2021年
APP个人信息法规标准企业红宝书

Enterprise Red Book for Apps Personal Information Regulations and Standards

安证合规集团
ANZHENG COMPLIANCE GROUP

广东北源律师事务所
GUANGDONG BEIYUAN LAW FIRM

目　录

第一篇 法律 1
中华人民共和国民法典 1
中华人民共和国网络安全法 3
中华人民共和国数据安全法 8
中华人民共和国密码法 14
中华人民共和国个人信息保护法（2021） 15
中华人民共和国消费者权益保护法（2013修正） 28
中华人民共和国未成年人保护法 29
全国人民代表大会常务委员会关于加强网络信息保护的决定 47
第二篇 行政法规 49
中华人民共和国电信条例（2016修订） 49
互联网信息服务管理办法（2011修订） 59
第三篇 地方法规 60
广东省数字经济促进条例 60
深圳经济特区数据条例 70
第四篇 规章 88
电信和互联网用户个人信息保护规定 88
儿童个人信息网络保护规定 91
汽车数据安全管理若干规定(试行) 95
第五篇 规范性文件 99
常见类型移动互联网应用程序必要个人信息范围规定 99
移动互联网应用程序个人信息保护管理暂行规定 104
关于银行业金融机构做好个人金融信息保护工作的通知 109
中国人民银行金融消费者权益保护实施办法 113

安证合规集团&北源律师事务所

个人信息和重要数据出境安全评估办法（征求意见稿）.....125
个人信息出境安全评估办法（征求意见稿）.....127
App违法违规收集使用个人信息行为认定方法.....132
关于开展纵深推进APP侵害用户权益专项整治行动的通知.....134
关于开展App违法违规收集使用个人信息专项治理的公告.....137
工业和信息化部关于开展APP侵害用户权益专项整治工作的通知.....139
第六篇 司法解释.....142
最高人民法院关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定.....142
最高人民法院、最高人民检察院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.....146
第七篇 标准等其他文件.....149
信息安全技术 个人信息安全规范（2020）.....149
信息安全技术 个人信息去标识化指南.....186
信息安全技术 个人信息安全影响评估指南.....198
信息安全技术 移动智能终端个人信息保护技术要求.....225
信息安全技术 个人信息告知同意指南.....229
个人金融信息保护技术规范.....260
移动互联网应用程序（App）收集使用个人信息自评估指南.....282

安证合规集团&北源律师事务所

第一篇 法律

中华人民共和国民法典

基本信息：	
【发布机关】全国人民代表大会	【时效性】 现行有效
【发文字号】主席令第45号	【效力级别】法律
【发布日期】2020.05.28	【实施日期】2021.01.01

中华人民共和国民法典【节选】

第一编 总则

第五章 民事权利

第一百一十条 自然人享有生命权、身体权、健康权、姓名权、肖像权、名誉权、荣誉权、隐私权、婚姻自主权等权利。

法人、非法人组织享有名称权、名誉权和荣誉权。

第一百一十一条 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。

第四编 人格权

第一章 一般规定

第九百九十九条 为公共利益实施新闻报道、舆论监督等行为的，可以合理使用民事主体的姓名、名称、肖像、个人信息等；使用不合理侵害民事主体人格权的，应当依法承担民事责任。

第一千条 行为人因侵害人格权承担消除影响、恢复名誉、赔礼道歉等民事责任的，应当与行为的具体方式和造成的影响范围相当。

行为人拒不承担前款规定的民事责任的，人民法院可以采取在报刊、网络等媒体上发布公告或者公布生效裁判文书等方式执行，产生的费用由行为人负担。

第五章 名誉权和荣誉权

第一千零三十条 民事主体与征信机构等

安证合规集团&北源律师事务所

信用信息处理者之间的关系，适用本编有关个人信息保护的规定和其他法律、行政法规的有关规定。

第六章 隐私权和个人信息保护

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。

第一千零三十三条 除法律另有规定或者权利人明确同意外，任何组织或者个人不得实施下列行为：

（一）以电话、短信、即时通讯工具、电子邮件、传单等方式侵扰他人的私人生活安宁；

（二）进入、拍摄、窥视他人的住宅、宾馆房间等私密空间；

（三）拍摄、窥视、窃听、公开他人的私密活动；

（四）拍摄、窥视他人身体的私密部位；

（五）处理他人的私密信息；

（六）以其他方式侵害他人的隐私权。

第一千零三十四条 自然人的个人信息受法律保护。

个人信息是以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人的各种信息，包括自然人的姓名、出生日期、身份证件号码、生物识别信息、住址、电话号码、电子邮箱、健康信息、行踪信息等。

个人信息中的私密信息，适用有关隐私权的规定；没有规定的，适用有关个人信息保护的规定。

第一千零三十五条 处理个人信息的，应当遵循合法、正当、必要原则，不得过度处理，并符合下列条件：

（一）征得该自然人或者其监护人同意，但是法律、行政法规另有规定的除外；

（二）公开处理信息的规则；

（三）明示处理信息的目的、方式和范围；

（四）不违反法律、行政法规的规定和双方的约定。

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、公开等。

第一千零三十六条 处理个人信息，有下列情形之一的，行为人不承担民事责任：

（一）在该自然人或者其监护人同意的范围内合理实施的行为；

（二）合理处理该自然人自行公开的或者其他已经合法公开的信息，但是该自然人明确拒绝

安证合规集团&北源律师事务所

或者处理该信息侵害其重大利益的除外；

（三）为维护公共利益或者该自然人合法权益，合理实施的其他行为。

第一千零三十七条 自然人可以依法向信息处理者查阅或者复制其个人信息；发现信息有错误的，有权提出异议并请求及时采取更正等必要措施。

自然人发现信息处理者违反法律、行政法规的规定或者双方的约定处理其个人信息的，有权请求信息处理者及时删除。

第一千零三十八条 信息处理者不得泄露或者篡改其收集、存储的个人信息；未经自然人同意，不得向他人非法提供其个人信息，但是经过加工无法识别特定个人且不能复原的除外。

信息处理者应当采取技术措施和其他必要措施，确保其收集、存储的个人信息安全，防止信息泄露、篡改、丢失；发生或者可能发生个人信息泄露、篡改、丢失的，应当及时采取补救措施，按照规定告知自然人并向有关主管部门报告。

第一千零三十九条 国家机关、承担行政职能的法定机构及其工作人员对于履行职责过程中知悉的自然人的隐私和个人信息，应当予以保密，不得泄露或者向他人非法提供。

第七编 侵权责任

第六章 医疗损害责任

第一千二百二十六条 医疗机构及其医务人员应当对患者的隐私和个人信息保密。泄露患者的隐私和个人信息，或者未经患者同意公开其病历资料的，应当承担侵权责任。

中华人民共和国网络安全法

基本信息：	
【发布机关】全国人大常委会	【时效性】 现行有效
【发文字号】主席令第53号	【效力级别】法律
【发布日期】2016.11.07	【实施日期】2017.06.01

中华人民共和国网络安全法【节选】

第一章 总则

第十二条 国家保护公民、法人和其他组织依法使用网络的权利，促进网络接入普及，提升网络服务水平，为社会提供安全、便利的网络服务，保障网络信息依法有序自由流动。

任何个人和组织使用网络应当遵守宪法法律，遵守公共秩序，尊重社会公德，不得危害网络

安证合规集团&北京律师事务所

安全，不得利用网络从事危害国家安全、荣誉和利益，煽动颠覆国家政权、推翻社会主义制度，煽动分裂国家、破坏国家统一，宣扬恐怖主义、极端主义，宣扬民族仇恨、民族歧视，传播暴力、淫秽色情信息，编造、传播虚假信息扰乱经济秩序和社会秩序，以及侵害他人名誉、隐私、知识产权和其他合法权益等活动。

第十四条 任何个人和组织有权对危害网络安全的行为向网信、电信、公安等部门举报。收到举报的部门应当及时依法作出处理；不属于本部门职责的，应当及时移送有权处理的部门。

有关部门应当对举报人的相关信息予以保密，保护举报人的合法权益。

第三章　网络运行安全

第一节　一般规定

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。网络产品、服务的提供者不得设置恶意程序；发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

网络产品、服务的提供者应当为其产品、服务持续提供安全维护；在规定或者当事人约定的期限内，不得终止提供安全维护。

网络产品、服务具有收集用户信息功能的，其提供者应当向用户明示并取得同意；涉及用户个人信息的，还应当遵守本法和有关法律、行政法规关于个人信息保护的规定。

第二十四条 网络运营者为用户办理网络接入、域名注册服务，办理固定电话、移动电话等入网手续，或者为用户提供信息发布、即时通讯等服务，在与用户签订协议或者确认提供服务时，应当要求用户提供真实身份信息。用户不提供真实身份信息的，网络运营者不得为其提供相关服务。

国家实施网络可信身份战略，支持研究开发安全、方便的电子身份认证技术，推动不同电子身份认证之间的互认。

第二节　关键信息基础设施的运行安全

第三十七条 关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。

第四章　网络信息安全

第四十条 网络运营者应当对其收集的用户信息严格保密，并建立健全用户信息保护制度。

第四十一条 网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。

安证合规集团&北源律师事务所

网络运营者不得收集与其提供的服务无关的个人信息，不得违反法律、行政法规的规定和双方的约定收集、使用个人信息，并应当依照法律、行政法规的规定和与用户的约定，处理其保存的个人信息。

第四十二条 网络运营者不得泄露、篡改、毁损其收集的个人信息；未经被收集者同意，不得向他人提供个人信息。但是，经过处理无法识别特定个人且不能复原的除外。

网络运营者应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。在发生或者可能发生个人信息泄露、毁损、丢失的情况时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

第四十三条 个人发现网络运营者违反法律、行政法规的规定或者双方的约定收集、使用其个人信息的，有权要求网络运营者删除其个人信息；发现网络运营者收集、存储的其个人信息有错误的，有权要求网络运营者予以更正。网络运营者应当采取措施予以删除或者更正。

第四十四条 任何个人和组织不得窃取或者以其他非法方式获取个人信息，不得非法出售或者非法向他人提供个人信息。

第四十五条 依法负有网络安全监督管理职责的部门及其工作人员，必须对在履行职责中知悉的个人信息、隐私和商业秘密严格保密，不得泄露、出售或者非法向他人提供。

第四十七条 网络运营者应当加强对其用户发布的信息的管理，发现法律、行政法规禁止发布或者传输的信息的，应当立即停止传输该信息，采取消除等处置措施，防止信息扩散，保存有关记录，并向有关主管部门报告。

第四十八条 任何个人和组织发送的电子信息、提供的应用软件，不得设置恶意程序，不得含有法律、行政法规禁止发布或者传输的信息。

电子信息发送服务提供者和应用软件下载服务提供者，应当履行安全管理义务，知道其用户有前款规定行为的，应当停止提供服务，采取消除等处置措施，保存有关记录，并向有关主管部门报告。

第四十九条 网络运营者应当建立网络信息安全投诉、举报制度，公布投诉、举报方式等信息，及时受理并处理有关网络信息安全的投诉和举报。

网络运营者对网信部门和有关部门依法实施的监督检查，应当予以配合。

第五十条 国家网信部门和有关部门依法履行网络信息安全监督管理职责，发现法律、行政法规禁止发布或者传输的信息的，应当要求网络运营者停止传输，采取消除等处置措施，保存有关记录；对来源于中华人民共和国境外的上述信息，应当通知有关机构采取技术措施和其他必要措施阻断传播。

安证合规集团&北源律师事务所

第六章　法律责任

第六十条 违反本法第二十二条第一款、第二款和第四十八条第一款规定，有下列行为之一的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处五万元以上五十万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款：

（一）设置恶意程序的；

（二）对其产品、服务存在的安全缺陷、漏洞等风险未立即采取补救措施，或者未按照规定及时告知用户并向有关主管部门报告的；

（三）擅自终止为其产品、服务提供安全维护的。

第六十一条 网络运营者违反本法第二十四条第一款规定，未要求用户提供真实身份信息，或者对不提供真实身份信息的用户提供相关服务的，由有关主管部门责令改正；拒不改正或者情节严重的，处五万元以上五十万元以下罚款，并可以由有关主管部门责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

第六十四条 网络运营者、网络产品或者服务的提供者违反本法第二十二条第三款、第四十一条至第四十三条规定，侵害个人信息依法得到保护的权利的，由有关主管部门责令改正，可以根据情节单处或者并处警告、没收违法所得、处违法所得一倍以上十倍以下罚款，没有违法所得的，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；情节严重的，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照。

违反本法第四十四条规定，窃取或者以其他非法方式获取、非法出售或者非法向他人提供个人信息，尚不构成犯罪的，由公安机关没收违法所得，并处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款。

第六十六条 关键信息基础设施的运营者违反本法第三十七条规定，在境外存储网络数据，或者向境外提供网络数据的，由有关主管部门责令改正，给予警告，没收违法所得，处五万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

第六十八条 网络运营者违反本法第四十七条规定，对法律、行政法规禁止发布或者传输的信息未停止传输、采取消除等处置措施、保存有关记录的，由有关主管部门责令改正，给予警告，没收违法所得；拒不改正或者情节严重的，处十万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员

安证合规集团&北源律师事务所

和其他直接责任人员处一万元以上十万元以下罚款。

电子信息发送服务提供者、应用软件下载服务提供者，不履行本法第四十八条第二款规定的安全管理义务的，依照前款规定处罚。

第六十九条 网络运营者违反本法规定，有下列行为之一的，由有关主管部门责令改正；拒不改正或者情节严重的，处五万元以上五十万元以下罚款，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：

（一）不按照有关部门的要求对法律、行政法规禁止发布或者传输的信息，采取停止传输、消除等处置措施的；

（二）拒绝、阻碍有关部门依法实施的监督检查的；

（三）拒不向公安机关、国家安全机关提供技术支持和协助的。

第七十条 发布或者传输本法第十二条第二款和其他法律、行政法规禁止发布或者传输的信息的，依照有关法律、行政法规的规定处罚。

第七十一条 有本法规定的违法行为的，依照有关法律、行政法规的规定记入信用档案，并予以公示。

第七十四条 违反本法规定，给他人造成损害的，依法承担民事责任。

违反本法规定，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。

第七章 附 则

第七十六条 本法下列用语的含义：

（一）网络，是指由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的系统。

（二）网络安全，是指通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

（三）网络运营者，是指网络的所有者、管理者和网络服务提供者。

（四）网络数据，是指通过网络收集、存储、传输、处理和产生的各种电子数据。

（五）个人信息，是指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。

安证合规集团&北源律师事务所

中华人民共和国数据安全法

基本信息:	
【发布机关】全国人大常委会	【时效性】现行有效
【发文字号】主席令84号	【效力级别】法律
【发布日期】2021.06.10	【实施日期】2021.09.01

安汇合规集团&北源律师事务所

中华人民共和国数据安全法

第一章 总 则

第一条 为了规范数据处理活动，保障数据安全，促进数据开发利用，保护个人、组织的合法权益，维护国家主权、安全和发展利益，制定本法。

第二条 在中华人民共和国境内开展数据处理活动及其安全监管，适用本法。

在中华人民共和国境外开展数据处理活动，损害中华人民共和国国家安全、公共利益或者公民、组织合法权益的，依法追究法律责任。

第三条 本法所称数据，是指任何以电子或者其他方式对信息的记录。

数据处理，包括数据的收集、存储、使用、加工、传输、提供、公开等。

数据安全，是指通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

第四条 维护数据安全，应当坚持总体国家安全观，建立健全数据安全治理体系，提高数据安全保障能力。

第五条 中央国家安全领导机构负责国家数据安全工作的决策和议事协调，研究制定、指导实施国家数据安全战略和有关重大方针政策，统筹协调国家数据安全的重大事项和重要工作，建立国家数据安全工作协调机制。

第六条 各地区、各部门对本地区、本部门工作中收集和产生的数据及数据安全负责。

工业、电信、交通、金融、自然资源、卫生健康、教育、科技等主管部门承担本行业、本领域数据安全监管职责。

公安机关、国家安全机关等依照本法和有关法律、行政法规的规定，在各自职责范围内承担数据安全监管职责。

国家网信部门依照本法和有关法律、行政法规的规定，负责统筹协调网络数据安全和相关监

管工作。

第七条 国家保护个人、组织与数据有关的权益，鼓励数据依法合理有效利用，保障数据依法有序自由流动，促进以数据为关键要素的数字经济发展。

第八条 开展数据处理活动，应当遵守法律、法规，尊重社会公德和伦理，遵守商业道德和职业道德，诚实守信，履行数据安全保护义务，承担社会责任，不得危害国家安全、公共利益，不得损害个人、组织的合法权益。

第九条 国家支持开展数据安全知识宣传普及，提高全社会的数据安全保护意识和水平，推动有关部门、行业组织、科研机构、企业、个人等共同参与数据安全保护工作，形成全社会共同维护数据安全和促进发展的良好环境。

第十条 相关行业组织按照章程，依法制定数据安全行为规范和团体标准，加强行业自律，指导会员加强数据安全保护，提高数据安全保护水平，促进行业健康发展。

第十一条 国家积极开展数据安全治理、数据开发利用等领域的国际交流与合作，参与数据安全相关国际规则和标准的制定，促进数据跨境安全、自由流动。

第十二条 任何个人、组织都有权对违反本法规定的行为向有关主管部门投诉、举报。收到投诉、举报的部门应当及时依法处理。

有关主管部门应当对投诉、举报人的相关信息予以保密，保护投诉、举报人的合法权益。

第二章 数据安全与发展

第十三条 国家统筹发展和安全，坚持以数据开发利用和产业发展促进数据安全，以数据安全保障数据开发利用和产业发展。

第十四条 国家实施大数据战略，推进数据基础设施建设，鼓励和支持数据在各行业、各领域的创新应用。

省级以上人民政府应当将数字经济发展纳入本级国民经济和社会发展规划，并根据需要制定数字经济发展规划。

第十五条 国家支持开发利用数据提升公共服务的智能化水平。提供智能化公共服务，应当充分考虑老年人、残疾人的需求，避免对老年人、残疾人的日常生活造成障碍。

第十六条 国家支持数据开发利用和数据安全技术研究，鼓励数据开发利用和数据安全等领域的技术推广和商业创新，培育、发展数据开发利用和数据安全产品、产业体系。

第十七条 国家推进数据开发利用技术和数据安全标准体系建设。国务院标准化行政主管部门和国务院有关部门根据各自的职责，组织制定并适时修订有关数据开发利用技术、产品和数据安全相关标准。国家支持企业、社会团体和教育、科研机构等参与标准制定。

安证合规集团&北源律师事务所

第十八条 国家促进数据安全检测评估、认证等服务的发展，支持数据安全检测评估、认证等专业机构依法开展服务活动。

国家支持有关部门、行业组织、企业、教育和科研机构、有关专业机构等在数据安全风险评估、防范、处置等方面开展协作。

第十九条 国家建立健全数据交易管理制度，规范数据交易行为，培育数据交易市场。

第二十条 国家支持教育、科研机构和企业等开展数据开发利用技术和数据安全相关教育和培训，采取多种方式培养数据开发利用技术和数据安全专业人才，促进人才交流。

第三章 数据安全制度

第二十一条 国家建立数据分类分级保护制度，根据数据在经济社会发展中的重要程度，以及一旦遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者个人、组织合法权益造成的危害程度，对数据实行分类分级保护。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。

关系国家安全、国民经济命脉、重要民生、重大公共利益等数据属于国家核心数据，实行更加严格的管理制度。

各地区、各部门应当按照数据分类分级保护制度，确定本地区、本部门以及相关行业、领域的重要数据具体目录，对列入目录的数据进行重点保护。

第二十二条 国家建立集中统一、高效权威的数据安全风险评估、报告、信息共享、监测预警机制。国家数据安全工作协调机制统筹协调有关部门加强数据安全风险信息的获取、分析、研判、预警工作。

第二十三条 国家建立数据安全应急处置机制。发生数据安全事件，有关主管部门应当依法启动应急预案，采取相应的应急处置措施，防止危害扩大，消除安全隐患，并及时向社会发布与公众有关的警示信息。

第二十四条 国家建立数据安全审查制度，对影响或者可能影响国家安全的数据处理活动进行国家安全审查。

依法作出的安全审查决定为最终决定。

第二十五条 国家对与维护国家安全和利益、履行国际义务相关的属于管制物项的数据依法实施出口管制。

第二十六条 任何国家或者地区在与数据和数据开发利用技术等有关的投资、贸易等方面对中华人民共和国采取歧视性的禁止、限制或者其他类似措施的，中华人民共和国可以根据实际情况对该国家或者地区对等采取措施。

安证合规集团&北源律师事务所

第四章 数据安全保护义务

第二十七条 开展数据处理活动应当依照法律、法规的规定，建立健全全流程数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，保障数据安全。利用互联网等信息网络开展数据处理活动，应当在网络安全等级保护制度的基础上，履行上述数据安全保护义务。

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。

第二十八条 开展数据处理活动以及研究开发数据新技术，应当有利于促进经济社会发展，增进人民福祉，符合社会公德和伦理。

第二十九条 开展数据处理活动应当加强风险监测，发现数据安全缺陷、漏洞等风险时，应当立即采取补救措施；发生数据安全事件时，应当立即采取处置措施，按照规定及时告知用户并向有关主管部门报告。

第三十条 重要数据的处理者应当按照规定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。

第三十一条 关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的重要数据的出境安全管理，适用《中华人民共和国网络安全法》的规定；其他数据处理者在中华人民共和国境内运营中收集和产生的重要数据的出境安全管理办法，由国家网信部门会同国务院有关部门制定。

第三十二条 任何组织、个人收集数据，应当采取合法、正当的方式，不得窃取或者以其他非法方式获取数据。

法律、行政法规对收集、使用数据的目的、范围有规定的，应当在法律、行政法规规定的目的和范围内收集、使用数据。

第三十三条 从事数据交易中介服务的机构提供服务，应当要求数据提供方说明数据来源，审核交易双方的身份，并留存审核、交易记录。

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。

第三十五条 公安机关、国家安全机关因依法维护国家安全或者侦查犯罪的需要调取数据，应当按照国家有关规定，经过严格的批准手续，依法进行，有关组织、个人应当予以配合。

第三十六条 中华人民共和国主管机关根据有关法律和中华人民共和国缔结或者参加的国际

安证合规集团&北源律师事务所

条约、协定，或者按照平等互惠原则，处理外国司法或者执法机构关于提供数据的请求。非经中华人民共和国主管机关批准，境内的组织、个人不得向外国司法或者执法机构提供存储于中华人民共和国境内的数据。

第五章 政务数据安全与开放

第三十七条 国家大力推进电子政务建设，提高政务数据的科学性、准确性、时效性，提升运用数据服务经济社会发展的能力。

第三十八条 国家机关为履行法定职责的需要收集、使用数据，应当在其履行法定职责的范围内依照法律、行政法规规定的条件和程序进行；对在履行职责中知悉的个人隐私、个人信息、商业秘密、保密商务信息等数据应当依法予以保密，不得泄露或者非法向他人提供。

第三十九条 国家机关应当依照法律、行政法规的规定，建立健全数据安全管理制度，落实数据安全保护责任，保障政务数据安全。

第四十条 国家机关委托他人建设、维护电子政务系统，存储、加工政务数据，应当经过严格的批准程序，并应当监督受托方履行相应的数据安全保护义务。受托方应当依照法律、法规的规定和合同约定履行数据安全保护义务，不得擅自留存、使用、泄露或者向他人提供政务数据。

第四十一条 国家机关应当遵循公正、公平、便民的原则，按照规定及时、准确地公开政务数据。依法不予公开的除外。

第四十二条 国家制定政务数据开放目录，构建统一规范、互联互通、安全可控的政务数据开放平台，推动政务数据开放利用。

第四十三条 法律、法规授权的具有管理公共事务职能的组织为履行法定职责开展数据处理活动，适用本章规定。

第六章 法律责任

第四十四条 有关主管部门在履行数据安全监管职责中，发现数据处理活动存在较大安全风险的，可以按照规定的权限和程序对有关组织、个人进行约谈，并要求有关组织、个人采取措施进行整改，消除隐患。

第四十五条 开展数据处理活动的组织、个人不履行本法第二十七条、第二十九条、第三十条规定的数据安全保护义务的，由有关主管部门责令改正，给予警告，可以并处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员可以处一万元以上十万元以下罚款；拒不改正或者造成大量数据泄露等严重后果的，处五十万元以上二百万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处五万元以上二十万元以下罚款。

安证合规集团&北源律师事务所

违反国家核心数据管理制度，危害国家主权、安全和发展利益的，由有关主管部门处二百万元以上一千万元以下罚款，并根据情况责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照；构成犯罪的，依法追究刑事责任。

第四十六条 违反本法第三十一条规定，向境外提供重要数据的，由有关主管部门责令改正，给予警告，可以并处十万元以上一百万元以下罚款，对直接负责的主管人员和其他直接责任人员可以处一万元以上十万元以下罚款；情节严重的，处一百万元以上一千万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，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。

第四十七条 从事数据交易中介服务的机构未履行本法第三十三条规定的义务的，由有关主管部门责令改正，没收违法所得，处违法所得一倍以上十倍以下罚款，没有违法所得或者违法所得不足十万元的，处十万元以上一百万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

第四十八条 违反本法第三十五条规定，拒不配合数据调取的，由有关主管部门责令改正，给予警告，并处五万元以上五十万元以下罚款，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。

违反本法第三十六条规定，未经主管机关批准向外国司法或者执法机构提供数据的，由有关主管部门给予警告，可以并处十万元以上一百万元以下罚款，对直接负责的主管人员和其他直接责任人员可以处一万元以上十万元以下罚款；造成严重后果的，处一百万元以上五百万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处五万元以上五十万元以下罚款。

第四十九条 国家机关不履行本法规定的数据安全保护义务的，对直接负责的主管人员和其他直接责任人员依法给予处分。

第五十条 履行数据安全监管职责的国家工作人员玩忽职守、滥用职权、徇私舞弊的，依法给予处分。

第五十一条 窃取或者以其他非法方式获取数据，开展数据处理活动排除、限制竞争，或者损害个人、组织合法权益的，依照有关法律、行政法规的规定处罚。

第五十二条 违反本法规定，给他人造成损害的，依法承担民事责任。

违反本法规定，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。

安证合规集团&北源律师事务所

第七章 附　则

第五十三条 开展涉及国家秘密的数据处理活动，适用《中华人民共和国保守国家秘密法》等法律、行政法规的规定。

在统计、档案工作中开展数据处理活动，开展涉及个人信息的数据处理活动，还应当遵守有关法律、行政法规的规定。

第五十四条 军事数据安全保护的办法，由中央军事委员会依据本法另行制定。

第五十五条 本法自2021年9月1日起施行。

中华人民共和国密码法

基本信息:	
【发布机关】全国人大常委会	【时效性】 现行有效
【发文字号】主席令第35号	【效力级别】法律
【发布日期】2019.10.26	【实施日期】2020.01.01

中华人民共和国密码法【节选】

第一章　总　　则

第十二条 任何组织或者个人不得窃取他人加密保护的信息或者非法侵入他人的密码保障系统。

任何组织或者个人不得利用密码从事危害国家安全、社会公共利益、他人合法权益等违法犯罪活动。

第三章　商用密码

第三十一条 密码管理部门和有关部门建立日常监管和随机抽查相结合的商用密码事中事后监管制度，建立统一的商用密码监督管理信息平台，推进事中事后监管与社会信用体系相衔接，强化商用密码从业单位自律和社会监督。

密码管理部门和有关部门及其工作人员不得要求商用密码从业单位和商用密码检测、认证机构向其披露源代码等密码相关专有信息，并对其在履行职责中知悉的商业秘密和个人隐私严格保密，不得泄露或者非法向他人提供。

第四章　法律责任

第三十二条 违反本法第十二条规定，窃取他人加密保护的信息，非法侵入他人的密码保障

安证合规集团&北源律师事务所

系统，或者利用密码从事危害国家安全、社会公共利益、他人合法权益等违法活动的，由有关部门依照《中华人民共和国网络安全法》和其他有关法律、行政法规的规定追究法律责任。

第四十条 密码管理部门和有关部门、单位的工作人员在密码工作中滥用职权、玩忽职守、徇私舞弊，或者泄露、非法向他人提供在履行职责中知悉的商业秘密和个人隐私的，依法给予处分。

第四十一条 违反本法规定，构成犯罪的，依法追究刑事责任；给他人造成损害的，依法承担民事责任。

中华人民共和国个人信息保护法（2021）

基本信息：	
【发布机关】全国人大常委会	【时效性】现行有效
【发文字号】--	【效力级别】法律
【发布日期】2021.08.20	【实施日期】2021.11.01

中华人民共和国个人信息保护法（2021）

第一章 总 则

第一条 为了保护个人信息权益，规范个人信息处理活动，促进个人信息合理利用，根据宪法，制定本法。

第二条 自然人的个人信息受法律保护，任何组织、个人不得侵害自然人的个人信息权益。

第三条 在中华人民共和国境内处理自然人个人信息的活动，适用本法。

在中华人民共和国境外处理中华人民共和国境内自然人个人信息的活动，有下列情形之一的，也适用本法：

（一）以向境内自然人提供产品或者服务为目的；

（二）分析、评估境内自然人的行为；

（三）法律、行政法规规定的其他情形。

第四条 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。

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。

安证合规集团&北源律师事务所

第五条　处理个人信息应当遵循合法、正当、必要和诚信原则，不得通过误导、欺诈、胁迫等方式处理个人信息。

第六条　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。

第七条　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。

第八条　处理个人信息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。

第九条　个人信息处理者应当对其个人信息处理活动负责，并采取必要措施保障所处理的个人信息的安全。

第十条　任何组织、个人不得非法收集、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；不得从事危害国家安全、公共利益的个人信息处理活动。

第十一条　国家建立健全个人信息保护制度，预防和惩治侵害个人信息权益的行为，加强个人信息保护宣传教育，推动形成政府、企业、相关社会组织、公众共同参与个人信息保护的良好环境。

第十二条　国家积极参与个人信息保护国际规则的制定，促进个人信息保护方面的国际交流与合作，推动与其他国家、地区、国际组织之间的个人信息保护规则、标准等互认。

第二章　个人信息处理规则

第一节　一般规定

第十三条　符合下列情形之一的，个人信息处理者方可处理个人信息：

（一）取得个人的同意；

（二）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；

（三）为履行法定职责或者法定义务所必需；

（四）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；

（五）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；

（六）依照本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；

（七）法律、行政法规规定的其他情形。

安证合规集团&北源律师事务所

依照本法其他有关规定，处理个人信息应当取得个人同意，但是有前款第二项至第七项规定情形的，不需取得个人同意。

第十四条　基于个人同意处理个人信息的，该同意应当由个人在充分知情的前提下自愿、明确作出。法律、行政法规规定处理个人信息应当取得个人单独同意或者书面同意的，从其规定。

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的，应当重新取得个人同意。

第十五条　基于个人同意处理个人信息的，个人有权撤回其同意。个人信息处理者应当提供便捷的撤回同意的方式。

个人撤回同意，不影响撤回前基于个人同意已进行的个人信息处理活动的效力。

第十六条　个人信息处理者不得以个人不同意处理其个人信息或者撤回同意为由，拒绝提供产品或者服务；处理个人信息属于提供产品或者服务所必需的除外。

第十七条　个人信息处理者在处理个人信息前，应当以显著方式、清晰易懂的语言真实、准确、完整地向个人告知下列事项：

（一）个人信息处理者的名称或者姓名和联系方式；

（二）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；

（三）个人行使本法规定权利的方式和程序；

（四）法律、行政法规规定应当告知的其他事项。

前款规定事项发生变更的，应当将变更部分告知个人。

个人信息处理者通过制定个人信息处理规则的方式告知第一款规定事项的，处理规则应当公开，并且便于查阅和保存。

第十八条　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。

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。

第二十条　两个以上的个人信息处理者共同决定个人信息的处理目的和处理方式的，应当约定各自的权利和义务。但是，该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本法规定的权利。

个人信息处理者共同处理个人信息，侵害个人信息权益造成损害的，应当依法承担连带责任。

第二十一条　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

安洁合规集团&北清律师事务所

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，并对受托人的个人信息处理活动进行监督。

受托人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；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。

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。

第二十二条　个人信息处理者因合并、分立、解散、被宣告破产等原因需要转移个人信息的，应当向个人告知接收方的名称或者姓名和联系方式。接收方应当继续履行个人信息处理者的义务。接收方变更原先的处理目的、处理方式的，应当依照本法规定重新取得个人同意。

第二十三条　个人信息处理者向其他个人信息处理者提供其处理的个人信息的，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，并取得个人的单独同意。接收方应当在上述处理目的、处理方式和个人信息的种类等范围内处理个人信息。接收方变更原先的处理目的、处理方式的，应当依照本法规定重新取得个人同意。

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。

通过自动化决策方式向个人进行信息推送、商业营销，应当同时提供不针对其个人特征的选项，或者向个人提供便捷的拒绝方式。

通过自动化决策方式作出对个人权益有重大影响的决定，个人有权要求个人信息处理者予以说明，并有权拒绝个人信息处理者仅通过自动化决策的方式作出决定。

第二十五条　个人信息处理者不得公开其处理的个人信息，取得个人单独同意的除外。

第二十六条　在公共场所安装图像采集、个人身份识别设备，应当为维护公共安全所必需，遵守国家有关规定，并设置显著的提示标识。所收集的个人图像、身份识别信息只能用于维护公共安全的目的，不得用于其他目的；取得个人单独同意的除外。

第二十七条　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；个人明确拒绝的除外。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，应当依照本法规定取得个人同意。

第二节　敏感个人信息的处理规则

第二十八条　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。

安汇合规集团&北京律师事务所

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，个人信息处理者方可处理敏感个人信息。

第二十九条　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。

第三十条　个人信息处理者处理敏感个人信息的，除本法第十七条第一款规定的事项外，还应当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；依照本法规定可以不向个人告知的除外。

