环球律师事务所
GLOBAL LAW OFFICE

致礼2022 成熟的数据合规年

——监管动态总结与趋势预判

A Tribute to 2022, Year of Maturity for Data Compliance: Regulatory Activity Summary and Trend Forecast

环球律师事务所数据合规团队编制

2022年1月5日

www.glo.com.cn
中国首家律师事务所
The First Chinese Law Firm

序言
Foreword

2021年，我们

见证了《**数据安全法**》和《**个人信息保护法**》两部数据领域核心法律的出台，与《**网络安全法**》并驾齐驱；

见证了监管机构**配套政策**有条不紊地推陈出新，也为产业界将数据运用在各行业各领域的高速发展**把住了方向盘**；

见证了全国信息安全标准化技术委员会发布的**各项国家标准**并不断成熟丰富，给企业提供了更有**操作性**的合规指引；

见证了用户**个人信息保护意识**的显著提升，隐私保护理念渐入人心；

也见证了企业对数据合规监管要求与落地思路的逐渐熟悉、适应和重视，对数据合规工作有了更细致、更深入的**了解**，也产生了更迫切的**需求**。

从2021走向2022，我们一起见证**数据合规年**。

本报告包括年终盘点、趋势预测和附录三部分。从立法、执法以及落地实施三方面梳理了2021年企业数据治理的监管要求与合规重点，并放眼未来，预测包括数据出境安全审查、平台治理、重要数据识别等2022年规制的关键内容，以期为产业界数据合规实践提供参考思路与方法。

目录

Part 01

2021 年终盘点

1. 三大法律框架建立与完善
2. 法律法规层级效力呈体系
3. 顶层设计：从内部机构设置到制度体系构建
4. App合规朝定期性检测方向深入、广泛发展
5. 企业数据资产地图与全生命周期数据梳理成效初显
6. 从客户端产品合规向与后台安全合规并重思路看齐
7. 数据分类分级管理与访问权限设置已成关注重点
8. 风险评估思路已逐步被接受，PIA工具从陌生到被熟练操作
9. 网络安全等级保护不再流于形式，安全测试与认证受到热捧
10. 人脸识别规制手段：行政监管与司法解释、判例双管齐下
11. 个人主体权利实现机制在产品侧落地卓有成效
12. 个别行业数据治理成为重点监管方向，如汽车行业
13. 网络安全审查：从关键信息基础设施运营者到网络平台运营者，并以拟国外上市企业为审查重点
14. 算法透明性要求被提出，推荐性算法备案开始尝试

Part 02

2022 趋势预测

1. 重要数据识别标准与清单逐步确立
2. 数据出境安全审查与报批流程完善
3. 关键信息基础设施认定边界更加明确
4. 平台治理：从数据汇聚到反垄断规制
5. 内部审计与外部审计相结合配置更加完备
6. 集团数据共享与向第三方提供数据规则与机制健全
7. 特殊行业数据处理要求更加细化，各行业主管部门规则更加清晰、科学
8. 年度报告报送与备案流程更加成熟
9. 网络安全审查标准与流程更具可操作性
10. 企业算法管理和可解释能力不断提升
11. 运用司法诉讼比例将大幅上升
12. 外部独立第三方监督作用逐渐发挥
13. 企业内部数据合规人才储备需求量翻番
14. 跨境传输标准合同条款即将出台，可携带权行使规则将进一步明确
15. “单独同意”的难点问题有望突破
16. 有望针对儿童监护人身份认证机制提出新的有效解决思路
17. 新技术新应用领域（如NFT、区块链等）提出数据合规新问题
18. 数据作为反制措施之一，需要各方权力动态平衡与力量把控
19. 除保护用户个人信息，将保护员工、合作伙伴联系人信息排上日程

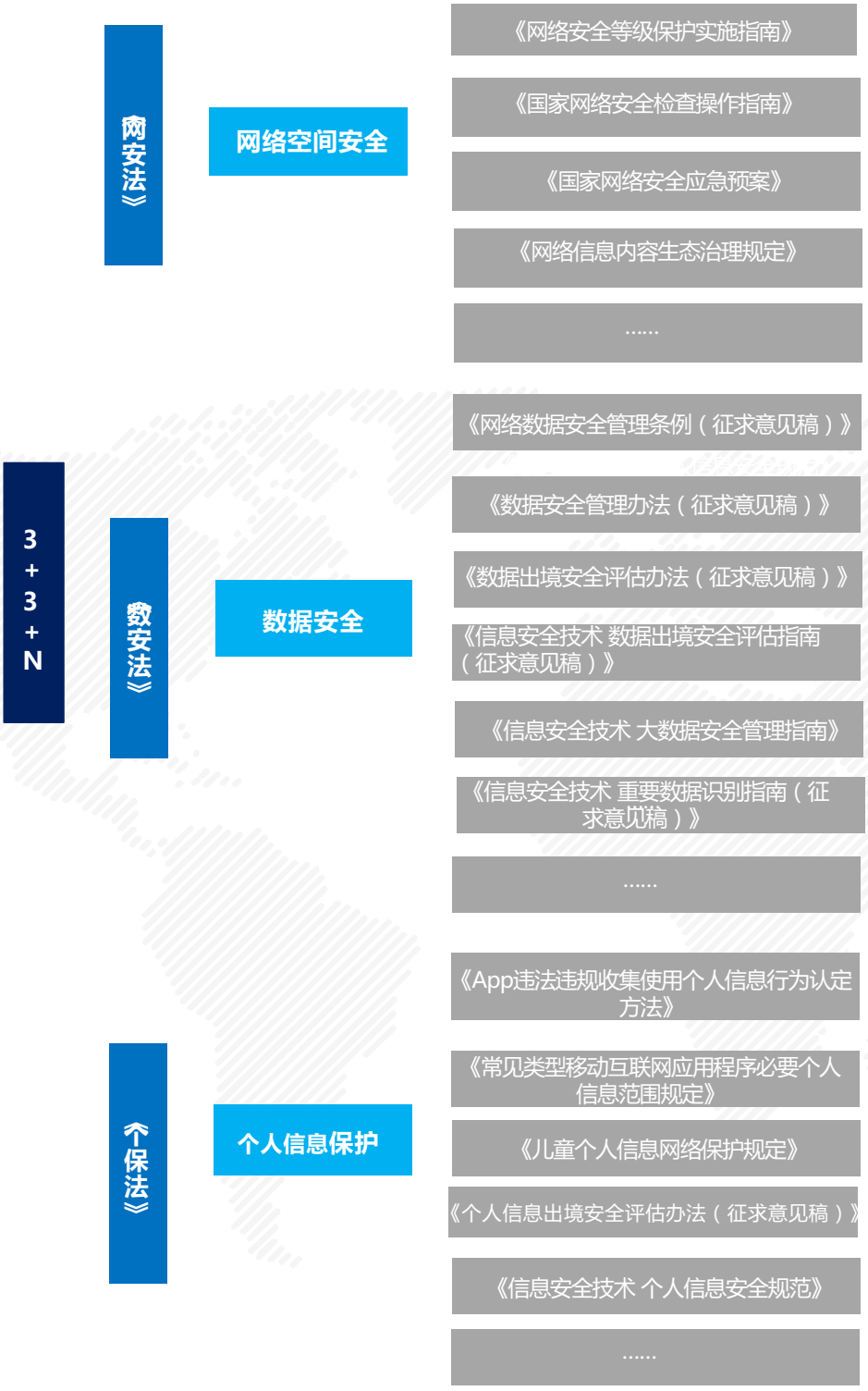

Part
01
2021
年终盘点

1.1 三大法律框架建立与完善

如果说2017年《中华人民共和国网络安全法》（以下简称“《网安法》”）的正式实施开启了“中国数据合规元年”，那么2021年无疑是中国数据合规及隐私保护领域历史上的又一座里程碑—中国正式迎来个人信息保护以及数据安全领域的两部专属立法，即《中华人民共和国个人信息保护法》（以下简称“《个保法》”）与《中华人民共和国数据安全法》（以下简称“《数安法》”）。这两部法律与《网安法》共同构建了中国数据合规及隐私保护的基础法律框架，对网络安全、数据安全和个人信息保护提出了方向性和基础性指引及监管要求。

随着两部新上位法的出台和正式实施，横向层面，各立法部门、监管机构的实施要求也不断出台；纵向方面，各垂分行业、领域的规定不断推陈出新，数据全生命周期各环节的规范要求与以往相比，也往更加细致的程度发展。此外，多部具有落地性指导意义的法规及国家标准，正在积极向公众征求意见并有望短期内发布。2022年1月4日，新年伊始，《网络安全审查办法》正式稿公布，将于2022年2月15日起施行。这些，从一定程度均昭示着数据合规及隐私保护领域的立法正逐步建立内在逻辑，并呈现出监管要求越来越明晰，且能够有效指导落地实践的状态和趋势。

1.2 法律法规层级效力呈体系



中国数据合规法律规范体系主要可以概括为“3+3+N”的格局。

首先，《网安法》《个保法》《数安法》这“3”部法律是我国数据合规法律规范体系的基石，奠定了国家对数据合规领域监管的总基调，把控着监管与执法趋势的大方向，是建立中国特色数据合规法律体系框架的底盘。

其次，从数据合规的重点治理域来看，大致又可以分为“3”部分：“网络空间安全”、”个人信息保护”、以及“数据安全”。从近年来出台的法律、法规、规范性文件、司法解释及国家标准等内容及核心思想来看，不难发现这三大领域其实是我国在数据合规治理域中立法、执法、司法的主要关注点，各项法律规范的出台、监管态势的收紧以及国家政策指引的着眼点和着力点大多围绕这三大治理域。

格局中的第三层—“N”即代表了我国在“网络空间安全”、“数据安全”，以及“个人信息保护”治理域下逐步推出，以完善不同维度的治理内容，丰富并提升治理水平。

1.3 顶层设计：从内部机构设置到制度体系构建

组织与负责人设置

个人信息保护负责人
网络安全等级保护工作责任人
网络安全管理负责人
数据安全责任人（若以经营为目的收集重要数据）
专门安全管理机构负责人（适用CIIO）

数据资产盘点+合法获取数据的前提论证

数据全生命周期合规要求
数据合法性基础梳理、论证
数据识别
数据流转

外部政策声明设计

国内与海外
单独与统一

内部制度流程设计

内部管理制度和操作规程
违规操作的内部惩戒机制

用户权利行使机制

隐私保护设计方案/ 同意机制设计方案
个人行权响应与行权机制
投诉/举报/反馈通道

与第三方合作设计

委托合同中的数据保护条款
专门的数据处理协议
采购网络产品和服务网络安全审查
第三方供应商背景审查与服务监测

数据安全管控及保障

数据分类分级管理
采取加密、去标识化等安全技术措施
合理确定操作权限
保存期限为实现处理目的所必要的最短时间或法定保存时限
定期开展渗透性测试与攻防演练

企业自评估

个人信息保护影响评估
重要数据处理活动风险评估
数据出境风险自评估
赴境外上市的数据处理者对数据安全自评估
赴国外上市的关基运营者对采购活动及互联网平台运营者对安全性及掌握个人信息数据量自评估

审计、记录与应急

定期审计
文档记录与存储
制定和实施应急预案
（可能）发生数据泄露，补救措施和通知报告义务（区分可以不通知的情形 & 依职权要求通知的情形）

培训、对外展示与能力提升

定期进行安全教育和培训
定期进行应急演练
对外合规能力展示

1.4 App合规朝定期性检测方向深入、广泛发展

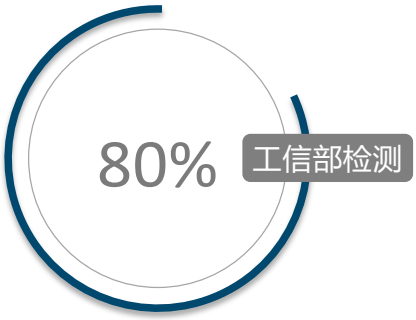
App个人信息保护专项治理行动

国家互联网信息办公室（以下简称“网信办”）等四部门联合印发的《常见类型移动互联网应用程序必要个人信息范围规定》于2021年5月1日起正式实施，明确39类常见App收集和使用必要个人信息的范围，成为监管部门判断App是否超范围收集个人信息的重要依据。此外，监管机构针对执法也进一步拓宽：工信部在10月首次对数款SDK进行了通报，监管工作更加细致具体；天津市网信办在专项治理行动中通报4款小程序，海南地方网信办则进一步对11款小程序和多家应用平台作出通报，将监管视角投向了更广的范畴。

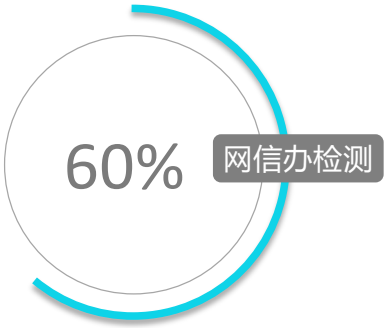
企业需定期对App等产品进行自测

App被通报后无法在规定期限内完成整改的，将被下架处理，这将会对企业的业务造成严重影响。因此，众多企业已经开始定期对旗下的App/小程序/SDK在合规和技术双重层面进行自检，提前排除问题，以避免因通报对品牌带来的负面效应，和被监管机构通报后因整改时间不足被迫下架而对业务带来冲击。

企业对App的自检将朝向定期化、深入化发展。一方面，不同时期，监管部门治理工作的重点不同，随着新法新规和技术标准的出台落地，针对移动应用程序的合规要求不断提高；另一方面，第三方SDK的行为可能不完全受宿主App控制，会出现嵌入后未经用户同意隐蔽或超范围收集个人信息及其他恶意行为，企业也需要定期对SDK的合规情况进行监督和审查。定期对App/小程序/SDK进行自检尤为必要。



工信部2021年1680款被通报的App中，超过80%的App均有违规收集个人信息的情况。



网信办2021年695款被通报的App中，有超过60%的App有超范围收集个人信息的情况。

2021年国家网信部门通报的App类别有三方面特点：受众广泛（如新闻、视频直播类）、涉及个人信息或敏感个人信息（如求职、健康、金融类）、基础功能类App和使用关键权限的App（如应用平台类）较多；而同时具有上述多项特点的App类别被优先审查（输入法、地图导航、系统管理类）。随着专项行动的进一步开展，更多App的类别将会逐一被纳入审查范畴，但可以预期的是，包含上述特点的App类别被审查的可能性更高。

如果您希望对监管部门2021年度的执法情况有更全面、更可视的了解，请参考本报告附录“2021监管与执法动态汇总”。

1.5 企业数据资产地图与全生命周期数据梳理成效初显

数据全生命周期覆盖数据收集、存储、使用、加工、传输、提供、公开、删除等环节。

1

此前，国内企业对数据全生命周期合规概念处于探索和适应阶段。

2

工信部于2021年发布了《网络安全产业高质量发展三年行动计划（征求意见稿）》。

3

中国多家科技企业升级了用户数据保护系统，对数据施行全生命周期的保护。

4

央行通过《金融数据安全 数据生命周期安全规范》建立了覆盖数据全生命周期的安全防护体系。

5

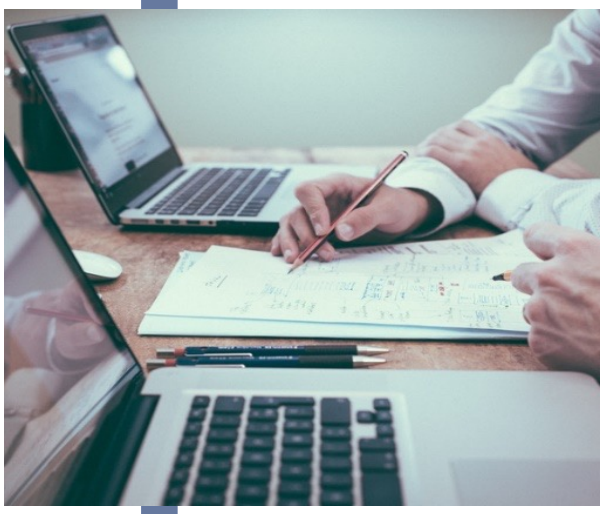
在《金融数据安全 数据生命周期安全规范》中，数据全生命周期中需要遵循的数据合规原则包括合法正当原则、目的明确原则、选择同意原则、最小够用原则、全程可控原则、动态控制原则、权责一致原则。

企业数据生命周期的每一环节都必须以掌握数据资产分布情况为前提条件。为实现这一点，企业需要首先对现有数据资产进行梳理，形成企业内部统一的数据资产地图，构建基于元数据的安全保护框架，帮助企业识别收集了哪些数据、数据存储在哪里、谁可以使用以及如何作用、提供给了哪些第三方，进而对数据情况的变动持续监测，并进行有针对性的治理。在该过程中，元数据的相关属性也需要进一步被识别，包括其是否构成《数安法》下的国家核心数据、重要数据、一般数据，以及《个保法》下的个人信息及敏感个人信息，从而明确该数据是否对应了特定的合规要求。

1.6 从客户端产品合规向与后台安全合规并重思路看齐

建立健全数据安全治理体系 提高数据安全保障能力

以客户端产品合规为基础，监管对数据处理者的后端数据治理层面提出了更高要求，如建立健全数据分类分级体系、完善重要数据保护制度和措施、建立数据安全审计和应急响应机制，以及数据安全技术防护能力等。



