup> 工信部官网。



其中,《征求意见稿》明确规定,互联网弹窗信息推送服务不得设置诱导用户沉迷、过度消费等违反法律法规或者违背伦理道德的算法模型;不得滥用个性化弹窗服务,利用算法屏蔽信息、过度推荐等;不得滥用算法,针对未成年用户进行画像,向未成年用户推送可能影响其身心健康的信息。

同时,《征求意见稿》强调,弹窗推送广告信息,必须进行内容合规审查,不得违反国家相关法律法规;应当具有可识别性,显著标明“广告”并明示用户;确保弹窗广告可一键关闭。不得以弹窗信息推送方式呈现恶意引流跳转的第三方链接、二维码等信息;不得通过弹窗信息推送服务诱导用户点击,实施流量造假、流量劫持。<sup>2</sup>

《互联网弹窗信息推送服务管理规定(征求意见稿)》全文请参见:

[http://www.cac.gov.cn/2022-03/02/c\\_1647826956995841.htm](http://www.cac.gov.cn/2022-03/02/c_1647826956995841.htm)

### 3. 网信办就《未成年人网络保护条例》再次公开征求意见

日前,国家互联网信息办公室发出《未成年人网络保护条例(征求意见稿)》(以下简称《征求意见稿》),再次征求公众意见,意见反馈截至4月13日。

《征求意见稿》共七章六十七条,主要内容包括四大方面。一是关于加强未成年人网络素养培育。二是关于加强网络信息内容规范。三是关于加强未成年人个人信息保护。四是关于加强未成年人网络沉迷防治。

其中,《征求意见稿》明确要求,网络游戏、网络直播、网络音视频、网络社交等网络服务提供者应当采取措施,合理限制未成年人在使用网络产品和服务中的单次消费数额和单日累计消费数额,不得向未成年人提供与其民事行为能力不符的付费服务。

---

<sup>2</sup> 网信办官网。



此外，《征求意见稿》还对有关违法行为补充规定了相应的法律责任。<sup>3</sup>

《未成年人网络保护条例》全文请参见：

[http://www.cac.gov.cn/2022-03/14/c\\_1648865100662480.htm](http://www.cac.gov.cn/2022-03/14/c_1648865100662480.htm)

#### 4. 《山东省公共数据开放办法》于 2022 年 4 月 1 日起施行

《山东省公共数据开放办法》（以下简称《办法》）将于 2022 年 4 月 1 日起施行。《办法》共包括 23 条内容，明确了公共数据的适用范围，并在加强数据安全保护等方面作出新规定，使公共数据开放有了“明白纸”。

《办法》与其他地方现有的公共数据开放立法相比，适用范围更全面。其明确了国家机关、法律法规授权的具有管理公共事务职能的组织、具有公共服务职能的企业事业单位、人民团体等在依法履行公共管理职责、提供公共服务过程中，收集和产生的各类数据均属于公共数据，应纳入公共数据开放办法管理。

《办法》还明确了重点和优先开放数据范围：重点和优先开放与数字经济、公共服务、公共安全、社会治理、民生保障等领域密切相关的市场监管、卫生健康、自然资源、生态环境、就业、教育、交通、气象等数据，以及行政许可、行政处罚、企业公共信用信息等数据。同时遵循“需求导向”原则，重点和优先开放的数据范围应当征求社会公众、行业组织、企业、行业主管部门的意见，满足公民、法人和其他组织开发利用公共数据的需求。

《办法》规定了鼓励、支持公民、法人和其他组织利用开放的公共数据开展科学研究、咨询服务、应用开发、创新创业等活动，明确利用合法获取的公共数据开发的数据产品和服务，可以按照规定进行交易，有关财产权益依法受保护。

---

<sup>3</sup> 网信办官网。

《办法》还规定，公共数据提供单位应当建立本单位公共数据安全保护制度，落实有关公共数据安全的法律、法规和国家标准以及网络安全等级保护制度，采取相应的技术措施和其他必要措施，保障公共数据安全。

同时，《办法》明确提出了，公民、法人和其他组织开发利用公共数据需采取必要的防护措施，保障公共数据安全等要求。<sup>4</sup>

《山东省公共数据开放办法》全文请参见：

[http://www.shandong.gov.cn/art/2022/2/9/art\\_107851\\_117339.html](http://www.shandong.gov.cn/art/2022/2/9/art_107851_117339.html)

## 5. 美国参议院通过《加强美国网络安全法》

2022年3月1日，美国参议院通过《加强美国网络安全法》（Strengthening American Cybersecurity Act）。

该法于2月8日提出，旨在加强美国的网络安全。在俄乌冲突升级背景下，美国参议院选择一致通过《加强美国网络安全法》。

该法由《网络事件报告法案》、《联邦信息安全现代化法案》和《联邦安全云改进和就业法案》三项网络安全法案构成。

《网络事件报告法案》更新了各机构向国会报告网络事件的规定，并赋予网络安全与基础设施安全局（CISA）更多权力，以确保其是民间网络安全事件主要负责机构。其中具体包括：

- （1）要求关键基础设施运营者在攻击事件发生后 72 小时内通知国土安全部；
- （2）在被支付勒索软件赎金后 24 小时内通知国土安全部。

---

<sup>4</sup> 网信办官网。

此外，《联邦信息安全现代化法案》还将国家网络安全主管等高级网络官员的职责写入法案，要求政府采取基于风险的网络安全方法。

总体来看，《加强美国网络安全法》包含旨在使美国联邦政府的网络安全态势现代化的若干措施，试图通过简化之前的网络安全法案来改善联邦机构之间的协调，并要求所有民间机构向 CISA 报告网络攻击事件。法案的通过将有助于确保银行、电网、供水网络和交通系统等关键基础设施实体能够在网络遭到破坏时迅速恢复并向人们提供基本服务。

目前，该法案还未签署成为法律，但现已提交美国众议院进一步审议。<sup>5</sup>

《加强美国网络安全法》(Strengthening American Cybersecurity Act) 全文请参见：

<https://www.congress.gov/bill/117th-congress/senate-bill/3600/text>

## 6. 英国和新加坡签署《数字经济协议》

2022 年 2 月 25 日，英国与新加坡签署了《数字经济协议》(UK-Singapore Digital Economy Agreement, DEA)，该协议将帮助两国企业抓住新的机遇，并促进两国间的跨境贸易。

英国国际贸易大臣 Anne-Marie Trevelyan 称，该数字经济协议发挥了英国作为服务业超级大国的优势，并将确保其优秀企业能够更好地从新冠疫情中恢复过来，更容易、更快、更可靠地进入利润丰厚的新加坡市场并从中受益。