第三十一条　个人信息处理者处理不满十四周岁未成年人个人信息的，应当取得未成年人的父母或者其他监护人的同意。

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。

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。

第三节　国家机关处理个人信息的特别规定

第三十三条　国家机关处理个人信息的活动，适用本法；本节有特别规定的，适用本节规定。

第三十四条　国家机关为履行法定职责处理个人信息，应当依照法律、行政法规规定的权限、程序进行，不得超出履行法定职责所必需的范围和限度。

第三十五条　国家机关为履行法定职责处理个人信息，应当依照本法规定履行告知义务；有本法第十八条第一款规定的情形，或者告知将妨碍国家机关履行法定职责的除外。

第三十六条　国家机关处理的个人信息应当在中华人民共和国境内存储；确需向境外提供的，应当进行安全评估。安全评估可以要求有关部门提供支持与协助。

第三十七条　法律、法规授权的具有管理公共事务职能的组织为履行法定职责处理个人信息，适用本法关于国家机关处理个人信息的规定。

第三章　个人信息跨境提供的规则

第三十八条　个人信息处理者因业务等需要，确需向中华人民共和国境外提供个人信息的，应当具备下列条件之一：

（一）依照本法第四十条的规定通过国家网信部门组织的安全评估；

（二）按照国家网信部门的规定经专业机构进行个人信息保护认证；

（三）按照国家网信部门制定的标准合同与境外接收方订立合同，约定双方的权利和义务；

（四）法律、行政法规或者国家网信部门规定的其他条件。

中华人民共和国缔结或者参加的国际条约、协定对向中华人民共和国境外提供个人信息的条

安证合规集团&北源律师事务所

件等有规定的，可以按照其规定执行。

个人信息处理者应当采取必要措施，保障境外接收方处理个人信息的活动达到本法规定的个人信息保护标准。

第三十九条　个人信息处理者向中华人民共和国境外提供个人信息的，应当向个人告知境外接收方的名称或者姓名、联系方式、处理目的、处理方式、个人信息的种类以及个人向境外接收方行使本法规定权利的方式和程序等事项，并取得个人的单独同意。

第四十条　关键信息基础设施运营者和处理个人信息达到国家网信部门规定数量的个人信息处理者，应当将在中华人民共和国境内收集和产生的个人信息存储在境内。确需向境外提供的，应当通过国家网信部门组织的安全评估；法律、行政法规和国家网信部门规定可以不进行安全评估的，从其规定。

第四十一条　中华人民共和国主管机关根据有关法律和中华人民共和国缔结或者参加的国际条约、协定，或者按照平等互惠原则，处理外国司法或者执法机构关于提供存储于境内个人信息的请求。非经中华人民共和国主管机关批准，个人信息处理者不得向外国司法或者执法机构提供存储于中华人民共和国境内的个人信息。

第四十二条　境外的组织、个人从事侵害中华人民共和国公民的个人信息权益，或者危害中华人民共和国国家安全、公共利益的个人信息处理活动的，国家网信部门可以将其列入限制或者禁止个人信息提供清单，予以公告，并采取限制或者禁止向其提供个人信息等措施。

第四十三条　任何国家或者地区在个人信息保护方面对中华人民共和国采取歧视性的禁止、限制或者其他类似措施的，中华人民共和国可以根据实际情况对该国家或者地区对等采取措施。

第四章　个人在个人信息处理活动中的权利

第四十四条　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；法律、行政法规另有规定的除外。

第四十五条　个人有权向个人信息处理者查阅、复制其个人信息；有本法第十八条第一款、第三十五条规定情形的除外。

个人请求查阅、复制其个人信息的，个人信息处理者应当及时提供。

个人请求将个人信息转移至其指定的个人信息处理者，符合国家网信部门规定条件的，个人信息处理者应当提供转移的途径。

第四十六条　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。

个人请求更正、补充其个人信息的，个人信息处理者应当对其个人信息予以核实，并及时更

安江合规集团&北源律师事务所

正、补充。

第四十七条　有下列情形之一的，个人信息处理者应当主动删除个人信息；个人信息处理者未删除的，个人有权请求删除：

（一）处理目的已实现、无法实现或者为实现处理目的不再必要；

（二）个人信息处理者停止提供产品或者服务，或者保存期限已届满；

（三）个人撤回同意；

（四）个人信息处理者违反法律、行政法规或者违反约定处理个人信息；

（五）法律、行政法规规定的其他情形。

法律、行政法规规定的保存期限未届满，或者删除个人信息从技术上难以实现的，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。

第四十八条　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。

第四十九条　自然人死亡的，其近亲属为了自身的合法、正当利益，可以对死者的相关个人信息行使本章规定的查阅、复制、更正、删除等权利；死者生前另有安排的除外。

第五十条　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。拒绝个人行使权利的请求的，应当说明理由。

个人信息处理者拒绝个人行使权利的请求的，个人可以依法向人民法院提起诉讼。

第五章　个人信息处理者的义务

第五十一条　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露、篡改、丢失：

（一）制定内部管理制度和操作规程；

（二）对个人信息实行分类管理；

（三）采取相应的加密、去标识化等安全技术措施；

（四）合理确定个人信息处理的操作权限，并定期对从业人员进行安全教育和培训；

（五）制定并组织实施个人信息安全事件应急预案；

（六）法律、行政法规规定的其他措施。

第五十二条　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。

个人信息处理者应当公开个人信息保护负责人的联系方式，并将个人信息保护负责人的姓名、联系方式等报送履行个人信息保护职责的部门。

安证合规集团&北源律师事务所

第五十三条　本法第三条第二款规定的中华人民共和国境外的个人信息处理者，应当在中华人民共和国境内设立专门机构或者指定代表，负责处理个人信息保护相关事务，并将有关机构的名称或者代表的姓名、联系方式等报送履行个人信息保护职责的部门。

第五十四条　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。

第五十五条　有下列情形之一的，个人信息处理者应当事前进行个人信息保护影响评估，并对处理情况进行记录：

（一）处理敏感个人信息；

（二）利用个人信息进行自动化决策；

（三）委托处理个人信息、向其他个人信息处理者提供个人信息、公开个人信息；

（四）向境外提供个人信息；

（五）其他对个人权益有重大影响的个人信息处理活动。

第五十六条　个人信息保护影响评估应当包括下列内容：

（一）个人信息的处理目的、处理方式等是否合法、正当、必要；

（二）对个人权益的影响及安全风险；

（三）所采取的保护措施是否合法、有效并与风险程度相适应。

个人信息保护影响评估报告和处理情况记录应当至少保存三年。

第五十七条　发生或者可能发生个人信息泄露、篡改、丢失的，个人信息处理者应当立即采取补救措施，并通知履行个人信息保护职责的部门和个人。通知应当包括下列事项：

（一）发生或者可能发生个人信息泄露、篡改、丢失的信息种类、原因和可能造成的危害；

（二）个人信息处理者采取的补救措施和个人可以采取的减轻危害的措施；

（三）个人信息处理者的联系方式。

个人信息处理者采取措施能够有效避免信息泄露、篡改、丢失造成危害的，个人信息处理者可以不通知个人；履行个人信息保护职责的部门认为可能造成危害的，有权要求个人信息处理者通知个人。

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，应当履行下列义务：

（一）按照国家规定建立健全个人信息保护合规制度体系，成立主要由外部成员组成的独立机构对个人信息保护情况进行监督；

（二）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

安证合规集团&北源律师事务所

个人信息的规范和保护个人信息的义务；

（三）对严重违反法律、行政法规处理个人信息的平台内的产品或者服务提供者，停止提供服务；

（四）定期发布个人信息保护社会责任报告，接受社会监督。

第五十九条　接受委托处理个人信息的受托人，应当依照本法和有关法律、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本法规定的义务。

第六章　履行个人信息保护职责的部门

第六十条　国家网信部门负责统筹协调个人信息保护工作和相关监督管理工作。国务院有关部门依照本法和有关法律、行政法规的规定，在各自职责范围内负责个人信息保护和监督管理工作。

县级以上地方人民政府有关部门的个人信息保护和监督管理职责，按照国家有关规定确定。

前两款规定的部门统称为履行个人信息保护职责的部门。

第六十一条　履行个人信息保护职责的部门履行下列个人信息保护职责：

（一）开展个人信息保护宣传教育，指导、监督个人信息处理者开展个人信息保护工作；

（二）接受、处理与个人信息保护有关的投诉、举报；

（三）组织对应用程序等个人信息保护情况进行测评，并公布测评结果；

（四）调查、处理违法个人信息处理活动；

（五）法律、行政法规规定的其他职责。

第六十二条　国家网信部门统筹协调有关部门依据本法推进下列个人信息保护工作：

（一）制定个人信息保护具体规则、标准；

（二）针对小型个人信息处理者、处理敏感个人信息以及人脸识别、人工智能等新技术、新应用，制定专门的个人信息保护规则、标准；

（三）支持研究开发和推广应用安全、方便的电子身份认证技术，推进网络身份认证公共服务建设；

（四）推进个人信息保护社会化服务体系建设，支持有关机构开展个人信息保护评估、认证服务；

（五）完善个人信息保护投诉、举报工作机制。

第六十三条　履行个人信息保护职责的部门履行个人信息保护职责，可以采取下列措施：

（一）询问有关当事人，调查与个人信息处理活动有关的情况；

（二）查阅、复制当事人与个人信息处理活动有关的合同、记录、账簿以及其他有关资料；

安证合规集团&北源律师事务所

（三）实施现场检查，对涉嫌违法的个人信息处理活动进行调查；

（四）检查与个人信息处理活动有关的设备、物品；对有证据证明是用于违法个人信息处理活动的设备、物品，向本部门主要负责人书面报告并经批准，可以查封或者扣押。

履行个人信息保护职责的部门依法履行职责，当事人应当予以协助、配合，不得拒绝、阻挠。

第六十四条　履行个人信息保护职责的部门在履行职责中，发现个人信息处理活动存在较大风险或者发生个人信息安全事件的，可以按照规定的权限和程序对该个人信息处理者的法定代表人或者主要负责人进行约谈，或者要求个人信息处理者委托专业机构对其个人信息处理活动进行合规审计。个人信息处理者应当按照要求采取措施，进行整改，消除隐患。

履行个人信息保护职责的部门在履行职责中，发现违法处理个人信息涉嫌犯罪的，应当及时移送公安机关依法处理。

第六十五条　任何组织、个人有权对违法个人信息处理活动向履行个人信息保护职责的部门进行投诉、举报。收到投诉、举报的部门应当依法及时处理，并将处理结果告知投诉、举报人。

履行个人信息保护职责的部门应当公布接受投诉、举报的联系方式。

第七章　法律责任

第六十六条　违反本法规定处理个人信息，或者处理个人信息未履行本法规定的个人信息保护义务的，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。

第六十七条　有本法规定的违法行为的，依照有关法律、行政法规的规定记入信用档案，并予以公示。

第六十八条　国家机关不履行本法规定的个人信息保护义务的，由其上级机关或者履行个人信息保护职责的部门责令改正；对直接负责的主管人员和其他直接责任人员依法给予处分。

履行个人信息保护职责的部门的工作人员玩忽职守、滥用职权、徇私舞弊，尚不构成犯罪的，依法给予处分。

第六十九条　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

安证合规集团&北源律师事务所

过错的，应当承担损害赔偿等侵权责任。

前款规定的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。

第七十条　个人信息处理者违反本法规定处理个人信息，侵害众多个人的权益的，人民检察院、法律规定的消费者组织和由国家网信部门确定的组织可以依法向人民法院提起诉讼。

第七十一条　违反本法规定，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。

第八章　附　　则

第七十二条　自然人因个人或者家庭事务处理个人信息的，不适用本法。

法律对各级人民政府及其有关部门组织实施的统计、档案管理活动中的个人信息处理有规定的，适用其规定。

第七十三条　本法下列用语的含义：

（一）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。

（二）自动化决策，是指通过计算机程序自动分析、评估个人的行为习惯、兴趣爱好或者经济、健康、信用状况等，并进行决策的活动。

（三）去标识化，是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。

（四）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。

第七十四条　本法自2021年11月1日起施行。

安证合规集团&北源律师事务所

中华人民共和国刑法（2020修正）

基本信息：	
【发布机关】全国人民代表大会	【时效性】 现行有效
【发文字号】-	【效力级别】法律
【发布日期】2020.12.26	【实施日期】2021.03.01

中华人民共和国刑法（2020修正）【节选】

第四章　侵犯公民人身权利、民主权利罪

第二百五十三条之一　【侵犯公民个人信息罪】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；情节特别严重的，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。

窃取或者以其他方法非法获取公民个人信息的，依照第一款的规定处罚。

单位犯前三款罪的，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，依照各该款的规定处罚。

第六章　妨害社会管理秩序罪

第一节　扰乱公共秩序罪

第二百八十五条　【非法侵入计算机信息系统罪】违反国家规定，侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统的，处三年以下有期徒刑或者拘役。

违反国家规定，侵入前款规定以外的计算机信息系统或者采用其他技术手段，获取该计算机信息系统中存储、处理或者传输的数据，或者对该计算机信息系统实施非法控制，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；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。

提供专门用于侵入、非法控制计算机信息系统的程序、工具，或者明知他人实施侵入、非法控制计算机信息系统的违法犯罪行为而为其提供程序、工具，情节严重的，依照前款的规定处罚。

单位犯前三款罪的，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，依照各该款的规定处罚。

**第二百八十六条　**【破坏计算机信息系统罪】违反国家规定，对计算机信息系统功能进行删

安证合规集团&北源律师事务所

除、修改、增加、干扰，造成计算机信息系统不能正常运行，后果严重的，处五年以下有期徒刑或者拘役；后果特别严重的，处五年以上有期徒刑。

违反国家规定，对计算机信息系统中存储、处理或者传输的数据和应用程序进行删除、修改、增加的操作，后果严重的，依照前款的规定处罚。

故意制作、传播计算机病毒等破坏性程序，影响计算机系统正常运行，后果严重的，依照第一款的规定处罚。

单位犯前三款罪的，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，依照第一款的规定处罚。

第二百八十六条之一 【拒不履行信息网络安全管理义务罪】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。 有前两款行为，同时构成其他犯罪的，依照处罚较重的规定定罪处罚。

安证合规集团&北源律师事务所

中华人民共和国消费者权益保护法（2013修正）

基本信息：	
【发布机关】全国人大常委会	【时效性】 现行有效
【发文字号】主席令第7号	【效力级别】法律
【发布日期】2013.10.25	【实施日期】2014.03.15

中华人民共和国消费者权益保护法【节选】

第二章 消费者的权利

第十四条 消费者在购买、使用商品和接受服务时，享有人格尊严、民族风俗习惯得到尊重的权利，享有个人信息依法得到保护的权利。

第三章 经营者的义务

第二十九条 经营者收集、使用消费者个人信息，应当遵循合法、正当、必要的原则，明示收集、使用信息的目的、方式和范围，并经消费者同意。经营者收集、使用消费者个人信息，应当公开其收集、使用规则，不得违反法律、法规的规定和双方的约定收集、使用信息。

经营者及其工作人员对收集的消费者个人信息必须严格保密，不得泄露、出售或者非法向他人提供。经营者应当采取技术措施和其他必要措施，确保信息安全，防止消费者个人信息泄露、丢失。在发生或者可能发生信息泄露、丢失的情况时，应当立即采取补救措施。

经营者未经消费者同意或者请求，或者消费者明确表示拒绝的，不得向其发送商业性信息。

第七章 法律责任

第五十条 经营者侵害消费者的人格尊严、侵犯消费者人身自由或者侵害消费者个人信息依法得到保护的权利的，应当停止侵害、恢复名誉、消除影响、赔礼道歉，并赔偿损失。

第五十一条 经营者有侮辱诽谤、搜查身体、侵犯人身自由等侵害消费者或者其他受害人人身权益的行为，造成严重精神损害的，受害人可以要求精神损害赔偿。

第五十六条 经营者有下列情形之一，除承担相应的民事责任外，其他有关法律、法规对处罚机关和处罚方式有规定的，依照法律、法规的规定执行；法律、法规未作规定的，由工商行政管理部门或者其他有关行政部门责令改正，可以根据情节单处或者并处警告、没收违法所得、处以违法所得一倍以上十倍以下的罚款，没有违法所得的，处以五十万元以下的罚款；情节严重的，责令停业整顿、吊销营业执照：

……

安证合规集团&北源律师事务所

（九）侵害消费者人格尊严、侵犯消费者人身自由或者侵害消费者个人信息依法得到保护的权利的；

……

经营者有前款规定情形的，除依照法律、法规规定予以处罚外，处罚机关应当记入信用档案，向社会公布。

中华人民共和国未成年人保护法

基本信息：	
【发布机关】全国人大常委会	【时效性】 现行有效
【发文字号】中华人民共和国主席令第57号	【效力级别】法律
【发布日期】2020年10月17日	【实施日期】2021年6月1日

中华人民共和国未成年人保护法(修订草案)

第一条为了保护未成年人身心健康,保障未成年人合法权益,促进未成年人德智体美劳全面发展,培养有理想、有道德、有文化、有纪律的社会主义建设者和接班人,培养担当民族复兴大任的时代新人,根据宪法,制定本法。

第二条本法所称未成年人是指未满十八周岁的公民。

对中国境内未满十八周岁的外国籍、无国籍未成年人,依照本法有关规定予以保护。

第三条未成年人享有生存权、发展权、受保护权、参与权等权利。

未成年人依法平等地享有各项权利,不因本人及其父母或者 其他监护人的民族、种族、性别、职业、宗教信仰、教育程度、财产状况、身体状况等受到歧视。

第四条 国家、社会、学校和家庭对未成年人进行理想教育、道德教育、文化教育、纪律和法治教育、国家安全教育,进行爱国主义、集体主义和中国特色社会主义的教育，提倡爱祖国、爱人民、爱劳动、爱科学、爱社会主义的公德,抵制资本主义的、封建主义的和其他腐朽思想的侵蚀,引导未成年人树立社会主义核心价值观。

第五条 保护未成年人享有的各项权益应当坚持最有利于未成年人原则。

保护未成年人工作,处理涉及未成年人事项,应当遵循下列原则:

(一)尊重未成年人人格尊严;

安证合规集团&北源律师事务所

(二)给予未成年人特殊、优先保护;

(三)适应未成年人身心发展的规律和特点;　　(四)保护与教育相结合。

第六条　保护未成年人,是国家机关、武装力量、政党、社会团体、企业事业组织、城乡基层群众性自治组织、未成年人的监护人和其他成年人的共同责任。

国家、社会、学校和家庭应当教育和帮助未成年人维护自身合法权益,增强自我保护的意识和能力。

第七条　任何组织和个人发现不利于未成年人身心健康或者侵犯未成年人合法权益的情形,都有权劝阻、制止或者向有关部门提出检举、控告。

国家机关、法律法规授权行使公权力的各类组织及法律规定的公职人员,以及密切接触未成年人行业的各类组织及其从业人员,在工作中发现未成年人身心健康受到侵害或者面临其他危险情形,应当立即向有关部门报告。

有关部门接到涉及未成年人的报案、投诉、检举、控告或者报告,应当依法及时受理、处置,并以适当方式告知相关人员和机构处理结果。

第八条 父母或者其他监护人对未成年人承担监护职责。

未成年人的父母或者其他监护人不能履行监护责任、严重侵害未成年人合法权益或者未成年人没有其他合法监护人的,由国家承担监护职责。

第九条　中央和地方各级国家机关应当在各自的职责范围内做好未成年人保护工作。

第十条　共产主义青年团、妇女联合会、工会、残疾人联合会、关心下一代工作委员会、青年联合会、学生联合会、少年先锋队以及其他有关社会团体,协助各级国家机关做好未成年人保护工作,维护未成年人合法权益。

第十一条　国家支持建设未成年人保护相关学科、设置相关专业,开展相关科学研究、人才培养等工作。

国家建立健全未成年人统计调查制度,开展未成年人状况统计、调查和分析。

第十二条国家对保护未成年人有显著成绩的组织和个人, 给予表彰和奖励。

第二章家庭保护

第十三条父母或者其他监护人应当创造良好、和睦的家庭环境,依法履行对未成年人的监护职责。

共同生活的其他成年家庭成员应当协助未成年人的父母或者其他监护人履行监护职责。

安徽合规集团&北源律师事务所

第十四条父母或者其他监护人应当履行下列监护职责:

(一)为未成年人提供衣食住行、医疗保健等方面的生活照顾;

(二)关注未成年人的生理、心理状况和情感需求;

(三)教育、引导未成年人养成良好的思想品德和行为习惯,

预防和制止未成年人不良行为,并进行合理管教;

(四)对未成年人进行安全教育,提供必要的安全保障设施, 预防、避免伤害和侵害的发生,当伤害、侵害发生时,应当及时制止和救助;

(五)尊重未成年人受教育权利,保障适龄未成年人依法接受并完成义务教育;

(六)保障未成年人的休息、娱乐和体育锻炼时间,引导未成年人进行有益身心健康的活动;

(七)妥善管理未成年人的财产;

(八)对于超出未成年人民事行为能力范围的事项,依法代表未成年人作出决定,进行民事行为的代理、同意、追认及诉讼的代理等;

(九)其他应当履行的监护职责。

第十五条父母或者其他监护人不得实施下列行为:

(一)虐待、遗弃未成年人或者对未成年人实施家庭暴力等人身伤害;

(二)胁迫、诱骗、利用未成年人乞讨;

(三)放任、教唆、利用未成年人实施违法犯罪行为;

(四)放任或者唆使未成年人吸烟、酗酒、流浪等不良行为;

(五)(放任或者唆使未成年人参与迷信活动或者接受宗教极端思想等侵害;

(六)放任或者迫使应当接受义务教育的未成年人失学、辍学;

(七)放任未成年人过度使用电子产品或者沉迷网络,放任

未成年人接触违法或者可能影响其身心健康的网络信息、音像制品、电子出版物和读物等;

(八)放任未成年人进入营业性娱乐场所、互联网上网服务营业场所等不适宜未成年人活动的场所;

(九)允许或者迫使未满十六周岁未成年人从事法律法规特别规定以外的劳动;

(十)允许或者迫使未成年人结婚或者为未成年人订立婚约;　(十一)违法处置、侵吞未成年人的财产;

(十二)其他侵害未成年人身心健康、财产权益或者怠于履行法律法规规定的未成年人保障义务的行为。

第十六条　父母或者其他监护人不得使未满八周岁或者由于心理、生理原因需要特别照顾的

安证合规集团&北源律师事务所

未成年人处于无人看护状态,或者将其交由无民事行为能力、限制民事行为能力、患有法定传染性疾病等不适当人员代为看护。

父母或者其他监护人不得使未满十六周岁未成年人脱离监护单独生活。

第十七条 父母或者其他监护人应当学习家庭教育知识,接受家庭教育指导,正确履行监护职责,抚养教育未成年人。

第十八条 父母或者其他监护人应当根据未成年人的年龄和智力发展状况,在作出与未成年人权益有关的决定时告知其本人,并听取其意见。

第十九条 父母或者其他监护人发现未成年人权益受到侵害或者疑似受到侵害的,应当及时了解情况;情节严重的,应当立即向公安机关报告。

第二十条 父母或者其他监护人因外出务工或者其他原因不能完全履行对未成年人监护职责的,应当委托有监护能力的其他成年人代为照护。

委托照护应当充分考虑被委托人的道德品质、家庭环境、经济和身心状况、与未成年人在生活和情感上的联系等情况。禁止委托具有下列情形之一的人员作为被委托人:

(一)曾实施过性侵害或者严重暴力伤害行为的;

(二)曾长期忽视未成年人照管需求,拒不履行照管责任的;

(三)有吸毒、酗酒、赌博等严重不良习性或者多次违法行为的;

(四)被禁止从事密切接触未成年人行业相关工作的; (五)具有其他不适宜担任被委托人情形的。

第二十一条 父母或者其他监护人委托照护的,应当将委托照护情况书面告知未成年人所在学校和实际居住地的居民委员会、村民委员会,并与未成年人和被委托人保持联系与交流,了解未成年人的生活、学习情况,并给予相应指导。

委托照护的父母或者其他监护人在收到被委托人、居民委员会、村民委员会、学校等机构或者人员关于未成年人的心理、行为异常的通知时,应当及时采取有效措施。

第二十二条 父母处理离婚事务时,应当妥善协商涉及未成年子女的抚养、教育、探望、财产等事宜,听取有表达意愿能力未成年人的合理意见。

父母离婚后,不直接抚养未成年子女的一方应当依协议约定、人民法院确定或者直接抚养人同意的时间和方式探望未成年子女,直接抚养的一方应当配合,但被人民法院裁判中止探望权的除外。

第三章学校保护

安证合规集团&北源律师事务所

第二十三条 学校应当全面贯彻国家教育方针,实施素质教育,提高教育质量,注重培养未成年学生独立思考能力、创新能力和实践能力,促进未成年学生全面发展。

学校应当建立健全学生行为规范,教育未成年学生养成遵规守纪的良好行为习惯。

第二十四条 幼儿园应当做好保育、教育工作,遵循幼儿身心发展规律,实施启蒙教育,促进幼儿在体质、智力、品德等方面和谐发展。

第二十五条 学校、幼儿园的教职员工应当尊重未成年人人格尊严,不得对未成年人实施体罚、变相体罚或者其他侮辱人格尊严的行为。

第二十六条学校应当保障未成年学生受教育权利,关心、爱护学生,对家境较贫困、身心有障碍的学生,应当提供帮助; 对行为有偏常、学习有困难的学生,应当耐心教育。不得因家庭、身体、学习能力等情况歧视学生,不得违反法律和国家规定开除、变相开除未成年学生或者限制未成年学生在校接受教育。

学校应当对尚未完成义务教育的辍学学生进行登记并劝返复学;劝返无效的,应当及时向教育行政部门书面报告。

学校应当配合政府有关部门建立因家庭或者自身原因处于困境未成年学生的信息档案,开展关爱帮扶工作。

第二十七条学校应当根据未成年学生身心发展特点,对其进行社会生活指导、心理健康辅导、安全教育和青春期教育。

第二十八条 学校应当与未成年学生的父母或者其他监护人互相配合,保障未成年学生的休息、娱乐和体育锻炼时间,合理安排其学习时间。

第二十九条学校、幼儿园应当提供必要的卫生保健条件, 协助卫生健康部门做好在校、在园未成年人的卫生保健工作。

第三十条学校、幼儿园应当建立安全管理制度,保障未成年人在校、在园期间的人身安全。

学校、幼儿园不得在危及未成年人人身安全、健康的校舍和其他设施、场所中进行教育教学活动。学校、幼儿园安排未成年人参加集会、文化娱乐、社会实践等集体活动,应当有利于未成年人的健康成长,防止发生人身安全事故。

第三十一条学校、幼儿园应当根据需要,制定应对各种灾害、传染性疾病、食品安全事故、意外伤害等突发事件的预案, 配备相应设施并定期进行必要的演练。学校、幼儿园对未成年人在校内、园内或者本校、本园组织的校外活动中发生人身伤害事故的,应当及时救护,妥善处理, 及时向有关主管部门报告并通知未成年人的父母或者其他监护人。

第三十二条 禁止学校、幼儿园指定购买或者直接推销保险产品。

安法合规集团&北源律师事务所

第三十三条　学校应当建立学生欺凌防控制度,对教职员工、学生开展防治学生欺凌的培训和教育。

学校对学生欺凌行为应当及时制止和处理,并通知被欺凌和实施欺凌行为的未成年学生的父母或者其他监护人;对相关未成年学生,应当给予及时的心理辅导和教育引导;对相关未成年学生的父母或者其他监护人,应当给予必要的家庭教育指导。

学校应当配合有关部门,根据欺凌行为性质和严重程度,依法对实施欺凌行为的未成年学生予以教育、矫治或者处罚。

第三十四条学校、幼儿园应当加强对教职员工的教育和管理,预防对未成年学生实施性侵害等违法犯罪行为的发生。

学校、幼儿园应当对未成年人开展适合其年龄的性健康教育,提高未成年人防范性侵害的自我保护意识和能力。

第三十五条对于在学校接受教育的有严重不良行为的未成年学生,学校与其父母或者其他监护人应当互相配合加以管教; 无力管教或者管教无效的,可以依法将其送专门学校继续接受教育。

专门学校实行寄宿制。学生的学籍保留在原学校,符合毕业条件的,由原学校颁发毕业证书。

专门学校在课程设置上应当与普通学校相同,并根据未成年人身心发展特点开展教育矫治。

家庭、学校、社会应当关心、爱护在专门学校就读的未成年学生,尊重其人格尊严,不得虐待和歧视。

第三十六条　婴幼儿照护服务机构、校外教育培训机构、校外托管机构等应当参照本章有关规定,根据不同年龄未成年人的成长特点和规律,做好未成年人安全保障工作。

第四章社会保护

第三十七条全社会应当树立尊重、保护、教育未成年人的良好风尚,关心、爱护未成年人。

国家鼓励、支持和引导社会团体、企业事业组织以及其他组织和个人,开展有利于未成年人健康成长的社会活动与服务。

第三十八条 居民委员会、村民委员会应当协助政府有关部门,宣传未成年人保护方面的法律法规,指导、监督家庭依法履行监护职责,建立因家庭或者自身原因处于困境未成年人的信息和帮扶档案。

居民委员会、村民委员会应当协助政府有关部门监督委托照护情况,发现被委托人缺乏照护能力、不能有效履行照护职责等情况,应当及时通知未成年人的父母或者其他监护人,由其要求被委托人履行照护职责或者委托其他有照护能力的成年人代为照护。

安证合规集团&北源律师事务所

第三十九条爱国主义教育基地、图书馆、青少年宫、儿童活动中心应当对未成年人免费开放;博物馆、纪念馆、科技馆、展览馆、美术馆、文化馆、社区公益性互联网上网服务场所以及 影剧院、体育场馆、动物园、公园等场所,应当按照有关规定对 未成年人免费或者优惠开放。

国家鼓励爱国主义教育基地、博物馆、科技馆、美术馆等公共场馆开设未成年人专场,为未成年人提供有针对性的服务。

国家鼓励国家机关、企业事业组织、部队等开发自身优质教育资源,设立针对未成年人的开放日,为未成年人主题教育、社会实践、职业体验等提供支持。

第四十条　城市公共交通以及公路、铁路、水路、航空客运等应当按照有关规定对未成年人实施免费或者优惠票价。

第四十一条 大型的公共场所、公共交通工具、旅游景区景点等应当按照国家有关规定设置母婴室、婴儿护理台以及方便幼童使用的坐便器、洗手台等卫生设施,为未成年人提供便利。

第四十二条任何组织或者个人不得以年龄以外的其他理由,限制未成年人按照有关规定应当享有的照顾或者优惠。

第四十三条　国家鼓励新闻出版、电影、广播电视、网络信息服务、文艺等单位和作家、艺术家、科学家以及其他公民,加强对未成年人保护工作的宣传,创作、出版、制作和传播有利于未成年人健康成长的图书、报刊、影视节目、音像制品、网络信息和电子出版物等。

国家鼓励科研机构和科技团体对未成年人开展科学知识普及活动。

第四十四条　禁止任何组织或者个人向未成年人提供含有淫秽、色情、暴力、邪教、迷信、凶杀、恐怖、赌博、涉毒等危害未成年人身心健康内容的图书、报刊、影视节目、音像制品、网络信息和电子出版物等。

任何组织和个人出版、播出、放映的图书、报刊、影视节目、音像制品和电子出版物等文化产品包含可能影响未成年人身心健康内容的,应当以显著方式进行分类提示。

第四十五条　任何组织或者个人不得刊登、播放、张贴或者散发含有危害未成年人身心健康内容的广告。

禁止在中小学校播放、张贴或者散发商业广告。

第四十六条禁止制作、复制、发布、传播或者持有有关未成年人的淫秽色情信息。

第四十七条禁止拐卖、绑架、虐待未成年人,禁止对未成年人实施性侵害。

禁止胁迫、诱骗、利用未成年人乞讨或者组织未成年人进行有害其身心健康的表演等活动。

第四十八条 生产、销售用于未成年人的食品、药品、玩具、用具和游戏游艺设备、游乐设施等,应当符合国家标准或者行业标准,不得有害于未成年人的安全和健康;需要标明注意事项的,应

安证合规集团&北源律师事务所

当在显著位置标明。

第四十九条 未成年人集中活动的公共场所应当符合国家或者行业安全标准,采取相应安全保护措施,对可能危及未成年人人身安全的设施,应当定期进行维护,在显著位置设置安全警示标志并标明适应年龄范围或者注意事项。必要时,应当设置专门人员看守。

大型的商场、超市、医院、图书馆、博物馆、科技馆、游乐场、车站、旅游景区景点等场所应当设置搜寻走失未成年人的安全警报系统。场所运营单位接到警报系统警示或者未成年人走失求助后,应当立即组织人员进行搜寻并向公安机关报告。

第五十条 中小学校园周边不得设置营业性娱乐场所、互联网上网服务营业场所等不适宜未成年人活动的场所。

营业性歌舞娱乐场所、互联网上网服务营业场所等不适宜未成年人活动的场所,不得允许未成年人进入;游艺娱乐场所设置的电子游戏机,除国家法定节假日外,不得向未成年人提供。经营者应当在显著位置设置未成年人禁入、限入标志;对难以判明是否已成年的,应当要求其出示身份证件。

第五十一条 禁止向未成年人出售烟酒、销售彩票或者兑付彩票奖金。烟酒经营者和彩票销售机构、彩票代销者应当在显著位置设置不向未成年人出售烟酒或者彩票的标志;对难以判明是否已成年的,应当要求其出示身份证件。

任何人不得在中小学校、幼儿园的教室、寝室、活动室和其他未成年人集中活动的场所吸烟、饮酒。

第五十二条 禁止向未成年人提供、出售管制刀具或者其他可能致人严重伤害的器具、器械和物品。相关经营者对购买者难以判明是否已成年的,应当要求其出示身份证件。

第五十三条任何组织或者个人不得招用未满十六周岁未成年人,国家另有规定的除外。

任何组织或者个人招用未成年人的,应当执行国家在工种、劳动时间、劳动强度和保护措施等方面的规定,不得安排其从事 过重、有毒、有害等危害未成年人身心健康的劳动或者危险作业。

经未成年人的父母或者其他监护人同意,未成年人参与演出、节目制作、网络直播等活动,活动组织方应当根据国家有关规定,保障未成年人合法权益。

第五十四条 招聘密切接触未成年人行业的从业人员时,用人单位应当向公安机关查询应聘者是否具有性侵害、虐待、暴力伤害等严重侵害未成年人的违法犯罪记录;查询发现其具有前述行为记录的,不得录用。密切接触未成年人行业的各类组织应当定期对本单位在职人员是否具有性侵害、虐待、暴力伤害等严重侵害未成年人的违法犯罪记录进行核查;查询发现其具有前述行为记录的,禁止其继续从业。

第五十五条任何组织或者个人不得披露未成年人个人隐私。对未成年人的信件、日记、电子

安证合规集团&北京律师事务所

邮件、网络通讯内容,任何组织或者个人不得隐匿、毁弃、删除;除因追查犯罪需要,由公安机关或者人民检察院依法进行检查,或者对无民事行为能力未成年人的信件、日记、电子邮件、网络通讯内容由其父母或者其他监护人代为开拆、查阅外,任何组织或者个人不得开拆、查阅。

第五十六条公共场所和学校、幼儿园等未成年人集中的场所发生突发事件时,应当优先救护未成年人。

第五章网络保护

第五十七条国家保护未成年人依法使用网络的权利,保障和引导未成年人安全、合理使用网络。

第五十八条家庭和学校应当培养和提高未成年人网络素养,开展网络安全和网络文明教育,提高未成年人安全、合理使用网络的意识和能力,增强未成年人自我保护意识。

第五十九条国家鼓励和支持有利于未成年人健康成长的网络内容的创作与传播,鼓励和支持专门以未成年人为服务对象、适合未成年人身心发展特点的网络技术、设备、产品、服务的研 发、生产和使用。

