企业上市数据合规白皮书

段和段律師事務所
DUAN & DUAN

上海数据交易所
SHANGHAI DATA EXCHANGE

二〇二四年二月

前言

从上市审核机构的视角，**我们总结梳理上市审核的最新实践案例，结合一线数据合规丰富项目实践经验**，撰写本《企业上市数据合规白皮书》。

机遇难挡：数据资本大时代

数据已经被誉为“第四产业”，我们正在迎接数据资本大时代。

数据作为生产要素，在驱动科研创新、推动数字经济发展等方面发挥战略作用，国家通过建立数据基础制度、实施数据资源入表政策、推动数据要素 X 试点工程等方式，打开数据资本化的大门。

- **重磅发布：数据 20 条，构建数据基础制度，奠定数据资本基调**。2022 年 12 月 19 日，《中共中央 国务院关于构建数据基础制度更好发挥数据要素作用的意见》（以下简称“数据二十条”）正式发布，**从数据产权、流通交易、收益分配、安全治理等方面构建数据基础制度**，提出 20 条政策举措。《数据二十条》的出台，将直接激活数据要素潜能。

- **重大突破：数据资源入表，赋予数据资源金融属性**。为充分实现《数据二十条》数据要素价值的目标，完善数据资产估值评价体系，2024 年 1 月 1 日，财政部发布的《企业数据资源相关会计处理暂行规定》正式施行。对企业而言意义非凡，最直观的影响体现在企业财务报表层面，数据资源在满足条件的情况下由原来利润表中的“费用”变成了“资产”进入了资产负债表，这种突破，**对数字企业的估值判断、质押融资、促进数据资源流通等方面产生诸多有利影响，为数据资源赋予了金融属性**，使得数据要素发挥真正的价值，是实现数据资产创新应用的第一步。

- **全域覆盖：数据要素 X 试点工程，支持场景化发展和数据产业融资。**2023 年 12 月 31 日，国家数据局等 17 部门发布《“数据要素×”三年行动计划(2024—2026 年)》，旨在通过推动数据在多场景应用，提高资源配置效率，创造新产业新模式，制定了工业制造、现代农业、商贸流通、交通运输、金融服务、科技创新、文化旅游、医疗健康、应急管理、气象服务、城市治理、绿色低碳等 12 个行业和领域的重点行动任务，并明确规定“依法合规探索多元化

投融资模式，发挥相关引导基金、产业基金作用，**引导和鼓励各类社会资本投向数据产业。支持数据商上市融资**”。

压力山大：数据合规的“一票否决”

数据合规，作为 IPO 审核重点，已成为影响企业能否上市的关键因素之一。因数据不合规被一票否决的案例逐渐显现。

标配上市：数据合规专项“如虎添翼”

监管机构的数据合规监管能力已基本配置到位，并在不断增强实战经验，以应对纷繁复杂的数据处理场景。

企业上市的“原配”中介服务机构：券商、会所和律所三家，其专业知识领域已无法覆盖和胜任数据合规维度上的特殊性要求。因此，企业上市的第四项标配服务——IPO 数据合规专项法律服务，应运而生。

这种新的变化趋势，在近期的上市企业中，不仅逐步常态化，更是显现了巨大的“能效”。

为积极应对上市审核机构数据合规专业细致的审查，不少拟上市企业在筹备上市阶段，甚至更早期，便开始配置数据合规专业法律服务，甚至是在数据产品的形成和确权过程就开始接受全程合规规划服务。

实战案例：审核视角下的“点睛”之术

从上市审核机构的视角，**我们总结梳理上市审核的最新实践案例，结合一线数据合规丰富项目实践经验**，撰写本《企业上市数据合规白皮书》。

本白皮书三大特点：

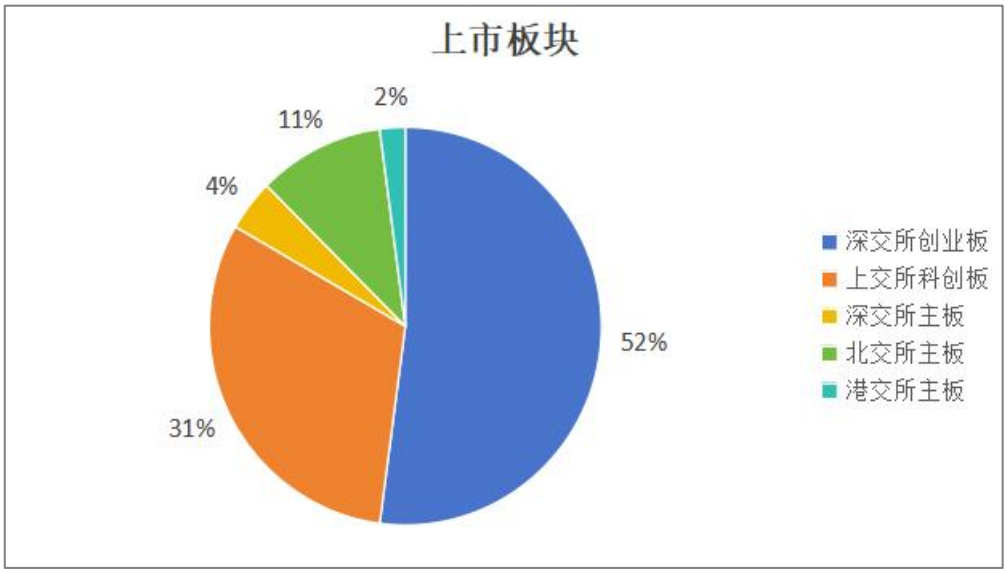
- **可视**：所见即所得。采用思维导图、表格等可视化方式（本文所有思维导图与表格均为原创），清晰体现合规要点；
- **可查**：分门别类。以数据处理全生命周期为视角，将审核问询中的各案例拆解后，贯穿到数据收集、数据使用、数据共享、数据存储、境外上市/数据出境及数据安全保障的各个环节；

- **可传**：将审核相对应的问题，转化为共性的问题进行呈现，少走弯路，少踩坑。

目 录

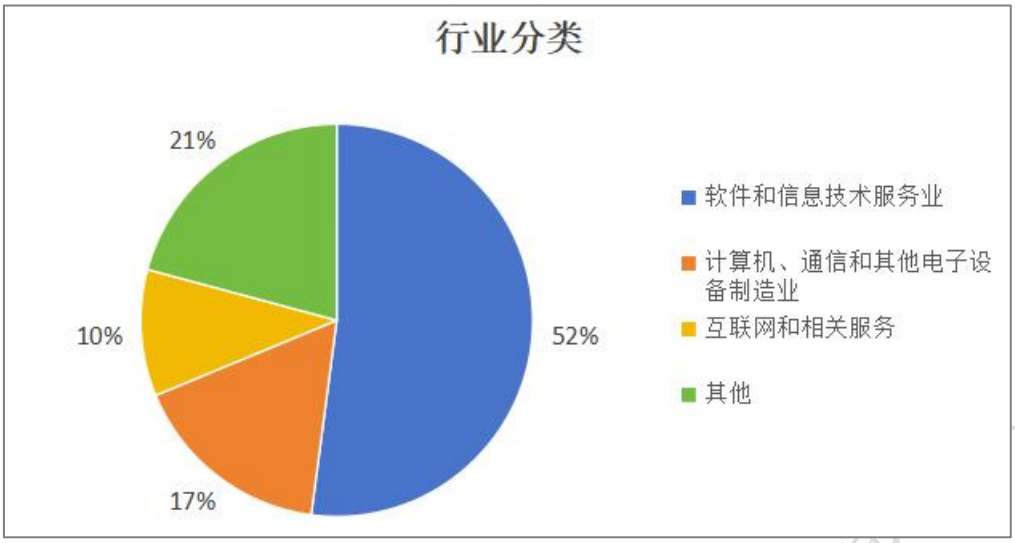
一、 遴选：案例分析说明

我们精心遴选了从 2019 年至 2024 年 1 月 5 日 **48 家具有典型代表性的企业**[1]，**汇总了这些企业**在上市过程中被审核机构问询的相关数据合规问题。**其中在深交所创业板申请上市的企业数量最多，共有 25 家企业（占比约为 52%）**、**在上交所科创板申请上市的企业数量次之，共有 15 家企业（占比约为 31%）**；其余，2 家企业在深交所主板申请上市、5 家企业申请在北交所申请主板上市、1 家企业在港交所主板申请上市。



在上市行业分类中，有 **25 家企业归类为软件和信息技术服务业，数量最多，8 家企业为计算机、通信和其他电子设备制造业，5 家企业为互联网和相关服务**，其他企业零散分布于零售业、商业服务业、电信、广播电视和卫星传输服务等行业。

[1] 截止 2024 年 1 月 5 日，本《企业上市数据合规白皮书》摘录的拟上市公司数据相关问询问题的案例截止至 2024 年 1 月 5 日。



具体如下表所示：

序号	发行人	行业分类
一	**深交所创业板**	
1	未来穿戴	计算机、通信和其他电子设备制造业
2	金智教育	软件和信息技术服务业
3	多彩新媒	电信、广播电视和卫星传输服务
4	衡泰技术	软件和信息技术服务业
5	联众网络	软件和信息技术服务业
6	麦驰物联	计算机、通信和其他电子设备制造业
7	长城信息	计算机、通信和其他电子设备制造业
8	绿联科技	计算机、通信和其他电子设备制造业
9	睿联技术	计算机、通信和其他电子设备制造业
10	数聚智连	零售业
11	东富龙科技	制药装备行业
12	小影创新	软件和信息技术服务业

序号	发行人	行业分类
13	大汉软件	软件和信息技术服务业
14	木瓜移动	互联网和相关服务
15	墨迹天气	科技推广和应用服务业
16	宇谷科技	软件和信息技术服务业
17	杭州小影	软件和信息技术服务业
18	木仓科技	互联网和相关服务
19	熙华检测	研究和试验发展
20	联众信息	软件和信息技术服务业
21	零点有数	商务服务业
22	兆尹科技	软件和信息技术服务业
23	新视云	软件和信息技术服务业
24	宇谷科技	互联网和相关服务
25	黔通智联	软件和信息技术服务业
二	**上交所科创板**	
26	佰聆数据	互联网和相关服务
27	合合信息	软件和信息技术服务业
28	碧兴物联	节能环保行业
29	长光卫星	软件和信息技术服务业
30	格蓝若	计算机、通信和其他电子设备制造业
31	沃太能源	电气机械和器材制造业

序号	发行人	行业分类
32	长光卫星	软件和信息技术服务业
33	中数智汇	软件和信息技术服务业
34	奥比中光	计算机、通信和其他电子设备制造业
35	蚂蚁集团	互联网和相关服务
36	青云科技	软件和信息技术服务业
37	京东数科	软件和信息技术服务业
38	微众信科	软件和信息技术服务业
39	海天瑞声	软件和信息技术服务业
40	旷视科技	软件和信息技术服务业
三	**深交所主板**	
41	太川股份	计算机、通信和其他电子设备制造业
42	玮言服饰	纺织服装、服饰业
四	**北交所主板**	
43	思迅软件	软件和信息技术服务业
44	华信永道	软件和信息技术服务业
45	路桥信息	软件和信息技术服务业
46	并行科技	软件和信息技术服务业
47	华夏电通	软件和信息技术服务业
五	**港交所主板**	
48	蔚来	非必需性消费-汽车

二、 数据合规“打底”问题解析

通过分析证监会/证券交易所（合称“上市审核机构”）披露的各拟上市企业数据相关问询内容可知，对于以数据为主营业务的拟上市企业，审核机构核心关注以下问题：

(1) 发行人是否存在处理个人信息、敏感个人信息的情形，处理方式是否合规；

(2) 发行人对个人信息主体权利保障情况；

(3) 发行人是否掌握重要数据；

(4) 发行人是否取得相关的数据权属；

(5) 发行人是否取得数据处理相关的资质、许可、认证及备案；

(6) 数据处理行为是否符合相关法律法规的规定，是否存在被处罚的风险。

关注焦点	问询对象/时间[2]	问询内容
个人信息	华信永道[3] 2022 年 10 月	公司是否存在收集或使用客户数据的情形。请发行人结合公司业务开展模式、具体业务内容、 产品应用场景及产品功能等，分析说明公司及其员工在业务开展过程中是否存在收集、存储、传输、处理、使用客户数据或个人信息的情形。
	未来穿戴[4] 2023 年 7 月	说明“未来穿戴”APP 获取用户个人信息的具体情况，包括获取个人信息的范围、个人信息存储地、访问权限、使用权归属、发行人对相关个人信息的使用情况及合法合规性，个人用户是否知情同意。
	玮言服饰[5] 2023 年 8 月	说明微商城的注册用户数及活跃用户数，线上销售（含淘宝/天猫、微商城等所有渠道）过程中是否可以直接或间接获得用户的具体数据和个人资料等信息，如是，请说明获取条件、获取方式和信息范围。

[2] 时间指发行人或发行人中介机构回复问询时间

[3] 关于华信永道（北京）科技股份有限公司向不特定合格投资者公开发行股票并在北京证券交易所上市申请文件的审核问询函的回复

[4] 关于未来穿戴健康科技股份有限公司首次公开发行股票并在创业板上市申请文件的第二轮审核问询函的回复

[5] 关于深圳市玮言服饰股份有限公司首次公开发行人民币普通股股票并在主板上市的补充法律意见书（二）

关注焦点	问询对象/时间[2]	问询内容
	金智教育[6] 2023 年 9 月	说明“今日校园”APP 及各类 SaaS 产品获取用户个人信息的具体情况，包括获取个人信息的范围、个人信息存储地、访问权限、使用权归属、发行人对相关个人信息的使用情况及合法合规性，个人用户是否知情同意。
	佰聆数据[7] 2023 年 9 月	数据来源、数据内容是否涉及个人隐私或涉密信息。
	多彩新媒[8] 2023 年 9 月	业务过程中所涉获取用户个人信息及合规性，并在招股说明书风险因素章节补充披露相关风险。
	衡泰技术[9] 2023 年 9 月	说明发行人控制和运营的 APP、小程序、公众号、网站及其运营模式，获取的个人数据数量及类型。
敏感个人信息	联众网络[10] 2022 年 7 月	说明报告期各期发行人仓储的病案数量及病案中所含信息，是否属于敏感个人信息，相关病案的存储方式及保护措施。
	麦驰物联[11] 2023 年 5 月	说明使用生物识别技术的具体产品及应用场景，是否存在采集、储存、使用业主身份证、手机号、人脸图像等敏感信息的情形，采集、储存、使用上述敏感信息的具体方式和使用情况，被采集人是否充分知情，发行人及相关主体是否取得被采集人的同意。
	太川股份[12] 2023 年 12 月	说明使用生物识别技术的具体产品及应用场景，是否存在采集、储存、使用业主身份证、手机号、人脸图像等敏感信息的情形，采集、储存、使用上述敏感信息的具体方式和使用情况。

[6] 关于江苏金智教育信息股份有限公司首次公开发行股票并在创业板上市申请文件的第二轮审核问询函的回复

[7] 关于佰聆数据股份有限公司首次公开发行股票并在科创板上市申请文件审核问询函的回复

[8] 广东华商律师事务所关于贵州多彩新媒体股份有限公司首次公开发行股票并在创业板上市的补充法律意见书(五)

[9] 《关于杭州衡泰技术股份有限公司首次公开发行股票并在创业板上市申请文件的审核问询函》之回复报告

[10] 关于上海联众网络信息股份有限公司首次公开发行股票并在创业板上市申请文件第二轮审核问询函的回复

[11] 关于深圳市麦驰物联股份有限公司首次公开发行股票并在创业板上市申请文件的审核问询函的回复

[12] 关于珠海太川云社区技术股份有限公司向不特定合格投资者公开发行股票并在北京证券交易所上市申请文件的审核问询函的回复

关注焦点	问询对象/时间[2]	问询内容
个人信息主体权利	太川股份[13] 2023 年 12 月	说明被采集人是否充分知情，发行人及相关主体是否取得被采集人的同意；**业主是否有权利拒绝发行人及相关主体收集相关数据**，如拒绝，是否影响业主正常出入小区等合法权益，相关约定是否实际具有强制性。补充披露发行人楼宇对讲门禁及智能家居产品相关 APP、小程序等软件是否持续调用用户位置、照片、联系人等信息，如是，说明相关功能的必要性，是否涉嫌侵犯用户隐私。
重要数据	长城信息[14] 2022 年 9 月	结合产品销售及经营模式，分析说明发行人是否掌握**重要数据或掌握 100 万人以上个人信息**。
	绿联科技[15] 2023 年 9 月	发行人是否属于“掌握重要数据，或者掌握 100 万人以上个人信息的企业机构”。
	睿联技术[16] 2023 年 9 月	请发行人说明是否掌握重要数据或掌握 100 万人以上个人信息。
数据权属	合合信息[17] 2022 年 9 月	发行人各项业务及研发分别获取、存储、使用哪些数据，对应的数据来源、数据权属，是否存在销售数据的情形。
	数聚智连[18] 2022 年 10 月	说明发行人自电商平台获取数据的主要类型（如用户个人信息、订单管理信息、平台运营信息等），是否取得相关数据的所有权。
	碧兴物联[19] 2023 年 4 月	发行人各项业务及研发分别获取、存储、使用哪些数据，对应的数据来源、数据权属，是否存在销售数据的情形；

[13] 关于珠海太川云社区技术股份有限公司向不特定合格投资者公开发行股票并在北京证券交易所上市申请文件的审核问询函的回复
[14] 关于长城信息股份有限公司首次公开发行股票并在创业板上市申请文件的审核问询函的回复
[15] 关于深圳市绿联科技股份有限公司首次公开发行人民币普通股股票并在创业板上市的补充法律意见书（六）
[16] 关于深圳市睿联技术股份有限公司首次公开发行股票并在创业板上市申请文件的第二轮审核问询函的回复
[17] 关于上海合合信息科技股份有限公司首次公开发行股票并在科创板上市申请文件的首轮审核问询函的回复
[18] 关于北京数聚智连科技股份有限公司首次公开发行股票并在创业板上市申请文件的第二轮审核问询函的回复
[19] 关于碧兴物联科技（深圳）股份有限公司首次公开发行股票并在科创板上市申请文件的审核问询函之回复报告

关注焦点	问询对象/时间[2]	问询内容
	华夏电通[20] 2023 年 11 月	发行人是否享有数据的所有权或获得相关数据主体的授权许可，相关授权许可是否存在使用范围、主体或期限等方面的限制
资质许可	并行科技[21] 2022 年 9 月	结合发行人超算云服务的业务模式和实质，涉及上游超算基础设施、下游高等院校、科研院所等客户的法律法规、监管政策对于超算设施管理、超算第三方服务、信息数据安全和保密等方面的要求，说明发行人从事超算领域业务是否已取得相关资质、许可或认证。
	东富龙科技[22] 2022 年 7 月	发行人及控股子公司、参股公司是否为客户提供个人数据存储及运营的相关服务，是否存在收集、存储个人数据，对相关数据挖掘及提供增值服务等情况；如是，请说明是否取得相应资质及提供服务的具体情况。
	佰聆数据[23] 2023 年 9 月	是否获得相关权利主体或主管部门的明确授权许可，是否存在适用范围、主体或期限等方面的限制，发行人是否存在超出前述限制使用数据或其他侵犯个人隐私、第三方合法权益的情形。
	金智教育[24] 2023 年 9 月	说明圆周网络运营“今日校园”APP 等相关业务是否需取得增值电信业务经营许可证；发行人及各子公司是否已取得经营所需的全部资质许可，经营业务是否存在超出许可资质或经营范围的情形。
处罚风险	小影创新[25] 2022 年 4 月	对个人信息的处理和使用是否符合《个人信息保护法》规定的处理规则；是否存在违法违规行为或被行政处罚的风险，是否对发行人构成重大不利影响。
	大汉软件[26] 2023 年 9 月	结合业务流程、合同条款等，说明业务开展中是否符合《数据安全法》《网络安全法》《个人信息保护法》《电信和互联网用户个人信息保护规定》等数据安全及信息保护相关法

[20] 关于北京华夏电通科技股份有限公司向不特定合格投资者公开发行股票并在北京证券交易所上市申请文件的审核问询函的回复

[21] 关于北京并行科技股份有限公司公开 发行股票并在北交所上市申请文件的审核问询函之回复

[22] 关于东富龙科技集团股份有限公司申请向特定对象发行股票的审核问询函之回复报告

[23] 关于佰聆数据股份有限公司首次公开发行股票并在科创板上市申请文件审核问询函的回复

[24] 关于江苏金智教育信息股份有限公司首次公开发行股票并在创业板上市申请文件的第二轮审核问询函的回复

[25] 关于杭州小影创新科技股份有限公司首次公开发行股票并在创业板上市申请文件的第二轮审核问询函的回复

[26] 上海市锦天城律师事务所关于大汉软件股份有限公司首次公开发行股票并在深圳证券交易所创业板上市的补充法律意见书（六）

关注焦点	问询对象/时间[2]	问询内容
		律法规的规定，是否存在纠纷或潜在纠纷。

表 1 数据基础相关问询

问题 1： 如何界定个人信息？

根据《个人信息保护法》[27]（下称“《个信法》”）的规定，个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。

即**个人信息=已识别个人信息+可识别个人信息－匿名化信息**。

其中“匿名化”是指个人信息经过处理无法识别特定自然人且不能复原的过程，与“去标识化”相对，后者指个人信息经过处理，使其在不借助额外信息的情况下无法识别特定自然人的过程。

我们以一个典型案例分析个人信息与非个人信息的区别。在 2022 年 5 月，为了维护网络空间的健康秩序，在用户在发表评论/发布内容时，各大网络平台强制公开用户 IP 属地[28]信息，一时间引发舆论监管与个人信息保护的激烈论战（具体参见本团队文章《“个人信息”的判定绝非易事——IP 属地遇到拦路虎“再识别技术”》）。

那么， IP 属地信息究竟是否构成个人信息？

(1) **IP 属地≠IP 地址**。IP 地址是指对计算机等上网设备进行唯一标识的一串 32 位二进制数，指向具有唯一性，能够单独识别到个人，因而属于个人信息；

(2) IP 属地对应的是宽泛的地理区域，单从境内账号展示的地域信息维度来看，省级地域内的用户数量庞大，难以直接通过该信息识别到或关联到特定的自然人，不构成“单独识别个人”的信息；然而，若与用户已于平台公开的工作单位、工作经历、头像等信息相结合，却有可能构成“与其他信息结合识别个人”的信息，或属于将 IP 地址进行去标识化（而非匿名化）措施后得到的

[27] 发布机构：全国人大常委会；2021.08.20 发布；2021.11.01 实施
[28] 针对境内账号，仅展示省（自治区、直辖市）；针对境外账号，仅展示国家（地区）

个人信息。

由此可见，IP 属地是否构成个人信息，需要结合具体场景，评估其对特定自然人的可识别性所起的作用程度；同时，亦有赖于实践对于“可识别”个人信息认定边界的把握尺度。

问题 2：　如何界定敏感个人信息？

与一般的个人信息相比，敏感个人信息一旦被泄露或者滥用，往往会对个人信息主体造成更大的人身或者财产损害，因此敏感个人信息应该受到更为严格的保护。根据《个信法》的规定，只有在具有特定的目的和充分的必要性，并采取严格保护措施的情形下，个人信息处理者才可处理敏感个人信息。

敏感个人信息的处理情况也愈加受到上市审核机构的重视。如联众网络[29]，一家作为为医疗管理部门、医院等提供无纸化病案、DRGs 绩效考核等软件服务的公司，在其上市审核过程中，被上市审核机构重点关注其业务开展过程中是否涉及病案信息等敏感个人信息的处理以及处理的合规性。

因此，如何在个人信息中精准识别并区分敏感个人信息尤为重要。

➢ 基础法律定义

根据《个信法》的规定，敏感个人信息是一旦**泄露**或者**非法使用**，容易**导致自然人的人格尊严受到侵害**或者**人身、财产安全受到危害**的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。

➢ 通用性国标

参考 GB/T35273—2020《信息安全技术 个人信息安全规范》[30]（下称“《个人信息安全规范》”），个人敏感信息是指一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息。通常情况下，14 岁以下（含）儿童的个人信息和涉及自然人隐私的信息属于敏感个人信息。具体如下表所示：

[29] 2021 年 12 月 29 日，深交所受理联众网络上市申请，经历 2 轮问询后，联众网络于 2022 年 8 月 30 日撤回申请并终止审核

[30] 发布机构：全国信息安全标准化技术委员会；2020.03.06 发布；2020.10.01 实施

要点	内容
个人财产信息	银行账户、鉴别信息（口令）、存款信息（包括资金数量、支付收款记录等）、房产信息、信贷记录、征信信息、交易和消费记录、流水记录等，以及虚拟货币、虚拟交易、游戏类兑换码等虚拟财产信息。
个人健康生理信息	个人因生病医治等产生的相关记录，如病症、住院志、医嘱单、检验报告、手术及麻醉记录、护理记录、用药记录、药物食物过敏信息、生育信息、以往病史、诊治情况、家族病史、现病史、传染病史等。
个人生物识别信息	个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部识别特征等。
个人身份信息	身份证、军官证、护照、驾驶证、工作证、社保卡、居住证等。
其他信息	性取向、婚史、宗教信仰、未公开的违法犯罪记录、通信记录和内容、通讯录、好友列表、群组列表、行踪轨迹、网页浏览记录、住宿信息、精准定位信息等。

表 2 敏感个人信息列举

- **特殊行业定义**

针对特殊行业，主管部门可能会结合实际监管需要，出台细化规定。如以汽车数据为例，对应的敏感个人信息定义如下：

根据《汽车数据安全管理若干规定（试行）》[31]的规定，敏感个人信息，是指一旦泄露或者非法使用，可能导致车主、驾驶人、乘车人、车外人员等受到歧视或者人身、财产安全受到严重危害的个人信息，包括**车辆行踪轨迹、音频、视频、图像和生物识别特征**等信息。

[31] 发布机构：网信办、发展改革委、工信部、公安部、交通运输部；2021.08.16 发布；2021.10.01 实施

问题 3：　处理敏感个人信息需要注意什么？

考虑到敏感个人信息的特殊性，我国在一般个人信息的处理规则的基础上，对敏感个人信息的全生命周期处理流程提出了特殊的保护要求。

在组织机构的设置上，根据《个人信息安全规范》第 11.1 条，处理超过 **10 万人** 的个人敏感信息的组织即应当设置个人信息保护负责人；而对于处理一般个人信息的，则放宽至 **100 万人**。（详见“问题 46：　什么情况下应当设置数据安全负责人、个人信息保护负责人？”）

根据《个信法》与《个人信息安全规范》，我们从敏感个人信息的处理原则、处理条件、特殊告知与同意要求、传输与存储、使用、注销账户、公开、安全事件、组织机构等维度，**独创**梳理敏感个人信息处理要点如下表所示，需要特别关注的内容我们加粗显示（下表中未涉及的内容应依据一般个人信息处理规则处理）：

