APP 运营合规重点问题分享

宁波市律师协会互联网与数字化专业委员会

二〇二五年十二月

序言

数字经济浪潮下，移动应用程序（APP）已深度融入社会生产生活，成为企业数字化转型的核心载体与服务用户的关键入口。然而，随着《网络安全法》《数据安全法》《个人信息保护法》等法律法规的密集出台与监管体系的日趋完善，APP 运营的合规门槛持续提升，从资质备案到数据治理、从内容管控到用户权益保护，全流程合规已成为企业可持续发展的基本前提。

实践中，不少企业因对合规要求理解不深、执行不到位，面临罚款、下架、停业整顿甚至刑事追责等风险，既损害用户信任，也制约自身发展。为帮助 APP 运营者精准把握合规要点、规避潜在风险，我们结合最新监管政策与行业实践，梳理了 ICP 备案与许可、公安联网备案、行业资质办理、数据安全与个人信息保护、算法合规、广告合规等 14 个核心合规领域，系统拆解合规要求、法律依据与实操要点。

本分享旨在为 APP 运营企业提供清晰的合规指引，助力企业建立健全合规管理体系，在依法合规的前提下实现创新发展，共同维护安全、健康、有序的网络空间生态。

宁波市律师协会互联网与数字化专业委员会

二〇二五年十二月

问题一：ICP 备案如何规范问题

1.根据《互联网信息服务管理办法》的规定，通过互联网向上网用户提供信息的服务活动被称为互联网信息服务，互联网信息服务分为经营性和非经营性两类，国家对经营性互联网信息服务实行许可制度（需办理增值电信业务经营许可，一般统称ICP许可证），对非经营互联网信息服务实行备案制度（需办理ICP备案）。

2.在很长一段时间里，ICP 备案的监管重点都停留在网站。2023年7月21日，工业和信息化部发布《关于开展移动互联网应用程序备案工作的通知》，正式要求所有APP（含小程序、快应用）均需办理 ICP 备案手续，否则不得从事互联网信息服务。 自此，APP 与网站一样，必须先办理ICP 备案方可上架运营。

3.企业需要结合自身实际情况判断自己运营的APP 是经营性业务还是非经营性业务，并进而确定是办理 ICP 备案还是ICP 许可。一般认为，企业利用自身APP 并以自营方式直接销售自身或其它企业的商品或服务，无其它单位或个人以自身名义入驻该APP实施销售行为的，无需办理ICP许可，办理ICP备案即可。

4.除了办理ICP备案或许可证之外，按照工信部的政策要求，企业还应当在APP显著位置标明其备案编号，并在备案编号下方按要求链接备案系统网址，供公众查询核对。

工业和信息化部 ICP/IP 地址/ 域名信息备案管理系统：https://beian.miit.gov.cn/

5. 根据《非经营性互联网信息服务备案管理办法》的规定，APP未履行ICP备案手续的，由住所地通信管理局责令限期改正，并处一万元罚款，拒不改正的，下架关停。未在备案编号下方链接工业和信息化部备案管理系统网址的， 由住所所在地省通信管理局责令限期改正；逾期不改正的，处五千元以上一万元以下罚款。

问题二：ICP 许可办理问题

1.根据《互联网信息服务管理办法》的规定，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，即ICP许可证。

2.根据《中华人民共和国电信条例》《电信业务经营许可管理办法》的规定，电信业务分为基础电信业务和增值电信业务，基础电信业务是指提供公共网络基础设施、公共数据传送和基本话音通信服务的业务，增值电信业务是指利用公共网络基础设施提供的电信与信息服务的业务。

3.根据《电信业务分类目录》，基础电信业务分为第一类基础电信业务和第二类基础电信业务，绝大部分APP运营者并不涉及，在此暂不展开。增值电信业务也分为两个大类，共十个子类，具体业态和持牌机构举例如下：

大类	子类	细分业态	持牌机构 / 业务举例
B1 第一类增值电信业务	B11- 互联网数据中心（IDC）业务	机房托管 互联网资源协作服务业务（云服务）	各电信运营商的数据中心业务、阿里云、腾讯云等
	B12- 内容分发网络（CDN）业务	—	网宿科技、阿里云、腾讯云、华为等
	B13- 国内互联网虚拟专用网业务（IP-VPN）	—	—
	B14- 互联网接入服务业务（ISP）	—	—
B2 第二类增值电信业务	B21- 在线数据处理与交易处理业务（EDI）	交易处理业务 电子数据交换业务 网络 / 电子设备数据处理业务	电商平台、网络借贷平台（P2P）
	B22- 国内多方通信服务业务	国内多方电话会议服务业务 国内可视电话会议服务业务 国内互联网会议电视及图像服务业务	—
	B23- 存储转发类业务	语音信箱业务 电子邮件业务 传真存储转发业务	—
	B24- 呼叫中心业务	呼叫中心系统业务 话务员座席出租业务 B24-1 国内呼叫业务 B24-2 离岸呼叫中心业务	—
	B25- 信息服务业务	信息发布平台和递送服务 信息搜索查询服务 信息社区平台服务 信息即时交互服务 信息保护和处理服务	门户网站（含新闻）、网络广告、网络游戏、音视频、直播、搜索引擎、论坛、即时通信、杀毒软件等
	B26- 编码和规程转换业务	B26-1 互联网域名解析服务业务	—

4. 企业需要结合自身APP的实际业务类型判断是否需要办理ICP许可证， 以及需要办理何种 ICP许可证。有些时候办理何种ICP许可证并不是很好判断，一方面可以参考同行业竞品的办证情况，另一方面可以直接向当地通信管理部门咨询。

