

个人信息保护合规建设

桔皮书

奇安信科技集团股份有限公司

2022年1月

版权声明

本文中出现的任何文字叙述、文档格式、插图、图片、方法、过程等内容，除另有特别注明，版权均为**奇安信集团（指包括但不限于奇安信科技集团股份有限公司、网神信息技术（北京）股份有限公司、北京网康科技有限公司）**所有，受到有关产权及版权法保护。任何个人、机构未经**奇安信集团**的书面授权许可，不得以任何方式复制或引用本文的任何片段**。**

# 前 言

随着大数据时代的到来，个人信息保护得到了前所未有的重视。国际上围绕个人信息的获取、分析、利用和控制的竞争越来越激烈，个人信息安全已成为维护国家安全、保持社会稳定、关系长远利益的关键组成部分，备受各国政府的关注和重视。如何确保个人信息安全已是各国政府及各种组织改进其竞争能力的一个新的具有挑战性的任务。

个人信息保护工作任重而道远，这不仅仅是个人信息保护专业人士的责任，也需要得到所有人的关注和投入。因此，个人信息保护工作也要与时俱进，成为数字化转型道路上的“照明灯”和“守护者”。企业或组织的管理者要主动应对各种个人信息风险和问题，持续关注个人信息监管和行业标准最新动态，并积极参与管理实践和隐私科技的发展。此外，个人信息保护能力也将作为企业或组织影响力的关键因素，从用户隐私体验、科技透明度和市场信任感上为业务赋能。

编订《个人信息保护合规建设实践桔皮书》，全面分析了企业或组织个人信息保护合规建设驱动力，所面临的挑战，提出了合规建设的技术应用探索，并全面阐述了建设方案和关键技术的应用探索。希冀本桔皮书能为企业或组织个人信息保护合规建设提供借鉴和参考，分享研究成果，共谋发展。

目 录

[一、 个人信息保护建设背景 1](#_Toc24421)

[（一） 合规监管要求逐渐完善 2](#_Toc27015)

[（二） 监管执法强度持续提高 3](#_Toc27044)

[二、 个人信息保护建设面临的问题和困境 5](#_Toc9006)

[（一） 数据挖掘与个人信息保护的矛盾 5](#_Toc7188)

[（二） 个人信息保护建设面临的困境 6](#_Toc3973)

[1. 业务与合规——经营模式的变革 6](#_Toc28341)

[2. 组织与制度——跨部门协作导致合规成本升高 7](#_Toc26827)

[3. 人员与技术——多学科交叉导致合规效果不理想 8](#_Toc9991)

[4. 目标与过程——合规建设的复杂性与持续性 8](#_Toc19593)

[三、 个人信息保护建设思考 10](#_Toc19022)

[（一） 识别监管要求聚焦安全保护重点 10](#_Toc6479)

[1. 个人信息处理原则合规 10](#_Toc22992)

[2. 个人信息处理规则明确 13](#_Toc15475)

[3. 个人信息处理责任落实 14](#_Toc25097)

[4. 个人信息主体权利保障 16](#_Toc6906)

[（二） 技术辅助企业或组织个人信息保护合规落地 17](#_Toc31868)

[四、 个人信息保护建设实践方法 18](#_Toc22181)

[（一） 识别监管要求建立企业或组织合规体系 18](#_Toc8458)

[（二） 嵌入全流程的个人信息合规管理 20](#_Toc30832)

[（三） 个人信息前端收集工具合规评估 21](#_Toc19183)

[（四） 个人信息使用过程中的风险管控 22](#_Toc5131)

[（五） 建立个人信息安全事件处置机制 24](#_Toc22241)

[（六） 通过个人信息安全影响评估持续改进 24](#_Toc21520)

[五、 结语 25](#_Toc27360)

##

## 个人信息保护建设背景

随着大数据时代的到来，作为数字经济时代最核心、最具价值的生产要素，数据已经成为国家基础性战略资源，对国家治理能力、经济运行机制、社会生活方式产生深刻影响。与此同时，在数字技术不断推动经济发展的同时，其背后的安全风险也日益显现出来。近年来，各类数据泄漏、数据滥用、个人隐私侵害等安全事件更是层出不穷。如何在保障数字经济高速发展的同时，正确开展数据安全治理，保护公民个人隐私不被侵害，已引起各国的高度重视和全社会的广泛探讨。

2021年8月20日，全国人大常委会会议通过《个人信息保护法》，2021年11月1日正式实施。《个人信息保护法》正式颁布实施，标志着我国个人信息保护立法体系进入新的阶段。《个人信息保护法》的出台为个人信息权益保护、信息处理者的义务以及主管机关的职权范围提供了全面的、体系化的法律依据，涵盖个人信息收集、存储、使用、加工、传输、提供、公开、删除等多个环节以及自动化决策、个人信息跨境提供等特定场景，与《民法典》《网络安全法》《数据安全法》等共同构成了我国个人信息保护的法律框架。该法将合法、正当、必要与最小必要、透明公开、公平公正作为个人信息活动的基本原则，明确个人信息跨境处理要求，充分保障用户对个人信息处理的知情权和控制权，赋予用户删除、查询、更正、补充个人信息等权利，明确个人信息处理者应当遵循告知、个人信息分类、个人信息安全加密、敏感个人信息事前影响评估等义务，保障用户个人信息安全。