监管动态及要求

2021年7月26日，工信部启动互联网行业专项整治行动。与以往监管仅集中在产品客户端层面的专项整治行动不同，本次监管将检查范围延伸至**数据安全管理制度和安全技术措施落地**方面，从制定数据全生命周期安全保护制度、采取数据分类、重要数据备份措施、对用户敏感数据进行加密存储、采取访问和权限控制措施等方面，对企业提出治理要求。

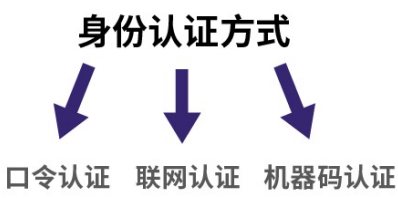
1.7 数据分类分级管理与访问权限设置已成关注重点

数据分类分级管理

《数安法》提出“国家建立数据分类分级保护制度”，确定了数据分类分级是数据安全的基本制度。实行数据分类分级是保障数据安全的前提，也是业界落地数据合规要求和数据治理的重要基础工作。各部门、各行业和各地区正在逐步制定所在部门、行业、地区的数据分类分级制度或指引，为企业落实本企业内部的数据分级分类工作提供参考。

访问权限管理设置

企业应根据业务实际情况和内部管理要求，配备相关人员。并且，根据不同岗位权限和职能，对可接触数据的人员角色进行分离，避免出现权责不清、责任不明等现象。权限的设置应遵循符合业务安全需求和最小够用原则。



1.8 风险评估思路已逐步被接受，PIA工具从陌生到被熟练操作

个人信息保护影响评估（PIA）是数据处理流程“必要原则”的体现，也是个人信息处理者在特定情形下处理个人信息必须履行的义务。《个保法》中明确规定，在特定情形下个人信息处理者应开展事前个人信息保护影响评估，并要求个人信息保护影响评估报告和处理记录应当**至少保存三年** 。同时，《个保法》对需要适用PIA评估的场景为非穷尽式列举，符合条件的对个人权益有重大影响的个人信息处理活动均应落入需评估范围，数据处理者应依照要求履行评估义务。

03 报告和记录

应当**至少保存三年**。

02 评估内容

- **处理目的、处理方式**是否合法、正当、必要；
- 对个人权益的**影响及风险程度**；
- 所采取的**安全保护措施是否合法、有效**并与风险程度相适应。

01 适用条件

①处理敏感个人信息；②利用个人信息进行自动化决策；③委托处理个人信息、向他人提供个人信息、公开个人信息；④向境外提供个人信息；⑤兜底：对个人权益有重大影响的个人信息处理活动。

03

02

01

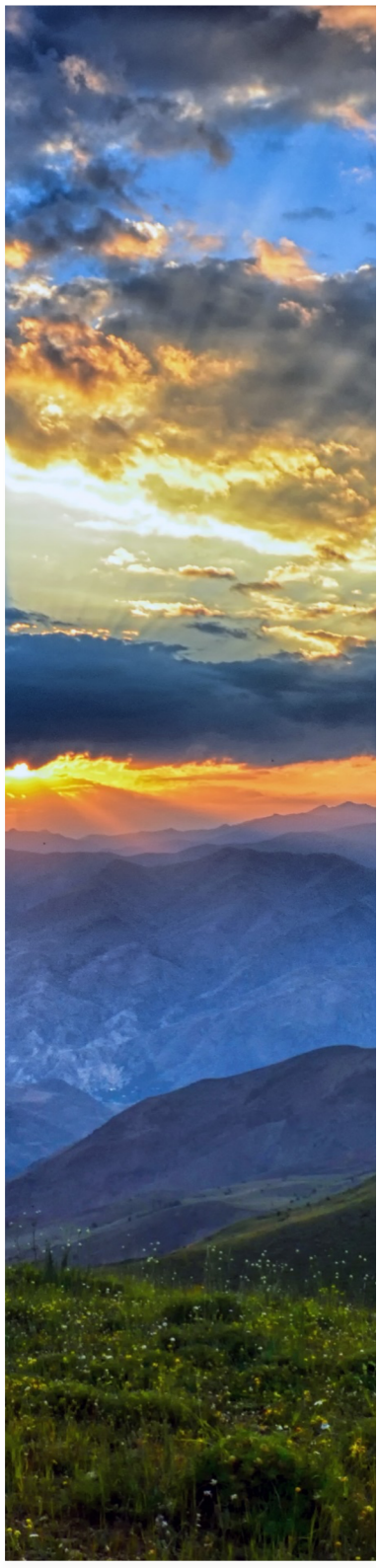
《个保法》中的PIA，是确立企业内部个人信息安全风险防范的“自律”管理机制 ，从源头预防风险发生。PIA制度在我国的确立，代表着各组织对内部风险管理意识不断强化，事前评估代替事后救济的合规时代已经来临。过渡期间，建议企业与律师保持沟通，及时规划并建立规范有效的风险评估合规体系。

在PIA的落地方面，作为该制度的配套国标《信息安全技术 个人信息安全影响评估指南》已于2021年6月1日施行，明确了开展PIA的原理、时间点和评估实施流程和方法等。该指南对个人信息处理者开展评估活动提供了更多细则，并列出了评估性合规的示例和高风险个人信息处理活动的示例，使个人信息保护影响评估的方法更加清晰、完整。

1.9 网络安全等级保护不再流于形式，安全测试与认证受到热捧

近年来，全国信息安全标准化技术委员会（以下简称“信安标委”）以《网安法》《网络安全等级保护条例（征求意见稿）》为基础，颁布了一系列网络安全等级保护的国家标准，相应地建立起我国网络安全等级保护规范2.0体系。

根据网络安全等级保护规范2.0体系的相关规定，按照等级保护对象（受侵害的客体）不同以及侵害程度的不同，针对等级保护对象在国家安全、经济建设、社会生活中的重要程度，遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织等合法权益的危害程度等不同，网络信息系统安全等级从低到高分为一至五级，级别越高，网络安全保障措施要求越高，相应的监管要求也会相应增强。



防范作用

网络安全等级保护规范有利于将有限的资源合理分配在不同风险的保护对象之中，以防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，并保障网络数据的完整性、保密性、可用性。

合规意识

虽然网络等级保护是一个系统性、复杂性、细节性极强的工作，但是为了保障国家安全和公共利益，同时保障企业自身合法权益，越来越多的企业逐渐认识到了落实和完善企业内部网络安全等级保护相关工作的重要性，通过引入第三方专业机构提供的安全测试和认证服务，并去公安机关进行定级结果备案，输出备案材料和备案证明，以查漏补缺、完善发展并确保企业自身的网络安全合法合规。

有力保障

坚定落实网络安全等级保护的潮流也与企业近年来对网络安全事故的防范意识增强有所关联，严格仔细地持续开展网络安全等级保护工作和履行相应的网络安全等级保护义务，不仅仅是企业高度重视数据合规工作的有力佐证，同时也是有效防范和避免网络安全事故发生的强有力保障。

1.10 人脸识别规制手段：行政监管与司法解释、判例双管齐下

人工智能技术的重要应用之一便是人脸识别技术，这项技术在为社会生活带来了便利，也带来了个人信息保护问题。2021年“3.15晚会”曝光人脸识别技术滥用乱象、郭某诉杭州野生动物世界有限公司的“人脸识别第一案”等，体现出人脸识别技术在社会中的广泛应用与个人信息保护的矛盾日渐尖锐。

针对这一情况，地方与中央也不断出台新的立法与司法解释，以完善处理人脸信息识别技术的适用规定。

1 《关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定》

最高人民法院

基于个人同意处理人脸信息的，未征得自然人或者其监护人的单独同意，或者未按照法律、行政法规的规定征得自然人或者其监护人的书面同意的，应当认定属于侵害自然人人格权益的行为 。

2 《网络数据安全管理条例（征求意见稿）》

网信办

数据处理者利用生物特征进行个人身份认证的，应当对其必要性、安全性进行风险评估，不得将人脸、步态、指纹、虹膜、声纹等生物特征作为唯一的个人身份认证方式，以强制个人同意收集其个人生物特征信息 。

3 《信息安全技术 人脸识别数据安全要求》

信安标委

开展人脸验证或人脸辨识时，应至少满足以下要求：

（1）不使用人脸识别方式的安全性或便捷性显著低于人脸识别方式。

（2）原则上不应使用人脸识别方式对不满十四周岁的未成年人进行身份识别。

（3）应同时提供非人脸识别的身份识别方式，并提供数据主体选择权。

（4）应提供安全措施保障数据主体的知情同意权。

（5）人脸识别数据不应用于除身份识别之外的其他目的。

4 《天津市社会信用条例》

天津市人大常委

市场信用信息提供单位不得采集自然人的宗教信仰、血型、疾病和病史、生物识别信息以及法律、行政法规规定禁止采集的其他个人信息。

5 《杭州市物业管理条例（修订草案）》

杭州市人大常委

物业服务不得强制业主通过指纹、人脸识别等生物信息方式使用公用设施设备。

对于滥用人脸识别技术的行政监管措施也进一步加强，人脸识别监管执法案例数量有所增加。例如，2021年7月，杭州市市场监督管理局因某房地产公司在未征得顾客同意的前提下抓拍人脸信息，对其处以25万元人民币罚款；2021年12月，上海市市场监督管理局因某汽车公司擅自采集人脸照片，对其处以10万元人民币罚款等。

从目前的执法情况来看，行政监管部门的处罚主要围绕数据处理者收集、使用人脸信息时是否明确告知个人主体会被采集人脸信息，或虽然通过告知牌等方式对人脸信息采集事宜进行公示，但并未明确告知收集使用的目的、方式和范围，抑或虽告知了收集、使用人脸信息的方式，但未征得消费者的同意这几方面。

1.11 个人主体权利实现机制在产品侧落地卓有成效

01 知情权、决定权、限制或拒绝权

02 查阅、复制权

03 可携带权

示例

04 要求说明权

（如自动化决策对个人权益有重大影响时）

05 更正权

06 删除权

07 撤回同意权

08 死者的个人信息处理权利

在11月1日《个保法》正式生效后，此前行业实践中较为少见的**“可携带权”**、**“撤回同意权”**等实现机制均陆续出现在了部分App产品界面中。例如，在“设置菜单”中增加“撤回同意隐私政策”的选项，或是在“个人中心”板块加入下载“个人信息副本”的产品界面设计。这体现了《个保法》生效后，行业内对于落实个人信息主体权利机制重视力度加大并敢于尝试创新的特点。

结合法规要求与企业实际需求，提出可落地合规的隐私保护设计方案十分重要。

1.12个别行业数据治理成为重点监管方向，如汽车行业

随着数据保护合规体系的构建，整体数据监管态势趋于严格。近年来，对于部分重要数据密集且智能化、网联化发展较快的行业，如金融行业和汽车行业，数据安全不仅仅涉及保护企业资产不被篡改、损毁、破坏和个人信息安全，还可能会影响社会安全、国家网络安全，或对个人权益造成重大影响。由此，在2021年，这些行业先行发力，数据安全与合规治理已经变成这部分行业的重要命题。

数据合规事件频发

2021年，智能网联汽车发展如火如荼，汽车智能化、网联化程度不断提升，智能网联汽车各环节之间都需要依靠数据交互来保证运营，多源异构数据深度耦合。2021年4月某车企女车主维权事件、2021年7月的某科技公司旗下App被下架等多起事件等，让智能汽车数据安全问题进入了公众视野。

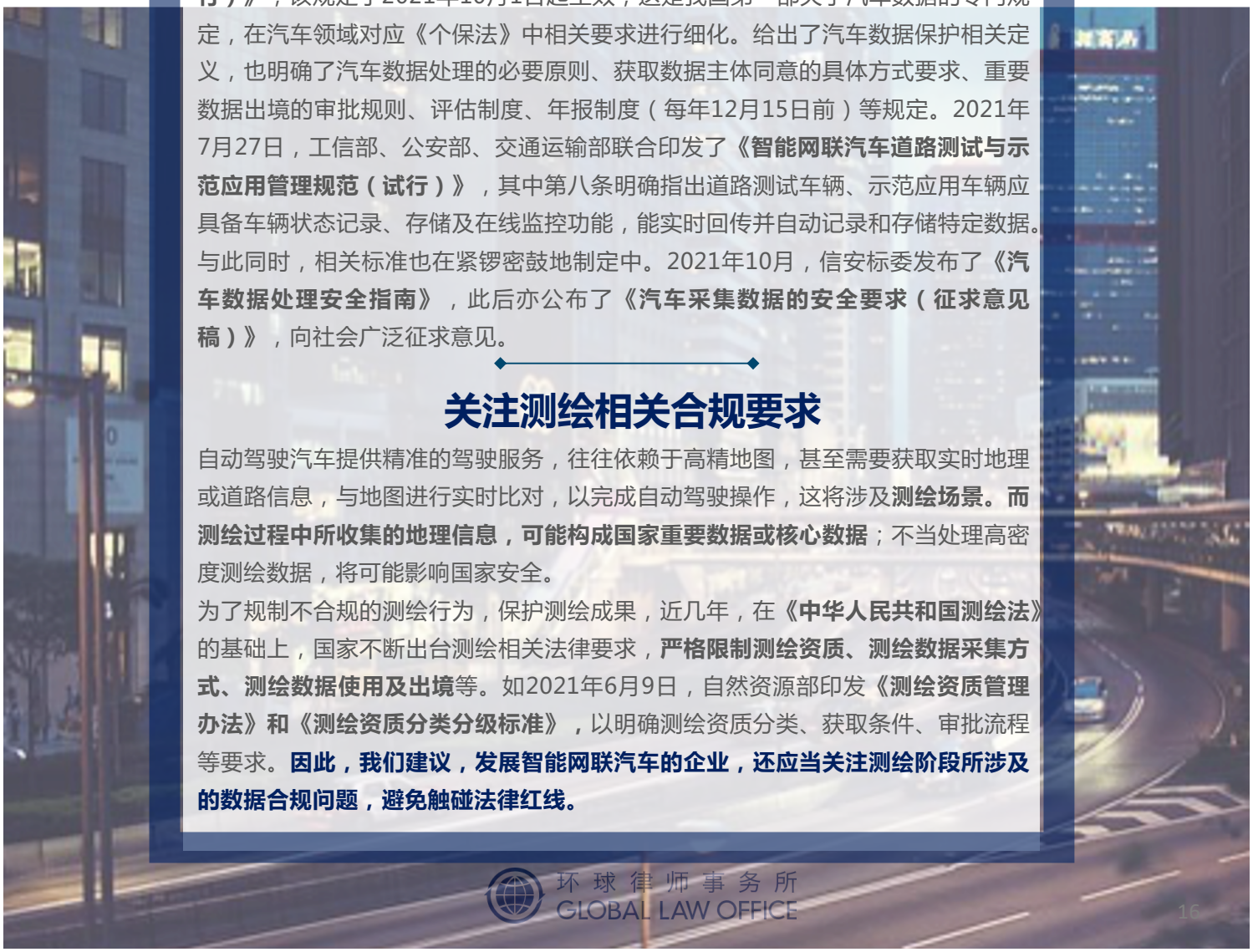
汽车数据安全规则不断出台

2021年5月12日，国家网信办等五部门公布了**《汽车数据安全管理若干规定（试行）》**；该规定于2021年10月1日起生效，这是我国第一部关于汽车数据的专门规定，在汽车领域对应《个保法》中相关要求进行细化。给出了汽车数据保护相关定义，也明确了汽车数据处理的必要原则、获取数据主体同意的具体方式要求、重要数据出境的审批规则、评估制度、年报制度（每年12月15日前）等规定。2021年7月27日，工信部、公安部、交通运输部联合印发了**《智能网联汽车道路测试与示范应用管理规范（试行）》**，其中第八条明确指出道路测试车辆、示范应用车辆应具备车辆状态记录、存储及在线监控功能，能实时回传并自动记录和存储特定数据。与此同时，相关标准也在紧锣密鼓地制定中。2021年10月，信安标委发布了**《汽车数据处理安全指南》**，此后亦公布了**《汽车采集数据的安全要求（征求意见稿）》**，向社会广泛征求意见。

关注测绘相关合规要求

自动驾驶汽车提供精准的驾驶服务，往往依赖于高精地图，甚至需要获取实时地理或道路信息，与地图进行实时比对，以完成自动驾驶操作，这将涉及**测绘场景。而测绘过程中所收集的地理信息，可能构成国家重要数据或核心数据**；不当处理高密度测绘数据，将可能影响国家安全。

为了规制不合规的测绘行为，保护测绘成果，近几年，在**《中华人民共和国测绘法》**的基础上，国家不断出台测绘相关法律要求，**严格限制测绘资质、测绘数据采集方式、测绘数据使用及出境**等。如2021年6月9日，自然资源部印发**《测绘资质管理办法》和《测绘资质分类分级标准》**，以明确测绘资质分类、获取条件、审批流程等要求。**因此，我们建议，发展智能网联汽车的企业，还应当关注测绘阶段所涉及的数据合规问题，避免触碰法律红线。**