5.根据通信管理部门意见，企业利用自身网站并以自营方式直接销售自身或其它企业的商品或服务，无其它单位或个人以自身名义入驻该网站实施销售行为的，或者利用自身网站自行发布与企业自身相关的信息，并非为其他单位或个人用户发布信息提供平台服务的，以及依托微信、支付宝等互联网平台的小程序、公众号等形式经营业务，且无其他独立运营平台的，不涉及增值电信业务，无需办理ICP许可证。

6. 根据《电信条例》的规定，未取得电信业务经营许可证，擅自经营电信业务，或者超范围经营电信业务的，由工信部或者省、自治区、直辖市电信管理机构依据职权责令改正，没收违法所得，处违法所得3倍以上5倍以下罚款；没有违法所得或者违法所得不足5万元的，处10万元以上100万元以下罚款；情节严重的，责令停业整顿。

问题三：公安联网备案问题

1.根据《计算机信息网络国际联网安全保护管理办法》的规定，互联单位、接入单位、使用计算机信息网络国际联网的法人和其他组织（包括跨省、自治区、直辖市联网的单位和所属的分支机构），应当自网络正式联通之日起30日内，到所在地的省、自治区、直辖市人民政府公安机关指定的受理机关办理备案手续。不履行备案手续的，由公安机关给予警告或者停机整顿不超过6个月的处罚。

2.与ICP备案类似，公安联网备案工作长期以来的监管重点也在网站。2023年下半年，公安部“全国互联网安全管理服务平台”正式上线了APP及小程序备案功能，部分公安机关也向属地企业发出了备案通知。

公安部“全国互联网安全管理服务平台”地址：https://beian.mps.gov.cn/

3. APP公安联网工作正在逐渐推进过程中，现阶段重点工作在于推进具有交互功能的APP联网备案。建议企业结合自身APP实际情况以及当地公安部门的政策及时办理APP 联网备案手续，以免影响APP的正常运营。

问题四：常见行业资质办理问题

1.除了电信业务资质以外，多个行业领域业务“上网”存在一定的准入门槛，主要表现为各类资质许可或备案要求，常见的行业许可或备案如下：

序号	资质名称	适用业态	设定依据	持牌举例
1	《互联网新闻信息服务许可证》	提供互联网新闻信息服务的网站、应用程序、论坛、博客、微博客、公众账号、即时通信工具、网络直播、自媒体等	《互联网新闻信息服务管理规定》	人民网、新华网、网易新闻、新浪博客、腾讯科技、一点资讯、芒果 TV
2	《网络出版服务许可证》	网络游戏（运营企业需要，可与其他持牌机构联合出版）、网络文学、互联网地图、音视频、互联网杂志、电子期刊等出版	《网络出版服务管理规定》	各大出版社、优酷、芒果 TV
3	《出版物经营许可证》	图书、报纸、期刊、音像制品、电子出版物的批发、零售	《出版物市场管理规定》	京东、当当、爱奇艺、知乎、得到
4	《网络文化经营许可证》	网络音乐、网络演出剧（节）目、网络表演、网络艺术品、网络动漫和展览、比赛活动等	《互联网文化管理暂行规定》	优酷、抖音、快手、知乎
5	《广播电视节目制作经营许可证》	专题、专栏、综艺、动画片、广播剧、电视剧等广播电视节目的制作和节目版权的交易、代理交易	《广播电视节目制作经营管理规定》	B 站、知乎、爱奇艺、芒果 TV
6	《信息网络传播视听节目许可证》	制作、编辑、集成并通过互联网向公众提供视音频节目，以及为他人提供上载传播视听节目服务	《互联网视听节目服务管理规定》	央视频、芒果 TV、优酷、爱奇艺、B 站、今日头条（收购）
7	《营业性演出许可证》	以营利为目的为公众举办的现场文艺表演活动	《营业性演出管理条例》	芒果 TV
8	《互联网药品信息服务许可证》	通过互联网向上网用户提供药品（含医疗器械）信息的服务活动	《互联网药品信息服务管理办法》	京东、淘宝、饿了么、大众点评

9	医疗器械网络销售备案/医疗器械网络交易服务第三方平台备案	医疗器械网络销售、医疗器械网络交易服务第三方平台	《医疗器械网络销售监督管理办法》	淘宝、丁香医生、饿了么
10	《食品经营许可证》/食品经营备案	食品销售	《食品经营许可和备案管理办法》	美团、饿了么
11	《支付业务许可证》	网络支付、预付卡的发行与受理、银行卡收单、人民银行确定的其他支付业务	《非金融机构支付服务管理办法》	支付宝、财付通、联通支付
12	《互联网宗教信息服务许可证》	互联网宗教信息发布、转载、其他与互联网宗教信息相关的服务	《互联网宗教信息服务管理办法》	少林寺、灵隐寺
13	网络借贷信息中介机构备案	网络借贷信息中介（P2P）	《网络借贷信息中介机构业务活动管理暂行办法》	各大 P2P 平台
14	《网络预约出租汽车经营许可证》《网络预约出租汽车运输证》	网约车平台	《网络预约出租汽车经营服务管理暂行办法》	滴滴、神州出行、曹操专车、T3 出行
15	《测绘资质证书》	互联网地图、地理位置定位、地理信息数据采集	《中华人民共和国测绘法》	高德地图、百度地图、京东、理想汽车
16	区块链信息服务备案	区块链项目	《区块链信息服务管理规定》	司法联盟链、百度区块链引擎、蚂蚁区块链 BaaS 平台、陆金所区块链
17	教育移动互联网应用备案	在线教育	《教育移动互联网应用程序备案管理办法》	学而思网校、VIPKID、51TALK
18	移动金融客户端应用软件备案	移动金融客户端	《关于发布金融行业标准加强移动金融客户端应用软件安全管理的通知》	工商银行、建设银行、京东金融、支付宝 SDK