随着数据价值的进一步凸显，侵犯个人隐私的情形不断增多。由于智能手机和移动应用的流行，企业或组织收集个人信息的主要手段包括App、小程序等，用户在智能手机上存储了大量个人信息，而如何对这些个人信息加以保护遂成为重要挑战。为此，国家监管机构发布了一系列的相关法律法规和监管标准，围绕App监管和个人信息违法犯罪活动开展了诸多执法专项行动。

### 合规监管要求逐渐完善

监管机关针对个人信息保护监管与执法都呈现出趋严趋紧的特点，不断加大个人信息保护监管力度。2019年11月28日，[国家互联网信息办公室](https://baike.baidu.com/item/%E5%9B%BD%E5%AE%B6%E4%BA%92%E8%81%94%E7%BD%91%E4%BF%A1%E6%81%AF%E5%8A%9E%E5%85%AC%E5%AE%A4/2045128%22%20%5Ct%20%22https%3A//baike.baidu.com/item/App%E8%BF%9D%E6%B3%95%E8%BF%9D%E8%A7%84%E6%94%B6%E9%9B%86%E4%BD%BF%E7%94%A8%E4%B8%AA%E4%BA%BA%E4%BF%A1%E6%81%AF%E8%A1%8C%E4%B8%BA%E8%AE%A4%E5%AE%9A%E6%96%B9%E6%B3%95/_blank)、工业和信息化部、公安部、市场监管总局联合制定了《App违法违规收集使用个人信息行为认定方法》，自印发之日起实施。重点关注可被认定为“未公开收集使用规则”的行为，可被认定为“未明示收集使用个人信息的目的、方式和范围”的行为，可被认定为“未经用户同意收集使用个人信息”的行为，可被认定为“违反必要原则，收集与其提供的服务无关的个人信息”的行为，可被认定为“未经同意向他人提供个人信息”的行为，以及可被认定为“未按法律规定提供删除或更正个人信息功能”或“未公布投诉、举报方式等信息”的行为，为App运营者提供合规指引。2020年5月，国家网信办等四部委联合制定的《常见类型移动互联网应用程序必要个人信息范围规定》正式实施，明确App不得强制收集非必要个人信息。工信部针对App的治理，开展了专项行动，采取一系列措施，总体效果比较明显，近期拟会同相关部门联合出台《移动互联网应用程序个人信息保护的管理暂行规定》，App个人信息处理活动应当采用合法、正当的方式，遵循诚信原则，不得通过欺骗、误导等方式处理个人信息，切实保障用户同意权、知情权、选择权和个人信息安全，对个人信息处理活动负责。此外，2021年11月，国家网信办会同相关部门研究起草的《网络数据安全管理条例》公开征求意见，其中“个人信息保护”章节详细规定了知情同意、最小必要、权利保障、生物特征信息等方面的要求，并明确提出处理一百万人以上个人信息应视为重要数据处理者进行管理，进一步强化消费者个人信息保护。

### 监管执法强度持续提高

根据国家计算机网络应急技术处理协调中心、中国网络空间安全协会发布的《App违法违规收集使用个人信息监测分析报告》，今年以来，国家网信办持续开展App违法违规收集使用个人信息专项治理工作，加大执法监管力度，组织对 39 种常见类型公众大量使用的1425款App开展了专项检测，已对其中存在严重违法违规问题的351款App进行了公开通报，责令限期整改;对未在规定时限内整改的依法采取了相关处罚措施。国家计算机网络应急技术处理协调中心积极运用大数据等新技术手段，建设App收集使用个人信息监测平台，实现对国内主流应用商店在架App存在的“不给权限不让用、频繁索权干扰用户、启动就索要无关权限、未经用户同意收集个人信息”等16项典型违法违规问题的全量快速检测。专项治理有力震慑了违法违规行为，大大提高了App运营者对个人信息保护工作的重视程度，取得了良好的治理效果和社会反响。此外，2021年1-4月，工信部已累计完成29万款App技术检测，对1862款违规App提出整改要求，公开通报319款整改不到位App，组织下架了107款拒不整改的App。通过持续整治热点难点问题。在前期App专项整治的基础上，进一步聚焦工具类、通信类等App，加大欺骗诱导用户下载、弹窗信息难以关闭、违规共享使用个人信息和利用第三方嵌入式软件损害用户权益等热点难点问题的整治力度。

面对不断加大的数据安全及个人信息保护监管力度，企业或组织如何建立健全符合企业或组织管理现状及发展需求的个人信息保护管理体系，确保个人信息安全合规，同时充分发挥数据对企业或组织发展的积极推动作用，已成为各行各业发展过程中的重大挑战。