当下，仅数字行业即为英国经济发展带来了 1510 亿英镑，数字行业人员的收入比英国其他行业从业人员的平均水平高出约 50%。

《数字经济协议》签署后，在新加坡运营的英国服务公司，包括金融巨头、电信公司和软件公司等，均将收益。此外，该协议还将减少货

---

<sup>5</sup> 安全内参。

物出口的繁杂程序，用电子签名和电子合同取代耗时和昂贵的文书工作。

《数字经济协议》具体包括以下几方面：

- (1) 搭建自由和可靠的数据跨境传输框架。
- (2) 确保两国间承诺具有约束力，以使得个人和企业了解到他们的数据、资金和知识产权是安全的。
- (3) 加强两国在金融服务方面的关系，确保数据自由流动，清除不合理的障碍，促进创新金融服务。
- (4) 建立新的伙伴关系，以建立更为强大的网络安全防御体系，防止私人运营商或敌对国家的攻击。

除了签署数字经济协议，两国还同意深化绿色经济方面的合作，并加强两国之间重要的双边投资关系。<sup>6</sup>

《数字经济协议（DEA）》全文请参见：

<https://www.gov.uk/government/publications/uk-singapore-digital-economy-agreement-agreement-in-principle-explainer/uk-singapore-digital-economy-agreement-agreement-in-principle-explainer>

---

<sup>6</sup> 安全内参。



# 监管动态



## 1. 工信部召开行政指导会规范 App 推荐下载行为及改善网页浏览服务体验

工业和信息化部信息通信管理局召开了行政指导会，针对有网友和媒体反映部分网站在用户浏览页面信息时，强制要求下载 App 的问题，督促相关互联网企业进行整改。

会议指出，随着移动互联网的快速发展，各类 App 蓬勃兴起，给用户提供了丰富的应用服务。但部分信息资讯、网络社区等网站在用户浏览网页时，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，妨碍用户使用网页浏览信息，侵害用户合法权益，群众反映强烈。

会议要求，相关互联网企业要坚持以人民为中心的发展思想，严格遵守相关法律法规要求，时刻把维护用户权益和改善服务体验作为赢得用户的根本，自查自纠、立行立改，坚决纠正存在的问题。在用户浏览页面内容时，一是未经用户同意或主动选择，不得自动或强制下载 App；推荐下载 App 时，应同步提供明显的“取消”选项，切实保障用户的知情权、选择权。二是无合理正当理由，不得要求用户不下载 App 就不给看，或者不让看全文。三是不得以折叠显示、主动弹窗、频繁提示、降低体验等方式强迫、误导用户下载、打开 App，或跳转至应用商店，影响用户正常浏览信息。

相关互联网企业表示，将认真落实有关要求，全面自查整改，依法合规经营，改进服务，提升用户体验，共同营造让群众放心满意的移动互联网应用环境。

工业和信息化部信息通信管理局将持续关注用户反映的问题，加强 App 监测检测，指导督促互联网企业切实维护好用户权益。<sup>7</sup>

---

<sup>7</sup> 工信部官网。

## 2. 工信部网络安全管理局召开全国会议指导推进车联网卡实名登记工作

2022年2月24日，为贯彻落实《中华人民共和国网络安全法》等相关法律法规要求，扎实推进车联网卡实名登记工作，工业和信息化部网络安全管理局组织召开车联网卡实名登记工作全国电视电话会议，深入解读车联网卡实名登记管理要求，指导道路机动车辆生产企业、电信企业规范开展车联网卡实名登记工作。

会议要求，各相关单位和企业要充分认识到车联网卡实名登记工作的基础性和重要性，增强法治意识和责任意识，健全管理制度和技术能力，加强工作协同，规范开展新用户实名登记，稳妥组织做好存量用户补登记；要制定详尽可行的工作方案，利用电话、短信、互联网等多种方式告知用户补登记要求，采用线上补登记、异地补登记等便捷方式方便用户办理，并加强政策宣传解释、用户投诉处理等服务保障工作。各级工业和信息化主管部门和省级通信管理局要加强指导监督，确保车联网卡实名登记要求落到实处，保障行业持续健康发展。

<sup>8</sup>

## 3. 北京市通管局就网络安全问题约谈两家互联网公司

2022年3月4日，按照有关工作安排，北京市通信管理局约谈了工信部通报的网络安全威胁问题突出的某两家互联网公司。

在深入了解这两家互联网公司的有关情况后，北京市通信管理局要求其要充分认识到做好网络安全工作的重要性和必要性，统筹好发展与安全的关系：

一是落实网络安全主体责任。要深入学习贯彻习近平网络强国战略思想，严格落实《网络安全法》《数据安全法》等法律法规，建立和

---

<sup>8</sup> 工信部官网。

完善网络安全制度体系，统筹企业内部资源，完善制度体系，把责任落实到岗，落实到人。

二是立即予以整改。对被通报的问题要深入分析原因，采取切实有效的措施，确保问题整改到位，并在规定时间内提交书面整改报告。

三是全面开展自查。要建立和完善相关工作机制和流程，按照《公共互联网网络安全威胁监测与处置办法》要求，建立健全网络安全防护工作机制和网络安全问题台账，对照通报问题举一反三、全面开展自查，切实做好网络安全威胁监测与处置，及时发现并消除各类安全隐患。<sup>9</sup>

#### 4. 美国就儿童隐私保护问题对某知名短视频 App 企业展开调查

近日，加州总检察长宣布对某知名短视频 App 企业关于儿童隐私保护问题进行调查。

加州总检察长对该企业向儿童和年轻人推广其社交媒体平台以及使用该平台所带来的潜在危害展开了调查。调查的重点是，该企业为提高用户参与度而采取的商业策略，以及该企业为了增加年轻用户在该平台上的花费时间而采取的措施。调查将确认年轻用户使用该企业的社交媒体平台造成的潜在危害，并评估该企业对上述危害的认识。

美国近年愈来愈关注社交媒体平台对儿童和青少年的负面影响。早在去年 11 月 Meta 公司的社交媒体平台 Instagram 就因被指控“剥削儿童而牟利”而遭到类似调查。此次各州将调查范围延伸至其他 App，体现了美国政府加大社交媒体平台管控力度的态度。<sup>10</sup>