第六十条网络产品和服务提供者以及智能终端产品制造者和销售者,应当依法履行未成年人网络保护义务。

第六十一条　学校、社区、图书馆、文化馆、青少年官等场所为未成年人提供的公益性互联网上网服务设施,应当安装未成年人上网保护软件。

智能终端产品制造者和销售者应当在智能终端产品上安装未成年人上网保护软件,或者采用显著方式告知用户安装未成年人上网保护软件情况以及安装渠道和方法。

第六十二条　任何组织和个人不得利用网络制作、复制、发布、传播含有淫秽、色情、暴力、邪教、迷信、凶杀、恐怖、赌博、涉毒等法律、行政法规禁止内容的信息。

网络产品和服务含有可能影响未成年人身心健康信息的,制作、复制、发布、传播该信息的组织和个人应当在信息展示前按照国家有关规定予以提示。

第六十三条　网络产品和服务提供者应当提示未成年人保护其个人信息,并对未成年用户使用其个人信息进行保护性限制。

网络产品和服务提供者通过网络收集、使用、保存未成年人个人信息的,应当符合国家有关规定,且经过未成年人及其父母或者其他监护人同意。

第六十四条　网络产品和服务提供者应当避免提供可能诱导未成年人沉迷的内容。网络产品和服务提供者应当设置相应的时间管理、权限管理、消费管理等功能,为父母或者其他监护人预防和干预未成年人沉迷网络提供便利。

安证合规集团&北源律师事务所

家庭、学校以及有关社会组织应当相互配合,预防和干预未成年人沉迷网络。

第六十五条对未成年人使用网络游戏实行时间管理,具体办法由国务院规定。

网络游戏服务提供者应当按照国家有关规定和标准,对游戏产品进行分类,作出提示,并采取技术措施,不得让未成年人接触不适宜其接触的游戏或者游戏功能。

第六十六条　任何组织或者个人不得通过网络以文字、图片、音视频等形式侮辱、诽谤、威胁未成年人或者恶意扭曲、损害未成年人形象。

发现未成年人遭受前款网络欺凌侵害或者形象遭到恶意扭曲、损害的,受害未成年人的父母或者其他监护人可以要求网络信息服务提供者及时采取删除、屏蔽等措施,停止侵害。

第六十七条 网络产品和服务提供者应当结合本单位提供的未成年人相关服务,建立便捷的举报渠道,通过显著方式公示举报途径和举报方法,配备与服务规模相适应的专职人员,及时受理并处置相关举报。

第六章政府保护

第六十八条　国务院和地方各级人民政府领导有关部门做好未成年人保护工作;将未成年人保护工作纳入国民经济和社会发展规划以及年度计划,相关经费纳入本级政府预算。

第六十九条　国务院和县级以上地方人民政府应当建立未成年人保护工作协调机制,统筹、协调、督促、指导有关部门做好未成年人保护工作。协调机制具体工作由同级民政部门承担。

第七十条　国务院和县级以上地方人民政府涉及未成年人保护的职能部门应当明确相关内设机构或者人员,负责本部门承担的未成年人保护工作。

乡镇人民政府和街道办事处应当设立未成年人保护工作站或者指定专门人员,及时办理与未成年人相关事务;支持、指导居民委员会、村民委员会设立专人专岗,做好未成年人保护有关工作。

第七十一条 各级人民政府应当将家庭教育指导服务纳入城乡公共服务体系,开展家庭教育知识宣传,鼓励和支持有关社会团体、企业事业组织开展家庭教育服务。

第七十二条 地方各级人民政府应当提供家庭监护监督和支持,采取措施监督家庭监护状况,为有需要的家庭提供指导和帮助。

第七十三条各级人民政府应当保障未成年人受教育权利, 并采取措施保障因家庭或者自身原因处于困境的未成年人接受义 务教育。

第七十四条 地方各级人民政府应当发展托幼事业,办好婴幼儿照护服务机构、幼儿园,支持社会组织和个人依法兴办哺乳室、婴幼儿照护服务机构、幼儿园。

各级人民政府及其有关部门应当培养和培训婴幼儿照护服务机构、幼儿园的保教人员,提高其

安证合规集团&北源律师事务所

职业道德素质和业务能力。

第七十五条　各级人民政府应当发展职业教育,保障没有进入普通高中学习的未成年人接受职业教育或者职业技能培训,鼓励和支持社会团体、企业事业组织为未成年人提供职业技能培训服务。

第七十六条各级人民政府应当保障具有接受普通教育能力、能适应校园生活的残疾未成年人在普通学校、幼儿园接受教 育;保障特殊教育学校、幼儿园的办学条件,对不具有接受普通 教育能力的残疾未成年人实施学前教育、义务教育、职业教育; 鼓励和支持有条件的儿童福利机构举办特殊教育学校、幼儿园。

第七十七条专门教育是国家教育体系的重要组成部分,专门学校是实施专门教育的主要机构。

国务院组织有关部门按照科学设置、合理布局、形式多样的原则,制定专门学校发展规划,制定专门学校办学标准、管理制度和考核评价等规范。

县级以上地方人民政府根据需要设置专门学校或者与周边区域合作建设专门学校;鼓励和支持社会力量举办或者参与举办专门学校,并加强管理。

第七十八条县级以上地方人民政府及其有关部门应当保障校园安全,监督、指导学校、幼儿园等单位落实校园安全责任, 并建立突发事件的报告、处置和协调机制。

第七十九条 县级人民政府及其有关部门应当依法维护校园周边的治安和交通秩序,设立监控设备和交通安全设施,预防和制止侵害未成年人合法权益的违法犯罪行为。

第八十条　各级人民政府应当建立和改善适合未成年人需要的活动场所和设施,支持公益性未成年人活动场所和设施的建设和运行,鼓励社会力量兴办适合未成年人的活动场所,并加强管理。

各级人民政府应当采取措施,防止任何组织或者个人侵占、破坏学校、幼儿园、婴幼儿照护服务机构等未成年人活动场所的 场地、房屋和设施。

县级以上人民政府及其教育行政部门应当采取措施,鼓励和支持中小学校在节假日、寒暑假期间将文化体育设施对未成年人免费或者优惠开放。

第八十一条　各级人民政府及其有关部门应当对未成年人进行卫生保健和营养指导,提供卫生保健服务。

卫生健康部门应当做好对未成年人的疾病预防工作,对国家免疫规划项目的预防接种实行免费,实施疫苗全程信息化追溯制度;防治未成年人常见病、多发病,加强对传染病防治工作的监督管理,加强对伤害防控的指导和评估,加强对学校、幼儿园、婴幼儿照护服务机构卫生保健的指导和监督。

教育部门应当加强对未成年人的心理健康教育,建立对未成年人心理问题的早期发现和及时干预机制。卫生健康部门应当做好未成年人心理治疗、心理危机干预以及精神障碍早期识别和诊断治疗等。

安证合规集团&北源律师事务所

第八十二条各级人民政府及其有关部门对因家庭或者自身原因处于困境的未成年人实施分类保障,采取措施满足其生活、教育、医疗康复、住房等方面的基本需要。

第八十三条 各级人民政府应当采取措施,加强未成年人网络素养教育,指导中小学校和社会团体、企业事业组织、城乡基层群众性自治组织等开展提高未成年人网络素养的教育教学活动。

教育、卫生健康等部门应当组织开展预防未成年人沉迷网络的宣传教育,对未成年人沉迷网络依法实施干预。

第八十四条国家网信部门会同文化、新闻出版、电影、广播电视等主管部门根据未成年人网络保护的需要,结合未成年人 的不同年龄阶段,确定可能影响未成年人身心健康信息的种类、范围和判断标准。

第八十五条 对于符合法定情形的未成年人,由县级以上人民政府代表国家进行监护。各级民政部门承担临时或者长期监护职责,教育、卫生健康、公安等部门应当根据各自职责予以配合。

县级以上人民政府及其民政部门应当根据需要设立未成年人救助保护机构、儿童福利机构,负责收留、抚养需要国家监护的未成年人。

第八十六条 未成年人具有下列情形之一,应当由国家对其进行临时监护:

(一)监护人不履行或者因故不能履行监护职责,且短期内无法指定或者不适合委托其他人代为照护导致未成年人无人照料

的;

(二)遭受监护人严重侵害需要被紧急带离的;

(三)来历不明、暂时查找不到父母或者其他监护人的;

(四)人民法院判决中止监护人资格的;

(五)其他需要由国家进行临时监护的情形的。

对临时监护的未成年人,应当优先考虑亲属寄养;不具备条件或者不适合的,可以由未成年人救助保护机构或者儿童福利机构进行收留、抚养。

临时监护期限一般不超过一年。临时监护期满后仍无法查明或者确定监护人的,由国家进行长期监护。

第八十七条未成年人具有下列情形之一,应当由国家对其进行长期监护:

(一)父母死亡或者宣告失踪且无其他依法具有监护资格的人的;

(二)父母无监护能力且无其他依法具有监护资格的人的; (三)无法查明其父母或者其他监护人的;

(四)人民法院判决撤销监护人资格并指定由民政部门担任监护人的;

安证合规集团&北源律师事务所

(五)法律规定应当由民政部门担任监护人的。

对由国家长期监护的未成年人,可以根据有关法律规定,通过收养等方式妥善安置。对于依法收养的,民政部门应当进行收养评估。收养关系成立后,对未成年人的国家监护终止。

第八十八条县级以上地方人民政府应当开通全国统一的未成年人保护热线,及时受理、转介侵害未成年人合法权益的投诉、举报;鼓励和支持社会团体、企业事业组织参与设立未成年人保护服务平台、服务热线、服务站点,为未成年人提供咨询、帮助。

第八十九条　国务院应当建立全国统一的性侵害、虐待、暴力伤害等严重侵害未成年人违法犯罪人员信息查询系统,由公安机关向有用工需求的密切接触未成年人行业的相关组织提供查询服务。

第九十条　县级以上人民政府应当培育、引导和规范有关社会组织参与未成年人保护工作,开展家庭教育指导和未成年人心理疏导、康复救助、收养评估等社会工作和服务。

第七章司法保护

第九十一条公安机关、人民检察院、人民法院和司法行政部门应当依法履行职责,保护未成年人合法权益。

第九十二条公安机关、人民检察院、人民法院和司法行政部门应当根据需要明确专门机构或者指定专门人员,负责办理涉未成年人案件。办理涉未成年人案件的人员应当经过专门培训,熟悉未成年人身心特点。专门机构或者专门人员中,应当有女性工作人员。

公安机关、人民检察院、人民法院和司法行政部门开展未成年人司法保护工作,应当实行专门的评价考核标准。

第九十三条　公安机关、人民检察院、人民法院和司法行政部门办理涉未成年人案件,应当考虑未成年人身心特点和健康成长的需要,使用未成年人能够理解的语言和表达方式,听取未成年人及其法定代理人的意见。

第九十四条　公安机关、人民检察院、人民法院和司法行政部门办理涉未成年人案件,不得公开涉案未成年人和未成年被害人的姓名、影像、住所、就读学校以及其他可能识别出其身份的信息。

任何组织或者个人不得在新闻报道、影视节目、公开出版物、网络上公布涉案未成年人和未成年被害人的姓名、影像、住所、就读学校以及其他可能识别出其身份的信息。

第九十五条　在司法活动中对需要法律援助或者司法救助的未成年犯罪嫌疑人、被告人、被害人以及家庭经济困难的未成年当事人,法律援助机构或者人民法院、人民检察院、公安机关应当

安证合规集团&北源律师事务所

给予帮助,依法为其提供法律援助或者司法救助。

法律援助机构应当指派熟悉未成年人身心特点的律师为未成年人提供辩护或者诉讼代理。

法律援助机构和律师协会应当对办理未成年人法律援助案件的律师进行指导和培训。

第九十六条　公安机关、人民检察院、人民法院可以与未成年犯罪嫌疑人、被告人、被害人的法定代理人就案件、家庭、学习、就业等情况进行沟通,发现未成年人的父母或者其他监护人存在暴力管教、疏于照顾或其他不利于未成年人身心健康行为的,应当责令其接受家庭教育指导。

因未达法定年龄而不予行政或者刑事处罚未成年人的法定代理人,适用前款规定。

第九十七条 未成年人合法权益受到侵害后,有权代为提起诉讼或者行使相关诉讼权利的组织或者个人放弃权利或者在合理时限内怠于行使权利的,人民检察院可以代为行使诉讼权利。

对于侵犯未成年人合法权益或者行政机关违法行使、怠于行使未成年人保护职能,涉及公共利益的,人民检察院可以提起公益诉讼。

第九十八条 人民法院审理继承案件,应当依法保护未成年人的继承权和受遗赠权。

人民法院审理离婚案件,涉及未成年子女抚养问题的,应当听取有表达意愿能力的未成年子女的意见,根据保障子女权益原则和双方具体情况依法处理。

第九十九条 父母或者其他监护人不履行监护职责或者侵害被监护的未成年人合法权益,具有下列情形之一,且经教育仍不改正,人民法院可以根据有关人员或者单位的申请,中止其监护人资格,由国家进行临时监护:

(一)怠于履行监护职责导致未成年人处于危困状态的;

(二)教唆、利用未成年人实施违法犯罪行为的;

(三)胁迫、诱骗、利用未成年人乞讨的。

被中止监护人资格的父母或者其他监护人应当依法继续负担抚养费用。

第一百条监护人资格被人民法院判决中止后,父母或者其他监护人确有悔改表现的,可以向人民法院申请恢复其监护人资格。

监护人资格中止一年内,原监护人未向人民法院申请恢复其监护人资格或者其申请被驳回的,原监护人丧失监护人资格,经人民法院判决,依法另行指定监护人或者由国家进行长期监护。第一百零一条父母或者其他监护人严重侵害被监护的未成年人合法权益,具有下列情形之一,人民法院可以根据有关人员或者单位的申请,撤销其监护人资格,依法另行指定监护人或者由国家进行长期监护:

(一)性侵害、出卖、遗弃、长期虐待、严重暴力伤害未成年人的;

(二)中止的监护人资格被恢复后,再次出现符合中止监护人资格的情形的。

安法合规集团&北源律师事务所

被撤销监护人资格的父母或者其他监护人应当依法继续负担抚养费用。

第一百零二条人民法院审理涉及未成年人的离婚、抚养、收养、监护、探望等民事案件,可以委托相关社会组织对未成年 人的家庭情况进行社会调查。

第一百零三条 公安机关、人民检察院、人民法院讯问未成年犯罪嫌疑人、被告人,询问未成年被害人、证人,应当依法通知其法定代理人或者其他合适成年人到场,并注意保护未成年人个人隐私和名誉,采取适当方式,在适当场所进行。

人民法院开庭审理涉未成年人案件,未成年被害人、证人一般不出庭作证,必须出庭的,应当采取心理干预等保护措施。

第一百零四条 公安机关、人民检察院、人民法院办理未成年人遭受性侵害或者严重暴力伤害的案件时, 应当采取适当措施,避免对未成年被害人造成再次伤害。询问遭受性侵害的女性未成年被害人,应当由女性工作人员进行。

公安机关、人民检察院、人民法院可以联合政府有关部门、社会团体以及有关社会组织,对遭受性侵害或者严重暴力伤害的未成年被害人及其家庭实施必要的经济救助、心理干预、转学安置等综合保护。

第一百零五条对违法犯罪未成年人,实行教育、感化、挽救方针,坚持教育为主、惩罚为辅原则。

对违法犯罪未成年人,应当依法予以从轻、减轻或者免除处罚。

第一百零六条对于被采取刑事强制措施的未成年学生,在人民法院判决生效前,就读学校不得取消其学籍。

第一百零七条 对于具有不良行为、严重不良行为以及因未达法定年龄而不予行政或者刑事处罚的未成年人,依法适用教育矫治措施。

第一百零八条公安机关、人民检察院、人民法院对于无固定住所、无法提供保证人的未成年人适用取保候审的,应当指定 合适成年人作为保证人,必要时可以安排在适当场所实施辅导、监督、观察、矫正、保护、管束等观护帮教措施。

第一百零九条 公安机关、人民检察院、人民法院办理涉未成年人刑事案件,可以委托社区矫正机构或者有关社会组织对未成年犯罪嫌疑人、被告人的成长经历、犯罪原因、监护教育等情况进行社会调查。

根据实际需要并经未成年犯罪嫌疑人、被告人、被害人及其监护人同意,可以对未成年人进行心理测评。社会调查和心理测评可以作为办理涉未成年人刑事案件的参考。

第一百一十条 公安机关、人民检察院、人民法院和司法行政部门不得向任何单位或者个人

安证合规集团&北源律师事务所

提供被封存的未成年人犯罪记录,但司法机关为办案需要或者有关单位根据国家有关规定进行查询的除外。查询者应当遵守保密义务。

对于未成年人的行政处罚、行政强制记录和被刑事立案、采取刑事强制措施、不起诉、免除刑事处罚、不予刑事处罚、不负刑事责任、终止审理、宣告无罪以及依法适用教育矫治措施的记录,适用前款规定。

第一百一十一条 对羁押、服刑未成年人,应当与成年人分别关押、分别管理、分别教育。

羁押、服刑未成年人没有完成义务教育的,应当对其进行义务教育。

第一百一十二条 公安机关、人民检察院、人民法院和司法行政部门发现有关单位未尽到未成年人教育、管理、救助、帮助等保护职责的,应当向该单位提出建议。被建议单位应当在两个月内作出回复。

第一百一十三条 国家鼓励和支持未成年人保护、社会工作服务等社会组织,参与对涉案未成年人和未成年被害人的心理干预、法律援助、社会调查、社会观护、教育矫治、社区矫正等工作。

第八章法律责任

第一百一十四条 违反本法规定,侵害未成年人的合法权益,造成人身财产损失或者其他损害的,依法承担民事责任;构成犯罪的,依法追究刑事责任。

违反本法规定,侵害未成年人的合法权益,本法已规定行政处罚的,依照本法进行处罚;本法没有规定的,依据其他法律、法规进行行政处罚。

第一百一十五条国家机关、法律法规授权行使公权力的各类组织及法律规定的公职人员不依法履行保护未成年人合法权益 责任,或者侵害未成年人合法权益,或者对提出申诉、控告、检举的人进行打击报复的,由其所在单位或者上级机关责令改正,对直接负责的主管人员和其他直接责任人员依法给予处分。

第一百一十六条 本法第七条第二款规定的单位或者个人未履行报告义务,由上级机关、主管部门或者所在单位依法予以处分;因未及时报告而造成严重后果的,同时追究直接负责的主管人员和其他直接责任人员的责任。

第一百一十七条 父母或者其他监护人不依法履行监护职责,或者侵害未成年人合法权益的,由其所在单位或者居民委员会、村民委员会予以劝诫、制止;情节严重的,由公安机关予以训诫或者责令其接受家庭教育指导。

人民检察院在办理案件过程中,发现未成年人的父母或者其他监护人不依法履行监护职责,或

安证合规集团&北源律师事务所

者侵害未成年人合法权益的, 应当予以训诫或者责令其接受家庭教育指导。

人民法院对于未成年人的父母或者其他监护人不依法履行监护职责,或者侵害未成年人合法权益的,除应当予以训诫或者责令其接受家庭教育指导外,经有关单位或者人员的申请,可以作出下列处置:

(一)作出人身安全保护令;

(二)对于拒不履行有关行政决定的,予以强制执行;　　(三)判令中止或者撤销监护人资格。

第一百一十八条　学校、幼儿园、婴幼儿照护服务等机构侵害未成年人合法权益的,由教育、卫生健康、市场监督管理等主管部门责令改正;情节严重的,对直接负责的主管人员和其他直接责任人员依法给予处分。

学校、幼儿园、婴幼儿照护服务等机构教职员工对未成年人实施体罚、变相体罚或者其他侮辱人格行为的,由其所在单位或者主管部门责令改正;情节严重的,依法给予处分。

第一百一十九条　公共场馆和公共场所未按照有关规定对未成年人免费或者优惠开放的,由市场监督管理、文化等主管部门给予警告,责令限期改正;拒不改正的,处一万元以上十万元以下罚款。

第一百二十条　城市公共交通以及公路、铁路、水路、航空客运等未按照有关规定对未成年人实施免费或者优惠票价的,由
市场监督管理、交通等主管部门给予警告,责令限期改正;拒不改正的,处一万元以上十万元以下罚款。

第一百二十一条大型的公共场所、公共交通工具、旅游景区景点等未按照有关规定设置母婴室、婴儿护理台或者方便幼童 使用的坐便器、洗手台等卫生设施的,由市场监督管理、交通、旅游等主管部门给予警告,责令限期改正;拒不改正的,处一万元以上十万元以下罚款。

第一百二十二条 有关单位或者个人以年龄以外的其他理由,限制未成年人应当依法享有的照顾或者优惠的,由市场监督管理部门给予警告,责令限期改正;拒不改正的,处一万元以上十万元以下罚款。

第一百二十三条 向未成年人提供淫秽、色情、暴力、邪教、迷信、凶杀、恐怖、赌博、涉毒等危害未成年人身心健康的图书、报刊、影视节目、音像制品、网络信息或者电子出版物等的,由出版、广播电视、网信、电影等主管部门给予警告,责令限期改正,可以并处五万元以下罚款; 情节严重或者拒不改正的,责令停产停业,吊销相关许可证,并没收违法所得,处违法所得一倍以上五倍以下的罚款;没有违法所得的,处五万元以上五十万元以下罚款。

出版、播出、放映的图书、报刊、影视节目、音像制品、网络信息和电子出版物等文化产品包含可能影响未成年人身心健康 内容,未按照有关规定处理的,由出版行政、广播电视、网信、电

安证合规集团&北源律师事务所

影等主管部门给予警告,责令限期改正,可以并处五万元以下罚款;情节严重或者拒不改正的,责令停产停业,吊销相关许可证,并没收违法所得,处违法所得一倍以上五倍以下的罚款;没有违法所得的,处五万元以上五十万元以下罚款。

第一百二十四条 组织未成年人进行有害其身心健康的表演等活动的,由文化主管部门给予警告,责令限期改正,可以并处五万元以下罚款;情节严重或者拒不改正的,责令停产停业,吊销相关许可证,可以并处五万元以上五十万元以下罚款。

第一百二十五条 未成年人集中活动的公共场所未按照规定履行安全管理义务的,由应急管理部门给予警告,责令限期改正;拒不改正的,责令停产停业,可以并处一万元以上十万元以下罚款。

大型的商场、超市、医院、图书馆、博物馆、科技馆、游乐场、车站、旅游景点等场所未按照规定设置搜寻走失未成年人的安全警报系统或者未及时履行搜索、报警义务的,由公安、市场监督管理等主管部门给予警告,责令限期整改;情节严重或者拒不改正的,责令停产停业,可以并处一万元以上十万元以下罚款。

第一百二十六条 向未成年人出售烟酒,或者未在显著位置设置不向未成年人出售烟酒标志的,由市场监督管理部门给予警告,责令限期改正,可以并处五万元以下罚款;情节严重或者拒不改正、多次违反的,责令停产停业,吊销营业执照,可以并处五万元以上五十万元以下罚款。

彩票销售机构未在显著位置设置不向未成年人出售彩票标志的,由民政、体育等主管部门予以纠正。

在未成年人集中活动的场所吸烟、饮酒的,由相关主管部门给予警告,责令限期改正,可以并处五百元以下罚款;情节严重或者拒不改正的,处五百元以上一千元以下罚款。

第一百二十七条 向未成年人提供或者出售管制刀具或者其他可能致人严重伤害的器具、器械和物品的,由公安、市场监督管理等主管部门给予警告,责令限期改正,可以并处五万元以下罚款;情节严重或者拒不改正、多次违反的,责令停产停业,吊销营业执照,可以并处五万元以上五十万元以下罚款。

第一百二十八条 密切接触未成年人行业的各类组织招聘从业人员或者对在职人员进行核查时,未按照规定向公安机关进行查询,或者录用、继续聘用具有性侵害、虐待、暴力伤害等严重侵害未成年人违法犯罪记录的人员从事密切接触未成年人行业的,由人力资源和社会保障部门给予警告,责令限期改正,可以并处五万元以下罚款;拒不改正的,责令停产停业,可以并处五万元以上五十万元以下罚款。

第九章附则

第一百二十九条本法中下列用语的含义及范围:

安证合规集团&北海律师事务所

密切接触未成年人行业,是指对未成年人负有监护、教育、培训、救助、看护、医疗等特殊职责的单位、组织、机构等,包括:中小学校、幼儿园等教育机构;文化教育、职业技能等校外教育培训机构;文艺、体育等技能训练机构;未成年人救助保护机构、儿童福利机构等未成年人安置、救助机构;婴幼儿照护和未成年人早期教育服务机构;午晚托班、暑托班、夏令营等校外托管、临时看护机构;为未成年人提供医疗服务的医疗机构等。学生欺凌,是指发生在校园内外、学生之间,一方个体或者群体单次或多次蓄意或者恶意通过肢体、语言及网络等手段实施欺负、侮辱,造成另一方个体或者群体身体伤害、财产损失或者精神损害等行为。

第一百三十条 本法自 年 月 日起施行。

全国人民代表大会常务委员会关于加强网络信息保护的决定

基本信息:

【发布机关】全国人大常委会	【时效性】 现行有效
【发文字号】-	【效力级别】有关法律问题的决定
【发布日期】2012.12.28	【实施日期】2012.12.28

全国人民代表大会常务委员会关于加强网络信息保护的决定

为了保护网络信息安全，保障公民、法人和其他组织的合法权益，维护国家安全和社会公共利益，特作如下决定:

一、国家保护能够识别公民个人身份和涉及公民个人隐私的电子信息。

任何组织和个人不得窃取或者以其他非法方式获取公民个人电子信息，不得出售或者非法向他人提供公民个人电子信息。

二、网络服务提供者和其他企业事业单位在业务活动中收集、使用公民个人电子信息，应当遵循合法、正当、必要的原则，明示收集、使用信息的目的、方式和范围，并经被收集者同意，不得违反法律、法规的规定和双方的约定收集、使用信息。

网络服务提供者和其他企业事业单位收集、使用公民个人电子信息，应当公开其收集、使用规则。

三、网络服务提供者和其他企业事业单位及其工作人员对在业务活动中收集的公民个人电子信息必须严格保密，不得泄露、篡改、毁损，不得出售或者非法向他人提供。

四、网络服务提供者和其他企业事业单位应当采取技术措施和其他必要措施，确保信息安全，

安证合规集团&北海律师事务所

防止在业务活动中收集的公民个人电子信息泄露、毁损、丢失。在发生或者可能发生信息泄露、毁损、丢失的情况时，应当立即采取补救措施。

五、网络服务提供者应当加强对其用户发布的信息的管理，发现法律、法规禁止发布或者传输的信息的，应当立即停止传输该信息，采取消除等处置措施，保存有关记录，并向有关主管部门报告。

六、网络服务提供者为用户办理网站接入服务，办理固定电话、移动电话等入网手续，或者为用户提供信息发布服务，应当在与用户签订协议或者确认提供服务时，要求用户提供真实身份信息。

七、任何组织和个人未经电子信息接收者同意或者请求，或者电子信息接收者明确表示拒绝的，不得向其固定电话、移动电话或者个人电子邮箱发送商业性电子信息。

八、公民发现泄露个人身份、散布个人隐私等侵害其合法权益的网络信息，或者受到商业性电子信息侵扰的，有权要求网络服务提供者删除有关信息或者采取其他必要措施予以制止。

九、任何组织和个人对窃取或者以其他非法方式获取、出售或者非法向他人提供公民个人电子信息的违法犯罪行为以及其他网络信息违法犯罪行为，有权向有关主管部门举报、控告；接到举报、控告的部门应当依法及时处理。被侵权人可以依法提起诉讼。

十、有关主管部门应当在各自职权范围内依法履行职责，采取技术措施和其他必要措施，防范、制止和查处窃取或者以其他非法方式获取、出售或者非法向他人提供公民个人电子信息的违法犯罪行为以及其他网络信息违法犯罪行为。有关主管部门依法履行职责时，网络服务提供者应当予以配合，提供技术支持。

国家机关及其工作人员对在履行职责中知悉的公民个人电子信息应当予以保密，不得泄露、篡改、毁损，不得出售或者非法向他人提供。

十一、对有违反本决定行为的，依法给予警告、罚款、没收违法所得、吊销许可证或者取消备案、关闭网站、禁止有关责任人员从事网络服务业务等处罚，记入社会信用档案并予以公布；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。侵害他人民事权益的，依法承担民事责任。

十二、本决定自公布之日起施行。

安泊智视集团&北京律师事务所

第二篇 行政法规

中华人民共和国电信条例（2016修订）

基本信息：	
【发布机关】国务院	【时效性】 现行有效
【发文字号】国务院令第666号	【效力级别】行政法规
【发布日期】2016.02.06	【实施日期】2016.02.06

中华人民共和国电信条例（2016修订）

第一章 总 则

第一条 为了规范电信市场秩序，维护电信用户和电信业务经营者的合法权益，保障电信网络和信息的安全，促进电信业的健康发展，制定本条例。

第二条 在中华人民共和国境内从事电信活动或者与电信有关的活动，必须遵守本条例。

本条例所称电信，是指利用有线、无线的电磁系统或者光电系统，传送、发射或者接收语音、文字、数据、图像以及其他任何形式信息的活动。

第三条 国务院信息产业主管部门依照本条例的规定对全国电信业实施监督管理。

省、自治区、直辖市电信管理机构在国务院信息产业主管部门的领导下，依照本条例的规定对本行政区域内的电信业实施监督管理。

第四条 电信监督管理遵循政企分开、破除垄断、鼓励竞争、促进发展和公开、公平、公正的原则。

电信业务经营者应当依法经营，遵守商业道德，接受依法实施的监督检查。

第五条 电信业务经营者应当为电信用户提供迅速、准确、安全、方便和价格合理的电信服务。

第六条 电信网络和信息的安全受法律保护。任何组织或者个人不得利用电信网络从事危害国家安全、社会公共利益或者他人合法权益的活动。

第二章 电信市场

第一节 电信业务许可

第七条 国家对电信业务经营按照电信业务分类，实行许可制度。

经营电信业务，必须依照本条例的规定取得国务院信息产业主管部门或者省、自治区、直辖市电信管理机构颁发的电信业务经营许可证。

未取得电信业务经营许可证，任何组织或者个人不得从事电信业务经营活动。

第八条 电信业务分为基础电信业务和增值电信业务。

安证合规集团&北源律师事务所

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。

电信业务分类的具体划分在本条例所附的《电信业务分类目录》中列出。国务院信息产业主管部门根据实际情况，可以对目录所列电信业务分类项目作局部调整，重新公布。

第九条 经营基础电信业务，须经国务院信息产业主管部门审查批准，取得《基础电信业务经营许可证》。

经营增值电信业务，业务覆盖范围在两个以上省、自治区、直辖市的，须经国务院信　息产业主管部门审查批准，取得《跨地区增值电信业务经营许可证》；业务覆盖范围在一个省、自治区、直辖市行政区域内的，须经省、自治区、直辖市电信管理机构审查批准，取得《增值电信业务经营许可证》。

运用新技术试办《电信业务分类目录》未列出的新型电信业务的，应当向省、自治区、直辖市电信管理机构备案。

第十条 经营基础电信业务，应当具备下列条件：

（一）经营者为依法设立的专门从事基础电信业务的公司，且公司中国有股权或者股份不少于51%；

（二）有可行性研究报告和组网技术方案；

（三）有与从事经营活动相适应的资金和专业人员；

（四）有从事经营活动的场地及相应的资源；

（五）有为用户提供长期服务的信誉或者能力；

（六）国家规定的其他条件。

第十一条 申请经营基础电信业务，应当向国务院信息产业主管部门提出申请，并提交本条例第十条规定的相关文件。国务院信息产业主管部门应当自受理申请之日起180日内审查完毕，作出批准或者不予批准的决定。予以批准的，颁发《基础电信业务经营许可证》；不予批准的，应当书面通知申请人并说明理由。

第十二条 国务院信息产业主管部门审查经营基础电信业务的申请时，应当考虑国家安全、电信网络安全、电信资源可持续利用、环境保护和电信市场的竞争状况等因素。

颁发《基础电信业务经营许可证》，应当按照国家有关规定采用招标方式。

第十三条 经营增值电信业务，应当具备下列条件：

（一）经营者为依法设立的公司；

（二）有与开展经营活动相适应的资金和专业人员；

（三）有为用户提供长期服务的信誉或者能力；

（四）国家规定的其他条件。

第十四条 申请经营增值电信业务，应当根据本条例第九条第二款的规定，向国务院信息产业主管部门或者省、自治区、直辖市电信管理机构提出申请，并提交本条例第十三条规定的相关

国汇金和集团&北源律师事务所

文件。申请经营的增值电信业务，按照国家有关规定须经有关主管部门审批的，还应当提交有关主管部门审核同意的文件。国务院信息产业主管部门或者省、自治区、直辖市电信管理机构应当自收到申请之日起60日内审查完毕，作出批准或者不予批准的决定。予以批准的，颁发《跨地区增值电信业务经营许可证》或者《增值电信业务经营许可证》；不予批准的，应当书面通知申请人并说明理由。

第十五条 电信业务经营者在经营过程中，变更经营主体、业务范围或者停止经营的，应当提前90日向原颁发许可证的机关提出申请，并办理相应手续；停止经营的，还应当按照国家有关规定做好善后工作。

第十六条 专用电信网运营单位在所在地区经营电信业务的，应当依照本条例规定的条件和程序提出申请，经批准，取得电信业务经营许可证。

第二节　电信网间互联

第十七条 电信网之间应当按照技术可行、经济合理、公平公正、相互配合的原则，实现互联互通。

主导的电信业务经营者不得拒绝其他电信业务经营者和专用网运营单位提出的互联互通要求。

前款所称主导的电信业务经营者，是指控制必要的基础电信设施并且在电信业务市场中占有较大份额，能够对其他电信业务经营者进入电信业务市场构成实质性影响的经营者。

主导的电信业务经营者由国务院信息产业主管部门确定。

第十八条 主导的电信业务经营者应当按照非歧视和透明化的原则，制定包括网间互联的程序、时限、非捆绑网络元素目录等内容的互联规程。互联规程应当报国务院信息产业主管部门审查同意。该互联规程对主导的电信业务经营者的互联互通活动具有约束力。