2. 目前，上述某些行业资质的办理具有相当的难度（比如信息网络传播视听节目许可证、支付业务许可证），不同监管部门、不同地区对无证经营的执法力度也不尽一致。总体而言，监管部门大多采取了审慎包容、鼓励创新的态度，但近年来随着部分行业乱象频出，监管部门执法力度亦有趋严之势头，建议从事相关业务的企业结合自己具体的业务形态，密切跟踪监管政策，并尽量取得相应的资质许可/备案，以避免因资质不全而产生重大合规风险。

问题五：用户身份认证问题

1“后台实名，前台自愿”是我国对于互联网信息服务用户身份认证的一贯监管原则，在多个监管规定中均有明确规定，比如《移动互联网应用程序信息服务管理规定》《互联网用户账号名称管理规定》《即时通信工具公众信息服务发展管理暂行规定》《互联网直播服务管理规定》《互联网论坛社区服务管理规定》《互联网群组信息服务管理规定》《微博客信息服务管理规定》《互联网跟帖评论服务管理规定》等。

2.在早期的互联网发展过程中，经常采用拍摄身份证照片、拍摄手持身份证照片、银行卡小额转账等方式进行身份认证，此类方式大多已经不满足现行的个人信息保护和数据安全合规要求，且效率较低，一般不建议使用。

3. 目前，基于我国对手机号码实行实名制管理，在APP 的运营中，可以基于手机号码对自然人用户进行真实身份认证，这是当前实践中相对简单且相对安全的身份认证方式。与此同时，部分大型平台（比如微信、支付宝）在多年的发展中已经事实上形成了“互联网基础设施”的地位，基于此类平台已对用户真实身份进行较为权威的认证，使用该等平台的接口进行注册登录，也可以满足大部分场景的身份认证需求。

4.随着技术的发展和电信诈骗活动的高发，在对用户真实身份核验要求较高的领域，仅基于电话号码或者第三方应用接口进行真实身份认证的方式可能不满足行业要求。以金融行业为例，需要使用指纹识别、人脸识别等技术对用户身份进行认证，方可满足监管要求。

5.除了对自然人用户进行身份认证外，企业用户也需要进行真实身份认证，企业用户身份认证一般基于统一社会信用代码（即营业执照）。涉及法定代表人身份认证的，参照对自然人用户进行身份认证的方式处理。

6.不论是基于手机号码的认证，还是基于生物识别技术的认证，背后大多离不开权威机关（比如公安部门）提供的可信身份认证平台（比如姓名与身份证号码、手机号码的一致性比对）。 目前市场上已有大量成熟的身份认证解决方案，企业根据自身需要选用即可。

7.需要特别说明的是，用户身份认证并非越严格越好，尤其是使用生物识别技术的身份认证，尽管可以更大程度对用户的真实身份进行识别和验证，但生物识别信息属于敏感信息，对敏感信息的收集和使用又必须遵守个人信息保护相关的法律法规。按照个人信息保护方面的合规要求，具体使用何种身份认证方式，需要遵守“最小必要”的原则，至于何为“最小必要”，一个简单的判断方式是参考同行的主流做法。

问题六：电子合同与电子签名问题

1.《民法典》第四百六十九条规定，当事人订立合同，可以采用书面形式、 口头形式或者其他形式。以电子数据交换、电子邮件等方式能够有形地表现所载内容，并可以随时调取查用的数据电文，视为书面形式。

2. 通过 APP开展业务，通常会通过点击交互的方式与用户达成一定的约定，这在法律上属于订立合同。对于一般的权利义务，通常使用《用户注册协议》和《平台交易规则》进行约定，而对于某些比较重要的事项，则可能通过单独的法律文本进行约定，比如要查询个人的征信，按照监管要求，需要取得个人的单独同意，通常就需要配置一份专门的《个人征信查询授权书》。

3.与线下的纸质合同不同， 电子合同不是依赖个人签字捺印或者公司盖章来确认合同内容的真实性和完整性，而是依赖电子数据，而电子数据天然存在易篡改、易毁损的问题。电子合同在早期发展阶段面临的主要问题是，如何保证电子数据在形成后，内容始终保持完整、未被更改？如何证明是特定当事人签署的？

4.早期的解决方案主要是依赖权威机构背书，比如具有资质的 CA 认证机构。但传统的CA认证机构流程较为复杂，成本较高，还不如签了纸质版邮寄。随着区块链等技术的发展，电子数据容易篡改的问题已经得到解决， 电子合同的效力也逐渐得到各级司法机关的广泛认可。根据 2019 年修正版《电子签名法》的规定，除涉及婚姻、收养、继承等人身关系和涉及停止供水、供热、供气等公用事业服务等少数场景不能使用电子合同，绝大部分合同都可以通过电子方式订立。

5.对于 To C业务而言，电子合同相比线下纸质合同的成本优势明显。市场上也已经有不少成熟的电子合同服务商，企业结合自身需求择优选用即可。当然，并非所有合同都有使用电子合同供应商的必要，也并非所有合同都适合采用电子合同方式签订，还是要结合具体场景具体分析。

6. 对于To B 的业务，建议结合合同标的额、签约频率、行业接受度、违约风险、行业特殊要求等因素综 合考虑。毕竟，在商事交易中， 电子合同的成本和便利性优势对比可能的商业利益、维权成本可能是微不足道的。