---

<sup>9</sup> 北京市通管局官网。

<sup>10</sup> 安全内参。



## 5. 美国证交会拟要求上市公司信息安全事件应在 4 天内披露

2022 年 3 月 10 日，美国证券交易委员会（以下简称“SEC”）公布了一项新规定，以完善上市公司数据泄露事件披露机制，包括披露方式、披露时间等。

根据 SEC 提议，公司必须在报告文件（包括 8-K 表格）中详细说明何时遇到了风险，以及采取了怎样的策略来应对和管理风险。

此外，新规定还要求公司应对信息安全风险对公司财务状况的潜在的影响进行分析，并定期报告数据情况以帮助投资者了解已披露的重大信息安全事件的更多信息。

SEC 以 3: 1 的投票结果通过了这一项新规定。目前，这一项新规定正在公开征求意见。SEC 表示，这将帮助投资者更高效地评估信息安全风险，并为此做好准备。<sup>11</sup>

---

<sup>11</sup> 安全内参。

# 相关新闻



## 1. 工信部通报 14 款侵害用户权益 App(2022 年第 2 批, 总第 22 批)

工业和信息化部高度重视用户权益保护工作, 持续开展 App 侵害用户权益专项整治行动。“3·15”国际消费者权益日来临前夕, 为巩固治理成效, 营造共同维护消费者权益的良好环境, 工业和信息化部开展 App 侵害用户权益整治“回头看”, 组织第三方检测机构对前期用户反映问题较多的内存清理类、手机优化类 App 进行重点检测, 并对 2021 年发现问题的 App 进行抽测, 共发现 14 款 App 仍然存在问题。上述 App 应在 3 月 21 日前完成整改, 逾期不整改或整改不到位的, 工业和信息化部将依法依规严厉处置。<sup>12</sup>

相关 App 的名单请参见:

[https://www.miit.gov.cn/xwdt/gxdt/sjdt/art/2022/art\\_05240d52758845d0b9116dfd814b8d61.html](https://www.miit.gov.cn/xwdt/gxdt/sjdt/art/2022/art_05240d52758845d0b9116dfd814b8d61.html)

## 2. 最高检印发第三十五批指导性案例, 督促保护儿童个人信息权益

2022 年 3 月 7 日, 最高人民检察院下发《关于印发最高人民检察院第三十五批指导性案例的通知》(以下简称《通知》)。

《通知》称, 现将浙江省杭州市余杭区人民检察院对北京某公司侵犯儿童个人信息权益提起民事公益诉讼、北京市人民检察院督促保护儿童个人信息权益行政公益诉讼案等五件案例(检例第 141-145 号)作为第三十五批指导性案例(未成年人保护检察公益诉讼主题)发布, 供参照适用。

根据《通知》, 这些案件办理主要有以下几个特点: 一是体现最有利于未成年人原则。二是体现综合司法保护理念。三是体现主动融入“五大保护”理念。四是体现督导不替代的理念。五是体现标本兼治的理念。

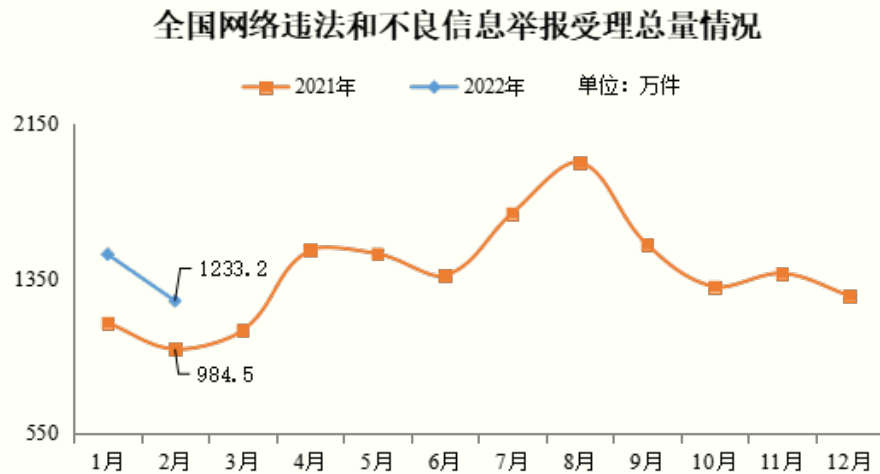
<sup>12</sup> 工信部官网。

其中，对检例第 141 号案件的办理，在未成年人保护公益诉讼案件线索发现，综合开展民事公益诉讼和行政公益诉讼促推未成年人网络保护，管辖权确定等方面具有较强指导意义。<sup>13</sup>

《关于印发最高人民法院第三十五批指导性案例的通知》全文请参见：

[https://www.spp.gov.cn/spp/jczdal/202203/t20220307\\_547759.shtml](https://www.spp.gov.cn/spp/jczdal/202203/t20220307_547759.shtml)

### 3. 2022 年 2 月全国受理网络违法和不良信息举报 1233.2 万件



2022 年 2 月，全国各级网络举报部门受理举报 1233.2 万件，环比下降 16.3%、同比增长 25.3%。其中，中央网信办（国家互联网信息办公室）违法和不良信息举报中心受理举报 31.7 万件，环比下降 13.1%、同比增长 68.2%；各地网信办举报部门受理举报 75.9 万件，环比下降 22.6%、同比下降 15.9%；全国主要网站受理举报 1125.5 万件，环比下降 16.0%、同比增长 28.6%。

在全国主要网站受理的举报中，主要商业网站受理量占 63.9%，达 718.7 万件。<sup>14</sup>

<sup>13</sup> 最高人民法院官网。

<sup>14</sup> 网信办官网。



#### 4. 浙江省 App 专项治理工作组通报 38 款违法违规收集使用个人信息 App

近期，针对群众反映强烈的 App 非法获取、超范围收集、过度索权等侵害个人信息的现象，浙江省 App 违法违规收集使用个人信息专项治理工作组依据《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》《App 违法违规收集使用个人信息行为认定方法》《常见类型移动互联网应用程序必要个人信息范围规定》等法律和有关规定，组织对实用工具类、网上购物类等常见类型且公众大量使用的 100 款 App 个人信息收集使用情况进行检测，并对存在问题的 App 进行点对点通报，责令违规 App 限期整改。

经复测核查，仍有 38 款 App 未能按要求整改，存在违法违规收集使用个人信息行为，浙江省 App 违法违规收集使用个人信息专项治理工作组对有关情况进行了通报。<sup>15</sup>

相关 App 的名单请参见：

[http://www.cac.gov.cn/2022-02/11/c\\_1646186253874039.htm](http://www.cac.gov.cn/2022-02/11/c_1646186253874039.htm)

#### 5. 上海市通管局发布关于通信网络安全防护管理情况的通报

根据《网络安全法》《通信网络安全防护管理办法》《公共互联网网络安全威胁监测与处置办法》等法律法规和《上海市通信管理局关于加强电信和互联网行业通信网络安全防护管理工作的通知》要求，上海市通管局定期对本市电信和互联网企业的通信网络安全防护管理情况进行督查审查，并对在上海市行政区域内提供通信网络安全评测、评估服务的网络安全专业机构及其信息通信领域安全服务资质予以备案登记。