序号	要点	内容
1	**处理原则**	(1)　具有特定的目的和充分的必要性； (2)　采取严格保护措施。
2	个人信息保护影响评估	个人信息处理者应当在处理敏感个人信息前，进行个人信息保护影响评估，并对处理情况进行记录（详见“问题 9：如何正确认知个人信息安全影响评估？”）。
3	特殊告知要求	(1)　**履行一般告知义务**（详见“问题 11：　直接从用户获得数据，需要关注什么？”）： (a) 个人信息处理者的名称或者姓名和联系方式； (b) 个人信息的处理目的、处理方式，处理的个人信息种类、保存期限； (c) 个人行使《个信法》规定权利的方式和程序； (d) 法律、行政法规规定应当告知的其他事项。 (2)　**履行特殊告知义务**：向个人告知处理敏感个人信息的必要性以及对个人权益的影响（依照《个信法》规定可以不向个人告知的除外[32]）；

[32] 根据《个信法》第十八条的规定：个人信息处理者处理个人信息，有法律、行政法规规定应当保密或者不需要告知的情形的，可以不向个人告知前条第一款规定的事项。紧急情况下为保护自然人的生命健康和

序号	要点	内容
		(3) **告知方式**：宜在收集敏感个人信息前，通过交互界面或设计（如弹窗、文字说明、填写框、提示条、提示音等形式），向个人信息主体履行告知义务。
4	**单独同意**	(1) **单独同意**：处理敏感个人信息应当取得个人的单独同意；法律、行政法规规定处理敏感个人信息应当取得书面同意的，从其规定； (2) **同意方式**：宜通过个人信息主体对信息收集主动作出肯定性动作（如勾选、点击“同意”或“下一步”等）征得其明示同意，而非默认同意； (3) **撤回同意**：所要求的交互界面或设计应方便个人信息主体再次访问及更改其同意的范围； (4) **未成年人的特殊情形**： (a) 应当取得未成年人的父母或者其他监护人的同意； (b) 个人信息处理者处理不满十四周岁未成年人个人信息的，应当制定专门的个人信息处理规则。
5	传输与存储	(1) 传输和存储个人敏感信息时，应采用加密[33]等安全措施； (2) 个人生物识别信息应与个人身份信息分开存储； (3) 原则上不应存储原始个人生物识别信息（如样本、图像等），可采取的措施包括但不限于： (a) 仅存储个人生物识别信息的摘要信息[34]； (b) 在采集终端中直接使用个人生物识别信息实现身份识别、认证等功能； (c) 在使用面部识别特征、指纹、掌纹、虹膜等实现识别身份、认证等功能后删除可提取个人生物识别信息的原始图像[35]。
6	使用	**访问权限**：对个人敏感信息的访问、修改等操作行为，宜在对角色权限控制的基础上，按照业务流程的需求触发操作授权。
7	注销账户	注销账户的过程中需收集敏感个人信息核验身份时，应明确收集个人敏感信息后的处理措施，如达成目的后立即删除或匿名

财产安全无法及时向个人告知的，个人信息处理者应当在紧急情况消除后及时告知

[33] 采用密码技术时宜遵循密码管理相关国家标准

[34] 摘要信息通常具有不可逆特点，无法回溯到原始信息

[35] 个人信息控制者履行法律法规规定的义务相关的情形除外

序号	要点	内容
		化处理等。
8	公开	(1) 进行个人信息保护影响评估； (2) 向个人信息主体告知公开的目的、涉及的个人敏感信息的内容； (3) 取得个人单独同意的； (4) 不应公开：我国公民的种族、民族、政治观点、宗教信仰等个人敏感数据的分析结果。
9	安全事件	考虑到敏感个人信息一旦泄露或者非法使用，容易导致自然人的合法权益受到侵害，若发生或者可能发生敏感个人信息泄露、篡改、丢失的，建议按照“问题 48：发生个人信息泄露时，应当怎么办？”履行法定补救与通知义务，并留存证件，以自证清白。
10	**组织机构**	(1) **个人信息保护负责人**：处理超过 10 万人的个人敏感信息的，应设立专职的个人信息保护负责人和个人信息保护工作机构，负责个人信息安全工作（详见“问题 46：什么情况下应当设置数据安全负责人、个人信息保护负责人？”）； (2) **员工管理**：应与从事个人信息处理岗位上的相关人员签署保密协议，对大量接触敏感个人信息的人员进行背景审查，以了解其犯罪记录、诚信状况等。

表 3 敏感个人信息处理规则

问题 4：　如何界定重要数据？

与一般数据相比，重要数据一旦被泄露或滥用，往往会给国家安全、公共利益造成更大的损害，因此，从《网络安全法》[36]（“《网安法》”）到《数据安全法》[37]（下称“《数安法》”）以及各类的国家标准，都对重要数据制定了特殊的保护制度。重要数据的处理也愈加受到上市审核机构的重视，如在长城信息[38]上市审核过程中，上市审核机构就问询到其是否涉及重要数据的处理。

然而，目前《网安法》及《数安法》尚未对“重要数据”的定义、范围进行明确。

➢　重要数据定义

参考 2022 年《信息安全技术 重要数据识别指南（征求意见稿）》[39]（下称“《重要数据识别指南》”），其将重要数据定义为“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**”，同时标注重要数据不包括国家秘密和个人信息，但基于海量个人信息形成的统计数据、衍生数据有可能属于重要数据。

➢　重要数据识别原则及识别因素

识别重要数据，需要遵循聚焦安全影响[40]、突出保护重点[41]、衔接既有规定[42]、综合考虑风险[43]、定量定性结合[44]与动态识别复评[45]六项基本原则，同时，依据《重要数据识别指南》，具备以下因素之一的，是重要数据：

[36] 发布机构：全国人大常委会；2016.11.07 发布；2017.06.01 实施
[37] 发布机构：全国人大常委会；2021.06.10 发布；2021.09.01 实施
[38] 深交所于 2021 年 12 月 29 日受理长城信息上市申请，经两轮问询后，于 2022 年 9 月 15 日上市委会议审议通过，于 2023 年 4 月 28 日终止上市审核
[39] 发布机构：全国信息安全标准化技术委员会；2022.01.13 发布；征求意见至 2022.03.13
[40] 从国家安全、经济运行、社会稳定、公共健康和安全等角度识别重要数据，只对组织自身而言重要或敏感的数据不属于重要数据，如企业的内部管理相关数据
[41] 通过对数据分级，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前提下有序流动，释放数据价值
[42] 充分考虑地方已有管理要求和行业特色，与地方、部门已经制定实施的有关数据管理政策和标准规范紧密衔接
[43] 根据数据用途、面临威胁等不同因素，综合考虑数据遭到篡改、破坏、泄露或者非法获取、非法利用等风险，从保密性、完整性、可用性、真实性、准确性等多个角度识别数据的重要性
[44] 以定量与定性相结合的方式识别重要数据，并根据具体数据类型、特性不同采取定量或定性方法
[45] 随着数据用途、共享方式、重要性等发生变化，动态识别重要数据，并定期复查重要数据识别结果

图 1　重要数据识别因素

➢ 汽车和基础电信行业重要数据目录

此外，根据《数安法》等法律法规要求，国家有关部门应制定重要数据目录，加强对重要数据的保护。目前，我国在**汽车行业、工业和信息化行业以及基础电信行业制定了现行有效的重要数据目录**（如下表所示）。鉴于其他行业重要数据目录尚未出台，建议拟上市公司及时与主管网信部门作进一步沟通，以明确其所处

理的数据性质是否构成重要数据。

行业	重要数据定义	重要数据范围	法律依据
汽车	是指一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能危害国家安全、公共利益或者个人、组织合法权益的数据	(1) 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； (2) 车辆流量、物流等反映经济运行情况的数据； (3) 汽车充电网的运行数据； (4) 包含人脸信息、车牌信息等的车外视频、图像数据； (5) 涉及个人信息主体超过 10 万人的个人信息； (6) 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。	《汽车数据安全管理若干规定（试行）》
基础电信	是指企业在运营中收集、产生、控制的不涉及国家秘密，但与国家安全、经济发展、社会稳定，以及公共利益密切相关的数据，特别是与国家基础通信网络安全密切相关的数据	(1) 基础电信企业掌握的能够反映通信行业整体情况的数据，如网络规划、建设、关键技术信息； (2) 基础电信企业掌握的通信网络基础资源信息，一旦被恶意利用，可能会导致国家基础通信网络中断，进而对国家安全和社会稳定造成重大影响； (3) 基础电信企业掌握的能够导致通信行业发生系统性风险的能够反映通信网络总体运行状况的数据，一旦完整性、保密性、可用性遭破坏可能对国家或社会带来负面影响的数据，如网络运行监控数据； (4) 基础电信企业掌握的通信网络与系统的设计、安全防护计划和策略方案，及其单元或设备选型、配置、软件等属性信息和脆弱性	《基础电信企业重要数据识别指南》

行业	重要数据定义	重要数据范围	法律依据
		信息等；以及包括密码技术在内的其它与国家安全相关的单元、装置、设备、系统或计划、设计能力和缺陷信息； (5) 基础电信企业掌握的与意识形态、舆情等有关的文化安全相关信息； (6) YD/T 3813-2020 中四级数据中的用户相关数据比照重要数据管理； (7) 基础电信企业掌握的其他与国家公共安全、经济发展、社会稳定，以及公共利益密切相关的数据。	
工业和信息化	——	危害程度符合下列条件之一的数据为重要数据： (1) 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； (2) 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； (3) 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； (4) 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； (5) 经工业和信息化部评估确定的其他重要数据。	《工业和信息化领域数据安全管理办法（试行）》

表 4 汽车、基础电信行业及工业和信息化行业制定的现行有效的重要数据目录

问题 5：　处理重要数据需要注意什么？

考虑到重要数据与国家安全、公共利益息息相关，我国对于处理重要数据制定了特殊的保护要求。根据《数安法》《网络数据安全管理条例（征求意见稿）》[46]等相关法律法规，我们初步总结出重要数据处理者需要重点关注的要点：

序号	要点	内容	来源
1	**设置人员及机构**	明确数据安全负责人和管理机构，落实数据安全保护责任。	《数安法》
2	**重要数据备案**	重要数据的处理者，应当在识别其重要数据后的十五个工作日内向设区的市级网信部门备案。	《网络数据安全管理条例（征求意见稿）》
3	**采购可信产品与服务**	重要数据的处理者，应当优先采购安全可信的网络产品和服务。	《网络数据安全管理条例（征求意见稿）》
4	**制定数据安全培训计划**	重要数据的处理者，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，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。	《网络数据安全管理条例（征求意见稿）》
5	**共享/交易/委托处理前征得主管部门同意**	数据处理者共享、交易、委托处理重要数据的，应当征得设区的市级及以上主管部门同意，主管部门不明确的，应当征得设区的市级及以上网信部门同意。	《网络数据安全管理条例（征求意见稿）》
6	**定期开展风险评估**	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。	《数安法》
7	**重要数据出境特别规定**	数据处理者向境外提供数据，有下列情形之一的，应当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：（一）数据处理者向境外提供重要数据……	《数据出境安全评估办法》

[46] 发布机构：网信办；2021.11.14 发布；征求意见至 2021.12.13

表 5 重点数据合规要点

其中，根据《工业和信息化领域数据安全管理办法（试行）》[47]的规定，针对工业和信息化领域的重要数据处理者，还应当：

(1) 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，建立常态化沟通与协作机制。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；

(2) 明确数据处理关键岗位和岗位职责，并要求关键岗位人员签署数据安全责任书，责任书内容包括但不限于数据安全岗位职责、义务、处罚措施、注意事项等内容；

(3) 建立内部登记、审批等工作机制，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。

[47] 发布机构：工信部；2022.12.08 发布

问题 6：　如何确认数据权属？

数据作为新型生产资料，其权属关系的界定是解决后续流通利用环节中权利义务关系界定、数据主体合法权益保障、数据秩序维护等核心问题的先决条件，但因其不存在资源枯竭问题，将随着反复使用与汇聚融合不断繁荣数据价值，在具有财产属性的同时，又具有相应的人身权特征，目前尚未在立法与司法层面形成明确规定或共识。

然而，由于数据权属问题与拟上市企业数据的资源利用合规性以及盈利能力息息相关，在上市审核过程中也屡被上市审核机构问询（如合合信息与数聚智联，皆被问询到数据权属问题）。由此可见，明确数据权属的确认规则对于拟上市企业而言至关重要。

➢ **立法层面：**

目前国内立法，涉及数据权属的规定主要有：

根据《民法典》（2020.05.28 发布，2021.01.01 实施）第 111 条规定：“自然人的个人信息受法律保护。任何组织或者个人需要获取他人个人信息的，应当依法取得并确保信息安全，不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开他人个人信息”；第 127 条规定：“**法律对数据、网络虚拟财产的保护有规定的，依照其规定**”。

相较于《民法典》的框架性规定，我国深圳市颁布的地方性法规《深圳经济特区数据条例》（2021.07.06 发布，2022.01.01 实施）则首次提出数据的“个人权益”与“财产权益”的概念：“自然人对个人数据享有法律、行政法规及本条例规定的人格权益”；“自然人、法人和非法人组织对其合法处理数据形成的数据产品和服务享有法律、行政法规及本条例规定的财产权益”，从立法层面做出了有益尝试。

➢ **实践层面：**

立法存在滞后性，经济社会发展中面临的数据权属问题已成为实践层面无法回避的对象，近年来也受到上市审核机构的重视，在企业上市过程中屡被问询。

除上市问询外，司法实践审判中对数据权属的问题亦有所涉及。

在杭州互联网法院审理的微信群控软件不正当竞争纠纷一案[48]中，法院将涉案数据形态分为两种，一是单一原始数据个体，二是数据资源整体。法院认为：

(a) 就单一原始数据个体而言，网络平台方只能依附于用户信息权益，依其与用户的约定享有原始数据的有限使用权。使用他人控制的单一原始数据只要不违反“合法、必要、征得用户同意”原则，一般不应被认定为侵权行为，网络平台方亦无赔偿请求权；

(b) 就数据资源整体而言，因系网络平台方经过长期经营积累聚集而成，且能够给网络平台方带来开发衍生产品获取增值利润和竞争优势的机会，网络平台方就此享有竞争权益。如果擅自规模化、破坏性地使用网络平台方数据资源的，网络平台方作为数据控制主体有权要求获得赔偿。

结合上述实践，我们依据数据来源、数据类型，初步总结确定以下数据权属规则[49]：

[48] （2020）浙 01 民终 5889 号

[49] 结合《信息安全技术 网络数据分类分级要求（征求意见稿）》，我们将衍生数据定义为：在原始数据的基础上，经过统计、关联、挖掘、聚合、去标识化等加工活动而产生的数据

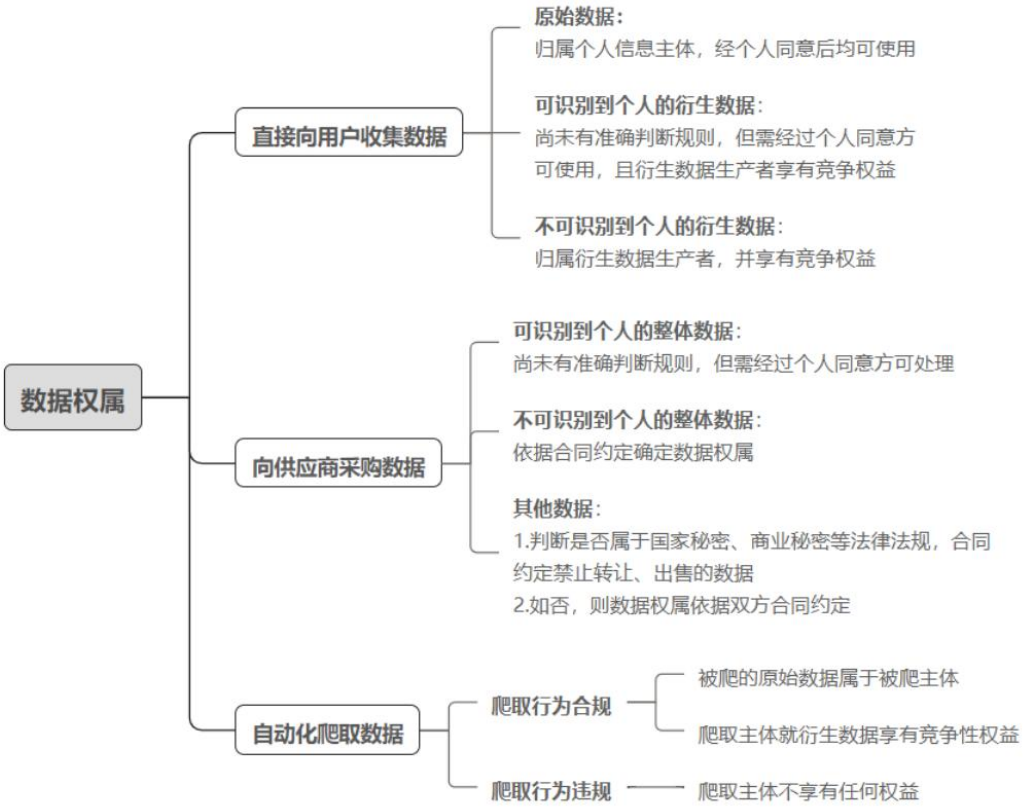


图 2 数据权属判断方式[50]

[50] 本图中涉及到个人同意的，含经个人同意或具备其他处理合法性依据两种情形

问题 7： 如何界定个人信息处理者与受托人？

根据我国《个信法》的规定：个人信息处理者，是指在个人信息处理活动中自主决定处理目的、处理方式的组织、个人；受托人则是指接受委托处理个人信息的主体。该规定与欧盟 *General Data Protection Regulation*（简称“《GDPR》”，中文译名为《通用数据保护条例》，2018.05.25 发布）中对于数据控制者与数据处理者的界定有异曲同工之处，我们简要对比如下：

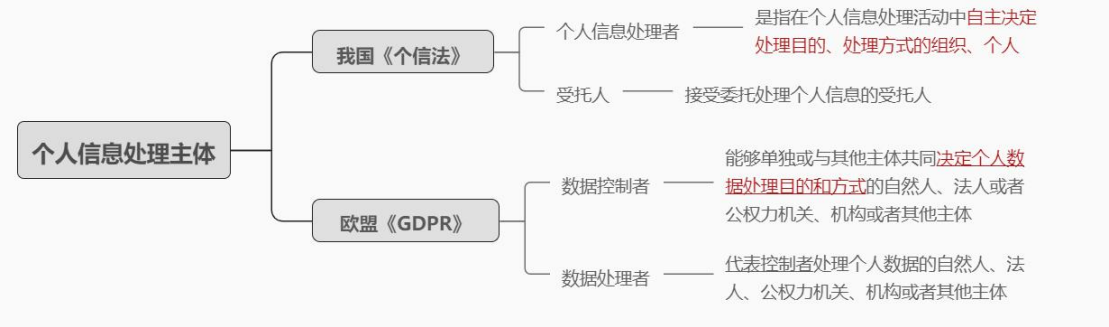


图 3 《个信法》与《GDPR》个人信息处理者与受托人界定对比

鉴于我国尚未出台具体的个人信息处理者与受托人的区分标准，建议拟上市企业参照欧盟数据保护委员会（EDPB）发布的 *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*（中文译名为《GDPR 下数据控制者及数据处理者概念的指南（07/2020）》，2020.09.02 更新）下**数据控制者（即对应我国个人信息处理者）与数据处理者（对应我国受托人）**的区分标准：

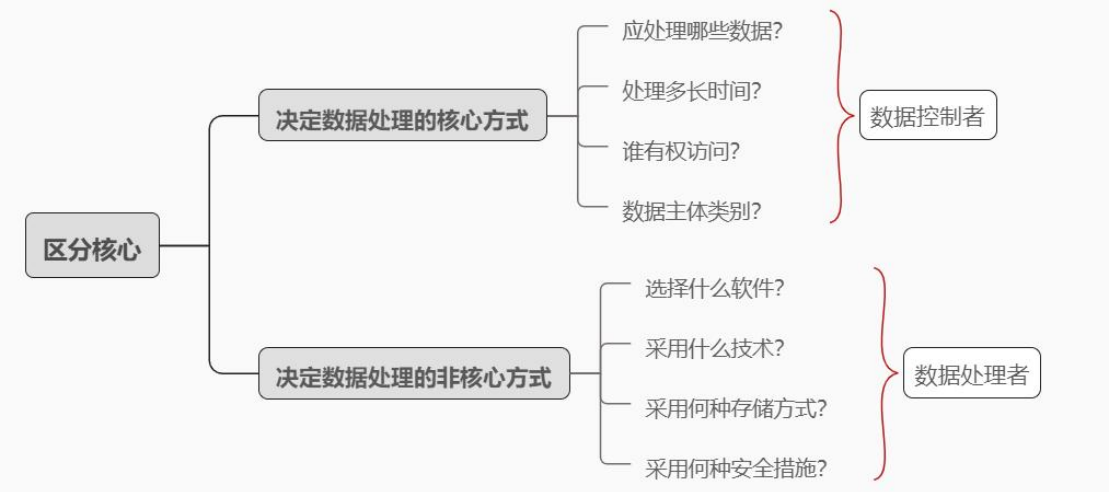


图 4 数据控制者与数据处理者区分标准

问题 8：　提供数据服务是否需要相关资质、许可、认证及备案？

我们将数据服务涉及的常见的可能需要的资质、许可、认证及备案内容整理如下图（具体应结合业务内容进行判断，其中，算法备案相关内容详见“问题 22：什么情况下需要进行算法备案？”与“问题 23：如何进行算法备案？”）：

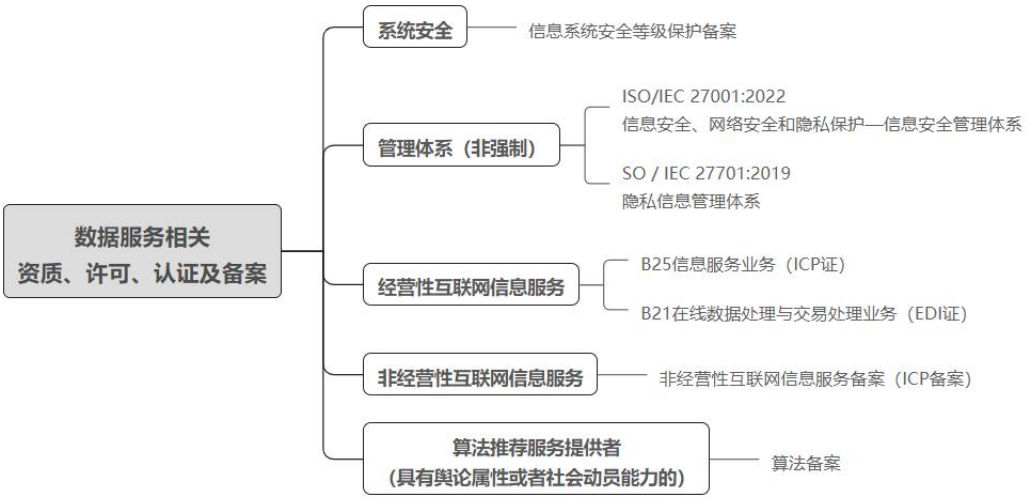


图 5　常见的数据服务相关资质、许可、认证及备案

我国相关法律法规对数据服务需要取得相关资质、许可、认证或备案的规定如下：

序号	法律法规	基础信息	主要内容
1	《数安法》	全国人大常委会 2021.06.10 发布 2021.09.01 实施	第三十四条　法律、行政法规规定提供数据处理相关服务应当取得行政许可的，服务提供者应当依法取得许可。
2	《网安法》	全国人大常委会 2016.11.07　发布 2017.06.01　实施	第二十一条　国家实**行网络安全等级保护制度**。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改： （一）制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任； （二）采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施； （三）采取监测、记录网络运行状态、网络

序号	法律法规	基础信息	主要内容
			安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月； （四）采取数据分类、重要数据备份和加密等措施； （五）法律、行政法规规定的其他义务。 第二十二条 网络产品、服务应当符合相关国家标准的强制性要求。…… 第二十三条 网络关键设备和网络安全专用产品应当按照相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求后，方可销售或者提供。……
3	《个信法》	全国人大常委会 2021.08.20 发布 2021.11.01 实施	第三十二条 法律、行政法规对处理敏感个人信息规定应当取得相关行政许可或者作出其他限制的，从其规定。
4	《信息安全等级保护管理办法》	公安部，国家保密局，国家密管局，国信办(已撤销) 2007.06.22 发布 2007.06.22 实施	第二条 国家通过制定统一的信息安全等级保护管理规范和技术标准，组织公民、法人和其他组织**对信息系统分等级实行安全保护，对等级保护工作的实施进行监督、管理**。
5	《电信业务经营许可管理办法》	工信部 2017.07.03 发布 2017.09.01 实施	第四条 经营电信业务，应当依法取得电信管理机构颁发的**经营许可证**。 电信业务经营者在电信业务经营活动中，应当遵守经营许可证的规定，接受、配合电信管理机构的监督管理。
6	《互联网信息服务管理办法》	国务院 2011.01.08 发布 2011.01.08 实施	第四条 **国家对经营性互联网信息服务实行许可制度；对非经营性互联网信息服务实行备案制度**。 未取得许可或者未履行备案手续的，不得从事互联网信息服务。 第七条 从事经营性互联网信息服务，应当向省、自治区、直辖市电信管理机构或者国务院信息产业主管部门申请办理互联网信息服务增值电信业务经营许可证。

序号	法律法规	基础信息	主要内容
			第八条 从事非经营性互联网信息服务，应当向省、自治区、直辖市电信管理机构或者国务院信息产业主管部门办理备案手续。
7	《互联网信息服务算法推荐管理规定》	网信办，工信部，公安部，市监总局 2021.12.31 发布 2022.03.01 实施	第二十四条 **具有舆论属性或者社会动员能力的算法推荐服务提供者**应当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**。
8	《互联网信息服务深度合成管理规定》	网信办，工信部，公安部 2022.11.25 发布 2023.01.10 实施	第十九条　具有舆论属性或者社会动员能力的深度合成服务提供者，应当按照《互联网信息服务算法推荐管理规定》履行备案和变更、注销备案手续。 深度合成服务技术支持者应当参照前款规定履行备案和变更、注销备案手续。 完成备案的深度合成服务提供者和技术支持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。
9	《生成式人工智能服务管理暂行办法》	网信办，工信部，公安部，国家发展和改革委员会，教育部，科学技术部，国家广电总局 2023.07.10 发布 2023.08.15 实施	第十七条　提供具有舆论属性或者社会动员能力的生成式人工智能服务的，应当按照国家有关规定开展安全评估，并按照《互联网信息服务算法推荐管理规定》履行算法备案和变更、注销备案手续。

表 7 数据许可、资质与备案相关法律法规梳理

问题 9：　如何正确认知个人信息安全影响评估？

根据我国国家市场监督管理总局、国家标准化管理委员出台的《信息安全技术—个人信息安全影响评估指南》（自 2021 年 6 月 1 日起正式实施），个人信息安全影响评估是指针对个人信息处理活动，检验其合法合规程度，判断其对个人信息主体合法权益造成损害的各种风险，以及评估用于保护个人信息主体的各项措施有效性的过程。其目的旨在发现、处置和持续监控个人信息处理过程中对个人信息主体合法权益造成不利影响的风险。

➢　个人信息安全影响评估的法定情形

触发个人信息安全影响评估的法定情形（含根据国家推荐标准进行评估的情形）目前散见于各个法律法规以及文件中，让处理数据的企业无所适从。对此，我们分析整理了相关规定，明确以下十种情景需进行个人信息安全评估，其中情景 1~情景 6、情景 10 为《个信法》等相关法律法规强制性要求，情景 7~情景 9 为有关部门制定的推荐性标准、指南，供个人信息处理者参考借鉴（详见本团队文章《个人信息安全评估十情景五豁免》）：