1.13 网络安全审查：从关键信息基础设施运营者到网络平台运营者，并以拟国外上市企业为审查重点

我国网络安全审查制度由来已久。早在2015年，《中华人民共和国国家安全法》（以下简称“《国家安全法》”）就确立了国家安全审查制度的法律基础，2021年9月1日正式施行的《数安法》以及2022年新年伊始即公布的《网络安全审查办法》（自2022年2月15日起施行）则在此基础上进一步确立了数据领域的国家安全审查制度，要求对于影响或者可能影响国家安全的数据处理活动进行数据网络安全审查，这在一定程度上揭示了网络安全审查的立法目的与机制定位。

在适用对象层面，自《网安法》在法律层面明确了关键信息基础设施运营者在符合条件时接受国家安全审查要求后，《网络数据安全管理条例（征求意见稿）》和《网络安全审查办法》相继将数据处理者纳入网络安全审查的范围。换言之，即使企业不落入或者不确定是否落入关键信息基础设施运营者范围，若开展数据处理活动且达到影响或可能影响国家安全的标准，也需要履行主动申报网络安全审查的义务；此外，根据《网络审查办法》第十六条，如监管机构认为网络产品和服务以及数据处理活动影响或可能影响国家安全的，其也可依职权进行审查。

值得关注的是，我国规制企业拟赴境外/国外上市的监管态度逐渐清晰：首先，《网络安全审查办法》第七条明确要求，**掌握超过100万用户个人信息、赴国外上市的网络平台运营者**必须向网络安全审查办公室申报网络安全审查—申报后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。其次，《网络数据安全管理条例（征求意见稿）》针对**赴境外上市的数据处理者**有数据安全评估及年度上报义务，并专门做出了规定。其中第三十二条指出，处理重要数据或者赴境外上市的数据处理者，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。这两份文件的发布进一步反映我国对于赴国外/境外上市企业所涉及数据安全问题的关注。尤其考虑到企业国外上市后，可能受制于当地监管部门管辖从而需要向国外传输中国境内相关数据，有可能受到外国政府影响、控制或恶意利用，我国有必要加强对拟国外上市企业的监管力度。结合早先网络安全审查办公室对“某知名互联网出行企业”突发实施的网络安全审查的急行动、重举措，监管机构的态度和国家政策导向可见一斑。**因此我们建议，拟上市企业在部署规划前，与律师沟通、进行法律评估，以确保在了解政策导向的同时，符合国家要求并履行相应的义务，减少不必要的风险和损失。**

1.14 算法透明性要求被提出，推荐性算法备案开始尝试

2021年算法推荐管理立法情况概览

《**个保法**》的生效和实施规范了平台企业的大数据使用和用户画像行为，通过约束处理个人信息的行为，从源头上遏制大数据“杀熟”行为的泛滥。

2021年9月29日，九部委印发了《**关于加强互联网信息服务算法综合治理的指导意见**》，提出利用三年左右时间，逐步建立健全算法治理机制、完善监管体系与算法生态规范的算法安全综合治理格局。

2021年10月19日，《**中华人民共和国反垄断法(修正草案)**》约束经营者通过滥用大数据、算法、技术及资本优势、平台规则等排除、限制竞争的不当行为，适用主体并不仅限于平台经济和互联网方面的实体。

2021年12月31日，网信办发布《**互联网信息服务算法推荐管理规定**》，作为《网安法》《数安法》《个保法》和《互联网信息服务管理办法》等法律法规的实施细则，对算法推荐活动将启动新一轮监管和规范。

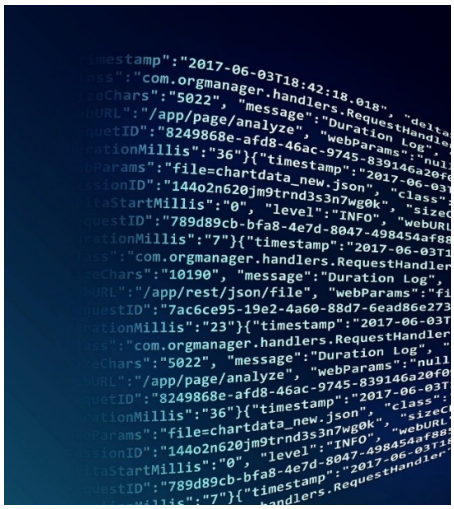
《互联网信息服务算法推荐管理规定》合规要点

义务类型	具体义务要求
算法推荐服务提供者的义务	
安全主体的义务	算法推荐服务提供者应当落实算法安全主体责任，建立健全算法机制机理审核、科技伦理审查、用户注册、信息发布审核、数据安全和个人信息保护、反电信网络诈骗、安全评估监测、安全事件应急处置等管理制度和技术措施，制定并公开算法推荐服务相关规则，配备与算法推荐服务规模相适应的专业人员和技术支撑。（第七条）
算法审查的义务	算法推荐服务提供者应当定期审核、评估、验证算法机制机理、模型、数据和应用结果等。（第八条）
用户模型关联的义务	算法推荐服务提供者应当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。（第十条）
禁止的用户模型	不得将违法和不良信息关键词记入用户兴趣点或者作为用户标签并据以推送信息。（第十条）
价值导向的义务	应当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，在首页首屏、热搜、精选、榜单类、弹窗等重点环节积极呈现符合主流价值导向的信息内容。（第十一条）
禁止干预舆论的义务	算法推荐服务提供者不得利用算法虚假注册账号、非法交易账号、操纵用户账号或者虚假点赞、评论、转发，不得利用算法屏蔽信息、过度推荐、操纵榜单或者检索结果排序、控制热搜或者精选等干预信息呈现，实施影响网络舆论或者规避监督管理行为。（第十四条）
保障用户权利的义务	算法推荐服务提供者应当以显著方式告知用户其提供算法推荐服务的情况，并以适当方式公示算法推荐服务的基本原理、目的意图和主要运行机制等。（第十六条）
	算法推荐服务提供者应当向用户提供选择或者删除用于算法推荐服务的针对其个人特征的用户标签的功能。（第十七条第二款）
	算法推荐服务提供者应当向用户提供不针对其个人特征的选项，或者向用户提供便捷的关闭算法推荐服务的选项。用户选择关闭算法推荐服务的，算法推荐服务提供者应当立即停止提供相关服务。（第十七条第一款）
	算法推荐服务提供者应用算法对用户权益造成重大影响的，应当依法予以说明并承担相应责任。（第十七条第三款）
	算法推荐服务提供者向消费者销售商品或者提供服务的，应当保护消费者公平交易的权利，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。（第二十一条）
	算法推荐服务提供者应当设置便捷有效的用户申诉和公众投诉、举报入口，明确处理流程和反馈时限，及时受理、处理并反馈处理结果。（第二十二条）
具有舆论属性、社会动员能力算法推荐服务提供者的额外义务	
备案的义务	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服务提供者的名称、服务形式、应用领域、算法类型、算法自评估报告、拟公示内容等信息，履行备案手续。（第二十四条第一款）算法推荐服务提供者的备案信息发生变更的，应当在变更之日起十个工作日内办理变更手续。（第二十四条第二款）
公示备案信息的义务	完成备案的算法推荐服务提供者应当在其对外提供服务的网站、应用程序等的显著位置标明其备案编号并提供公示信息链接。（第二十六条）
开展安全评估	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。（第二十七条）

Part
02

2022
趋势预测

2.1重要数据识别标准与清单逐步确立



随着企业依据自身合规需求、运营需要、对数据出境与境外上市需求的增强，企业对自身数据资产中的相关数据是否构成重要数据，以及判断是否需要履行持有重要数据的网络运营者增强性合规义务，变成当务之急。

国家标准：《信息安全技术 数据出境安全评估指南（征求意见稿）》

2017

附录A：重要数据识别指南对28类行业领域规定重要数据范畴，尚未生效。

国家标准：《信息安全技术 重要数据识别指南（征求意见稿）》

2021

与2017年版指南中按照行业对重要数据给出分类的方式相比，当前的监管思路从数据的性质和作用着眼，发挥业务自主性，打破数据孤岛的建设思路，识别了重要数据的八个方面特征：与经济运行相关、与人口和健康相关、与自然资源和环境相关、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，以及其他影响国家安全的特征，涵盖了对国家安全影响的主要关切。

《网安法》

2017

初次提出重要数据概念，与关键信息基础设施运营者有关。

《数安法》

2021

合规主体扩展至任何重要数据的处理者，各地区各部门根据国家分类分级制度建立重要数据目录。

重要数据处理者需要履行三类增强型义务，包括明确数据安全责任人和管理机构、定期进行风险评估、以及数据出境的合法开展。

可见未来

2022

《数据出境安全评估办法（征求意见稿）》要求数据处理者向境外提供重要数据前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。

可以期待，国家将在近期确立重要数据的识别标准，以供各地区和部门进一步明确重要数据相关标准。届时，企业需明确数据安全责任人和管理机构，进行风险评估，并按照相应标准对自身数据进行审视，识别出重要数据并报送识别结果；有重要数据需要出境的，也需要申报国家网信部门进行安全评估。

2.2 数据出境安全审查与报批流程完善

《数据出境安全评估办法（征求意见稿）》（以下简称“《办法》”）于2021年10月29日发布。虽然该《办法》仍处于征求意见阶段，但其中关于数据出境评估的规定已逐渐呈现体系化，为企业提供了更加明确的出境评估依据，其中主要包括**企业自评估制度**与**监管机构安全评估制度**两部分。

关于**数据出境风险自评估制度**，主要是指数据处理者在向境外提供数据前，应事先开展数据出境风险自评估，即明确数据处理者无论是关键信息基础设施运营者或一般网络运营者，其所处理的数据类型无论涉及国家核心数据、重要数据或一般数据，均应当在数据出境前进行风险自评估。

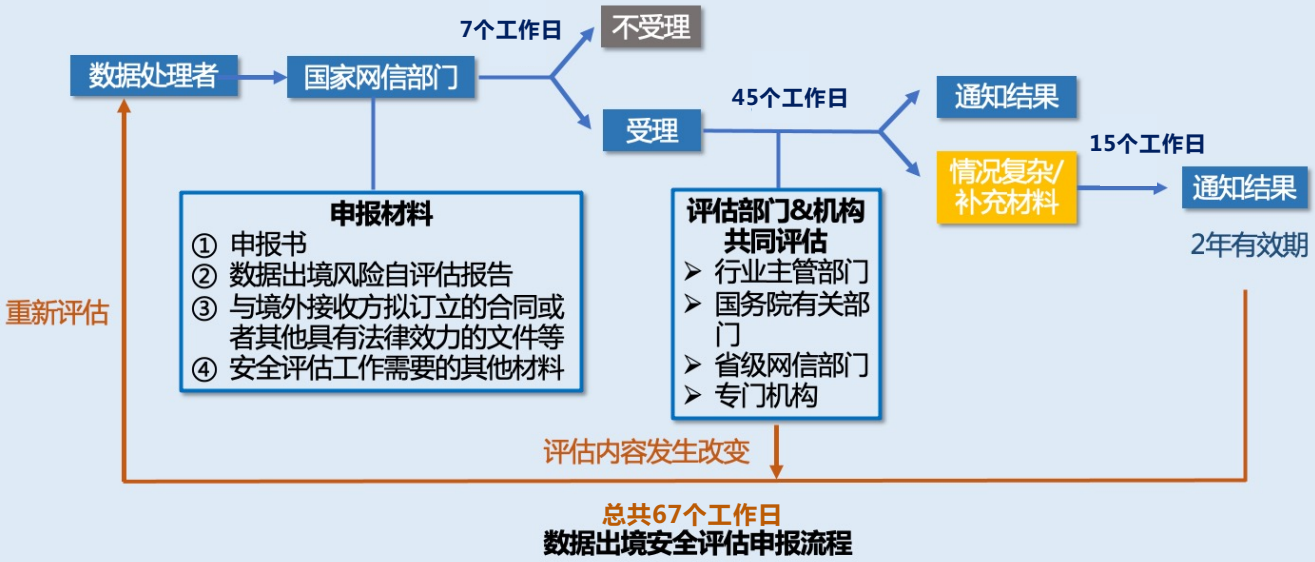
在风险自评估后，企业应当形成《数据出境风险自评估报告》，并参照个人信息保护影响评估的要求，报告与评估记录**至少留存三年**，并视自评估结果判断是否申请监管机构安全评估。

关于**数据出境安全评估义务**，主要是指企业需要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。这一义务的适用对象包括：

（1）向境外提供重要数据的所有数据处理者（包括关键信息基础设施运营者与一般数据处理者）；及

（2）向境外提供个人信息的关键信息基础设施运营者以及处理数据量达到《办法》第4条第3、4款规定的一般数据处理者（可参考上图红色虚线框部分）。

2.2 数据出境安全审查与报批流程完善



根据《办法》规定，数据处理者申报数据出境安全评估时，应当提交的材料包括：①申报书；②数据出境风险自评估报告；③数据处理者与境外接收方拟订立的合同；或者④其他具有法律效力的文件以及安全评估工作需要的其他材料。

国家网信部门于**收到申报材料之日起七个工作日内**，确定是否受理评估并书面反馈受理结果。

国家网信部门在确认受理后，将组织行业主管部门、国务院有关部门、省级网信部门、专门机构等共同进行安全评估。一般情况下，最终的评估结果会在**六十个工作日内**以书面通知的形式反馈申报数据出境安全评估的数据处理者。

数据出境评估结果的有效期为两年。若有效期届满，数据处理者需要继续开展原先范围数据出境活动的，应当在有效期届满六十个工作日前重新申报评估。

特别需要注意，在收到评估结果后，若此前被评估的事项发生改变，则需要重新依据上述流程申报安全评估。

2.3 关键信息基础设施认定边界更加明确

自《网安法》颁布后，关键信息基础设施的认定一直是人们热议的话题。2021年7月30日，《关键信息基础设施安全保护条例》（以下简称“《关基条例》”）公布，并于2021年9月1日起正式生效。《关基条例》的出台，旨在落实《网安法》中有关关键信息基础设施运营者的合规要求，为我国深入开展关键信息基础设施安全保护工作提供有力保障。

《关基条例》第二条进一步明确了关键信息基础设施的认定边界，即典型的关键信息基础设施，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。这与《网安法》第三十一条的定义方式保持了一致，采用的仍是举例+后果概括的方式，但修正了2017年网信办发布的《关键信息基础设施安全保护条例（征求意见稿）》对行业进行具体细化的列举方式，改为只列举行业大类，从实质上扩大关键信息基础设施的认定范围，使行业主管机构对基础网络设施及重要信息系统的认定具有更大的灵活性。

《关基条例》从行政法规的角度还给出了详细的指南，明确指出第二条中涉及的重要行业和领域的主管部门、监督管理部门需要根据本行业、本领域的实际情况，制定关键信息基础设施认定规则。

主要考虑因素包括：（一）正向角度：网络设施、信息系统等对于本行业、本领域关键核心业务的依赖程度重要；（二）负向角度：网络设施、信息系统等一旦遭到破坏、丧失功能或者数据泄露可能带来的危害程度大；（三）关联角度：对其他行业和领域有关联影响。

鉴于《国家网络安全检查操作指南》对网站类和平台类运营者是否为关键信息基础设施运营者制定了特定的判断标准，且关键信息基础设施与关键业务之间的支撑和相互依赖关系处于动态变化之中，主管部门与监管部门将结合上述因素并根据实际情况，动态地裁减不同行业、不同领域针对关键信息基础设施自身安全基线的要求，提供给企业更加实际可行的认定规则。根据《关基条例》第十条，重要行业和领域的主管部门、监督管理部门根据认定规则负责组织认定本行业、本领域的关键信息基础设施，及时将认定结果通知运营者，并报国务院公安部门备案。

2.4 平台治理：从数据汇聚到反垄断规制

超大型互联网平台关于数据竞争的治理

近年来，互联网超级平台通过打造网络生态系统吸引了大量用户和海量数据，也为大众的生活和工作带来了诸多便利。然而，数字经济中普遍存在的**网络效应**不断扩大，市场领先者在获取用户、留存用户方面的竞争优势，造成“**赢者通吃**”的自然局面。随着数据和资源不断向头部企业聚集，超级平台对竞争对手**设置市场或技术壁垒**，或依靠平台优势对自身关联业务进行**自我优待**的行为更容易达成巩固自身垄断地位的效果，与此同时也可能造成限制市场正当竞争的不利局面。

《个保法》第58条提出大型互联网平台的多项义务。此外，针对此类行为，我国出台了多项文件，明确了杜绝此类现象的监管意图，也表明了希望通过平台治理增强大型平台的正向责任，以便其利用自身优势为行业发展和良性竞争创造更多便利的治理方针。

1

《中华人民共和国反垄断法（修正草案）》

草案中明确，具有市场支配地位的经营者利用**数据和算法、技术以及平台规则**等设置障碍，对其他经营者进行不合理限制的，**属于滥用市场支配地位的行为。**

2

《国务院反垄断委员会关于平台经济领域的反垄断指南》

对平台可能存在的**滥用市场经济地位**等问题进行了规制。在互联网领域，“**二选一**”行为得到了执法机构的重点关注。

3

《互联网平台分类分级指南（征求意见稿）》

并不是所有的互联网平台都需要承担同样的责任或受到同样的限制。根据**能力越大，责任越大**的原则，指南将通过对平台的**分类分级**以确认责任类别。

4

《互联网平台落实主体责任指南（征求意见稿）》

互联网平台经营者需承担算法规制、知识产权保护、自然人隐私与个人信息保护；而超大型平台经营者除此之外还要承担**平等治理**（不实施自我优待）、**开放生态**等责任。