---

<sup>15</sup> 网信办官网。

前期，上海市通管局公开通报了 44 家存在未落实通信网络安全防护管理要求等违规行为的单位，并责令其限期整改。经复测核查，尚有 10 家单位未按照要求落实整改。依据《网络安全法》《公共互联网网络安全威胁监测与处置办法》等法律法规要求，上海市通管局对上述 10 家单位的相关通信网络系统采取了停止互联网服务等措施。

具体名单请参见：

<https://mp.weixin.qq.com/s/Emd8Sb7q4NJE-PI-vn2kPg>

## 6. 意大利对 Clearview AI 罚款 2000 万欧元并令其删除数据

意大利数据保护机构对 Clearview AI 处以罚款 2000 万欧元，同时命令其删除其所持有的所有意大利人数据，并禁止其进一步处理公民的面部识别数据。据悉，该公司从互联网上搜集用户自拍，积累了约 100 亿张照片的数据库。

意大利数据保护机构称，该公司除了违反隐私法之外，还一直在追踪意大利公民和位于意大利的个人的动态。调查结果确认，该公司非法持有个人数据，包括生物识别和地理定位数据。

同时，该公司还违反欧洲《通用数据保护条例》（GDPR），例如透明度义务，因为该公司没有充分告知用户其对用户自拍所做的事情。因此，该公司的数据处理活动侵害了数据主体的权利，包括数据完整性和机密性，以及不被歧视的权利。

但该公司在发表的声明中称其在意大利或欧盟没有营业场所和任何客户，也没有从事任何违反 GDPR 的活动。它只从开放的互联网上收集公共数据，并遵守所有的隐私和法律标准。

英国信息专员办公室（ICO）早在 2021 年 11 月就警告 Clearview 可能会对其处以罚款，并命令 Clearview 停止处理数据。2021 年 12 月，法国数据保护委员会（CNIL）也命令 Clearview 停止处理其公民

的数据，并给它两个月的时间来删除它所持有的任何数据，但没有提到经济制裁。<sup>16</sup>

## 7. 美国对 **Weight Watchers** 处以 150 万美元罚款

2022 年 3 月 4 日，美国联邦贸易委员会（以下简称“FTC”）因儿童隐私问题对 **Weight Watchers** 处以 150 万美元罚款。

FTC 表示，**Weight Watchers** 及其面向年轻用户的 **Kurbo** 子公司被处以 150 万美元的罚款，因其非法收集儿童数据。**Weight Watchers** 和 **Kurbo** 推销一种允许 8 岁以上儿童使用的减肥应用程序，在未获得父母同意的情况下，非法收集了 18000 多名 13 岁以下儿童的个人数据。该应用跟踪儿童的食物摄入量、活动和体重，还收集其他个人信息，如姓名、电子邮件地址和出生日期。除了经济处罚外，**Weight Watchers** 和 **Kurbo** 还必须销毁以前所收集的儿童数据，以及从这些数据中得出的任何算法。

FTC《儿童在线隐私保护法》要求网站、应用程序和在线服务在收集、使用或披露 13 岁以下儿童的个人信息之前，必须通知父母并获得他们的同意。虽然 **Kurbo** 在注册过程中明文要求 13 岁以下儿童必须通过父母注册，但事实上，大量儿童用户在注册时可以谎称已超过 13 岁，并在个人资料上修改其出生日期以表明其实际是 13 岁以下，事后这些用户仍然可以继续使用该应用程序。

**Kurbo** 未能提供一种机制已确保那些选择父母注册选项的人确实是父母，且无限期保留儿童的个人信息，这显然违反了《儿童在线隐私保护法》。<sup>17</sup>

---

<sup>16</sup> 安全内参。

<sup>17</sup> 安全内参。

# 环球评论





## 1. 《工业和信息化领域数据安全管理办法（试行）（第二次征求意见稿）》要点解读

2021年6月10日，第十三届全国人大常委会第二十九次会议审议并通过了《中华人民共和国数据安全法》（以下简称“《数据安全法》”），并于2021年9月1日起施行。《数据安全法》作为数据安全领域的一部基础性、框架性法律，虽然对数据安全与数据利用并举问题进行了规定，但是很多内容较为原则和笼统，有待各行业、各地区和各部门进行细化与进一步规定。为贯彻落实《数据安全法》等法律法规，工业和信息化部（“工信部”）于2021年9月30日发布了《工业和信息化领域数据安全管理办法（试行）（征求意见稿）》（以下简称“《管理办法（一审稿）》”），向社会公开征求意见。该办法旨在加快推动工业和信息化领域数据安全管理工作制度化、规范化，提升相关行业的数据安全保护能力，防范数据安全风险。经过首次征求意见和内部修订后，工信部于2022年2月10日发布新版《工业和信息化领域数据安全管理办法（试行）（征求意见稿）》（以下简称“《管理办法（二审稿）》”），截至2月21日前再次向社会公开征求意见。

《数据安全法》从国家法律的层面，对于国家与数据活动实施者两个角色，规定了一系列提升数据安全治理和数据开发利用水平的原则、制度与措施，落实主体责任；以适应电子政务发展的需要，建立数据流通利用与安全管理的的要求。《管理办法（二审稿）》作为《数据安全法》的下位法，是对《数据安全法》中提出的“工业、电信、自然资源、卫生健康、教育、国防科技工业、金融业等行业主管部门承担本行业、本领域数据安全监管职责”的落实与贯彻。其目的是为了规范在我国境内开展的工业和信息化领域数据处理活动，加强数据安全管理工作，保障数据安全，促进数据开发利用，保护个人、组织的合法权益，维护国家安全和利益。

本文将通过结合《数据安全法》的要点，对作为下位法的《管理办法（二审稿）》如何进行支撑进行初步梳理，供相关企业参考。

### 一、明确监管与被监管的范围

#### （一）被监管的范围

##### 1. 适用范围

《数据安全法》的适用地域范围不仅包含境内，还将效力延伸至境外。即“在中华人民共和国境内开展数据处理活动及其安全监管”，以及“在中华人民共和国境外开展数据处理活动，损害中华人民共和国国家安全、公共利益或者公民、组织合法权益的”均适用该办法。

《管理办法（二审稿）》虽沿用了《数据安全法》关于中国境内处理数据活动的判断标准，规定“在中华人民共和国境内开展的工业和信息化领域数据处理活动及其安全监管”适用于此办法。但是《管理办法（二审稿）》并未明确将适用范围延伸至境外，没有采用《数据安全法》对在境外处理数据活动危害国家安全行为具有一定程度上管辖权的适用维度。