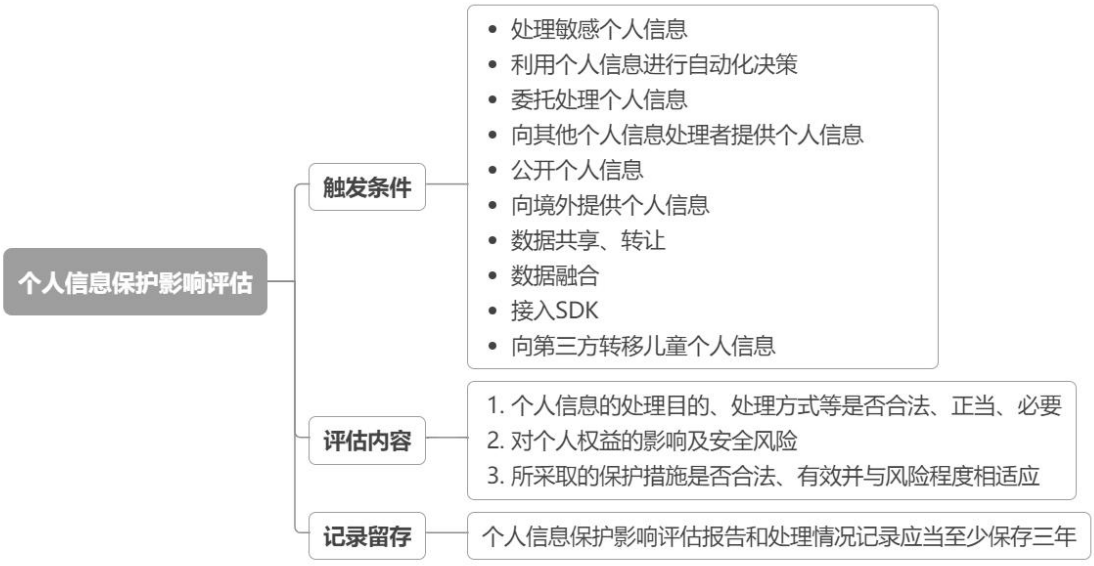


图 6　个人信息保护影响评估要点梳理

(1) 情景 1:处理个人敏感信息

敏感个人信息是一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。

《个信法》第 55 条。

(2) 情景 2:自动化决策

利用个人信息自动化决策且对个人信息主体权益造成显著影响的。如某宝获取用户位置、消费能力、使用软件时长等信息，给用户精准推送产品等，还比如软件根据个人信息决定个人征信及贷款额度等。

《个信法》第 55 条、《个人信息安全规范》第 7.7 条。

(3) 情景 3:委托第三方处理

委托他人处理自身收集的个人信息。即满足授权同意的前提下，自身不具备信息处理能力或与外部第三方进行合作时，委托其他技术团队等为其处理信息。

《个信法》第 55 条、《互联网个人信息安全保护指南》[51]第 6.5 条、《个人信息安全规范》第 9.1 条。

(4) 情景 4:向第三方提供

向第三方提供个人信息的情形是自身收集信息之后，提供给其他人使用，不论是有偿还是无偿。

《个信法》第 55 条。

(5) 情景 5:公开个人信息

个人信息原则上不得公开，除非经过法律授权或者具备合理事由需要公开个人信息。

[51] 发布机构：公安部网络安全保卫局、北京网络行业协会、公安部第三研究所；2019.04.10 发布

《个信法》第 55 条、《互联网个人信息安全保护指南》第 6.7 条。

(6) 情景 6:向境外提供个人信息

一般情况下，应当将在境内收集和产生的信息存储在境内，向境外提供时原则上应当经过国家网信部门组织的安全评估。

《网安法》第 37 条、《个信法》第 55 条。

(7) 情景 7:数据共享、转让

数据共享：是指与数据处理企业以外的任何企业、组织和个人分享用户的个人信息。如某打车软件，为了提供地图服务与某导航软件进行用户信息共享。

数据转让：是指数据处理企业将用户的个人信息以有偿或无偿的方式转让给任何企业、组织和个人。如某征信企业，将其收集到用户征信信息转让给某贷款企业。

《互联网个人信息安全保护指南》第 6.6 条、《个人信息安全规范》第 9.2 条

(8) 情景 8：数据融合

所谓数据融合：是指将不同来源的数据进行整合来获得更高质量的信息。如电商平台公司除了提供传统的电商平台服务，还通过平台向用户提供金融服务，为了提供更精准的服务，电商平台公司将两条产品线的数据库打通，根据用户的消费能力和消费习惯来调整贷款额度和利息。

《个人信息安全规范》第 7.6 条。

(9) 情景 9:接入 SDK

接入第三方产品时的 APP 开发者和第三方产品开发者。接入 SDK（辅助开发某一类应用软件的相关文档、范例和工具的集合）收集个人信息前需要对第三方 SDK 进行安全性评估，不仅如此，SDK 提供者在发布上线前，也应进行安全评估。

《个人信息安全规范》第 9.7 条、《网络安全标准实践指南—移动互联网应用

程序（App）使用软件开发工具包（SDK）安全指引》[52]第 5.2 条、第 5.3 条。

(10)情景 10:向第三方转移儿童个人信息

网络运营者向第三方转移儿童个人信息的，应当自行或者委托第三方机构进行安全评估。

《儿童个人信息网络保护规定》[53]第 17 条。

- **个人信息安全影响评估的价值**

《个信法》现已将个人信息保护影响评估制度作为一项强制性义务，若触发个人信息安全影响评估却未进行，个人信息处理者将面临最高可达五千万元以下或者上一年度营业额百分之五以下罚款（详见“问题 10：违规处理数据，需要承担哪些法律责任？”）；

通过评估，**有助于企业规范日常经营管理活动、减少管理和合规成本、树立企业形象**，并且可以在发生个人信息安全事件后，企业“自证清白”。

（详见本团队文章《个人信息安全影响评估——“自证清白”第一步（上）》《个人信息安全影响评估——“自证清白”第一步（下）》）

[52] 发布机构：全国信息安全标准化技术委员会；2020.11.27 发布
[53] 发布机构：网信办；2019.08.22 发布；2019.10.01 施行

问题 10：　违规处理数据，需要承担哪些法律责任？

实际上，根据数据违规行为的不同适用场景，企业所面临的法律责任也不尽相同。在这里，我们根据《个信法》《数安法》及《网安法》的规定，通过思维导图的方式，厘清在不同数据违规场景下，将面临何种法律责任：

(1) 刑事责任

图 7　数据违规行为之刑事责任

(2) 行政及民事责任

图 8 数据违规行为之行政及民事责任

三、 IPO 数据合规核心 40 问

数据合规不过关，将直接成为申请上市的实质性障碍。

某人工智能及大数据科技企业在 IPO 过程中因数据处理合规性问题受到上市审核机构的三轮问询，一路问至数据科技伦理等终极问题。可以说以数据处理为核心价值的企业，如若能在早期关注、规划并构建数据合规体系，将为后续 IPO 奠定坚实的基础。

对此，我们结合数据处理的全生命周期（如下图所示），梳理、分析上市过程中上市审核机构的问询问题，总结 IPO 过程中有关数据合规的 40 个核心问题，并结合一线项目实战经验凝练、提取合规要点，帮助拟上市企业厘清重点，做到心中有“数”。

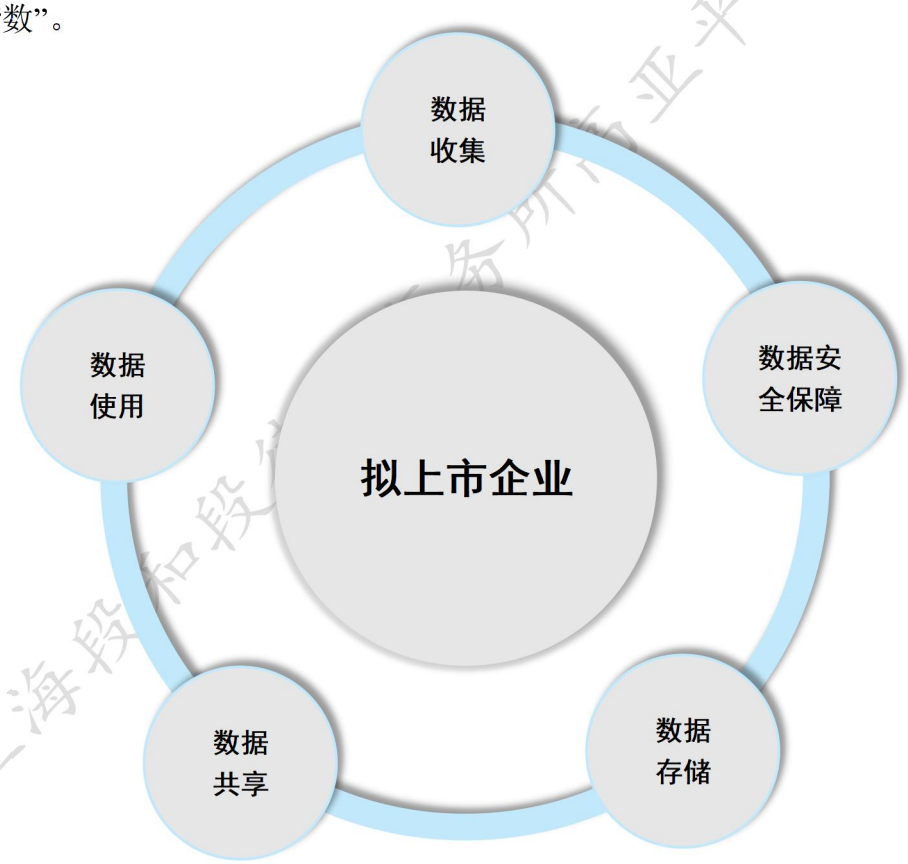


图 9 数据处理全生命周期图

(一)数据收集合规 6 问

通过分析上市审核机构披露的各拟上市企业接受的数据相关问询内容可知，在数据收集环节，审核机构的核心关注点在于：

(1) **数据来源的合规性**；

实践中数据常见的获取方式如下图所示，对应暗藏的数据合规风险点详见本团队文章《APP 个人信息采集侵权风险要点识别（上篇）——基于审判案例的分析》《APP 个人信息采集侵权风险要点识别（下篇）——基于审判案例的分析》：

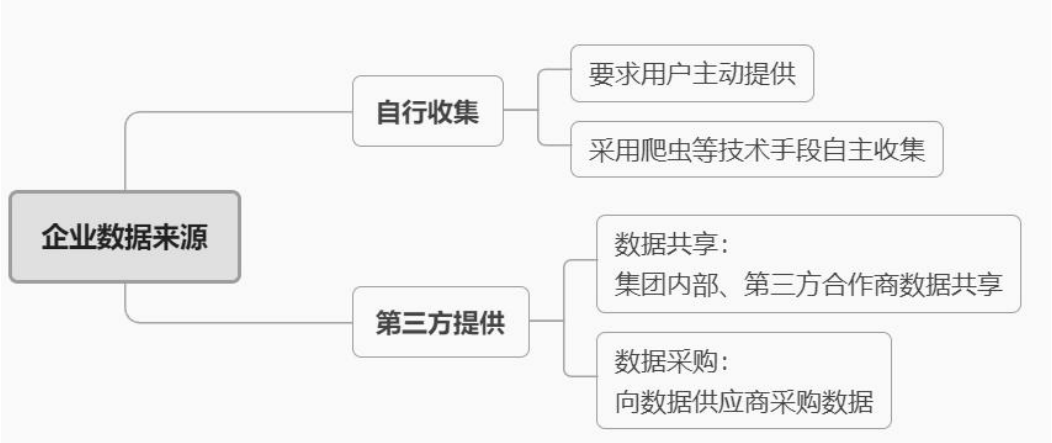


图 10企业数据来源图

(2) **数据获取方式的合规性**（包括第三方数据来源合规）；

(3) **是否建立相应机制保障第三方数据的合法合规性**。

关注焦点	问询对象/时间	问询内容
数据来源	中数智汇[54] 2020 年 8 月	发行人是否存在因**从互联网违规采集信息**而受到主管当局处罚、信息主体投诉或诉讼等纠纷事项。
	木瓜移动[55] 2020 年 11 月	补充披露发行人业务活动中使用数据及**获取数据的基本情况**，包括但不限于**数据来源、途径、所有权方**、存储位置、运用环节。

[54] 关于北京中数智汇科技股份有限公司首次公开发行股票并在科创板上市申请文件审核问询函的回复
[55] 北京市康达律师事务所关于北京木瓜移动科技股份有限公司首次公开发行股票并在创业板上市的补充法律意见书（一）

关注焦点	问询对象/时间	问询内容
	微众信科[56] 2020 年 12 月	发行人及发行人的**数据供应商**从事数据服务是否需要取得特殊资质、许可或备案，当前数据服务行业(提供商)的相关主要监管规定；发行人当前从事数据交易是否要求数据提供方**说明数据来源**，并留存审核、交易记录等内控机制。
	华夏电通[57] 2023 年 11 月	请发行人说明公司是否存在对外采购原料数据的情形，如是，请进一步说明发行人及其原料数据采集供应商相关数据的获取方式及其合规性。
获取方式	微众信科[58] 2020 年 12 月	发行人**自行采集数据采用的技术，内容是否合法合规，程序是否正当；是否存在采用特殊互联网手段（或技术）采集法律法规规定不属于公开的社会信息或需要特殊许可等前置程序方可获取数据的情形；发行人采集需要信息主体授权方能获取的信息（包括纳税）等获得授权的具体实现方式**。
	合合信息[59] 2022 年 9 月	**自动化访问获取的企业数据确保来源合法性**的具体方式。
	麦驰物联[60] 2023 年 5 月	说明业主是否有权利拒绝发行人收集相关数据，如拒绝，是否影响业主正常出入小区等合法权益，相关约定是否实际具有强制性。
内部机制	中数智汇[61] 2020 年 10 月	发行人向供应商采购的数据其来源是否合法合规，发行人**是否有相应机制保障供应商提供数据的合法合规性**。

表 8 数据收集合规相关问询

问题 11： 直接从用户获得数据，需要关注什么？

处理个人信息，应当具备《个信法》规定的合法性基础。根据《个信法》，除下

[56] 关于深圳微众信用科技股份有限公司首次公开发行股票并在科创板上市申请文件的审核问询函之回复报告

[57] 关于北京华夏电通科技股份有限公司向不特定合格投资者公开发行股票并在北京证券交易所上市申请文件的审核问询函的回复

[58] 关于深圳微众信用科技股份有限公司首次公开发行股票并在科创板上市申请文件的审核问询函之回复报告

[59] 关于上海合合信息科技股份有限公司首次公开发行股票并在科创板上市申请文件的首轮审核问询函的回复

[60] 关于深圳市麦驰物联股份有限公司首次公开发行股票并在创业板上市申请文件的审核问询函的回复

[61] 关于北京中数智汇科技股份有限公司首次公开发行股票并在科创板上市申请文件审核问询函的回复

列情形外，直接从用户获得数据，需要以“告知”用户并取得用户“同意”为前提（特殊情形下还需要获得用户的“单独同意”，详见本团队文章《平台处理个人数据需要取得“单独同意”的情形》）。除下列情形外：

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

(2) 为履行法定职责或者法定义务所必需；

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

(4) 为公共利益实施新闻报道、舆论监督等行为，在合理的范围内处理个人信息；

(5) 依照《个信法》规定在合理的范围内处理个人自行公开或者其他已经合法公开的个人信息；

(6) 法律、行政法规规定的其他情形。

可见，无需用户同意的情形在一般业务开展中难以直接适用，**“告知-同意”则成为企业直接获取用户数据最为常见的合法性基础**。具体而言，应“**以显著方式、清晰易懂的语言**”告知，并取得个人在“**充分知情**”、“**自愿**”、“**明确**”的前提下作出的同意。利用文字和 UI 界面设计诱导用户作出同意的“**黑模式**”（Dark Pattern）[62]，如利用 APP 界面上的字体颜色、大小，来影响用户作出知情、自愿给出的同意，并不满足《个信法》的要求，将面临侵犯用户个人信息权益的法律风险。

“告知-同意”规则详细如下图所示：

[62] 根据欧盟数据保护委员会（EDPB）于 2022 年 3 月发布的《Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them》，黑模式是指一种产品设计模式，其目的是通过软件界面（interface）及用户体验（user experiences）致使用户对其个人数据作出无意识、非自愿且可能有害的决定

图 11"告知-同意"规则合规要点

问题 12： 爬取第三方企业数据，是否会构成不正当竞争行为？

爬虫系一种高效数据收集方式，深受青睐。然而，技术中立，法律有界。爬虫行为若不加以规制，则有可能侵犯第三方的合法权益，或面临刑事上的侵犯公民个人信息罪、非法侵入计算机系统罪等入罪风险，或面临民事上的不正当竞争等风险（详见本团队文章《一文读懂个人信息爬虫技术合规风险——基于爬虫相关侵权案件的梳理》）。从披露的法院案例数量分析，以爬取第三方企业的数据构成不正当竞争案件数量占大多数。因此，我们就爬取行为是否会面临不正当竞争的法律风险，梳理如下：

➢ 法律规制

当前我国关于爬虫行为的反不正当竞争法规制，具体如下表所示

要点	法条内容
不正当竞争行为类型	
一般不正当竞争行为	**《反不正当竞争法》[63]第二条：** 本法所称的不正当竞争行为，是指经营者在生产经营活动中，违反本法规定，扰乱市场竞争秩序，损害其他经营者或者消费者的合法权益的行为。
特殊不正当竞争行为	**《反不正当竞争法》第十二条：** 经营者利用网络从事生产经营活动，应当遵守本法的各项规定。 经营者不得利用技术手段，通过影响用户选择或者其他方式，实施下列妨碍、破坏其他经营者合法提供的网络产品或者服务正常运行的行为： （一）未经其他经营者同意，在其合法提供的网络产品或者服务中，插入链接、强制进行目标跳转； （二）误导、欺骗、强迫用户修改、关闭、卸载其他经营者合法提供的网络产品或者服务； （三）恶意对其他经营者合法提供的网络产品或者服务实施不兼容； （四）其他妨碍、破坏其他经营者合法提供的网络产品或者服务正常运行的行为。

[63] 发布机构：全国人大常委会；2019.04.23 发布；2019.04.23 施行

要点	法条内容
	《禁止网络不正当竞争行为规定(公开征求意见稿)》[64]第二十条： 经营者不得利用技术手段，非法抓取、使用其他经营者的数据，并对其他经营者合法提供的网络产品或者服务的主要内容或者部分内容构成实质性替代，或者不合理增加其他经营者的运营成本，减损其他经营者用户数据的安全性，妨碍、破坏其他经营者合法提供的网络产品或者服务的正常运行。
法律责任	
民事责任	**《反不正当竞争法》第十七条：** 经营者违反本法规定，给他人造成损害的，应当依法承担民事责任。 经营者的合法权益受到不正当竞争行为损害的，可以向人民法院提起诉讼。 因不正当竞争行为受到损害的经营者的赔偿数额，按照其因被侵权所受到的实际损失确定；实际损失难以计算的，按照侵权人因侵权所获得的利益确定。
行政责任	**《反不正当竞争法》第二十四条：** 经营者违反本法第十二条规定妨碍、破坏其他经营者合法提供的网络产品或者服务正常运行的，由监督检查部门责令停止违法行为，处十万元以上五十万元以下的罚款；情节严重的，处五十万元以上三百万元以下的罚款。
	《禁止网络不正当竞争行为规定(公开征求意见稿)》第三十五条： 经营者违反本规定第二十条的，由市场监管部门依据反不正当竞争法第二十四条的规定处罚。

表 9 爬虫行为反不正当竞争法规制要点

➢ 判定维度

我们以“爬虫”等关键词在中国裁判文书网检索并筛选出 9 例[65]涉不正当竞争纠纷案件，经梳理后发现，这类案件的争议焦点主要集中于以下三个方面：涉案双方是否构成竞争关系、涉案行为是否构成不正当竞争以及赔偿额如何确定。具体分

[64] 发布机构：国家市场监督管理总局；2021.08.17 发布；征求意见至 2021.09.15

[65] (2020)粤 0104 民初 46873 号； (2021)浙 8601 民初 309 号；(2017)京 0108 民初 24512 号； (2019)京 73 民终 2799 号； (2016)京 73 民终 588 号； (2019)京 73 民终 3789 号； (2019)浙 0108 民初 5049 号； (2021)京民终 281 号； (2020)粤 0104 民初 46873 号

析总结如下图所示：

图 12爬虫不正当竞争之判定维度

(一)竞争关系的认定

法院在判断爬虫行为是否构成不正当竞争时，首先会分析涉案双方之间是否构成竞争关系。现有司法实践均未局限于涉案双方是否构成在整体业务模式上构成同业竞争，而是聚焦于**爬虫行为所涉及的双方之间的产品或服务是否有替代关系**。

除此之外，若该爬取数据并使用的行为导致对其他经营者利益造成损害的可能性，且其同时会基于该行为获得现实或潜在的经济利益，**构成“此消彼长”的关系，亦可能被法院判定为构成“竞争关系”**。

(二)不正当竞争行为的认定

1. 《反不正当竞争法》具体条款的适用

在判定具体爬虫行为是否构成不正当竞争行为前，需要先明确判断标准：爬虫行为是属于《反不正当竞争法》第十二条规定的特殊不正当竞争行为；还是适用第二条规定的一般兜底条款进行判定。

2. 爬取行为是否具备不正当性的判定维度

(1) 特殊不正当竞争行为

部分案件在审查爬虫行为是否构成特殊不正当竞争行为时，会从爬取的是否为公开数据、爬取公开/非公开数据的行为是否正当来进行判断；

部分案件在审查时，还会结合《反不正当竞争法》第二条进行考虑，即额外考虑该爬虫行为是否有违诚实信用原则、属于技术创新的公平竞争、是否有违竞争者自由竞争利益、消费者自主决策权利及社会公共利益等。

(2) 一般不正当竞争行为

当爬虫行为被认定为可能构成一般不正当竞争行为时，部分法院聚焦于被爬取方是否因不正当竞争行为受到损害；而部分法院则考虑该不正当竞争是否侵害其他经营者的合法权益、违反市场竞争秩序及侵犯消费者的合法权益。

(三)赔偿额的认定

一旦爬虫行为被认定为构成不正当竞争行为，爬取方所应承担的赔偿责任成为案件焦点。赔偿额一般包括经济损失及合理支出，具体数额则往往取决于法院的酌定考量。

对于经济损失，被爬取方需提供证据证明其因此所遭受的实际损失或爬取方的非法获利，但在绝大多数案件中，涉案双方很难向法院提交充分证据证明损失或获利，因此法院往往还会综合被爬方的公证费、律师费等合理支出，酌情予以确定。

问题 13： 如何避免爬虫被认定构成不正当竞争行为？

从“问题 12：爬取第三方企业数据，是否构成不正当竞争行为？”可知，法院认定爬虫行为是否构成不正当竞争首要条件是判断双方是否具有竞争关系，而基于互联网公司的特性，法院在认定双方是否构成竞争关系时并不局限于同业竞争，只要在某一范围内用户出现重合，法院即倾向于认定双方存在竞争利益。

我们以“爬虫”、“不正当竞争”为关键词在中国裁判文书网进行检索，共筛选出近十年（2011-2022）发生的 12 起典型案例[66]，发现爬取方胜诉的仅 2 起。

因此，我们建议，若采用爬虫方式获取数据，应注意以下几点，以避免被认定构成不正当竞争行为：

(1) **合规评估**：建议建立第三方审查制度，与专业的中立机构（如律师事务所、专业咨询机构等）合作，在爬取数据前结合爬取目的、性质、方式、频率等方面进行评估。

(2) **合法获取**：

(a) **依法申请**：就政府公共数据而言，对于有条件开放的公共数据，应当根据当地公共数据开放的具体流程，依法向有关部门提交申请；

(b) **协议许可**：遵守被爬取方的 Robots 协议，如若面对不合理的 Robots 协议，可以尝试走“协商-通知”路径（详见本团队文章《爬虫之责：反不正当竞争案中的胜诉机会在哪里？（上篇）》《爬虫之责：反不正当竞争案中的胜诉机会在哪里？（下篇）》）；

(c) **三重授权**：如爬取数据涉及用户的个人信息，建议遵守“用户授权平台+平台授权爬取方+用户授权爬取方”的三重授权原则进行抓取。

(3) **合理限度**：抓取数据需要在合理限度内，不能对服务器造成压力；

(4) **合法使用**：抓取数据涉及个人信息的，建议遵循《个信法》规定的公开个人信息处理规则，对于个人明确提出拒绝的，应当及时撤回或删除相关个人信

[66]（2021）浙 0110 民初 2914 号；（2017）京 0108 民初 24510 号；（2016）沪 73 民终 242 号；（2011）中民终字第 7512 号案例；(2019)京 73 民终 3789 号；(2016)京 73 民终 588 号； (2017)京 0108 民初 24512 号；(2021)浙 8601 民初 309 号；(2013)一中民初字第 2668 号； (2021)浙 8601 民初 309 号；(2019)浙 0108 民初 5049 号； (2015)浦民三(知)初字第 143 号

息；若处理已公开的个人信息，对个人权益有重大影响的，还应当取得个人同意。

(5) **呈现形式**：在爬取数据的呈现形式上，建议明确显示数据来源，并考虑设置跳转链接等不影响被爬取方平台正常经营活动的形式。

如在前锦网络信息技术(上海)有限公司（下称“前锦公司”，前程无忧网站运营主体）与上海逸橙信息科技有限公司（下称“逸橙公司”）其他不正当竞争纠纷一案[67]中，逸橙公司向用户提供关联前程无忧网站账号的功能，并通过该账号在前程无忧网站下载简历，保存在自身服务器中并在日常经营中使用。

法院认定，逸橙公司提供的是关联、并同步企业用户已获得的简历的功能，企业用户如需购买简历、发布职位信息等，仍需登录前锦公司网站完成，因此该功能给前锦公司流量造成的损失有限，尚未达到需要司法救济的程度，最终认定不构成不正当竞争。

[67] (2019)沪 73 民终 263 号

问题 14：　爬取政府公共数据，需要关注什么？

在“数字政务”的时代下，相关政府部门掌握着大量的公共数据。为了最大限度地释放公共数据的价值，打破“数据孤岛”的困境，上海、浙江、江苏、深圳等地纷纷出台专门面向公共数据领域的法律规范，有序开放、共享公共数据，鼓励第三方深化对公共数据的挖掘利用。但是目前可见的数据利用方式，通常依托政府自身搭建的数据服务中心或服务平台。

因此对于未开放或者有条件开放的公共数据，如果利用爬虫技术避开或者突破计算机信息系统的安全保护措施，未经授权或者超越授权获取前述数据的，根据计算机信息系统的类型不同，将可能构成下述刑事犯罪：