问题七：电子商务平台的合规义务

1.根据《电子商务法》的规定，电子商务是指通过互联网等信息网络销售商品或者提供服务的经营活动，电子商务经营者是指通过互联网等信息网络从事销售商品或者提供服务的经营活动的自然人、法人和非法人组织，包括电子商务平台经营者、平台内经营者以及通过自建网站、其他网络服务销售商品或者提供服务的电子商务经营者，电子商务平台经营者是指在电子商务中为交易双方或者多方提供网络经营场所、交易撮合、信息发布等服务，供交易双方或者多方独立开展交易活动的法人或者非法人组织。

2.作为一种非常典型的业态，电子商务主要分为自营型电商和平台型电商两种。《电子商务法》对于电商平台课以了大量合规义务，除了依法办理市场主体登记、依法纳税、办理相关行政许可、消费者保护等通用型合规义务外，还包括电商平台的一些特殊合规义务，包括：（1）依法记录、保存商品、服务信息以及交易信息；

（2）制定并公示平台服务协议和交易规则，并在修改前述协议和规则时确保有关各方充分表达意见；

（3）禁止对平台内商家交易、交易价格等进行不合理限制、附加不合理条件或收取不合理费用；

（4）显著标记平台自营业务与平台内商家开展的业务；

（5）建立健全信用评价制度，公示信用评价规则，禁止删除消费者对商品、服务的评价；

（6）以多种方式向消费者显示商品或服务的搜索结果，并对竞价排名的商品或服务显著标明“广告”；

（7）依法向平台内商家提供服务，禁止采取集中竞价、做市商等集中交易方式以及标准化合约交易；

（8）对商家信息进行核验、登记，建立登记档案并定期核验更新；

（9）向市场监督管理部门以及税务部门报送商家相关信息，提示并配合办理市场主体登记和税务登记；

（10）对违法商品、服务信息采取必要处置并向主管部门报告；

（11）对平台内商家侵害消费者合法权益行为采取必要措施；

（12）对平台内商家侵犯知识产权行为采取必要措施。

3.根据《电子商务法》的规定，违反上述合规义务的，主管机关可以根据具体情况进行行政处罚，处罚形式包括责令限期改正、罚款、没收违法所得以及责令停业整顿.

问题八：第三方支付与电商平台“二清”问题

1.《非金融机构支付服务管理办法》规定，非金融机构提供支付服务，应当取得《支付业务许可证》，并依法接受中国人民银行的监督管理。未经中国人民银行批准，任何非金融机构和个人不得从事或变相从事支付业务。

2.从电商平台的发展历史来看，或出于难以抵制占有大量交易资金获取利息补贴甚至挪用交易资金的诱惑，或出于电商平台分账模式的现实商业需求，或者囿于同行竞争顾虑，很多电商平台都选择过以平台对接或者“大商户”模式接入持证机构，先通过自有资金账户归集用户资金，再自行开展资金清算，并支付给下游户。这种自行开展资金清算的行为，即所谓“二清”。

3. 由于“二清”行为破坏了支付结算业务许可制度，危害支付市场秩序和安全，属于非法从事金融业务，且容易被利用于赌博、诈骗等犯罪活动，是监管部门的重点打击行为，除了严厉的行政处罚外，情节严重的，还可能构成“非法经营罪”或者“帮助信息网络犯罪活动罪”。

4. 经过多年的发展和探索，市场上已出现多种合规的电商平台支付结算业务模式。运营电商类 APP 的企业需要抑制“二清”的冲动，结合自身的实际情况，选择合适的持牌支付机构合作，构建合规的支付结算解决方案。

问题九：网络信息内容治理问题

1. 网络不是法外之地。根据《网络信息内容生态治理规定》，网络信息内容服务平台应当履行信息内容管理主体责任，加强本平台网络信息内容生态治理，培养积极健康、向上向善的网络文化，具体要求是建立网络信息内容生态治理机制，制定本平台网络信息内容生态治理细则，健全用户注册、账号管理、信息发布审核、跟帖评论审核、版面页面生态管理、实时巡查、应急处置和网络谣言、黑色产业链信息处置等制度。

2.需要特别注意的是，APP即使不具备发帖或者发布音视频等常见的信息发布功能，也不能在网络信息内容治理方面掉以轻心。在用户昵称、产品介绍、产品评价这类比较通用的功能中，也不能出现违法信息或者不良信息。

3.按照《网络信息内容生态治理规定》的精神，鼓励网络信息内容生产者制作、复制、发布含有下列内容的信息：

•宣传习近平新时代中国特色社会主义思想，全面准确生动解读中国特色社会主义道路、理论、制度、文化的；

•宣传党的理论路线方针政策和中央重大决策部署的；

•展示经济社会发展亮点，反映人民群众伟大奋斗和火热生活的；

•弘扬社会主义核心价值观，宣传优秀道德文化和时代精神，充分展现中华民族昂扬向上精神风貌的；

•有效回应社会关切，解疑释惑，析事明理，有助于引导群众形成共识的；

•有助于提高中华文化国际影响力，向世界展现真实立体全面的中国的；

其他讲品味讲格调讲责任、讴歌真善美、促进团结稳定等的内容.