## 个人信息保护建设面临的问题和困境

数字经济的持续深化推进，数据已成为影响世界各国竞争的战略性资源。能够充分发挥数据经济价值和战略意义的数据开发利用技术蓬勃发展的同时，防止数据泄漏，丢失，滥用，保障数据安全流通共享与流通的数据安全技术也愈发重要。主要包括二方面难点，一方面是数据安全与数据开发利用效率之间尚存在明显矛盾，成为制约数据价值释放的重要短板。另一方面，随着《数据安全法》《个人信息保护法》的实施，在个人信息保护工作中，大多数企业或组织面临的首要挑战是监管合规，了解监管要求后，企业或组织需要摸索个人信息保护体系建设。

### 数据挖掘与个人信息保护的矛盾

数字经济时代，数据蕴含的巨大价值，越来越多的企业或组织利用大数据分析、数据中台分析、评估消费者的个人特征用于商业营销或与产业上下游的业务伙伴通过数据流通实现深度合作，以此来挖掘数据价值，获取竞争优势。

手机应用程序（App）因其便捷性等优势，被广泛运用于日常生活、专业服务和社会治理等多领域，为人们带来便捷的同时，也带来了信息安全隐患。近年来，App违规违法收集使用用户信息事件频发，有报告显示，超七成App存在过度索权行为，即在非必要的情况下获取用户隐私权限，增加了个人信息泄漏的风险。随着个人信息保护相关法规标准的不断出台，加上监管治理的不断深入，企业或组织原本的发展方式必然受到影响，一些依靠收集使用个人信息推动业务发展的模式甚至面临违法犯罪风险。企业或组织的经营模式由原来的“先发展后治理”转变为“边发展边治理”。另一方面频发的个人信息泄漏事件也引发了公众对数字经济发展中的个人信息保护的意识觉醒。对待数字经济时代的数据价值挖掘，需要结合日渐趋严的合规监管要求，积极探索个人信息保护和数据价值挖掘的平衡点，平衡信息化、数字化发展需求与保障个人信息安全之间的矛盾，成为亟待解决的问题。

### 个人信息保护建设面临的困境

#### 1. 业务与合规——经营模式的变革

当数据已经成为重要的生产要素时，个人信息已经成为各大企业或组织需要重点保护的核心数据资产，在复杂的全球个人信息保护框架下，用户个人信息保护在收集、存储、使用、共享等环节流动起来时，任何企业或组织都面临着前所未有的数据安全与个人信息保护的挑战。

随着个人信息保护相关法规标准的不断出台，加上监管治理的不断深入，企业或组织原本的发展方式必然受到影响，一些依靠收集使用个人信息推动业务发展的模式甚至面临违法犯罪风险。企业或组织的经营模式由原来的“先发展后治理”转变为“边发展边治理”。

处理个人信息应当具有明确、合理的目的，并应当与处理目的直接相关，采取对个人权益影响最小的方式。收集个人信息，应当限于实现处理目的的最小范围，不得过度收集个人信息。在建立健全隐私政策和执行符合实际企业或组织需求的个人信息保护策略同时，企业或组织要抓紧转变当前的经营模式，除去大数据杀熟、调整App个性化推荐的方案、梳理广告投放方案等内容，还需根据合规的要求调整业务逻辑，比如减少诱导性下载，诱导用户注册以及通过线下推广等方式获取用户信息的行为，实现业务内容的良性发展。

#### 2. 组织与制度——跨部门协作导致合规成本升高

相对于以往发展模式，企业或组织在稳步经营的前提下，需要增加额外资源对新的合规要求进行及时响应。根据合规要求，企业或组织需要投入资源在管理制度、人力资源、技术保障方面进行完善。

随着监管机构对合规问题的越来越重视，未来会有更多的App会被纳入监管的检测、通报和下架的范围之中，如何在业务持续不断开拓创新与为用户提供更好更安全更尊重的个人信息保护体验之间，建立有力的可落地完备的解决方案是当前合规面临的主要难题，而“有力的落地方案”是企业或组织内部多部门协作的结果。而企业或组织需要根据法规要求，设置“数据安全负责人”、“个人信息保护负责人”，而这个“负责人”需要协调公司的安全、IT、产品线、测试线、法务、企业或组织政府关系以及客服等多个部门才可体系化的完善公司合规方案，避免公司运营过程中的合规风险。

#### 3. 人员与技术——多学科交叉导致合规效果不理想

个人信息保护是典型的多学科交叉领域，个人信息保护既是行政法问题，也是技术规则问题，存在于所有涉及行政监管的领域，需要“技管结合”，概括起来包括三个方面。

（1）个人信息保护规范制定：需要专业的法律界人士、具备丰富合规建设经验企业或组织人士和具备专业技术检测能力的业内人士。

（2）个人信息保护行为检测：也需要专业的法律人员和技术人员配合。

（3）个人信息违规行为处罚：更是一个复杂领域“鉴定”结果认定过程。

因此，单纯从隐私政策或者违规行为检测任一一个方向都无法彻底解决合规治理不理想的问题，需要从技术检测、管理跟进和法律服务等多维度进行综合治理。

从历史被通报的App合规问题来看，典型的违规场景如第三方SDK违规收集、用户同意前收集、后台静默收集、高频收集、隐私政策明示不到位、未提供投诉举报方式、历史版本遗留问题等，既有技术手段检测的内容，又有法律框架合规内容，同时也有企业或组织内部管理上的问题。