可预见，在接下来的一年中，互联网平台运营者需要对法律中适用于自身体量的平台责任要求予以积极落实，对自身的商业模型、内部流程、运行规则等做出量身订制的调整。

2.4 平台治理：从数据汇聚到反垄断规则

应用分发平台应落实主体责任

《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）》均表明，国家市场监督管理总局已根据“鼓励竞争、限制垄断”的思路对平台提出了要求。与此同时，基于对应用市场治理角度，网信办和工信部均要求应用分发平台加强落实平台主体责任，强调了应用分发平台应起到的“**守门员**”作用。

工信部 App侵害用户权益专项整治行动

2021年，工信部对应用分发平台上未明示App权限列表、用户数据收集范围以及其相关用途的，以及应用平台对App上架审核不严格、对违规App下架不及时、对App开发者身份验证不到位的情况持续进行了重点整治，并在通报中对数家应用分发平台的相关问题进行了点名批评。

工信部《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）》

明确了App分发平台应当履行个人信息保护义务，包括对第三方App相关主体信息、用户终端权限列表和数据收集情况明示和审核义务、App开发运营者管理机制的建立、对问题App投诉渠道的设立，以及对问题App上报和处置工作的开展等要求进行规定。

网信办《网络数据安全管理条例（征求意见稿）》

该条例第四十四条规定了应用分发平台需要对第三方App承担数据安全管理责任，且明确第三方App对用户产生侵害时，用户可直接要求分发该App的应用平台运营者先行赔偿。

上述执法趋势和发文已经明确表示，应用分发平台未来需要承担起对在其平台上架App的审查、管控和处置责任；在网信办2022年1月5日发布的《移动互联网应用程序信息服务管理规定（征求意见稿）》的第三章中，也将上述责任进行了进一步细化，这也对平台运营者的相关技术、管理和规则设定提出了更高的要求。面对着趋于强化的平台治理和平台监管责任，作为责任主体，应用平台运营者需要基于现有平台运营的框架，根据自身情况，对体系进行构建和适配。

从执行层面而言，应用分发平台在满足法定义务的同时，也可以通过流程设计，确保相关规则在设计和执行上体现公平性，避免不正当竞争行为的产生。

2.5 内部审计与外部审计相结合配置更加完备

个人信息保护合规审计

《个保法》第五十四条和第六十四条规定了针对个人信息处理活动的合规审计制度：当发现**个人信息处理活动存在较大风险**或者**发生个人信息安全事件**时，或**在履行个人信息保护职责的部门要求**下，个人信息处理者应当按照相关规定，对其处理个人信息遵守法律、行政法规的情况，由**内部审计机构**或者**委托专业机构**进行合规审计。

履行个人信息保护职责的部门要求个人信息处理者委托第三方进行合规审计的，个人信息处理者应当委托专业机构进行合规审计。

预计在2022年，个人信息保护合规审计规则的制定与实施都会有进一步的探索：法律法规及标准将陆续出台，明确**合规审计依据、目的、目标、原则、范围、人员要求、机构资质、相关处罚机制**等实施细节，推进合规审计工作切实可落地。

内部审计

企业内部合规审计规则、审计范围的确定；
企业内部合规机构及人员配置的设立；
企业内部进行合规审计的频率；
企业内部合规审计依据的明确及结果保存等。

外部审计

外部合规专业机构的资质确认；
合规审计专业人员的资质确认；
外部合规审计规则与流程的确认；
明确外部合规审计依据的明确及结果保存等。

2.6 数据集团内部共享及向第三方共享规则与机制健全

随着数据的海量增长和潜在价值的不断提升，数据逐渐成为企业的重要资产和核心竞争力。数据只有共享和流动才能产生价值，数据共享和流通的合法化一直是学术界和产业界的热题。上海市和深圳市分别发布了《上海市数据条例》和《深圳经济特区数据条例》，一方面推动数据交易平台，促进市场主体在交易平台内外依法对数据进行交易；另一方面对“公共数据”的管理做出了规定，鼓励对公共数据的开放和共享。

文件	数据共享相关规定
《数安法》	鼓励数据依法合理有效利用，保障数据依法有序自由流动。国家建立健全数据交易管理制度，规范数据交易行为，培育数据交易市场。
《上海市数据条例》	• 鼓励和引导市场主体依法开展数据共享、开放、交易、合作，促进跨区域、跨行业的数据流通利用； • 提出了数据交易平台的设立（设立浦东新区数据交易所）； • 市场主体可在政府授权范围内、依托统一规划的公共数据运营平台提供的安全环境，对公共数据实施开发利用，并提供数据产品；明确使用、加工等数据处理活动中形成的财产权益； • 制定上海市重要数据目录，以及在临港新片区内探索制定低风险跨境流动数据目录。
《深圳经济特区数据条例》	• 推动构建数据收集、加工、共享、开放、交易、应用等数据要素市场体系； • 推动建立数据交易平台，并引导市场主体通过该平台进行数据交易； • 推动公共数据最大限度的开放利用；合法处理数据所形成的数据产品和服务具有财产权益； • 保护数据全生命周期安全；强化个人信息保护，规范画像和个性化推荐的应用等。

数据共享要点及管理措施

管理模块		管理措施	
		数据来源于第三方	数据共享给第三方
法律文书	承诺函	第三方承诺数据来源合法	第三方承诺不超过用户授权范围使用数据
	合同	约定双方履行数据保护义务，明确双方数据安全权利和义务的责任边界	约定双方履行数据保护义务，明确双方数据安全权利和义务的责任边界
	授权协议	审查用户对第三方的授权协议，确保数据使用未超出授权范围	在授权协议中告知用户共享目的、数据类型、第三方类型等
内控体系	机制流程	建立第三方的准入管理机制和工作流程，建立安全评估机制（准入、定期审计）	
	安全措施	明确双方的安全责任及实施的数据保护措施	
	留存记录	留存平台第三方接入合同和管理记录，确保可回溯	
	响应申诉	建立个人信息主体请求、申诉等机制和处置流程	
	审计	定期审计第三方数据保护落实情况，督促整改	

2.6 集团数据共享与向第三方提供数据规则机制健全

集团内数据共享和融合注意要点

区别于向第三方共享数据，鉴于属于同一集团内部，对落实统一的数据安全保护管理措施集团有较大优势，因此在实践中，同一集团下不同企业和不同业务部门之间的数据融合，企业对内部转让和共享规则机制关注度相对较低。我们建议当集团内进行数据共享和融合时，仍需注意以下合规要点：

- **区分数据融合和共享：**

  数据融合关注不同数据源的数据汇聚（包括数据共享方式），以及不同数据源的数据使用目的的变化，数据共享主要是指决定数据处理的处理方发生变化。

- **用户授权：**

  数据共享和融合前，应明确告知用户上述数据处理行为的目的及范围，并取得明确授权。

- **符合用户的合理预期：**

  数据共享和融合行为的目的以及方式，不应当超出用户的合理预期。

- **数据区分和分类保护：**

  区分同类业务数据融合和不同类业务数据融合，比如金融数据与其他数据融合时，需遵循金融特殊监管规则。

- **进行个人信息保护影响评估：**

  数据共享和融合前，进行个人信息保护影响评估，以评估上述数据处理行为的安全性以及可能对用户造成的影响。

- **将数据进行匿名化处理：**

  将数据进行匿名化后再进行共享和融合，例如可以对标签类信息进行共享和融合。

- **加强数据审计和评估，控制风险：**

  加强集团内数据审计和评估，以控制数据共享和融合带来的安全风险。

2.7 特殊行业数据处理要求更加细化，各行业主管部门规则更加清晰、科学

纵观立法趋势，对于一些特殊行业（以金融、医疗领域、智能网联汽车为例）的数据处理要求将有望进一步细化，各行业主管部门的规则设置也将更加清晰、科学，并呈现出各司其职地履行专业监管，同时将与网信部门协调磋商，形成跨部门数据合规监管的新常态。

01. 金融领域

2021年9月30日，中国人民银行发布了《征信业务管理办法》，对于信用信息的范围、采集、整理、保存、加工、对外提供、使用、安全及跨境流动等进行了系统性规定，重点强调了信用信息的安全保护与合规使用，保护信息主体的合法权益。《征信业务管理办法》第五条规定金融机构不得与未取得合法征信业务资质的市场机构开展商业合作获取征信服务。结合第十四条规定，可以体现出对驻贷平台“断直连”的总体要求，即大数据公司只有在与持牌征信机构合作的情况下，由持牌征信机构向中国人民银行报告后，方可为金融经济活动提供个人信用信息。

02. 医疗领域

近年来，“互联网+医疗”行业发展得如火如荼。2021年7月1日起，国家市场监督管理总局和国家标准化管理委员会联合发布的推荐性国家标准《信息安全技术 健康医疗数据安全指南》正式实施，在《个保法》和《数安法》等相关法律法规的基础上，以及此前的《人口健康信息管理办法（试行）》《人类遗传资源管理条例》以及《互联网医院管理办法》提出的“最少够用”原则、“获取书面同意”规则，以及医疗机构必须实施第三级网络安全等级保护要求基础上，该指南明确了“健康医疗数据”的定义和分类，并规定了数据生命周期的不同阶段以及典型数据场景中宜采取的安全措施。现有法律法规，正在为“互联网+医疗”发展以及疫情防控常态化背景下健康医疗行业的数据开发与使用提供一套日趋完善的安全合规体系，也为“互联网+医疗”的合规化提出更高要求。

03. 智能网联汽车领域

2021年，我国在智能网联汽车领域的监管文件密集出台，先后发布了《关于加强智能网联汽车生产企业及产品准入管理的意见》《汽车数据安全管理若干规定（试行）》《车联网（智能网联汽车）网络安全标准体系建设指南》《车联网网络安全标准体系建设指南》《车联网信息服务 用户个人信息保护要求》《智能网联汽车生产企业及产品准入管理指南（试行）（征求意见稿）》《深圳经济特区智能网联汽车管理条例（征求意见稿）》《信息安全技术 汽车采集数据的安全要求（征求意见稿）》《智能网联汽车数据安全共享参考架构》《汽车采集数据处理安全指南》等涉及智能网联汽车信息安全的政策文件。**2021年是智能网联汽车数据安全的元年，车联网安全顶层设计不断完善，初步形成了我国汽车数据合规框架。未来我国将会继续从数据分类分级、重要数据境内存储、健全网络安全保障技术等方面细化现有制度标准，加强汽车数据和网络安全管理。**

2.8 年度报告报送与备案流程更加成熟

法律法规依据	报送/备案机关	报送/备案要求	频率
《数安法》	有关主管部门	**重要数据的处理者**对其数据活动定期开展**风险评估，并报送风险评估报告。风险评估报告应当包括本组织掌握的重要数据的种类、数量、收集、存储、加工、使用数据的情况、面临的数据安全风险及其应对措施等。**	**定期报送报告**
《工业和信息化领域数据安全管理办法（试行）（征求意见稿）》	工业和信息化部备案管理平台	工业和电信数据处理者应当将处理其**重要数据以及核心数据的数量、类别、处理目的和方式、使用范围、主体责任、安全保护措施等基本情况，数据提供、公开、出境、承接（因兼并、重组、破产等原因需要转移数据），以及数据安全风险、事件处置等情况进行备案。**	/
	所在地工业和信息化主管部门或通信管理局	涉及重要数据和核心数据的安全事件，应当第一时间向所在地工业和信息化主管部门或通信管理局报告。事件处置完成后应当在规定期限内形成总结报告。	**每年**
《网络交易监督管理办法》	住所地省级市场监督管理部门	网络交易平台经营者报送平台内经营者的身份信息。	**每年1月和7月**
《互联网信息服务算法推荐管理规定》	国家和省、自治区、直辖市网信部门	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通过互联网信息服务算法备案系统填报服务提供者的名称、服务形式、应用领域、算法类型、算法自评估报告、拟公示内容等信息，履行备案手续。	**在提供服务之日起十个工作日内**

2.8 年度报告报送与备案流程更加成熟

法律法规依据	报送/备案机关	报送/备案要求	频率
《汽车数据安全管理若干规定（征求意见稿）》	省级网信部门和有关部门	运营者处理重要数据，应当提前报告数据类型、规模、范围、保存地点与时限、使用方式，以及是否向第三方提供等。	/
	省级网信部门和有关部门	处理个人信息涉及个人信息主体超过10万人、或者处理重要数据的运营者应将年度数据安全管理情况报告，内容包括： （一）数据安全负责人以及负责处理用户权益相关事务责任人的姓名和联系方式； （二）处理数据的类型、规模、目的及必要性； （三）数据的安全防护和管理措施，包括保存地点、期限等； （四）与境内第三方共享数据情况； （五）数据安全事故及处理情况； （六）与个人信息和数据相关的用户投诉及处理情况； （七）国家网信部门明确的其他数据安全情况。	**每年十二月十五日前**
	省级网信部门和有关部门	如运营者存在向境外提供数据的情况应当报告，内容包括： （一）接收者的名称和联系方式； （二）出境数据的类型、数量及目的； （三）数据在境外的存放地点、使用范围和方式； （四）涉及向境外提供数据的用户投诉及处理情况； （五）国家网信部门明确的向境外提供数据需要报告的其他情况。	**每年十二月十五日前**
《关于报送2021年度汽车数据安全管理情况的通知》	上海市互联网信息办公室网络安全处	注册地为上海的汽车数据处理者应参照《2021年度汽车数据安全管理情况报告模板》，提交2021年度汽车数据安全管理情况报告。报告中需包含汽车数据处理者企业名称&联系人、数据安全管理负责人、用户事宜联系人、处理数据类型、汽车数据所在地、数据共享情况、安全事件、投诉情况、风险评估报告、是否涉及数据出境、车外视频、车外雷达、行踪轨迹等个人信息全生命周期情况等。	**十二月二十二日前**
《广东省互联网信息办公室关于报送2021年度汽车数据安全管理情况的通知》	广东省互联网信息办公室与有关部门	广东省的汽车数据处理者开展重要数据处理活动的，应报送2021年度汽车数据安全管理情况。	**十二月十五日前**
《天津市互联网信息办公室关于报送2021年度汽车数据安全管理情况的通知》	天津市互联网信息办公室与有关部门	天津市的汽车数据处理者开展重要数据处理活动的，应报送2021年度汽车数据安全管理情况。在具体报送材料中可对“安全管理要求”内容详细描述。	**十二月十五日前**
《省委网信办开展年度汽车数据安全管理情况收集工作》	河北省互联网信息办公室	汽车数据处理者（即开展汽车数据处理活动的组织，包括汽车制造商、零部件和软件供应商、经销商、维修机构以及出行服务企业等）应报送2021年度汽车数据安全管理情况。	/
《湖南省互联网信息办公室关于报送2021年度汽车数据安全管理情况的通知》	湖南省互联网信息办公室与有关部门	湖南省的汽车数据处理者开展重要数据处理活动的，应报送2021年度汽车数据安全管理情况。	**十二月二十日前**

2.9 网络安全审查标准与流程更具可操作性

PRACTICAL GUIDANCE

数据犹如黄金与石油，对于国家发展的重要意义已不言而喻。数据安全缺乏保障将直接损害到本国企业开发利用数据资源的机会，影响我国数字产业和数字经济竞争力的提升，甚至危害国家的安全与社会稳定。

从《网安法》《个保法》《数安法》到《网络数据安全管理条例（征求意见稿）》《网络安全审查办法》，我国网络安全审查制度及配套标准、流程已逐步走向完善、细化、可落地。这不仅体现了我国对于网络数据安全的高度重视，而且也是我国遵循“总体国家安全观”下推动数字经济健康持续发展的必然要求。

目前数据处理者因需要履行网络安全审查申报等义务而需要遵守一系列的合规措施，这可能给企业带来一定的合规成本。但随着网络安全审查标准与流程变得具有可操作性，遵守该等义务不但能为企业提前排除不合规风险，而且将为企业合法合规经营带来信心，从而进一步使得企业能够更精准、有力地把握数字经济发展的新机遇。

有鉴于此，企业未来应当同时评估数据处理活动对国家安全的影响，通过与专业律师团队的沟通与协作，正确把握和健全完善国家总体安全观指引下的企业数据安全治理水平，有效防范因数据安全问题可能引发国家安全和需要接受网络安全审查的风险。

2.9 网络安全审查标准与流程更具可操作性

在网络安全审查的适用与启动方面，《网络数据安全管理条例（征求意见稿）》和最新出台的《网络安全审查办法》作出相应规定：

- 《网络数据安全管理条例（征求意见稿）》仅针对应主动申报网络安全审查的适用范围作出规定，即在如下情况下，**一般数据处理者**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**；以及（4）其他影响或者可能影响国家安全的数据处理活动。
- 《网络安全审查办法》（《办法》）明确，网络安全审查的启动有下述情形：企业主动申报、网络安全审查工作机制成员单位依职权提请审查、以及社会举报。
  - **主动申报审查：**（1）**关键信息基础设施运营者采购网络产品和服务**，应预判该产品和服务投入使用后可能带来的国家安全风险；（2）**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；（3）**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。**
  - **依职权审查：**（1）网络安全审查工作机制成员单位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，由网络安全审查办公室按程序报中央网络安全和信息化委员会批准后，依照《办法》进行审查。（2）网络安全审查办公室通过接受举报等形式加强事前事中事后监督，如审查办公室认为被举报的某产品或者服务或者某数据处理活动已经或者可能对国家安全产生风险的，可按《办法》启动审查。