4. 与此同时，网络信息内容生产者不得制作、复制、发布含有下列内容的违法信息：

•反对宪法所确定的基本原则的；

•危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一的；

•损害国家荣誉和利益的；

•歪曲、丑化、亵渎、否定英雄烈士事迹和精神， 以侮辱、诽谤或者其他方式侵害英雄烈士的姓名、 肖像、名誉、荣誉的；

•宣扬恐怖主义、极端主义或者煽动实施恐怖活动、极端主义活动的；

•煽动民族仇恨、民族歧视，破坏民族团结的；

• 破坏国家宗教政策，宣扬邪教和封建迷信的；

•散布谣言，扰乱经济秩序和社会秩序的；

•散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的；

•侮辱或者诽谤他人，侵害他人名誉、隐私和其他合法权益的；

•法律、行政法规禁止的其他内容。

5.除此之外，网络信息内容生产者还应当采取措施，防范和抵制制作、复制、发布含有下列内容的不良信息：

•使用夸张标题，内容与标题严重不符的；

•炒作绯闻、丑闻、劣迹等的；

•不当评述自然灾害、重大事故等灾难的；

•带有性暗示、性挑逗等易使人产生性联想的；

•展现血腥、惊悚、残忍等致人身心不适的；

•煽动人群歧视、地域歧视等的；

•宣扬低俗、庸俗、媚俗内容的；

•可能引发未成年人模仿不安全行为和违反社会公德行为、诱导未成年人不良嗜好等的；

•其他对网络生态造成不良影响的内容。

问题十：网络安全、数据安全与等保、关保问题

1.根据《网络安全法》和《数据安全法》的规定，国家实行网络安全等级保护制度，利用信息网络开展数据处理活动的，应在网络安全等级保护制度的基础上履行数据安全保护义务。APP作为一种典型的信息系统，运营者应当在网络安全等级保护制度的基础上做好网络安全和数据安全保护工作。

2.所谓网络安全等级保护，是指根据在国家安全、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、法人和其他组织的合法权益的危害程度等，所有网络由低到高划分为五个安全保护等级，不同的安全保护等级在物理环境、通信网络、计算环境、管理制度、管理机构、管理人员等方面均对应不同的要求，安全保护等级越高的，等级保护工作要求也更高。

定级要素与安全保护等级的关系

受侵害的客体	对客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第三级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

3.实际上，在《网络安全法》实施之前，我国就已经在实施网络安全等级保护制度。随着《网络安全法》及配套的《网络安全等级保护条例（征求意见稿）》《网络安全等级保护测评机构管理办法》和相应的新的等级保护相关标准的颁布，我国逐渐建立起升级版的网络安全等级保护体系，业内称之为等级保护2.0。

4.根据等级保护2.0相关文件的规定，网络运营者应当履行的一般安全保护义务包括：

•确定网络安全等级保护工作责任人，建立网络安全等级保护工作责任制，落实责任追究制度；

•建立安全管理和技术保护制度，建立人员管理、教育培训、系统安全建设、系统安全运维等制度；

•落实机房安全管理、设备和介质安全管理、网络安全管理等制度，制定操作规范和工作流程；

•落实身份识别、防范恶意代码感染传播、防范网络入侵攻击的管理和技术措施；

•落实监测、记录网络运行状态、网络安全事件、违法犯罪活动的管理和技术措施，并

按照规定留存六个月以上可追溯网络违法犯罪的相关网络日志；

•落实数据分类、重要数据备份和加密等措施；

•依法收集、使用、处理个人信息，并落实个人信息保护措施，防止个人信息泄露、损毁、篡改、窃取、丢失和滥用；

•落实违法信息发现、阻断、消除等措施，落实防范违法信息大量传播、违法犯罪证据灭失等措施；

•落实联网备案和用户真实身份查验等责任；

•对网络中发生的案事件，应当在二十四小时内向属地公安机关报告；泄露国家秘密的，应当同时向属地保密行政管理部门报告等。

5.根据等级保护 2.0 相关文件的要求，网络运营者应当在规划设计阶段确定网络的安全保护等级，第二级以上网络运营者应当在网络的安全保护等级确定后 10 个工作日内，到县级以上公安机关备案。另根据公安部《贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见》，第三级以上网络运营者应委托符合国家有关规定的等级测评机构，每年开展一次网络安全等级测评，并及时将等级测评报告提交受理备案的公安机关和行业主管部门。

6.关于如何判断“一般损害”“严重损害”和“特别严重损害”，没有形成完全统一的公开标准，不同地区、不同行业可能有不同的细节性要求。运营者可先自行或委托第三方机构参考公共安全行业标准《信息安全技术 网络安全等级保护定级指南》（GA/T 1389-2017）进行初步评测，根据初步评测结果进行备案申报，若公安机关认为运营者自主定级不准确的，将会要求重新定级并重新递交备案材料，最终定级以公安机关认定的等级为准。在等保定级备案的过程中，若公安机关认为运营者提交的材料不符合等保要求，会要求进行整改，整改合格的，才予以通过并颁发《信息系统安全等级保护备案证明》。

7.除了等保之外，国家对于关键信息基础设施的安全保护另有更加严格的要求，一般简称为“关保”。根据《关键信息基础设施安全保护条例》，所谓关键信息基础设施，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。

8.企业是否属于关键信息基础设施运营者， 由上述行业和领域的主管部门、监管部门进行认定，并报公安部门备案。与此同时，认定结果将通知运营者。如果被认定为关键性基础设施运营者，企业还应当履行关键信息基础设施保护的相关义务。

9.根据现行《网络安全法》和《数据安全法》的规定，拒不履行网络安全保护义务或者数据安全保护义务，造成严重后果的，主管部门可以对单位以及直接负责的主管人员和其他直接责任人员进行行政处罚，处罚形式包括责令改正、给予警告、责令暂停业务、停业整顿、吊销业务许可证、吊销营业执照、罚款等，其中对单位的最高行政处罚为一千万元，对个人的最高行政处罚为二十万元。