第十九条 公用电信网之间、公用电信网与专用电信网之间的网间互联，由网间互联双方按照国务院信息产业主管部门的网间互联管理规定进行互联协商，并订立网间互联协议。

第二十条 网间互联双方经协商未能达成网间互联协议的，自一方提出互联要求之日起60日内，任何一方均可以按照网间互联覆盖范围向国务院信息产业主管部门或者省、自治区、直辖市电信管理机构申请协调；收到申请的机关应当依照本条例第十七条第一款规定的原则进行协调，促使网间互联双方达成协议；自网间互联一方或者双方申请协调之日起45日内经协调仍不能达成协议的，由协调机关随机邀请电信技术专家和其他有关方面专家进行公开论证并提出网间互联方案。协调机关应当根据专家论证结论和提出的网间互联方案作出决定，强制实现互联互通。

第二十一条 网间互联双方必须在协议约定或者决定规定的时限内实现互联互通。遵守网间互联协议和国务院信息产业主管部门的相关规定，保障网间通信畅通，任何一方不得擅自中断互联互通。网间互联遇有通信技术障碍的，双方应当立即采取有效措施予以消除。网间互联双方在互联互通中发生争议的，依照本条例第二十条规定的程序和办法处理。

网间互联的通信质量应当符合国家有关标准。主导的电信业务经营者向其他电信业务经营者提供网间互联，服务质量不得低于本网内的同类业务及向其子公司或者分支机构提供的同类业务

质量。

第二十二条 网间互联的费用结算与分摊应当执行国家有关规定，不得在规定标准之外加收费用。

网间互联的技术标准、费用结算办法和具体管理规定，由国务院信息产业主管部门制定。

第三节 电信资费

第二十三条 电信资费实行市场调节价。电信业务经营者应当统筹考虑生产经营成本、电信市场供求状况等因素，合理确定电信业务资费标准。

第二十四条 国家依法加强对电信业务经营者资费行为的监管，建立健全监管规则，维护消费者合法权益。

第二十五条 电信业务经营者应当根据国务院信息产业主管部门和省、自治区、直辖市电信管理机构的要求，提供准确、完备的业务成本数据及其他有关资料。

第四节 电信资源

第二十六条 国家对电信资源统一规划、集中管理、合理分配，实行有偿使用制度。

前款所称电信资源，是指无线电频率、卫星轨道位置、电信网码号等用于实现电信功能且有限的资源。

第二十七条 电信业务经营者占有、使用电信资源，应当缴纳电信资源费。具体收费办法由国务院信息产业主管部门会同国务院财政部门、价格主管部门制定，报国务院批准后公布施行。

第二十八条 电信资源的分配，应当考虑电信资源规划、用途和预期服务能力。

分配电信资源，可以采取指配的方式，也可以采用拍卖的方式。

取得电信资源使用权的，应当在规定的时限内启用所分配的资源，并达到规定的最低使用规模。未经国务院信息产业主管部门或者省、自治区、直辖市电信管理机构批准，不得擅自使用、转让、出租电信资源或者改变电信资源的用途。

第二十九条 电信资源使用者依法取得电信网码号资源后，主导的电信业务经营者和其他有关单位有义务采取必要的技术措施，配合电信资源使用者实现其电信网码号资源的功能。

法律、行政法规对电信资源管理另有特别规定的，从其规定。

第三章 电信服务

第三十条 电信业务经营者应当按照国家规定的电信服务标准向电信用户提供服务。电信业务经营者提供服务的种类、范围、资费标准和时限，应当向社会公布，并报省、自治区、直辖市电信管理机构备案。

电信用户有权自主选择使用依法开办的各类电信业务。

第三十一条 电信用户申请安装、移装电信终端设备的，电信业务经营者应当在其公布的时限内保证装机开通；由于电信业务经营者的原因逾期未能装机开通的，应当每日按照收取的安装费、移装费或者其他费用数额1%的比例，向电信用户支付违约金。

第三十二条 电信用户申告电信服务障碍的，电信业务经营者应当自接到申告之日起，城镇

安证合规集团&北源律师事务所

48小时、农村72小时内修复或者调通；不能按期修复或者调通的，应当及时通知电信用户，并免收障碍期间的月租费用。但是，属于电信终端设备的原因造成电信服务障碍的除外。

第三十三条 电信业务经营者应当为电信用户交费和查询提供方便。电信用户要求提供国内长途通信、国际通信、移动通信和信息服务等收费清单的，电信业务经营者应当免费提供。

电信用户出现异常的巨额电信费用时，电信业务经营者一经发现，应当尽可能迅速告知电信用户，并采取相应的措施。

前款所称巨额电信费用，是指突然出现超过电信用户此前3个月平均电信费用5倍以上的费用。

第三十四条 电信用户应当按照约定的时间和方式及时、足额地向电信业务经营者交纳电信费用；电信用户逾期不交纳电信费用的，电信业务经营者有权要求补交电信费用，并可以按照所欠费用每日加收3‰的违约金。

对超过收费约定期限30日仍不交纳电信费用的电信用户，电信业务经营者可以暂停向其提供电信服务。电信用户在电信业务经营者暂停服务60日内仍未补交电信费用和违约金的，电信业务经营者可以终止提供服务，并可以依法追缴欠费和违约金。

经营移动电信业务的经营者可以与电信用户约定交纳电信费用的期限、方式，不受前款规定期限的限制。

电信业务经营者应当在迟延交纳电信费用的电信用户补足电信费用、违约金后的48小时内，恢复暂停的电信服务。

第三十五条 电信业务经营者因工程施工、网络建设等原因，影响或者可能影响正常电信服务的，必须按照规定的时限及时告知用户，并向省、自治区、直辖市电信管理机构报告。

因前款原因中断电信服务的，电信业务经营者应当相应减免用户在电信服务中断期间的相关费用。

出现本条第一款规定的情形，电信业务经营者未及时告知用户的，应当赔偿由此给用户造成的损失。

第三十六条 经营本地电话业务和移动电话业务的电信业务经营者，应当免费向用户提供火警、匪警、医疗急救、交通事故报警等公益性电信服务并保障通信线路畅通。

第三十七条 电信业务经营者应当及时为需要通过中继线接入其电信网的集团用户，提供平等、合理的接入服务。

未经批准，电信业务经营者不得擅自中断接入服务。

第三十八条 电信业务经营者应当建立健全内部服务质量管理制度，并可以制定并公布施行高于国家规定的电信服务标准的企业标准。

电信业务经营者应当采取各种形式广泛听取电信用户意见，接受社会监督，不断提高电信服务质量。

第三十九条 电信业务经营者提供的电信服务达不到国家规定的电信服务标准或者其公布的企业标准的，或者电信用户对交纳电信费用持有异议的，电信用户有权要求电信业务　经营者予

安讯合规集团&北源律师事务所

以解决；电信业务经营者拒不解决或者电信用户对解决结果不满意的，电信用户有权向国务院信息产业主管部门或者省、自治区、直辖市电信管理机构或者其他有关部门申诉。收到申诉的机关必须对申诉及时处理，并自收到申诉之日起30日内向申诉者作出答复。

电信用户对交纳本地电话费用有异议的，电信业务经营者还应当应电信用户的要求免费提供本地电话收费依据，并有义务采取必要措施协助电信用户查找原因。

第四十条 电信业务经营者在电信服务中，不得有下列行为：

（一）以任何方式限定电信用户使用其指定的业务；

（二）限定电信用户购买其指定的电信终端设备或者拒绝电信用户使用自备的已经取得入网许可的电信终端设备；

（三）无正当理由拒绝、拖延或者中止对电信用户的电信服务；

（四）对电信用户不履行公开作出的承诺或者作容易引起误解的虚假宣传；

（五）以不正当手段刁难电信用户或者对投诉的电信用户打击报复。

第四十一条 电信业务经营者在电信业务经营活动中，不得有下列行为：

（一）以任何方式限制电信用户选择其他电信业务经营者依法开办的电信服务；

（二）对其经营的不同业务进行不合理的交叉补贴；

（三）以排挤竞争对手为目的，低于成本提供电信业务或者服务，进行不正当竞争。

第四十二条 国务院信息产业主管部门或者省、自治区、直辖市电信管理机构应当依据职权对电信业务经营者的电信服务质量和经营活动进行监督检查，并向社会公布监督抽查结果。

第四十三条 电信业务经营者必须按照国家有关规定履行相应的电信普遍服务义务。

国务院信息产业主管部门可以采取指定的或者招标的方式确定电信业务经营者具体承担电信普遍服务的义务。

电信普遍服务成本补偿管理办法，由国务院信息产业主管部门会同国务院财政部门、价格主管部门制定，报国务院批准后公布施行。

第四章　电信建设

第一节　电信设施建设

第四十四条 公用电信网、专用电信网、广播电视传输网的建设应当接受国务院信息产业主管部门的统筹规划和行业管理。

属于全国性信息网络工程或者国家规定限额以上建设项目的公用电信网、专用电信网、广播电视传输网建设，在按照国家基本建设项目审批程序报批前，应当征得国务院信息产业主管部门同意。

基础电信建设项目应当纳入地方各级人民政府城市建设总体规划和村镇、集镇建设总体规划。

第四十五条 城市建设和村镇、集镇建设应当配套设置电信设施。建筑物内的电信管线和配线设施以及建设项目用地范围内的电信管道，应当纳入建设项目的设计文件，并随建设项目同时施工与验收。所需经费应当纳入建设项目概算。

安证合规集团北源律师事务所

有关单位或者部门规划、建设道路、桥梁、隧道或者地下铁道等，应当事先通知省、自治区、直辖市电信管理机构和电信业务经营者，协商预留电信管线等事宜。

第四十六条 基础电信业务经营者可以在民用建筑物上附挂电信线路或者设置小型天线、移动通信基站等公用电信设施，但是应当事先通知建筑物产权人或者使用人，并按照省、自治区、直辖市人民政府规定的标准向该建筑物的产权人或者其他权利人支付使用费。

第四十七条 建设地下、水底等隐蔽电信设施和高空电信设施，应当按照国家有关规定设置标志。

基础电信业务经营者建设海底电信缆线，应当征得国务院信息产业主管部门同意，并征求有关部门意见后，依法办理有关手续。海底电信缆线由国务院有关部门在海图上标出。

第四十八条 任何单位或者个人不得擅自改动或者迁移他人的电信线路及其他电信设施；遇有特殊情况必须改动或者迁移的，应当征得该电信设施产权人同意，由提出改动或者迁移要求的单位或者个人承担改动或者迁移所需费用，并赔偿由此造成的经济损失。

第四十九条 从事施工、生产、种植树木等活动，不得危及电信线路或者其他电信设施的安全或者妨碍线路畅通；可能危及电信安全时，应当事先通知有关电信业务经营者，并由从事该活动的单位或者个人负责采取必要的安全防护措施。

违反前款规定，损害电信线路或者其他电信设施或者妨碍线路畅通的，应当恢复原状或者予以修复，并赔偿由此造成的经济损失。

第五十条 从事电信线路建设，应当与已建的电信线路保持必要的安全距离；难以避开或者必须穿越，或者需要使用已建电信管道的，应当与已建电信线路的产权人协商，并签订协议；经协商不能达成协议的，根据不同情况，由国务院信息产业主管部门或者省、自治区、直辖市电信管理机构协调解决。

第五十一条 任何组织或者个人不得阻止或者妨碍基础电信业务经营者依法从事电信设施建设和向电信用户提供公共电信服务；但是，国家规定禁止或者限制进入的区域除外。

第五十二条 执行特殊通信、应急通信和抢修、抢险任务的电信车辆，经公安交通管理机关批准，在保障交通安全畅通的前提下可以不受各种禁止机动车通行标志的限制。

第二节　电信设备进网

第五十三条 国家对电信终端设备、无线电通信设备和涉及网间互联的设备实行进网许可制度。

接入公用电信网的电信终端设备、无线电通信设备和涉及网间互联的设备，必须符合国家规定的标准并取得进网许可证。

实行进网许可制度的电信设备目录，由国务院信息产业主管部门会同国务院产品质量监督部门制定并公布施行。

第五十四条 办理电信设备进网许可证的，应当向国务院信息产业主管部门提出申请，并附送经国务院产品质量监督部门认可的电信设备检测机构出具的检测报告或者认证机构出具的产品

安证合规集团&北源律师事务所

质量认证证书。

国务院信息产业主管部门应当自收到电信设备进网许可申请之日起60日内，对申请及电信设备检测报告或者产品质量认证证书审查完毕。经审查合格的，颁发进网许可证；经审查不合格的，应当书面答复并说明理由。

第五十五条 电信设备生产企业必须保证获得进网许可的电信设备的质量稳定、可靠，不得降低产品质量和性能。

电信设备生产企业应当在其生产的获得进网许可的电信设备上粘贴进网许可标志。

国务院产品质量监督部门应当会同国务院信息产业主管部门对获得进网许可证的电信设备进行质量跟踪和监督抽查，公布抽查结果。

第五章 电信安全

第五十六条 任何组织或者个人不得利用电信网络制作、复制、发布、传播含有下列内容的信息：

（一）反对宪法所确定的基本原则的；

（二）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；

（三）损害国家荣誉和利益的；

（四）煽动民族仇恨、民族歧视，破坏民族团结的；

（五）破坏国家宗教政策，宣扬邪教和封建迷信的；

（六）散布谣言，扰乱社会秩序，破坏社会稳定的；

（七）散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的；

（八）侮辱或者诽谤他人，侵害他人合法权益的；

（九）含有法律、行政法规禁止的其他内容的。

第五十七条 任何组织或者个人不得有下列危害电信网络安全和信息安全的行为：

（一）对电信网的功能或者存储、处理、传输的数据和应用程序进行删除或者修改；

（二）利用电信网从事窃取或者破坏他人信息、损害他人合法权益的活动；

（三）故意制作、复制、传播计算机病毒或者以其他方式攻击他人电信网络等电信设施；

（四）危害电信网络安全和信息安全的其他行为。

第五十八条 任何组织或者个人不得有下列扰乱电信市场秩序的行为：

（一）采取租用电信国际专线、私设转接设备或者其他方法，擅自经营国际或者香港特别行政区、澳门特别行政区和台湾地区电信业务；

（二）盗接他人电信线路，复制他人电信码号，使用明知是盗接、复制的电信设施或者码号；

（三）伪造、变造电话卡及其他各种电信服务有价凭证；

（四）以虚假、冒用的身份证件办理入网手续并使用移动电话。

第五十九条 电信业务经营者应当按照国家有关电信安全的规定，建立健全内部安全保障制度，实行安全保障责任制。

京北方信息技术集团股份有限公司 北源律师事务所

第六十条 电信业务经营者在电信网络的设计、建设和运行中，应当做到与国家安全和电信网络安全的需求同步规划，同步建设，同步运行。

第六十一条 在公共信息服务中，电信业务经营者发现电信网络中传输的信息明显属于本条例第五十六条所列内容的，应当立即停止传输，保存有关记录，并向国家有关机关报告。

第六十二条 使用电信网络传输信息的内容及其后果由电信用户负责。

电信用户使用电信网络传输的信息属于国家秘密信息的，必须依照保守国家秘密法的规定采取保密措施。

第六十三条 在发生重大自然灾害等紧急情况下，经国务院批准，国务院信息产业主管部门可以调用各种电信设施，确保重要通信畅通。

第六十四条 在中华人民共和国境内从事国际通信业务，必须通过国务院信息产业主管部门批准设立的国际通信出入口局进行。

我国内地与香港特别行政区、澳门特别行政区和台湾地区之间的通信，参照前款规定办理。

第六十五条 电信用户依法使用电信的自由和通信秘密受法律保护。除因国家安全或者追查刑事犯罪的需要，由公安机关、国家安全机关或者人民检察院依照法律规定的程序对电信内容进行检查外，任何组织或者个人不得以任何理由对电信内容进行检查。

电信业务经营者及其工作人员不得擅自向他人提供电信用户使用电信网络所传输信息的内容。

第六章 罚则

第六十六条 违反本条例第五十六条、第五十七条的规定，构成犯罪的，依法追究刑事责任；尚不构成犯罪的，由公安机关、国家安全机关依照有关法律、行政法规的规定予以处罚。

第六十七条 有本条例第五十八条第（二）、（三）、（四）项所列行为之一，扰乱电信市场秩序，构成犯罪的，依法追究刑事责任；尚不构成犯罪的，由国务院信息产业主管部门或者省、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1万元的，处1万元以上10万元以下罚款。

第六十八条 违反本条例的规定，伪造、冒用、转让电信业务经营许可证、电信设备进网许可证或者编造在电信设备上标注的进网许可证编号的，由国务院信息产业主管部门或者省、自治区、直辖市电信管理机构依据职权没收违法所得，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1万元的，处1万元以上10万元以下罚款。

第六十九条 违反本条例规定，有下列行为之一的，由国务院信息产业主管部门或者省、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：

（一）违反本条例第七条第三款的规定或者有本条例第五十八条第（一）项所列行为，擅自经营电信业务的，或者超范围经营电信业务的；

（二）未通过国务院信息产业主管部门批准，设立国际通信出入口进行国际通信的；

（三）擅自使用、转让、出租电信资源或者改变电信资源用途的；

（四）擅自中断网间互联互通或者接入服务的；

（五）拒不履行普遍服务义务的。

第七十条 违反本条例的规定，有下列行为之一的，由国务院信息产业主管部门或者省、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1倍以上3倍以下罚款；没有违法所得或者违法所得不足1万元的，处1万元以上10万元以下罚款；情节严重的，责令停业整顿：

（一）在电信网间互联中违反规定加收费用的；

（二）遇有网间通信技术障碍，不采取有效措施予以消除的；

（三）擅自向他人提供电信用户使用电信网络所传输信息的内容的；

（四）拒不按照规定缴纳电信资源使用费的。

第七十一条 违反本条例第四十一条的规定，在电信业务经营活动中进行不正当竞争的，由国务院信息产业主管部门或者省、自治区、直辖市电信管理机构依据职权责令改正，处10万元以上100万元以下罚款；情节严重的，责令停业整顿。

第七十二条 违反本条例的规定，有下列行为之一的，由国务院信息产业主管部门或者省、自治区、直辖市电信管理机构依据职权责令改正，处5万元以上50万元以下罚款；情节严重的，责令停业整顿：

（一）拒绝其他电信业务经营者提出的互联互通要求的；

（二）拒不执行国务院信息产业主管部门或者省、自治区、直辖市电信管理机构依法作出的互联互通决定的；

（三）向其他电信业务经营者提供网间互联的服务质量低于本网及其子公司或者分支机构的。

第七十三条 违反本条例第三十三条第一款、第三十九条第二款的规定，电信业务经营者拒绝免费为电信用户提供国内长途通信、国际通信、移动通信和信息服务等收费清单，或者电信用户对交纳本地电话费用有异议并提出要求时，拒绝为电信用户免费提供本地电话收费依据的，由省、自治区、直辖市电信管理机构责令改正，并向电信用户赔礼道歉；拒不改正并赔礼道歉的，处以警告，并处5000元以上5万元以下的罚款。

第七十四条 违反本条例第四十条的规定，由省、自治区、直辖市电信管理机构责令改正，并向电信用户赔礼道歉，赔偿电信用户损失；拒不改正并赔礼道歉、赔偿损失的，处以警告，并处1万元以上10万元以下的罚款；情节严重的，责令停业整顿。

第七十五条 违反本条例的规定，有下列行为之一的，由省、自治区、直辖市电信管理机构责令改正，处1万元以上10万元以下的罚款：

（一）销售未取得进网许可的电信终端设备的；

（二）非法阻止或者妨碍电信业务经营者向电信用户提供公共电信服务的；

（三）擅自改动或者迁移他人的电信线路及其他电信设施的。

安汇合邦集团&北源律师事务所

第七十六条 违反本条例的规定，获得电信设备进网许可证后降低产品质量和性能的，由产品质量监督部门依照有关法律、行政法规的规定予以处罚。

第七十七条 有本条例第五十六条、第五十七条和第五十八条所列禁止行为之一，情节严重的，由原发证机关吊销电信业务经营许可证。

国务院信息产业主管部门或者省、自治区、直辖市电信管理机构吊销电信业务经营许可证后，应当通知企业登记机关。

第七十八条 国务院信息产业主管部门或者省、自治区、直辖市电信管理机构工作人员玩忽职守、滥用职权、徇私舞弊，构成犯罪的，依法追究刑事责任；尚不构成犯罪的，依法给予行政处分。

第七章 附则

第七十九条 外国的组织或者个人在中华人民共和国境内投资与经营电信业务和香港特别行政区、澳门特别行政区与台湾地区的组织或者个人在内地投资与经营电信业务的具体办法，由国务院另行制定。

第八十条 本条例自公布之日起施行。

互联网信息服务管理办法（2011修订）

基本信息:	
【发布机关】国务院	【时效性】 现行有效
【发文字号】国务院令第588号	【效力级别】行政法规
【发布日期】2011.01.08	【实施日期】2011.01.08

互联网信息服务管理办法（2011修订）【节选】

第六条 从事经营性互联网信息服务，除应当符合《中华人民共和国电信条例》规定的要求外，还应当具备下列条件:

（一）有业务发展计划及相关技术方案;

（二）有健全的网络与信息安全保障措施，包括网站安全保障措施、信息安全保密管理制度、用户信息安全管理制度;

（三）服务项目属于本办法第五条规定范围的，已取得有关主管部门同意的文件。

第十四条 从事新闻、出版以及电子公告等服务项目的互联网信息服务提供者，应当记录提供的信息内容及其发布时间、互联网地址或者域名；互联网接入服务提供者应当记录上网用户的

安证合规集团&北源律师事务所

上网时间、用户账号、互联网地址或者域名、主叫电话号码等信息。

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。

第十五条 互联网信息服务提供者不得制作、复制、发布、传播含有下列内容的信息：

……

（八）侮辱或者诽谤他人，侵害他人合法权益的；

（九）含有法律、行政法规禁止的其他内容的。

第十六条 互联网信息服务提供者发现其网站传输的信息明显属于本办法第十五条所列内容之一的，应当立即停止传输，保存有关记录，并向国家有关机关报告。

第二十条 制作、复制、发布、传播本办法第十五条所列内容之一的信息，构成犯罪的，依法追究刑事责任；尚不构成犯罪的，由公安机关、国家安全机关依照《中华人民共和国治安管理处罚法》、《计算机信息网络国际联网安全保护管理办法》等有关法律、行政法规的规定予以处罚；对经营性互联网信息服务提供者，并由发证机关责令停业整顿直至吊销经营许可证，通知企业登记机关；对非经营性互联网信息服务提供者，并由备案机关责令暂时关闭网站直至关闭网站。

第三篇 地方法规

广东省数字经济促进条例

基本信息：	
【发布机关】广东省工业和信息化厅	【时效性】 现行有效
【发布文号】广东省第十三届人民代表大会常务委员会公告第85号	【效力级别】地方性法规
	【实施日期】2021.09.01
【发布日期】2021.07.30	

第一章 总 则

第一条 为了促进数字经济发展，推进数字产业化和产业数字化，推动数字技术与实体经济深度融合，打造具有国际竞争力的数字产业集群，全面建设数字经济强省，根据有关法律、行政法规，结合本省实际，制定本条例。

安证合规集团&北源律师事务所

第二条 本条例适用于本省行政区域内促进数字经济发展，以及为数字经济提供支撑保障等相关活动。

本条例所称数字经济，是指以数据资源为关键生产要素，以现代信息网络作为重要载体，以信息通信技术的有效使用作为效率提升和经济结构优化的重要推动力的一系列经济活动。

第三条 数字经济发展应当遵循创新引领、数据驱动、融合赋能、包容审慎、安全发展的原则。

第四条 数字经济发展以数字产业化和产业数字化为核心。数字产业化主要促进数字产品制造业、数字产品服务业、数字技术应用业、数字要素驱动业的发展；产业数字化主要促进工业数字化、农业数字化、服务业数字化等数字化效率提升业的发展。

第五条 县级以上人民政府应当将数字经济发展纳入国民经济和社会发展规划，并根据需要制定本级数字经济发展规划。

省人民政府应当加强对全省数字经济发展的统筹部署，营造数字经济发展良好环境。地级以上市、县级人民政府应当及时掌握数字经济发展动态，协调解决重大问题，按照上级人民政府统筹部署组织实施。

第六条 省人民政府发展改革主管部门负责拟制促进数字化发展战略、规划和重大政策，推进数字化发展重大工程和项目实施；工业和信息化主管部门负责促进数字经济发展工作，拟制促进数字经济发展的战略、规划和政策措施并组织实施；统计主管部门负责建立数字经济统计监测机制，开展数字经济统计调查和监测分析，依法向社会公布。

地级以上市、县级人民政府工业和信息化主管部门或者本级人民政府确定的主管部门，负责推进数字经济发展具体工作。

县级以上人民政府其他有关部门按照职责分工，做好数字经济发展工作。

第七条 省人民政府及有关部门应当加强与“一带一路”沿线国家和地区在数字基础设施、数字商贸、数字金融、智慧物流等领域的交流合作，扩大数字经济领域开放。加强粤港澳大湾区数字经济规则衔接、机制对接，推进网络互联互通、数字基础设施共建共享、数字产业协同发展。

县级以上人民政府及有关部门应当按照本省关于珠三角核心区、沿海经济带、北部生态发展区的区域发展格局，加强数字经济区域优势互补、差异化协调发展。

鼓励社会力量参与数字经济发展，加强国内外交流合作。

第八条 引导企业等市场主体在促进数字经济发展政策支持下，进行数字化转型。支持和鼓励各类市场主体参与数字经济领域投资建设。

安证合规集团&北源律师事务所

支持行业协会、科研机构、高等学校以及其他组织为促进数字经济发展提供创业孵化、投资融资、技术支持、法律服务、产权交易等服务

第二章　数字产业化

第九条 县级以上人民政府应当促进计算机通信和其他电子设备制造业、电信广播电视和卫星传输服务、互联网和相关服务、软件和信息技术服务业等发展，培育人工智能、大数据、区块链、云计算、网络安全等新兴数字产业，谋划布局未来产业。

第十条 省人民政府及发展改革、科技、工业和信息化等有关部门应当统筹规划集成电路产业发展，提升基金、平台、高等学校、园区支撑水平，从制造、设计、封测、材料、装备、零部件、工具、应用等方面构建产业支柱，支持优质项目投资建设，打造集成电路产业创新发展高地。

第十一条 省人民政府及科技、工业和信息化等有关部门应当统筹规划软件产业发展，培育具有自主知识产权的软件产业，推进软件产品迭代、平台搭建、产业化应用、适配测试和开源开放，拓展用户市场，构建安全可控、共建共享的软件产业生态。

第十二条 省人民政府及工业和信息化、通信管理等有关部门应当统筹规划新一代移动通信产业发展和应用创新，加强材料、制造工艺等领域前沿布局，构建集材料、芯片、基站、设备、终端、应用于一体的新一代移动通信产业链。

第十三条 县级以上人民政府及发展改革、商务、市场监督管理等有关部门应当培育互联网平台企业，支持利用互联网平台推进资源集成共享和优化配置。依法依规明确平台企业定位和监管规则，促进平台经济和共享经济规范有序创新健康发展。

互联网平台经营者应当建立健全平台管理规则和制度，依法依约履行产品和服务质量保障、网络安全保障、数据安全保障、消费者权益保护、个人信息保护等方面的义务。

第十四条 县级以上人民政府及发展改革、科技、工业和信息化、商务、市场监督管理等有关部门应当引导支持数字经济领域的龙头企业、高新技术企业，以及科技型中小企业和专业化、精细化、特色化、新颖化中小企业发展。

县级以上人民政府及地方金融监督管理等有关部门应当培育数字经济领域企业上市资源，支持有条件的企业依法到证券交易机构上市。

第十五条 县级以上人民政府及发展改革、科技、工业和信息化等有关部门应当结合本地实际，引导支持数字产业基地和园区建设，重点培育下列数字产业集群：

（一）新一代电子信息；

（二）软件与信息服务；

君泽君集团&北京律师事务所

（三）超高清视频显示；

（四）半导体与集成电路；

（五）智能机器人；

（六）区块链与量子信息；

（七）数字创意；

（八）其他重要数字产业集群。

第十六条 引导互联网企业、行业龙头企业、基础电信企业开放数据资源和平台计算能力等，支持企业、科研机构、高等学校等创建数字经济领域众创空间、科技企业孵化器、科技企业加速器、大学科技园等创新创业载体，构建协同共生的数字经济产业创新生态。

第三章　工业数字化

第十七条 县级以上人民政府应当推进工业实施全方位、全角度、全链条的改造，提升全要素生产率，加快工业生产模式和企业形态变革，促进工业数字化、网络化、智能化转型。

第十八条 县级以上人民政府及工业和信息化、通信管理等有关部门应当推动跨行业、跨领域以及特色型、专业型工业互联网平台建设，支持企业改造提升工业互联网内外网络，建立完善工业互联网标识解析体系，健全工业互联网安全保障体系。

第十九条 省人民政府及科技、工业和信息化、通信管理等有关部门应当通过推动工业互联网平台、网络、标识解析、安全等关键技术突破，增强工业芯片、工业软件、工业操作系统等供给能力，实现工业制造技术和工艺数字化、软件化。

第二十条 县级以上人民政府及工业和信息化等有关部门应当推动工业数字化产业生态建设，培育工业数字化转型服务商，以提供数字化平台、系统解决方案以及数字产品和服务。

第二十一条 县级以上人民政府及工业和信息化等有关部门应当推动发展智能制造，加强工业互联网创新应用，支持工业企业实施数字化改造，推进工业设备和业务系统上云上平台，建设智能工厂、智能车间，培育推广智能化生产、网络化协同、个性化定制、服务化延伸、数字化管理等新业态新模式。

第二十二条 县级以上人民政府及工业和信息化、国有资产监督管理等有关部门应当推动大型工业企业开展集成应用创新，推进关键业务环节数字化，带动供应链企业数字化转型。推动中小型工业企业运用低成本、快部署、易运维的工业互联网解决方案，普及应用工业互联网。

第二十三条 县级以上人民政府及工业和信息化等有关部门应当结合本地实际，推进产业集群数字化改造，推动产业集群利用工业互联网进行全要素、全产业链、全价值链的连接，通过信息、技术、产能、订单共享，实现跨地域、跨行业资源的精准配置与高效对接。

安证合规集团&北源律师事务所

支持产业集群骨干企业、工业数字化转型服务商等组建产业联合体，开发推广行业通用的技术集成解决方案，促进集群企业协同发展。

第四章　农业数字化

第二十四条 县级以上人民政府应当加快种植业、种业、林业、畜牧业、渔业、农产品加工业等数字化转型，推动发展智慧农业，促进乡村振兴。

第二十五条 县级以上人民政府及农业农村等有关部门应当推动遥感监测、地理信息等信息通信技术在农田建设、农机作业、农产品质量安全追溯等的应用，支持建设智慧农业云平台和农业大数据平台，探索智慧农业技术集成应用解决方案，提升农业生产精细化、智能化水平。

第二十六条 县级以上人民政府及农业农村、商务等有关部门应当支持新型农业规模经营主体、加工流通企业与电子商务企业融合，推动农产品加工、包装、冷链、仓储、配送等物流设施数字化建设，培育电子商务农产品品牌，促进农业农村电子商务发展。

第二十七条 县级以上人民政府及农业农村、通信管理等有关部门应当提升乡村信息网络水平，推动乡村信息服务供给和基础设施数字化转型。

第二十八条 县级以上人民政府及农业农村、文化和旅游等有关部门应当推动互联网与特色农业融合发展，培育推广创意农业、认养农业、观光农业以及游憩休闲、健康养生、创意民宿等数字乡村新业态新模式。

第五章　服务业数字化

第二十九条 县级以上人民政府应当重点推动智能交通、智慧物流、数字金融、数字商贸、智慧教育、智慧医疗、智慧文旅等数字应用场景建设，创新服务内容和模式，提升服务质量和效率。

第三十条 县级以上人民政府交通运输主管部门应当推动发展智能交通，加速交通基础设施网、运输服务网、能源网与信息网络融合发展，构建泛在先进的交通信息基础设施。构建综合交通大数据中心体系。培育推广智能网联汽车、自动驾驶船舶、自动化码头，以及定制公交、智能公交、智能停车等新业态新模式。

第三十一条 县级以上人民政府及发展改革、交通运输、邮政管理等有关部门应当推动发展智慧物流，推进货物、运输工具、场站等物流要素数字化，支持物流园区、大型仓储设施、货运车辆等普及应用数字化技术和智能终端设备，提升物流智能化水平。

第三十二条 县级以上人民政府地方金融监督管理部门应当推动发展数字金融，优化移动支付应用，推进数字金融与产业链、供应链融合。

按照国家规定探索数字人民币的应用和国际合作。

安证合规集团&北源律师事务所

第三十三条 县级以上人民政府及商务等有关部门应当推动发展数字商贸，引导支持服务贸易和数字贸易的集聚区、平台及其促进体系发展。促进跨境电子商务综合试验区、数字服务出口基地建设，培育推广云服务、数字内容、数字服务、跨境电子商务等新业态新模式，支持数字化商贸平台建设，发展社交电子商务、直播电子商务等，完善发展机制、监管模式，建设与国际接轨的高水平服务贸易和数字贸易开放体系，提升数字商贸水平。

第三十四条 县级以上人民政府教育主管部门应当推动发展智慧教育，推进教育数据和数字教学资源互通共享，支持建设智慧校园、智慧课堂、互联网教育资源服务大平台，培育推广并规范管理互动教学、个性定制等在线教育新业态新模式。

第三十五条 县级以上人民政府卫生健康主管部门应当推动发展智慧医疗，推进人工智能、大数据、区块链和云计算在医学影像辅助诊断、临床辅助决策、智能化医学设备、公共卫生事件防控等领域的应用，加快开展网上预约、咨询、挂号、分诊、问诊、结算以及药品配送、检查检验报告推送等网络医疗服务，建设互联网医院，拓展医疗卫生机构服务空间和内容。

县级以上人民政府民政、卫生健康主管部门应当推动发展智慧健康养老产业，推动个人、家庭、社区、机构与健康养老资源有效对接和优化配置，促进健康养老服务智慧化升级，以满足个人和家庭多层次、多样化健康养老服务需求。

第三十六条 县级以上人民政府及网信、文化和旅游、广电、版权等有关部门应当推动发展互联网文体娱乐业等，支持建设公共文化云平台和智慧图书馆、博物馆等数字文化场馆，培育推广游戏、动漫、电竞、网络直播、融媒体等新业态新模式，发展网络视听、数字出版、数字娱乐、线上演播等产业，鼓励拓展优秀传统文化产品和影视剧、游戏等数字文化产品的海外市场。

县级以上人民政府及文化和旅游等有关部门应当推动发展智慧旅游，加强线上旅游宣传，推广在线预约预订服务，创新道路信息、气象预警等旅游公共服务模式，引导旅游景区开发数字化体验产品并普及景区电子地图、线路推荐、语音导览等智慧化服务。