虽然二者关于网络安全审查的文字描述稍有区别，但考虑到两份文件均由网信办起草，因此《网络数据安全管理条例（征求意见稿）》后期也有可能与《网络安全审查办法》保持一致，但仍有待观察。

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主动申报网络安全审查已然成为拟赴国外上市企业所需面临的新课题。因此，一方面，拟在国外上市的企业需在上市前搭建较为完整的数据合规体系，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，有可能需要申报网络安全审查的企业，应当在上市材料递交前履行该义务，以符合监管要求，避免该报未报风险。

2.10 企业算法管理和可解释能力不断提升

《互联网信息服务算法推荐管理规定》提出了对算法推荐服务提供者应当落实**算法安全主体责任**，建立健全**管理制度和技术措施**，亦明确鼓励算法推荐服务提供者综合运用内容去重、打散干预等策略，并优化检索、排序、选择、推送、展示等规则的**可解释性**。

我们理解，上述法律法规等规则明确了企业的算法安全主体责任，并提出了算法管理的要求，虽然现行规则并未对算法管理的规则、算法解释的方式等相关问题做出进一步阐释，但此类基础性要求将推进企业不断提升算法管理和可解释能力。

欧盟《通用数据保护条例》GDPR → **可解释性**

《互联网信息服务算法推荐管理规定》 → **公开算法推荐相关服务规则**

算法管理水平提升

从制度上来讲，《互联网信息服务算法推荐管理规定》明确企业的算法安全主体责任，要求企业建立健全用户注册、信息发布审核、算法机制机理审核、安全评估监测、安全事件应急处置、数据安全保护和个人信息保护等管理制度，制定并公开算法推荐相关服务规则，配备与算法推荐服务规模相适应的专业人员。从技术上来讲，企业也应进一步探索算法管理的技术支撑。此外，《互联网信息服务算法推荐管理规定》还规定了法律责任，如算法推荐服务提供者违反上述相关规定的，法律、行政法规有规定的，依照其规定；法律、行政法规没有规定的，由网信部门和电信、公安、市场监管等有关部门依据职责给予警告、通报批评，责令限期改正；拒不改正或者情节严重的，责令暂停信息更新，并处一万元以上十万元以下罚款。构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。由此，我们理解，依照法律法规制定管理制度，提升算法管理水平，将是相关企业应当完成的合规义务。

算法可解释能力加强

在探索算法管理的过程中，对于以深度学习算法为代表的人工智能算法可解释性问题的探讨不可避免。实践中，已经有企业从业务侧和技术侧思考如何保证算法的透明度，以及受到问询时如何恰当完成算法解释工作，例如在隐私政策或用户协议中适当披露算法服务规则；单独对公众关注的热点算法问题作出单独解释；探索加入拒绝自动化决策的通道等。也有观点提出，监管机构和个人信息主体对于算法透明度的要求和要求获取算法规则解释的目的是不同的。对于不同的主体，可以有针对性地提供不同维度、深度、范围、形式的算法解释，以保证对用户的透明性、配合监管的问询以及保护企业商业秘密。我们理解，探讨研究如何提升算法可解释能力将会形成趋势，从而在产业侧形成推动。

我们建议，除了从政策端了解合规要求外，企业需及时跟进了解国内外先进的算法管理、解释思路和前沿尝试，结合技术侧和业务侧的实际情况，形成一套与企业自身情况相契合的解决方案。

2.11 运用司法诉讼比例将大幅上升

公益诉讼

为非法处理个人信息侵害众多个人权益的行为提供公益诉讼的法律依据，从而**《个保法》**第七十条规定：个人信息处理者违反本法规定处理个人信息，侵害众多个人的权益的，人民检察院、法律规定的消费者组织和由国家网信部门确定的组织可以依法向人民法院提起诉讼。

2021年8月21日最高人民检察院下发**《关于贯彻执行个人信息保护法推进个人信息保护公益诉讼检察工作的通知》**明确“加强个人信息公益保护，是贯彻落实习近平法治思想，推进国家治理，强化法律监督的必然要求，要深刻领会个人信息保护法设置公益诉讼条款的重要意义，……，推动公益诉讼条款落地落实。”

最高人民检察院2020年9月出台**《关于积极稳妥拓展公益诉讼案件范围的指导意见》**，明确将“个人信息保护”作为网络侵害领域的办案重点。

根据最高人民检察院于2021年4月22日发布的11起检察机关个人信息保护公益诉讼典型案例，个人信息保护公益诉讼主要有行政公益诉讼、民事公益诉讼和刑事附带民事公益诉讼三类。**其中行政公益诉讼6起、民事公益诉讼案例2起和刑事附带民事公益诉讼3起**，具体情况如下表：

个人信息保护公益诉讼典型案例

类别	名称	裁判要旨
行政公益诉讼	江西省南昌市人民检察院督促整治手机App侵害公民个人信息行政公益诉讼	针对手机App等互联网软件侵害公民个人信息损害社会公共利益的情形，检察机关督促行政机关依法履职。
	浙江省温州市鹿城区人民检察院督促保护就诊者个人信息行政公益诉讼	针对非法获取就诊者个人信息用于商业营销的市场乱象，检察机关督促行政机关依法履职，加强类案监督，完善社会治理，构建长效机制，形成个人信息保护合力。
	甘肃省平凉市人民检察院督促整治快递单泄露公民个人信息行政公益诉讼	针对快递单直接显示用户个人信息的安全隐患，检察机关督促行政机关加强快递收发前端和末端的监管，避免个人信息泄露风险。
	江苏省无锡市人民检察院督促保护学生个人信息行政公益诉讼	针对校外培训机构非法获取学生个人信息用于营销招生、侵害学生合法权益的行为，检察机关通过诉前磋商和检察建议等方式督促教育行政部门依法履职，保护学生个人信息安全。
	江西省乐安县人民检察院督促规范政府信息公开行政公益诉讼	针对行政机关在履行政府信息公开职能时泄露不应公开的公民个人信息的情形，检察机关通过制发诉前检察建议，依法督促行政机关履职整改，保护公民个人信息安全。
	河南省濮阳市华龙区人民检察院督促整治装饰装修行业泄露公民个人信息行政公益诉讼	针对房地产及装饰装修等行业泄露消费者个人信息、导致大量骚扰电话短信推销的行为，检察机关通过诉前检察建议督促有关部门依法履行监管职责，推动行业治理，切实加强公民个人信息保护。
民事公益诉讼	浙江省杭州市余杭区人民检察院诉某网络科技有限公司侵害公民个人信息民事公益诉讼	针对App违法违规收集、存储个人信息的侵权行为，检察机关在通过行政公益诉讼督促行政机关依法履职的同时，还可以对App服务提供者的侵权行为依法提起民事公益诉讼，要求侵权者承担侵权责任，多维度保护众多不特定用户的合法权益。
	河北省保定市人民检察院诉李某侵害公民个人信息民事公益诉讼	针对非法获取消费者个人信息并进行消费欺诈的行为，检察机关提出惩罚性赔偿诉讼请求，加大侵害消费者个人信息和权益的惩治力度，维护消费者个人信息安全和合法权益。
刑事附带民事公益诉讼	上海市宝山区人民检察院诉H科技有限公司、韩某某等人侵犯公民个人信息刑事附带民事公益诉讼案	针对网络服务提供者、网络用户利用互联网侵犯公民个人信息的犯罪行为，网络运营者未依法履行其社会管理职责的情形，检察机关在提起刑事附带民事公益诉讼时，可以依法追加其为附带民事公益诉讼被告，要求其承担侵权责任。
	贵州省安顺市西秀区人民检察院诉熊某某等人侵犯公民个人信息刑事附带民事公益诉讼案	针对在互联网上非法获取、出售公民个人信息，损害社会公共利益的行为，检察机关在依法追究违法行为人刑事责任的同时，依法提起刑事附带民事公益诉讼，要求其支付赔偿金并公开赔礼道歉。
	广东省广宁县人民检察院诉谭某某等人侵犯公民个人信息刑事附带民事公益诉讼案	检察机关以侵犯公民个人信息刑事附带民事公益诉讼为切入点，通过诉讼判决被告承担停止侵害、消除危险等侵权责任，并督促行政主管部门全面依法履职，以案为鉴推动行业规范治理，全方位保护公民个人信息安全。

2.11 运用司法诉讼比例将大幅上升

民事侵权诉讼

近年来随着个人信息保护相关法律法规的不断完善，民事侵权诉讼的数量也在不断增加，典型案例如下：

2016年某互联网社交平台诉某互联网科技公司案。该案的典型意义在于保护数据开放平台对于用户信息等平台数据的合法权益，本案中二审法院认定，**在 Open API开发合作模式中，第三方通过Open API获取用户信息时应坚持“用户授权”平台1+“平台授权”+“用户授权”平台2的三重授权原则。本案代表了三重授权原则的诞生。**

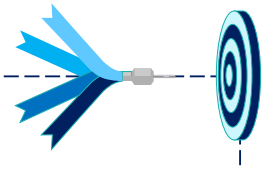
2017年庞某诉某航空公司和某互联网旅行平台案。该案的典型意义在于，二审判决认为：从收集证据的资金、技术等成本上看，作为普通人的庞某根本不具备对二被告内部数据信息管理是否存在漏洞等情况进行举证证明的能力。原告的非隐私信息与隐私信息结合之后已形成不可分的权利整体，应当按照隐私权的保护规则一体救济。被告掌握了原告身份证号、手机号和航程信息，其后，相关信息又在合理时间内发生泄露，根据高度盖然性的证明标准，足以认定信息泄露系被告导致，故二被告构成对原告隐私权的侵犯，应当承担侵权责任。**本案确立了可通过隐私权对个人信息安全予以保护的规则，明确了认定个人信息泄露应适用民事证据高度盖然性证明标准，对规范网络平台行为，维护个人信息安全具有重要意义。**

2019年凌某某诉某短视频平台隐私权、个人信息权益网络侵权责任纠纷案。北京互联网法院将平台未经信息主体同意而进行超过合理期限的存储、未征得信息主体同意的情况下收集信息主体的地理位置信息的行为认定为对信息主体个人信息的侵害。**该案重申了平台在处理个人信息时，必须遵守处理个人信息的必要原则，否则不得援引合理利用作为抗辩理由。**

2019年黄某诉某移动App隐私权、网络侵权责任纠纷案。北京互联网法院首先对读书信息是否属于个人信息，进行了判定，符合一种判定方式的即为个人信息。并进一步认定了**平台收集用户好友列表，向用户并未主动添加关注的好友自动公开读书信息，且未以合理的“透明度”告知用户并获得用户同意的行为构成了对用户个人信息的侵害。**

2020年肖某诉某平台泄露个人信息纠纷案。北京市第四中级人民法院认为，在交易方发生纠纷后，电子商务平台的经营者向交易对方披露其联系方式属于违反广告法泄露了举报信息的行为，判定电商平台应当承担侵权责任。由此，**电商平台处理协查工商调查时，应注意履行广告法规定的相应义务，注意保护举报人的私密信息，并强化其保护个人信息的意识，建立合法、必要、正当使用个人信息的行业规则。**

2021年杭州野生动物世界人脸识别案。法院指出：**人脸识别信息相比其他生物识别信息而言，呈现出敏感度高，采集方式多样、隐蔽和灵活的特性，不当使用将给公民的人身、财产带来不可预测的风险，应当作出更加严格的规制和保护。**原告同意在办卡时拍摄照片，**仅系为了配合指纹年卡的使用，不应视为其已授权同意野生动物世界将照片用于人脸识别。野生动物世界虽自述其并未将收集的照片激活作为人脸识别信息，但其欲利用收集的照片扩大信息处理范围，超出事前收集目的，违反了正当性原则。**



其他典型案例

1. 某公司因拒绝许可数据，被起诉数据垄断；
2. 某网站经营者因爬取微信公众号，被判系不正当竞争，赔偿60万；
3. 某平台通过算法自动化决策进行平台使用方监测与处罚，法院判决认定平台使用方存在违规推广行为，平台有权采取处罚措施；
4. ...

2.12 外部独立第三方监督作用逐渐发挥

《个保法》第五十八条，对于提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者，即**超大型互联网平台**，提出了建立健全个人信息保护合规制度体系，成立主要由外部成员组成的独立监督机构的合规义务。全国人大法工委在新闻发布会上表示，《个保法》的上述规定是为了提高大型互联网平台经营业务的透明度，完善平台治理，强化外部监督，形成全社会共同参与的个人信息保护机制。

目前已有部分企业响应并建立外部监督机构。2021年10月15日，某互联网企业发布招募公告以成立“个人信息保护外部监督委员会”。委员会成员包括法学与技术专家、行业协会代表等个人信息保护领域的专业人士，也将涵盖律师、媒体以及其他公众。同期，另一家互联网平台也在官方微信公众号发布“个人信息保护外部监督专家团”招募公告，明确提出“专家团将独立监督、评估该平台集团及旗下各产品的个人信息保护相关工作，并为其提出指导和修改建议等”。专家团的监督方式包括但不限于日常检查和产品监督、组织专家会议等。

就《个保法》的实施要求来看，外部监督机构可能担任的职责包括：（1）评审隐私政策、平台规则、产品界面隐私设计；（2）审查内部制度是否完备；（3）审查企业是否制订个人信息合规审计报告；（4）参与并听取企业个人信息保护工作报告；（5）参与制订并评议企业个人信息保护社会责任报告；（6）向公众批露企业个人信息保护情况，或者当发现有违法违规行为时，可以要求企业及时整改，或者向有关机构进行举报等。

期待大型互联网平台能够积极探索出适合自身实际需求和形成真正发挥作用的独立、专业的个人信息保护外部监督机构和相应机制。

2.13 企业内部数据合规人才储备需求量翻番

市场需求

与以往仅在通讯企业和头部互联网企业常见的独立数据合规岗位不同，根据市场观察，目前数据合规相关人才需求量翻番，对应岗位呈现出高速增长的态势，各类企业争先聘用专职数据合规人员。

从业人员

数据合规从业者、储备人才数量也不断增长，部分高校设立“数据法学”等相关专业，咨询机构、律师事务所等纷纷成立专门的数据合规团队并配置相应经验的工作人员，可谓“千帆竞发”，但是短期内综合性和高素质的数据合规人才仍然出现供给失衡的状况。以下为我们对培养法律、技术与管理相结合复合型数据合规人才的一些思考。

法律、技术与管理结合的复合型人才

熟悉个人信息保护法和相关规定

- 从理论基础或者研究分析出发，发现问题，提出问题
- 紧跟立法、司法解释、执法实践、标准出台动向

掌握风险管理及产品运营

- 产品思维与运营逻辑的紧密结合
- 前中后端紧密结合，具备提出统一解决方案的能力

了解隐私技术

- 掌握系统架构、数据链路及安全技术的基础知识
- 深入多业务场景，充分考虑隐私保护要求与实际产品需求结合

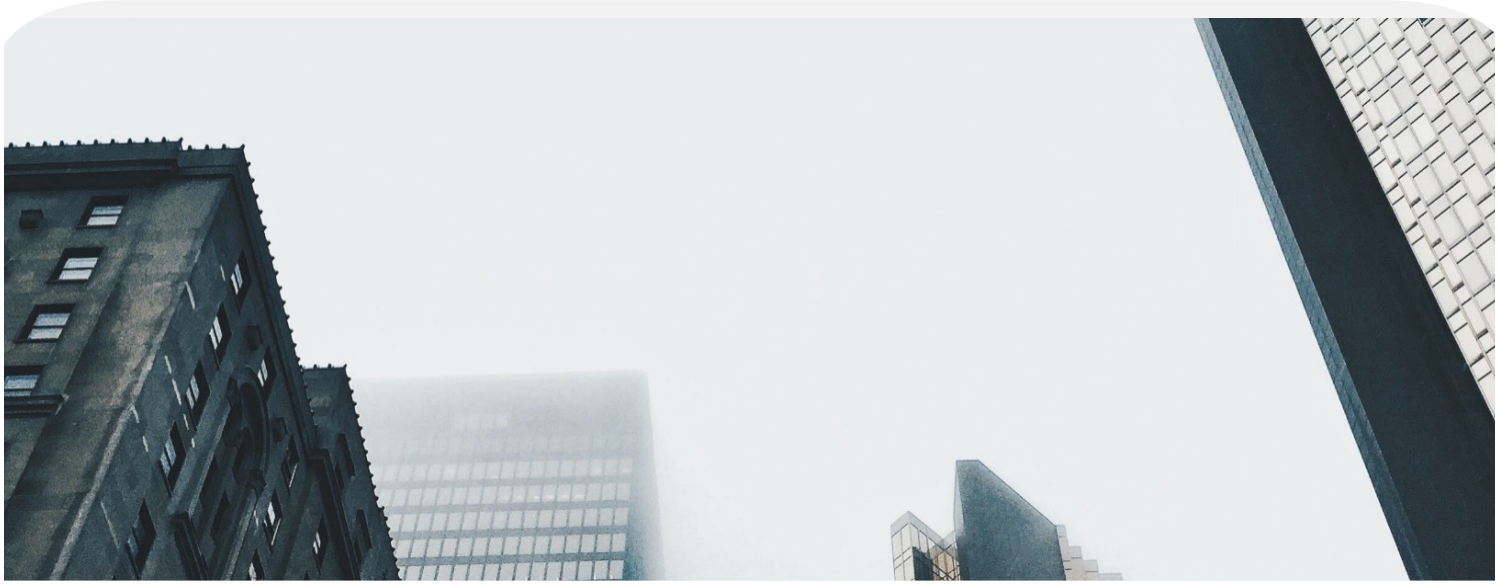
2.14 跨境传输标准合同条款即将出台，可携带权行使规则将进一步明确

中国版标准合同条款

- 我国《个保法》第三十八条规定了数据跨境的四种保护性措施，包括通过国家网信部门组织的数据出境安全评估、国家网信部门认定的专业机构进行的个人信息保护认证、签订国家网信部门制定的关于标准合同和法律、行政法规或者国家网信部门规定的其他条件。
- 我们预测，国家网信部门将会在本年度出台个人信息跨境传输的标准合同条款，企业可密切关注监管部门相关动态并选择最适合本企业的个人信息出境合规机制。对此，以完善个人信息跨境传输的具体制度和流程，企业可以先行了解自2021年9月27日起，欧洲经济区（EEA）实体与欧洲经济区以外实体需要签署的新版本数据跨境转移标准合同条款（SCC）。