10.除此之外，《刑法》第二百八十六条之一规定："网络服务提供者不履行法律、行政法规规定的信息网络安全管理义务，经监管部门责令采取改正措施而拒不改正，有下列情形之一的，处三年以下有期徒刑、拘役或者管制，并处或者单处罚金：（一）致使违法信息大量传播的；（二）致使用户信息泄露，造成严重后果的；（三）致使刑事案件证据灭失，情节严重的；（四）有其他严重情节的。单位犯前款罪的，对单位判处罚金,并对其直接负责的主管人员和其他直接责任人员，依照前款的规定处罚。

这是2015年《刑法修正案（九）》增加的一个罪名，叫做"拒不履行信息网络安全管理义务罪"。该罪名知名度不高，实践中应用还比较少，其中一个原因是作为一种不作为犯罪，该罪名的适用前提是"经监管部门责令采取改正措施而拒不改正"，而实践中关于网络安全的执法活动在多数省份尚未大规模开展。

问题十一：数据与个人信息保护问题

1.一方面，个人信息的滥用和泄露以及因此导致的营销泛滥、电信网络诈骗等问题由来已久，几乎所有人都饱受其扰甚至深受其害；另一方面，数据作为一种生产要素已经被提升到相当的高度。作为一种比较重要的数据——个人信息应当如何保护和有效利用，成为了我们这个时代面临的重大课题。在此大背景下，《个人信息保护法》以及各种配套的监管制度应运而生。在APP 的运营过程中，势必会收集和产生大量的个人信息和其他数据，数据安全与个人信息保护合规因此成为了APP 运营者合规工作的重中之重。

2.根据《数据安全法》的定义，数据是指任何以电子或者其他方式对信息的记录；根据《个人信息保护法》的定义，个人信息是指以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息；根据《民法典》的定义，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。很明显，仅从概念上看就可以知道，“数据”与“个人信息”并不等同，“个人信息”与“隐私”也并不等同。

3.从我国现行法律法规来看，对数据的监管主要是对重要数据和对个人信息的监管。如果企业业务不涉及处理重要数据或者个人信息，其实在数据合规方面无需过于担心。对于非重要数据、非个人信息的数据，只要不是通过不正当的方式取得，一般而言没有特别大的合规风险（当然，数据安全仍然需要重视）。

4.《数据安全法》规定，国家数据安全工作协调机制统筹协调有关部门制定重要数据目录，加强对重要数据的保护，对重要数据的处理应当定期开展风险评估。加强重要数据的保护，首先当然需要识别哪些数据属于重要数据。关于重要数据的识别规则几易其稿，终于在2024年3 月15 日发布的国标《数据安全技术 数据分类分级规则》中有了正式的识别指南，但该指南仍然较为原则。目前，除部分行业（比如汽车行业、电信行业）已对重要数据进行明确列举外，诸多行业重要数据的具体认定标准和范围仍需要行业主管部门的进一步明确。尽管如此，对于身处关键敏感行业，或者掌握了大量个人信息的APP经营者，仍需要结合自身的实际情况，参考前述国标给出的识别指南，提前预判自己处理的数据是否构成重要数据，如果判断可能构成，则应主动按照重要数据标准对其进行重点保护。

5.与重要数据不同，个人信息的认定标准和范围已经比较明确，尽管在特殊场景下对特定信息是否构成个人信息尚有争论，但大部分常见的个人信息字段已在业内达成广泛共识。且随着《个人信息保护法》及相关配套制度（比较重要的包括《App违法违规收集使用

个人信息行为认定方法》《信息安全技术 个人信息安全规范》《信息安全技术 个人信息处理中告知和同意的实施指南》等） 的生效和落地实施，APP 运营者在个人信息保护方面的合规义务也已经非常明确、具体和丰富。

6.根据《个人信息保护法》及相关配套制度的规定，APP 运营者作为个人信息处理者在个人信息保护方面的合规义务主要包括如下维度：

•个人信息处理行为的合法性基础维度；

•必要性原则落实维度；

•个人信息处理规则内容维度；

•个人信息处理规则告知、公开、解释说明维度；

•共同处理维度；

•委托处理维度；

•个人信息转移维度；

•对外提供（共享）维度；

•利用自动化决策处理个人信息维度；

•公开个人信息维度；

•公共场所安装图像采集、个人身份识别设备维度；

•已公开个人信息处理维度；

•处理敏感个人信息维度；

•处理不满十四周岁未成年人个人信息维度；

•向境外提供个人信息维度；

•个人信息删除权保障维度；

•个人信息主体权益保障维度；

•个人信息保护主体责任履行维度；

•内部管理制度和操作规程维度；

•安全技术措施采取情况和有效性维度；

•教育培训计划的制定和实施维度；

•个人信息保护负责人指定维度；

•个人信息保护影响评估维度；

•个人信息安全事件应急预案维度；

•大型互联网平台特殊要求维度。

7.在现行法律法规和监管背景下，违规收集和使用个人信息将同时在行政处罚、民事赔偿、刑事处罚、资本市场等方面面临重大风险。

（1）在行政方面，《个人信息保护法》第六十六条规定，违反该法规定处理个人信息，或者处理个人信息未履行该法规定的，由履行个人信息保护职责的部门责令改正，给予警告，没收违法所得，对违法处理个人信息的应用程序，责令暂停或者终止提供服务；拒不改正的，并处一百万元以下罚款；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。有前款规定的违法行为，情节严重的，由省级以上履行个人信息保护职责的部门责令改正，没收违法所得，并处五千万元以下或者上一年度营业额百分之五以下罚款，并可以责令暂停相关业务或者停业整顿、通报有关主管部门吊销相关业务许可或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款，并可以决定禁止其在一定期限内担任相关企业的董事、监事、高级管理人员和个人信息保护负责人。