计算机信息系统类型	非法行为	适用罪名
国家事务、国防建设、尖端科学技术领域**以内**的计算机信息系统	违反国家规定侵入。	非法侵入计算机信息系统罪
国家事务、国防建设、尖端科学技术领域**以外**的计算机信息系统	违反国家规定侵入或者采用其他技术手段： (1) 获取系统中存储、处理或传输的数据，情节严重的；	非法获取计算机信息系统数据罪
	(2) 对该系统实施非法控制，情节严重的。	非法控制计算机信息系统罪
计算机信息系统	(1) 提供专门用于侵入、非法控制系统的程序、工具，情节严重的，或者； (2) 明知他人实施侵入、非法控制系统的犯罪行为而为其提供程序、工具，情节严重的。	提供侵入、非法控制计算机信息系统程序、工具罪
	(1) 违反国家规定对系统功能进行删除、修改、增加、干扰，造成其不能正常运行，后果严重的； (2) 违反国家规定对系统中存储、处理或者传输的数据和	破坏计算机信息系统罪

计算机信息系统类型	非法行为	适用罪名
	应用程序进行删除、修改、增加的操作，后果严重的。	

表 10爬取政府公共数据相关刑事风险

除此之外，即使是依法合规地获取公开数据，也不意味着可以随心所欲地使用。建议从下述维度完善合规使用流程和制度：

(1) 保障个人拒绝权：

根据《个信法》规定，个人信息处理者可以在合理的范围内处理个人自行公开或者其他已经合法公开的个人信息，但个人明确拒绝的除外。对于公开数据的获取，应向个人提供便于拒绝的通道，保障个人信息主体的拒绝权。

(2) 评估影响度：

根据《个信法》规定，个人信息处理者处理已公开的个人信息，对个人权益有重大影响的，应当取得个人同意。为防止处理的个人信息对个人权益造成重大影响而应当事前取得个人同意，建议在获取公开数据前评估对于个人权益可能造成的影响，并保存评估记录。

(3) 评估与监测正当性：

为预防前述法律风险，建议事前评估所采取的技术措施是否具有正当性，并重视事中监测，定期进行检测与复盘，包括但不限于：

(a) 被采集网站是否具备 Robots 协议或公示条款限制自动化采集；

(b) 被采集网站是否具备自动化采集限制措施；

(c) 自动化采集数量及频率是否影响采集对象网站的正常运行；

(d) 自身自动化采集技术能否确保不删除、不篡改、不破坏被采集网站数据，不存在钓鱼链接、木马程序、植入后门等可能干扰被采集网站的情形等。

问题 15：　直接从第三方采购数据，需要关注什么？

若从第三方采购数据，上市审核机构会特别关注数据供应商是否具备相关资质、其提供数据行为是否合法等问题。

对此，我们建议通过以下方式，针对数据供应商建立审核评价机制以及证据链留存机制：

(1) **资质有效**：确认数据供应商的数据提供行为是否需要具备相应资质（包含数据安全相关资质（如 ISO27001 信息安全体系认证、网络安全等级保护三级认证等，如涉及征信业务的，还应取得征信资质，详见“问题 8：提供数据服务是否需要相关资质、许可、认证及备案？”），并要求其承诺在数据供应过程中保证资质持续有效；

(2) **来源合规**：

- **数据主体的有效授权**：通过要求数据供应商出示数据主体的授权许可文件及要求其签署承诺函等方式，保障数据来源合规采集；
- **特殊数据的保护要求**：如重要数据处理者应当采购可信的产品或服务，并且交易重要数据时，应尽量取得相关主管部门的许可；采购敏感个人信息、儿童个人信息时，应注意进行个人信息安全影响评估；
- **采购境外数据**：若涉及到采购境外数据，可要求数据供应商出具出售境外数据不违背境外法律法规的承诺函；

(3) **责任明确**：明确需要数据供应商提供的数据范围，包括但不限于数据主体范围、数据类别（如个人信息/敏感个人信息/重要数据等）、采购数量等，并通过协议明确约定数据范围以及双方的权利义务。同时，针对可能发生的数据安全纠纷事件，设定好责任承担及纠纷解决机制；

(4) **证据留存**：建立证据留存机制，保留数据采购全流程的书面记录。当后续发生数据泄露等事件时，有助于“自证清白”。

问题 16：　如何建立数据收集环节的内控制度？

数据收集环节为整个数据处理流程的初始阶段，建立有效的内控制度是**防止“出师不利”**的有效手段。

实践中，上市审核机构亦会重点关注拟上市企业在数据收集环节建立的内控制度（拟上市企业整体数据安全内部管理制度的构建，详见本文“问题 45：如何建立数据安全内部管理制度？”）。

对此，我们建议结合数据收集的对象与方式，建立对应风险防范内控制度：

(1) **数据收集记录制度**；

(2) **自动化访问影响度评估制度**；

(3) **自动化访问正当性评估制度**；

(4) **自动化访问定期检测制度**；

(5) **第三方数据供应商准入与筛选制度**；

(6) **第三方数据供应商评价与追责制度**；

(7) **数据主体权益保障与纠纷解决机制**等。

其中以**数据收集记录制度**为例，建立有效的数据收集记录制度，应涵盖记录主体、记录方式、记录内容、记录周期、检查机制等必要内容。针对数据收集记录的内容，应包含数据获取方式、数据来源主体信息（含其数据安全负责人/个人信息保护负责人姓名及联系方式）、数据收集内容、拟使用目的、采取的安全保障措施等。

(二)数据使用合规 12 问

通过分析各拟上市企业披露的问询函可知，在数据使用合规环节，上市审核机构核心关注以下六点：

(1) 是否超出相应的授权范围使用数据？

(2) 数据使用过程中是否侵犯个人隐私或其他合法权益？

(3) 使用数据进行商业化变现是否合理？是否存在违规使用数据牟利行为？

(4) 算法推荐技术的使用是否合规？

(5) 是否涉及科技伦理等敏感领域？

(6) 个人信息处理者与受托人的合作机制？

关注焦点	问询对象/时间	问询内容
数据使用	蚂蚁集团[68] 2020 年 9 月	对于业务开展过程中获取的海量数据如何进行管理和运用，**是否存在侵犯其他方数据隐私的情况**，是否履行了与其他方关于数据安全的约定，对于数据的获取、**管理和使用是否合法合规**。
	微众信科[69] 2020 年 12 月	发行人是否**存在超出法律规定、信息主体授权的范围和目的**收集信息、向客户提供数据的情形，**是否在法律、行政法规规定的范围内履行必要的限度原则**采集和**运用信息**。
	墨迹天气[70] 2019 年 10 月	发行人通过自主收集及第三方途径获取用户数据及标签，并利用数据进行商业化变现，发行人于 2019 年 7 月 16 日收到 APP 专项治理组发出的《关于 APP 收集使用个人信息相关问题的通知》，APP 专项治理工作组要求发行人就收集使用个人信息中存在的问题进行整改。请发行人代表说明：…（2）**发行人使用用户数据是否合法合规，尤其是商业化变现的合规性**，结合相关媒体报道的墨迹天气上传用户隐私等情况，对照《网安法》《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》等法规和司法解释，说明报告期发行人是否存在侵犯用户隐私或数据的的情况，是否存在法律风

[68] 上海市方达律师事务所关于蚂蚁科技集团股份有限公司首次公开发行人民币普通股（A 股）股票并在科创板上市的补充法律意见书

[69] 关于深圳微众信用科技股份有限公司首次公开发行股票并在科创板上市申请文件的审核问询函之回复报告

[70] 证监会《第十八届发审委 2019 年第 142 次会议审核结果公告》

关注焦点	问询对象/时间	问询内容
		险或潜在法律风险…
	合合信息 2023 年 6 月[71]	发行人关于获取、存储、使用数据的相关制度规范的制定时间、主要内容、执行情况，是否能够有效保障数据安全及业务合法合规
	睿联技术[72] 2023 年 9 月	是否存在发行人利用相关个人消费者或企业客户信息进行牟利等违法违规行为，是否存在侵犯个人隐私、商业秘密或其他侵权方面的情形。
	宇谷科技[73] 2023 年 11 月	是否存在利用获取、保管的用户、客户数据**开展商业用途**的情形。
	思迅软件[74] 2023 年 9 月	说明公司支付技术服务业务开展过程中是否存在收集、存储、传输、处理、使用客户数据或个人信息的情形，如是，请说明是否存在发行人利用相关个人消费者或企业客户信息进行牟利等违法违规行为，相关信息或数据获取及使用的合法合规性、风险控制制度及执行情况以及是否存在受到行政处罚的法律风险。
算法服务	杭州小影[75] 2022 年 2 月	结合《关于加强互联网信息服务算法综合治理的指导意见》的精神分析说明发行人产品所使用算法的发展趋势，前述《指导意见》规定的发展方向安全治理规则等对发行人技术研发、核心技术在产品或服务中的运用拟产生的影响，如有必要，请在招股说明书中细化提示相关产业政策、治理目标对发行人产品方向和业务内容产生影响的风险。
	木仓科技[76] 2022 年 6 月	请说明信息推送、交易推荐、提供算法推荐服务、用户权益保护等内容是否符合《互联网信息服务算法荐管理规定》。
		请说明公司驾考宝典 APP 在 360 手机助手应用上涉及“强制用户使用定向推送功能”等问题的整改情况。

[71] 关于上海合合信息科技股份有限公司首次公开发行股票并在科创板上市申请文件的首轮审核问询函的回复
[72] 关于深圳市睿联技术股份有限公司首次公开发行股票并在创业板上市申请文件的审核问询函的回复
[73] 北京市通商律师事务所关于杭州宇谷科技股份有限公司 首次公开发行股票并在创业板上市之补充法律意见书（二）
[74] 关于深圳市思迅软件股份有限公司公开发行股票并在北交所上市申请文件的审核问询函的回复
[75] 关于杭州小影创新科技股份有限公司首次公开发行股票并在创业板上市申请文件审核问询函的回复
[76] 关于武汉木仓科技股份有限公司首次公开发行股票并在创业板上市申请文件的审核问询函的回复

关注焦点	问询对象/时间	问询内容
科技伦理	奥比中光[77] 2022 年 4 月	结合自身技术特点，产品的应用场景，数据合规和科技伦理方面的法律法规、政策等，说明相关情况是否影响发行人下游行业的发展，进而影响发行人的持续经营能力；充分披露数据合规和科技伦理方面的法律法规、政策对发行人技术商业化带来的不利影响。
	合合信息[78] 2022 年 9 月	发行人是否涉及科技伦理敏感领域。
个人信息处理者与受托人合作机制	数聚智连[79] 2022 年 10 月	进一步说明发行人可获取、使用的数据具体类型、数量规模，与电商平台、品牌方之间关于用户个人数据使用的合作机制、权责划分机制。

表 11 数据使用合规相关问询

[77] 关于对奥比中光科技集团股份有限公司首次公开发行股票并在科创板上市发行注册环节反馈意见落实函的回复

[78] 关于上海合合信息科技股份有限公司首次公开发行股票并在科创板上市申请文件的首轮审核问询函的回复

[79] 关于北京数聚智连科技股份有限公司首次公开发行股票并在创业板上市申请文件的第二轮审核问询函的回复

问题 17：　未超范围使用数据，如何证明？

证明未超范围使用数据，可按以下四个步骤走：

(1) 第一步：谨遵最小必要

应谨遵最小必要原则，明确处理个人信息的目的，并在实现处理目的的最小范围内处理个人信息。最小必要的要求包括最小影响、直接关联、最小类型、最小频度、最小数量、最小权限、最短时间等维度（具体详见本团队文章《身份信息给不给？当“实名认证”遇到拦路虎：“最小必要原则”》《互联网平台“七步走”，从容应对<个信法>》）。

(2) 第二步：明示收集内容

在明确最小必要范围后，应在《隐私政策》中明确列示所需收集的个人信息，并清楚告知用户收集其个人信息后的使用目的是什么。

(3) 第三步：实现系统留痕

应严格按照《隐私政策》的规定范围对用户个人信息进行使用，并于系统中对用户同意处理个人信息的记录（如勾选同意《隐私政策》、点击同意按钮等）进行留痕。

(4) 第四步：重新取得同意

当个人信息的处理目的、处理方式和处理的个人信息种类发生变更时，应当重新取得个人同意。

问题 18：　未侵犯个人隐私或其他合法权益，如何证明？

个人信息往往与个人隐私权[80]、肖像权[81]等人格权益息息相关，但却无法完全将其完全归于个人信息权的范畴，具有独立的保护路径。因此，如需使用涉及个人肖像或隐私的个人信息，除了依据《个信法》要求保障个人信息主体权益外，亦需注意不可侵犯他人隐私权及肖像权。

(1) 个人隐私权、肖像权等人格权益

第一步：获取明确授权并留痕记录

如使用的个人信息中包含用户的肖像权、个人隐私权等相关权益的，应当以获得其授权同意、主动提供配合并许可使用相关权益为前提，且不得采用欺诈、诱骗或强迫等方式诱导用户。

第二步：采取去标识化等安全措施

建议针对这类个人信息采取去标识化处理措施，以保障用户个人的隐私权、肖像权等权益。

(2) 个人信息主体权利

根据《个信法》的规定，个人对其个人信息处理享有知情决定权、限制处理权、查阅复制权、可携带权、更正补充权、删除权、解释说明权、拒绝权等权利，个人信息处理者应当建立便捷的个人行使权利的申请受理和处理机制。因此，我们建议拟上市企业通过以下方式，保障个人信息主体权利：

第一步：严格落实“告知-同意”原则

个人信息处理者应按照“问题 11：　直接从用户获得数据，需要关注什么？”的建议，通过《隐私政策》等协议文本或系统提示向用户告知其拥有的个人信息主体权利，以及具体的行使方式。

第二步：系统功能中设置便捷的个人信息主体权利使用方式

---

[80] 《民法典》第一千零三十二条 自然人享有隐私权。任何组织或者个人不得以刺探、侵扰、泄露、公开等方式侵害他人的隐私权。隐私是自然人的私人生活安宁和不愿为他人知晓的私密空间、私密活动、私密信息

[81] 《民法典》第一千零一十八条 自然人享有肖像权，有权依法制作、使用、公开或者许可他人使用自己的肖像。肖像是通过影像、雕塑、绘画等方式在一定载体上所反映的特定自然人可以被识别的外部形象

在向用户告知个人信息主体权利后，系统设置亦应匹配《隐私政策》等协议中明确的个人信息主体权利行使路径，而非仅仅停留在“纸面上的合规”，或存在系统设置与《隐私政策》中告知的路径不一致等情形。

同时，该系统功能设置应足够便捷，建议从用户点击进入平台至行使相应权利的步骤不大于 4 步。

第三步：设置申诉、建议机制

个人信息处理者可于《隐私政策》等协议文本以及系统功能设置中明确个人信息权利行使的申诉、建议渠道，并及时反馈用户需求，保障其权利行使。

第四步：实现系统留痕

个人信息处理者可于平台系统中对用户同意处理个人信息的记录、行使个人信息主体权利的功能及记录、申诉建议渠道及用户具体的反馈内容和处理进度等内容进行留痕。

问题 19：　如何分清不同数据处理身份的责任和义务？

数据处理过程中，通常会涉及到**个人信息处理者（包含共同处理情形）**与**受托人**两个角色，角色定位不同代表着承担的法定义务不同。具体如下表所示：

序号	要点	内容
角色一	**个人信息处理者**	
1-1	**概念**	指在个人信息处理活动中自主决定处理目的、处理方式的组织、个人。
1-2	**核心义务**	**我们根据《个信法》独创梳理出“MACTOP”六大核心义务：** (1) M（“Management”）： 从系统资质、人员岗位设置及管理制度方面“自外而内”进行管理： (a) 建立与个人信息保护相关的内部管理制度和管理规程； (b) 落实个人信息保护负责人岗位设置； (c) 申请获得 ISO27001 信息安全管理体系认证、网络安全等级保护等资质。 (2) A（“Authorization ”&“Assessment”）： (a) 确定个人信息处理的操作权限，根据业务流、个人信息流，授权不同部门、人员进行相应的处理； (b) 定期进行合规审计，并依法履行个人信息保护影响评估义务，予以记录与留痕。 (3) C（“Category”）： 对个人信息进行分类管理，根据不同类别赋予不同数据保护工具。如区分一般个人信息、敏感个人信息等类别给予不同维度的保护层级。 (4) T（“Technology”）： 采取相应的加密、去标识化等安全技术措施，来保护经分类和授权处理的个人信息。 (5) O（“Organization”）： 定期对从业人员进行安全教育和培训。如通过签署保密协议、进行背景调查、定期安全教育、定期培训等方式，增强从业人员对于个人信息保护的合规意识，亦可进一步明确内部涉

序号	要点	内容
		及个人信息处理不同岗位职责和处罚机制。 (6) P（“Plan”）： 建立个人信息安全事件应急预案并定期组织相关人员进行演练，履行个人信息泄露通知、补救等各项义务与流程，明确各主体责任。
角色二	**受托人**	
2-1	**概念**	受个人信息处理者的委托处理个人信息的主体。
2-2	**核心义务**	(1) **应当按照约定处理个人信息，不得超出约定的处理目的、处理方式等处理个人信息**； (2) 委托合同不生效、无效、被撤销或者终止的，应当将个人信息返还个人信息处理者或者予以删除，不得保留； (3) 未经个人信息处理者同意，受托人**不得转委托**他人处理个人信息； (4) 受托人应当**采取必要措施保障所处理的个人信息的安全**，并**协助个人信息处理者履行《个信法》规定的义务**。

表 12个人信息处理者与受托人的主要区别

问题 20：　委托他人处理个人信息，应该怎么做？

在数聚智连上市审核过程中，上市审核机构已经开始关注个人信息处理者与受托人关于个人信息处理合作机制与权责分担的问题，因此，建议拟上市企业在委托他人处理个人信息时，通过以下步骤[82]，确保委托处理行为合规：

(1) 第一步：进行个人信息安全影响评估

根据我国《个信法》明确要求，委托他人处理个人信息的，属于个人信息安全影响评估的法定情形（详见“问题 9：如何正确认知个人信息安全影响评估？”）。

(2) 第二步：明确具体的约定委托处理内容

个人信息处理者委托处理个人信息的，应当与受托人约定委托处理的目的、期限、处理方式、个人信息的种类、保护措施以及双方的权利和义务等内容。

个人信息处理者还应注意，委托处理范围不应超过个人信息主体授权同意的范围，除非属于无需获得同意的情形（详见“问题 11：直接从用户获得数据，需要关注什么？”）。

(3) 第三步：对受托人处理行为进行监督

个人信息处理者应对受托人的处理行为进行监督，方式包括通过合同等方式规定受托人的责任和义务、对受托人进行审计等。

(4) 第四步：准确及时记录委托行为

个人信息处理者应准确并及时记录和存储委托处理个人信息的情况，包括受托人名称、联系方式、资质许可、委托处理目的、范围、期限、处理方式、签署的合同文本等内容。

(5) 第五步：及时采取补救措施

若个人信息处理者发现受托人未按照委托要求处理个人信息，或未能有效履行个人信息安全保护责任的，应立即要求受托人停止相关行为并采取有效补救措施，控制或消除个人信息面临的安全风险。必要时个人信息处理者应终止与受托人的业务关系，并要求受托人及时删除其获得的个人信息。

[82] 参考《个人信息安全规范》

问题 21： 作为算法服务提供者，需要承担哪些主体义务与责任？

算法，是为解决某个问题、完成某项任务或达到某种目的而采取的处理规则、运算指令、策略机制，体现为一种辅助人类决策或自主决策机制[83]。

根据《互联网信息服务算法推荐管理规定》[84]，算法服务提供者主体义务及应当承担的义务及法律责任如下图所示：

[83] 《算法治理蓝皮书》，中国信息通信研究院和新华网大数据中心著，2022 年 1 月出版
[84] 发文机构：网信办；2021.12.31 日 发布；2022.03.01 施行

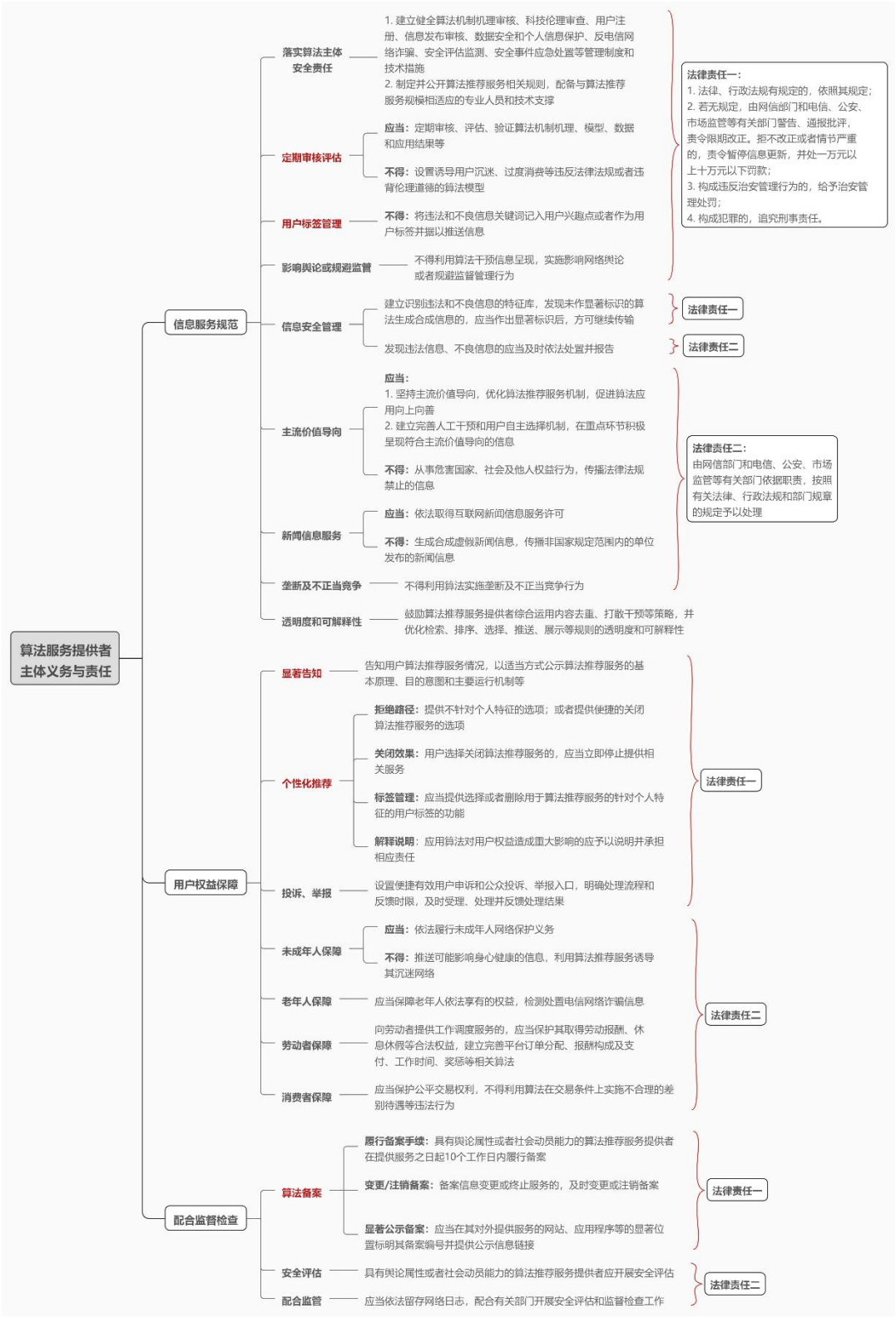


图 13算法服务提供者主体义务及责任要点梳理

问题 22： 什么情况下需要进行算法备案？

根据《互联网信息服务算法推荐管理规定》的要求，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履行备案手续。

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。

而根据《具有舆论属性或社会动员能力的互联网信息服务安全评估规定》[85]，具有舆论属性或社会动员能力的互联网信息服务，包括下列情形：

（一）开办论坛、博客、微博客、**聊天室、通讯群组、公众账号、短视频、网络直播、信息分享、小程序等信息服务或者附设相应功能**；

（二）开办提供公众舆论表达渠道或者具有发动社会公众从事特定活动能力的其他互联网信息服务。

符合上述规定的互联网平台，均应进行算法备案。

[85] 发布机构：网信办、公安部；发布时间：2018.11.15；生效时间：2018.11.30

问题 23：　如何进行算法备案？

根据《互联网信息服务算法推荐管理规定》的要求，具体备案程序如下表所示（详见本团队文章《算法之治：我的信息成了你的生意》）：

序号	要点	内容
1	**应备案内容**	应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。 ***注：根据《互联网信息服务算法备案系统使用手册》，具体备案信息如下：*** ***(1) 算法基础属性信息：****包括算法类型、算法名称、上线时间、应用领域、算法安全自评估报告、拟公示内容等；* *(2)* ***算法详细属性信息：****包括算法简介、使用场景、算法数据、算法模型、算法策略和算法风险与防范机制等信息；* *(3)* ***产品及功能信息：****产品信息：产品名称、产品的服务形式、访问地址、服务状态、服务对象、产品使用是否需要实名认证和前置许可、产品功能访问路径等；功能信息：功能名称、功能介绍。*
2	**备案审查机构**	(1) **审查主体**：国家和省、自治区、直辖市网信部门； (2) **备案方式**：互联网信息服务算法备案系统，https://beian.cac.gov.cn； (3) **审查时间**：收到备案材料后在三十个工作日内。
3	**变更与终止**	(1) **备案信息变更**：应当在变更之日起十个工作日内办理变更手续； (2) **终止提供服务**：应当在终止服务之日起二十个工作日内办理注销备案手续，并作出妥善安排。
4	**备案信息公示**	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。
5	**法律责任**	(1) **应备案未备案** 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

序号	要点	内容
		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。 **(2) 备案瑕疵** 具有舆论属性或者社会动员能力的算法推荐服务提供者通过隐瞒有关情况、提供虚假材料等不正当手段取得备案的，由国家和省、自治区、直辖市网信部门予以撤销备案，给予警告、通报批评；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。

表 13算法备案流程[86]

[86] 截至 2023 年 4 月，已有 262 个算法于互联网信息服务算法备案系统进行算法备案；截至 2023 年 6 月，已有 41 个算法于互联网信息服务算法备案系统进行深度合成服务算法备案。

问题 24：　使用数据进行个性化推荐，需要注意什么？

个性化推荐属于算法推荐中的一种典型形式，是商业变现场景中最为普遍的一种技术实现路径。

为了向用户提供个性化的服务，不少拟上市企业会通过对数据进行分析、整理及自动化决策，以求更精准地触达用户需求，同时能够实现数据的商业化变现。因此上市审核机构也愈发重视个性化推荐功能的合规性，如木仓科技在上市审核过程中，就被问询到其主要产品“驾考宝典”使用算法推荐服务是否符合《互联网信息服务算法推荐管理规定》、被通报过的“强制用户使用定向推送功能”整改情况。

➢ 个人信息保护

根据《个信法》的规定，针对自动化决策，企业可以采取以下两个路径：

(1) 为个人提供**不针对个人特征**的选项；

(2) 为用户提供**便捷**的拒绝方式。

基于大部分企业难以割舍商业化利用用户信息的资源禀赋，往往会选择第二种路径，给予用户拒绝权，但在保障用户的拒绝权上，便捷度与彻底度上尽显“暧昧”态度，存在侵犯个人信息主体权益的法律风险（详见本团队文章《个性化推荐：头部平台割舍不下的“唐僧肉”》）：