可携权之数据向第三方平台迁移

- 根据《个保法》第四十五条，除个人有权获得个人信息副本外，还有权请求数据处理者直接将与其有关的个人信息传输给指定的另一数据处理者。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。
- 建议企业密切关注网信部门发布的有关个人信息向第三方平台迁移的细则，建立并完善可携权响应机制，及时评估并处理用户的数据获取和传输请求，统一数据传输格式，实现互操作与便利性。
- 实现数据可携带权，一定程度上有利于解决大型平台的数据垄断问题，降低数据获取方涉嫌不正当竞争的风险。一旦相关规则更加明晰，各平台逐步实现数据接口互联互通，可携带权的行使规则将会更加明确，在个人信息权益得到保障的同时促进数据市场的信息流动。



2.15 “单独同意”的难点问题有望突破

《个保法》规定了必须取得“单独同意”的五种场景。目前，行业内的普遍做法是在用户触及产品的相关业务功能时，通过弹窗、文字提示且由用户主动填写、阅读说明并主动勾选同意等方式增强告知用户处理其个人信息的详细情况并单项表达同意，在用户未点击同意前，不得处理其个人信息。同时，提供撤回该事项同意的选项。

区别于《个保法》项下一般同意规则，个人信息处理者在下列五种场景下，须将处理目的、行为等单独向个人进行充分告知并取得逐项“同意”。单独同意仅针对单一事项，不得通过一揽子授权的方式取得主体同意。

但是，在程序化广告场景下向第三方提供个人信息时，获得用户单独同意往往变得困难。程序化广告的关键之一在于依托数字化交易平台，对目标用户展开实时的数据收集、挖掘，并根据用户画像进行精准投放。企业往往会采用第三方SDK来监控程序化广告的可见性。对此，企业可尝试参照国外“TCF”框架（Transparency and Consent Framework）设计产品交互界面向用户披露第三方信息，并征得单独同意。例如，给予用户一键同意或一键拒绝向第三方共享个人数据请求的选择，也同时保证用户可以针对单个第三方，进一步作出是否向其共享个人数据的细化同意选择，这样一来避免出现获取用户一揽子授权同意的情形。

在向境外提供数据方面，如何获取用户的单独同意也是一个实践难点。例如，在使用产品的过程中应当何时获取用户对个人信息出境的单独同意，同时不会导致用户使用体验大打折扣，这是企业常常遇到的问题。**对此，我们目前建议的实践解决方案有二：**

- **在用户首次使用产品时，在用户勾选同意隐私政策下方加入个人信息出境告知说明，由用户同时进行主动勾选同意；**
- **在用户同意隐私政策后，具体触及需要向境外提供个人信息的功能时，再弹窗询问用户是否同意个人信息出境；**
- **当用户不同意时，企业也需考虑在境内设立服务器存储数据的问题。**

1. 向其他个人信息处理者提供其处理的个人信息
2. 向境外提供个人信息
3. 处理敏感个人信息
4. 公开个人信息
5. 公开或向他人提供公共场所收集的个人图像/身份特征信息

2.16 有望针对儿童监护人身份认证机制提出新的有效解决思路

国内对儿童隐私保护的监管呈现出越来越严格的趋势

目前法律法规要求企业在收集和处理儿童个人信息时，征求其监护人的同意。实践中，企业在落实获取监护人同意这一项法律合规要求时，如何设置监护人认证机制成为一大难点。

探索

2021

我国第一部专门针对儿童网络保护的立法——《儿童个人信息网络保护规定》，于2021年10月1日起施行，对于在中国处理不满十四周岁的儿童个人信息进行规范。

强化

2021

《个保法》第三十一条明确，个人信息处理者处理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同意。

法规名称	具体条款
《信息安全技术 个人信息安全规范》	5.4 收集个人信息时的授权同意 对个人信息控制者的要求包括： c) 收集**年满十四周岁未成年人**的个人信息前，应征得**未成年人或其监护人的明示同意**；**不满十四周岁**的，应征得其**监护人的明示同意**；
《儿童个人信息网络保护规定》	第七条 网络运营者收集、使用**儿童个人信息**的，应当以显著、清晰的方式告知儿童监护人，并应当征得儿童**监护人的明示同意**。明示同意应当具体、清楚、明确，基于自愿。

强化

2020

2020年12月26日，《中华人民共和国预防未成年人犯罪法》修正案通过。

发展

2020

2020年10月17日，全国人民代表大会常务委员会通过《中华人民共和国未成年人保护法》修正案，其中专设了第五章“网络保护”。

法规名称	具体条款
《数据安全管理办法（征求意见稿）》	第十二条 收集**十四周岁以下未成年人**个人信息的，应当征得**其监护人同意**。
《未成年人保护法》	第七十二条 处理**不满十四周岁未成年人**个人信息的，应当征得未成年人的**父母或者其他监护人同意**，但法律、行政法规另有规定的除外。

发展

2019

2019年11月5日，国家新闻出版署下发了《关于防止未成年人沉迷网络游戏的通知》。

初步

2019

2019年5月28日，网信办发布《数据安全管理办法（征求意见稿）》规定了收集儿童个人信息应取得监护人同意的要求。

Start Here

环球律师事务所 GLOBAL LAW OFFICE

2.16 有望针对儿童监护人身份认证机制提出新的有效解决思路

合规要求

01 开发适合未成年人使用的模式；

02 获得监护人的同意；

03 设置专门的儿童个人信息保护规则和用户协议；

04 指定专人负责儿童个人信息保护；

05 用加密等措施存储儿童个人信息。

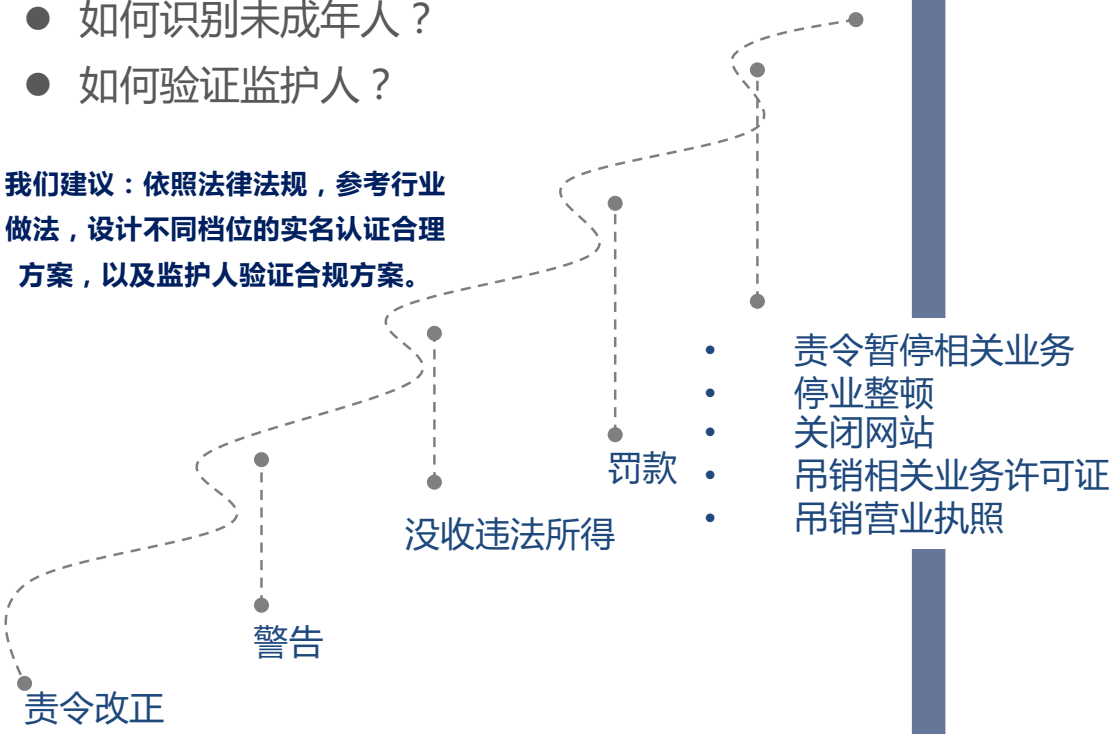
我们观察到，行业已对此作出探索，比如某通讯软件近期新增监护人授权功能，但对于如何确认设置青少年模式的“家长”身份，依然需要进一步研究并形成解决方案。

我们期待，在2022年，监管部门能够给出推荐方案，行业也能形成良好实践，通过家长监护切实保护未成年人的权益。

合规难点

- 如何识别未成年人？
- 如何验证监护人？

我们建议：依照法律法规，参考行业做法，设计不同档位的实名认证合理方案，以及监护人验证合规方案。



2.17 新技术新应用领域（如NFT、区块链等）提出数据合规新问题

技术推动社会更加快速地进步，但随之而来的各类新型网络安全事件，让各国政府意识到新技术新应用领域（如人工智能、云计算、物联网、NFT、区块链、大数据等）有关网络安全和数据保护的重要性。国际上，部分新技术新应用发展较快的国家，如美国、欧盟等已经出台了相关规则或白皮书，以规范相关行业的数据保护和网络安全。

目前，我国虽然尚无专门规制新技术新应用的法律法规，但相关新技术新应用的国家标准与行业标准已经陆续出台并形成体系。

我们理解，新技术新应用领域的数据合规将会被提到更加重要的高度。

例如，《区块链信息服务管理规定》对区块链合规提出了如下要求：

技术

具备与其服务相适应的技术条件、技术方案应当符合国家相关标准规范。目前国家对区块链相关标准多在制定阶段，建议企业关注相关标准的出台，及时比标并做好合规工作。

评估

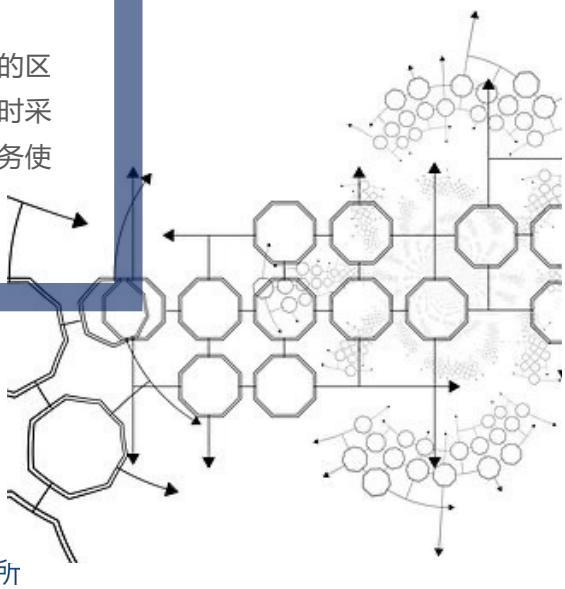
开发上线新产品、新应用、新功能，应当按照有关规定报国家和省、自治区、直辖市网信部门进行安全评估。

备案

通过网信办区块链信息服务备案管理系统，履行备案手续。对外提供服务的互联网站、应用程序等的显著位置标明其备案编号。

备份

对违反法律、行政法规规定和服务协议的区块链信息服务使用者及违法信息内容及时采取相应的处理措施，并对区块链信息服务使用者进行记录备份。



2.18 数据作为反制措施之一，需要各方权力动态平衡与力量把控

01 中美对抗深入

美国在技术领域通过出口管制实体清单对中国多家公司和机构进行进一步的封锁。

02 美国打击中国科技企业

美国曾试图以数据安全和国家安全等理由对我国某企业旗下的头部互联网应用进行强制出售。

03 “清洁网络”行动

美国取消中资运营商企业在美运营牌照。

04 限制中国企业融资

根据《外国公司问责法》，从2021年7月起停止处理中国企业在美国上市的申请，要求其向美国公众公司会计监督委员会提供审计底稿。

05 我国反制措施

《数安法》第二十六条和《个保法》第四十三条均规定我国可以对他国歧视性禁止或限制措施采取对等反制措施。

两部法律当前尚未对“歧视性”措施进行定义，保留了实际执行法律时的弹性空间。

此外，针对美国通过CLOUD法案，利用该国网络服务商在全球的优势地位，收集服务商控制下在境外服务器储存信息的意图，我国《数安法》第三十六条和《个保法》第四十一条明确规定，非经批准，中国境内的组织、个人不得向外国司法或者执法机构提供存储于中华人民共和国境内的数据。

- 美国不断试图巩固其网络信息领域的霸权地位的行为，和我国出自保护国家安全、社会和人民福祉利益为目的而采取的反制措施，必然在可见的将来，在高科技和需要高度依赖数据的其他领域持续产生冲突与竞争。

- **跨国企业需要对相关法律法规和执法动态保持关注，对自身的数据收集和存储策略进行妥善安排和合规，对可能出现的冲突场景有预案，以避免陷入两难的境地。**

2.19 除保护用户个人信息，将保护员工、合作伙伴联系人信息排上日程

个人信息保护贯穿个人信息全生命周期的方方面面，而在《个保法》出台前，企业进行数据治理及个人信息保护工作的着眼点主要在于保护用户、消费者的个人信息及合法权益，以求减少争讼的发生；而《个保法》出台后，其不仅在《民法典》的基础上对个人信息的定义、处理活动、个人信息主体的主要权利、义务等方面做出细化规定，更是将《民法典》中针对员工个人信息权益的精神落到实处，引起了企业的广泛重视。**不仅如此，企业还逐渐认识到，不单单是员工的个人信息，企业在商务合作过程中收集到的合作伙伴、供应商的联系人个人信息，均应当纳入到企业个人信息合规整体框架中。**

以员工个人信息为例，企业处理员工个人信息时是否满足“为按照依法制定的劳动规章制度和依法签订的集体合同实施人力资源管理所必需”的合法性基础；如果处理的员工个人信息并非属于“实施人力资源管理所必需”的范围，那么处理员工敏感个人信息的，或者将员工个人信息提供给诸如商业保险供应商、差旅报销系统供应商等第三方机构，是否需要获取员工的单独同意；对于外企来说，如果存在员工个人信息出境的情形，企业是否满足了出境的条件、是否遵守了数据出境的评估申报流程和员工的单独同意等，这些都是企业开始逐渐关注和必须重视的实践问题。**必要时，企业应及时咨询专业律师，以确保在充分理解相关法律要求同时，正确有效地履行合规义务。**

Part
03

附录
2021监管与执法动态汇总

各监管机构执法动态综述

以 App 监测为主

监管部门除了对App进行评测以外，也对小程序进行了评测。《App个人信息安全防范指引（征求意见稿）》《常见类型移动互联网应用程序必要个人信息范围规定》均明确，App是指安装、运行在智能移动终端上的应用软件，包括在应用市场上架的软件、移动智能终端预装的软件、小程序等。**我们提示企业注意，小程序也适用移动应用程序的监管程序，故App合规要求同样适用于小程序。**App运营主体使用SDK时应当做好评估与审查工作，一旦APP接入的SDK存在问题，除第三方SDK与用户单独授权获取用户信息外，第一责任主体为App运营主体。例如，App 嵌入含有恶意代码的第三方 SDK，可首先追究APP运营者的责任，App运营者和SDK提供者对用户损失承担连带赔偿责任。

工信部2021年10月15日的通报显示，三家头部互联网平台广告SDK问题较多，分别占问题总量比例的37.4%、29.9%、8.0%，虽此次通报暂未公布SDK涉及的具体问题，我们还是建议企业关注SDK的合规情况。

对某网约车平台、某货运平台、某某某互联网招聘平台等 4 平台开展网络安全审查

《网络安全审查办法》明确规定，“网络安全审查”**坚持防范网络安全风险与促进先进技术应用相结合、过程公正透明与知识产权保护相结合、事前审查与持续监管相结合、企业承诺与社会监督相结合，从产品和服务以及数据处理活动安全性、可能带来的国家安全风险等方面进行审查。**