虽然《管理办法（二审稿）》对其他定义进行了厘清，但是仍未明确“境内开展”的概念，未来该法落地过程中可能存在判断标准不明、难以执法的问题。关于该概念的理解，在监管机关的配套文件出台之前，可以参考我们在《<数据安全法>正式出台，企业合规义务与红线，你了解吗？》一文中的解读。

## 2. 被监管的对象与主体

《数据安全法》下的适用对象——数据是指任何以电子或者其他方式对信息的记录；《管理办法（二审稿）》则结合工业、电信和无线电行业的特定场景，明确工业和信息化领域数据包括工业数据、电信数据和无线电数据，其中“无线电数据”系《管理办法（一审稿）》的基础上新增内容。在《管理办法（一审稿）》中，“工业数据”主要限定在原材料工业、装备工业、软件和信息技术服务业等行业领域；《管理办法（二审稿）》对“工业数据”的定义扩大至工业各行业各领域的生产运营等环节中产生和收集的数据。详细释义见表一。

	数据类型	数据处理者类型	数据定义
工业和信息化领域数据及处理者定义	工业数据	工业企业、软件和信息技术服务企业	工业各行业各领域在研发设计、生产制造、经营管理、运行维护、平台运营等过程中产生和收集的数据。
	电信数据	取得电信业务经营许可证的电信业务经营者	在电信业务经营活动中产生和收集的数据。
	无线电数据	无线电频率、台（站）使用单位	在开展无线电业务活动中产生和收集的无线电频率、台（站）等电波参数数据。

表一

此外,《数据安全法》的附则将国家秘密、统计和档案处理活动中涉及的数据、个人信息以及军事数据排除在适用对象范围以外,《管理办法(二审稿)》附则部分也沿袭了这一思路,并结合工业和信息化领域的行业特点,将以下几类利用数据行为排除在适用范围外:涉及军事、国家秘密信息和密码使用等数据处理活动、工业和信息化领域政务的数据处理活动以及国防科技工业、烟草领域的数据安全管理工作。国家秘密保护、密码、军事、政务、烟草领域的行业性或专业性较强,该等领域的数据处理活动应遵循国家另行出台的法律法规。另外,《管理办法(二审稿)》明确如开展涉及个人信息的数据处理活动,还应当遵守《中华人民共和国个人信息保护法》(以下简称“《个人信息保护法》”)等法律法规。

关于适用主体,《数据安全法》没有进行特别限制,仅使用“数据处理者”的概念。《管理办法(二审稿)》则将适用主体聚焦在“工业和信息化领域的数据处理者”,具体是指对工业和信息化领域数据进行收集、存储、使用、加工、传输、提供、公开等数据处理活动的工业企业、软件和信息技术服务企业、取得电信业务经营许可证的电信业务经营者和无线电频率、台(站)使用单位等工业和信息化领域各类主体。

## (二) 监管主体范围

《数据安全法》内核为国家安全观,呈现出从国家层面构建数据安全的顶层设计和国家与信息安全保障体系与防护能力,到深入不同行业、根据行业实际情况与发展战略制定适合于本行业的数据开发利用与安全保障并举的发展趋势。因此,《数据安全法》从框架上规定了工业、电信等主管部门承担本行业、本领域数据安全监管职责,而《管理办法(二审稿)》进一步细化了工业和信息化领域行业监管部门的职责范围,建立起权责一致的工作机制。

在此总体思路下,行业监管框架进一步分为国家与省二级体系。在全国层面上,由工信部负责督促指导地方工业和信息化主管部门、地方通信管理局和地方无线电管理机构开展数据安全监管,对工业和信息化领域数据处理者的数据处理活动和安全保护进行监督管理;在地方层面上,由省级工信主管部门、省级通信管理局以及省级无线电管理机构分别对本地区工业数据处理者、电信数据处理者以及无线电数据处理者的数据处理活动和安全保护进行监督管理(详见表二)。

监管层级	行业（领域） 监管部门	监管管理内容
国家层面	工信部	督促指导地方工业和信息化主管部门、地方通信管理局和地方无线电管理机构开展数据安全监管，对工业和信息化领域数据处理者的数据处理活动和安全保护进行监督管理
地方层面	省级工信主管部门	本地区工业数据处理者的数据处理活动和安全保护
	省级通信管理局	本地区电信数据处理者的数据处理活动和安全保护
	省级无线电管理机构	本地区无线电数据处理者的数据处理活动和安全保护

表二

## 二、细化数据分类分级标准及其管理制度

《数据安全法》初步构建了落实数据分类分级制度的体系；《管理办法（二审稿）》沿用了该立法思路并进一步明确工业和信息化领域的分类分级框架，同时指出工业和信息化领域数据处理者可在此基础上细分数据的类别和级别。根据《管理办法（二审稿）》第七条至第十条，数据分类主要是针对工业和信息化领域数据处理者所掌握的研发数据、生产运行数据、管理数据、运维数据、业务服务数据等进行的；数据分级也主要包括一般数据、重要数据和核心数据三级，并明确分级的判定标准为“数据遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者个人、组织合法权益等造成的危害程度”（具体分级详见表三）。虽然《管理办法（二审稿）》提出了比《数据安全法》更细致的分级判定条件，但上述条件中的“影响”“威胁”等如何具体定性仍然比较笼统，期待办法生效后监管机构能对如何落地实施进一步澄清。

数据级别	法律定义
一般数据	危害程度符合下列条件之一的数据为一般数据： （一）对公共利益或者个人、组织合法权益造成较小影响，社会负面影响小； （二）受影响的用户和企业数量较少、生产生活区域范围较小、持续时间较短，对企业经营、行业发展、技术进步和产业生态等影响较小； （三）其他未纳入重要数据、核心数据目录的数据。
重要数据	危害程度符合下列条件之一的数据为重要数据：



	<p>(一) 对政治、国土、军事、经济、文化、社会、科技、电磁、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、人工智能等与国家安全相关的重点领域；</p> <p>(二) 对工业和信息化领域发展、生产、运行和经济利益等造成严重影响；</p> <p>(三) 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；</p> <p>(四) 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；</p> <p>(五) 恢复数据或消除负面影响所需付出的代价大；</p> <p>(六) 经工业和信息化部评估确定的其他重要数据。</p>
核心数据	<p>危害程度符合下列条件之一的数据为核心数据：</p> <p>(一) 对政治、国土、军事、经济、文化、社会、科技、电磁、网络、生态、资源、核安全等构成严重威胁，严重影响海外利益、生物、太空、极地、深海、人工智能等与国家安全相关的重点领域；</p> <p>(二) 对工业和信息化领域及其重要骨干企业、关键信息基础设施、重要资源等造成重大影响；</p> <p>(三) 对工业生产运营、电信网络（含互联网）运行和服务、无线电业务开展等造成重大损害，导致大范围停工停产、大面积无线电业务中断、大规模网络与服务瘫痪、大量业务处理能力丧失等；</p> <p>(四) 经工业和信息化部评估确定的其他核心数据。</p>