（2）在民事责任方面，根据《个人信息保护法》第六十九条、第七十条规定，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，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。前述损害赔偿责任按照个人因此受到的损失或者个人信息处理者因此获得的利益确定；个人因此受到的损失和个人信息处理者因此获得的利益难以确定的，根据实际情况确定赔偿数额。

（3）在刑事处罚方面，根据《刑法》第二百五十三条之一规定，违反国家有关规定，向他人出售或者提供公民个人信息，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节严重的，处三年以上七年以下有期徒刑，并处罚金。违反国家有关规定，将在履行职责或者提供服务过程中获得的公民个人信息，出售或者提供给他人的，依照前款的规定从重处罚。需要特别强调的是，侵犯公民个人信息罪的入罪门槛应该说并不高，实践中已出现大量企业因侵犯公民个人信息而涉刑的案例，需要数字化转型企业高度重视。

（4）在资本市场融资方面，对于涉及个人信息处理的企业而言，数据安全与个人信息合规问题目前已几乎成了证券监管部门必定关注的事项。资本市场已经多次出现因存在个人信息保护合规问题而折戟 IPO 的案例。

8. 根据我们的经验和对监管实践的观察，对于APP运营者而言，现阶段需要关注的合规重点是APP的UI界面设计问题、敏感信息收集和敏感权限获取时的提示文案问题、隐私

政策（亦称个人信息保护政策）和“双清单”（已收集个人清单和向第三方共享个人信息清单）的撰写和配置问题、频繁自启动和关联启动问题、个性化推送问题、注销权益保障以及是否涉及个人信息出境等问题。

9. 撰写隐私政策往往是企业开展个人信息保护合规的第一步，也是非常关键的一步，其核心要求是务必要与 APP 实际收集使用个人信息的情况一致。

10. 作为一种检视企业在个人信息保护方面合规义务履行情况的重要方式（同时本身也是一项合规义务），《个人信息保护法》第五十四条规定：“个人信息处理者应当定期对其处理个人信息遵守法律、行政法规的情况进行合规审计。”作为落实这一法律规定的配套性制度，国家网信办于2025年2月发布了《个人信息保护合规审计管理办法》，对个人信息保护合规审计的相关方法、流程和审计要点进行了规定。按照该征求意见稿，处理超过100万人个人信息的个人信息处理者，应当每年至少开展一次个人信息保护合规审计，其他个人信息处理者应当每二年至少开展一次个人信息保护合规审计。应该说，近几年针对个人信息保护的立法颇多，作为一种比较典型的个人信息处理者，APP运营企业在个人信息保护方面面临的合规义务也随之变得颇为复杂。与此同时，个人信息保护合规审计其实也是检视自身合规程度、发现风险、建设完善合规体系的有效手段，建议企业（尤其是 C 端用户数量较大的企业）及早着手此项工作。

问题十二：数据出境安全评估与个人信息出境标准合同备案问题

1.数据出境涉及国家安全，是一个热门且严肃的话题，《网络安全法》《数据安全法》和《个人信息保护法》三大法律均对此有所规定，要求规定符合规定情形的数据出境需要向国家网信部门申报数据出境安全评估、或者签订个人信息出境标准合同并备案、或者通过个人信息保护认证。

2.由于国际环境和经济形势等复杂因素的叠加，我国数据出境的监管政策这两年经历了一个从严到松、从紧到宽的发展历程。2024年3月22日，《促进和规范数据跨境流动规定》正式发布，该规定对相当一部分根据原有规定需要申报数据出境安全评估或者签订个人信息出境标准合同的情形进行了豁免，预计将成为很长一段时期内的数据出境监管基本政策。

3. 根据《促进和规范数据出境流动规定》，以下两种情况需要向国家网信部门申报数据出境安全评估：（1）关键信息基础设施运营者向境外提供个人信息或者重要数据（从数据处理者的身份维度判断）；（2）关键信息基础设施运营者以外的数据处理者向境外提供重要数据，或者自当年1月1 日起累计向境外提供100万人以上个人信息（不含敏感个人信息）或者1万人以上敏感个人信息（从出境数据的类型和数量维度判断）。同时，数据处理者应当按照相关规定识别、申报重要数据。未被相关部门、地区告知或者公开发布为重要数据的，数据处理者不需要作为重要数据申报数据出境安全评估。关键信息基础设施运营者以外的数据处理者自当年1月1日起累计向境外提供10万人以上、不满100万人个人信息（不含敏感个人信息）或者不满1万人敏感个人信息的，应当依法与境外接收方订立个人信息出境标准合同或者通过个人信息保护认证。

4. 根据规定，数据出境监管的对象仍然是重要数据和个人信息，如果出境的数据不属于重要数据或者个人信息，不需要进行数据安全评估，也不需要签订个人信息出境标准或者通过个人信息保护认证。同时，规定对跨境经济活动中一些常见的个人信息出境情形也进行了豁免，包括：