从App监测到网络安全审查，可以看出监管部门的执法关注点发生变化：

- 从侵害用户权益专项整治，逐渐转向于全面网络安全合规整治工作；
- 从前端技术性检测到后端全面性审查。

工信部执法动态

第一阶段

《关于开展App侵害用户权益专项整治工作的通知》（337号文）2019.11.04

处置原因

违规收集用户个人信息
- 私自收集
- 超范围收集

违规使用用户个人信息
- 私自共享给第三方
- 强制用户使用定推功能

不合理索取用户权限
- 不给权限不让用
- 频繁申请权限
- 过度索取权限

为用户账号注销设置障碍
- 注销难

处置措施：

责令整改、向社会公告、组织App下架、停止App接入服务、纳入电信业务经营不良、失信名单

第二阶段

《关于开展纵深推进App侵害用户权益专项整治行动的通知》(164号文）2020.07.24

处置原因

App、SDK违规处理用户个人信息方面
- 违规收集个人信息
- 超范围收集个人信息
- 违规使用个人信息
- 强制用户使用定向推送功能

设置障碍、频繁骚扰用户方面
- App强制、频繁、过度索取权限
- App频繁自启动和关联启动

欺骗误导用户方面
- 欺骗误导用户下载App
- 欺骗误导用户提供个人信息

应用分发平台责任落实不到位方面
- 应用分发平台上的App信息明示不到位
- 应用分发平台管理责任落实不到位

整治对象：
- App、SDK、小程序
- 应用分发平台，如应用商店

工信部执法动态

全方位一体化整治

第三阶段

《移动互联网应用程序个人信息保护管理暂行规定》

部门规章、效力层级更高

- App（第八条、第九条）

知情同意、最小必要

- App开发运营者义务（第十条）
- App分发平台，如应用商店、网站（第十一条）

规定6项义务：包括在显著位置说明App申请的权限列表、隐私政策、不得欺骗误导用户下载App等。

- 第三方SDK（第十二条）

规定5项义务：包括：制定并公开隐私政策、未经用户同意或在无合理业务场景下，不得自行进行唤醒、调用、更新等行为，未经用户同意，不得将收集到的用户个人信息分享转让等。

- 移动智能终端生产企业，如手机厂商（第十三条）

规定6项义务：包括及时弥补权限管理漏洞、建立终端启动和关联启动App管理机制，为用户提供关闭自启动和关联启动的功能选项。

- 网络接入服务提供者，如IDC服务提供者、ISP服务提供者、CDN服务提供者（第十四条）

规定了2项义务：如依法对违规App采取停止接入等必要的措施，阻止其继续违规侵犯用户个人信息。

工信部执法动态

第四阶段

工信部App侵害用户权益“回头看”专项

三次“回头看”共通报95款App

七月
2021年第7批
App开屏弹窗信息骚扰用户问题
1

八月
2021年第8批
App违规调用通信录、位置信息以及开屏弹窗骚扰用户等问题
2

九月
2021年第11批
App超范围索取权限、过度收集用户个人信息等问题
3

“回头看”是指

03 App曾被工信部通报或地方通管局通报

02 App未被通报，但属于不同公司主体的同名App曾被通报

01 App未被通报，但其所属公司主体的企业App曾被通报

注意要点：

1. 在隐私政策中须向用户告知个人信息处理规则；向用户提供**App隐私政策摘要**。
2. 涉及调用用户终端中**相册、通讯录、位置等敏感权限**的，应当通过适当方式，如**通过蒙层、顶栏浮窗等，在服务场景实际发生时同步向用户告知调用权限的目的**。
3. 开屏弹窗信息展示方式上，不得出现“**广告标识近于无形、关闭按钮小如蝼蚁、页面伪装瞒天过海、诱导点击暗度陈仓**”等违规行为。
4. App开屏信息和弹窗信息窗口应**设置明显、有效的关闭按钮**；不得使用整屏图片、视频等作为跳转链接。
5. 建立已收集**个人信息清单和与第三方共享个人信息清单**。

工信部将建立跟踪、约谈、排名、社会公示机制，及时交流、推广典型案例和成功做法

《工业和信息化部关于开展信息通信服务感知提升行动的通知（工信部信管函〔2021〕292号）》

信息通信服务感知提升行动

工信部执法动态

工信部一般执法流程

检测 → 通报 → 下架

5个工作日内
未完成整改

5个工作日内
未完成整改

40个工作日内
不得重新上架

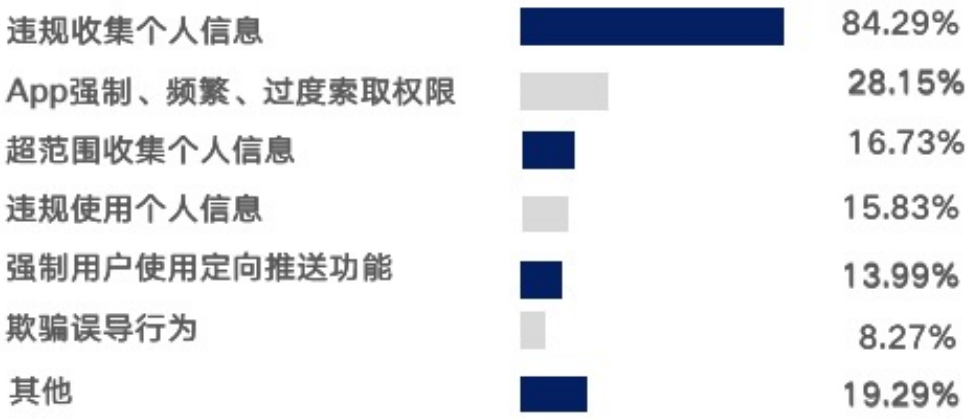
工信部“回头看”执法流程

- 直接通报+**5个自然日内**整改不到位下架。
- 问题严重的（反复出现问题、技术对抗、要求整改未整改）：**直接予以下架 +可能会有相应的行政处罚措施。**

2021工信部通报App情况

2021年共有1680款App被工信部通报

主要问题

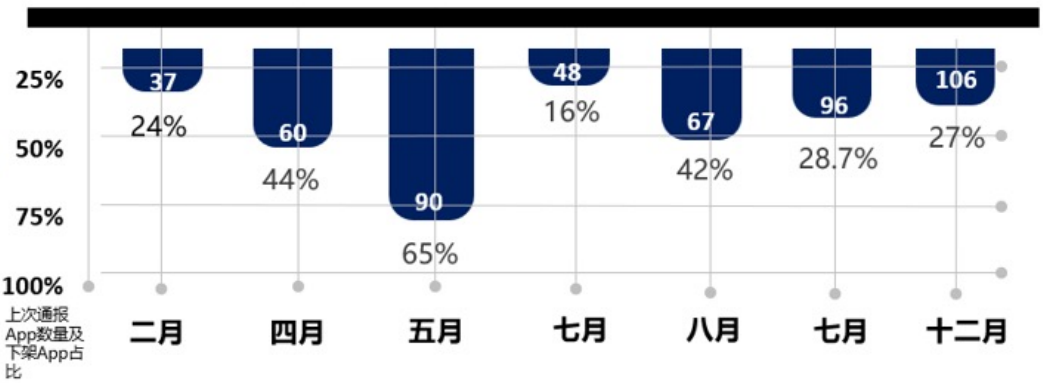


注：同一App常有多个问题

2021工信部下架App情况

2021年共507款App被工信部下架

下架比例



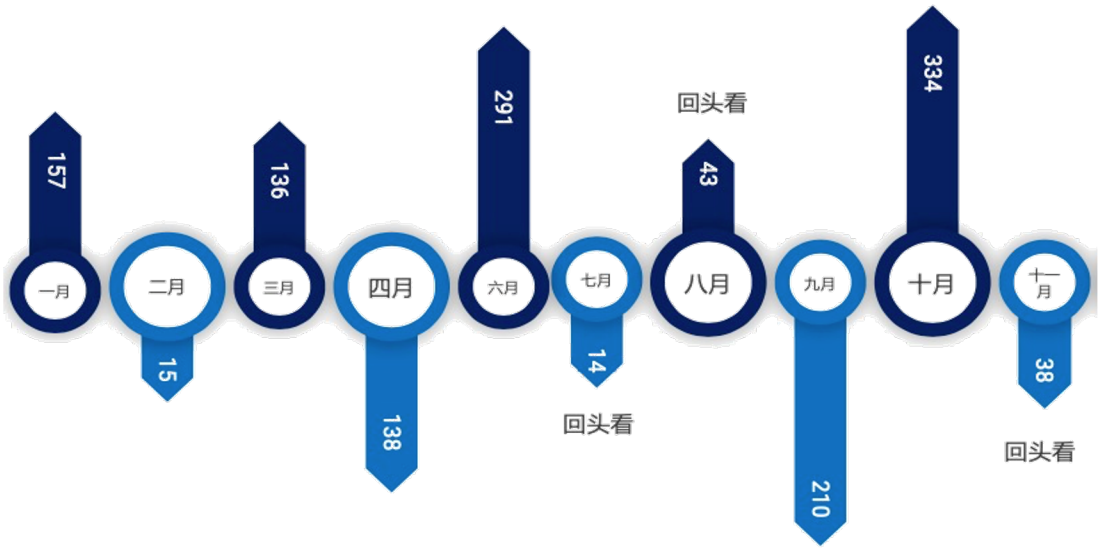
注：以上数据来源于对工信部通报公告信息的汇总

工信部监管动态

工信部地方通管局重点关注地区前四名

	通报频率	通报App数量
浙江省	5	260
广东省	3	242
上海市	4	138
四川省	4	78

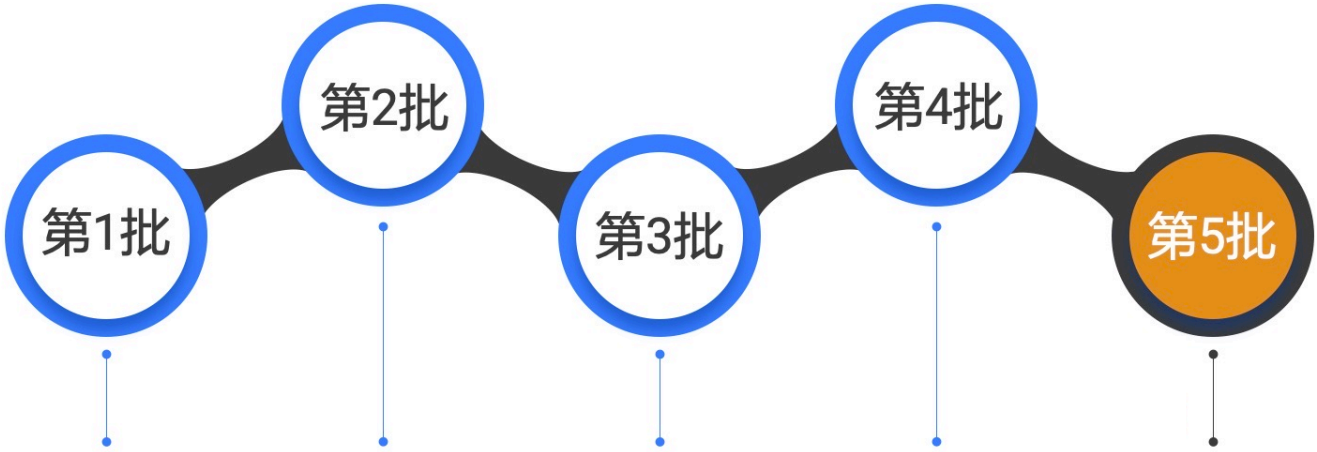
注：以上数据来源于对工信部通报公告信息的汇总



2021年工信部共通报 11 批次，平均每月有 127 个App被通报，并进行了 3 次回头看。

网信办执法动态

2021年网信办共通报 5 批次
共有 695 个App被通报，平均每批通报 73 个



	第1批	第2批	第3批	第4批	第5批
	2021年5月1日	2021年5月10日	2021年5月21日	2021年6月11日	2021年7月9日
	输入法类、地图导航类、即时通讯类	安全管理类、网络借贷类	短视频类、浏览器类、求职招聘类、实用工具类，包括抖音、快手等头部App	运动健身类、新闻资讯类、网络直播类、应用商店类、女性健康类、网络购物类、学习教育类、婚恋相亲类。	均为某出行平台产品，此批未列明具体通报事由
通报App数量	22	84	105	129	25

其中：

约**55%**的通报原因是：**违反必要原则，收集与其提供的服务无关的信息**等；

约**30%**的通报原因是：**未经用户同意收集使用个人信息**；

其他15%的原因有：未按法律规定提供删除或更正个人信息功能、诱导用户授权其读取手机通讯录信息并向通讯录联系人发送营销短信；未公开收集使用规则；未按法律规定提供删除或更正个人信息功能等；未公开收集使用规则；严重违法违规收集使用个人信息等。

地方网信重点关注三个地区

省份	被通报App数量
浙江省	260
江苏省	242
海南省	18*

根据目前汇总的监管通报数据，地方监管通常依据App运营者注册地进行通报，而各地监管的活跃度相差很大，其中最为活跃和值得关注的是浙江省。

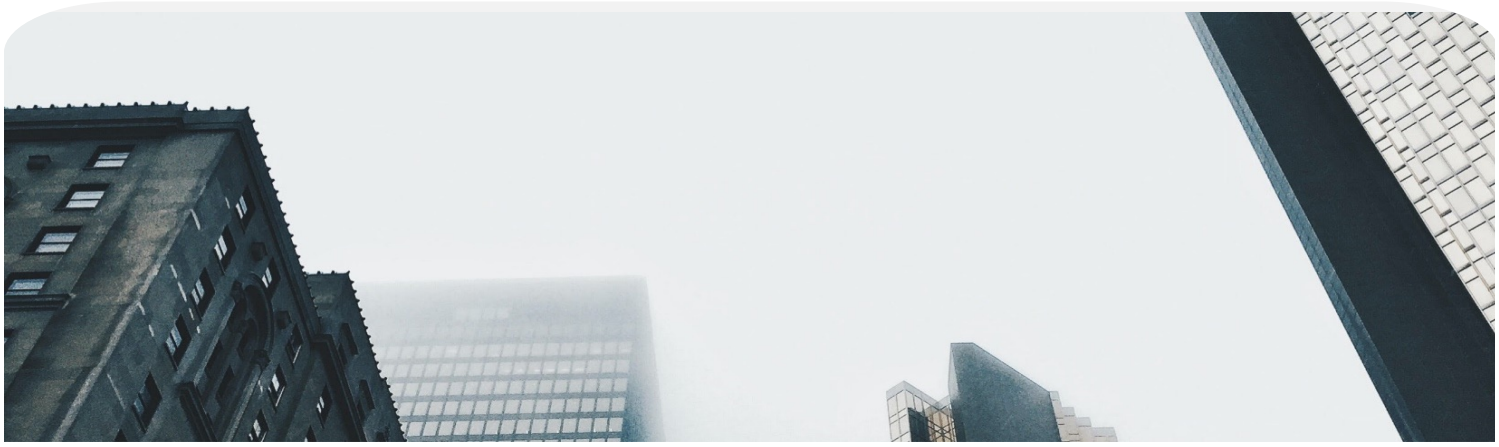
注：以上数据来源于对网信办通报公告信息的汇总
*** 包含7款小程序**

网信办执法动态

地方网信通报数量		国家网信办通报数量	含有该问题App的比例*
180	违反必要原则，收集与其提供的服务无关的个人信息	259	63.17%
147	未经用户同意收集使用个人信息	153	43.17%
213	未提供法定信息	30	34.96%
222	存在引起个人信息泄露的安全漏洞等		31.94%
68	未按法律规定提供删除或更正个人信息功能或投诉渠道	38	15.25%
19	其他	2	3.02%

* 同一App常有多个问题

注：以上数据来源于对网信办通报公告信息的汇总



其他专项整治行动

2021年工信部、网信办共展开多项专项整治活动

01

2021年5月 对摄像头偷拍人脸进行集中整治行动

- 中央网信办与工信部、公安部、市场监管总局

02

2021年7月 互联网行业市场秩序专项整治行动

- 工信部：严查扰乱竞争秩序、侵害用户权益、威胁数据安全、违反资质和资源管理规定等社会高度关注的重点问题

03

2021年8月 清朗·移动应用程序PUSH弹窗突出问题专项整治

- 中央网信办：解决移动应用程序PUSH弹窗违规推送、过滥推送等扰乱网络传播秩序问题

04

2021年9月 信息通信服务感知提升行动

- 工信部：包含三个方面共十项重点任务，提出了推动实现服务举措“五优化”，建立个人信息保护“双清单”，实现服务能力“四提升”要求，简称“524”行动

其他

2021年国家计算机病毒应急处理中心共通报 11 批次，
共有 243 个App被通报

2021年中国消费者协会共通报 1 批次，
共有 24 个App被通报

中国消费者协会的检测和通报重点关注**App账号注销**和**自动化推荐退订测评**两项。

CLOSING

结束语

迈向成熟的数据合规年

2021年是数据合规成长的一年，伴随着政府机构、企业组织、广大用户一路走来，确立了以法律为骨架、技术为肌肉、管理为躯干、意识为血液、经验为灵魂的数据合规方法论，并且能够清晰地展示出来，并被社会广泛认可。