第六章　数据资源开发利用保护

第三十七条 鼓励对数据资源实行全生命周期管理，挖掘数据资源要素潜力，发挥数据的关键资源作用和创新引擎作用，提升数据要素质量，培育数据要素市场，促进数据资源开发利用保护。

第三十八条 国家机关以及法律、法规授权的具有管理公共事务职能的组织在依法履行职责、提供服务过程中产生或者获取的公共数据，应当按照国家和省的有关规定进行分类分级，实行目录制管理。

安证合规集团&北源律师事务所

县级以上人民政府政务服务数据管理部门统筹推进公共数据资源共享开放和开发利用，规范公共数据产品服务。国家机关以及法律、法规授权的具有管理公共事务职能的组织应当建立公共数据开放范围的动态调整机制，创新公共数据资源开发利用模式和运营机制，满足市场主体合理需求。

第三十九条 县级以上人民政府及政务服务数据管理等有关部门应当促进各类数据深度融合，鼓励依法依规利用数据资源开展科学研究、数据加工等活动，引导各类主体通过省统一的开放平台开放数据资源。支持构建工业、农业、服务业等领域数据资源开发利用场景。

第四十条 自然人、法人和非法人组织对依法获取的数据资源开发利用的成果，所产生的财产权益受法律保护，并可以依法交易。法律另有规定或者当事人另有约定的除外。

探索数据交易模式，培育数据要素市场，规范数据交易行为，促进数据高效流通。有条件的地区可以依法设立数据交易场所，鼓励和引导数据供需方在数据交易场所进行交易。

第四十一条 数据的收集、存储、使用、加工、传输、提供、公开等处理活动，应当遵守法律、法规，履行数据安全保护义务，尊重社会公德和伦理，遵守商业道德和职业道德，诚实守信，承担社会责任。

开展数据处理活动，不得危害国家安全、公共利益，不得损害个人、组织的合法权益。

个人信息受法律保护。个人信息的收集、存储、使用、加工、传输、提供、公开等处理活动，应当遵循合法、正当、必要原则，不得过度处理，并符合法律、法规规定的条件。

第四十二条 县级以上人民政府及网信、发展改革、工业和信息化、农业农村、商务、市场监督管理、政务服务数据管理等有关部门应当推广数据管理相关国家标准和行业标准，规范数据管理，提升数据质量。

探索推动产业数据的收集、存储、使用、加工、传输和共享，加强产业数据分类分级管理，支持企业提升数据汇聚、分析、应用能力，以及构建数据驱动的生产方式和企业管理模式。

第七章 数字技术创新

第四十三条 省人民政府及有关部门应当围绕数据的产生、传输、存储、计算与应用环节，推动数字技术创新，加强数字技术基础研究、应用基础研究和技术成果转化，完善产业技术创新体系和共性基础技术供给体系。

第四十四条 省人民政府及科技等有关部门应当围绕数字经济实施省重点领域研发计划重大专项，构建国家重大科技项目承接机制，推动获取重大原创科技成果和自主知识产权。

第四十五条 省人民政府及科技等有关部门应当探索建立数字经济关键核心技术攻关新型体制机制,重点在集成电路、基础软件、工业软件等基础领域，新一代移动通信、人工智能、区块

安证合规集团&北源律师事务所

链、数字孪生、量子科技、类脑计算等前沿技术领域，加快推进基础理论、基础算法、装备材料等关键核心技术攻关和突破。

第四十六条 省人民政府应当统筹规划、科学布局，推进数字经济领域省实验室建设，打造数字技术大型综合研究基地和原始创新策源地。

第四十七条 省人民政府及发展改革、科技、工业和信息化、市场监督管理等有关部门应当推动数字经济领域的科技创新平台、公共技术服务平台和重大科技基础设施建设，构建以企业为主体、市场为导向的技术创新体系。

第四十八条 县级以上人民政府及教育、科技等有关部门应当推进数字经济产学研合作，支持科研机构、高等学校等与企业共建技术创新联盟、科技创新基地、博士工作站、博士后科研工作站等创新平台，加强科研力量优化配置和资源共享，促进关键共性技术研发、系统集成和工程化应用。

支持数字技术开源平台、开源社区和开放技术网络建设，鼓励企业开放软件源代码、硬件设计和应用服务。

第四十九条 县级以上人民政府市场监督管理部门，以及其他行政主管部门应当加强数字经济标准化工作，依法对数字经济标准的实施进行监督。

支持社会团体、企业及其他组织开展数字经济国际国内标准交流合作，参与制定数字经济国际规则、国际国内标准，自主制定数字经济团体标准和企业标准。

第五十条 县级以上人民政府及教育、科技、工业和信息化、财政等有关部门应当支持科研机构、高等学校和企业完善数字技术转移机制；探索实施政府采购首台（套）装备、首批次产品、首版次软件等政策，支持创新产品和服务的应用推广；鼓励将财政资金支持形成的科技成果许可给中小企业使用，提升成果转化与产业化水平。

第八章 数字基础设施建设

第五十一条 县级以上人民政府应当完善数字基础设施体系，重点统筹通信网络基础设施、新技术基础设施、存储和计算基础设施等建设，推进传统基础设施的数字化改造，布局卫星互联网等未来网络设施。

第五十二条 数字基础设施的建设和布局应当纳入国土空间规划，市政、交通、电力、公共安全等相关基础设施规划应当结合数字经济发展需要，与数字基础设施相关规划相互协调和衔接。

第五十三条 县级以上人民政府及通信管理等有关部门应当支持新一代固定宽带网络和移动通信网络建设，推进核心网、承载网、接入网及基站、管线等信息通信网络建设。

安证合规集团&北源律师事务所

工程建设、设计等相关单位应当按照有关建设设计标准和规范，预留信息通信网络设施所需的空间、电力等资源，并与主体工程同时设计、同时施工、同时验收。

推动通信设施与铁路、城市轨道、道路、桥梁、隧道、电力、地下综合管廊、机场、港口、枢纽站场、智慧杆塔等基础设施以及相关配套设施共商共建共享共维。

第五十四条 县级以上人民政府及有关部门应当推进物联网建设，积极部署低成本、低功耗、高精度、高可靠的智能化传感器，推进基础设施、城市治理、物流仓储、生产制造、生活服务、应急管理、生态保护等领域感知系统的建设应用、互联互通和数据共享。

县级以上人民政府及有关部门可以根据实际情况推进车联网建设，扩大车联网覆盖范围，提高路侧单元与道路基础设施、智能管控设施的融合接入能力，推进道路基础设施、交通标志标识的数字化改造和建设。

第五十五条 省人民政府及发展改革、科技、工业和信息化等有关部门应当统筹推进人工智能、区块链、云计算等新技术基础设施建设，支持建设底层技术平台、算法平台、开源平台等基础平台，建立领先的通用技术能力支撑体系。

第五十六条 省人民政府及发展改革、科技、工业和信息化、通信管理等有关部门应当统筹推进数据中心、智能计算中心、超级计算中心、边缘计算节点等存储和计算基础设施建设，支持优化升级改造，提升计算能力，构建高效协同的数据处理体系。

第五十七条 县级以上人民政府应当结合本地实际，推动能源、交通、城市、物流、医疗、教育、文化、自然资源、农业农村、水利、生态环境、应急等领域的传统基础设施数字化、智能化改造。

第五十八条 省人民政府自然资源主管部门应当统筹建设本省卫星导航定位基准服务系统和配套基础设施，提供卫星导航定位基准信息公共服务。

鼓励符合法定条件的组织参与卫星互联网基础设施建设，构建通信、导航、遥感空间基础设施体系。

第九章 保障措施

第五十九条 县级以上人民政府应当坚持数字经济、数字政府、数字社会一体建设，营造良好数字生态。在政务服务、财政、税收、金融、人才、知识产权，以及土地供应、电力接引、设施保护、政府采购等方面完善政策措施，为促进数字经济发展提供保障。

第六十条 省人民政府及政务服务数据管理部门应当推进数字政府改革建设，完善管运分离、政企合作的管理体制，创新建设运营模式，优化一网通办政务服务，推动一网统管省域治理，强化一网协同政府运行，提高政府数字化服务数字经济发展效能。

君证合规集团&北源律师事务所

省人民政府及政务服务数据管理部门应当统筹规划全省政务网络基础设施建设，打造全省统一的政务基础网络、政务云平台和政务大数据中心，推进一体化网上政务服务平台以及移动政务平台的建设和应用。

第六十一条 省人民政府及有关部门统筹使用省级专项资金，有条件的地级以上市、县级人民政府在本级财政预算中安排资金，重点用于数字经济关键核心技术攻关、重大创新平台、公共技术平台和产业载体建设、应用示范和产业化发展、企业培育等领域。

县级以上人民政府应当依法落实数字经济的税收优惠政策。完善投融资服务体系，拓宽数字经济市场主体融资渠道。发挥省级政策性基金作用，重点支持数字经济领域重大项目建设和高成长、初创型数字经济企业发展。

第六十二条 县级以上人民政府及教育、人力资源社会保障等有关部门应当鼓励企事业单位、社会组织等培养创新型、应用型、技能型、融合型人才，支持高等学校、中等职业学校与企业开展合作办学，培养数字经济专业人才。

县级以上人民政府及人力资源社会保障主管部门应当将数字经济领域引进的高层次、高技能以及紧缺人才纳入政府人才支持政策范围，按照规定享受入户、住房、子女教育等优惠待遇。探索建立适应数字经济新业态发展需要的人才评价机制。

第六十三条 县级以上人民政府及市场监督管理、版权等有关部门应当加强数字经济领域知识产权保护，培育知识产权交易市场，探索建立知识产权保护规则和快速维权体系，依法打击知识产权侵权行为。

第六十四条 县级以上人民政府及市场监督管理部门应当依法查处滥用市场支配地位、实施垄断协议以及从事不正当竞争等违法行为，保障各类市场主体的合法权益，营造公平竞争市场环境。

县级以上人民政府及人力资源社会保障等有关部门应当加强劳动用工服务指导，清理对灵活就业的不合理限制，鼓励依托数字经济创造更多灵活就业机会，完善平台经济、共享经济等新业态从业人员在工作时间、报酬支付、保险保障等方面政策规定。

第六十五条 县级以上人民政府及网信、应急管理、政务服务数据管理、通信管理等有关部门，企业、平台等处理数据的主体应当落实数字经济发展过程中的安全保障责任，健全安全管理制度，加强重要领域数据资源、重要网络、信息系统和硬件设备安全保障，健全关键信息基础设施保障体系，建立安全风险评估、监测预警和应急处置机制，采取必要安全措施，保护数据、网络、设施等方面的安全。

安证合规集团&北源律师事务所

第六十六条 县级以上人民政府应当建立数字经济创新创业容错免责机制，对新技术、新产业、新业态、新模式等实行包容审慎监管。

第六十七条 县级以上人民政府及有关部门应当加强数字经济宣传、教育、培训，加强数字技能教育和培训，普及提升全社会数字素养。

支持举办数字经济领域的国际国内会展、赛事等活动，搭建数字经济展示交易、交流合作平台，畅通供需对接渠道，提高市场开拓能力。

第六十八条 县级以上人民政府及有关部门应当推进信息无障碍建设，坚持创新智能化服务与改进传统服务并行。鼓励针对老年人、残疾人等运用智能技术困难的群体的出行、就医、消费、文娱、办事等，提供适用的智能化产品和服务，帮助其共享数字生活。

第六十九条 县级以上人民政府有关部门应当按照职责分工，制定执行本条例的工作计划，并定期向本级人民政府报告执行情况。

第七十条 县级以上人民政府应当定期对本级数字经济发展情况进行评估，并对下一级人民政府数字经济发展情况开展监督检查。

数字经济发展情况评估可以委托第三方机构开展，并向社会公布。

第七十一条 各级人民政府及有关部门在数字经济促进工作中不依法履行职责的，依照法律、法规追究责任，对直接负责的主管人员和其他直接责任人员依法给予处分。

违反有关网络安全、数据安全、个人信息保护等法律、法规的，由有关主管部门依法予以处罚；构成犯罪的，依法追究刑事责任。

第十章 附 则

第七十二条 本条例自2021年9月1日起施行。

深圳经济特区数据条例

基本信息：	
【发布机关】深圳市司法局	【时效性】 未施行
【发布文号】深圳市第七届人民代表大会常务委员会公告第10号	【效力级别】经济特区法规
【发布日期】2021.07.06	【实施日期】2022.01.01

（2021年6月29日深圳市第七届人民代表大会常务委员会第二次会议通过）

第一章 总则

第一条 为了规范数据处理活动，保护自然人、法人和非法人组织的合法权益，促进数据作为生产要素开放流动和开发利用，加快建设数字经济、数字社会、数字政府，根据有关法律、行政法规的基本原则，结合深圳经济特区实际，制定本条例。

第二条 本条例中下列用语的含义：

（一）数据，是指任何以电子或者其他方式对信息的记录。

（二）个人数据，是指载有可识别特定自然人信息的数据，不包括匿名化处理后的数据。

（三）敏感个人数据，是指一旦泄露、非法提供或者滥用，可能导致自然人受到歧视或者人身、财产安全受到严重危害的个人数据，具体范围依照法律、行政法规的规定确定。

（四）生物识别数据，是指对自然人的身体、生理、行为等生物特征进行处理而得出的能够识别自然人独特标识的个人数据，包括自然人的基因、指纹、声纹、掌纹、耳廓、虹膜、面部识别特征等数据。

（五）公共数据，是指公共管理和服务机构在依法履行公共管理职责或者提供公共服务过程中产生、处理的数据。

（六）数据处理，是指数据的收集、存储、使用、加工、传输、提供、开放等活动。

（七）匿名化，是指个人数据经过处理无法识别特定自然人且不能复原的过程。

（八）用户画像，是指为了评估自然人的某些条件而对个人数据进行自动化处理的活动，包括为了评估自然人的工作表现、经济状况、健康状况、个人偏好、兴趣、可靠性、行为方式、位置、行踪等进行的自动化处理。

（九）公共管理和服务机构，是指本市国家机关、事业单位和其他依法管理公共事务的组织，以及提供教育、卫生健康、社会福利、供水、供电、供气、环境保护、公共交通和其他公共服务的组织。

第三条 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。

处理个人数据应当具有明确、合理的目的，并遵循最小必要和合理期限原则。

第四条 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。但是，不得危害国家安全和公共利益，不得损害他人的合法权益。

安证合规集团&北源律师事务所

第五条 处理公共数据应当遵循依法收集、统筹管理、按需共享、有序开放、充分利用的原则，充分发挥公共数据资源对优化公共管理和服务、提升城市治理现代化水平、促进经济社会发展的积极作用。

第六条 市人民政府应当建立健全数据治理制度和标准体系，统筹推进个人数据保护、公共数据共享开放、数据要素市场培育及数据安全监督管理工作。

第七条 市人民政府设立市数据工作委员会，负责研究、协调本市数据管理工作中的重大事项。市数据工作委员会的日常工作由市政务服务数据管理部门承担。

市数据工作委员会可以设立若干专业委员会。

第八条 市网信部门负责统筹协调本市个人数据保护、网络数据安全、跨境数据流通等相关监督管理工作。

市政务服务数据管理部门负责本市公共数据管理的统筹、指导、协调和监督工作。

市发展改革、工业和信息化、公安、财政、人力资源保障、规划和自然资源、市场监管、审计、国家安全等部门依照有关法律、法规，在各自职责范围内履行数据监督管理相关职能。

市各行业主管部门负责本行业数据管理工作的统筹、指导、协调和监督。

第二章 个人数据

第一节 一般规定

第九条 处理个人数据应当充分尊重和保障自然人与个人数据相关的各项合法权益。

第十条 处理个人数据应当符合下列要求:

（一）处理个人数据的目的明确、合理，方式合法、正当;

（二）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，不得进行与处理目的无关的个人数据处理;

（三）依法告知个人数据处理的种类、范围、目的、方式等，并依法征得同意;

（四）保证个人数据的准确性和必要的完整性，避免因个人数据不准确、不完整给当事人造成损害;

（五）确保个人数据安全，防止个人数据泄露、毁损、丢失、篡改和非法使用。

安汇合规集团&北源律师事务所

第十一条 本条例第十条第二项所称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，包括但是不限于下列情形：

（一）处理个人数据的种类、范围应当与处理目的有直接关联，不处理该个人数据则处理目的无法实现；

（二）处理个人数据的数量应当为实现处理目的所必需的最少数量；

（三）处理个人数据的频率应当为实现处理目的所必需的最低频率；

（四）个人数据存储期限应当为实现处理目的所必需的最短时间，超出存储期限的，应当对个人数据予以删除或者匿名化，法律、法规另有规定或者经自然人同意的除外；

（五）建立最小授权的访问控制策略，使被授权访问个人数据的人员仅能访问完成职责所需的最少个人数据，且仅具备完成职责所需的最少数据处理权限。

第十二条 数据处理者不得以自然人不同意处理个人数据为由，拒绝向其提供相关核心功能或者服务。但是，该个人数据为提供相关核心功能或者服务所必需的除外。

第十三条 市网信部门应当会同市工业和信息化、公安、市场监管等部门以及相关行业主管部门建立健全个人数据保护监督管理联合工作机制，加强对个人数据保护和相关监督管理工作的统筹和指导；建立个人数据保护投诉举报处理机制，依法处理相关投诉举报。

第二节 告知与同意

第十四条 处理个人数据应当在处理前以通俗易懂、明确具体、易获取的方式向自然人完整、真实、准确地告知下列事项：

（一）数据处理者的姓名或者名称以及联系方式；

（二）处理个人数据的种类和范围；

（三）处理个人数据的目的和方式；

（四）存储个人数据的期限；

（五）处理个人数据可能存在的安全风险以及对其个人数据采取的安全保护措施；

（六）自然人依法享有的相关权利以及行使权利的方式；

（七）法律、法规规定应当告知的其他事项。

安证合规集团&北源律师事务所

处理敏感个人数据的，应当依照前款规定，以更加显著的标识或者突出显示的形式告知处理敏感个人数据的必要性以及对自然人可能产生的影响。

第十五条 紧急情况下为了保护自然人的人身、财产安全等重大合法权益，无法依照本条例第十四条规定进行事前告知的，应当在紧急情况消除后及时告知。

处理个人数据有法律、行政法规规定应当保密或者无需告知情形的，不适用本条例第十四条规定。

第十六条 数据处理者应当在处理个人数据前，征得自然人的同意，并在其同意范围内处理个人数据，但是法律、行政法规以及本条例另有规定的除外。

前款规定应当征得同意的事项发生变更的，应当重新征得同意。

第十七条 数据处理者不得通过误导、欺骗、胁迫或者其他违背自然人真实意愿的方式获取其同意。

第十八条 处理敏感个人数据的，应当在处理前征得该自然人的明示同意。

第十九条 处理生物识别数据的，应当在征得该自然人明示同意时，提供处理其他非生物识别数据的替代方案。但是，处理生物识别数据为处理个人数据目的所必需，且不能为其他个人数据所替代的除外。

基于特定目的处理生物识别数据的，未经自然人明示同意，不得将该生物识别数据用于其他目的。

生物识别数据具体管理办法由市人民政府另行制定。

第二十条 处理未满十四周岁的未成年人个人数据的，按照处理敏感个人数据的有关规定执行，并应当在处理前征得其监护人的明示同意。

处理无民事行为能力或者限制民事行为能力的成年人个人数据的，应当在处理前征得其监护人的明示同意。

第二十一条 处理个人数据有下列情形之一的，可以在处理前不征得自然人的同意：

（一）处理自然人自行公开或者其他已经合法公开的个人数据，且符合该个人数据公开时的目的；

（二）为了订立或者履行自然人作为一方当事人的合同所必需；

安证合规集团&北源律师事务所

（三）数据处理者因人力资源管理、商业秘密保护所必需，在合理范围内处理其员工个人数据；

（四）公共管理和服务机构为了依法履行公共管理职责或者提供公共服务所必需；

（五）新闻单位依法进行新闻报道所必需；

（六）法律、行政法规规定的其他情形。

第二十二条 自然人有权撤回部分或者全部其处理个人数据的同意。

自然人撤回同意的，数据处理者不得继续处理该自然人撤回同意范围内的个人数据。但是，不影响数据处理者在自然人撤回同意前基于同意进行的合法数据处理。法律、法规另有规定的，从其规定。

第二十三条 处理个人数据应当采用易获取的方式提供自然人撤回其同意的途径，不得利用服务协议或者技术等手段对自然人撤回同意进行不合理限制或者附加不合理条件。

第三节 个人数据处理

第二十四条 个人数据不准确或者不完整的，数据处理者应当根据自然人的要求及时补充、更正。

第二十五条 有下列情形之一的，数据处理者应当及时删除个人数据：

（一）法律、法规规定或者约定的存储期限届满；

（二）处理个人数据的目的已经实现或者处理个人数据对于处理目的已经不再必要；

（三）自然人撤回同意且要求删除个人数据；

（四）数据处理者违反法律、法规规定或者双方约定处理数据，自然人要求删除；

（五）法律、法规规定的其他情形。

有前款第一项、第二项规定情形，但是法律、法规另有规定或者经自然人同意的，数据处理者可以保留相关个人数据。

数据处理者根据本条第一款规定删除个人数据的，可以留存告知和同意的证据，但是不得超过其履行法定义务或者处理纠纷需要的必要限度。

第二十六条 数据处理者向他人提供其处理的个人数据，应当对个人数据进行去标识化处理，使得被提供的个人数据在不借助其他数据的情况下无法识别特定自然人。法律、法规规定或

安证合规集团&北源律师事务所

者自然人与数据处理者约定应当匿名化的，数据处理者应当依照法律、法规规定或者双方约定进行匿名化处理。

第二十七条 数据处理者向他人提供其处理的个人数据有下列情形之一的，可以不进行去标识化处理：

（一）应公共管理和服务机构依法履行公共管理职责或者提供公共服务的需要且书面要求提供的；

（二）基于自然人的同意向他人提供相关个人数据的；

（三）为了订立或者履行自然人作为一方当事人的合同所必需的；

（四）法律、行政法规规定的其他情形。

第二十八条 自然人可以向数据处理者要求查阅、复制其个人数据，数据处理者应当按照有关规定及时提供，并不得收取费用。

第二十九条 数据处理者基于提升产品或者服务质量的目的，对自然人进行用户画像的，应当向其明示用户画像的具体用途和主要规则。

自然人可以拒绝数据处理者根据前款规定对其进行用户画像或者基于用户画像推荐个性化产品或者服务，数据处理者应当以易获取的方式向其提供拒绝的有效途径。

第三十条 数据处理者不得基于用户画像向未满十四周岁的未成年人推荐个性化产品或者服务。但是，为了维护其合法权益并征得其监护人明示同意的除外。

第三十一条 数据处理者应当建立自然人行使相关权利和投诉举报的处理机制，并以易获取的方式提供有效途径。

数据处理者收到行使权利要求或者投诉举报的，应当及时受理，并依法采取相应处理措施；拒绝要求事项或者投诉的，应当说明理由。

第三章 公共数据

第一节 一般规定

第三十二条 市数据工作委员会设立公共数据专业委员会，负责研究、协调公共数据管理工作中的重大事项。

安证合规集团&北京律师事务所

市政务服务数据管理部门承担市公共数据专业委员会日常工作，并负责统筹全市公共数据管理工作，建立和完善公共数据资源管理体系，推进公共数据共享、开放和利用。

区政务服务数据管理部门在市政务服务数据管理部门指导下，负责统筹本区公共数据管理工作。

第三十三条 市人民政府应当建立城市大数据中心，建立健全其建设运行管理机制，实现对全市公共数据资源统一、集约、安全、高效管理。

各区人民政府可以按照全市统一规划，建设城市大数据中心分中心，将公共数据资源纳入城市大数据中心统一管理。

城市大数据中心包括公共数据资源和支撑其管理的软硬件基础设施。

第三十四条 市政务服务数据管理部门负责推动公共数据向城市大数据中心汇聚，组织公共管理和服务机构依托城市大数据中心开展公共数据共享、开放和利用。

第三十五条 实行公共数据分类管理制度。

市政务服务数据管理部门负责统筹本市公共数据资源体系整体规划、建设和管理，并会同相关部门建设和管理人口、法人、房屋、自然资源与空间地理、电子证照、公共信用等基础数据库。

各行业主管部门应当按照公共数据资源体系整体规划和相关制度规范要求，规划本行业公共数据资源体系，建设并管理相关主题数据库。

公共管理和服务机构应当按照公共数据资源体系整体规划、行业专项规划和相关制度规范要求，建设、管理本机构业务数据库。

第三十六条 实行公共数据目录管理制度。

市政务服务数据管理部门负责建立全市统一的公共数据资源目录体系，制定公共数据资源目录编制规范，组织公共管理和服务机构按照公共数据资源目录编制规范要求编制目录、处理各类公共数据，明确数据来源部门和管理职责。

公共管理和服务机构应当按照公共数据资源目录编制规范要求，对本机构的公共数据进行目录管理。

第三十七条 公共管理和服务机构收集数据应当符合下列要求：

安理合规集团&北源律师事务所

（一）为依法履行公共管理职责或者提供公共服务所必需，且在其履行的公共管理职责或者提供的公共服务范围内；

（二）收集数据的种类和范围与其依法履行的公共管理职责或者提供的公共服务相适应；

（三）收集程序符合法律、法规相关规定。

公共管理和服务机构可以通过共享方式获得的数据，不得另行向自然人、法人和非法人组织收集。

第三十八条 公共管理和服务机构应当按照有关规定保存公共数据处理的过程记录。

第三十九条 市政务服务数据管理部门应当组织制定公共数据质量管理制度和规范，建立健全质量监测和评估体系，并组织实施。

公共管理和服务机构应当按照公共数据质量管理制度和规范，建立和完善本机构数据质量管理体系，加强数据质量管理，保障数据真实、准确、完整、及时、可用。

市公共数据专业委员会应当定期对公共管理和服务机构数据管理工作进行评价，并向市数据工作委员会报告评价结果。

第四十条 市人民政府应当加强公共数据共享、开放和利用体制机制和技术创新，不断提高公共数据共享、开放和利用的质量与效率。

第二节 公共数据共享

第四十一条 公共数据应当以共享为原则，不共享为例外。

市政务服务数据管理部门应当建立以公共数据资源目录体系为基础的公共数据共享需求对接机制和相关管理制度。

第四十二条 纳入公共数据共享目录的公共数据，应当按照有关规定通过城市大数据中心的公共数据共享平台在有需要的公共管理和服务机构之间及时、准确共享，法律、法规另有规定的除外。

公共数据共享目录由市政务服务数据管理部门另行制定，并及时调整。

第四十三条 公共管理和服务机构可以根据依法履行公共管理职责或者提供公共服务的需要提出公共数据共享申请，明确数据使用的依据、目的、范围、方式及相关需求，并按照本级政务

安证合规集团&北源律师事务所

服务数据管理部门和数据提供部门的要求，加强共享数据使用管理，不得超出使用范围或者用于其他目的。

公共数据提供部门应当在规定时间内，回应公共数据使用部门的共享需求，并提供必要的数据使用指导和技术支持。

第四十四条 公共管理和服务机构依法履行公共管理职责或者提供公共服务所需要的数据，无法通过公共数据共享平台共享获得的，可以由市人民政府统一对外采购，并按照有关规定纳入公共数据共享目录，具体工作由市政务服务数据管理部门统筹。

第三节 公共数据开放

第四十五条 本条例所称公共数据开放，是指公共管理和服务机构通过公共数据开放平台向社会提供可机器读取的公共数据的活动。

第四十六条 公共数据开放应当遵循分类分级、需求导向、安全可控的原则，在法律、法规允许范围内最大限度开放。

第四十七条 依照法律、法规规定开放公共数据，不得收取任何费用。法律、行政法规另有规定的，从其规定。

第四十八条 公共数据按照开放条件分为无条件开放、有条件开放和不予开放三类。

无条件开放的公共数据，是指应当无条件向自然人、法人和非法人组织开放的公共数据；有条件开放的公共数据，是指按照特定方式向自然人、法人和非法人组织平等开放的公共数据；不予开放的公共数据，是指涉及国家安全、商业秘密和个人隐私,或者法律、法规等规定不得开放的公共数据。

第四十九条 市政务服务数据管理部门应当建立以公共数据资源目录体系为基础的公共数据开放管理制度，编制公共数据开放目录并及时调整。

有条件开放的公共数据，应当在编制公共数据开放目录时明确开放方式、使用要求及安全保障措施等。

第五十条 市政务服务数据管理部门应当依托城市大数据中心建设统一、高效的公共数据开放平台，并组织公共管理和服务机构通过该平台向社会开放公共数据。

公共数据开放平台应当根据公共数据开放类型，提供数据下载、应用程序接口和安全可信的数据综合开发利用环境等多种数据开放服务。

安汇合规集团&北源律师事务所

第四节 公共数据利用

第五十一条 市人民政府应当加快推进数字政府建设，深化数据在经济调节、市场监管、社会管理、公共服务、生态环境保护中的应用，建立和完善运用数据管理的制度规则，创新政府决策、监管及服务模式，实现主动、精准、整体式、智能化的公共管理和服务。

第五十二条 市人民政府应当依托城市大数据中心建设基于统一架构的业务中枢、数据中枢和能力中枢，形成统一的城市智能中枢平台体系，为公共管理和服务以及各区域各行业应用提供统一、全面的数字化服务，促进技术融合、业务融合、数据融合。

市人民政府可以依托城市智能中枢平台建设政府管理服务指挥中心，建立和完善运行管理机制，推动政府整体数字化转型，深化跨层级、跨地域、跨系统、跨部门、跨业务的数据共享和业务协同，建立统一指挥、一体联动、智能精准、科学高效的政府运行体系。

各行业主管部门应当依托城市智能中枢平台建设本行业管理服务平台，推动本行业管理服务全面数字化。

各区人民政府应当依托城市智能中枢平台，以服务基层为目标，整合数据资源、优化业务流程、创新管理模式，推进基层治理与服务科学化、精细化、智能化。

第五十三条 市人民政府应当依托城市智能中枢平台，推动业务整合和流程再造，深化前台统一受理、后台协同审批、全市一体运作的整体式政务服务模式创新。

市政务服务数据管理部门应当推动公共管理和服务机构加强公共数据在公共管理和服务过程中的创新应用，精简办事材料、环节，优化办事流程；对于可以通过数据比对作出审批决定的事项，可以开展无人干预智能审批。

第五十四条 市人民政府应当依托城市智能中枢平台，加强监管数据和信用数据归集、共享，充分利用公共数据和各领域监管系统，推行非现场监管、信用监管、风险预警等新型监管模式，提升监管水平。

第五十五条 市政务服务数据管理部门可以组织建设数据融合应用服务平台，向社会提供安全可信的数据综合开发利用环境，共同开展智慧城市应用创新。

第四章 数据要素市场

第一节 一般规定

安证合规集团&北源律师事务所

第五十六条 市人民政府应当统筹规划，加快培育数据要素市场，推动构建数据收集、加工、共享、开放、交易、应用等数据要素市场体系，促进数据资源有序、高效流动与利用。

第五十七条 市场主体开展数据处理活动，应当落实数据管理主体责任，建立健全数据治理组织架构、管理制度和自我评估机制，对数据实施分类分级保护和管理，加强数据质量管理，确保数据的真实性、准确性、完整性、时效性。

第五十八条 市场主体对合法处理数据形成的数据产品和服务，可以依法自主使用，取得收益，进行处分。

第五十九条 市场主体向第三方开放或者提供使用个人数据的，应当遵守本条例第二章的有关规定；向特定第三方开放、委托处理、提供使用个人数据的，应当签订相关协议。

第六十条 使用、传输、受委托处理其他市场主体的数据产品和服务，涉及个人数据的，应当遵守本条例第二章的规定以及相关协议的约定。

第二节 市场培育

第六十一条 市人民政府应当组织制定数据处理活动合规标准、数据产品和服务标准、数据质量标准、数据安全标准、数据价值评估标准、数据治理评估标准等地方标准。

支持数据相关行业组织制定团体标准和行业规范，提供信息、技术、培训等服务，引导和督促市场主体规范其数据行为，促进行业健康发展。

鼓励市场主体制定数据相关企业标准，参与制定相关地方标准和团体标准。

第六十二条 数据处理者可以委托第三方机构进行数据质量评估认证；第三方机构应当按照独立、公开、公正原则，开展数据质量评估认证活动。

第六十三条 鼓励数据价值评估机构从实时性、时间跨度、样本覆盖面、完整性、数据种类级别和数据挖掘潜能等方面，探索构建数据资产定价指标体系，推动制定数据价值评估准则。

第六十四条 市统计部门应当探索建立数据生产要素统计核算制度，明确统计范围、统计指标和统计方法，准确反映数据生产要素的资产价值，推动将数据生产要素纳入国民经济核算体系。

第六十五条 市人民政府应当推动建立数据交易平台，引导市场主体通过数据交易平台进行数据交易。

安证合规集团&北源律师事务所

市场主体可以通过依法设立的数据交易平台进行数据交易，也可以由交易双方依法自行交易。

第六十六条 数据交易平台应当建立安全、可信、可控、可追溯的数据交易环境，制定数据交易、信息披露、自律监管等规则，并采取有效措施保护个人数据、商业秘密和国家规定的重要数据。

第六十七条 市场主体合法处理数据形成的数据产品和服务，可以依法交易。但是，有下列情形之一的除外：

（一）交易的数据产品和服务包含个人数据未依法获得授权的；

（二）交易的数据产品和服务包含未经依法开放的公共数据的；

（三）法律、法规规定禁止交易的其他情形。

第三节 公平竞争

第六十八条 市场主体应当遵守公平竞争原则，不得实施下列侵害其他市场主体合法权益的行为：

（一）使用非法手段获取其他市场主体的数据；

（二）利用非法收集的其他市场主体数据提供替代性产品或者服务；

（三）法律、法规规定禁止的其他行为。

第六十九条 市场主体不得利用数据分析，对交易条件相同的交易相对人实施差别待遇，但是有下列情形之一的除外：

（一）根据交易相对人的实际需求，且符合正当的交易习惯和行业惯例，实行不同交易条件的；

（二）针对新用户在合理期限内开展优惠活动的；

（三）基于公平、合理、非歧视规则实施随机性交易的；

（四）法律、法规规定的其他情形。

前款所称交易条件相同，是指交易相对人在交易安全、交易成本、信用状况、交易环节、交易持续时间等方面不存在实质性差别。

安证合规集团&北源律师事务所

第七十条 市场主体不得通过达成垄断协议、滥用在数据要素市场的支配地位、违法实施经营者集中等方式，排除、限制竞争。

第五章 数据安全

第一节 一般规定

第七十一条 数据安全管理遵循政府监管、责任主体负责、积极防御、综合防范的原则，坚持安全和发展并重，鼓励研发数据安全技术，保障数据全生命周期安全。

市人民政府应当统筹全市数据安全管理工作，建立和完善数据安全综合治理体系。

第七十二条 数据处理者应当依照法律、法规规定，建立健全数据分类分级、风险监测、安全评估、安全教育等安全管理制度，落实保障措施，不断提升技术手段，确保数据安全。

数据处理者因合并、分立、收购等变更的，由变更后的数据处理者继续落实数据安全管理责任。

第七十三条 处理敏感个人数据或者国家规定的重要数据的，应当按照有关规定设立数据安全管理机构、明确数据安全管理责任人，并实施特别技术保护。

第七十四条 市网信部门应当统筹协调相关主管部门和行业主管部门按照国家数据分类分级保护制度制定本部门、本行业的重要数据具体目录，对列入目录的数据进行重点保护。

第二节 数据安全管理

第七十五条 数据处理者应当对其数据处理全流程进行记录，保障数据来源合法以及处理全流程清晰、可追溯。

第七十六条 数据处理者应当依照法律、法规规定以及国家标准的要求，对所收集的个人数据进行去标识化或者匿名化处理，并与可用于恢复识别特定自然人的数据分开存储。

数据处理者应当针对敏感个人数据、国家规定的重要数据制定并实施去标识化或者匿名化处理等安全措施。

第七十七条 数据处理者应当对数据存储进行分域分级管理，选择安全性能、防护级别与安全等级相匹配的存储载体；对敏感个人数据和国家规定的重要数据还应当采取加密存储、授权访问或者其他更加严格的安全保护措施。