#### 4. 目标与过程——合规建设的复杂性与持续性

由于立法、标准和规范相对滞后，移动互联网应用个人信息保护水平参差不齐，用户信息强制收集、过度收集、非授权转移共享、个性化展示、定向推送不规范、账户注销难等问题严重侵害了广大人民群众的切身利益。个人信息保护工作涉及政府监管、企业或组织自律与群众举报等多个方面。在互联网已经深入到经济建设的方方面面，合规工作不仅包括“健全隐私政策，减少个人信息的使用，修改公司产品”等几项内容，还需要考虑其所属的行业（比如，电子政务、金融支付、电力能源、交通运输等）进行针对性治理。

互联网服务提供商产品的更新速率远远超过传统制造型的产品，其主要特点如下。

产品生命周期短：部分企业或组织提供互联网产品服务后可能由于业绩不能达到预期很快下架了该产品甚至是重新开发产品。

产品更新频率快：产品上市初期部分产品甚至每周1更，即使产品稳定后也基本保持每两周1更的频率。

企业或组织并购融合多：当前互联网企业或组织间存在各种各样的投资与并购，这种情况个人信息流转将不可避免并且过程中存在管理缺失。

实际上个人信息保护建设工作无法做到一劳永逸，综合考虑互联网企业或组织自身的特点以及其服务的行业特点，个人信息保护建设工作将是一个复杂而持续的过程。

## 个人信息保护建设思考

### 识别监管要求聚焦安全保护重点

#### 1. 个人信息处理原则合规

《个人信息保护法》总则中规定了个人信息处理的合法、正当、必要、诚信、公开透明等，这些基本原则既是处理者开展个人信息处理活动的基本遵循，也是构建个人信息保护具体规则的制度基础。需要明确的是企业或组织在个人信息的处理中占据绝对的主导地位，在处理个人信息必须遵循合法、正当、必要和诚信原则，具有明确、合理的目的并与处理目的直接相关，采取对个人权益影响最小的方式，限于实现处理目的的最小范围，公开处理规则，保证信息质量，采取安全保护措施等，而这些措施必须贯穿于个人信息处理的全过程、各环节。

**第一、合法原则。**按照《个人信息保护法》《民法典》《网络安全法》《消费者权益保护法》的相关规定其内涵包括：处理者处理个人信息必须具备法律法规规定的合法性基础和处理者在处理个人信息时必须履行法律法规为其设定的义务两个方面，即权利与义务的统一性，既要符合法律法规的要求，又要履行法律法规富裕的义务，企业或组织在个人信息处理的过程中避免出现只使用权利而承担应尽义务的情况。

**第二、正当原则。**正当包括目的正当与手段正当，目的正当即在进行个人信息处理时，要提供一个合法、合理的目的。手段正当即其处理个人信息的过程需要公开、公正、透明。而非通过欺骗、诈骗等方式获取并处理个人信息。比如诈骗或者帮助他人诈骗或者个人信息等就属于目的不正当和手段不正当。

**第三、最小必要原则。**主要指处理者处理个人信息不应当超过可以实现处理目的的最低限度，其处理的个人信息应当限于满足处理目的的最小范围之内，个人信息的过度采集或者加工极容易造成难以预见对主体的损害甚至带来财产损失乃至造成生命威胁。而现实中App端普遍存在违规采集个人信息、超范围采集个人信息、违规使用个人信息、过度索取权限以的现象，同时使用谐音、刷屏、差评等行为对个人进行诋毁、污蔑等现象也普遍存在。因此，合理最低限度的收集与使用个人信息是个保法中的重要原则。

**第四、诚信原则。**诚信是一个道德范畴，以真诚之心,行信义之事。“人之所助者，信也”，“言必信，行必果”。讲诚信，并不是说说，很多人说得容易做起来难，其中《个人信息保护法》相较于《网络安全法》和《消费者权益保护法》更是重点突出了诚信原则。信要求处理者对个人保有基本的善意，尊重个人的合理信赖，在价值取向上优先保护个人信息权益，恪守个人信息处理活动的规范化。诚信贯穿于个人信息处理的各个环节

**第五、公开透明原则。**《个人信息保护法》第7条规定：“处理个人信息应当遵循公开、透明原则，公开个人信息处理规则，明示处理的目的、方式和范围。” 在个人信息处理活动中，个人信息的处理者拥有丰富的收集和处理个人信息的技术手段，个人无法知晓其何种个人信息将以何种方式被处理，也难以了解其个人信息被用于何种处理目的，更难以预测个人信息处理活动可能产生的效果与影响。为了强化个人在个人信息处理活动中的主体地位，保护个人对其个人信息以公平、公正的方式被处理的合理信赖，处理者应当对有关个人信息处理与利用的一般政策、事项等予以公开，个人也有权知悉本人个人信息处理的一般情况。比如依照《个人信息保护法》第18条第2款的规定，当出现紧急情况无法及时向个人履行告知义务时，处理者应当在紧急情况消除后及时告知。