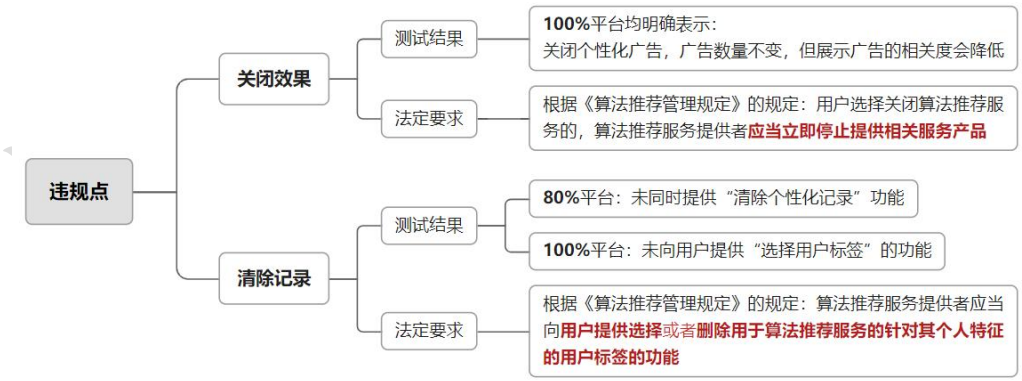


图 14 自动化决策违规要点[87]

[87] 截止至 2022 年 4 月

对此，建议拟上市企业事先依法进行个人信息安全影响评估并对处理情况予以记录（使用个人信息进行个性化推荐等自动化决策行为，属于《个信法》规定的个人信息安全影响评估的法定触发要件之一，因此拟上市企业必须进行评估），确保“用之有度”，嵌入保障用户各项合法权益的功能设计，畅通用户权利响应通道，及时处理用户的各项请求。

- **算法推荐管理**

同时，由于平台向用户提供的个性化推荐服务，属于以算法推荐技术提供互联网信息服务，应当受到《算法推荐管理规定》的制约，承担算法推荐服务提供者主体责任（详见问题 21：作为算法服务提供者，需要承担哪些主体责任），若属于具有舆论属性或者社会动员能力的算法推荐服务提供者，还应进行算法备案（详见问题 22：什么情况下需要进行算法备案？）。

问题 25：　什么是互联网服务深度合成技术？

深度合成技术，是指利用深度学习、虚拟现实等生成合成类算法制作文本、图像、音频、视频、虚拟场景等网络信息的技术。2017 年，一位名叫“Deepfakes”的用户在美国 Reddit 网站上分享了篡改人脸的色情视频，将深度合成技术带到了大众面前[88]。随后，深度合成技术强大的仿真能力引发了公众对于金融诈骗、色情内容、个人隐私、商业诋毁等方面的担忧。为加强我国深度合成技术管理，保护国家、社会和个人的合法权益，网信办、工信部、公安部三部门联合制定并发布了《互联网信息服务深度合成管理规定》[89]（下称《管理规定》），根据该《管理规定》及相关研究报告，深度合成技术类别及实践案例包括但不限于：

序号	《管理规定》定义	实践案例[90]
1	篇章生成、文本风格转换、问答对话等生成或者编辑文本内容的技术	2017 年底，清华大学发布了基于深度学习技术的诗歌写作系统“九歌”
2	文本转语音、语音转换、语音属性编辑等生成或者编辑语音内容的技术	2019 年央视《经典咏流传》，推出了 AI 小工具“读诗成曲”。用户仅需朗读一段诗词，就能听到用自己声音唱诵的经典诗词唱段
3	音乐生成、场景声编辑等生成或者编辑非语音内容的技术	词曲写作、伴奏生成、歌声合成
4	人脸生成、人脸替换、人物属性编辑、人脸操控、姿态操控等生成或者编辑图像、视频内容中生物特征的技术	AI 换脸“拯救”被劣迹艺人殃及的影视作品，电视剧《长安十二时辰》、《光荣时代》等多部作品均使用了该技术
5	图像生成、图像增强、图像修复等生成或者编辑图像、视频内容中非生物特征的技术	绘制像素画，辅助动画和游戏设计
6	三维重建、数字仿真等生成或者编辑数字人物、虚拟场景的技术	元宇宙、虚拟偶像洛天依

表 14深度合成技术类别及实践案例

[88] 《深度合成十大趋势报告（2022）》，清华大学人工智能研究院、北京瑞莱智慧科技有限公司、清华大学新传院智媒研究中心、国家工业信息安全发展研究中心著，2022 年 2 月

[89] 发布机关：网信办、工信部、公安部；2022.11.25 发布；2023.01.10 实施

[90] 《深度合成十大趋势报告（2022）》，清华大学人工智能研究院、北京瑞莱智慧科技有限公司、清华大学新传院智媒研究中心、国家工业信息安全发展研究中心著，2022 年 2 月

问题 26：　深度合成服务提供者具有哪些义务？

根据《管理规定》，深度合成主体分为深度合成服务提供者[91]、深度合成服务技术支持者、深度合成服务使用者[92]三类。对于**深度合成服务提供者**从**落实信息安全主体责任、数据和技术管理规范、算法备案与安全评估**等提出应履行以下义务：

序号	要点	内容
一	**落实信息安全主体责任**	
1-1	平台管理责任	1. **健全管理制度**：建立健全用户注册、算法机制机理审核、科技伦理审查、信息发布审核、数据安全、个人信息保护、反电信网络诈骗、应急处置等管理制度； 2. **技术保障措施**：具有安全可控的技术保障措施； 3. **提示信息安全义务**：以**显著方式提示**深度合成服务技术支持者和使用者承担信息安全义务； 4. **实名认证**：对深度合成服务使用者进行真实身份信息认证； 5. **投诉、举报机制**：建立投诉举报入口并及时受理反馈。
1-2	内容管理责任	1. **禁止发布**：不得发布法律、行政法规禁止的信息及虚假新闻信息； 2. **审核义务**：应对输入数据和合成结果进行审核； 3. **不良信息处理**：及时处理不良信息并向有关部门报告。
二	**数据和技术管理规范**	
2-1	加强训练数据管理	1. 采取必要措施保障训练数据安全； 2. 提供人脸、人声等生物识别信息编辑功能的，应当**提示**深度合成服务使用者**依法告知**被编辑的个人，并取得其**单独同意**。
2-2	加强技术管理	定期审核、评估、验证生成合成类算法机制机理。

[91] 深度合成服务提供者，是指提供深度合成服务的组织、个人
[92] 深度合成服务使用者，是指使用深度合成服务制作、复制、发布、传播信息的组织、个人

序号	要点	内容
2-3	信息标识	1. **一般标识：** 对使用其服务生成或者编辑的信息内容，应当采取技术措施添加不影响用户使用的标识，并依法保存日志信息。 **2. 显著标识：** **(1) 必须显著标识的服务内容** 深度合成服务提供者提供以下深度合成服务，**可能导致公众混淆或者误认的**，应当在生成或者编辑的信息内容的合理位置、区域进行**显著标识**，向公众提示深度合成情况： (a) 智能对话、智能写作等模拟自然人进行文本的生成或者编辑服务； (b) 合成人声、仿声等语音生成或者显著改变个人身份特征的编辑服务； (c) 人脸生成、人脸替换、人脸操控、姿态操控等人物图像、视频生成或者显著改变个人身份特征的编辑服务； (d) 沉浸式拟真场景等生成或者编辑服务； (e) 其他具有生成或者显著改变信息内容功能的服务。 **(2) 其他服务内容应提供显著标识功能** 提供前款规定之外的深度合成服务的，应当提供显著标识功能，并提示深度合成服务使用者可以进行显著标识。
三	**算法备案与安全评估**	
3-1	进行算法备案	**具有舆论属性或者社会动员能力的深度合成服务提供者**，应履行算法备案和变更、注销备案手续。
3-2	开展安全评估	1. 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； 2. 以下情形应当依法自行或者委托专业机构开展安全评估： (1) 生成或者编辑人脸、人声等生物识别信息的； (2) 生成或者编辑可能涉及国家安全、国家形象、国家利益和社会公共利益的特殊物体、场景等非生物识别信息。

表 15深度合成服务提供者义务要点

问题 27：　哪些企业会被关注科技伦理问题？

科技伦理是开展科学研究、技术开发等科技活动需要遵循的**价值理念和行为规范**，是促进科技事业健康发展的重要保障。

在 2021 年以前，我国主要聚焦于生物医药领域的科技伦理问题，通过《药品管理法》、《基本医疗卫生与健康促进法》、《医师法》、《生物安全法》等法律法规，规定了从事药物、医疗器械临床试验、医学研究、生物技术研究及医师诊疗应当遵循伦理规范，通过伦理审查。

算法及人工智能技术的广泛应用在提升生产效率、优化用户体验的同时，也带来算法歧视、大数据杀熟、不正当竞争等科技伦理道德方面的问题，因此，我国对于算法向善、可信人工智能等科技伦理治理的合规要求也在不断提高。

基于此，在拟上市企业审核过程中，以合合信息为代表的多家科技公司均受到来自上市审核机构关于科技伦理合规的问询，主要关注是否涉及科技伦理敏感领域，如是，则需论述在科技伦理领域是否符合相关法律法规规定。

根据《中共中央办公厅 国务院办公厅关于加强科技伦理治理的意见》（2022.03.20 实施，下称“《科技伦理治理意见》”）的规定，拟上市企业同时符合下述两个条件的，**应当设立科技伦理（审查）委员会**：

(1) **主体**：从事**生命科学、医学、人工智能**等科技活动的单位，且

(2) **研究内容：涉及科技伦理敏感领域**。当前，有关“科技伦理敏感领域”的具体涵义及范围尚未明确，有待相关细则文件的进一步出台。

问题 28：　如何进行科技伦理治理？

根据《科技伦理治理意见》，涉及科技伦理领域的企业，应当做好以下治理工作：

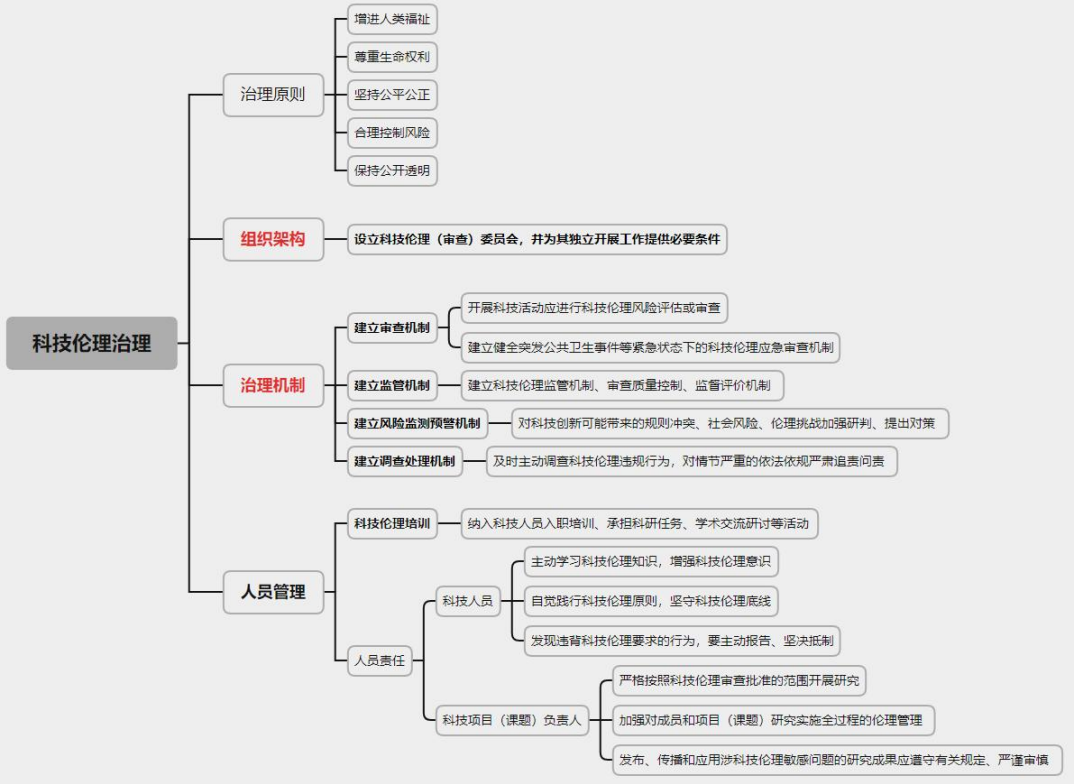


图 15科技伦理治理要点梳理

其中，针对人工智能领域，在科技伦理治理过程中，还应当关注国家新一代人工智能治理专业委员会所制定的《新一代人工智能伦理规范》（2021.09.25 实施）所规定的特别要求：

序号	要点	内容
一	**管理规范**	
1-1	推动敏捷治理	尊重人工智能发展规律，充分认识人工智能的潜力与局限，持续优化治理机制和方式，在战略决策、制度建设、资源配置过程中，不脱离实际、不急功近利，有序推动人工智能健康和可持续发展。
1-2	积极实践示范	遵守人工智能相关法规、政策和标准，主动将人工智能伦理道德融入管理全过程，率先成为人工智能伦理治理的实践者和推动者，及时总结推广人工智能治理经验，积极回应社会对人工智能的伦

序号	要点	内容
		理关切。
1-3	正确行权用权	**(1) 明确人工智能相关管理活动的职责和权力边界，规范权力运行条件和程序。** (2) 充分尊重并保障相关主体的隐私、自由、尊严、安全等权利及其他合法权益，禁止权力不当行使对自然人、法人和其他组织合法权益造成侵害。
1-4	加强风险防范	增强底线思维和风险意识，加强人工智能发展的潜在风险研判，及时开展**系统的风险监测和评估**，建立有效的风险预警机制，提升人工智能伦理风险管控和处置能力。
1-5	促进包容开放	充分重视人工智能各利益相关主体的权益与诉求，鼓励应用多样化的人工智能技术解决经济社会发展实际问题，鼓励跨学科、跨领域、跨地区、跨国界的交流与合作，推动形成具有广泛共识的人工智能治理框架和标准规范。
二	**研发规范**	
2-1	强化自律意识	加强人工智能研发相关活动的自我约束，主动将人工智能伦理道德融入技术研发各环节，自觉开展自我审查，加强自我管理，不从事违背伦理道德的人工智能研发。
2-2	**提升数据质量**	**在数据收集、存储、使用、加工、传输、提供、公开等环节，严格遵守数据相关法律、标准与规范，提升数据的完整性、及时性、一致性、规范性和准确性等**。
2-3	**增强安全透明**	在算法设计、实现、应用等环节，**提升透明性、可解释性、可理解性、可靠性、可控性**，增强人工智能系统的韧性、自适应性和抗干扰能力，**逐步实现可验证、可审核、可监督、可追溯、可预测、可信赖**。
2-4	**避免偏见歧视**	在数据采集和算法开发中，加强伦理审查，充分考虑差异化诉求，**避免可能存在的数据与算法偏见，努力实现人工智能系统的普惠性、公平性和非歧视性**。
三	**供应规范**	
3-1	尊重市场规则	严格遵守市场准入、竞争、交易等活动的各种规章制度，积极维护市场秩序，营造有利于人工智能发展的市场环境，不得以数据垄断、平台垄断等破坏市场有序竞争，禁止以任何手段侵犯其他

序号	要点	内容
		主体的知识产权。
3-2	加强质量管控	强化人工智能产品与服务的质量监测和使用评估，避免因设计和产品缺陷等问题导致的人身安全、财产安全、用户隐私等侵害，不得经营、销售或提供不符合质量标准的产品与服务。
3-3	**保障用户权益**	(1) 在产品与服务中使用人工智能技术应明确告知用户，应标识人工智能产品与服务的功能与局限，**保障用户知情、同意等权利**。 (2) 为用户**选择使用或退出人工智能模式提供简便易懂的解决方案**，**不得为用户平等使用人工智能设置障碍**。
3-4	强化应急保障	**研究制定应急机制和损失补偿方案或措施，及时监测人工智能系统，及时响应和处理用户的反馈信息**，及时防范系统性故障，随时准备协助相关主体依法依规对人工智能系统进行干预，减少损失，规避风险。
四	**使用规范**	
4-1	提倡善意使用	加强人工智能产品与服务使用前的论证和评估，充分了解人工智能产品与服务带来的益处，充分考虑各利益相关主体的合法权益，更好促进经济繁荣、社会进步和可持续发展。
4-2	避免误用滥用	充分了解人工智能产品与服务的适用范围和负面影响，切实尊重相关主体不使用人工智能产品或服务的权利，避免不当使用和滥用人工智能产品与服务，避免非故意造成对他人合法权益的损害。
4-3	禁止违规恶用	禁止使用不符合法律法规、伦理道德和标准规范的人工智能产品与服务，禁止使用人工智能产品与服务从事不法活动，严禁危害国家安全、公共安全和生产安全，严禁损害社会公共利益等。
4-4	及时主动反馈	积极参与人工智能伦理治理实践，对使用人工智能产品与服务过程中发现的技术安全漏洞、政策法规真空、监管滞后等问题，应及时向相关主体反馈，并协助解决。
4-5	提高使用能力	积极学习人工智能相关知识，主动掌握人工智能产品与服务的运营、维护、应急处置等各使用环节所需技能，确保人工智能产品与服务安全使用和高效利用。

表 16《新一代人工智能伦理规范》要点梳理

(三)数据共享合规 5 问

根据我国《数安法》与《个信法》[93]，并未将“共享”作为数据处理行为的正列举项，仅在《个人信息安全规范》中将“共享”定义为“个人信息控制者向其他控制者**提供**个人信息，且双方分别对个人信息拥有独立控制权的过程。”而欧盟的 GDPR[94]中，亦未将共享作为数据处理行为的正列举项。

因此，我们认为数据共享（包括数据融合）行为并非标准的法律用语表述，是基于商业数据处理的需求，对于**数据提供、共同处理、委托处理**等行为（相较《个人信息安全规范》而言，本文的定义较为延展）的概括性表达，各方的责任义务需视具体的处理情况而定。

通过分析各拟上市企业披露的问询信息情况可知，在数据共享环节（此处不包括因合并、分立、解散、破产等原因共享的），上市审核机构核心关注点在于：

(1) 数据共享是否符合与用户/客户的协议约定以及相关的法律法规规定；

(2) 数据共享可能给公司业务带来的相关风险，如数据共享的运作机制是否会给公司独立性以及市场竞争力带来影响。

关注焦点	问询对象/时间	问询内容
共享合规	蚂蚁集团[95] 2020 年 8 月	发行人与阿里巴巴集团的**数据共享是否符合各自与客户的协议约定，是否存在侵害客户合法利益的情况**；结合发行人与阿里巴巴等相关主体的数据共享协议，**说明该等安排是否违反有关互联网用户信息保护的有关法律法规及规范性文件**。
	京东数科[96] 2020 年 10 月	**数据共享是否符合各自与客户的协议约定，是否存在侵害客户合法利益的情况**；结合发行人与相关主体的数据共享协议，**说明该等安排是否违反有关互联网用户信息保护的有关**

[93] 根据《数据安全法》“数据处理，包括数据的收集、存储、使用、加工、传输、提供、公开等。”根据《个人信息保护法》“个人信息的处理包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等。”

[94] GDPR ‘processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

[95] 上海市方达律师事务所关于蚂蚁科技集团股份有限公司首次公开发行股票并在科创板上市的法律意见书

[96] 关于京东数字科技控股股份有限公司首次公开发行人民币普通股并在上海证券交易所科创板上市之补充法律意见书

关注焦点	问询对象/时间	问询内容
		法律法规及规范性文件。
	数聚智连[97] 2022 年 10 月	进一步说明发行人可获取、使用的数据具体类型、数量规模，与电商平台、品牌方之间关于**用户个人数据使用**的合作机制、权责划分机制。
共享风险	蚂蚁集团[98] 2020 年 8 月	发行人与阿里巴巴集团**数据共享的总体运作机制**，数据平台管理委员会的人员构成方式与职责定位，上述事项对发行人运营独立性、数据安全、市场竞争优劣势的影响，并按重要性原则完善相关风险揭示。
	京东数科[99] 2020 年 10 月	**数据共享的总体运作机制**、对发行人运营独立性、数据安全、市场竞争优劣势的影响，**是否存在京东集团单方终止数据共享的风险**，按重要性原则完善相关风险揭示。

表 17数据共享合规相关问询

[97] 关于北京数聚智连科技股份有限公司首次公开发行股票并在创业板上市申请文件的第二轮审核问询函的回复
[98] 上海市方达律师事务所关于蚂蚁科技集团股份有限公司首次公开发行股票并在科创板上市的法律意见书
[99] 关于京东数字科技控股股份有限公司首次公开发行股票并在科创板上市申请文件审核问询函的回复

问题 29： 共享数据前，需要做些什么？

在进行数据共享前，应当按照以下流程，明确数据共享场景：

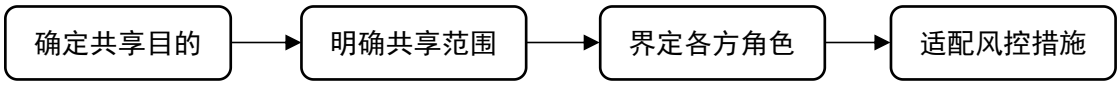


图 16共享数据合规流程图

(1) **第一步：确定共享目的**

在决定是否进行数据共享前，首先需要确定共享的目的，知道共享什么以及与谁共享，并形成书面记录；

(2) **第二步：明确共享范围**

应只共享实现目的所需的最少数据，以便遵循最小必要原则，并明确是否包括敏感个人信息、重要数据等特殊种类的数据，对于特殊种类数据，应当匹配相应的加密传输、去标识化等技术安全措施；

(3) **第三步：界定各方角色**

作为数据提供方，应当明确共享场景及各自角色（提供、共同处理或委托处理），并基于此明确双方各自权利、义务及责任承担问题；

角色	提供方义务
提供	(1) 应当向个人告知接收方的名称或者姓名、联系方式、处理目的、处理方式和个人信息的种类； (2) 取得个人的单独同意。
共同处理	(1) 需约定各自的权利和义务，但约定不影响个人向其中任何一个个人信息处理者要求行使权利； (2) 侵害个人信息权益造成损害的，双方应当依法承担连带责任。
受托处理	(1) 应当与受托人约定委托处理的目的、期限、处理方式、个人信息的种类、保护措施以及双方的权利和义务等； (2) 对受托人的个人信息处理活动进行监督。

表 18不同共享场景下提供方义务

(4) **第四步：适配风控措施**

基于数据共享场景，明确数据共享可能会给数据主体带来的风险（如是否侵犯个人信息及隐私权）、是否符合与第三方的约定以及是否会对于公司的独立性以及数据安全带来风险，并制定适配相应的风控措施。

问题 30：　作为共享数据接收方，需要关注什么？

作为数据接收方，应当基于确定的共享场景（提供、共同处理或委托处理），履行相应责任义务。

共享场景	接收方义务
提供	(1) 应当在处理目的、处理方式和个人信息的种类等范围内，处理个人信息； (2) 变更原先的处理目的、处理方式的，应当重新取得个人同意。
共同处理	(1) 需约定各自的权利和义务，但约定不影响个人向其中任何一个个人信息处理者要求行使权利； (2) 侵害个人信息权益造成损害的，双方应当依法承担连带责任。
受托处理	(1) 应当按照约定处理个人信息，不得超出约定的处理目的、处理方式等处理个人信息； (2) 委托合同不生效、无效、被撤销或者终止的，受托人应当将个人信息返还个人信息处理者或者予以删除，不得保留； (3) 未经个人信息处理者同意，受托人不得转委托他人处理个人信息； (4) 应当依照《个信法》和有关法律、行政法规的规定，采取必要措施保障所处理的个人信息的安全，并协助个人信息处理者履行《个信法》规定的义务。

表 19不同共享场景下接收方义务

问题 31： 数据共享场景下，各方的权责如何划分？

在不同数据共享场景下，各方的权责划分及责任承担如下表所示：

<table>
<tr><th>主体类型
共享场景</th><th>共享方</th><th>接收方</th></tr>
<tr><td rowspan="2">提供</td><td colspan="2"><u>权责划分</u>：作为相互独立的个人信息处理者，需保障用户对接收方及处理行为的知情权及同意权（如适用），履行个人信息保护义务，并对各自处理用户个人信息的行为负责。</td></tr>
<tr><td><u>责任承担</u>：
行政处罚：单独承担
民事责任：单独承担</td><td><u>责任承担</u>：
行政处罚：单独承担
民事责任：单独承担</td></tr>
<tr><td rowspan="2">共同处理</td><td colspan="2"><u>权责划分</u>：作为相互独立的个人信息处理者，履行个人信息保护义务，并对各自处理用户个人信息的行为负责（含在侵害个人信息权益造成损害的情形下，依法承担的连带责任）。</td></tr>
<tr><td><u>责任承担</u>：
行政处罚：单独承担
民事责任：连带责任</td><td><u>责任承担</u>：
行政处罚：单独承担
民事责任：连带责任</td></tr>
<tr><td rowspan="2">委托处理</td><td><u>权责划分</u>：作为个人信息处理者，履行个人信息保护义务，并对接收方受托处理用户个人信息的行为对外负责。</td><td><u>权责划分</u>：按照双方约定处理个人信息，并就受托处理行为向共享方负责。</td></tr>
<tr><td><u>责任承担</u>：
行政处罚：单独承担
民事责任：单独承担</td><td><u>责任承担</u>：
行政处罚：未明确规定
民事责任：原则上不承担，但若知道/明知处理行为违法的，承担连带责任。
<u>特别地，若超出受托处理范围与边界，构成新的个人信息处理者的，则独立承担相应责任</u>。</td></tr>
</table>

表 20数据共享场景下权责划分及责任承担

问题 32：　集团数据融合/场景下，如何证明数据资产的独立性？

对于多业务条线的集团公司而言，集团内部的数据融合（即一个集团内不同业务子公司之间的业务、产品数据进行融合）不可避免。对于单独上市的业务子公司而言，如何实现数据资产的独立性，是问询时会被重点关注的问题。对此，我们建议：

(1) **独立部署**：集团母公司与各业务条线子公司之间应独立部署数据平台，对于各自采集的数据进行独立存储，不得共用、混用数据池；

(2) **明确权责**：集团母公司与各业务条线子公司之间应确认关联公司各自的角色定位，并通过《数据共享协议》明确各自的权利、义务，并根据《个信法》及协议约定，履行自身职责。

同时，在数据融合场景下，应注意以下合规要点：

(1) **在不同共享场景下，依法保障用户的个人信息权益**

例如在提供场景下，业务子公司需要保障用户的知情权并获得其单独同意；在委托/受托处理场景下，业务子公司需要在隐私政策中明确委托处理的情形；在共同处理场景下，集团母公司与业务子公司均需要向用户明确主体身份及范围（即“我们”是谁）、处理目的及处理方式等信息。

(2) **创新数据处理场景，通过数据中台能力产品化，实现真正技术赋能**

其实，无论是在提供、委托/受托处理还是共同处理的场景下，集团母公司及业务子公司都因为或多或少直接碰了用户数据，因而需要承担大小不一的义务和责任。但在很多应用场景下，集团母公司只是为业务子公司提供了数据高效、融合、统一处理的技术能力，并非一定要处理用户的个人信息。