安证合规集团&北京律师事务所

第七十八条 数据处理者应当对数据处理过程实施安全技术防护，并建立重要系统和核心数据的容灾备份制度。

第七十九条 数据处理者共享、开放数据的，应当建立数据共享、开放安全管理制度，建立和完善对外数据接口的安全管理机制。

第八十条 数据处理者应当建立数据销毁规程,对需要销毁的数据实施有效销毁。

数据处理者终止或者解散，没有数据承接方的，应当及时有效销毁其控制的数据。法律、法规另有规定的除外。

第八十一条 数据处理者委托他人代为处理数据的，应当与其订立数据安全保护合同，明确双方安全保护责任。

受托方完成处理任务后，应当及时有效销毁其存储的数据，但是法律、法规另有规定或者双方另有约定的除外。

第八十二条 数据处理者向境外提供个人数据或者国家规定的重要数据，应当按照有关规定申请数据出境安全评估，进行国家安全审查。

第八十三条 数据处理者应当落实与数据安全防护级别相适应的监测预警措施，对数据泄露、毁损、丢失、篡改等异常情况进行监测和预警。

监测到发生或者可能发生数据泄露、毁损、丢失、篡改等数据安全事件的，数据处理者应当立即采取补救、预防措施。

第八十四条 处理敏感个人数据或者国家规定的重要数据，应当按照有关规定定期开展风险评估，并向有关主管部门报送风险评估报告。

第八十五条 数据处理者应当建立数据安全应急处置机制，制定数据安全应急预案。数据安全应急预案应当按照危害程度、影响范围等因素对数据安全事件进行分级，并规定相应的应急处置措施。

第八十六条 发生数据泄露、毁损、丢失、篡改等数据安全事件的，数据处理者应当立即启动应急预案，采取相应的应急处置措施，及时告知相关权利人，并按照有关规定向市网信、公安部门和有关行业主管部门报告。

第三节 数据安全监督

安证合规集团&北源律师事务所

第八十七条 市网信部门应当依照有关法律、行政法规以及本条例规定负责统筹协调数据安全和相关监督工作，并会同市公安、国家安全等部门和有关行业主管部门建立健全数据安全监督机制，组织数据安全监督检查。

第八十八条 市网信部门应当会同有关主管部门加强数据安全风险分析、预测、评估，收集相关信息；发现可能导致较大范围数据泄露、毁损、丢失、篡改等数据安全事件的，应当及时发布预警信息，提出防范应对措施，指导、监督数据处理者做好数据安全保护工作。

第八十九条 市网信部门以及其他履行数据安全监督职责的部门可以委托第三方机构，按照法律、法规规定和相关标准要求，对数据处理者开展数据安全管理认证以及数据安全评估工作，并对其进行安全等级评定。

第九十条 市网信部门以及其他履行数据安全监督职责的部门在履行职责过程中，发现数据处理者未按照规定落实安全管理责任的，应当按照规定约谈数据处理者，督促其整改。

第九十一条 市网信部门以及其他数据监督管理部门及其工作人员，应当对在履行职责过程中知悉的个人数据、商业秘密和需要保守秘密的其他数据严格保密，不得泄露、出售或者非法向他人提供。

第六章 法律责任

第九十二条 违反本条例规定处理个人数据的，依照个人信息保护有关法律、法规规定处罚。

第九十三条 公共管理和服务机构违反本条例有关规定的，由上级主管部门或者有关主管部门责令改正；拒不改正或者造成严重后果的，依法追究法律责任；因此给自然人、法人、非法人组织造成损失的，应当依法承担赔偿责任。

第九十四条 违反本条例第六十七条规定交易数据的，由市市场监督管理部门或者相关行业主管部门按照职责责令改正，没收违法所得，交易金额不足一万元的，处五万元以上二十万元以下罚款；交易金额一万元以上的，处二十万元以上一百万元以下罚款；并可以依法给予法律、行政法规规定的其他行政处罚。法律、行政法规另有规定的，从其规定。

第九十五条 违反本条例第六十八条、第六十九条规定，侵害其他市场主体、消费者合法权益的，由市市场监督管理部门或者相关行业主管部门按照职责责令改正，没收违法所得；拒不改正的，处五万元以上五十万元以下罚款；情节严重的，处上一年度营业额百分之五以下罚款，最

安证合规集团&北清律师事务所

高不超过五千万元；并可以依法给予法律、行政法规规定的其他行政处罚。法律、行政法规另有规定的，从其规定。

市场主体违反本条例第七十条规定，有不正当竞争行为或者垄断行为的，依照反不正当竞争或者反垄断有关法律、法规规定处罚。

第九十六条 数据处理者违反本条例规定，未履行数据安全保护责任的，依照数据安全有关法律、法规规定处罚。

第九十七条 履行数据监督管理职责的部门以及公共管理和服务机构不履行或者不正确履行本条例规定职责的，对直接负责的主管人员和其他直接责任人员依法给予处分；构成犯罪的，依法追究刑事责任。

第九十八条 违反本条例规定处理数据，致使国家利益或者公共利益受到损害的，法律、法规规定的组织可以依法提起民事公益诉讼。法律、法规规定的组织提起民事公益诉讼，人民检察院认为有必要的，可以支持起诉。

法律、法规规定的组织未提起民事公益诉讼的，人民检察院可以依法提起民事公益诉讼。

人民检察院发现履行数据监督管理职责的部门违法行使职权或者不作为，致使国家利益或者公共利益受到损害的，应当向有关行政机关提出检察建议；行政机关不依法履行职责的，人民检察院可以依法提起行政公益诉讼。

第九十九条 数据处理者违反本条例规定处理数据，给他人造成损害的，应当依法承担民事责任；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。

第七章 附则

第一百条 本条例自2022年1月1日起施行。

安证合规集团&北源律师事务所

安证合规集团&北源律师事务所

第四篇 规章

电信和互联网用户个人信息保护规定

基本信息：	
【发布机关】工业和信息化部	【时效性】 现行有效
【发文字号】工业和信息化部令第24号	【效力级别】部门规章
【发布日期】2013.07.16	【实施日期】2013.09.01

电信和互联网用户个人信息保护规定

第一章 总则

第一条 为了保护电信和互联网用户的合法权益，维护网络信息安全，根据《全国人民代表大会常务委员会关于加强网络信息保护的决定》、《中华人民共和国电信条例》和《互联网信息服务管理办法》等法律、行政法规，制定本规定。

第二条 在中华人民共和国境内提供电信服务和互联网信息服务过程中收集、使用用户个人信息的活动，适用本规定。

第三条 工业和信息化部和各省、自治区、直辖市通信管理局（以下统称电信管理机构）依法对电信和互联网用户个人信息保护工作实施监督管理。

第四条 本规定所称用户个人信息，是指电信业务经营者和互联网信息服务提供者在提供服务的过程中收集的用户姓名、出生日期、身份证件号码、住址、电话号码、账号和密码等能够单独或者与其他信息结合识别用户的信息以及用户使用服务的时间、地点等信息。

第五条 电信业务经营者、互联网信息服务提供者在提供服务的过程中收集、使用用户个人信息，应当遵循合法、正当、必要的原则。

第六条 电信业务经营者、互联网信息服务提供者对其在提供服务过程中收集、使用的用户个人信息的安全负责。

第七条 国家鼓励电信和互联网行业开展用户个人信息保护自律工作。

第二章 信息收集和使用规范

第八条 电信业务经营者、互联网信息服务提供者应当制定用户个人信息收集、使用规则，并在其经营或者服务场所、网站等予以公布。

第九条 未经用户同意，电信业务经营者、互联网信息服务提供者不得收集、使用用户个人信息。

实证合规集团&北源律师事务所

电信业务经营者、互联网信息服务提供者收集、使用用户个人信息的，应当明确告知用户收集、使用信息的目的、方式和范围，查询、更正信息的渠道以及拒绝提供信息的后果等事项。

电信业务经营者、互联网信息服务提供者不得收集其提供服务所必需以外的用户个人信息或者将信息用于提供服务之外的目的，不得以欺骗、误导或者强迫等方式或者违反法律、行政法规以及双方的约定收集、使用信息。

电信业务经营者、互联网信息服务提供者在用户终止使用电信服务或者互联网信息服务后，应当停止对用户个人信息的收集和使用，并为用户提供注销号码或者账号的服务。

法律、行政法规对本条第一款至第四款规定的情形另有规定的，从其规定。

第十条 电信业务经营者、互联网信息服务提供者及其工作人员对在提供服务过程中收集、使用的用户个人信息应当严格保密，不得泄露、篡改或者毁损，不得出售或者非法向他人提供。

第十一条 电信业务经营者、互联网信息服务提供者委托他人代理市场销售和技术服务等直接面向用户的服务性工作，涉及收集、使用用户个人信息的，应当对代理人的用户个人信息保护工作进行监督和管理，不得委托不符合本规定有关用户个人信息保护要求的代理人代办相关服务。

第十二条 电信业务经营者、互联网信息服务提供者应当建立用户投诉处理机制，公布有效的联系方式，接受与用户个人信息保护有关的投诉，并自接到投诉之日起十五日内答复投诉人。

第三章　安全保障措施

第十三条 电信业务经营者、互联网信息服务提供者应当采取以下措施防止用户个人信息泄露、毁损、篡改或者丢失：

（一）确定各部门、岗位和分支机构的用户个人信息安全管理责任；

（二）建立用户个人信息收集、使用及其相关活动的工作流程和安全管理制度；

（三）对工作人员及代理人实行权限管理，对批量导出、复制、销毁信息实行审查，并采取防泄密措施；

（四）妥善保管记录用户个人信息的纸介质、光介质、电磁介质等载体，并采取相应的安全储存措施；

（五）对储存用户个人信息的信息系统实行接入审查，并采取防入侵、防病毒等措施；

（六）记录对用户个人信息进行操作的人员、时间、地点、事项等信息；

（七）按照电信管理机构的规定开展通信网络安全防护工作；

（八）电信管理机构规定的其他必要措施。

第十四条 电信业务经营者、互联网信息服务提供者保管的用户个人信息发生或者可能发生泄露、毁损、丢失的，应当立即采取补救措施；造成或者可能造成严重后果的，应当立即向准予

安证合规集团&北源律师事务所

其许可或者备案的电信管理机构报告，配合相关部门进行的调查处理。

电信管理机构应当对报告或者发现的可能违反本规定的行为的影响进行评估；影响特别重大的，相关省、自治区、直辖市通信管理局应当向工业和信息化部报告。电信管理机构在依据本规定作出处理决定前，可以要求电信业务经营者和互联网信息服务提供者暂停有关行为，电信业务经营者和互联网信息服务提供者应当执行。

第十五条 电信业务经营者、互联网信息服务提供者应当对其工作人员进行用户个人信息保护相关知识、技能和安全责任培训。

第十六条 电信业务经营者、互联网信息服务提供者应当对用户个人信息保护情况每年至少进行一次自查，记录自查情况，及时消除自查中发现的安全隐患。

第四章　监督检查

第十七条 电信管理机构应当对电信业务经营者、互联网信息服务提供者保护用户个人信息的情况实施监督检查。

电信管理机构实施监督检查时，可以要求电信业务经营者、互联网信息服务提供者提供相关材料，进入其生产经营场所调查情况，电信业务经营者、互联网信息服务提供者应当予以配合。

电信管理机构实施监督检查，应当记录监督检查的情况，不得妨碍电信业务经营者、互联网信息服务提供者正常的经营或者服务活动，不得收取任何费用。

第十八条 电信管理机构及其工作人员对在履行职责中知悉的用户个人信息应当予以保密，不得泄露、篡改或者毁损，不得出售或者非法向他人提供。

第十九条 电信管理机构实施电信业务经营许可及经营许可证年检时，应当对用户个人信息保护情况进行审查。

第二十条 电信管理机构应当将电信业务经营者、互联网信息服务提供者违反本规定的行为记入其社会信用档案并予以公布。

第二十一条 鼓励电信和互联网行业协会依法制定有关用户个人信息保护的自律性管理制度，引导会员加强自律管理，提高用户个人信息保护水平。

第五章　法律责任

第二十二条 电信业务经营者、互联网信息服务提供者违反本规定第八条、第十二条规定的，由电信管理机构依据职权责令限期改正，予以警告，可以并处一万元以下的罚款。

第二十三条 电信业务经营者、互联网信息服务提供者违反本规定第九条至第十一条、第十三条至第十六条、第十七条第二款规定的，由电信管理机构依据职权责令限期改正，予以警告，可以并处一万元以上三万元以下的罚款，向社会公告；构成犯罪的，依法追究刑事责任。

安证合规集团&北源律师事务所

第二十四条 电信管理机构工作人员在对用户个人信息保护工作实施监督管理的过程中玩忽职守、滥用职权、徇私舞弊的，依法给予处理；构成犯罪的，依法追究刑事责任。

第六章　附则

第二十五条 本规定自2013年9月1日起施行。

儿童个人信息网络保护规定

基本信息：	
【发布机关】国家互联网信息办公室	【时效性】 现行有效
【发文字号】-	【效力级别】部门规章
【发布日期】2019年8月22日	【实施日期】2019年10月1日

国家互联网信息办公室令

第4号

《儿童个人信息网络保护规定》已经国家互联网信息办公室室务会议审议通过，现予公布，自2019年10月1日起施行。

主任 庄荣文

2019年8月22日

儿童个人信息网络保护规定

第一条 为了保护儿童个人信息安，促进儿童健康成长，根据《中华人民共和国网络安全法》《中华人民共和国未成年人保护法》等法律法规，制定本规定。

第二条 本s规定所称儿童，是指不满十四周岁的未成年人。

第三条 在中华人民共和国境内通过网络从事收集、存储、使用、转移、披露儿童个人信息等活动，适用本规定。

第四条 任何组织和个人不得制作、发布、传播侵害儿童个人信息安全的信息。

第五条 儿童监护人应当正确履行监护职责，教育引导儿童增强个人信息保护意识和能力，保护儿童个人信息安全。

第六条 鼓励互联网行业组织指导推动网络运营者制定儿童个人信息保护的行业规范、行为

准则等，加强行业自律，履行社会责任。

第七条 网络运营者收集、存储、使用、转移、披露儿童个人信息的，应当遵循正当必要、知情同意、目的明确、安全保障、依法利用的原则。

第八条 网络运营者应当设置专门的儿童个人信息保护规则和用户协议，并指定专人负责儿童个人信息保护。

第九条 网络运营者收集、使用、转移、披露儿童个人信息的，应当以显著、清晰的方式告知儿童监护人，并应当征得儿童监护人的同意。

第十条 网络运营者征得同意时，应当同时提供拒绝选项，并明确告知以下事项：

（一）收集、存储、使用、转移、披露儿童个人信息的目的、方式和范围；

（二）儿童个人信息存储的地点、期限和到期后的处理方式；

（三）儿童个人信息的安全保障措施；

（四）拒绝的后果；

（五）投诉、举报的渠道和方式；

（六）更正、删除儿童个人信息的途径和方法；

（七）其他应当告知的事项。

前款规定的告知事项发生实质性变化的，应当再次征得儿童监护人的同意。

第十一条 网络运营者不得收集与其提供的服务无关的儿童个人信息，不得违反法律、行政法规的规定和双方的约定收集儿童个人信息。

第十二条 网络运营者存储儿童个人信息，不得超过实现其收集、使用目的所必需的期限。

第十三条 网络运营者应当采取加密等措施存储儿童个人信息，确保信息安全。

第十四条 网络运营者使用儿童个人信息，不得违反法律、行政法规的规定和双方约定的目的、范围。因业务需要，确需超出约定的目的、范围使用的，应当再次征得儿童监护人的同意。

第十五条 网络运营者对其工作人员应当以最小授权为原则，严格设定信息访问权限，控制儿童个人信息知悉范围。工作人员访问儿童个人信息的，应当经过儿童个人信息保护负责人或者其授权的管理人员审批，记录访问情况，并采取技术措施，避免违法复制、下载儿童个人信息。

第十六条 网络运营者委托第三方处理儿童个人信息的，应当对受委托方及委托行为等进行安全评估，签署委托协议，明确双方责任、处理事项、处理期限、处理性质和目的等，委托行为不得超出授权范围。

前款规定的受委托方，应当履行以下义务：

（一）按照法律、行政法规的规定和网络运营者的要求处理儿童个人信息；

安证合规集团&北源律师事务所

（二）协助网络运营者回应儿童监护人提出的申请；

（三）采取措施保障信息安全，并在发生儿童个人信息泄露安全事件时，及时向网络运营者反馈；

（四）委托关系解除时及时删除儿童个人信息；

（五）不得转委托；

（六）其他依法应当履行的儿童个人信息保护义务。

第十七条 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。

第十八条 网络运营者不得披露儿童个人信息，但法律、行政法规规定应当披露或者根据与儿童监护人的约定可以披露的除外。

第十九条 儿童或者其监护人发现网络运营者收集、存储、使用、披露的儿童个人信息有错误的，有权要求网络运营者予以更正。网络运营者应当及时采取措施予以更正。

第二十条 儿童或者其监护人要求网络运营者删除其收集、存储、使用、披露的儿童个人信息的，网络运营者应当及时采取措施予以删除，包括但不限于以下情形：

（一）网络运营者违反法律、行政法规的规定或者双方的约定收集、存储、使用、转移、披露儿童个人信息的；

（二）超出目的范围或者必要期限收集、存储、使用、转移、披露儿童个人信息的；

（三）儿童监护人撤回同意的；

（四）儿童或者其监护人通过注销等方式终止使用产品或者服务的。

第二十一条 网络运营者发现儿童个人信息发生或者可能发生泄露、毁损、丢失的，应当立即启动应急预案，采取补救措施；造成或者可能造成严重后果的，应当立即向有关主管部门报告，并将事件相关情况以邮件、信函、电话、推送通知等方式告知受影响的儿童及其监护人，难以逐一告知的，应当采取合理、有效的方式发布相关警示信息。

第二十二条 网络运营者应当对网信部门和其他有关部门依法开展的监督检查予以配合。

第二十三条 网络运营者停止运营产品或者服务的，应当立即停止收集儿童个人信息的活动，删除其持有的儿童个人信息，并将停止运营的通知及时告知儿童监护人。

第二十四条 任何组织和个人发现有违反本规定行为的，可以向网信部门和其他有关部门举报。

网信部门和其他有关部门收到相关举报的，应当依据职责及时进行处理。

第二十五条 网络运营者落实儿童个人信息安全管理责任不到位，存在较大安全风险或者发

安证合规集团&北源律师事务所

生安全事件的，由网信部门依据职责进行约谈，网络运营者应当及时采取措施进行整改，消除隐患。

第二十六条 违反本规定的，由网信部门和其他有关部门依据职责，根据《中华人民共和国网络安全法》《互联网信息服务管理办法》等相关法律法规规定处理；构成犯罪的，依法追究刑事责任。

第二十七条 违反本规定被追究法律责任的，依照有关法律、行政法规的规定记入信用档案，并予以公示。

第二十八条 通过计算机信息系统自动留存处理信息且无法识别所留存处理的信息属于儿童个人信息的，依照其他有关规定执行。

第二十九条 本规定自2019年10月1日起施行。

安证合规集团&北源律师事务所

汽车数据安全管理若干规定(试行)

基本信息:

【发布机关】 国家互联网信息办公室　　【时效性】 现行有效

【发文字号】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、中华人民共和国交通运输部令第7号　　【效力级别】部门规章

【实施日期】2021.10.01

【发布日期】2021.08.16

汽车数据安全管理若干规定(试行)

第一条 为了规范汽车数据处理活动，保护个人、组织的合法权益，维护国家安全和社会公共利益， 促进汽车数据合理开发利用，根据《中华人民共和国网络安全法》、《中华人民共和国数据安全法》等法 律、行政法规，制定本规定。

第二条 在中华人民共和国境内开展汽车数据处理活动及其安全监管，应当遵守相关法律、行政法规和本规定的要求。

第三条 本规定所称汽车数据，包括汽车设计、生产、销售、使用、运维等过程中的涉及个人信息数据和重要数据。

汽车数据处理，包括汽车数据的收集、存储、使用、加工、传输、提供、公开等。

汽车数据处理者，是指开展汽车数据处理活动的组织，包括汽车制造商、零部件和软件供应商、经销 商、维修机构以及出行服务企业等。

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车主、驾驶人、乘车人、车外人员 等有关的各种信息，不包括匿名化处理后的信息。

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。

重要数据是指一旦遭到篡改、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，包括:

（一）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

安汇合规集团&北源律师事务所

流量、车 辆流量等数据；

（二）车辆流量、物流等反映经济运行情况的数据；

（三）汽车充电网的运行数据；

（四）包含人脸信息、车牌信息等的车外视频、图像数据；

（五）涉及个人信息主体超过10万人的个人信息；

（六）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。

第四条 汽车数据处理者处理汽车数据应当合法、正当、具体、明确，与汽车的设计、生产、销售、使用、运维等直接相关。

第五条 利用互联网等信息网络开展汽车数据处理活动，应当落实网络安全等级保护等制度，加强汽 车数据保护，依法履行数据安全义务。

第六条 国家鼓励汽车数据依法合理有效利用，倡导汽车数据处理者在开展汽车数据处理活动中坚持：

（一）车内处理原则，除非确有必要不向车外提供；

（二）默认不收集原则，除非驾驶人自主设定，每次驾驶时默认设定为不收集状态；

（三）精度范围适用原则，根据所提供功能服务对数据精度的要求确定摄像头、雷达等的覆盖范围、 分辨率；

（四）脱敏处理原则，尽可能进行匿名化、去标识化等处理。

第七条 汽车数据处理者处理个人信息应当通过用户手册、车载显示面板、语音、汽车使用相关应用程序等显著方式，告知个人以下事项：

（一）处理个人信息的种类，包括车辆行踪轨迹、驾驶习惯、音频、视频、图像和生物识别特征等；

（二）收集各类个人信息的具体情境以及停止收集的方式和途径；

（三）处理各类个人信息的目的、用途、方式；

（四）个人信息保存地点、保存期限，或者确定保存地点、保存期限的规则；

安汇合规集团&北源律师事务所

（五）查阅、复制其个人信息以及删除车内、请求删除已经提供给车外的个人信息的方式和途径；

（六）用户权益事务联系人的姓名和联系方式；

（七）法律、行政法规规定的应当告知的其他事项。

第八条汽车数据处理者处理个人信息应当取得个人同意或者符合法律、行政法规规定的其他情形。 因保证行车安全需要，无法征得个人同意采集到车外个人信息且向车外提供的，应当进行匿名化理，包括删除含有能够识别自然人的画面，或者对画面中的人脸信息等进行局部轮廓化处理等。

第九条 汽车数据处理者处理敏感个人信息，应当符合以下要求或者符合法律、行政法规和强制性国 家标准等其他要求：

（一）具有直接服务于个人的目的，包括增强行车安全、智能驾驶、导航等；

（二）通过用户手册、车载显示面板、语音以及汽车使用相关应用程序等显著方式告知必要性以及对 个人的影响；

（三）应当取得个人单独同意，个人可以自主设定同意期限；

（四）在保证行车安全的前提下，以适当方式提示收集状态，为个人终止收集提供便利；

（五）个人要求删除的，汽车数据处理者应当在十个工作日内删除。

汽车数据处理者具有增强行车安全的目的和充分的必要性，方可收集指纹、声纹、人脸、心律等生物识别特征信息。

第十条 汽车数据处理者开展重要数据处理活动，应当按照规定开展风险评估，并向省、自治区、直辖市网信部门和有关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、范围、保存地点与期限、使用方式，开展数据处理活动情况以及是否向第三方提供，面临的数据安全风险及其应对措施等。

第十一条 重要数据应当依法在境内存储，因业务需要确需向境外提供的，应当通过国家网信部门会同国务院有关部门组织的安全评估。未列入重要数据的涉及个人信息数据的出境安全管理，适用法律、行政法规的有关规定。

我国缔结或者参加的国际条约、协定有不同规定的，适用该国际条约、协定，但我国声明保

安法合规集团&北源律师事务所

留的条款除外。

第十二条 汽车数据处理者向境外提供重要数据，不得超出出境安全评估时明确的目的、范围、方式和数据种类、规模等。

国家网信部门会同国务院有关部门以抽查等方式核验前款规定事项，汽车数据处理者应当予以配合，并以可读等便利方式予以展示。

第十三条 汽车数据处理者开展重要数据处理活动，应当在每年十二月十五日前向省、自治区、直辖市网信部门和有关部门报送以下年度汽车数据安全管理情况：

（一）汽车数据安全管理负责人、用户权益事务联系人的姓名和联系方式；

（二）处理汽车数据的种类、规模、目的和必要性；

（三）汽车数据的安全防护和管理措施，包括保存地点、期限等；

（四）向境内第三方提供汽车数据情况；

（五）汽车数据安全事件和处置情况；

（六）汽车数据相关的用户投诉和处理情况；

（七）国家网信部门会同国务院工业和信息化、公安、交通运输等有关部门明确的其他汽车数据安全管理情况。

第十四条 向境外提供重要数据的汽车数据处理者应当在本规定第十三条要求的基础上，补充报告以下情况：

（一）接收者的基本情况；

（二）出境汽车数据的种类、规模、目的和必要性；

（三）汽车数据在境外的保存地点、期限、范围和方式；

（四）涉及向境外提供汽车数据的用户投诉和处理情况；

（五）国家网信部门会同国务院工业和信息化、公安、交通运输等有关部门明确的向境外提供汽车数 据需要报告的其他情况。

第十五条 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依据职责，根据处理数据情况对汽车数据处理者进行数据安全评估，汽车数据处理者应当予以配合。

安证合规集团&北源律师事务所

参与安全评估的机构和人员不得披露评估中获悉的汽车数据处理者商业秘密、未公开信息，不得将评估中获悉的信息用于评估以外目的。

第十六条 国家加强智能（网联）汽车网络平台建设，开展智能（网联）汽车入网运行和安全保障服务等，协同汽车数据处理者加强智能（网联）汽车网络和汽车数据安全防护。

第十七条 汽车数据处理者开展汽车数据处理活动，应当建立投诉举报渠道，设置便捷的投诉举报入口，及时处理用户投诉举报。

开展汽车数据处理活动造成用户合法权益或者公共利益受到损害的，汽车数据处理者应当依法承担相应责任。

第十八条 汽车数据处理者违反本规定的，由省级以上网信、工业和信息化、公安、交通运输等有关部门依照《中华人民共和国网络安全法》、《中华人民共和国数据安全法》等法律、行政法规的规定进行处罚；构成犯罪的，依法追究刑事责任。

第十九条 本规定自2021年10月1日起施行。

第五篇 规范性文件

常见类型移动互联网应用程序必要个人信息范围规定

基本信息：	
【发布机关】国家互联网信息办公室	【时效性】 现行有效
【发文字号】国信办秘字〔2021〕14号	【效力级别】部门规范性文件
【发布日期】2021.03.12	【实施日期】2021.05.01

第一条 为了规范移动互联网应用程序（App）收集个人信息行为，保障公民个人信息安全，根据《中华人民共和国网络安全法》，制定本规定。

第二条 移动智能终端上运行的App存在收集用户个人信息行为的，应当遵守本规定。法律、行政法规、部门规章和规范性文件另有规定的，依照其规定。

App包括移动智能终端预置、下载安装的应用软件，基于应用软件开放平台接口开发的、用户无需安装即可使用的小程序。

第三条 本规定所称必要个人信息，是指保障App基本功能服务正常运行所必需的个人信

安证合规集团&北源律师事务所

息，缺少该信息 App 即无法实现基本功能服务。具体是指消费侧用户个人信息，不包括服务供给侧用户个人信息。

第四条 App 不得因为用户不同意提供非必要个人信息，而拒绝用户使用其基本功能服务。

第五条 常见类型 App 的必要个人信息范围：

（一）地图导航类，基本功能服务为“定位和导航”，必要个人信息为：位置信息、出发地、到达地。

（二）网络约车类，基本功能服务为“网络预约出租汽车服务、巡游出租汽车电召服务”，必要个人信息包括：

1.注册用户移动电话号码；

2.乘车人出发地、到达地、位置信息、行踪轨迹；

3.支付时间、支付金额、支付渠道等支付信息（网络预约出租汽车服务）。

（三）即时通信类，基本功能服务为“提供文字、图片、语音、视频等网络即时通信服务”，必要个人信息包括：

1.注册用户移动电话号码；

2.账号信息：账号、即时通信联系人账号列表。

（四）网络社区类，基本功能服务为“博客、论坛、社区等话题讨论、信息分享和关注互动”，必要个人信息为：注册用户移动电话号码。

（五）网络支付类，基本功能服务为“网络支付、提现、转账等功能”，必要个人信息包括：

1.注册用户移动电话号码；

2.注册用户姓名、证件类型和号码、证件有效期限、银行卡号码。

（六）网上购物类，基本功能服务为“购买商品”，必要个人信息包括：

1.注册用户移动电话号码；

2.收货人姓名（名称）、地址、联系电话；

3.支付时间、支付金额、支付渠道等支付信息。

（七）餐饮外卖类，基本功能服务为“餐饮购买及外送”，必要个人信息包括：

1.注册用户移动电话号码；

2.收货人姓名（名称）、地址、联系电话；

3.支付时间、支付金额、支付渠道等支付信息。

（八）邮件快件寄递类，基本功能服务为“信件、包裹、印刷品等物品寄递服务”，必要个

安证合规集团&北源律师事务所

人信息包括：

1.寄件人姓名、证件类型和号码等身份信息；

2.寄件人地址、联系电话；

3.收件人姓名（名称）、地址、联系电话；

4.寄递物品的名称、性质、数量。

（九）交通票务类，基本功能服务为“交通相关的票务服务及行程管理（如票务购买、改签、退票、行程管理等）”，必要个人信息包括：

1.注册用户移动电话号码；

2.旅客姓名、证件类型和号码、旅客类型。旅客类型通常包括儿童、成人、学生等；

3.旅客出发地、目的地、出发时间、车次/船次/航班号、席别/舱位等级、座位号（如有）、车牌号及车牌颜色（ETC 服务）；

4.支付时间、支付金额、支付渠道等支付信息。

（十）婚恋相亲类，基本功能服务为“婚恋相亲”，必要个人信息包括：

1.注册用户移动电话号码；

2.婚恋相亲人的性别、年龄、婚姻状况。

（十一）求职招聘类，基本功能服务为“求职招聘信息交换”，必要个人信息包括：

1.注册用户移动电话号码；

2.求职者提供的简历。

（十二）网络借贷类，基本功能服务为“通过互联网平台实现的用于消费、日常生产经营周转等的个人申贷服务”，必要个人信息包括：

1.注册用户移动电话号码；

2.借款人姓名、证件类型和号码、证件有效期限、银行卡号码。

（十三）房屋租售类，基本功能服务为“个人房源信息发布、房屋出租或买卖”，必要个人信息包括：

1.注册用户移动电话号码；

2.房源基本信息：房屋地址、面积/户型、期望售价或租金。

（十四）二手车交易类，基本功能服务为“二手车买卖信息交换”，必要个人信息包括：

1.注册用户移动电话号码；

2.购买方姓名、证件类型和号码；

3.出售方姓名、证件类型和号码、车辆行驶证号、车辆识别号码。

安证合规集团&北源律师事务所

（十五）问诊挂号类，基本功能服务为“在线咨询问诊、预约挂号”，必要个人信息包括：

1.注册用户移动电话号码；

2.挂号时需提供患者姓名、证件类型和号码、预约挂号的医院和科室；

3.问诊时需提供病情描述。

（十六）旅游服务类，基本功能服务为“旅游服务产品信息的发布与订购”，必要个人信息包括：

1.注册用户移动电话号码；

2.出行人旅游目的地、旅游时间；

3.出行人姓名、证件类型和号码、联系方式。

（十七）酒店服务类，基本功能服务为“酒店预订”，必要个人信息包括：

1.注册用户移动电话号码；

2.住宿人姓名和联系方式、入住和退房时间、入住酒店名称。

（十八）网络游戏类，基本功能服务为“提供网络游戏产品和服务”，必要个人信息为：注册用户移动电话号码。

（十九）学习教育类，基本功能服务为“在线辅导、网络课堂等”，必要个人信息为：注册用户移动电话号码。

（二十）本地生活类，基本功能服务为“家政维修、家居装修、二手闲置物品交易等日常生活服务”，必要个人信息为：注册用户移动电话号码。

（二十一）女性健康类，基本功能服务为“女性经期管理、备孕育儿、美容美体等健康管理服务”，无须个人信息，即可使用基本功能服务。

（二十二）用车服务类，基本功能服务为“共享单车、共享汽车、租赁汽车等服务”，必要个人信息包括：

1.注册用户移动电话号码；

2.使用共享汽车、租赁汽车服务用户的证件类型和号码，驾驶证件信息；

3.支付时间、支付金额、支付渠道等支付信息；

4.使用共享单车、分时租赁汽车服务用户的位置信息。

（二十三）投资理财类，基本功能服务为“股票、期货、基金、债券等相关投资理财服务”，必要个人信息包括：

1.注册用户移动电话号码；

2.投资理财用户姓名、证件类型和号码、证件有效期限、证件影印件；

安证合规集团&北源律师事务所

3.投资理财用户资金账户、银行卡号码或支付账号。

（二十四）手机银行类，基本功能服务为“通过手机等移动智能终端设备进行银行账户管理、信息查询、转账汇款等服务”，必要个人信息包括：

1.注册用户移动电话号码；

2.用户姓名、证件类型和号码、证件有效期限、证件影印件、银行卡号码、银行预留移动电话号码；

3.转账时需提供收款人姓名、银行卡号码、开户银行信息。

（二十五）邮箱云盘类，基本功能服务为“邮箱、云盘等”，必要个人信息为：注册用户移动电话号码。

（二十六）远程会议类，基本功能服务为“通过网络提供音频或视频会议”，必要个人信息为：注册用户移动电话号码。

（二十七）网络直播类，基本功能服务为“向公众持续提供实时视频、音频、图文等形式信息浏览服务”，无须个人信息，即可使用基本功能服务。

（二十八）在线影音类，基本功能服务为“影视、音乐搜索和播放”，无须个人信息，即可使用基本功能服务。

（二十九）短视频类，基本功能服务为“不超过一定时长的视频搜索、播放”，无须个人信息，即可使用基本功能服务。

（三十）新闻资讯类，基本功能服务为“新闻资讯的浏览、搜索”，无须个人信息，即可使用基本功能服务。

（三十一）运动健身类，基本功能服务为“运动健身训练”，无须个人信息，即可使用基本功能服务。

（三十二）浏览器类，基本功能服务为“浏览互联网信息资源”，无须个人信息，即可使用基本功能服务。

（三十三）输入法类，基本功能服务为“文字、符号等输入”，无须个人信息，即可使用基本功能服务。

（三十四）安全管理类，基本功能服务为“查杀病毒、清理恶意插件、修复漏洞等”，无须个人信息，即可使用基本功能服务。

（三十五）电子图书类，基本功能服务为“电子图书搜索、阅读”，无须个人信息，即可使用基本功能服务。

（三十六）拍摄美化类，基本功能服务为“拍摄、美颜、滤镜等”，无须个人信息，即可使

安证合规集团&北源律师事务所

用基本功能服务。

（三十七）应用商店类，基本功能服务为“App 搜索、下载”，无须个人信息，即可使用基本功能服务。

（三十八）实用工具类，基本功能服务为“日历、天气、词典翻译、计算器、遥控器、手电筒、指南针、时钟闹钟、文件传输、文件管理、壁纸铃声、截图录屏、录音、文档处理、智能家居助手、星座性格测试等”，无须个人信息，即可使用基本功能服务。