**第六、公平公正的原则。**《个人信息保护法》第五十八条“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，应当履行遵循公开、公平、公正的原则，制定平台规则，明确平台内产品或者服务提供者处理个人信息的规范和保护个人信息的义务。”第二十四条“个人信息处理者利用个人信息进行自动化决策，应当保证决策的透明度和结果公平、公正，不得对个人在交易价格等交易条件上实行不合理的差别待遇。”当前，越来越多的企业或组织利用大数据分析、数据中台分析、评估消费者的个人特征用于商业营销。其中有一些企业或组织通过掌握消费者的经济状况、采购需求、消费习惯、对价格的敏感程度等信息，对消费者在交易价格等方面实行歧视性的差别待遇。面对海量数据的使用，企业或组织需要摒弃偏见，分拆企业或组织内部不透明的服务体系，不滥用其市场支配地位对消费者进行 “大数据杀熟”。鼓励企业或组织通过提供差异化的产品和服务方式为企业或组织提供优良的竞争力和市场活力，摒弃以“算法霸权”谋取市场地位的思维。同时，在日常管理中进行常态化检查和调研，切实防范技术滥用。

#### 2. 个人信息处理规则明确

1. **完善个人信息处理机制。**当前，个人信息收集、使用规则不透明及违规收集、过度收集、超范围收集、违规使用等问题突出。个人信息处理者需要明示个人信息主体其收集使用个人信息的目的，并征求个人信息主体的同意；处理个人信息应当限于实现处理目的所必要的最小范围、采取对个人权益影响最小的方式；处理个人信息应当公开个人信息处理规则，明示处理目的、方式和范围，并应当保证个人信息的质量，避免因个人信息不准确、不完整对个人权益造成不利影响。
2. **明确“告知—同意”是核心规则。**长期以来，应用程序过度收集、使用个人信息问题是社会关注的一大焦点。虽然国家的工信、网信等各级监管部门进行多轮次的通报与下架，但在实践中，互联网企业或组织推出的App仍存在“一揽子授权” “频繁申请权限”“不同意不让用”的问题。企业或组织在面临该问题时，需要放弃在数据处理过程中“霸权”行为，充分授权给个人；并做到敏感个人信息单独取得用户同意；处理个人信息应当在事先充分告知的前提下取得个人同意等。围绕“告知-同意’的核心确立的个人信息保护核心规则，保障个人对其个人信息处理知情权和决定权。

#### 3. 个人信息处理责任落实

个人信息处理者应当根据个人信息的处理目的、处理方式、个人信息的种类以及对个人权益的影响、可能存在的安全风险等，采取下列措施确保个人信息处理活动符合法律、行政法规的规定，并防止未经授权的访问以及个人信息泄漏、篡改、丢失；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。

个人信息保护法中对个人信息处理者的义务有详尽的要求。违反相关条目的要求将受到责令改正，没收违法所得，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以及直接进行罚款等各类处罚，因此个人信息合规工作面临监管层面的压力巨大，需要从以下几点进行落实：

**第一、合法处理个人信息。**在《个人信息保护法》中，明确了个人信息处理的七项合法依据，除“同意”外，企业或组织可以通过履约、履责等合法依据对个人信息进行处理。对企业或组织来说，应特别注意避免将个人信息主体置于“被动”或“无感知”的情形，慎重使用“为履行个人作为一方当事人的合同”作为合法依据的情形。在明确告知、清晰告知和全面告知的基础上，充分取得个人信息主体的同意，从严要求企业或组织的内部业务，切实落实“能不用就不用，能少用就少用”个人信息的原则最小化使用个人信信息，切实落实《常见类型移动互联网应用程序必要个人信息范围规定》中关于39类App必要个人信息范围规定要求。

**第二、确定委托的第三方责任，加强风险评估。**GB/T 35273-2020《信息安全技术 个人信息安全规范》中个人信息的委托处理、共享、转让、公开披露中要求“受委托者应严格按照个人信息控制者的要求处理个人信息。受委托者因特殊原因未按照个人信息控制者的要求处理个人信息的，应及时向个人信息控制者反馈”、“个人信息控制者共享、转让个人信息时，应充分重视风险”。业务委托合同中应与受托人约定处理目的、期限、处理方式、信息种类、保护措施以及双方的权利与义务。同时企业或组织有责任对受托人的个人信息处理活动进行监督，确保受托人处理行为依照合同约束开展。监督行为可通过对受托人的现场审查、发放评估问卷等形式定期开展，同时保留记录存档。接受委托处理个人信息的受托人，应当履行个保法规定的相关义务，同时有义务协助个人信息处理者履行个保法的要求。

**第三、加强敏感个人信息保护。**在了解涉及处理的个人信息类型的基础上，应区分其中的敏感个人信息类型，制定企业或组织内部的分类分级标准，并采取更高水平的技术措施（脱敏、防泄漏、访问控制等）予以保护。针对未满十四周岁的未成年人信息，企业或组织应在产品/服务端设计青少年模式，通过家长身份验证等方式确保个人信息处理合规，并制定专门的个人信息处理规则予以公示。