在这种情形下，集团母公司可考虑创新数据处理场景，将数据中台能力产品化，通过提供 SaaS 服务等方式，将个人信息的处理决定权交回给业务子公司，自身不再参与个人信息的处理目的及处理方式。这样能够在减轻自身的个人信息合规义务的同时，清晰个人信息的处理主体与边界。（详见本团队文章《集团内各业务数据融合场景下，如何应对 5%的顶格罚》）

问题 33： APP 运营者如何安全使用 SDK？

第三方软件开发工具包（SDK）被广泛应用于各类 App 开发中，由第三方 SDK 带来的安全问题已经引起多方关注，**从工信部 2021 年 11 月 3 日与 2022 年 2 月 18 日的通报案件对比可以看出，其已经将 SDK 作为和 App 同等重要的针对侵害用户个人信息权益行为的常规检测项**。

关于APP超范围索取权限、过度收集用户个人信息等问题“回头看”的通报（2021年第11批，总第20批）

发布时间：2021-11-03 17:39　来源：信息通信管理局

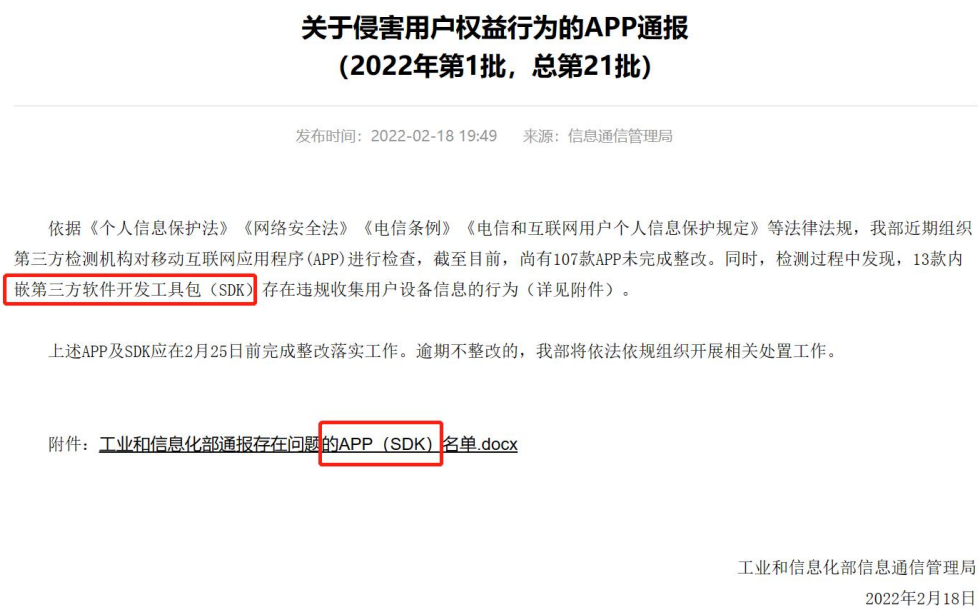
今年以来，我部持续加大对APP侵害用户权益的整治力度，先后三次组织对重点问题开展“回头看”。前期，重拳整治了APP违规调用通信录、位置信息以及弹窗信息骚扰用户等问题。近期，针对用户反映强烈的APP超范围、高频次索取权限，非服务场景所必需收集用户个人信息，欺骗误导用户下载等违规行为进行了检查，共发现38款APP（详见附件1）存在问题。各通信管理局按照我部统筹部署，积极开展APP技术检测，截至目前尚有17款APP未按时限要求完成整改（详见附件2-4），上述55款APP应在11月9日前完成整改，逾期不整改或整改不到位的，我部将依法依规进行处置并予以行政处罚。

附件1：工业和信息化部通报存在问题的应用软件名单.docx
附件2：山西省通信管理局通报存在问题的应用软件名单.doc
附件3：辽宁省通信管理局通报存在问题的应用软件名单.doc
附件4：重庆市通信管理局通报存在问题的应用软件名单.doc

工业和信息化部信息通信管理局

2021年11月3日

图 172021 年 11 月 3 日工信部通报存在问题的应用软件名单



关于侵害用户权益行为的APP通报
（2022年第1批，总第21批）

发布时间：2022-02-18 19:49　　来源：信息通信管理局

依据《个人信息保护法》《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，我部近期组织第三方检测机构对移动互联网应用程序(APP)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（详见附件）。

上述APP及SDK应在2月25日前完成整改落实工作。逾期不整改的，我部将依法依规组织开展相关处置工作。

附件：工业和信息化部通报存在问题的APP（SDK）名单.docx

工业和信息化部信息通信管理局
2022年2月18日

图 182022 年 2 月 18 日工信部通报存在问题的 APP（SDK）名单

若 App 运营者（即 SDK 使用者）使用不合规的 SDK，也容易殃及自身，SDK 使用者与 SDK 提供者的个人信息保护责任划分包括以下三种情况[100]：

(1) SDK 提供者独立处理个人信息的，应自行承担个人信息保护责任；

(2) SDK 提供者受 SDK 使用者委托或与 SDK 使用者共同处理个人信息的，可按照合作协议或共同协商各自承担的责任；

(3) 当 SDK 使用者独立处理个人信息的，应由 SDK 使用者承担个人信息保护的责任。

为减少因第三方 SDK 造成的 App 安全与个人信息安全问题，我们建议 App 运营者[101]：

(1) 应遵循合法、正当、必要的原则选择使用第三方 SDK；

(2) 涉及个人信息处理时，需履行个人信息处理者义务[102]：

(a) 若 SDK 使用者与 SDK 提供者共同处理个人信息，应双方协商确定如何

[100] 参考电信终端产业协会发布的《软件开发包（SDK）个人信息处理规范》团体标准
[101] 参考全国信息安全标准化技术委员会秘书处发布的《网络安全标准实践指南—移动互联网应用程序（App）中的第三方软件开发工具包（SDK）安全指引（征求意见稿）》
[102] 参考电信终端产业协会发布的《软件开发包（SDK）个人信息处理规范》团体标准

告知用户，征得用户的同意以及提供用户权利保障功能；

(b) 若 SDK 提供者，作为受托方，根据 SDK 使用者的要求处理个人信息，应由 SDK 使用者告知用户征得用户同意，并提供用户权利保障功能，SDK 提供者应协助 SDK 使用者完成上述义务；

(c) 若 SDK 提供者独立处理个人信息的，应自行告知用户，征得用户同意，并提供用户权利保障功能，SDK 使用者协助 SDK 提供者实现相应功能。

(3) 建立第三方 SDK 接入管理机制和工作流程，必要时应建立安全评估等机制设置接入条件，如

(a) 来源安全性评估：包括但不限于：SDK 提供者的基本信息、SDK 提供者的沟通反馈渠道、SDK 提供者的安全能力、SDK 的基本功能、SDK 的版本号、SDK 的安全性评估报告等；

(b) 代码安全性评估：包括但不限于：是否存在已知的恶意代码、是否存在已知的安全漏洞、是否申请敏感权限、是否嵌入了其他第三方 SDK 等；

(c) 行为安全性评估：包括但不限于调用的敏感权限、目的和频率；收集的个人信息类型、目的和频率；个人信息回传服务器域名、IP 地址、所在地域；是否存在热更新行为及热更新是否可主动关闭；传输数据是否加密；是否存在单独收集用户个人信息的界面；是否存在后台自启动和关联启动后收集个人信息的行为等；

(4) 与第三方 SDK 提供者通过合同等形式明确双方的安全责任及应实施的个人信息安全措施，妥善留存与第三方 SDK 提供者有关合同和管理记录；

(5) 应监督第三方产品或服务提供者加强个人信息安全管理，发现第三方产品或服务没有落实安全管理要求和责任的，应及时督促整改，必要时停止接入。

(四)数据存储合规 3 问

通过分析各拟上市企业披露的问询信息情况可知，在数据存储环节，上市审核机构的核心关注点在于：

(1) 数据存储的方式、期限是否符合法律规定及合同约定；

(2) 数据存储是否存在潜在数据泄露风险。

关注焦点	问询对象/时间	问询内容
数据存储	金智教育[103] 2021 年 1 月	**发行人对相关信息的储存及使用情况**，是否存在转授权或流转给第三方的情况，**是否存在相关信息泄露的情况**，是否存在侵犯用户隐私及数据的情况，是否存在法律风险、纠纷或潜在纠纷。
	零点有数[104] 2021 年 3 月	针对客户委托项目中各类采购的原始数据及后续处理完毕数据的**保存期限，是否符合行业惯例及合同约定。**
	合合信息[105] 2022 年 3 月	发行人各项业务及研发分别获取、**存储**、使用**哪些数据**，对应的数据来源、数据权属，是否存在销售数据的情形。
	衡泰技术[106] 2023 年 9 月	对个人信息的储存及使用情况是否存在信息泄露、侵犯用户隐私及数据的情况。

表 21数据存储合规相关问询

[103] 关于江苏金智教育信息股份有限公司首次公开发行股票并在科创板上市申请文件的第二轮审核问询函的回复

[104] 关于北京零点有数数据科技股份有限公司申请首次公开发行股票并在创业板上市的审核中心意见落实函的回复

[105] 关于上海合合信息科技股份有限公司首次公开发行股票并在科创板上市申请文件的首轮审核问询函的回复

[106] 《关于杭州衡泰技术股份有限公司首次公开发行股票并在创业板上市申请文件的审核问询函》之回复报告

问题 34：　数据存储，需要关注哪些合规要点？

存储也属于处理的行为之一，应当以取得用户同意为前提，并明确告知其存储期限及存储地点（如于**隐私政策中明确数据存储相关规则**），具体而言：

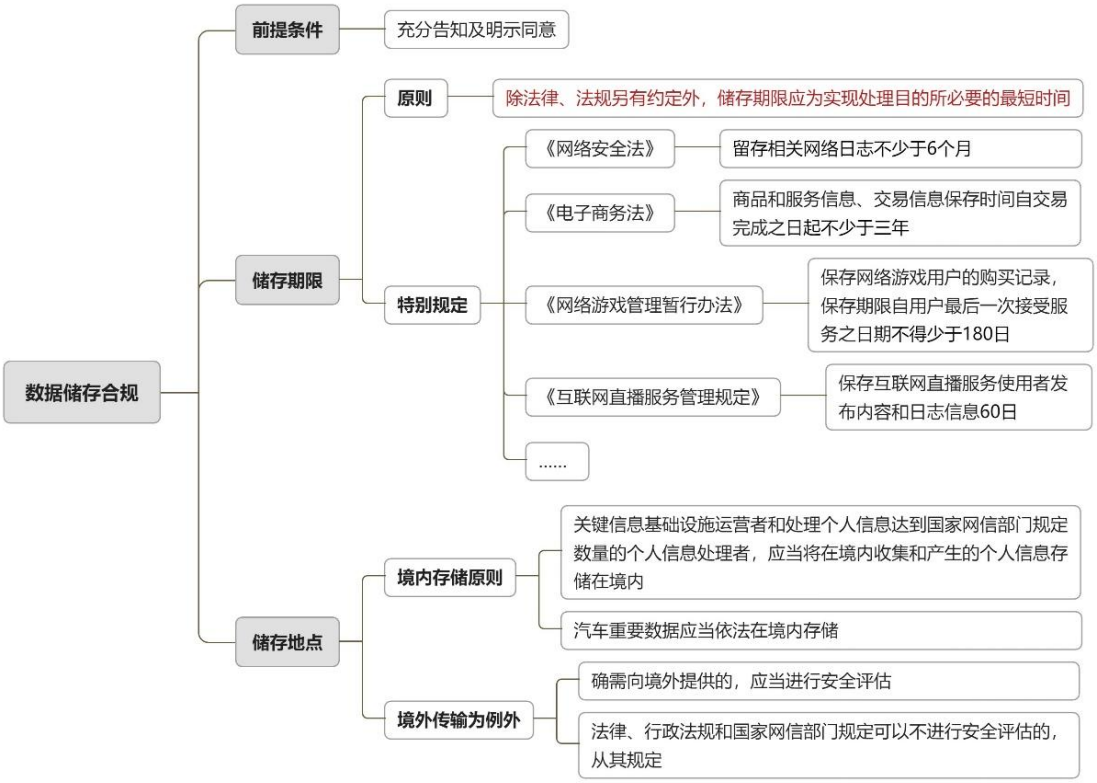


图 19数据存储合规要点

基于最小储存期限的要求，我们整理部分行业法律法规要求的储存期限如下表所示：

序号	法律法规	基本信息	主要内容
1	个人信息保护法	全国人大常委会 2021.08.20 发布 2021.11.01 实施	第十九条 除法律、行政法规另有规定外，**个人信息的保存期限应当为实现处理目的所必要的最短时间**。
2	中华人民共和国电子商务法	全国人大常委会 2018.08.31 发布 2019.01.01 实施	第三十一条 电子商务平台经营者应当**记录、保存平台上发布的商品和服务信息、交易信息**，并确保信息的完整性、保密性、可用性。**商品和服务信息、交易信息保存时间自交易完成之日起不少于三年**；法律、行政法规另有规定的，依照其

序号	法律法规	基本信息	主要内容
			规定。 第五十三条第三款 电子支付服务提供者应当**向用户免费提供对账服务以及最近三年的交易记录**。
3	网络交易监督管理办法	市监总局 2021.03.15 发布 2021.05.01 实施	第三十一条 网络交易平台经营者对**平台内经营者身份信息**的保存时间**自其退出平台之日起不少于三年**；对商品或者服务信息，支付记录、物流快递、退换货以及售后等**交易信息的保存时间自交易完成之日起不少于三年**。法律、行政法规另有规定的，依照其规定。
4	中华人民共和国证券法	全国人大常委会 2019.12.28 发布 2020.03.01 实施	第一百三十七条 证券公司应当建立**客户信息查询制度，确保客户能够查询其账户信息、委托记录、交易记录以及其他与接受服务或者购买产品有关的重要信息**。 证券公司应当妥善保存客户开户资料、委托记录、交易记录和与内部管理、业务经营有关的各项信息，任何人不得隐匿、伪造、篡改或者毁损。**上述信息的保存期限不得少于二十年。**
5	中华人民共和国电子签名法	全国人大常委会 2019.04.23 发布 2019.04.23 实施	第二十四条 电子认证服务提供者应当妥善保存与认证相关的信息，**信息保存期限至少为电子签名认证证书失效后五年**。
6	征信业管理条例	国务院 2013.01.21 发布 2013.03.15 实施	第十六条 **征信机构对个人不良信息的保存期限，自不良行为或者事件终止之日起为 5 年；超过 5 年的，应当予以删除。** 在不良信息保存期限内，信息主体可以对不良信息作出说明，征信机构应当予以记载。
7	中华人民共和国反洗钱法	全国人大常委会 2006.10.31 发布 2007.01.01 实施	第十九条 金融机构应当按照规定建立客户身份资料和交易记录保存制度。 在业务关系存续期间，客户身份资料发生变更的，应当及时更新客户身份资料。 **客户身份资料在业务关系结束后、客户交易信息在交易结束后，应当至少保存五年。** 金融机构破产和解散时，应当将客户身份资料和

序号	法律法规	基本信息	主要内容
			客户交易信息移交国务院有关部门指定的机构。
8	互联网信息服务管理办法	国务院 2011.01.08 发布 2011.01.08 实施	第十四条第二款 **互联网信息服务提供者和互联网接入服务提供者的记录备份应当保存 60 日**，并在国家有关机关依法查询时，予以提供。
9	网络餐饮服务食品安全监督管理办法	市监总局 2020.10.23 发布 2020.10.23 实施	第十五条 网络餐饮服务第三方平台提供者和自建网站餐饮服务提供者应当履行记录义务，如实记录网络订餐的订单信息，**包括食品的名称、下单时间、送餐人员、送达时间以及收货地址，信息保存时间不得少于 6 个月**。
10	人力资源市场暂行条例	国务院 2018.06.29 发布 2018.10.01 实施	第三十三条 人力资源服务机构应当加强内部制度建设，健全财务管理制度，建立服务台账，**如实记录服务对象、服务过程、服务结果等信息。服务台账应当保存 2 年以上。**

表 22部分行业法律法规要求的储存期限

问题 35：　个人生物识别信息应如何存储？

企业业务活动中往往涉及不同类型、不同级别的个人信息，应相应采取分类分级管理制度，配套不同数据存储策略。

而**个人生物识别信息属于敏感个人信息**（是指一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息），应配备更高安全性级别的储存策略：

(1) **采用加密等安全措施**：

存储个人生物识别信息等敏感个人信息时，应采用加密等安全措施（采用密码技术时宜遵循密码管理相关国家标准），保证数据库用户权限严格分离，并对涉及敏感个人信息数据库加强权限控制和安全审计；

(2) **单独存储**：

个人生物识别信息应与个人身份信息分开存储，原则上不应存储原始个人生物识别信息（如样本、图像等），可采取的措施包括但不限于：

(a) 仅存储个人生物识别信息的摘要信息（摘要信息通常具有不可逆特点，无法回溯到原始信息）；

(b) 在采集终端中直接使用个人生物识别信息实现身份识别、认证等功能；

(c) 在使用面部识别特征、指纹、掌纹、虹膜等实现识别身份、认证等功能后删除可提取个人生物识别信息的原始图像。

(3) **及时备份**：

在符合前述第(2)项的基础上，对个人生物识别信息等敏感个人信息采取相应备份机制，确保其可用性。

问题 36：　数据存储的尽头是删除？

除了删除，还可以采用匿名化处理的方式。

基于最小必要原则，企业存储的个人信息，在存储期限届满后，应主动依法对个人信息进行删除（若删除个人信息从技术上难以实现的，根据《个信法》的规定，个人信息处理者应当停止除存储和采取必要的安全保护措施之外的处理）或匿名化处理（匿名化处理后的信息无法识别到个人，不是个人信息，详见本文“问题 1：如何界定个人信息？”）。

然而，若企业采取匿名化处理方式，鉴于再识别技术[107]日益精进（具体参见本团队文章《“个人信息”的判定绝非易事——IP 属地遇到拦路虎“再识别技术”》），**匿名化已非绝对性概念**，企业应加强匿名化处理情形下的风险识别，制定内部匿名化处理“回头看”制度，**定期基于技术发展与识别技术的成本投入程度等因素进行“再识别评估”**，以防止已进行匿名化处理的个人信息被再识别，从而违反个人信息保护相关法律要求。

[107] 再识别技术指通过使用数据匹配或类似技术将匿名化数据转换回个人数据的过程

(五)境外上市/数据出境合规 7 问

针对拟上市企业赴境外上市，或者选择境内上市但涉及数据出境业务的，审核机构重点关注以下三点：

(1) 赴境外上市是否应申报网络安全审查；

(2) 境外发行证券和上市的数据出境合规；

(3) 拟境内上市企业是否涉及数据出境业务以及该业务的合规性。

关注焦点	问询对象/时间	问询内容
网络安全审查	蔚来[108] 2022 年 2 月	蔚来赴港上市文件披露，其于香港上市是否须接受网络安全审查仍然存在重大不确定性。
数据出境	熙华检测[109] 2023 年 10 月	发行人取得的数据内容、使用、存储、传输方式，数据跨境传输安全性及是否需要取得许可，发行人是否存在利用相关试验数据营利情况。
	海天瑞声[110] 2023 年 12 月	请发行人进一步说明：数据出境安全评估申报审批的具体流程及对发行人未来境外客户订单的影响，发行人认为《规范和促进数据跨境流动规定（征求意见稿）》未来如出台对发行人开展境外业务的影响将进一步减小的依据是否充分。
涉外业务	微众信科[111] 2020 年 12 月	发行人是否从事**境外数据的获取、处理、提供等涉外服务**，如涉及，请说明是否符合征信相关法律、数据安全相关法律规定的涉外信息、数据安全的要求和程序，该类业务的合法合规性。
	海天瑞声[112] 2020 年 8 月	发行人及其子公司为境外客户提供训练数据服务或产品，涉及境外销售， 该境外经营是否符合当地规定，是否符合我国出口管制规定。

[108] 蔚來集團以介紹方式在香港聯合交易所有限公司主板上市（上市文件）
[109] 北京市君合律师事务所关于上海熙华检测技术服务股份有限公司首次公开发行股票并在创业板上市的补充法律意见书（一）
[110] 关于北京海天瑞声科技股份有限公司 2023 年度向特定对象发行 A 股股票申请文件的第二轮审核问询函的回复
[111] 关于深圳微众信用科技股份有限公司首次公开发行股票并在科创板上市申请文件的审核问询函之回复报告
[112] 关于北京海天瑞声科技股份有限公司首次公开发行股票并在科创板上市申请文件审核问询函的回复

关注焦点	问询对象/时间	问询内容
	合合信息[113] 2022 年 9 月	核查发行人是否从事境外数据业务，是否存在向境外主体提供或销售数据产品及服务的情形，并就该类业务是否合法合规发表明确核查意见。
	睿联技术[114] 2023 年 9 月	说明在开展业务过程中是否可以获取用户相关个人信息和商业秘密等用户数据，业务开展是否符合各国数据保护和网络安全等法律法规的规定。
	沃太能源[115] 2023 年 12 月	相关数据存储、使用等安排是否符合所在业务地区/国家的数据安全、个人信息保护等法律法规的规定（涉及跨境储存）。

表 23境外上市/数据出境合规相关披露/问询

[113] 关于上海合合信息科技股份有限公司首次公开发行股票并在科创板上市申请文件的第二轮审核问询函的回复

[114] 关于深圳市睿联技术股份有限公司首次公开发行股票并在创业板上市申请文件的审核问询函的回复

[115] 关于沃太能源股份有限公司首次公开发行股票并在科创板上市申请文件的审核问询函之回复报告

问题 37：　什么情形下构成数据出境行为？

根据国家互联网信息办公室发布的《数据出境安全评估申报指南（第一版）》（2022.08.31 发布）（下称“《数据出境申报指南》”）的规定，下列情形属于数据出境行为：

(1) 数据处理者将在境内运营中收集和产生的数据传输、存储至境外；

(2) 数据处理者收集和产生的数据存储在境内，境外的机构、组织或者个人可以查询、调取、下载、导出；

(3) 国家网信办规定的其他数据出境行为。

特别地，该境外包含香港特别行政区、澳门特别行政区与台湾地区。

问题 38：境外（香港或国外）上市，应申报网络安全审查吗？

数据作为除土地、资本、技术等传统生产要素外的新兴重要生产要素，已成为各国国际竞争中，国家安全与发展的重要考量因素。

对此，我国专门出台《网络安全审查办法》[116]，其中，针对企业赴境外（香港或国外）上市可能涉及的网络安全审查作出了详细规定。

(1) 主动申报情形

根据《网络安全审查办法》的规定，**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（注意，这里用语非“**境外**”），必须向网络安全审查办公室**主动申报**网络安全审查。**这个体量对于拟上市企业而言，显然很容易达到**。

这里有个难点，在于“**掌握**”的涵义。我们认为，应从实质角度进行判断，即**是否实际控制个人信息或对个人信息存在重大影响**。

比如，受个人信息处理者委托处理个人信息，对个人信息处理的目的与方式不存在任何决定权的情形，即可能不构成该条所述的“掌握”。但若受托人超出授权委托的处理范围与权限，而能够决定处理的目的与方式的，则可能构成“掌握”。

(2) 被动审查情形

网络安全审查办公室对于其认为**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，有权**依职责进行审查**（注意，这里未区分境外还是国外上市）。

总结而言，对于掌握超过 100 万用户个人信息的网络平台运营者：

(1) **赴香港上市**：不适用该主动申报规则，存在适用被动审查的可能。

> 注意：根据《网络数据安全管理条例（征求意见稿）》的规定，处理一百万人以上个人信息的数据处理者赴**国外**上市的；数据处理者**赴香港上市，影响或者可能影响国家安全的**，应当按照国家有关规定，申报网络安全审查。该征求意见稿尚未正式发布，未对影响国家安全进行明确界定。

[116] 发布机构：国家互联网信息办公室、中华人民共和国国家发展和改革委员会、中华人民共和国工业和信息化部、中华人民共和国公安部、中华人民共和国国家安全部、中华人民共和国财政部、中华人民共和国商务部、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；2021.12.28 发布；2022.02.15 施行

虽暂无明确法律依据约束赴香港上市应主动申报网络完全审查，但正如赴港上市的蔚来集团所披露的信息，于香港上市是否须接受网络安全审查仍然存在重大不确定性，建议拟上市企业实时关注立法动态。

(2) **赴国外上市**：应适用主动申报规则，亦存在适用被动审查的可能。

问题 39： 境外上市过程中的数据出境，如何合规？

美国国会众议院于当地时间 2020 年 12 月 2 日通过《控股外国公司问责法案》（Holding Foreign Companies Accountable Act, HFCAA），要求在美上市外国公司需向美国公众公司会计监督委员会（以下简称“PCAOB”）提交可供检查的会计师事务所出具的审计报告；若连续三次出现无法检查年度，则其将被禁止在美国相关证券交易所进行证券交易。这意味着中美证券监管合作争议再度升级，随后不少知名中概股公司（如百度、爱奇艺、微博等）因此被美国证券交易委员会纳入预摘牌名单，在此大背景下，拟于境外上市企业需要更加重视境外发行证券和上市的数据出境合规问题。

根据证监会先后出台的《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）》[117]（下称“《境外上市规定（草案）》”）、《关于加强境内企业境外发行证券和上市相关保密和档案管理工作的规定（征求意见稿）》[118]（下称“《境外上市保密新规》”）的规定，拟境外上市企业在境外上市过程中，主要需要重点关注数据出境、保密及档案管理合规：

- **数据出境合规**

2021 年 12 月 24 日，证监会就《境外上市规定（草案）》公开征求意见，其中明确了拟境外上市企业在上市过程中的**数据出境合规**要求：

(1) **约束对象：境内企业**

(a) 境外直接发行上市的境内股份有限公司（如 H 股上市企业）；

(b) 境外间接发行上市主体的境内运营实体（如 WOFE、VIE 结构下的运营实体）。

(2) **数据出境合规：**

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，还应当符合国家法律法规和有关规定，否则国务院证券监督管理机构、国务院有关主管部门将依法追究法律责任。

[117] 发布机构：证监会；2021.12.24 发布；征求意见至 2022.01.23
[118] 发布机构：证监会；2022.04.02 发布；征求意见至 2022.04.17

➢ **保密及档案管理合规**

在《境外上市规定（草案）》相关规定的基础上，证监会于 2022 年 4 月 2 日，制定了《境外上市保密新规》，在进一步细化规定的同时，对境内企业境外发行证券和上市的保密和档案管理提出明确要求：

(1) **约束对象**：

(a) **境内企业**（范围与**《境外上市规定（草案）》**同）；

(b) **证券公司、证券服务机构**：境内外证券公司、证券服务机构以及其在境内的成员机构、代表机构、联营机构、合作机构等关联机构。

(2) **严格履行程序：**

(a) 提供、公开披露**涉及国家秘密、机关单位工作秘密的文件、资料的**，应当依法报有审批权限的主管部门批准，并报同级保密行政管理部门备案；

(b) 提供、公开披露其他泄露后会**对国家安全或者公共利益造成不利影响的文件、资料的**，应当按照国家有关规定，严格履行相应程序；

(c) 提供**对国家和社会具有重要保存价值的会计档案或会计档案复制件的**，应当按照国家有关规定履行相应程序。

(3) 底稿存放：

(a) **存放境内为原则**：工作底稿等档案**应当存放在境内**。未经有关主管部门批准，**不得通过携带、寄运等任何方式将其转移至境外或者通过信息技术等任何手段传递给境外机构或者个人**；