•为订立、履行个人作为一方当事人的合同，如跨境购物、跨境寄递、跨境汇款、跨境支付、跨境开户、机票酒店预订、签证办理、考试服务等，确需向境外提供个人信息；

•按照依法制定的劳动规章制度和依法签订的集体合同实施跨境人力资源管理，确需向境外提供员工个人信息的；

•紧急情况下为保护自然人的生命健康和财产安全，确需向境外提供个人信息的；

•关键信息基础设施运营者以外的数据处理者自当年1月1日起累计向境外提供不满10万人个人信息（不含敏感个人信息）的。

•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；

•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。

•确定与所提供服务相适应的安全管理负责人、信息审核人员或者建立安全管理机构的情况；

•用户真实身份核验以及注册信息留存措施；

•对用户的账号、操作时间、操作类型、网络源地址和目标地址、网络源端口、客户端硬件特征等日志信息， 以及用户发布信息记录的留存措施；

•对用户账号和通讯群组名称、昵称、简介、备注、标识，信息发布、转发、评论和通讯群组等服务功能中违法有害信息的防范处置和有关记录保存措施；

•个人信息保护以及防范违法有害信息传播扩散、社会动员功能失控风险的技术措施；

•建立投诉、举报制度，公布投诉、举报方式等信息，及时受理并处理有关投诉和举报的情况；

•建立为网信部门依法履行互联网信息服务监督管理职责提供技术、数据支持和协助的工作机制的情况；

•建立为公安机关、国家安全机关依法维护国家安全和查处违法犯罪提供技术、数据支持和协助的工作机制的情况。

5.如果落入需要向国家网信部门申报数据出境安全评估或者需要订立个人信息出境标准合同并备案或者通过个人信息保护认证的情形，则需要依法履行相应义务，不然将属于违法出境，可能面临较为严厉的行政处罚风险。就目前的实践而言，不论是申报数据出境安全评估、订立个人信息出境标准合同还是个人信息保护认证，涉及的工作在技术维度和法律维度均具有相当的专业性（相关评估报告动辄大几十页乃至数百页），建议企业委托专业机构协助。

问题十三：算法备案、生成式人工智能备案与安全评估问题

1.根据《互联网信息服务算法推荐管理规定》，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到网信部门办理备案手续，备案需要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，其中算法自评估报告是进行算法备案非常重要的一份材料。

2.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》，所谓“具有舆论属性或社会动员能力的互联网信息服务”指的是：

•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；

•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。

3.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》，具有舆论属性或社会动员能力的互联网信息服务达到规定情形的，应当开展安全评估，且应当对信息服务和新技术新应用的合法性，落实法律、行政法规、部门规章和标准规定的安全措施的有效性，防控安全风险的有效性等情况进行全面评估，并重点评估下列内容：

• 确定与所提供服务相适应的安全管理负责人、信息审核人员或者建立安全管理机构的情况；

• 用户真实身份核验以及注册信息留存措施；

• 对用户的账号、操作时间、操作类型、网络源地址和目标地址、网络源端口、客户端硬件特征等日志信息， 以及用户发布信息记录的留存措施；

• 对用户账号和通讯群组名称、昵称、简介、备注、标识，信息发布、转发、评论和通讯群组等服务功能中违法有害信息的防范处置和有关记录保存措施；

• 个人信息保护以及防范违法有害信息传播扩散、社会动员功能失控风险的技术措施；

• 建立投诉、举报制度，公布投诉、举报方式等信息，及时受理并处理有关投诉和举报的情况；

• 建立为网信部门依法履行互联网信息服务监督管理职责提供技术、数据支持和协助的工作机制的情况；

• 建立为公安机关、国家安全机关依法维护国家安全和查处违法犯罪提供技术、数据支持和协助的工作机制的情况。

4.根据《互联网信息服务深度合成管理规定》，提供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。

5.根据《生成式人工智能服务管理暂行办法》的规定，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。

6.近年来，以生成式人工智能为代表的新技术、新应用发展迅速，相关监管规定也迅速出台。从上述规定不难看出，要求算法、生成式人工智能备案的出发点是看是否具有“舆论属性或社会动员能力”，而备案的核心材料安全评估报告。从监管规定以及我们与监管部门沟通的情况来看，监管部门的目标是“规范和促进发展”，而非“管死”，企业无需畏惧监管，而是应当积极主动拥抱监管，监管部门通常也是乐意与企业进行交流的。

问题十四：互联网广告合规问题

1.根据《互联网广告管理办法》规定，所谓互联网广告，是指利用网站、网页、互联网应用程序等互联网媒介，以文字、图片、音频、视频或者其他形式，直接或者间接地推销商品或者服务的商业广告活动。

2.互联网广告，本质上仍然是广告，《广告法》所规定的所有合规要求，互联网广告当然必须要首先遵循，比如不能使用“ 国家级 ”“最高级 ”“最佳 ”等用语，不能使用或者变相使用国家机关、国家机关工作人员的名义或者形象，不能以虚假或者引人误解的内容欺骗、误导消费者，涉及医疗、药品、医疗器械、农药、兽药、保健食品、特殊医学用途配方食品广告等法律、行政法规规定应当进行审查的广告，应当在发布前由广告审查机关对广告内容进行审查。

3.除了《广告法》规定的通用合规要求外，互联网广告还有一些特殊合规要求，比如以弹出等形式发布互联网广告，应当显著标明关闭标志，确保一键关闭，互联网平台经营者应当对利用其信息服务发布的广告内容进行监测、排查，防范和制止违法广告等。

4.可以说，互联网广告是 APP 运营企业很难绕开的一个话题。企业既可能是广告主，也可能是广告经营者或者广告发布者，不管是何种身份，都需要仔细看看《广告法》和《互联网广告管理办法》，广告发布量大的企业，最好配备专职的广告审查人员，以避免各种行政处罚风险和民事赔偿风险。