**第四、满足个人信息出境要求**，企业或组织涉及个人信息出境时，应遵循“境内存储”原则，确有必要向境外提供个人信息的，应事先进行个人信息保护影响评估，明确个人信息出境的合法依据。在国家网信办关于《网络数据安全管理条例（征求意见稿）》公开征求意见的通知中提到：“关键信息基础设施运营者和处理一百万人以上个人信息的数据处理者向境外提供个人信息”，企业或组织应当通过国家网信部门组织的数据出境安全评估，同时处理者向境外提供数据应当履行“存留相关日志记录和数据出境审批记录三年以上”的义务。

#### 4. 个人信息主体权利保障

《个人信息保护法》提到，个人对其个人信息的处理享有知情权、决定权，有权限制或者拒绝他人对其个人信息进行处理；个人有权向个人信息处理者查阅、复制其个人信息；个人发现其个人信息不准确或者不完整的，有权请求个人信息处理者更正、补充；人有权请求删除；个人有权要求个人信息处理者对其个人信息处理规则进行解释说明等七大项权利。企业或组织应建立多样化的请求接收方式、响应处理流程、响应时限要求以及技术手段予以支持，确保个人信息主体可以随时行使自己的权益（如∶访问权、纠正权、拒绝权、限制处理权及可携带权等），并可以在指定响应期间内予以满足。另一方面，为实现处理来源于真实个人信息主体的请求，应具备强有效的身份校验机制，以对个人信息主体的身份进行准确识别，以确保可以及时并准确的实现个人信息主体所提请求。整体而言更强调个人在信息的收集、处理、利用、保管、传播等行为的权利，对个人权利的保护远远超出了传统隐私权的范围。

### 技术辅助企业或组织个人信息保护合规落地

在个人信息收集、存储、使用、加工、传输、提供、公开等流程中，需要将管理制度落实到每个具体的活动，同时确保管理制度落实的效果。在不同的环节里需要特定的技术手段进行辅助，提升合规管理的效果。在企业或组织内部，这些流程又可以根据研发、测试、运维、法务等参与角色的不同，分为产品设计、研发、发布、运营等阶段，每个阶段应进行相应的过程管理。

**在设计阶段，**在个人信息收集前端工具的设计过程中，可采用PbD的设计原则进行产品设计及实施策略的制定。

**在研发过程中**，可通过合规培训、SDK准入审核、合规评估等策略进行研发过程管理，避免由于研发人员对合规要求不了解、第三方SDK自身风险等造成合规隐患。

**在发布阶段，**通过技术手段进行整体的合规评估。如针对App强制授权、过度索权、超范围收集个人信息等典型问题，企业或组织可以先尝试从第三方的视角对App合规状态进行快速摸底，通过对App违规收集隐私数据的行为进行检测，包括权限声明、第三方SDK收集信息、App各功能模块实际获取的个人信息等，对企业或组织个人信息保护水平的合规性、有效性、完整性进行测试及验证。

**在运营阶段，**通过安全防护技术、访问控制策略、风险评估、应急处置预案等方式进行存储、使用、加工等流程中的管理及保障工作。

除管理流程外，企业或组织还要将个人信息保护真正融入到日常的业务和产品中，才能让个人信息保护不再流于表面，随着监管执法力度的加强，企业或组织在管理体系建设方面的完备性和有效性验证，需要管理和技术手段并行，并且嵌入到企业或组织系统及业务开展过程中，从根本上建立健全个人信息保护管理体系，为数据价值的发挥助力。

## 个人信息保护建设实践方法

### 识别监管要求建立企业或组织合规体系

首先，企业或组织应充分理解监管要求。2021年11月1日起，《个人信息保护法》正式颁布实施，标志着我国个人信息保护立法体系进入新的阶段。《个人信息保护法》的出台为个人信息权益保护、信息处理者的义务以及主管机关的职权范围提供了全面的、体系化的法律依据，涵盖个人信息收集、存储、使用、加工、传输、提供、公开、删除等多个环节以及自动化决策、个人信息、跨境提供等特定场景，与《民法典》《网络安全法》《数据安全法》等共同构成了我国个人信息保护的法律框架。5月，国家网信办等四部委联合制定的《常见类型移动互联网应用程序必要个人信息范围规定》正式实施，明确App不得强制收集非必要个人信息。11月，国家网信办会同相关部门研究起草的《网络数据安全管理条例》公开征求意见，其中“个人信息保护”章节详细规定了知情同意、最小必要、权利保障、生物特征信息等方面的要求，并明确提出处理一百万人以上个人信息应视为重要数据处理者进行管理。

现有法律法规和标准规范已提出了较为系统全面的个人信息保护要求。企业或组织处理个人信息的过程包括收集、存储、使用、加工、传输、提供、公开、销毁等每个生命周期过程中充分考虑合规制度的建设及落实。企业或组织收集个人信息的主要工具包括App、小程序、网站等，在构建这些收集工具的时候，应当在设计、开发、运维等阶段将合规活动嵌入进去，如App强制要求用户打开非必要权限问题、App超范围收集个人信息的问题、知情同意前收集个人信息或频繁、误导收集个人信息等问题、隐私政策不合规问题、收集敏感个人信息未进行明示问题、SDK越权收集问题等。企业或组织需要对自身的个人信息保护成熟度和个人信息现状进行识别，并在产品或服务功能设计阶段进行个人信息收集使用相关的合规评审活动，并充分考虑到第三方SDK准入审核要求，提升整体个人信息保护工作落地的质量和有效性。