(b) **审批出境**：涉及对国家和社会具有重要保存价值的**档案或档案复制件需要出境的**，按照国家有关规定办理审批手续。

此外，境外上市应关注网络安全审查，具体详见本文“问题 38：境外（香港或国外）上市，应申报网络安全审查吗？”。

问题 40：　向境外提供数据前，需要做些什么？

为进一步规范数据出境活动，我国制定了数据出境安全评估制度，国家互联网信息办公室于 2022 年 7 月出台了《数据出境安全评估办法》，规定了触发数据出境安全评估的情形、安全评估的申报要点、审核资料、审核周期及安全评估结果有效期等内容，对此，我们整理要点如下，以供参考：

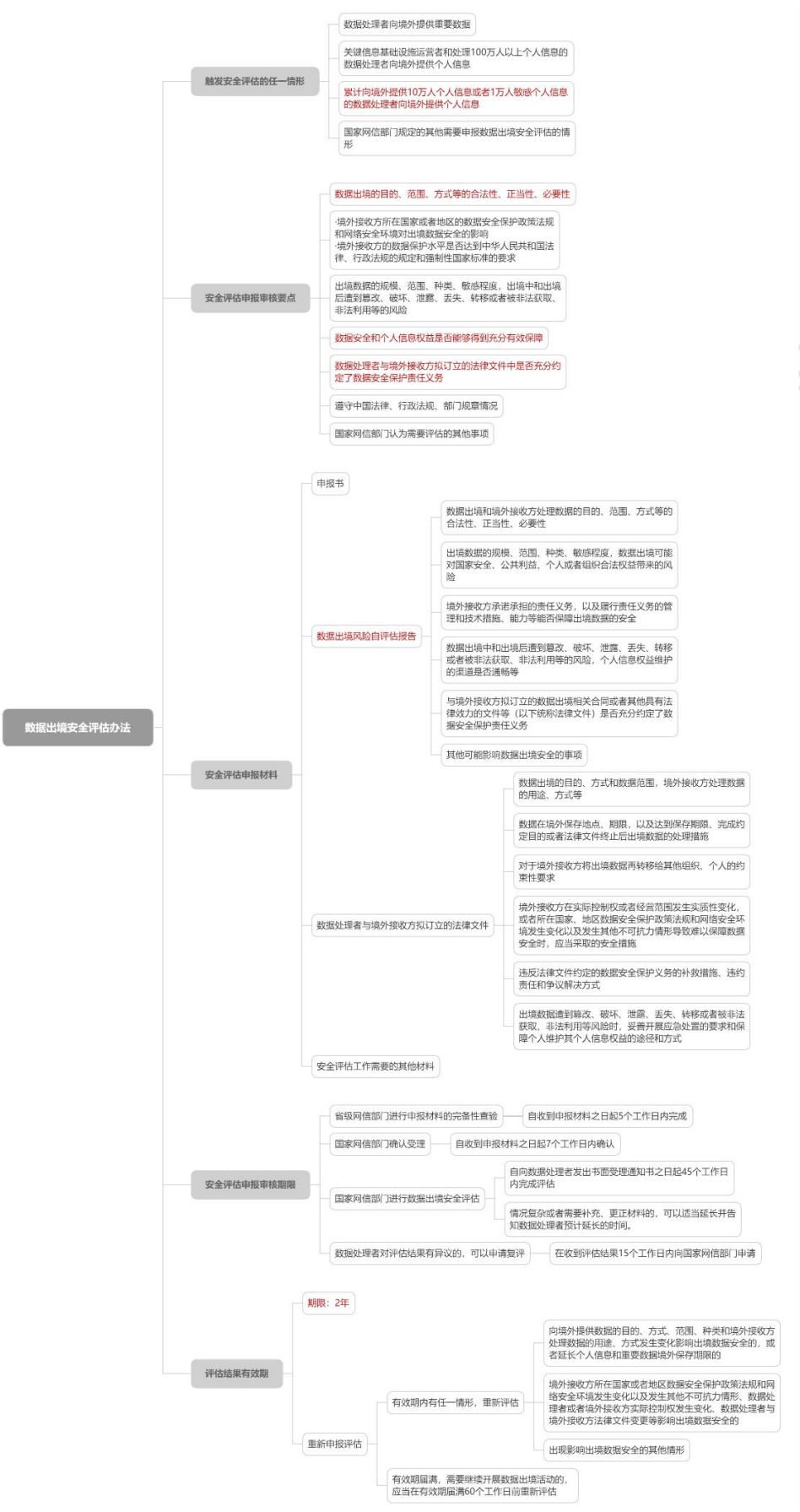


图 20《数据出境安全评估办法》解读要点

问题 41：　触发数据出境安全评估的情形有哪些？

根据《数据出境安全评估办法》、《数据出境申报指南》（2022.08.31 发布）的规定，数据出境安全评估的触发要件为（1）数据处理者向境外提供重要数据；（2）关键信息基础设施运营者和处理 100 万人以上个人信息的数据处理者向境外提供个人信息；（3）自上年 1 月 1 日起累计向境外提供 10 万人个人信息或者 1 万人敏感个人信息的数据处理者向境外提供个人信息；（4）其他情形。

具体分析如下图：

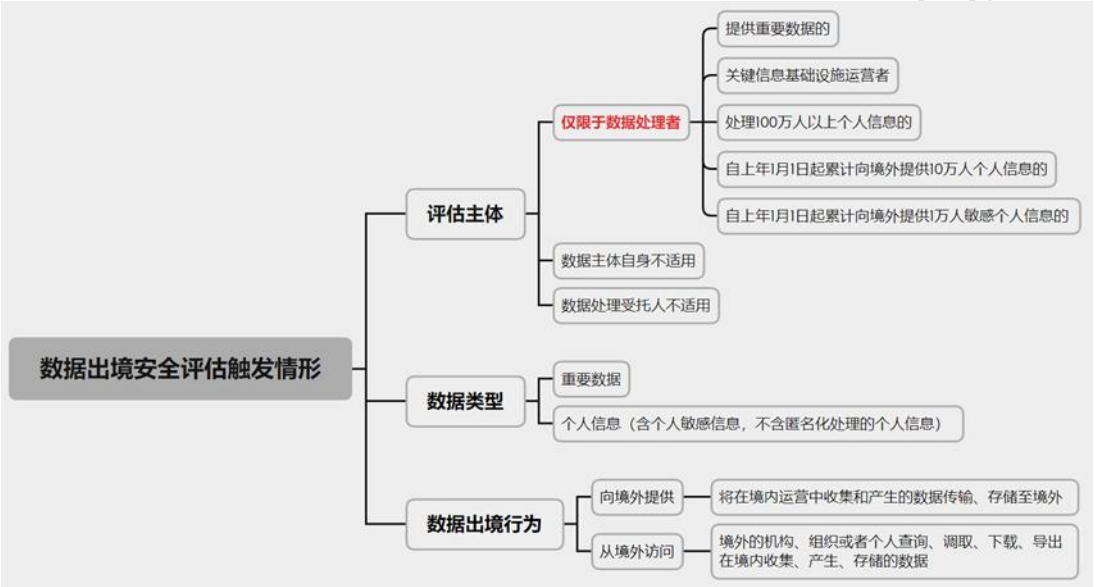


图 21触发数据出境安全评估的条件

问题 42：　如何进行数据出境安全评估？

根据《数据出境安全评估办法》、《数据出境申报指南》的规定，触发数据出境安全评估情形的，应当向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。而在申请评估前，还应当开展数据出境风险自评估，并形成风险自评估报告。

同时，根据《个信法》、《个人信息出境标准合同规定（征求意见稿）》[119]的规定，如果出境的数据范围包含个人信息的，还应当完成个人信息安全影响评估（参见本文"问题 9：如何正确认知个人信息安全影响评估？"）。

具体如下：

- **第一步：风险自评估**

(1) 评估主体：数据处理者

(2) 重点评估事项：

(a) 数据出境和境外接收方处理数据的目的、范围、方式等的合法性、正当性、必要性；

(b) 出境数据的规模、范围、种类、敏感程度，数据出境可能对国家安全、公共利益、个人或者组织合法权益带来的风险；

(c) 境外接收方承诺承担的责任义务，以及履行责任义务的管理和技术措施、能力等能否保障出境数据的安全；

(d) 数据出境中和出境后遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等的风险，个人信息权益维护的渠道是否通畅等；

(e) 与境外接收方拟订立的数据出境相关合同或者其他具有法律效力的文件等（以下统称法律文件）是否充分约定了数据安全保护责任义务；

(f) 其他可能影响数据出境安全的事项。

[119] 发布机构：网信办；2022.06.30 发布；征求意见至 2022.07.29

- **第二步：个人信息安全影响评估**

(1) 触发情形：向境外提供个人信息的

(2) 评估主体：数据处理者

(3) 评估事项：

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

(b) 出境个人信息的数量、范围、类型、敏感程度，个人信息出境可能对个人信息权益带来的风险；

(c) 境外接收方承诺承担的责任义务，以及履行责任义务的管理和技术措施、能力等能否保障出境个人信息的安全；

(d) 个人信息出境后泄露、损毁、篡改、滥用等的风险，个人维护个人信息权益的渠道是否通畅等；

(e) 境外接收方所在国家或者地区的个人信息保护政策法规对标准合同履行的影响；

(f) 其他可能影响个人信息出境安全的事项。

- **第三步：安全评估**

(1) 评估主体：国家网信部门组织国务院有关部门、省级网信部门、专门机构等

(2) 评估事项：

(a) 数据出境的目的、范围、方式等的合法性、正当性、必要性；

(b) 境外接收方所在国家或者地区的数据安全保护政策法规和网络安全环境对出境数据安全的影响；境外接收方的数据保护水平是否达到中华人民共和国法律、行政法规的规定和强制性国家标准的要求；

(c) 出境数据的规模、范围、种类、敏感程度，出境中和出境后遭到篡

改、破坏、泄露、丢失、转移或者被非法获取、非法利用等的风险；

(d) 数据安全和个人信息权益是否能够得到充分有效保障；

(e) 数据处理者与境外接收方拟订立的法律文件中是否充分约定了数据安全保护责任义务；

(f) 遵守中国法律、行政法规、部门规章情况；

(g) 国家网信部门认为需要评估的其他事项。

(3) 评估周期：发出书面受理通知书之日起 45 个工作日内完成；情况复杂或者需要补充、更正材料的，可以适当延长并告知预计延长的时间

(4) 评估有效期：2 年，自评估结果出具之日起计算

(5) 重新申报情形：

(a) 在有效期内出现以下情形之一的应当重新申报评估：

- 向境外提供数据的目的、方式、范围、种类和境外接收方处理数据的用途、方式发生变化影响出境数据安全的，或者延长个人信息和重要数据境外保存期限的；
- 境外接收方所在国家或者地区数据安全保护政策法规和网络安全环境发生变化以及发生其他不可抗力情形、数据处理者或者境外接收方实际控制权发生变化、数据处理者与境外接收方法律文件变更等影响出境数据安全的；
- 出现影响出境数据安全的其他情形。

(b) **有效期届满，需要继续开展数据出境活动的，应当在有效期届满 60 个工作日前重新申报评估。**

问题 43： 个人信息跨境处理的合规路径有哪些？

《个信法》为个人信息跨境提供了三条路径，安全评估路径（问题 42：如何进行数据出境安全评估？）、个人信息跨境处理活动安全认证路径以及个人信息出境标准合同路径。

具体如下图所示：

图 22个人信息跨境提供规则

(六)数据安全保障合规 7 问

通过分析各拟上市企业披露的问询信息情况可知，在数据安全保障方面，审核机构的核心关注点在于：

(1) 是否符合数据合规的法定义务；

(2) 是否发生过数据安全事件及对应有效解决措施；

(3) 是否已建立完善的数据安全保障内控制度；

(4) 是否存在涉及数据合规与数据安全的诉讼争议或受处罚的情形；

(5) 是否存在被数据合规相关监管部门要求整改的情形以及具体整改措施、是否会对上市造成实质性阻碍。

关注焦点	问询对象/时间	问询内容
数据合规法定义务	联众信息[120] 2022 年 7 月	充分论证“业务开展过程中不涉及对个人信息的收集、存储、传输、处理、使用”是否符合业务实质，逐条对照《个人信息保护法》《数据安全法》等相关法律法规，说明发行人相关业务开展的合规性。
	木仓科技[121] 2022 年 6 月	发行人的经营活动、个人信息的处理（含收集、存储、使用、加工、传输、提供、公开、删除等）、发行人履行的义务是否符合《个人信息保护法》的相关要求及合规性，进行必要的风险揭示。
	长光卫星[122] 2023 年 1 月	发行人核心业务与卫星遥感数据相关，请说明发行人遥感数据收集、使用、存储、运输、销售、管理等各个环节的合规性；发行人是否符合数据安全相关的法律法规，保障数据安全的相关措施
	黔通智联[123] 2023 年 6 月	结合《个人信息保护法》《数据安全法》等相关法律法规，说明在业务开展过程中相关个人或用户信息和数据安全方面的合规性。

[120] 关于上海联众网络信息股份有限公司 首次公开发行股票并在创业板上市申请文件第二轮审核问询函的回复
[121] 关于武汉木仓科技股份有限公司首次公开发行股票并在创业板上市申请文件的审核问询函的回复
[122] 关于长光卫星技术股份有限公司首次公开发行股票并在科创板上市审核问询函的回复
[123] 关于贵州黔通智联科技股份有限公司首次公开发行股票并在创业板上市申请文件第二轮审核问询函的回复

关注焦点	问询对象/时间	问询内容
	佰聆数据[124] 2023 年 9 月	发行人产品/服务研发、生产、销售及使用过程中涉及到的数据采集、处理、存储、分析挖掘、应用等情况及其合规性。
	熙华检测[125] 2023 年 10 月	结合《数据安全法》等数据信息相关法律法规，以及行业内关于临床试验数据管理的相关要求，说明发行人数据管理的合规性。
	太川股份[126] 2023 年 11 月	发行人的产品属于安防产品,平台采集和储存的数据（指的是楼宇对讲门禁模块的数据）为公安机关所关注,对照《网络安全法》《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》等相关法律法规，说明发行人采集、储存、使用个人信息的行为是否合法合规。
	格蓝若[127] 2023 年 12 月	请发行人说明：发行人业务开展过程中，是否涉及相关信息数据的采集、获取、使用、存储、管理等环节，是否符合数据安全、信息管理相关法律法规的规定。
合规措施及有效性	零点有数[128] 2021 年 3 月	发行人针对数据使用、隐私及**安全方面的内部控制措施及其有效性，是否存在泄密及其他数据使用风险。**
		发行人**是否存在数据或信息被窃取、篡改、假冒、恶意破坏或攻击等网络安全事件风险及法律风险。**
	旷视科技[129] 2021 年 6 月	发行人**保证数据采集、清洗、管理、运用等各方面的合规措施。**
	金智教育[130] 2023 年 9 月	说明关于信息安全与数据保护的相关内部控制制度及执行情况。

[124] 关于佰聆数据股份有限公司首次公开发行股票并在科创板上市申请文件审核问询函的回复
[125] 北京市君合律师事务所关于上海熙华检测技术服务股份有限公司首次公开发行股票并在创业板上市的补充法律意见书（一）
[126] 关于珠海太川云社区技术股份有限公司向不特定合格投资者公开发行股票并在北京证券交易所上市申请文件的审核问询函的回复
[127] 关于武汉格蓝若智能技术股份有限公司首次公开发行股票并在科创板上市申请文件的审核问询函的回复
[128] 关于北京零点有数数据科技股份有限公司申请首次公开发行股票并在创业板上市的审核中心意见落实函的回复
[129] 关于旷视科技有限公司首次公开发行存托凭证并在科创板上市申请文件的审核问询函之回复
[130] 关于江苏金智教育信息股份有限公司首次公开发行股票并在创业板上市申请文件的审核问询函的回复

关注焦点	问询对象/时间	问询内容
	麦驰物联[131] 2023 年 9 月	结合加密传输协议、云平台访问权限、与客户的终端数据安全条款等，说明对用户信息的保护措施及其有效性，是否符合《网络安全法》《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》等相关法律法规的规定。
	长光卫星[132] 2023 年 12 月	就发行人接触核心数据、核心技术秘密的关键岗位人员，如何防范泄密风险，发行人关于核心数据、核心技术秘密、核心知识产权保护的相关内控措施。
争议纠纷情况	青云科技[133] 2020 年 6 月	发行人**关于数据安全与网络安全保护的相关制度及措施**，与客户签订的服务协议中**关于安全责任约定与免责条款情况。**
		报告期内安全事故的发生类型、原因及发生概率统计，是否**存在涉及数据安全与网络安全的诉讼和仲裁纠纷或其他争议情况。**
	微众信科[134] 2020 年 12 月	发行人报告期内是否存在**因数据合规问题而受到处罚、监管等情形。**
	衡泰技术[135] 2023 年 9 月	对个人信息的储存及使用情况是否存在信息泄露、侵犯用户隐私及数据的情况，是否存在法律风险、纠纷或潜在纠纷，关于信息安全与数据保护的相关内部控制制度及执行情况
风险责任	兆尹科技[136] 2023 年 12 月	结合相关法规规定和软件产品的功能及所处业务环节，说明发行人面对银行等金融机构开展业务时，若软件产品发生故障导致市场风险时，发行人面临的合同责任，行政法律责任或刑事法律责任，并在招股说明书中补充披露上述法律风险。
通报、处罚、问询、整改	路桥信息[137] 2022 年 7 月	说明上述《网络与信息安全限期整改通知书》下发的原因、具体认定情况及整改情况，2021 年连续两次收到整改通知的合理性，该 APP 是否存在下架的风险。上述违法行为是否存在诉讼纠纷，以及对发行人业务的影响，上述违法行为

[131] 关于深圳市麦驰物联股份有限公司首次公开发行股票并在创业板上市申请文件的第二轮审核问询函的回复（2023 年半年报财务数据更新版）
[132] 关于长光卫星技术股份有限公司首次公开发行股票并在科创板上市申请文件的审核问询函的回复
[133] 关于北京青云科技股份有限公司首次公开发行股票并在科创板上市申请文件的审核问询函的回复
[134] 关于深圳微众信用科技股份有限公司首次公开发行股票并在科创板上市申请文件的审核问询函之回复
[135] 《关于杭州衡泰技术股份有限公司首次公开发行股票并在创业板上市申请文件的审核问询函》之回复报告
[136] 关于安徽兆尹信息科技股份有限公司首次公开发行股票并在创业板上市申请文件的审核问询函的回复报告
[137] 关于厦门路桥信息股份有限公司公开发行股票并在北交所上市申请文件的审核问询函的回复

关注焦点	问询对象/时间	问询内容
		是否构成本次发行的障碍。
	合合信息[138] 2022 年 9 月	近期发行人接受上海市市场监督管理局调查核实的具体情况、进展及影响，该事项是否构成本次发行上市的实质障碍。
	金智教育[139] 2023 年 9 月	说明收到相关部门核查整改通知的具体情况，包括违规时间、事实、造成影响、整改情况，是否构成重大违法违规行为；除上述事项外，报告期内发行人还有无其他违规收集个人信息被相关部门要求整改、核查或行政处罚的情形。
	金智教育[140] 2023 年 9 月	相关部门对发行人通报及责令整改的内容，发行人的整改情况，包括整改措施、效果、是否经有权机关验收通过等；在招股说明书中就“今日校园”APP 被通报及责令整改对发行人持续经营能力的相关风险进行提示。
	大汉软件[141] 2023 年 9 月	说明“爱山东”APP 涉及违规信息收集的具体情况，发行人在项目承建中承担的义务，是否存在因相关问题面临行政处罚的风险，是否属于重大违法违规行为。
	新视云[142] 2023 年 10 月	未经许可转载互联网新闻信息的整改措施及其有效性、整改验收情况，相关违规情形是否属于重大违法违规行为及判断依据。
	宇谷科技[143] 2023 年 11 月	发行人 APP 曾违规收集个人信息、超范围收集个人信息，被浙江省通信管理局通报、要求落实整改。请发行人说明前述事项的具体情况，发行人违规超范围收集个人信息是否构成重大违法行为，落实整改情况，是否整改完毕并获得主管部门认可及其依据。

[138] 关于上海合合信息科技股份有限公司首次公开发行股票并在科创板上市申请文件的第三轮审核问询函的回复
[139] 关于江苏金智教育信息股份有限公司首次公开发行股票并在创业板上市申请文件的审核问询函的回复
[140] 关于江苏金智教育信息股份有限公司首次公开发行股票并在创业板上市申请文件的第二轮审核问询函的回复
[141] 上海市锦天城律师事务所关于大汉软件股份有限公司首次公开发行股票并在深圳证券交易所创业板上市的补充法律意见书（六）
[142] 关于江苏新视云科技股份有限公司首次公开发行股票并在创业板上市补充法律意见书（二）
[143] 北京市通商律师事务所关于杭州宇谷科技股份有限公司 首次公开发行股票并在创业板上市之补充法律意见书（二）

关注焦点	问询对象/时间	问询内容
媒体质疑	大汉软件[144] 2023 年 9 月	说明是否存在其他涉及数据安全、违规信息收集等方面的媒体质疑，若是，请说明具体情况及对本次发行上市的影响。

表 24数据安全保障合规相关问询

问题 44： 数据合规的法定义务有哪些？

在联众网络、木仓科技的上市审核过程中，上市审核机构均要求发行人对于符合《个信法》《数安法》等法定义务进行合规性说明，因此，拟上市企业首先需要明确数据合规的法定义务有哪些，以便于对照实施、免于处罚并通过监督问询，对此，我们总结《个信法》、《数安法》、《网安法》的数据合规法定义务如下：

(1) 《个信法》项下法定义务

根据《个信法》，针对一般个人信息处理者与特殊个人信息处理者（即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，下称“特殊个人信息处理者”），法定义务不尽相同。

对于拟上市企业而言，往往会构成“特殊个人信息处理者”，所需履行的义务具体如下图所示（详见本团队文章《互联网平台“七步走”，从容应对<个信法>》）：

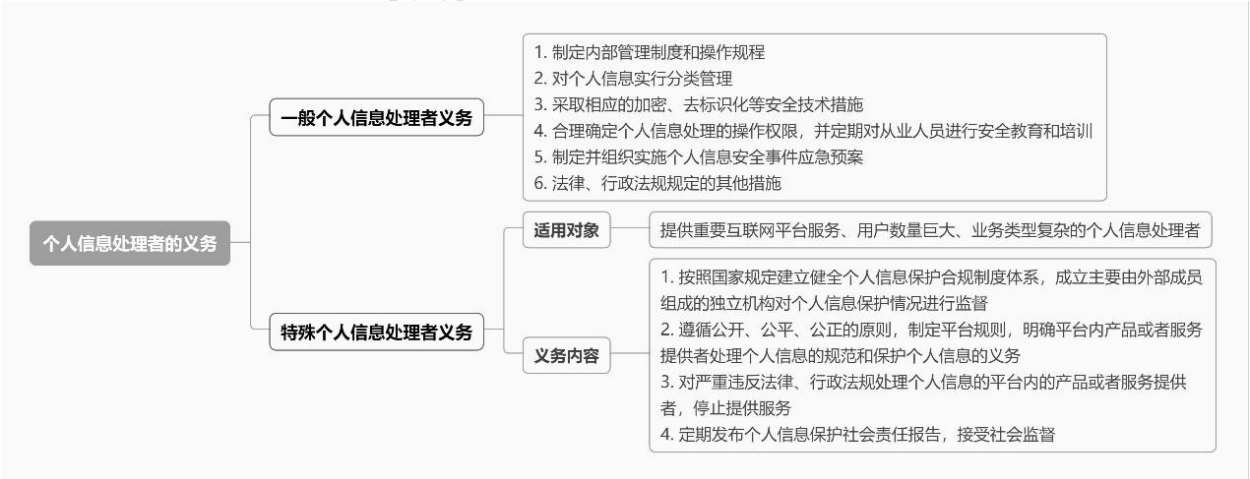


图 23个人信息处理者义务要点梳理

[144] 上海市锦天城律师事务所关于大汉软件股份有限公司首次公开发行股票并在深圳证券交易所创业板上市的补充法律意见书（六）

(2) 《数安法》项下法定义务

根据《数安法》，数据处理者应当合法合规获取数据，依法合规开展相应数据处理业务；同时应当建立数据安全制度，并加强风险监测、开展风险评估。其中，对于数据中介而言，还需额外就数据交易履行审核存证义务。

具体如下图所示：

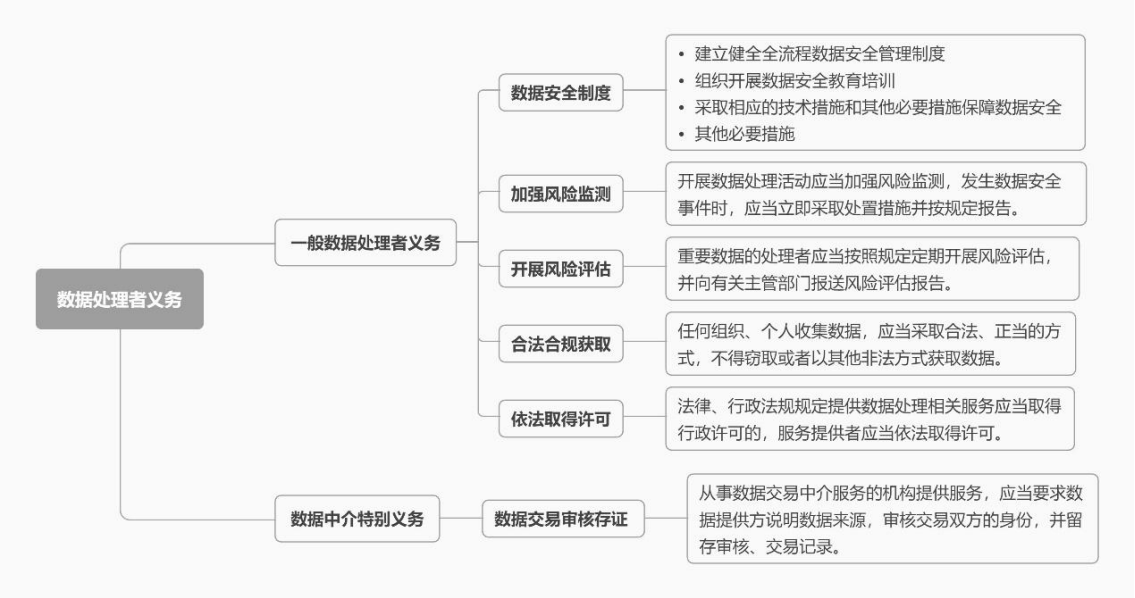


图 24数据处理者义务要点梳理

(3) 《网安法》项下法定义务

根据《网安法》，网络运营者（指网络的所有者、管理者和网络服务提供者），在网络安全方面主要需要履行网络安全保护义务、监测预警及应急处置义务。

具体如下图所示：

图 25《网安法》主要义务梳理

问题 45：　如何建立数据安全内部管理制度？

上医治未病。为有效保障数据安全，上市审核机构会十分关注企业的数据安全内部管理制度，以期防患于未然。如在零点有数上市过程中，被问询到“发行人针对数据使用、隐私及安全方面的内部控制措施及其有效性，是否存在泄密及其他数据使用风险。”；旷世科技被问询到“发行人保证数据采集、清洗、管理、运用等各方面的合规措施。”；青云科技被问询到“发行人关于数据安全与网络安全保护的相关制度及措施，与客户签订的服务协议中关于安全责任约定与免责条款情况。”