表三

同时，根据《数据安全法》规定，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，各地区、各部门确定本地区、本部门以及相关行业、领域的重要数据具体目录，对列入目录的数据进行重点保护。为加强地区和行业管理，《管理办法（二审稿）》相应规定，在工信部组织和指导下，地方工业和信息化主管部门、通信管理局、无线电管理机构将制定本地区行业（领域）重要数据和核心数据具体目录并上报工信部。由此可见，未来工信部组织制定的目录也将成为所管辖企业开展分类分级工作的重要参考标准。

另外，国家信息安全标准化委员会于 2022 年 1 月 13 日公布的《信息安全技术 重要数据识别指南（征求意见稿）》划分了重要数据的定义范围，即重要数据是指“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”（详见表四）。该规定明确了以造成不利后果为判断重要数据的唯

一标准，与《管理办法（二审稿）》数据分级的判断标准相似。同时，《信息安全技术 重要数据识别指南（征求意见稿）》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，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或企业识别其自身掌握的重要数据提供参考和指引。详细分析可以参考我们在《<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》一文中的解读。

重要数据定义	重要数据识别因素
重要数据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，可能危害国家安全、公共利益的数据	<ul style="list-style-type: none"> <li>- 支撑<b>关键基础设施</b>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、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；</li> <li>- 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；</li> <li>- 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；</li> </ul>

表四

此外，《管理办法（二审稿）》还顺应着《数据安全法》关于构建数据分级分类管理制度的要求，提出了三点更细化的落地思路。即其一，工业和信息化领域数据处理者应当定期梳理数据，按照《信息安全技术 重要数据识别指南（征求意见稿）》等相关标准规范识别重要数据和核心数据并形成目录。其二，企业应根据自身性质，将重要数据和核心数据目录向对应的地方工业和信息化主管部门（工业领域）或通信管理局（电信领域）或无线电管理机构（无线电领域）进行备案。其三，企业应对各类数据按照一般数据、重要数据和国家核心数据三个等级的不同要求实行分级防护，对于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“就高不就低”。换言之，当不同类别的数据在评估其危害对象时，不同对象可能遭受到的危害程度各有不同时，以所有适用的保护对象中受危害程度最深（暨需要保护级别最高）的那一类为最后定级的标准。

### 三、明确数据全生命周期安全管理制度

#### （一）细化数据处理者职责

《数据安全法》原则性地规定了开展数据处理活动应建立健全数据安全管理制度，履行相应的数据安全保护义务；《管理办法（二审稿）》进一步规定了数据处理者的主体责任，并针对不同级别数据，从数据收集、存储、使用、加工、传输、提供、公开等全生命周期环节提出分级保护要求。如《数据安全法》仅就数据收集进行规定，“任何组织、个人收集数据，应当采取合法、正当的方式，不得窃取或者以其他非法方式获取数据”。《管理办法（二审稿）》第十四条在此基础上，进一步明确企业应当采取的管理措施和记录内容，并就间接途径获取重要数据和国家核心数据的情形对数据提供方提出签署相关协议、承诺书等要求。此外，除了数据采集环节，《管理办法（二审稿）》还就数据的存储、使用加工、传输、提供、公开、销毁、出境以及转移等环节进行了详细规定，并明确该等环节中涉及重要数据与核心数据时的特殊要求（详见表五），为相关企业履行数据安全保护义务提供了具体的合规指引。

	一般数据	重要数据	核心数据
数据收集	收集数据应当遵循合法、正当的原则，不得窃取或者以其他非法方式收集数据。数据收集过程中，应当根据数据安全级别采取相应的安全措施，加强重要数据和核心数据收集人员、设备的管理，并对数据收集的时间、类型、数量、频度、流向等进行记录。	通过间接途径获取重要数据和核心数据的，工业和信息化领域数据提供者应当与数据提供方通过签署相关协议、承诺书等方式，明确双方法律责任。	
数据存储	应当依据法律规定或者与用户约定的方式和期限存储数据。	采用 <b>校验技术、密码技术</b> 等措施进行安全存储。不得直接提供存储系统的公共信息网络访问，并实施数据容灾备份和存储介质安全管理，定期开展数据恢复测试。	除了采取与重要数据同等的保护措施外，还应当实施 <b>异地容灾备份</b> 。
数据使用加工	利用数据进行自动化决策分析的，应当保证决策的透明度和结果公平合理。	<b>加强访问控制</b> 。	
数据传输	应当根据传输的数据类型、级别和应用场景，制定安全策略并采取保护措施。	采取 <b>校验技术、密码技术、安全传输通道</b> 或者 <b>安全传输协议</b> 等措施。	
数据提供	应当明确数据提供的范围、类别、条件、程序等，并与数据获取方签订数据安全协议。	应当对数据获取方 <b>数据安全保护能力</b> 进行评估或核实，采取必要的安全保护措施。	
数据公开	应当在数据公开前分析研判可能对公共利益、国家安全产生的影响，存在重大影响的不得公开。	/	
数据销毁	应当建立数据销毁制度，明确销毁对象、规则、流程和技术等要求，对销毁活动进行记录和留存。个人、组织依据法律规定、合同约定等请求销毁的，应当销毁相应数据。	及时 <b>更新备案</b> ，不得以任何理由、任何方式对销毁数据进行恢复。	
数据出境	/	在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 <b>数据出境安全评估</b> 。非经工信部批准，不得向外国工业、电信、无线电执法机构提供存储于境内的工业和信息化领域数据。	
数据转移	因兼并、重组、破产等原因需要转移数据的，应当明确数据转移方案，并通过电话、短信、邮件、公告等方式通知受影响用户。	应当及时 <b>更新备案</b> 。	
委托处理	应当通过签订合同协议等方式，明确委托方与被委托方的数据安全责任和义务。	对被委托方的数据安全保护能力、资质进行评估或核实。	

表五

其中，需要重点关注以下几方面：

## 1. 数据出境

《中华人民共和国网络安全法》（以下简称“《网络安全法》”）第三十七条规定，关键信息基础设施的运营者在境内运营中收集和产生的重要数据应当在境内存储。确需向境外提供的，应当进行安全评估。《数据安全法》沿用了《网络安全法》的这一规定，并明确其他数据处理者所收集的重要数据的出境适用国家网信部门会同国务院有关