随着监管机构对合规问题越来越重视，未来会有更多的个人信息处理服务会被纳入监管的检测、通报和下架的范围之中，如何在业务持续不断开拓创新与为用户提供更好更安全更尊重的个人信息保护体验之间，建立有力的可落地完备的个人信息保护管理体系是当前合规的主要目标，通常，建设企业或组织的个人信息保护管理体系首先应建立个人信息保护管理组织，组织由企业或组织高层管理者牵头，安全团队、业务团队、法务合规团队共同组成。该组织的工作职责包括但不限于：制定个人信息保护战略，统筹企业或组织不同部门的个人信息保护工作重心、工作方法和计划，与业务发展进行平衡，并协调公司的安全、IT、产品线、测试线、法务等多个部门才可体系化的完善公司个人信息保护合规方案，避免公司运营过程中的个人信息保护合规风险。

### 嵌入全流程的个人信息合规管理

在个人信息收集、存储、使用、加工、传输、提供、公开等流程中，需要将管理制度落实到每个具体的活动，同时确保管理制度落实的效果。在不同的环节里需要特定的技术手段进行辅助，提升合规管理的效果。在企业或组织内部，这些流程又可以根据研发、测试、运维、法务等参与角色的不同，分为产品设计、研发、发布、运营等阶段，每个阶段应进行相应的过程管理。

在个人信息收集前端工具的设计过程中，可采用PbD的设计原则进行产品设计及实施策略的制定。在研发过程中，可通过合规培训、SDK准入审核、合规评估等策略进行研发过程管理，避免由于研发人员对合规要求不了解、第三方SDK自身风险等造成合规隐患。在发布阶段通过技术手段进行整体的合规评估，根据风险容忍能力进行执行上架发布动作，并建立风险清单。在运营阶段通过安全防护技术、访问控制策略、风险评估、应急处置预案等方式进行存储、使用、加工等流程中的管理及保障工作。

### 个人信息前端收集工具合规评估

企业或组织内部在做合规的过程中，由于多角色跨部门协作，多学科交叉协作，在协作过程中可能存在信息传递的误差，所以仅仅依靠制度要求，很难保证合规实施的质量。技术辅助能在合规过程中对客观信息进行描述，进而对各方反馈的信息进行审核和校准，帮助合规团队对实质风险进行发现。同时技术手段辅助能够让实施流程标准化，提高合规工作效率和质量。以App合规为例，合规要求内容多且覆盖面较广，大多数的合规内容依靠人工分析会消耗大量的时间和精力，如第三方SDK违规收集，如果依靠研发人员对嵌入的第三方SDK进行识别和分析，那么可能会由于SDK嵌套、对SDK行为不了解等原因造成信息反馈不准确。另外用户同意前收集、后台静默收集、高频收集等违规问题的发现，也需要技术手段辅助检查才能准确发现。

在合规问题发现和整改的过程中，不同角色关注的信息又有所区别，法务人员关注的是带来的法律风险，产品设计人员关注的是对产品本身的影响，研发人员则更关注的问题是具体代码位置及整改带来的额外成本。因此，技术辅助工具必须能同时为不同的角色提供辅助，让合规工作参与的多方能有一个共同协作的平台。在检测评估工作的实施过程中，通常会为了追求效率使用自动化检测技术进行辅助，但由于自动化技术本身的限制，在具体功能场景下收集的个人信息内容往往无法通过自动化技术进行覆盖，如下单、支付、客服、注销账号等。过度追求自动化会让部分隐私行为被忽略，从而在合规检测评估的过程中造成漏报的风险。这种情况下，需要检测实施的人员进行功能的逐一验证，是否出现违反合规要求的情况出现。

相比于应用上架发行后发现合规问题，在设计研发阶段提前发现合规问题能极大地降低合规风险带来的成本。这里需要结合企业或组织的DevOps平台，为产品研发测试过程进行赋能。嵌入研发流程的关键过程之一是：在版本迭代过程中，持续进行技术检测，排查合规风险。根据App版本规划及迭代开发进度要求，可在软件版本提测时同步进行收集使用个人信息合规风险检测排查。通常该阶段需要合规专员介入进行技术检测及合规评估工作，在实践过程中发现，此过程中的功能测试工作与Q&A有着一定的共同之处，所以在部分合规场景下，企业或组织也可以Q&A承担一部分合规检查的工作，将检查结果反馈给研发、产品、法务等角色。在这个阶段通常产品的功能还并不完善，部分合规场景的检测评估尚不具备实施条件，企业或组织可对关键的检测场景使用自动化/半自动化的检测。常规的自动化检测技术在检测覆盖率上会存在一定的缺失，需要介入一定的人工操作进行辅助，这样才能比较全面的排查合规风险。