结合问询答复，拟上市企业可以参照以下维度，并参照《ISO/IEC 27001:2022 信息安全、网络安全和隐私保护—信息安全管理体系—要求》[145]，结合自身实际情况，建立数据安全内部管理制度：

➢ **数据安全内部管理制度体系建立**

(1) **组织架构**：设置设立数据安全委员会/数据安全管理小组，并由个人信息保护负责人/数据安全负责人担任最高领导，主要负责公司个人信息保护及数据安全相关制度的制定和执行（详见本团队文章《互联网平台如何打造数据安全合规体系之 ——数据安全应当责任到人》）；

(2) **制度文件**：制订并贯彻执行企业数据管理相关制度、管理规定等，如：

(a) **制度大纲层面：**

通过制定《数据安全合规管理制度体系》，明确数据安全合规管理目标、方针、组织架构及职责、管理重点、管理运行机制、管理安全保障等内容；

(b) **管理规定层面：**

如通过制定《数据管理规定》明确数据分级分类规则与数据采集、使用、共享、传输、存储、删除等全生命周期管理与保护规范；通过制定《个人信息安全管理规定》明确个人信息保护负责人任职及职责安排、个人

[145] 该 ISO27001 新版标准已于 2022 年 10 月 25 日正式发布，与旧版相比，新版所列的控制项从 114 项减少到 93 项，转版时间为 3 年，现有证书需要在 2025 年 11 月前转版到新版本

信息处理规范、个人信息保护规程等、个人信息安全事件的应急响应机制等；通过《信息安全管理规定》明确数据风控管理机制、投诉举报机制等内容；

(c) **具体操作层面：**

如通过制定《数据采购管理规范》明确对于数据采购行为的供应商准入、审批、数据源的合规管理；通过制定《网络安全事件应急预案》明确在发生数据泄露、篡改、丢失等安全事件时的应急响应制度；通过制定《隐私政策管理规范》明确隐私政策的制定、修订、上线流程及规范，保护用户个人信息权利。

(3) <u>人员管理</u>：

(a) **入职审查与责任约定：**

可在员工入职前进行背景审核，考察其的数据风险感知能力与职业道德，并通过《劳动合同》《保密协议》等内容明确员工在信息安全方面的责任义务；

(b) **教育与培训：**

积极进行员工数据安全相关的教育与培训，增强其信息安全意识、能力；

(c) **建立举报机制：**

可要求员工通过适当的渠道及时报告已发现或怀疑的信息安全事件，并采取匿名举报等措施保护员工任职安全，或给予适当的激励机制；

(d) **违规处理惩处：**

对违反企业相关信息安全管理制度的人员采取相应的惩处措施；

(e) **离职数据处理：**

在与员工劳动关系解除或终止时，应要求员工返还其掌握的数据并继续承担保密义务。

(4) <u>技术支持</u>：

(a) 加密存储：对敏感个人信息及重要数据采取相应备份机制及同时进行加密和脱敏处理，保证数据库用户权限严格分离，并采用一整套数据库密码轮换制度和加密存储机制；

(b) 权限管理：设置用户权限管理系统，按特权分散原则和最小授权原则对不同等级的使用者设置不同的信息查看、管理、修改配置等权限。

本团队提示，不同类型的企业在管理制度建设过程中应各有侧重，如采用爬虫技术获取数据的企业应额外建立《数据自动化采集制度》等规范文件，建议拟上市企业依据自身主营业务内容及数据处理独特因素，个性化定制合适的管理制度。

- **数据安全内部管理制度体系运行及完善**

通过“数据安全内部管理制度体系建立”的实施，企业内部已经建立起一套比较完善的制度体系，然而，仅仅依靠纸面上的制度规范是不够的，企业需要建立一个持续循环的长效管理机制，确保管理制度的落地、实施、运行、检查、保持以及改进，如此才能保障管理制度发挥最大的价值，具有生命力。

因此，建议企业依据“PDCA（PLAN、DO、CHECK、ACT）”管理思想，不断运行及完善上述管理制度。

问题 46：　什么情况下应当设置数据安全负责人、个人信息保护负责人？

根据我国现行法律法规及相关的国家标准，当拟上市企业处理数据满足一定情形时，应当分别设立数据安全负责人、个人信息保护负责人以及儿童个人信息保护负责人：

(1) **数据安全负责人**：

根据《数安法》，**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。

关于“重要数据”的认定，详见本文“问题 4：如何界定重要数据？”。

(2) **个人信息保护负责人**：

根据《个信法》，处理个人信息**达到国家网信部门规定数量**的个人信息处理者应当指定个人信息保护负责人，负责对个人信息处理活动以及采取的保护措施等进行监督。

对于上述“规定数量”，有待国家网信部门进一步出台细则予以明确。

目前可参考国家推荐性标准《个人信息安全规范》：**满足以下条件之一的组织**，应设立专职的个人信息保护负责人和个人信息保护工作机构，负责个人信息安全工作：

(a) 主要业务涉及个人信息处理，**且从业人员规模大于 200 人**；

(b) 处理超过 **100 万人**的个人信息，或预计在 12 个月内处理超过 **100 万人**的个人信息；

(c) 处理超过 **10 万人**的个人敏感信息的。

(3) **儿童个人信息保护负责人：**

若涉及到处理不满十四周岁的儿童个人信息，根据《儿童个人信息网络保护规定》，**应当指定专人负责儿童个人信息保护**。

（详见本团队文章《安全 1 号位：Are You Ready?——个人信息保护负责人的机遇与挑战》）

问题 47： APP/小程序被监管部门责令限期整改，是否会对上市造成影响？

路桥信息就曾受到上市审核机构的问询，要求其说明《网络与信息安全限期整改通知书》下发的原因、具体认定情况及整改情况，2021 年连续两次收到整改通知的合理性，该 APP 是否存在下架的风险……上述违法行为是否构成本次发行的障碍。

根据《首次公开发行股票并上市管理办法》的规定，发行人不得有下列情形：…（二）最近 36 个月内违反工商、税收、土地、环保、海关以及其他法律、行政法规，**受到行政处罚**，**且情节严重**。

即若拟上市公司在报告期内受到行政处罚且情节严重的，则将无缘上市。

因此，在判断 APP/小程序被监管部门责令限期整改是否会对上市造成影响时，需要先判断是否构成行政处罚。

根据《行政处罚法》的规定，行政处罚的种类包括（1）警告、通报批评；（2）罚款、没收违法所得、没收非法财物；（3）暂扣许可证件、降低资质等级、吊销许可证件；（4）限制开展生产经营活动、责令停产停业、责令关闭、限制从业；（5）行政拘留；（6）法律、行政法规规定的其他行政处罚。

其中并不包括“责令限期整改”，即“责令限期整改”不属于行政处罚。最高院在王元和诉山东省淄博市政府行政复议一案[146]中亦有论述，最高院从二者的**概念辨析、性质内容、规制角度、具体形式**四方面论证了责令（限期）改正不属于行政处罚[147]。因此，仅被责令限期整改并不会对上市造成直接的实质性阻碍。

但拟上市企业仍应以此警醒，按时保质地在期限之内完成整改，避免从“限期整

[146] (2018)最高法行申 4718 号

[147] 首先，责令改正（或者限期改正）与行政处罚概念有别。行政处罚是行政主体对违反行政管理秩序的行为依法定程序所给予的法律制裁；而责令改正或限期改正违法行为是指行政机关在实施行政处罚的过程中对违法行为人发出的一种作为命令。
其次，两者性质、内容不同。行政处罚是法律制裁，是对违法行为人的人身自由、财产权利的限制和剥夺，是对违法行为人精神和声誉造成损害的惩戒；而责令改正或者限期改正违法行为，其本身并不是制裁，只是要求违法行为人履行法定义务，停止违法行为，消除不良后果，恢复原状。
第三，两者的规制角度不同。行政处罚是从惩戒的角度，对行政相对人科处新的义务，以告诫违法行为人不得再违法，否则将受罚；而责令改正或者限期改正则是命令违法行为人履行既有的法定义务，纠正违法，恢复原状。
第四，两者形式不同。行政处罚法第八条规定了行政处罚的具体种类，具体有：警告，罚款，没收违法所得、非法财物，责令停产停业，暂扣或者吊销许可证、执照和行政拘留等；而责令改正或者限期改正违法行为，因各种具体违法行为不同而分别表现为停止违法行为、责令退还、责令赔偿、责令改正、限期拆除等形式。综上，责令改正或限期改正违法行为是与行政处罚相不同的一种行政行为。

改”演变为“下架处理”，若由此导致旗下运营的 APP 直接无法使用的，将会对业务持续运营造成不利影响，此时，将很大可能对上市造成阻碍。

更重要的是，应当在事前做好 APP 合规工作，定期或不定期（如 APP 业务功能等发生重大变更等情形）自行或委托第三方进行 APP 个人信息保护合规检测，及时发现违规情形并进行合规整改，降低后续由此被处以行政处罚的可能性。

问题 48：　发生个人信息泄露时，个人信息处理者应当怎么办？

根据安全公司 Proofpoint 对全球 1400 位 CISO（即 Chief Information Security Officer，首席信息安全官）对当前网络安全形势的看法的最新调查《2022 VOICE OF THECISO REPORT》[148]显示，约 48%的受访 CISO 表示，其所在公司有可能在未来 12 个月里遭受实质性网络攻击。

网络安全风险可谓是防不胜防，若一旦发生网络安全事件导致个人信息泄露，建议个人信息处理者立即采取法定的补救与通知义务，以尽可能的降低损害，维护个人信息主体权益；同时也要注意留存证据，以“自证清白”。

➢ 法定补救与通知义务

根据《个信法》，发生个人信息泄露事件后，个人信息处理者需要及时采取补救措施，并履行通知报告义务。

需要特别说明的是：若个人信息处理者能够有效避免信息泄露、篡改、丢失造成危害的，**可以不履行通知义务**。具体而言：

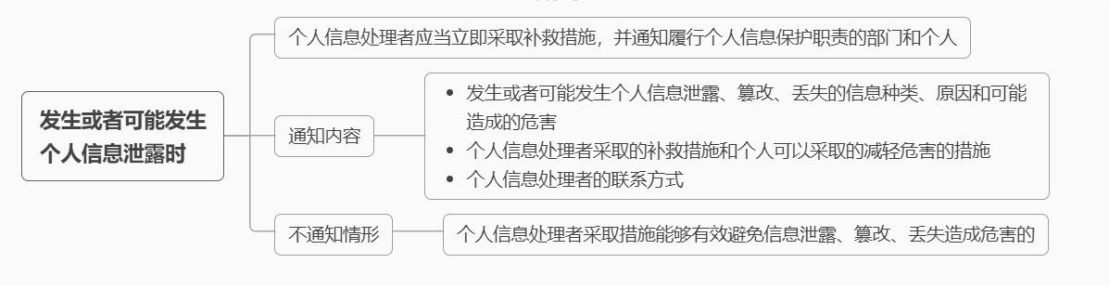


图 26个人信息泄露处置合规要点梳理

➢ 留存记录、准备“自证清白”

《个信法》第六十九条规定，“处理个人信息侵害个人信息权益造成损害，个人信息处理者不能证明自己没有过错的，应当承担损害赔偿等侵权责任。”

也就是说，个人信息权益遭受损害的情形下：

个人信息处理者承担侵权责任 ＝ 推定具有过错 ＋ 不能证明自身没有过错的。

[148] Proofpoint《2022 年 CISO 之声》白皮书：https://www.proofpoint.com/us/resources/white-papers/voice-of-the-ciso-report，2022 年 12 月 17 日第一次访问

该条款确定的过错推定原则，直接加重了个人信息处理者的举证责任，若无法证明自己无过错的，需承担相应侵权责任。

因此，在发生个人信息泄露事件时，应对该泄露事件发生的原因、造成的影响、对应采取的各类补救措施、履行的通知报告义务等事宜，留存完善记录，以在可能存在的诉讼争议环节进行“自证清白”。

（详见本文“问题 50：如何对外证明数据合规实力？”）

问题 49： 数据处理涉刑，是否还有机会？

在数据处理过程中，刑事责任风险不容忽视。一旦被提起刑事诉讼，上市之路也几乎断送[149]。

机遇是，“合规不起诉”制度，给了企业一线生机。如 2022 年 8 月，最高检发布了第三批涉案企业合规典型案例[150]。其中，上海市普陀区检察院办理的**首例数据合规不起诉案例**，让因数据处理涉刑的拟上市企业看到了起死回生的希望。该案中，涉案 Z 公司未经 E 公司授权许可，通过爬虫程序非法获取其运营的 E 公司外卖平台数据，Z 公司及其涉案员工因涉嫌非法获取计算机信息系统数据罪被移送检察院。经检察机关与 Z 公司协力履行合规不起诉流程，**最终作出不起诉决定**。

因此，合规不起诉制度可谓是数据处理涉刑中实控人和企业的“救命稻草”。

所谓“合规不起诉”，是指由检察机关主导，对于符合一定条件的单位犯罪案件，督促涉刑企业建立健全合规管理体系。如其能在一定期限后经监督考察合格，则对该涉刑企业不予起诉的制度。

该制度由最高人民检察院自 2020 年推行，现已在全国检察机关全面推开。全国工商联、最高检、财政部、国税总局等九部门已联合发布了《涉案企业合规建设、评估和审查办法》[151]（下称“《办法》”），以规范促进合规不起诉相关试点工作有序开展。

具体适用流程如下图所示：

[149] 根据《首次公开发行股票并上市管理办法》的规定，发行人不得有下列情形：…（二）最近 36 个月内违反工商、税收、土地、环保、海关以及其他法律、行政法规，受到行政处罚，且情节严重

[150]最高人民检察院官网，https://www.spp.gov.cn/xwfbh/wsfbt/202208/t20220810_570413.shtml#2，最后访问日期 2022 年 12 月 18 日

[151] 发布机构：中华全国工商业联合会、最高人民检察院、司法部、财政部、生态环境部、国务院国有资产监督管理委员会、国家税务总局、国家市场监督管理总局、中国国际贸易促进委员会；2022.04.19 发布；2022.04.19 实施

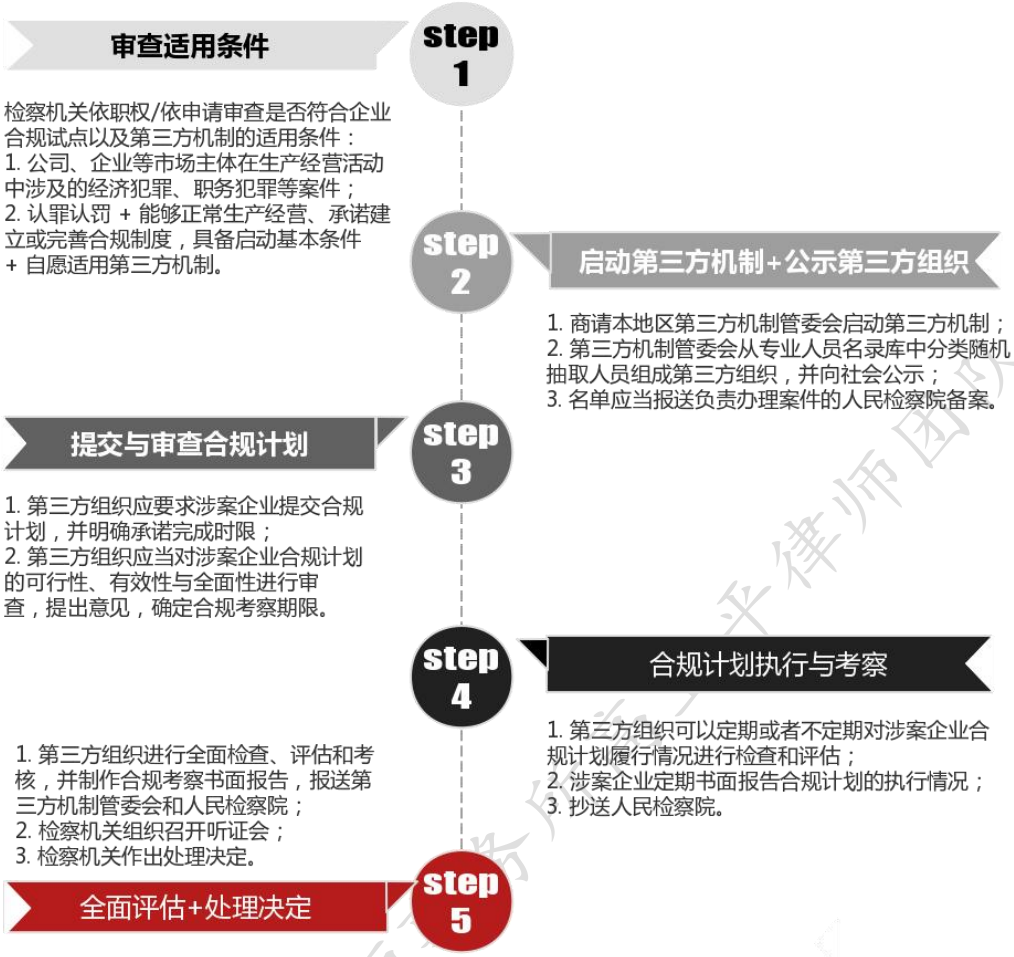


图 27涉案企业合规整改流程

在上述涉案企业合规整改流程中，合规计划执行与考察为核心环节，其中：

(1) 合规考察期如何确定？

根据《关于建立涉案企业合规第三方监督评估机制的指导意见（试行）》[152]（下称“《指导意见》”）的规定，合规考察期由第三方组织（即由第三方监督评估机制管理委员会选任组成的第三方监督评估组织，下称“第三方组织”）基于其对涉案企业合规计划的可行性、有效性与全面性进行的审查，根据案件具体情况和涉案企业承诺履行的期限予以确定。实践中，各地检察机关根据各自适用的政策文件，**合规考察期少则 1 个**

[152] 发布机构：最高人民检察院、司法部、财政部、生态环境部、国务院国有资产监督管理委员会、国家税务总局、国家市场监督管理总局、中华全国工商业联合会、中国国际贸易促进委员会；2021.06.03 发布；2021.06.03 施行

月~3 个月，多则 6 个月以上。

如根据《辽宁省人民检察院等十机关于建立涉罪企业合规考察制度的意见》的规定，合规考察期为 3 个月到 5 个月；根据《苏州检察机关优化营商环境八条措施》的规定，合规考察期为 1 个月到 3 个月；根据宁波市检察院《关于建立涉罪企业合规考制度的意见》的规定，合规考察期为 6 个月到 12 个月。

(2) 合规考察什么内容？

根据《指导意见》的规定，在合规考察期内，第三方组织可以**定期或者不定期对涉案企业合规计划履行情况进行检查和评估**，可以要求涉案企业**定期书面报告合规计划的执行情况**，同时抄送负责办理案件的人民检察院。结合第三方组织对涉案企业专项合规整改计划和相关合规管理体系有效性的评估内容，合规考察期内，涉案企业须能满足下述几个方面：

(a) 对涉案合规风险的有效识别、控制；

(b) 对违规违法行为的及时处置；

(c) 合规管理机构或者管理人员的合理配置；

(d) 合规管理制度机制建立以及人力物力的充分保障；

(e) 监测、举报、调查、处理机制及合规绩效评价机制的正常运行；

(f) 持续整改机制和合规文化已经基本形成。

可见，涉案企业在合规考察环节，“**时间紧、任务重**”。对于拟上市企业而言，面对涉案企业合规整改这一“救命稻草”，若仅依赖于事后的合规整改，在有限的合规考察期内建立合规机制，任务繁重，压力巨大。因此，不妨“未雨绸缪”，针对高危风险，事前利用 ISO37301 等为代表的标准认证工具，建立成体系、全流程、全覆盖的刑事合规体系，将合规融入组织的治理、管理、业务过程以及人员的行为和意识之中，建立并维护企业合规文化。一方面能够有效预防与降低自身刑事犯罪风险，另一方面，一旦“失足”，亦能证明主观合规意愿，并为事后合规整改打下基础，降低通过合规审查的难度。

问题 50：　如何对外证明数据合规实力？

拟上市企业在数据领域展现的合规状态，需通过设计“个人信息保护合规环”，由内而外地贯彻个人信息保护措施，实现“自证清白”（详见本团队文章 《个人数据“丢失”，平台如何“自证清白”》），同时充分彰显数据合规的意愿、能力和实力：

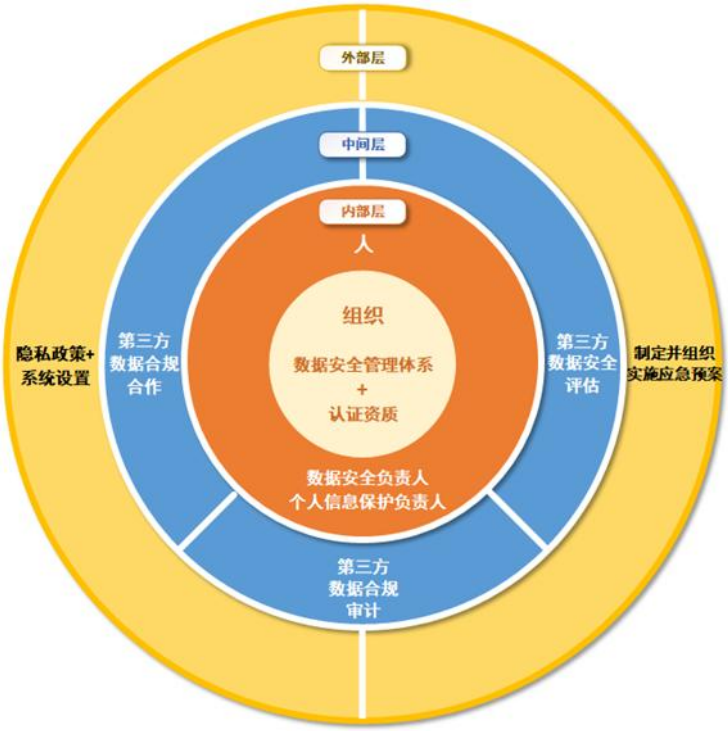


图 28个人信息保护合规环

(1) 内核层：建立内部数据合规/个人信息保护管理制度+设置数据安全及/或个人信息保护负责人+具备对应认证资质

拟上市企业可考虑根据自己的业务模式及技术特点，申请获得数据安全合规管理相应认证资质（如 ISO27001 信息安全管理体系认证、网络安全等级保护等资质，详见本团队文章《互联网平台如何打造数据安全合规体系之风险评估与数据安全管理制度》），以此来证明其已建立起一整套个人信息安全合规管理体系。

除数据合规相关资质外，拟上市企业也可以考虑获得 ISO37301 合规管理体系认证，通过建设整体的合规管理体系，对外彰显自身具备的完善管理能力。

(2) 中间层：与中立专业第三方机构建立集合规合作、安全评估及合规审计于一体的全方位合作

在既往的问询答复中，不少企业会通过委托律师事务所等第三方专业合规机构出具相应报告或证明（如《数据安全管理尽职调查报告》）或委托专业第三方机构进行数据合规审计等，作为自身数据合规的辅助证明材料。

因此，若拟上市企业能够提交证据证明其已与中立专业第三方机构开展个人信息安全合规合作，提供对应专项报告、安全评估记录、合规审计文件等证明材料，则能从侧面彰显其对于个人信息安全合规义务的重视程度。

(3) 外部层：制定完备的隐私政策+嵌入系统功能设置+制定并组织实施应急预案

基于内核层及中间层并未完全对外，对于用户而言，其无法直接知晓拟上市企业内部对于数据安全保护以及对用户个人信息权益保护的安排，因此法定应当制备的隐私政策就是天然的对外高效传达的通道。

当然，仅仅提供一份“完美的隐私政策文本”并不足够，更重要的是隐私政策的内容能够真正匹配对应到相应系统设置，从个人信息的收集、共享、传输、转让、存储、删除等环节，将个人信息保护规则一一落到实处，并为个人信息主体依法设置高友好度的权利（如删除权、查阅权、复制权、携带权、更正权、补充权等）实现路径，切忌将隐私政策落成一纸空文。

除此之外，制定并组织实施个人信息安全事件应急预案，亦能够彰显拟上市企业对于个人信息安全事件的高度重视。通过应急响应培训和应急演练，使得内部相关人员在应急情形发生时更好地处理个人信息安全问题，这也是拟上市企业对外展示的重要窗口之一。

[以下无正文]

作者介绍：

上海段和段律师事务所：

段和段律师事务所 1993 年在上海成立，是一家拥有 30 多家境内外分所/办公室的综合性和国际化律所。段和段秉承法律至上、依法治国和客户为先、回馈社会的基本准则，走出了中国律所国际化、专业化、规模化的成功发展之路。

主要编写成员：段和段高亚平律师团队

上海段和段律师事务所数据合规专业委员会主任高亚平律师牵头的 IPO 数据合规团队（高亚平律师团队），是**国内数据合规领域特色法律服务的创新开拓者与引领者，以 IPO 数据合规专项为团队典型特色法律服务，担任多家企业 IPO 数据合规法律顾问，尤其擅长特殊数据领域（如金融数据、汽车数据、人工智能等）疑难合规问题的处理与解决方案的创新设计。**

高亚平律师团队聚焦国内数据合规领域法律服务，擅长处理多主体、多场景、跨境、特殊行业领域的疑难合规问题，为垂直领域行业提供定制化数据合规法律服务，客户涵盖互联网、车联网、金融、征信、第三方支付、测绘、生物医药、大数据、人工智能、碳交易、教育、数字营销、电子商务等垂直行业细分领域，具有为客户提供一站式、整合性的闭环法律服务的能力与丰富的实践经验。

高亚平律师团队在数据出境领域具备独特资源优势与丰富业务经验。凭借段和段律所高度国际化、布局全球化、涉外服务专业化的鲜明特色，在协助中国企业“走出去”等跨境数据流通环节的合规建设等方面具有独特优势， 为多家企业提供数据出境安全评估、个人信息标准合同备案等法律服务，同时担任多家出海企业数据合规法律顾问。

高亚平律师团队 100%团队成员获得 EXIN（国际信息科学考试学会，DPO 权威认证机构）组织的 DPO（数据保护官）认证，其中高亚平、周梦、李燊是获得 DPO 授权讲师资质的律师，于法律出版社出版《成功 CEO 的临门一脚 数据合规管理》《灵活用工平台的合规之路》，发布《数据出境实操白皮书》《灵工行业风险自查白皮书》。

上海数据交易所：

上海数据交易所是由上海市人民政府指导下组建的准公共服务机构。**上海数据交易所紧扣建设国家数据交易所的定位，以构建数据要素市场、推进数据资产化进程为使命，承担数据要素流通制度和规范探索创新、数据要素流通基础设施服务、数据产品登记和数据产品交易等职能。**

主要编写成员：上海数据交易所合规风控团队

上海数据交易所合规风控团队深耕数据交易合规领域，**探索高效合规与审慎监管结合的新路径，**以期助力数据要素市场蓬勃健康发展。合规风控团队牵头制定《上海数据交易所数据交易安全合规指引》及配套清单，为数据交易主体提供合法、清晰、可落地的合规向导。

知识产权保护声明：

更多资讯 敬请联系