2022年，我们将迈向数据合规成熟的一年。各行各业应更加明确自己的位置，懂得自己的责任，确信自身的价值，更加坦然地迎接数字经济时代的各种机遇与挑战。

环球数据合规团队 编制

主编： 孟洁
邮箱/E. mengjie@glo.com.cn
电话/T.（86 10）6584 6768
手机/M.（86 10）158 1105 0850

参编：
姚牧之、王程、戴畅、
高亚鹏、董杰睿、赵琳琳

订阅/E.
dataprotection@glo.com.cn

请您知悉，本报告的所有内容均不构成任何形式的法律意见。

如您欲进一步了解本报告所涉及的内容，您可以通过上述方式联系我们。

主编简介

孟洁

孟洁 | 合伙人
环球律师事务所
mengjie@glo.com.cn

执业资格
中国执业律师

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、个人信息与隐私保护、互联网、电商合规、反腐败反商业贿赂合规、垄断与不正当竞争合规。

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。曾经及目前向大型跨国公司及知名互联网企业、车企、IoT、电信、云服务、人工智能、电商、金融、医疗、工业互联网、广告、大数据等领域的国内外企业提供境内/境外的数据合规体系建设与数据合规专项及常年法律服务，总结出不少可落地的实操方法论，颇受客户好评。

孟律师曾是国际隐私保护协会（IAPP）中国区联席主席，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Legal Band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。

孟律师在各大期刊、公号发表过数百篇专业文章、著作，并且，与中国信息通信研究院合著《SDK安全与合规白皮书》V1.0版与V2.0版，与中国信息通信研究院和南都个人信息保护研究中心共著《个性化展示安全与合规报告》，与威科数据库合作出版《数据全球化与隐私保护指引》《个人信息保护监管要求比标分析报告》，与小米集团合作发布《Cookie合规指引报告》，与微软公司合作发布《国内外标准兼容下的个人信息合规体系建构》。近期，《新技术新应用数据合规指引》《致礼2022成熟的数据合规年——监管动态总结与趋势预判》《从TCF框架看单独同意获取的落地方式》等报告也将陆续发布。

环球律师事务所

环球律师事务所由中国国际贸易促进委员会在1979年创建，是中国改革开放后成立的第一家律师事务所。经过四十多年来的不懈努力和发展，我们已成为中国律师业中最优秀的大型综合性律师事务所之一。

自成立伊始，我们即确立了“以国际化的视野、国际化的团队、国际化的质量服务于国内外客户”的宗旨，这使我们虽置身于多变的全球经济形势之中，却始终能够保持不变的业界领先地位。我们连续多年被众多的国内外权威法律评级机构评选为顶级的中国律师事务所之一，包括《钱伯斯》、《法律500强》、《亚洲法律杂志》等。

我们的律师均毕业于中国一流的法学院，其中绝大多数律师拥有法学硕士以上的学历，多数律师还曾学习或工作于北美、欧洲、澳洲和亚洲等地一流的法学院和国际性律师事务所，部分合伙人还拥有美国、英国、澳大利亚、瑞士、新西兰、香港等地的律师执业资格。

我们能够为来自广泛行业的国内外客户，提供跨业务领域综合的一站式法律服务。我们深耕的行业包括但不限于银行、金融、保险、证券、投资、贸易、能源、矿业、化工、钢铁、制造业、交通运输、基础及公共设施、生命科学及医疗、电信、传媒、高科技、文娱体育、房地产、酒店休闲、餐饮、大消费等众多的细分领域。

四十多年来，我们凭借精湛的法律知识、丰富的执业经验、高度的敬业精神以及良好的职业道德，向国内外客户展示和证明了我们的价值，同时也赢得了国内外客户的信赖。在未来的日子里，我们将继续凭借我们独到的优势助力国内外客户取得更为持久和长远的成功。

北京总部　上海办公室　深圳办公室　成都办公室

中国领先的律师事务所
逾700名专业律师

环球监管与合规业务

- 作为该领域最佳律师事务所之一，我们在法律风险评估、合规政策制定、合规培训、合规调查以及违规举报等方面具有丰富的经验，能够提供客户在合规与风控方面所需要的所有法律服务。我们能够帮助企业、金融机构、专业服务机构、政府和非政府组织以及企业家发现行业及法律监管方面的漏洞，理顺监管和报告体系，制定并落实有效的预防措施。当客户面临监管机关的调查时，我们能够在第一时间内指导客户依法有效地应对调查。

- **我们能够帮助客户建立有效的合规与风控体系。**我们能够帮助企业、金融机构、专业服务机构、政府和非政府组织以及企业家发现行业及法律监管方面的漏洞，理顺监管和报告体系，制定并落实有效的预防措施。同时，我们能够通过对风险的预判、分析、处置，为企业建立有效的法律风险控制体系，控制或降低企业运营、流程操作中存在的潜在风险，帮助企业提高防范和化解法律风险的能力，保障企业高效稳健安全运营，提高经营管理水平，增强竞争力。

- **我们能够帮助客户依法应对各种法律风险事件和法律合规调查。**企业一旦出现相关风险事件，我们将会在第一时间介入和分析，从而提出解决方案和媒体沟通方案。发现和核实企业内部风险事件的线索，协助企业进行日常的合规调查和处理。当客户面临监管机关的调查时，我们能够在第一时间内指导客户依法有效地应对调查。

- **我们能够为企业的合规与风控工作提供全面而及时的法律信息服务支持。**我们可以帮助企业收集相关行业领域新出台的法律法规和相关负面新闻。例如，在央视3·15后，紧急开展对相关监管信息的研判，帮助被点名企业顺利完成整改合规工作等；在《常见类型移动互联网应用程序必要个人信息范围规定》以及主管部门的整改通知发出后，预先将有关分析报告递交相关客户，协助客户有效改进数据合规落地工作，在关键时刻作客户的坚强后盾。

环球网络安全与数据合规业务

- **境内、外丰富的数据合规经验。**团队律师们长期从事各国数据保护法的实务与研究，曾经翻译过美国、欧盟、印度、巴西、俄罗斯等国的数据保护法案，撰写过大量数据与隐私保护方面的专著与文章。已经完成的数据合规项目涵盖了广泛的行业，包括互联网、通讯、IoT（含车联网）、媒体内容、文化娱乐、银行、保险、投资担保公司、金融科技、医疗健康与医药、教育、汽车（自动驾驶）、电器、制造业等。代表中国企业“走出去”项目中涉及支持境外法域数据合规的国家已经多达三十几个，帮助客户搭建及完善全球统一化的数据合规体系。

- **企业内、外部的数据合规经验。**我们的团队律师有1/3曾在企业法务从事企业内部产品研发和运营合规工作的实务经验。并且，他们在公司内部从事法律工作。我们对公司一线业务有更为深入的认知，能够更清晰明确地了解客户的实际需求，为我们的客户提供更贴合业务实际情况的个性化法律服务，从而指导企业如何进行合规落地，为客户提供满足其商业运营需求和产品与技术结合发展需要的优质法律服务。

- **前、中、后端相结合的数据合规经验。**我们的合伙人深入一线积极参与各法律法规的征求意见反馈及标准的制定，熟谙前沿法规政策动态，与国家和地方政府机构有良好的沟通咨询与磋商经验。我们还有长期战略性合作的外部技术专家与PR专家团队，可协同提供专业的数据合规技术服务与数据危机处理的整体化解决方案。

- **面向技术和产品落地方案实现的合规建议。**环球律师事务所是标准化制定组织TC260成员单位之一，积极参与各项标准的立项与制定的讨论，有着行业内领先的解决问题的能力。我们与中国信息通信研究院建立长期合作关系，如您需要提供技术支持/测评时，信通院将与我们提供一体化的解决方案。

- **快速高效响应客户需求。**我们的律师团队在业内以“提供服务时反应迅速”而闻名。我们的客户普遍对我们提供服务时反应速度之快感到满意。我们十分清楚地认识到，客户的任何需求都期待我们在第一时间给予答复和反馈。我们也意识到，只有以最快的反应速度来提供法律服务才是赢得市场的最好法宝和回报客户对我们的信任的最佳方式。因此，我们的服务宗旨是在力所能及的范围内、以最快的反应速度向客户交出满意的“答卷”。在我们“以非常快的速度”来回应客户的法律需求的同时，我们所提供的法律服务仍然可以达到优秀的水平。

环球律师事务所

2021年度业界嘉许

- 通信媒体业务位列“领先的中国律师事务所”，《钱伯斯亚太》
- 科技、媒体与通信业务位列“领先的律师事务所”，《亚太法律五百强》
- 科技、媒体与通信业务位列“领先的中国律师事务所”，《LEGALBAND》
- 科技与电信业务位列“领先的中国律师事务所”，《亚洲法律概况》
- 媒体及娱乐业务位列“领先的中国律师事务所”，《亚洲法律概况》

- 数据保护业务位列“领先的中国律师事务所”，《亚太法律五百强》
- 网络安全与数据业务位列“一流的律师事务所”，《LEGALBAND》

该团队活跃于TMT领域，运用其丰富的私募股权融资经验，为高科技等企业就各类并购和投融资业务提供全方位的法律服务。并在数据保护和隐私方面提供专业的法律服务。

——《钱伯斯亚太2021》

给一位客户留下深刻印象：“他们在文件起草及审查、尽职调查方面一丝不苟。”

——《钱伯斯亚太2021》

环球律师事务所

Chambers AND PARTNERS

数据保护业务位列“领先的中国律师事务所”

《亚太法律五百强》
2021

THE LEGAL 500

合规业务位列
“领先的中国律师事务所”

《亚太法律五百强》
2018 - 2020

asialaw PROFILES

合规业务位列
“领先的中国律师事务所”

《亚洲法律概况》
2019 - 2022

CHINA BUSINESS LAW JOURNAL 商法

荣获“年度卓越律所大奖
——企业合规”

《商法杂志》
2020

CHINA BUSINESS LAW JOURNAL 商法

荣获“年度卓越律所大奖
——反腐败及合规”

《商法杂志》
2019

LEGALBAND

合规业务位列
“一流的中国律师事务所”

《LEGALBAND》
2021

LEGALBAND

合规业务位列
“顶级的中国律师事务所”

《LEGALBAND》
2020

LEGALBAND

合规业务位列
“领先的中国律师事务所”

《LEGALBAND》
2016 - 2019

LEGALBAND

网络安全与数据业务业务位列
“一流的中国律师事务所”

《LEGALBAND》
2019 - 2021

ASIAN LEGAL BUSINESS

TMT业务提名
“年度沿海地区科技、媒体与电信律师事务所大奖”

《亚洲法律杂志》
2021

ASIAN LEGAL BUSINESS

合规业务提名
“年度沿海地区合规律师事务所大奖”

《亚洲法律杂志》
2021

ASIAN LEGAL BUSINESS

合规业务提名
“年度最佳合规律师事务所大奖”

《亚洲法律杂志》
2014 – 2016、2018 - 2021

环球网络安全与数据合规业务

成功案例及既往业绩

国内某知名物联网科技公司

- 受国内某知名物联网科技公司委托，提供上市前数据合规治理法律服务。该企业产品形态较为丰富，所开发的平台复杂且数量较多，夹杂定制与非定制的内容。所持有的信息包含个人信息、重要数据等内容。项目整体综合性与复杂性较高。在本项目中，我们首先对集团旗下的各业务线进行梳理，分析数据全生命周期的合规性以及业务合规性，就数据法律问题出具法律意见、协助公司制定数据安全相关的内部规章制度、审阅起草公司合同、代表公司进行谈判磋商、以及协助公司了解境内外数据合规的监管动态等。由于该企业属于交通物流领域，在滴滴事件后，该企业上市可能会受到监管的压力与资本市场的双重压力。因而对时间和反馈文件质量的要求均较高，我们高效且高质量的服务得到了客户的高度评价。

国内知名二手车交易平台

- 受某国内知名二手车交易平台委托，作为其外部法律顾问为其提供常年数据合规和互联网法律方面的法律服务。在日常法律服务中，协助其建立各类平台，基于不同业务场景制定各平台及集团相关数据合规体系。同时，我们也协助其开展并办理了安全评估资质审查工作、平台支付流程与合规评估、知识产权问题、平台反垄断评估、平台所有协议起草、精准营销的法律合规处理，并根据最新法律法规要求及实践需要，为其提供整套合规制度以及培训在内的全套内部合规体系。在上市过程中，我们根据上市要求，为其提供数据合规咨询法律服务。

国内头部互联网健身平台

- 受国内头部互联网健身平台委托，作为其外部法律顾问，为其数据合规业务提供全方位的法律服务，包括协助对公司的数据保护状况进行摸底排查、就数据法律问题出具法律意见、协助公司制定数据安全相关的内部规章制度、审阅起草公司合同、代表公司进行谈判磋商、以及协助公司了解境内外数据合规的监管动态、产品出海以及数据合规审查的专业法律支持。与安全咨询公司一起合作，为客户提供前、中、后端全方位的法律服务，协助客户进行风险识别并进行整改，包括法规、技术、制度等多层次的内容。同时，在客户面临上市等资本运作关键节点时，协助公司与投行审计进行有效沟通，帮助客户就资本市场的选择和网络安全审查等问题进行确认，并被指派为公司出具上市《数据合规法律意见》。

国内知名新能源汽车运营服务商

- 该国内知名新能源汽车运营服务商准备在2022年上市，我们受其委托，为其提供上市前数据合规法律服务，该公司业务形态复杂，我们通过深入尽调，梳理公司业务数据合规情况，提出存在的相关问题，根据其上市计划，做出合规整改方案，辅助落地实施数据合规制度，为其上市工作做准备。

环球网络安全与数据合规业务

国际性跨国保险及金融服务机构集团

- 我们受国际性跨国保险及金融服务机构集团的委托，作为其外部法律顾问，为其数据安全、个人信息保护合规提供法律服务。包括为其出具上市所需的《网络安全审查报告》，在工作过程中，我们对公司的相关人员进行现场访谈，以更加了解公司的运营情况，与网信办沟通上市相关方案，并向公司及时反馈相关意见。就无法实施的方案部分为公司提出解决新思路，提出整改建议，并协助整改。我们亦协助其在向联交所交表前，出具上市《数据合规法律意见》，并沟通与协助回复投行与中介机构的问询。

国内知名职场社交平台

- 我们受国内知名职场社交平台的委托，作为其外部法律顾问，基于其上市计划，为其数据安全、个人信息保护合规提供法律服务。包括对公司的相关人员进行现场访谈，并制作发放问卷，为其识别上市过程中可能出现的数据合规风险。

国内知名网络科技公司

- 受某国内知名网络科技公司的委托，作为其外部法律顾问，为其上市过程中所涉及的数据保护相关协议与条款，提出修改意见，并协助其完成修改与相应数据合规整改工作。同时，我们还多次就其日常业务中出现的问题提供法律咨询服务，包括是否可能被启动网络安全审查等问题。

国内某知名科技公司

- 受国内某知名科技公司委托，为其就数据合规方面的业务提供常年法律顾问服务，包括帮助公司梳理数据生命周期，以及协助公司了解数据合规的相关法律规定，并解答公司有关于数据合规的问题。同时，还为该知名科技公司提供产品出海方面的专业法律意见，协助公司了解境内外数据合规的监管动态等。

某国际知名食品生产商

- 我们受某知名食品生产商的委托，作为其外部法律顾问，为其提供常年与专项数据合规法律服务。在日常法律服务中，协助其建立整个数据合规体系框架，网络安全等级保护咨询，修改并完善隐私政策、内部制度等文件，并就企业日常运行中数据相关问题提供咨询服务。同时，在专项法律服务中，就企业并购境外企业过程中提供数据合规方面的协助，帮助公司对并购对象数据保护状况进行摸底排查，就交易中出现的数据法律问题出具法律意见，代表公司进行谈判磋商，并协助公司了解境内外数据合规监管动态。同时，我们还前往公司进行企业数据合规的内部培训，主要就该公司的产品提供了数据保护与电商方面的提示与建议。

环球律师事务所
GLOBAL LAW OFFICE

北京市朝阳区建国路81号华贸中心
1号写字楼15层&20层
邮编: 100025
15 & 20/F Tower 1,
China Central Place,
No. 81 Jianguo Road, Chaoyang
District, Beijing 100025, China
电话/T. (86 10) 6584 6688
传真/F. (86 10) 6584 6666

上海市徐汇区淮海中路999号
环贸广场办公楼一期35层&36层
邮编: 200031
35 & 36/F
Shanghai One ICC, No. 999
Middle Huai Hai Road, Xuhui District,
Shanghai 200031, China
电话/T. (86 21) 2310 8288
传真/F. (86 21) 2310 8299

深圳市南山区深南大道9668号
华润置地大厦B座27层
邮编：518052
27/F Tower B,
China Resources Land Building,
No. 9668 Shennan Avenue, Nanshan
District, Shenzhen 518052, China
电话/T. (86 755) 8388 5988
传真/F. (86 755) 8388 5987

成都市高新区天府大道北段966号
天府国际金融中心11号楼37层
邮编：610041
37/F Building 11,
Tianfu International Finance Center,
No. 966 Tianfu Avenue North Section,
High-tech Zone, Chengdu 610041, China
电话/T. (86 28) 8605 9898
传真/F. (86 28) 8313 5533

环球律师事务所
GLOBAL LAW OFFICE