（三十九）演出票务类，基本功能服务为“演出购票”，必要个人信息包括：

1.注册用户移动电话号码；

2.观演场次、座位号（如有）；

3.支付时间、支付金额、支付渠道等支付信息。

第六条 任何组织和个人发现违反本规定行为的，可以向相关部门举报。

相关部门收到举报后，应当依法予以处理。

第七条 本规定自 2021 年 5 月 1 日起施行。

移动互联网应用程序个人信息保护管理暂行规定

基本信息：	
【发布机关】工业和信息化部	【时效性】 未施行
【发文字号】-	【效力级别】部门规范性文件
【发布日期】2021年4月26日	【实施日期】-

移动互联网应用程序个人信息保护管理暂行规定

（征求意见稿）

第一条 为保护个人信息权益，规范移动互联网应用程序（以下简称App）个人信息处理活动，促进个人信息合理利用，依据《中华人民共和国网络安全法》等法律法规，制定本规定。

第二条 在中华人民共和国境内开展的App个人信息处理活动，应当遵守本规定。法律、行政法规对个人信息处理活动另有规定的，从其规定。

第三条 本规定所称App个人信息处理活动，是指移动智能终端中运行的应用程序收集、

安证合规集团&北源律师事务所

存储、使用、加工、传输个人信息的活动。

本规定所称App开发运营者，是指从事App开发和运营活动的主体。

本规定所称App分发平台，是指通过应用商店、应用市场、网站等方式提供App下载、升级服务的软件服务平台。

本规定所称App第三方服务提供者，是指相对于用户和App以外的，为App提供软件开发工具包（SDK）、封装、加固、编译环境等第三方服务的主体。

本规定所称移动智能终端生产企业，是指生产能够接入公众网络，提供预置App或者具备安装App能力的移动智能终端设备的主体。

本规定所称网络接入服务提供者，是指从事互联网数据中心（IDC）业务、互联网接入服务（ISP）业务和内容分发网络（CDN）业务，为App提供网络接入服务的电信业务经营者。

第四条 国家互联网信息办公室负责统筹协调 App 个人信息保护工作和相关监督管理工作，会同工业和信息化部、公安部、市场监管总局建立健全 App 个人信息保护监督管理联合工作机制，统筹推进政策标准规范等相关工作，加强信息共享及对 App 个人信息保护工作的指导。各部门在各自职责范围内负责 App 个人信息保护和监督管理工作。

省、自治区、直辖市网信办、通信管理局、公安厅（局）、市场监管局负责本行政区域内App个人信息保护监督管理工作。

前两款规定的部门统称为App个人信息保护监督管理部门。

第五条 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。

相关行业组织和专业机构按照有关法律法规、标准及本规定，开展App个人信息保护能力评估、认证。

第六条 从事App个人信息处理活动的，应当以清晰易懂的语言告知用户个人信息处理规则，由用户在充分知情的前提下，作出自愿、明确的意思表示。

（一）应当在App登录注册页面及App首次运行时，通过弹窗、文本链接及附件等简洁明显且易于访问的方式，向用户告知涵盖个人信息处理主体、处理目的、处理方式、处理类型、保存期限等内容的个人信息处理规则；

（二）应当采取非默认勾选的方式征得用户同意；

（三）应当尊重用户选择权，在取得用户同意前或者用户明确表示拒绝后，不得处理个人信息；个人信息处理规则发生变更的，应当重新取得用户同意；

安证合规集团&北源律师事务所

（四）应当在对应业务功能启动时，动态申请App所需的权限，不应强制要求用户一揽子同意打开多个系统权限，且未经用户同意，不得更改用户设置的权限状态；

（五）需要向本App以外的第三方提供个人信息的,应当向用户告知其身份信息、联系方式、处理目的、处理方式和个人信息的种类等事项,并取得用户同意；

（六）处理种族、民族、宗教信仰、个人生物特征、医疗健康、金融账户、个人行踪等敏感个人信息的，应当对用户进行单独告知，取得用户同意后，方可处理敏感个人信息。

第七条 从事App个人信息处理活动的，应当具有明确、合理的目的，并遵循最小必要原则，不得从事超出用户同意范围或者与服务场景无关的个人信息处理活动。

（一）处理个人信息的数量、频次、精度等应当为服务所必需，不得超范围处理个人信息；

（二）个人信息的本地读取、写入、删除、修改等操作应当为服务所必需，不得超出用户同意的操作范围；

（三）用户拒绝相关授权申请后，不得强制退出或者关闭App，不得提前申请超出其业务功能或者服务外的权限，不得利用频繁弹窗反复申请与当前服务场景无关的权限；

（四）在非服务所必需或者无合理场景下，不得自启动或者关联启动其他App；

（五）用户拒绝提供非该类服务所必需的个人信息时，不得影响用户使用该服务；

（六）不得以改善服务质量、提升使用体验、研发新产品、定向推送信息、风险控制等为由，强制要求用户同意超范围或者与服务场景无关的个人信息处理行为。

第八条 App开发运营者应当履行以下个人信息保护义务:

（一）切实提升产品和服务个人信息保护意识，将个人信息保护要求落实在产品设计、开发及运营环节；以显著、清晰的方式定期向用户呈现App的个人信息收集使用情况；

（二）基于个人信息向用户提供商品或者服务的搜索结果的，应当保证结果公平合理，同时向该用户提供不针对其个人特征的选项，尊重和平等保护用户合法权益；

（三）使用第三方服务的，应当制定管理规则，明示App第三方服务提供者的名称、功能、个人信息处理规则等内容；应与第三方服务提供者签订个人信息处理协议，明确双方相关权利义务，并对第三方服务提供者的个人信息处理活动和信息安全风险进行管理监督；App开发运营者未尽到监督义务的，应当依法与第三方服务提供者承担连带责任；

（四）对于不影响其他服务功能的独立服务功能模块，应当向用户提供关闭或者退出该独立服务功能的选项，不得因用户采取关闭或者退出操作而拒绝提供其他服务；

（五）加强前端和后端安全防护、访问控制、技术加密、安全审计等工作，主动监测发现个人信息泄露等违规行为，及时响应处置要求；

安证合规集团&北京律师事务所

（六）国家规定的其他个人信息保护义务。

第九条 App分发平台应当履行以下个人信息保护义务：

（一）登记并核验App开发运营者、提供者的真实身份、联系方式等信息；

（二）在显著位置标明App运行所需获取的用户终端权限列表和个人信息收集的类型、内容、目的、范围、方式、用途及处理规则等相关信息；

（三）不得欺骗误导用户下载App；

（四）对新上架App实行上架前个人信息处理活动规范性审核，对已上架App在本规定实施后1个月内完成补充审核，并根据审核结果进行更新或者清理；

（五）建立App开发运营者信用积分、风险App名单、平台信息共享及签名验证等管理机制；

（六）按照监督管理部门的要求，完善报送机制，及时配合监督管理部门开展问题App上报、响应和处置工作；

（七）设置便捷的投诉举报入口，及时处理公众对本平台所分发App的投诉举报；

（八）国家规定的其他个人信息保护义务。

第十条 App第三方服务提供者应当履行以下个人信息保护义务：

（一）制定并公开个人信息处理规则；

（二）以明确、易懂、合理的方式向App开发运营者公开其个人信息处理目的、处理方式、处理类型、保存期限等内容，其个人信息处理活动应当与公开的个人信息处理规则保持一致；

（三）未经用户同意或者在无合理业务场景下，不得自行进行唤醒、调用、更新等行为；

（四）采取足够的管理措施和技术手段保护个人信息，发现安全风险或者个人信息处理规则变更时应当及时进行更新并告知App开发运营者；

（五）未经用户同意，不得将收集到的用户个人信息共享转让；

（六）国家规定的其他个人信息保护义务。

第十一条 移动智能终端生产企业应当履行以下个人信息保护义务：

（一）完善终端权限管控机制，及时弥补权限管理漏洞，持续优化和规范敏感行为的记录能力，主动为用户权限申请和告知提供便利；

（二）建立终端启动和关联启动App管理机制，为用户提供关闭自启动和关联启动的功能选项；

（三）持续优化个人信息权限在用状态，特别是录音、拍照、视频等敏感权限在用状态的显著提示机制，帮助用户及时准确了解个人信息权限的使用状态；

（四）建立重点App关注名单管理机制，完善移动智能终端App管理措施；

安证合规集团&北源律师事务所

（五）对预置App进行审核，持续监测预置App的个人信息安全风险；

（六）在安装过程中以显著方式告知用户App申请的个人信息权限列表；

（七）完善终端设备标识管理机制；

（八）国家规定的其他个人信息保护义务。

第十二条 网络接入服务提供者应当履行以下个人信息保护义务：

（一）在为App提供网络接入服务时，登记并核验App开发运营者的真实身份、联系方式等信息；

（二）按照监督管理部门的要求，依法对违规App采取停止接入等必要措施，阻止其继续违规侵害用户个人信息和其他合法权益；

（三）国家规定的其他个人信息保护义务。

第十三条 从事App个人信息处理活动的相关主体，应当加强人员教育培训，制定个人信息保护内部管理制度，落实网络安全等级保护和应急预案等制度要求；采取加密、去标识化等安全技术措施，防止未经授权的访问及个人信息泄露或者被窃取、篡改、删除等风险；需要认证用户真实身份信息的，应当通过国家统一建设的公民身份认证基础设施所提供的网上公民身份核验认证服务进行。

第十四条 任何组织和个人发现违反本规定行为的，可以向监督管理部门或者中国互联网协会、中国网络空间安全协会投诉举报，监督管理部门和相关组织应当及时受理并调查处理。

从事App个人信息处理活动的相关主体应当自觉接受社会监督。

第十五条 根据公众投诉举报情况和监管中发现的问题，监督管理部门可以对存在问题和风险的App实施个人信息保护检查。

从事App个人信息处理活动的相关主体应当对监督管理部门依法实施的监督检查予以配合。

第十六条 发现从事个人信息处理活动的相关主体违反本规定的，监督管理部门可依据各自职责采取以下处置措施：

（一）责令整改与社会公告。对检测发现问题App的开发运营者、App分发平台、第三方服务提供者及相关主体提出整改，要求5个工作日内进行整改及时消除隐患；未完成整改的，向社会公告。

（二）下架处置。对社会公告5个工作日后，仍拒绝整改或者整改后仍存在问题的，可要求相关主体进行下架处置；对反复出现问题、采取技术对抗等违规情节严重的，将对其进行直接下架；被下架的App在40个工作日内不得通过任何渠道再次上架。

（三）断开接入。下架后仍未按要求完成整改的，将对其采取断开接入等必要措施。

安证合规集团&北源律师事务所

（四）恢复上架。被下架的App完成整改，并完善技术和管理机制及作出企业自律承诺后，可向作出下架要求的监督管理部门申请恢复上架。

（五）恢复接入。被断开网络接入的App完成整改后，可向作出断开接入要求的监督管理部门申请恢复接入。

（六）信用管理。对相应违规主体，可纳入信用管理，实施联合惩戒。

第十七条 对整改反复出现问题的App及其开发运营者开发的相关App，监督管理部门可以指导组织App分发平台和移动智能终端生产企业在集成、分发、预置和安装等环节进行风险提示，情节严重的采取禁入措施。

第十八条 从事App个人信息处理活动侵害个人信息权益的，将依照有关规定予以处罚；构成犯罪的，公安机关依法追究刑事责任。

第十九条 监督管理部门应当对履行职责中知悉的用户个人信息予以保密，不得泄露、篡改或者毁损，不得出售或者非法向他人提供。

第二十条 本规定自 年 月 日起施行。

关于银行业金融机构做好个人金融信息保护工作的通知

基本信息：	
【发布机关】中国人民银行	【时效性】 现行有效
【发文字号】银发[2011]17号	【效力级别】部门规范性文件
【发布日期】2011-01-21	【实施日期】2011-05-01

关于银行业金融机构做好个人金融信息保护工作的通知

人民银行上海总部，各分行、营业管理部，各省会(首府)城市中心支行，国有商业银行，股份制商业银行，中国邮政储蓄银行：

个人金融信息是金融机构日常业务工作中积累的一项重要基础数据，也是金融机构客户个人隐私的重要内容。如何收集、使用、对外提供个人金融信息，既涉及到银行业金融机构业务的正常开展，也涉及客户信息、个人隐私的保护。如果出现与个人金融信息有关的不当行为，不但会直接侵害客户的合法权益，也会增加银行业金融机构的诉讼风险，加大运营成本。近年来，个人金融信息侵权行为时有发生，并引起社会的广泛关注。因此，强化个人金融信息保护和银行业金融机构法制意识，依法收集、使用和对外提供个人金融信息，十分必要。对个人金融信息的保护

安证合规集团&北源律师事务所

是银行业金融机构的一项法定义务。为了规范银行业金融机构收集、使用和对外提供个人金融信息行为，保护金融消费者合法权益，维护金融稳定，根据《中华人民共和国中国人民银行法》、《中华人民共和国商业银行法》、《中华人民共和国反洗钱法》、《个人存款账户实名制规定》等法律、法规的规定，现就个人金融信息保护的有关事项通知如下:

一、本通知所称个人金融信息，是指银行业金融机构在开展业务时，或通过接入中国人民银行征信系统、支付系统以及其他系统获取、加工和保存的以下个人信息:

(一)个人身份信息，包括个人姓名、性别、国籍、民族、身份证件种类号码及有效期限、职业、联系方式、婚姻状况、家庭状况、住所或工作单位地址及照片等;

(二)个人财产信息，包括个人收入状况、拥有的不动产状况、拥有的车辆状况、纳税额、公积金缴存金额等;

(三)个人账户信息，包括账号、账户开立时间、开户行、账户余额、账户交易情况等;

(四)个人信用信息，包括信用卡还款情况、贷款偿还情况以及个人在经济活动中形成的，能够反映其信用状况的其他信息;

(五)个人金融交易信息，包括银行业金融机构在支付结算、理财、保险箱等中间业务过程中获取、保存、留存的个人信息和客户在通过银行业金融机构与保险公司、证券公司、基金公司、期货公司等第三方机构发生业务关系时产生的个人信息等;

(六)衍生信息，包括个人消费习惯、投资意愿等对原始信息进行处理、分析所形成的反映特定个人某些情况的信息;

(七)在与个人建立业务关系过程中获取、保存的其他个人信息。

二、银行业金融机构在收集、保存、使用、对外提供个人金融信息时，应当严格遵守法律规定，采取有效措施加强对个人金融信息保护，确保信息安全，防止信息泄露和滥用。特别是在收集个人金融信息时，应当遵循合法、合理原则，不得收集与业务无关的信息或采取不正当方式收集信息。

三、银行业金融机构应当建立健全内部控制制度，对易发生个人金融信息泄露的环节进行充分排查，明确规定各部门、岗位和人员的管理责任，加强个人金融信息管理的权限设置，形成相互监督、相互制约的管理机制，切实防止信息泄露或滥用事件的发生。

银行业金融机构要完善信息安全技术防范措施，确保个人金融信息在收集、传输、加工、保存、使用等环节中不被泄露。

银行业金融机构要加强对从业人员的培训，强化从业人员个人金融信息安全意识，防止从业人员非法使用、泄露、出售个人金融信息。接触个人金融信息岗位的从业人员在上岗前，应当书

安证合规集团&北源律师事务所

面做出保密承诺。

四、银行业金融机构不得篡改、违法使用个人金融信息。使用个人金融信息时，应当符合收集该信息的目的，并不得进行以下行为：

(一)出售个人金融信息；

(二)向本金融机构以外的其他机构和个人提供个人金融信息，但为个人办理相关业务所必需并经个人书面授权或同意的，以及法律法规和中国人民银行另有规定的除外；

(三)在个人提出反对的情况下，将个人金融信息用于产生该信息以外的本金融机构其他营销活动。

银行业金融机构通过格式条款取得客户书面授权或同意的，应当在协议中明确该授权或同意所适用的向他人提供个人金融信息的范围和具体情形。同时，还应当在协议的醒目位置使用通俗易懂的语言明确提示该授权或同意的可能后果，并在客户签署协议时提醒其注意上述提示。

五、银行业金融机构不得将客户授权或同意其将个人信息用于营销、对外提供等作为与客户建立业务关系的先决条件，但该业务关系的性质决定需要预先做出相关授权或同意的除外。

六、在中国境内收集的个人金融信息的储存、处理和分析应当在中国境内进行。除法律法规及中国人民银行另有规定外，银行业金融机构不得向境外提供境内个人金融信息。

七、银行业金融机构通过外包开展业务的，应当充分审查、评估外包服务供应商保护个人金融信息的能力，并将其作为选择外包服务供应商的重要指标。

银行业金融机构与外包服务供应商签订服务协议时，应当明确其保护个人金融信息的职责和保密义务，并采取必要措施保证外包服务供应商履行上述职责和义务，确保个人金融信息安全。银行业金融机构应要求外包服务供应商在外包业务终止后，及时销毁因外包业务而获得的个人金融信息。

八、银行业金融机构通过接入中国人民银行征信系统、支付系统以及其他系统获取的个人金融信息，应当严格按照系统规定的用途使用，不得违反规定查询和滥用。

九、银行业金融机构发生个人金融信息泄露事件的，或银行业金融机构的上级机构发现下级机构有违反规定对外提供个人金融信息及其他违反本通知行为的，应当在事件发生之日或发现下级机构违规行为之日起7个工作日内将相关情况及初步处理意见报告中国人民银行当地分支机构。

中国人民银行分支机构在收到银行业金融机构报告后，应视情况予以处理，并及时向中国人民银行报告。

十、中国人民银行及其地市中心支行以上分支机构受理投诉或发现银行业金融机构可能未履行个人金融信息保护义务的，可依法进行核实，认定银行业金融机构存在违反本通知规定，或存

安证合规集团&北源律师事务所

在其他未履行个人金融信息保护义务情形的，可采取以下处理措施：

(一)约见其高管人员谈话，要求说明情况；

(二)责令银行业金融机构限期整改；

(三)在金融系统内予以通报；

(四)建议银行业金融机构对直接负责的高级管理人员和其他直接责任人员依法给予处分；

(五)涉嫌犯罪的，依法移交司法机关处理。

十一、银行业金融机构违反规定通过中国人民银行征信系统、支付系统以及其他系统查询或滥用个人金融信息的，中国人民银行及其地市中心支行以上分支机构可按照本通知第十条及其他相关规定予以处理。

银行业金融机构违法情节严重或拒不改正的，中国人民银行可决定暂停其使用，或禁止其新设分支机构接入上述系统。

十二、银行业金融机构及其工作人员违反规定使用和对外提供个人金融信息，给客户造成损害的，应当依法承担相应的法律责任。

本通知自2011年5月1日起执行。请中国人民银行上海总部，各分行、营业管理部、省会（首府)城市中心支行将本通知转发至辖区内各银行业金融机构。本通知执行过程中发现的新情况、新问题，请及时向中国人民银行报告。

安证合规集团&北源律师事务所

中国人民银行金融消费者权益保护实施办法

基本信息：	
【发布机关】中国人民银行	【时效性】 现行有效
【发文字号】中国人民银行令〔2020〕第5号	【效力级别】部门规范性文件
【发布日期】2020年9月15日	【实施日期】2020年11月1日

中国人民银行令

〔2020〕第5号

《中国人民银行金融消费者权益保护实施办法》已经2020年9月1日中国人民银行2020年第6次行务会议审议通过，现予发布，自2020年11月1日起施行。

行 长 易纲

2020年9月15日

中国人民银行金融消费者权益保护实施办法

第一章 总 则

第一条 为了保护金融消费者合法权益，规范金融机构提供金融产品和服务的行为，维护公平、公正的市场环境，促进金融市场健康稳定运行，根据《中华人民共和国中国人民银行法》《中华人民共和国商业银行法》《中华人民共和国消费者权益保护法》和《国务院办公厅关于加强金融消费者权益保护工作的指导意见》（国办发〔2015〕81号）等，制定本办法。

第二条 在中华人民共和国境内依法设立的为金融消费者提供金融产品或者服务的银行业金融机构（以下简称银行），开展与下列业务相关的金融消费者权益保护工作，适用本办法：

（一）与利率管理相关的。

（二）与人民币管理相关的。

（三）与外汇管理相关的。

（四）与黄金市场管理相关的。

（五）与国库管理相关的。

（六）与支付、清算管理相关的。

（七）与反洗钱管理相关的。

（八）与征信管理相关的。

（九）与上述第一项至第八项业务相关的金融营销宣传和消费者金融信息保护。

（十）其他法律、行政法规规定的中国人民银行职责范围内的金融消费者权益保护工作。

安证合规集团&北源律师事务所

在中华人民共和国境内依法设立的非银行支付机构（以下简称支付机构）提供支付服务的，适用本办法。

本办法所称金融消费者是指购买、使用银行、支付机构提供的金融产品或者服务的自然人。

第三条 银行、支付机构向金融消费者提供金融产品或者服务，应当遵循自愿、平等、公平、诚实信用的原则，切实承担金融消费者合法权益保护的主体责任，履行金融消费者权益保护的法定义务。

第四条 金融消费者应当文明、理性进行金融消费，提高自我保护意识，诚实守信，依法维护自身的合法权益。

第五条 中国人民银行及其分支机构坚持公平、公正原则，依法开展职责范围内的金融消费者权益保护工作，依法保护金融消费者合法权益。

中国人民银行及其分支机构会同有关部门推动建立和完善金融机构自治、行业自律、金融监管和社会监督相结合的金融消费者权益保护共同治理体系。

第六条 鼓励金融消费者和银行、支付机构充分运用调解、仲裁等方式解决金融消费纠纷。

第二章 金融机构行为规范

第七条 银行、支付机构应当将金融消费者权益保护纳入公司治理、企业文化建设和经营发展战略，制定本机构金融消费者权益保护工作的总体规划和具体工作措施。建立金融消费者权益保护专职部门或者指定牵头部门，明确部门及人员职责，确保部门有足够的人力、物力能够独立开展工作，并定期向高级管理层、董（理）事会汇报工作开展情况。

第八条 银行、支付机构应当落实法律法规和相关监管规定关于金融消费者权益保护的相关要求，建立健全金融消费者权益保护的各项内控制度：

（一）金融消费者权益保护工作考核评价制度。

（二）金融消费者风险等级评估制度。

（三）消费者金融信息保护制度。

（四）金融产品和服务信息披露、查询制度。

（五）金融营销宣传管理制度。

（六）金融知识普及和金融消费者教育制度。

（七）金融消费者投诉处理制度。

（八）金融消费者权益保护工作内部监督和责任追究制度。

（九）金融消费者权益保护重大事件应急制度。

（十）中国人民银行明确规定应当建立的其他金融消费者权益保护工作制度。

安证合规集团&北源律师事务所

第九条 银行、支付机构应当建立健全涉及金融消费者权益保护工作的全流程管控机制，确保在金融产品或者服务的设计开发、营销推介及售后管理等各个业务环节有效落实金融消费者权益保护工作的相关规定和要求。全流程管控机制包括但不限于下列内容：

（一）事前审查机制。银行、支付机构应当实行金融消费者权益保护事前审查，及时发现并更正金融产品或者服务中可能损害金融消费者合法权益的问题，有效督办落实金融消费者权益保护审查意见。

（二）事中管控机制。银行、支付机构应当履行金融产品或者服务营销宣传中须遵循的基本程序和标准，加强对营销宣传行为的监测与管控。

（三）事后监督机制。银行、支付机构应当做好金融产品和服务的售后管理，及时调整存在问题或者隐患的金融产品和服务规则。

第十条 银行、支付机构应当开展金融消费者权益保护工作人员培训，增强工作人员的金融消费者权益保护意识和能力。

银行、支付机构应当每年至少开展一次金融消费者权益保护专题培训，培训对象应当全面覆盖中高级管理人员、基层业务人员及新入职人员。对金融消费者投诉多发、风险较高的业务岗位，应当适当提高培训的频次。

第十一条 银行、支付机构开展考核评价时，应当将金融消费者权益保护工作作为重要内容，并合理分配相关指标的占比和权重，综合考虑业务合规性、客户满意度、投诉处理及时率与合格率等，不得简单以投诉数量作为考核指标。

第十二条 银行、支付机构应当根据金融产品或者服务的特性评估其对金融消费者的适合度，合理划分金融产品和服务风险等级以及金融消费者风险承受等级，将合适的金融产品或者服务提供给适当的金融消费者。

第十三条 银行、支付机构应当依法保障金融消费者在购买、使用金融产品和服务时的财产安全，不得挪用、非法占用金融消费者资金及其他金融资产。

第十四条 银行、支付机构应当尊重社会公德，尊重金融消费者的人格尊严和民族风俗习惯，不得因金融消费者性别、年龄、种族、民族或者国籍等不同实行歧视性差别对待，不得使用歧视性或者违背公序良俗的表述。

第十五条 银行、支付机构应当尊重金融消费者购买金融产品或者服务的真实意愿，不得擅自代理金融消费者办理业务，不得擅自修改金融消费者的业务指令，不得强制搭售其他产品或者服务。

第十六条 银行、支付机构应当依据金融产品或者服务的特性，及时、真实、准确、全面地向

安证合规集团&北清律师事务所

金融消费者披露下列重要内容:

（一）金融消费者对该金融产品或者服务的权利和义务，订立、变更、中止和解除合同的方式及限制。

（二）银行、支付机构对该金融产品或者服务的权利、义务及法律责任。

（三）贷款产品的年化利率。

（四）金融消费者应当负担的费用及违约金，包括金额的确定方式，交易时间和交易方式。

（五）因金融产品或者服务产生纠纷的处理及投诉途径。

（六）银行、支付机构对该金融产品或者服务所执行的强制性标准、推荐性标准、团体标准或者企业标准的编号和名称。

（七）在金融产品说明书或者服务协议中，实际承担合同义务的经营主体完整的中文名称。

（八）其他可能影响金融消费者决策的信息。

第十七条 银行、支付机构对金融产品和服务进行信息披露时，应当使用有利于金融消费者接收、理解的方式。对利率、费用、收益及风险等与金融消费者切身利益相关的重要信息，应当根据金融产品或者服务的复杂程度及风险等级，对其中关键的专业术语进行解释说明，并以适当方式供金融消费者确认其已接收完整信息。

第十八条 银行、支付机构向金融消费者说明重要内容和披露风险时，应当依照法律法规和监管规定留存相关资料，自业务关系终止之日起留存时间不得少于3年。法律、行政法规另有规定的，从其规定。

留存的资料包括但不限于:

（一）金融消费者确认的金融产品说明书或者服务协议。

（二）金融消费者确认的风险提示书。

（三）记录向金融消费者说明重要内容的录音、录像资料或者系统日志等相关数据电文资料。

第十九条 银行、支付机构不得利用技术手段、优势地位，强制或者变相强制金融消费者接受金融产品或者服务，或者排除、限制金融消费者接受同业机构提供的金融产品或者服务。

第二十条 银行、支付机构在提供金融产品或者服务的过程中，不得通过附加限制性条件的方式要求金融消费者购买、使用协议中未作明确要求的产品或者服务。

第二十一条 银行、支付机构向金融消费者提供金融产品或者服务时使用格式条款的，应当以足以引起金融消费者注意的字体、字号、颜色、符号、标识等显著方式，提请金融消费者注意金融产品或者服务的数量、利率、费用、履行期限和方式、注意事项、风险提示、纠纷解决等与金融消费者有重大利害关系的内容，并按照金融消费者的要求予以说明。格式条款采用电子形式的，

安证合规集团&北京律师事务所

应当可被识别且易于获取。

银行、支付机构不得以通知、声明、告示等格式条款的方式作出含有下列内容的规定：

（一）减轻或者免除银行、支付机构造成金融消费者财产损失的赔偿责任。

（二）规定金融消费者承担超过法定限额的违约金或者损害赔偿金。

（三）排除或者限制金融消费者依法对其金融信息进行查询、删除、修改的权利；

（四）排除或者限制金融消费者选择同业机构提供的金融产品或者服务的权利。

（五）其他对金融消费者不公平、不合理的规定。

银行、支付机构应当对存在侵害金融消费者合法权益问题或者隐患的格式条款和服务协议文本及时进行修订或者清理。

第二十二条 银行、支付机构应当对营销宣传内容的真实性负责。银行、支付机构实际承担的义务不得低于在营销宣传活动中通过广告、资料或者说明等形式对金融消费者所承诺的标准。

前款“广告、资料或者说明”是指以营销为目的，利用各种传播媒体、宣传工具或者方式，就银行、支付机构的金融产品或者服务进行直接或者间接的宣传、推广等。

第二十三条 银行、支付机构在进行营销宣传活动时，不得有下列行为：

（一）虚假、欺诈、隐瞒或者引人误解的宣传。

（二）引用不真实、不准确的数据和资料或者隐瞒限制条件等，对过往业绩或者产品收益进行夸大表述。

（三）利用金融管理部门对金融产品或者服务的审核或者备案程序，误导金融消费者认为金融管理部门已对该金融产品或者服务提供保证。

（四）明示或者暗示保本、无风险或者保收益等，对非保本投资型金融产品的未来效果、收益或者相关情况作出保证性承诺。

（五）其他违反金融消费者权益保护相关法律法规和监管规定的行为。

第二十四条 银行、支付机构应当切实承担金融知识普及和金融消费者教育的主体责任，提高金融消费者对金融产品和服务的认知能力，提升金融消费者金融素养和诚实守信意识。

银行、支付机构应当制定年度金融知识普及与金融消费者教育工作计划，结合自身特点开展日常性金融知识普及与金融消费者教育活动，积极参与中国人民银行及其分支机构组织的金融知识普及活动。银行、支付机构不得以营销金融产品或者服务替代金融知识普及与金融消费者教育。

第二十五条 银行、支付机构应当重视金融消费者需求的多元性与差异性，积极支持普惠金融重点目标群体获得必要、及时的基本金融产品和服务。

第二十六条 出现侵害金融消费者合法权益重大事件的，银行、支付机构应当根据重大事项报

安证合规集团&北源律师事务所

告的相关规定及时向中国人民银行或其分支机构报告。

第二十七条 银行、支付机构应当配合中国人民银行及其分支机构开展金融消费者权益保护领域的相关工作，按照规定报送相关资料。

第三章 消费者金融信息保护

第二十八条 本办法所称消费者金融信息，是指银行、支付机构通过开展业务或者其他合法渠道处理的消费者信息，包括个人身份信息、财产信息、账户信息、信用信息、金融交易信息及其他与特定消费者购买、使用金融产品或者服务相关的信息。

消费者金融信息的处理包括消费者金融信息的收集、存储、使用、加工、传输、提供、公开等。

第二十九条 银行、支付机构处理消费者金融信息，应当遵循合法、正当、必要原则，经金融消费者或者其监护人明示同意，但是法律、行政法规另有规定的除外。银行、支付机构不得收集与业务无关的消费者金融信息，不得采取不正当方式收集消费者金融信息，不得变相强制收集消费者金融信息。银行、支付机构不得以金融消费者不同意处理其金融信息为由拒绝提供金融产品或者服务，但处理其金融信息属于提供金融产品或者服务所必需的除外。

金融消费者不能或者拒绝提供必要信息，致使银行、支付机构无法履行反洗钱义务的，银行、支付机构可以根据《中华人民共和国反洗钱法》的相关规定对其金融活动采取限制性措施；确有必要时，银行、支付机构可以依法拒绝提供金融产品或者服务。

第三十条 银行、支付机构收集消费者金融信息用于营销、用户体验改进或者市场调查的，应当以适当方式供金融消费者自主选择是否同意银行、支付机构将其金融信息用于上述目的；金融消费者不同意的，银行、支付机构不得因此拒绝提供金融产品或者服务。银行、支付机构向金融消费者发送金融营销信息的，应当向其提供拒绝继续接收金融营销信息的方式。

第三十一条 银行、支付机构应当履行《中华人民共和国消费者权益保护法》第二十九条规定的明示义务，公开收集、使用消费者金融信息的规则，明示收集、使用消费者金融信息的目的、方式和范围，并留存有关证明资料。

银行、支付机构通过格式条款取得消费者金融信息收集、使用同意的，应当在格式条款中明确收集消费者金融信息的目的、方式、内容和使用范围，并在协议中以显著方式尽可能通俗易懂地向金融消费者提示该同意的可能后果。

第三十二条 银行、支付机构应当按照法律法规的规定和双方约定的用途使用消费者金融信息，不得超出范围使用。

第三十三条 银行、支付机构应当建立以分级授权为核心的消费者金融信息使用管理制度，根

安证合规集团&北海律师事务所

据消费者金融信息的重要性、敏感度及业务开展需要，在不影响本机构履行反洗钱等法定义务的前提下，合理确定本机构工作人员调取信息的范围、权限，严格落实信息使用授权审批程序。