部门制定的管理办法。《管理办法（二审稿）》在沿用《网络安全法》《数据安全法》的基础上，对“核心数据”提出了相同要求，即工业和信息化领域数据处理者应对在境内收集和产生的重要数据和核心数据进行本地化存储，确需向境外提供的，应当依法依规进行数据出境安全评估。与《管理办法（一审稿）》“核心数据一律不得出境”的规定相比，本次修订为核心数据的出境保留了可能。对于一般数据出境的规则，则应先判断其数据类型。如果属于个人信息的，适用《个人信息保护法》对于个人信息的出境思路，即针对非属于关键信息基础设施运营者和处理个人信息未达到国家网信部门规定数量的个人信息处理者，在没有特殊行业约束信息必须本地化外，一般根据《个人信息保护法》要求数据处理者实施了相关出境合规措施后，可以出境。如果属于关键信息基础设施运营者和处理个人信息达到国家网信部门规定数量的个人信息处理者，原则上需要将在中华人民共和国境内收集和产生的个人信息存储在境内。确需向境外提供的，应当通过国家网信部门组织的安全评估后即可出境（但法律、行政法规和国家网信部门规定可以不进行安全评估的，从其规定）。对于不属于个人信息的一般数据，则需要进一步评估相关部门规章是否对出境有限制性要求，如果没有，还要看是否落入到出口管制的负面清单范围，如果没有，则可以出境。

## 2. 数据删除

《管理办法（二审稿）》要求针对不同级别数据，从包括销毁等环节落实分级保护要求，同时建立数据销毁制度。有关数据销毁的要求并不是《管理办法（二审稿）》第一次提出，如国家标准《信息安全技术 个人信息安全规范》（GB/T 35273—2020）中亦有提出。销毁是数据全生命周期的最后一环也因此形成了闭环，是一种物理删除。数据一经销毁后则无法再复原。《管理办法（二审稿）》对核心数据与重要数据的销毁处理尤其关注，我们理解这是因为该部分数据如果处理不当会对国家安全与社会稳定造成特别重大的影响。因此，如果基于法律规定、实际需求或合同约定，这些数据不再有保留需要，必须永久且不可恢复地删除的，该数据处理者就需要采取销毁数据的手段，以免留下安全隐患。但具体实践中，对于销毁工具的审核、流程及实施人员的处理规则、以及销毁后的审计与报备措施，可能会遇到实践中的挑战。

## 3. 安全风险评估



《管理办法（二审稿）》在《管理办法（一审稿）》的基础上，新增了关于安全风险评估和日志存留期限的规定。如果工业和信息化领域数据处理者跨主体提供、转移、委托处理核心数据的，应当评估安全风险，采取必要的安全保护措施，并经相应领域的主管部门报工信部后，由工信部按照有关规定进行审查。

#### 4. 明确留存处理日志的最低期限

工业和信息化领域数据处理者应当在数据全生命周期处理过程中，记录数据处理、权限管理、人员操作等日志，且日志留存时间不少于六个月。这与《网络安全法》的要求也是衔接和相称的。

##### （二）增加负责人管理义务

《数据安全法》规定重要数据的处理者应当明确数据安全负责人和管理机构，落实数据安全保护责任。虽然《数据安全法》规定了单位与直接负责的主管人员都可能会受到处罚。但在实践中，企业内部参与项目的部门众多，谁为主要责任人的厘清仍然存在困惑。较为清楚地明确工业和信息化领域数据处理者应配备数据安全管理人员，统筹负责数据处理活动的安全监督管理。对于涉及重要数据和核心数据的工业和信息化领域数据处理者，应当建立覆盖本单位相关部门的数据安全工作体系，明确数据安全负责人和管理机构，本单位法定代表人或者主要负责人是数据安全第一责任人，领导团队中分管数据安全的成员是直接责任人。针对很多企业困惑究竟哪些人可能成为《数据安全法》下的直接责任人，《管理办法（二审稿）》第一次提出了如此清晰的界定。同时，明确要求关键岗位人员签署数据安全责任书。由此可见，一旦《工业和信息化领域数据安全管理办法》依照二审稿的状态生效试行，涉及重要数据和核心数据的企业需要进一步明确企业内部相关部门和岗位的设置要求，并按照上述要求落地实施。

#### 四、构建对重要数据和核心数据的目录备案制度和登记审批机制

《数据安全法》未就备案制度进行规定，《管理办法（一审稿）》首次提出备案的概念，《管理办法（二审稿）》在其基础上进一步明确目录备案制度，并新增了数据类别、级别等备案要求。构建该制度的原因在于工业和信息化领域的数据多与经济运行相关，属于国家重点监管的数据类型之一，加强监管部门对相关企业的管控，有利于保障国家经济安全与发展。因此，作为监管对象的工业和信息化领域数据处理者应当按照有关要求进行了目录备案，备案内容应当包括但不限于数据类别、级别、规模、处理目的和方式、使用范围、责任主体、对

外共享、跨境传输、安全保护措施等基本情况，不包括具体数据本身。同时，《管理办法（二审稿）》新增了主管部门的审核期限，即各领域主管部门应当在工业和信息化领域数据处理者提交备案申请的二十个工作日内完成审核工作，备案内容符合要求的，予以备案并发放备案凭证，同时将备案情况报工信部；不予备案的应当及时将决定反馈备案申请人并说明理由。另外，关于备案内容，《管理办法（一审稿）》仅笼统规定备案内容发生变化的，应在三个月内报备变更情况，同时对整体备案情况进行更新，没有进一步指出哪些“备案内容”变化需要更新，接收报备的部门，以及进行备案情况更新的责任主体。而《管理办法（二审稿）》明确了变化时需进行更新的“备案内容”，即对重要数据、核心数据的变化和其他内容的变化进行区分，并细化了“变化”的判断标准，即重要数据和核心数据的类别或规模变化达到 30% 以上，或者其它备案内容发生重大变化的，工业和信息化领域数据处理者应当在上述发生变化之日起三个月内履行备案变更手续。同时，《管理办法（二审稿）》也要求工业和信息化领域数据处理者当其重要数据和核心数据处理环节发生变化时提交更新备案，例如销毁重要数据和核心数据的，或因兼并、重组、破产等原因需要转移重要数据和核心数据的，均应当及时更新备案。

此外，《管理办法（一审稿）》仅规定在使用、加工这一环节对重要数据和核心数据建立登记、审批机制并留存记录。而《管理办法（二审稿）》删除了这一限定范围，意味着工业和信息化领域数据处理者应在重要数据和核心数据的处理活动全生命周期内建立内部登记、审批机制，对重要数据和核心数据的处理活动进行严格管理并留存记录。