### 个人信息使用过程中的风险管控

**个人信息最小化与匿名化：**企业或组织在收集和使用个人信息时应遵循最小必要原则， 在功能可实现的前提下应在最小范围内收集使用个人信息。最小必要原则要求在个人信息收集阶段应符合功能所需的最小必要范围，在存储阶段应符合最小的存储期限要求，在流转使用过程中应限定个人信息流通的内容和范围。在个人信息流转使用过程中，企业或组织可通过使用如联邦学习、差分隐私等个人信息保护计算技术来降低个人信息处理过程中的风险。

**个人信息分类分级处理：**综合考虑个人信息属性、特点、数量、质量、格式、重要性、敏感程度以及违规使用、信息泄漏后对个人造成的影响等因素，建议将个人信息进行分类分级处理，针对不同类型、不同级别的个人信息内容，采用不同的保护机制，以降低个人信息安全风险的发生。个人信息分类分级相关的标准目前尚未出台，企业或组织可结合一般个人信息、个人敏感信息的定义，以及企业或组织业务的实际情况进行内部的分类分级处理。针对高敏感级别的个人信息，建议采用高强度的安全防护技术及严格的访问控制策略，并在运营过程中持续对个人信息使用的记录进行风险评估和审计。

**个人信息安全防护：**使用前端工具收集到的个人信息在传输、存储、使用、对外提供等过程中，应增加网络安全防护措施并确保有效性。安全防护策略的制定应在传输过程中，应使用数据加密的传输方式，避免在传输链路上的信息泄漏事件发生；在接收及获取个人信息的Web API接口上，应做好鉴权、防注入、防泄漏等安全防护工作，通过API接口使用信息的监测做好安全风险发现及预警工作；在服务器的数据存储上，应使用多种防护措施确保信息的防泄漏、防篡改、防破坏等安全防护工作；在个人信息的访问过程中，应制定安全的访问控制策略，防止信息的越权访问等安全隐患发生。针对个人信息的安全防护，应定期进行安全风险评估及审计工作，对于发现的安全漏洞及时制定修复策略，确保安全防护措施的有效性。

### 建立个人信息安全事件处置机制

根据《个人信息保护法》内容要求，企业或组织内部应建立个人信息安全事件处置的紧急预案，从制度、人员、技术保障措施方面进行规划和落实。

**预案制定**：个人信息安全应急预案应从制度、流程、人员上进行保障。预案内容应包括应急团队组织架构、相关职责描述、事件发生时的沟通机制、事件影响评估方案、对应的事中处置策略、与监管单位的事件上报、安全事件告知、事后审计、总结、追责等内容。

**事前阶段**：定期（至少每年一次）组织内部相关人员进行应急响应培训和应急演练，使其掌握岗位职责和应急处置策略和规程；

**事中阶段**：记录事件内容，包括但不限于：发现事件的人员、时间、地点，涉及的个人信息及人数，发生事件的系统名称，对其他互联系统的影响，是否已联系执法机关或有关部门；评估事件可能造成的影响，并采取必要措施控制事态，消除隐患；及时与监督、管理部门保持沟通，通报或报告个人信息保护和事件处置等情况。

**事后阶段：**对个人信息安全事件进行复盘总结，发现问题原因，提升个人信息保护水平，并根据事件影响对相关人员进行追责。

### 通过个人信息安全影响评估持续改进

企业或组织应建立个人信息安全影响评估制度，定期开展个人信息安全影响评估活动，评估并处置个人信息处理活动存在的安全风险，并对评估结果进行归档留存。

个人信息安全影响评估过程需要法务、研发、运维、安全等多方参与，评估过程中可以根据各方职责制定评估基线模版，并基于客观数据进行个人信息数据识别和梳理、安全风险识别、个人权益影响分析活动。这些客观信息的收集需要从个人信息收集使用信息、访问控制策略、敏感信息访问记录、系统中存在的安全风险等方面进行梳理。

通过持续有效的个人信息安全影响评估活动，可以发现个人信息保护工作中的风险点，通过对这些风险的跟踪及修复，能够不断提升企业或组织的个人信息保护建设水平。

## 结语

面对不断加大的数据安全及个人信息保护监管力度，企业或组织如何建立健全符合企业或组织管理现状及发展需求的个人信息保护管理体系，确保个人信息使用安全合法，同时充分发挥数据对企业或组织发展的积极推动作用，已成为各行各业发展过程中的重大挑战。针对企业或组织的个人信息保护合规建设，应综合考虑企业或组织自身的特点以及其服务的行业特点，如互联网服务提供商产品的更新速率远远超过传统制造型的产品，互联网企业或组织间存在各种各样的投资与并购，这种情况需要重点关注个人信息流转过程中的管理缺失隐患。

个人信息保护合规建设工作不仅仅是编制隐私政策文件，简单修改公司产品、增加提醒和通知等内容，企业或组织还要将个人信息保护真正融入到日常的业务和产品中，才能让个人信息保护不再流于表面，随着监管执法力度的加强，企业或组织在管理体系建设方面的完备性和有效性验证，需要管理和技术手段并行，并且嵌入到企业或组织系统及业务开展过程中，从根本上建立健全个人信息保护管理体系，为数据价值的发挥助力。