## 五、强化安全评估、监测预警与应急管理义务

《管理办法（二审稿）》第四章至第六章明确了工业和信息化领域数据处理者应承担开展安全评估、加强监测预警与应急管理、协助监督检查以及配合安全审查的义务。

### （一）开展安全评估的义务

《数据安全法》第三十条规定了重要数据处理者定期开展风险评估并向主管部门报送评估报告的义务；《管理办法（二审稿）》第三十一条细化了安全评估规则，即工业和信息化领域重要数据和核心数据处理者应当自行或委托第三方评估机构，每年至少开展一次安全评估，及时整改风险问题，并向相应领域的主管部门报送评估报告。关于评估的具体实施以及评估机构的管理标准，仍然没有特别具体，有待监管部门未来进一步出台机构管理制度、评估规范或实施细则等文件。

## （二）加强监测预警与应急管理的义务

根据《数据安全法》第二十九条的规定，开展数据活动应当加强风险监测，在发现数据安全缺陷、漏洞等风险时，应当立即采取处置措施；发生数据安全事件时，应当按照规定及时告知用户并向有关主管部门报告。根据该规定，企业在发生数据安全事件时应负有报告义务，但该条未明确“数据安全事件”的概念以及上报的时间限制（详细分析见《<数据安全法>正式出台，企业合规义务与红线，你了解吗？》一文）。《管理办法（二审稿）》第二十六条承接《数据安全法》的上述要求，明确了工业和信息化领域数据处理器具有风险监测义务，并且根据第二十七条要求，将防控风险的义务提前，规定工业和信息化领域数据处理器应及时将可能造成较大及以上安全事件的风险向相应领域主管部门报告。与《数据安全法》相比，这一规定增加了相关企业在发生数据安全缺陷、漏洞等风险并且可能造成安全事件时的报告义务。此外，为规范网络产品安全漏洞发现、报告、修补和发布等行为，《网络产品安全漏洞管理规定》提出了网络产品提供者、网络运营者以及从事网络产品安全漏洞发现、收集、发布等活动的组织或者个人在发生网络漏洞时的相应义务。其中，网络产品提供者应履行网络产品安全漏洞管理义务，确保其产品安全漏洞得到及时修补和合理发布，网络运营者发现或者获知其网络、信息系统及其设备存在安全漏洞后，应当立即采取措施，及时对安全漏洞进行验证并完成修补。

另外，《管理办法（二审稿）》第二十八条进一步细化了相关企业的应急处置义务，即工业和信息化领域数据处理器在数据安全事件发生后，应当按照应急预案，及时开展应急处置，涉及重要数据和核心数据的安全事件，应当第一时间向相应领域主管部门报告，并要求相关企业每年向主管部门提交数据安全事件处置情况的总结报告。但是，“第一时间”在实践中如何界定仍是问题。此外，对于可能损害用户合法权益的数据安全事件，《管理办法（二审稿）》还要求企业应当及时告知用户，并提供减轻危害措施。该规定与《个人信息保护法》第五十七条规定的“发生或者可能发生个人信息泄露、篡改、丢失的，个人信息处理者应当立即采取补救措施，并通知履行个人信息保护职责的部门和个人”相衔接。但是，“及时”与“第一时间”的区别，法律也未作明确的规定。如何在实践中对二者进行更好的分辨，可能也需要进一步观察监管机构的执法案例。

## （三）协助监督检查的义务



为加强监管部门对企业重要数据和核心数据报送和备案制度落实情况的监督力度,《管理办法(二审稿)》第三十二条规定,行业监管部门有权对工业和信息化领域数据处理者落实该办法的情况进行监督检查,工业和信息化领域数据处理者应当配合行业(领域)监管部门开展监督检查。

#### (四) 配合安全审查的义务

根据《数据安全法》第二十四条,对影响或者可能影响国家安全的数据处理活动应进行国家安全审查。《管理办法(二审稿)》沿袭《数据安全法》关于安全审查的思路,明确工信部应在国家数据安全工作协调机制指导下,开展数据安全审查相关工作。另外,根据2022年2月15日生效的《网络安全审查办法》,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。审查重点分为两类,一类是核心数据、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,一类是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,以及网络信息安全风险。

因此,如果工业和信息化领域数据处理者的数据处理活动影响或可能影响国家安全的,则相关企业可能需要同时接受工信部和网信办的安全审查。

## 六、建立投诉举报机制

《数据安全法》第十二条赋予了个人、组织向关主管部门投诉、举报的权利。《管理办法(一审稿)》细化了企业的答复方式和时限,即应当建立用户投诉处理机制,公布电子邮件、电话、传真、在线客服等联系方式,配备受理人员接收投诉,并于15个工作日内答复。但是在《管理办法(二审稿)》中,仅保留“鼓励工业和信息化领域数据处理者建立用户投诉处理机制”的表述,删除了关于答复方式和时限的规定。我们认为,关于投诉举报机制的详细规定,多出现于个人信息保护领域的《App违法违规收集使用个人信息行为认定方法》《网络安全标准实践指南—移动互联网应用程序(App)收集使用个人信息自评估指南》等文件中。在非个人信息的领域中,投诉举报机制的建立难以一蹴而就,仍需在逐步提高企业合规意识的同时循序渐进、缓步推行。

## 结语



《管理办法（二审稿）》作为工业、电信和无线电行业的部门规章，厘清了“工业数据”、“电信数据”、“无线电数据”、“工业和信息化领域数据处理者”的基本概念，明确了界定不同级别数据（一般数据、重要数据、核心数据）的判定条件，构建了“中央部委-地方-企业”三级联动的数据分类分级、数据分级防护工作机制，和数据全生命周期管理制度等基本制度体系，规范了各参与主体的职责与权力，为监管机关的执法活动和企业的合规体系建设提供了重要指引。我们建议在中国境内开展工业和信息化领域数据处理活动的企业在该办法生效之前，尽可能按照《管理办法（二审稿）》的要求事先梳理本企业所涉数据及处理活动，重点对可能涉及的重要数据、核心数据，提前规划实施办法提出的各项合规要求。一旦办法正式出台并生效，则可以做到成竹在胸，从容应对。<sup>18</sup>

---

<sup>18</sup> 作者：孟洁、张淑怡、李楠，<https://mp.weixin.qq.com/s/gRAeJ7RdXUWCdAjdDcNzpA>。



环球律师事务所  
GLOBAL LAW OFFICE

2022 年 第二期 / 总第三十六期

## 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](mailto: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。