第三十四条 银行、支付机构应当按照国家档案管理和电子数据管理等规定，采取技术措施和其他必要措施，妥善保管和存储所收集的消费者金融信息，防止信息遗失、毁损、泄露或者被篡改。

银行、支付机构及其工作人员应当对消费者金融信息严格保密，不得泄露或者非法向他人提供。在确认信息发生泄露、毁损、丢失时，银行、支付机构应当立即采取补救措施；信息泄露、毁损、丢失可能危及金融消费者人身、财产安全的，应当立即向银行、支付机构住所地的中国人民银行分支机构报告并告知金融消费者；信息泄露、毁损、丢失可能对金融消费者产生其他不利影响的，应当及时告知金融消费者，并在72小时以内报告银行、支付机构住所地的中国人民银行分支机构。中国人民银行分支机构接到报告后，视情况按照本办法第五十五条规定处理。

第四章 金融消费争议解决

第三十五条 金融消费者与银行、支付机构发生金融消费争议的，鼓励金融消费者先向银行、支付机构投诉，鼓励当事人平等协商，自行和解。

金融消费者应当依法通过正当途径客观、理性反映诉求，不扰乱正常的金融秩序和社会公共秩序。

本办法所称金融消费争议，是指金融消费者与银行、支付机构因购买、使用金融产品或者服务所产生的民事争议。

第三十六条 银行、支付机构应当切实履行金融消费投诉处理的主体责任，银行、支付机构的法人机构应当按年度向社会发布金融消费者投诉数据和相关分析报告。

第三十七条 银行、支付机构应当通过金融消费者方便获取的渠道公示本机构的投诉受理方式，包括但不限于营业场所、官方网站首页、移动应用程序的醒目位置及客服电话主要菜单语音提示等。

第三十八条 银行、支付机构应当按照中国人民银行要求，加强对金融消费者投诉处理信息系统的建设与管理，对投诉进行正确分类并按时报送相关信息，不得迟报、漏报、谎报、错报或者瞒报投诉数据。

第三十九条 银行、支付机构收到金融消费者投诉后，依照相关法律法规和合同约定进行处理，并告知投诉人处理情况，但因投诉人原因导致无法告知的除外。

第四十条 中国人民银行分支机构设立投诉转办服务渠道。金融消费者对银行、支付机构作出的投诉处理不接受的，可以通过银行、支付机构住所地、合同签订地或者经营行为发生地中国人

安证合规集团&北源律师事务所

民银行分支机构进行投诉。

通过电子商务、网络交易购买、使用金融产品或者服务的，金融消费者通过银行、支付机构住所地的中国人民银行分支机构进行投诉。

第四十一条 金融消费者通过中国人民银行分支机构进行投诉，应当提供以下信息：姓名，有效身份证件信息，联系方式，明确的投诉对象及其住所地，具体的投诉请求、事实和理由。

金融消费者可以本人提出投诉，也可以委托他人代为提出投诉。以来信来访方式进行委托投诉的，应当向中国人民银行分支机构提交前款规定的投诉材料、授权委托书原件、委托人和受托人的身份证明。授权委托书应当载明受托人、委托事项、权限和期限，并由委托人本人签名。

第四十二条 中国人民银行分支机构对下列投诉不予接收：

（一）投诉人投诉的机构、产品或者服务不属于中国人民银行监管范围的。

（二）投诉人未提供真实身份，或者没有明确的被投诉人、没有具体的投诉请求和事实依据的。

（三）投诉人并非金融消费者本人，也未经金融消费者本人委托的。

（四）人民法院、仲裁机构、其他金融管理部门、行政部门或者依法设立的调解组织已经受理、接收或者处理的。

（五）双方达成和解协议并已经执行，没有新情况、新理由的。

（六）被投诉机构已提供公平合理的解决方案，投诉人就同一事项再次向中国人民银行分支机构投诉的。

（七）其他不符合法律、行政法规、规章有关规定的。

第四十三条 中国人民银行分支机构收到金融消费者投诉的，应当自收到投诉之日起7个工作日内作出下列处理：

（一）对投诉人和被投诉机构信息、投诉请求、事实和理由等进行登记。

（二）作出是否接收投诉的决定。决定不予接收的，应当告知投诉人。

（三）决定接收投诉的，应当将投诉转交被投诉机构处理或者转交金融消费纠纷调解组织提供调解服务。

需要投诉人对投诉内容进行补正的，处理时限于补正完成之日起计算。

银行、支付机构应当自收到中国人民银行分支机构转交的投诉之日起15日内答复投诉人。情况复杂的，经本机构投诉处理工作负责人批准，可以延长处理期限，并告知投诉人延长处理期限的理由，但最长处理期限不得超过60日。

第四十四条 银行、支付机构收到中国人民银行分支机构转交的投诉，应当按要求向中国人民

安证合规集团&北清律师事务所

银行分支机构反馈投诉处理情况。

反馈的内容包括投诉基本情况、争议焦点、调查结果及证据、处理依据、与金融消费者的沟通情况、延期处理情况及投诉人满意度等。

银行、支付机构应当妥善保存投诉资料，投诉资料留存时间自投诉办结之日起不得少于3年。法律、行政法规另有规定的，从其规定。

第四十五条 银行、支付机构、金融消费者可以向调解组织申请调解、中立评估。调解组织受理调解、中立评估申请后，可在合理、必要范围内请求当事人协助或者提供相关文件、资料。

本办法所称中立评估，是指调解组织聘请独立专家就争议解决提出参考性建议的行为。

第四十六条 金融消费纠纷调解组织应当依照法律、行政法规、规章及其章程的规定，组织开展金融消费纠纷调解、中立评估等工作，对银行、支付机构和金融消费者进行金融知识普及和教育宣传引导。

第五章 监督与管理机制

第四十七条 中国人民银行综合研究金融消费者保护重大问题，负责拟定发展规划和业务标准，建立健全金融消费者保护基本制度。

第四十八条 中国人民银行及其分支机构与其他金融管理部门、地方政府有关部门建立健全金融消费者权益保护工作协调机制，加强跨市场跨业态跨区域金融消费者权益保护的监管，强化信息共享和部门间沟通协作。

第四十九条 中国人民银行及其分支机构统筹开展金融消费者教育，引导、督促银行、支付机构开展金融知识普及宣传活动，协调推进金融知识纳入国民教育体系，组织开展消费者金融素养调查。

第五十条 中国人民银行及其分支机构会同有关部门构建监管执法合作机制，探索合作开展金融消费者权益保护监督检查、评估等具体工作。

第五十一条 中国人民银行及其分支机构牵头构建非诉第三方解决机制，鼓励、支持金融消费者权益保护社会组织依法履行职责，推动构建公正、高效、便捷的多元化金融消费纠纷解决体系。

第五十二条 中国人民银行及其分支机构协调推进相关普惠金融工作，建立健全普惠金融工作机制，指导、督促银行、支付机构落实普惠金融发展战略，组织开展职责范围内的普惠金融具体工作。

第五十三条 中国人民银行及其分支机构对金融消费者投诉信息进行汇总和分析，根据汇总和分析结果适时优化金融消费者权益保护监督管理方式、金融机构行为规范等。

第五十四条 中国人民银行及其分支机构可以采取下列措施，依法在职责范围内开展对银行、

安证合规集团&北源律师事务所

支付机构金融消费者权益保护工作的监督检查：

（一）进入被监管机构进行检查。

（二）询问被监管机构的工作人员，要求其对有关检查事项作出说明。

（三）查阅、复制被监管机构与检查事项有关的文件、资料，对可能被转移、隐匿或者毁损的文件、资料予以登记保存。

（四）检查被监管机构的计算机网络与信息系统。

进行现场检查时，检查人员不得少于二人，并应当出示合法证件和检查通知书。

银行、支付机构应当积极配合中国人民银行及其分支机构的现场检查和非现场检查，如实提供有关资料，不得拒绝、阻挠、逃避检查，不得谎报、隐匿、销毁相关证据材料。

第五十五条 银行、支付机构有侵害金融消费者合法权益行为的，中国人民银行及其分支机构可以对其采取下列措施：

（一）要求提交书面说明或者承诺。

（二）约见谈话。

（三）责令限期整改。

（四）视情将相关信息向其上级机构、行业监管部门反馈，在行业范围内发布，或者向社会公布。

（五）建议银行、支付机构对直接负责的董事、高级管理人员和其他直接责任人员给予处分。

（六）依法查处或者建议其他行政管理部门依法查处。

（七）中国人民银行职责范围内依法可以采取的其他措施。

第五十六条 中国人民银行及其分支机构组织开展银行、支付机构履行金融消费者权益保护义务情况的评估工作。

评估工作以银行、支付机构自评估为基础。银行、支付机构应当按年度进行自评估，并于次年1月31日前向中国人民银行或其分支机构报送自评估报告。

中国人民银行及其分支机构根据日常监督管理、投诉管理以及银行、支付机构自评估等情况进行非现场评估，必要时可以进行现场评估。

第五十七条 中国人民银行及其分支机构可以根据具体情况开展金融消费者权益保护环境评估工作。

第五十八条 中国人民银行及其分支机构建立金融消费者权益保护案例库制度，按照预防为先、教育为主的原则向银行、支付机构和金融消费者进行风险提示。

第五十九条 中国人民银行及其分支机构对于涉及金融消费者权益保护的重大突发事件，应当

安证合规集团&北源律师事务所

按照有关规定做好相关应急处置工作。

第六章 法律责任

第六十条 银行、支付机构有下列情形之一，侵害消费者金融信息依法得到保护的权利的，中国人民银行或其分支机构应当在职责范围内依照《中华人民共和国消费者权益保护法》第五十六条的规定予以处罚：

（一）未经金融消费者明示同意，收集、使用其金融信息的。

（二）收集与业务无关的消费者金融信息，或者采取不正当方式收集消费者金融信息的。

（三）未公开收集、使用消费者金融信息的规则，未明示收集、使用消费者金融信息的目的、方式和范围的。

（四）超出法律法规规定和双方约定的用途使用消费者金融信息的。

（五）未建立以分级授权为核心的消费者金融信息使用管理制度，或者未严格落实信息使用授权审批程序的。

（六）未采取技术措施和其他必要措施，导致消费者金融信息遗失、毁损、泄露或者被篡改，或者非法向他人提供的。

第六十一条 银行、支付机构有下列情形之一，对金融产品或者服务作出虚假或者引人误解的宣传的，中国人民银行或其分支机构应当在职责范围内依照《中华人民共和国消费者权益保护法》第五十六条的规定予以处罚：

（一）实际承担的义务低于在营销宣传活动中通过广告、资料或者说明等形式对金融消费者所承诺的标准的。

（二）引用不真实、不准确的数据和资料或者隐瞒限制条件等，对过往业绩或者产品收益进行夸大表述的。

（三）利用金融管理部门对金融产品或者服务的审核或者备案程序，误导金融消费者认为金融管理部门已对该金融产品或者服务提供保证的。

（四）明示或者暗示保本、无风险或者保收益等，对非保本投资型金融产品的未来效果、收益或者相关情况作出保证性承诺的。

第六十二条 银行、支付机构违反本办法规定，有下列情形之一，有关法律、行政法规有处罚规定的，依照其规定给予处罚；有关法律、行政法规未作处罚规定的，中国人民银行或其分支机构应当根据情形单处或者并处警告、处以五千元以上三万元以下罚款：

（一）未建立金融消费者权益保护专职部门或者指定牵头部门，或者金融消费者权益保护部门没有足够的人力、物力独立开展工作的。

安证合规集团&北源律师事务所

（二）擅自代理金融消费者办理业务，擅自修改金融消费者的业务指令，或者强制搭售其他产品或者服务的。

（三）未按要求向金融消费者披露与金融产品和服务有关的重要内容的。

（四）利用技术手段、优势地位，强制或者变相强制金融消费者接受金融产品或者服务，或者排除、限制金融消费者接受同业机构提供的金融产品或者服务的。

（五）通过附加限制性条件的方式要求金融消费者购买、使用协议中未作明确要求的产品或者服务的。

（六）未按要求使用格式条款的。

（七）出现侵害金融消费者合法权益重大事件未及时向中国人民银行或其分支机构报告的。

（八）不配合中国人民银行及其分支机构开展金融消费者权益保护领域相关工作，或者未按照规定报送相关资料的。

（九）未按要求对金融消费者投诉进行正确分类，或者迟报、漏报、谎报、错报、瞒报投诉数据的。

（十）收到中国人民银行分支机构转交的投诉后，未在规定期限内答复投诉人，或者未按要求向中国人民银行分支机构反馈投诉处理情况的。

（十一）拒绝、阻挠、逃避检查，或者谎报、隐匿、销毁相关证据材料的。

第六十三条 对银行、支付机构侵害金融消费者权益重大案件负有直接责任的董事、高级管理人员和其他直接责任人员，有关法律、行政法规有处罚规定的，依照其规定给予处罚；有关法律、行政法规未作处罚规定的，中国人民银行或其分支机构应当根据情形单处或者并处警告、处以五千元以上三万元以下罚款。

第六十四条 中国人民银行及其分支机构的工作人员在开展金融消费者权益保护工作过程中有下列情形之一的，依法给予处分；涉嫌构成犯罪的，移送司法机关依法追究刑事责任：

（一）违反规定对银行、支付机构进行检查的。

（二）泄露知悉的国家秘密或者商业秘密的。

（三）滥用职权、玩忽职守的其他行为。

第七章 附 则

第六十五条 商业银行理财子公司、金融资产管理公司、信托公司、汽车金融公司、消费金融公司以及征信机构、个人本外币兑换特许业务经营机构参照适用本办法。法律、行政法规另有规定的，从其规定。

第六十六条 本办法中除“工作日”以外的“日”为自然日。

安证合规集团&北源律师事务所

第六十七条 本办法由中国人民银行负责解释。

第六十八条 本办法自2020年11月1日起施行。《中国人民银行金融消费权益保护工作管理办法（试行）》（银办发〔2013〕107号文印发）与《中国人民银行金融消费者权益保护实施办法》（银发〔2016〕314号文印发）同时废止。

个人信息和重要数据出境安全评估办法（征求意见稿）

基本信息:	
【发布机关】国家互联网信息办公室	【时效性】 未施行
【发文字号】-	【效力级别】部门规范性文件
【发布日期】2017.04.11	【实施日期】-

个人信息和重要数据出境安全评估办法（征求意见稿）

第一条 为保障个人信息和重要数据安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法利益，根据《中华人民共和国国家安全法》《中华人民共和国网络安全法》等法律法规，制定本办法。

第二条 网络运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据，应当在境内存储。因业务需要，确需向境外提供的，应当按照本办法进行安全评估。

第三条 数据出境安全评估应遵循公正、客观、有效的原则，保障个人信息和重要数据安全，促进网络信息依法有序自由流动。

第四条 个人信息出境，应向个人信息主体说明数据出境的目的、范围、内容、接收方及接收方所在的国家或地区，并经其同意。未成年人个人信息出境须经其监护人同意。

第五条 国家网信部门统筹协调数据出境安全评估工作，指导行业主管或监管部门组织开展数据出境安全评估。

第六条 行业主管或监管部门负责本行业数据出境安全评估工作，定期组织开展本行业数据出境安全检查。

第七条 网络运营者应在数据出境前，自行组织对数据出境进行安全评估，并对评估结果负责。

第八条 数据出境安全评估应重点评估以下内容:

安证合规集团&北源律师事务所

（一）数据出境的必要性；

（二）涉及个人信息情况，包括个人信息的数量、范围、类型、敏感程度，以及个人信息主体是否同意其个人信息出境等；

（三）涉及重要数据情况，包括重要数据的数量、范围、类型及其敏感程度等；

（四）数据接收方的安全保护措施、能力和水平，以及所在国家和地区的网络安全环境等；

（五）数据出境及再转移后被泄露、毁损、篡改、滥用等风险；

（六）数据出境及出境数据汇聚可能对国家安全、社会公共利益、个人合法利益带来的风险；

（七）其他需要评估的重要事项。

第九条 出境数据存在以下情况之一的，网络运营者应报请行业主管或监管部门组织安全评估：

（一）含有或累计含有50万人以上的个人信息；

（二）数据量超过1000GB；

（三）包含核设施、化学生物、国防军工、人口健康等领域数据，大型工程活动、海洋环境以及敏感地理信息数据等；

（四）包含关键信息基础设施的系统漏洞、安全防护等网络安全信息；

（五）关键信息基础设施运营者向境外提供个人信息和重要数据；

（六）其他可能影响国家安全和社会公共利益，行业主管或监管部门认为应该评估。

行业主管或监管部门不明确的，由国家网信部门组织评估。

第十条 行业主管或监管部门组织的安全评估，应当于六十个工作日内完成，及时向网络运营者反馈安全评估情况，并报国家网信部门。

第十一条 存在以下情况之一的，数据不得出境：

（一）个人信息出境未经个人信息主体同意，或可能侵害个人利益；

（二）数据出境给国家政治、经济、科技、国防等安全带来风险，可能影响国家安全、损害社会公共利益；

（三）其他经国家网信部门、公安部门、安全部门等有关部门认定不能出境的。

第十二条 网络运营者应根据业务发展和网络运营情况，每年对数据出境至少进行一次安全评估，及时将评估情况报行业主管或监管部门。

当数据接收方出现变更，数据出境目的、范围、数量、类型等发生较大变化，数据接收方或出境数据发生重大安全事件时，应及时重新进行安全评估。

第十三条 对违反相关法律法规和本办法向境外提供数据的行为，任何个人和组织有权向国

安证合规集团&北源律师事务所

家网信部门、公安部门等有关部门举报。

第十四条 违反本办法规定的，依照有关法律法规进行处罚。

第十五条 我国政府与其他国家、地区签署的关于数据出境的协议，按照协议的规定执行。

涉及国家秘密信息的按照相关规定执行。

第十六条 其他个人和组织在中华人民共和国境内收集和产生的个人信息和重要数据出境的安全评估工作参照本办法执行。

第十七条 本办法下列用语的含义：

网络运营者，是指网络的所有者、管理者和网络服务提供者。

数据出境，是指网络运营者将在中华人民共和国境内运营中收集和产生的个人信息和重要数据，提供给位于境外的机构、组织、个人。

个人信息，是指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。

重要数据，是指与国家安全、经济发展，以及社会公共利益密切相关的数据，具体范围参照国家有关标准和重要数据识别指南。

第十八条 本办法自2017年 月 日起实施。

个人信息出境安全评估办法（征求意见稿）

基本信息：	
【发布机关】国家互联网信息办公室	【时效性】 未施行
【发文字号】-	【效力级别】部门规章
【发布日期】2019.06.13	【实施日期】-

个人信息出境安全评估办法（征求意见稿）

第一条 为保障数据跨境流动中的个人信息安全，根据《中华人民共和国网络安全法》等相关法律法规，制定本办法。

第二条 网络运营者向境外提供在中华人民共和国境内运营中收集的个人信息（以下称个人信息出境），应当按照本办法进行安全评估。经安全评估认定个人信息出境可能影响国家安全、

安汇合规集团&北源律师事务所

损害公共利益，或者难以有效保障个人信息安全的，不得出境。

国家关于个人信息出境另有规定的，从其规定。

第三条 个人信息出境前，网络运营者应当向所在地省级网信部门申报个人信息出境安全评估。

向不同的接收者提供个人信息应当分别申报安全评估，向同一接收者多次或连续提供个人信息无需多次评估。

每2年或者个人信息出境目的、类型和境外保存时间发生变化时应当重新评估。

第四条 网络运营者申报个人信息出境安全评估应当提供以下材料，并对材料的真实性、准确性负责：

（一）申报书。

（二）网络运营者与接收者签订的合同。

（三）个人信息出境安全风险及安全保障措施分析报告。

（四）国家网信部门要求提供的其他材料。

第五条 省级网信部门在收到个人信息出境安全评估申报材料并核查其完备性后，应当组织专家或技术力量进行安全评估。安全评估应当在15个工作日内完成，情况复杂的可以适当延长。

第六条 个人信息出境安全评估重点评估以下内容：

（一）是否符合国家有关法律法规和政策规定。

（二）合同条款是否能够充分保障个人信息主体合法权益。

（三）合同能否得到有效执行。

（四）网络运营者或接收者是否有损害个人信息主体合法权益的历史、是否发生过重大网络安全事件。

（五）网络运营者获得个人信息是否合法、正当。

（六）其他应当评估的内容。

第七条 省级网信部门在将个人信息出境安全评估结论通报网络运营者的同时，将个人信息出境安全评估情况报国家网信部门。

网络运营者对省级网信部门的个人信息出境安全评估结论存在异议的，可以向国家网信部门提出申诉。

第八条 网络运营者应当建立个人信息出境记录并且至少保存5年，记录包括：

（一）向境外提供个人信息的日期时间。

（二）接收者的身份，包括但不限于接收者的名称、地址、联系方式等。

安证合规集团&北源律师事务所

（三）向境外提供的个人信息的类型及数量、敏感程度。

（四）国家网信部门规定的其他内容。

第九条 网络运营者应当每年12月31日前将本年度个人信息出境情况、合同履行情况等报所在地省级网信部门。

发生较大数据安全事件时，应及时报所在地省级网信部门。

第十条 省级网信部门应当定期组织检查运营者的个人信息出境记录等个人信息出境情况，重点检查合同规定义务的履行情况、是否存在违反国家规定或损害个人信息主体合法权益的行为等。

发现损害个人信息主体合法权益、数据泄露安全事件等情况时，应当及时要求网络运营者整改，通过网络运营者督促接收者整改。

第十一条 出现以下情况之一时，网信部门可以要求网络运营者暂停或终止向境外提供个人信息：

（一）网络运营者或接收者发生较大数据泄露、数据滥用等事件。

（二）个人信息主体不能或者难以维护个人合法权益。

（三）网络运营者或接收者无力保障个人信息安全。

第十二条 任何个人和组织有权对违反本办法规定向境外提供个人信息的行为，向省级以上网信部门或者相关部门举报。

第十三条 网络运营者与个人信息接收者签订的合同或者其他有法律效力的文件（统称合同），应当明确：

（一）个人信息出境的目的、类型、保存时限。

（二）个人信息主体是合同中涉及个人信息主体权益的条款的受益人。

（三）个人信息主体合法权益受到损害时，可以自行或者委托代理人向网络运营者或者接收者或者双方索赔，网络运营者或者接收者应当予以赔偿，除非证明没有责任。

（四）接收者所在国家法律环境发生变化导致合同难以履行时，应当终止合同，或者重新进行安全评估。

（五）合同的终止不能免除合同中涉及个人信息主体合法权益有关条款规定的网络运营者和接收者的责任和义务，除非接收者已经销毁了接收到的个人信息或作了匿名化处理。

（六）双方约定的其他内容。

第十四条 合同应当明确网络运营者承担以下责任和义务：

（一）以电子邮件、即时通信、信函、传真等方式告知个人信息主体网络运营者和接收者的

安证合规集团&北源律师事务所

基本情况，以及向境外提供个人信息的目的、类型和保存时间。

（二）应个人信息主体的请求，提供本合同的副本。

（三）应请求向接收者转达个人信息主体诉求，包括向接收者索赔；个人信息主体不能从接收者获得赔偿时，先行赔付。

第十五条 合同应当明确接收者承担以下责任和义务：

（一）为个人信息主体提供访问其个人信息的途径，个人信息主体要求更正或者删除其个人信息时，应在合理的代价和时限内予以响应、更正或者删除。

（二）按照合同约定的目的使用个人信息，个人信息的境外保存期限不得超出合同约定的时限。

（三）确认签署合同及履行合同义务不会违背接收者所在国家的法律要求，当接收者所在国家和地区法律环境发生变化可能影响合同执行时，应当及时通知网络运营者，并通过网络运营者报告网络运营者所在地省级网信部门。

第十六条 合同应当明确接收者不得将接收到的个人信息传输给第三方，除非满足以下条件：

（一）网络运营者已经通过电子邮件、即时通信、信函、传真等方式将个人信息传输给第三方的目的、第三方的身份和国别，以及传输的个人信息类型、第三方保留时限等通知个人信息主体。

（二）接收者承诺在个人信息主体请求停止向第三方传输时，停止传输并要求第三方销毁已经接收到的个人信息。

（三）涉及到个人敏感信息时，已征得个人信息主体同意。

（四）因向第三方传输个人信息对个人信息主体合法权益带来损害时，网络运营者同意先行承担赔付责任。

第十七条 网络运营者关于个人信息出境安全风险及安全保障措施分析报告应当至少包括：

（一）网络运营者和接收者的背景、规模、业务、财务、信誉、网络安全能力等。

（二）个人信息出境计划，包括持续时间、涉及的个人信息主体数量、向境外提供的个人信息规模、个人信息出境后是否会再向第三方传输等。

（三）个人信息出境风险分析和保障个人信息安全和个人信息主体合法权益的措施。

第十八条 网络运营者违反本办法规定向境外提供个人信息的，依照有关法律法规进行处理。

第十九条 我国参与的或者与其他国家和地区、国际组织缔结的条约、协议等对个人信息出境有明确规定的，适用其规定，我国声明保留的条款除外。

第二十条 境外机构经营活动中，通过互联网等收集境内用户个人信息，应当在境内通过法

安证合规集团&北源律师事务所

定代表人或者机构履行本办法中网络运营者的责任和义务。

第二十一条 本办法下列用语的含义:

（一）网络运营者，是指网络的所有者、管理者和网络服务提供者。

（二）个人信息，是指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。

（三）个人敏感信息，是指一旦被泄露、窃取、篡改、非法使用可能危害个人信息主体人身、财产安全，或导致个人信息主体名誉、身心健康受到损害等的个人信息。

第二十二条 本办法自 年 月 日起实施。

安证合规集团&北源律师事务所

App违法违规收集使用个人信息行为认定方法

基本信息：	
【发布机关】国家互联网信息办公室，工业和信息化部，公安部，国家市场监督管理总局	【时效性】 现行有效
	【效力级别】部门工作文件
【发文字号】国信办秘字[2019]191号	【实施日期】2019.12.30
【发布日期】2019.12.30	

关于印发《App违法违规收集使用个人信息行为认定方法》的通知

国信办秘字〔2019〕191号

各省、自治区、直辖市及新疆生产建设兵团网信办、通信管理局、公安厅(局)、市场监管局(厅、委)：

根据《关于开展App违法违规收集使用个人信息专项治理的公告》，为认定App违法违规收集使用个人信息行为提供参考，落实《网络安全法》

等法律法规，国家互联网信息办公室、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》。现印发你们，请结合监管和执法工作实际参考执行。

国家互联网信息办公室秘书局

工业和信息化部办公厅

公安部办公厅

市场监管总局办公厅

2019年11月28日

App违法违规收集使用个人信息行为认定方法

根据《关于开展App违法违规收集使用个人信息专项治理的公告》，为监督管理部门认定App违法违规收集使用个人信息行为提供参考，为App

运营者自查自纠和网民社会监督提供指引，落实《网络安全法》等法律法规，制定本方法。

一、以下行为可被认定为“未公开收集使用规则”

1.在App中没有隐私政策，或者隐私政策中没有收集使用个人信息规则；

2.在App首次运行时未通过弹窗等明显方式提示用户阅读隐私政策等收集使用规则；

3.隐私政策等收集使用规则难以访问，如进入App主界面后，需多于4次点击等操作才能访问到；

安证合规集团&北源律师事务所

4.隐私政策等收集使用规则难以阅读，如文字过小过密、颜色过淡、模糊不清，或未提供简体中文版等。

二、以下行为可被认定为“未明示收集使用个人信息的目的、方式和范围”

1.未逐一列出App(包括委托的第三方或嵌入的第三方代码、插件)收集使用个人信息的目的、方式、范围等；

2.收集使用个人信息的目的、方式、范围发生变化时，未以适当方式通知用户，适当方式包括更新隐私政策等收集使用规则并提醒用户阅读等；

3.在申请打开可收集个人信息的权限，或申请收集用户身份证号、银行账号、行踪轨迹等个人敏感信息时，未同步告知用户其目的，或者目的不明确、难以理解；

4.有关收集使用规则的内容晦涩难懂、冗长繁琐，用户难以理解，如使用大量专业术语等。

三、以下行为可被认定为“未经用户同意收集使用个人信息”

1.征得用户同意前就开始收集个人信息或打开可收集个人信息的权限；

2.用户明确表示不同意后，仍收集个人信息或打开收集个人信息的权限，或频繁征求用户同意、干扰用户正常使用；

3.实际收集的个人信息或打开的可收集个人信息权限超出用户授权范围；

4.以默认选择同意隐私政策等非明示方式征求用户同意；

5.未经用户同意更改其设置的可收集个人信息权限状态，如App更新时自动将用户设置的权限恢复到默认状态；

6.利用用户个人信息和算法定向推送信息，未提供非定向推送信息的选项；

7.以欺诈、诱骗等不正当方式误导用户同意收集个人信息或打开可收集个人信息的权限，如故意欺瞒、掩饰收集使用个人信息的真实目的；

8.未向用户提供撤回同意收集个人信息的途径、方式；

9.违反其所声明的收集使用规则，收集使用个人信息。

四、以下行为可被认定为“违反必要原则，收集与其提供的服务无关的个人信息”

1.收集的个人信息类型或打开的可收集个人信息权限与现有业务功能无关；

2.因用户不同意收集非必要个人信息或打开非必要权限，拒绝提供业务功能；

3.App新增业务功能申请收集的个人信息超出用户原有同意范围，若用户不同意，则拒绝提供原有业务功能，新增业务功能取代原有业务功能的除外；

4.收集个人信息的频度等超出业务功能实际需要；

安证合规集团&北源律师事务所

5.仅以改善服务质量、提升用户体验、定向推送信息、研发新产品等为由，强制要求用户同意收集个人信息；

6.要求用户一次性同意打开多个可收集个人信息的权限，用户不同意则无法使用。

五、以下行为可被认定为“未经同意向他人提供个人信息”

1.既未经用户同意，也未做匿名化处理，App客户端直接向第三方提供个人信息，包括通过客户端嵌入的第三方代码、插件等方式向第三方提供个人信息；

2.既未经用户同意，也未做匿名化处理，数据传输至App后台服务器后，向第三方提供其收集的个人信息；

3.App接入第三方应用，未经用户同意，向第三方应用提供个人信息。

六、以下行为可被认定为“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”

1.未提供有效的更正、删除个人信息及注销用户账号功能；

2.为更正、删除个人信息或注销用户账号设置不必要或不合理条件；

3.虽提供了更正、删除个人信息及注销用户账号功能，但未及时响应用户相应操作，需人工处理的，未在承诺时限内（承诺时限不得超过15个工作日，无承诺时限的，以15个工作日为限）完成核查和处理；

4.更正、删除个人信息或注销用户账号等用户操作已执行完毕，但App后台并未完成的；

5.未建立并公布个人信息安全投诉、举报渠道，或未在承诺时限内（承诺时限不得超过15个工作日，无承诺时限的，以15个工作日为限）受理_并处理的。

关于开展纵深推进APP侵害用户权益专项整治行动的通知

基本信息：

【发布机关】工业和信息化部	【时效性】现行有效
【发文字号】工信部信管函〔2020〕164号	【效力级别】部门工作文件
【发布日期】2020.07.22	【实施日期】2020.07.22

工信部信管函〔2020〕164号

各省、自治区、直辖市通信管理局，中国信息通信研究院、中国互联网协会，各相关单位：

安证合规集团&北源律师事务所

按照2020年信息通信行业行风建设暨纠风工作部署，为切实加强用户个人信息保护，为人民群众提供更安全、更健康、更干净的信息环境，我部决定开展纵深推进APP侵害用户权益专项整治行动。专项整治时间为通知印发之日至2020年12月10日。具体事项通知如下：

一、整治目标

依据《网络安全法》、《电信条例》、《规范互联网信息服务市场秩序若干规定》（工业和信息化部令第20号）、《电信和互联网用户个人信息保护规定》（工业和信息化部令第24号）和《移动智能终端应用软件预置和分发管理暂行规定》（工信部信管〔2016〕407号）等规定，深入推进技管结合，加强监督检查，督促相关企业强化APP个人信息保护，及时整改消除违规收集、使用用户个人信息和骚扰用户、欺骗误导用户、应用分发平台管理责任落实不到位等突出问题，净化APP应用空间。2020年8月底前上线运行全国APP技术检测平台管理系统，12月10日前完成覆盖40万款主流APP检测工作。

二、整治对象

（一）APP服务提供者，即互联网信息服务提供者提供的可以下载、安装、升级的应用软件，包括快应用和小程序等新应用形态。

（二）软件工具开发包（SDK）提供者，即集成在手机APP里的第三方工具集合。

（三）应用分发平台，包括网站、应用商店、APP等承担下载、安装、升级等分发服务的各类平台。

三、整治任务

（一）APP、SDK违规处理用户个人信息方面。

1.违规收集个人信息。重点整治APP、SDK未告知用户收集个人信息的目的、方式、范围且未经用户同意，私自收集用户个人信息的行为。

2.超范围收集个人信息。重点整治APP、SDK非服务所必需或无合理应用场景，特别是在静默状态下或在后台运行时，超范围收集个人信息的行为。

3.违规使用个人信息。重点整治APP、SDK未向用户告知且未经用户同意，私自使用个人信息，将用户个人信息用于其提供服务之外的目的，特别是私自向其他应用或服务器发送、共享用户个人信息的行为。

4.强制用户使用定向推送功能。重点整治APP、SDK未以显著方式标示且未经用户同意，将收集到的用户搜索、浏览记录、使用习惯等个人信息，用于定向推送或广告精准营销，且未提供关闭该功能选项的行为。

（二）设置障碍、频繁骚扰用户方面。

安证合规集团&北源律师事务所

5.APP强制、频繁、过度索取权限。重点整治APP安装、运行和使用相关功能时，非服务所必需或无合理应用场景下，用户拒绝相关授权申请

后，应用自动退出或关闭的行为。重点整治短时长、高频次，在用户明确拒绝权限申请后，频繁弹窗、反复申请与当前服务场景无关权限的行为。

重点整治未及时明确告知用户索取权限的目的和用途，提前申请超出其业务功能等权限的行为。

6.APP频繁自启动和关联启动。重点整治APP未向用户告知且未经用户同意，或无合理的使用场景，频繁自启动或关联启动第三方APP的行为。

（三）欺骗误导用户方面。

7.欺骗误导用户下载APP。重点整治通过“偷梁换柱”“移花接木”等方式欺骗误导用户下载APP，特别是具有分发功能的移动应用程序欺骗误

导用户下载非用户所自愿下载APP的行为。

8.欺骗误导用户提供个人信息。重点整治非服务所必需或无合理场景，通过积分、奖励、优惠等方式欺骗误导用户提供身份证号码以及个人生

物特征信息的行为。

（四）应用分发平台责任落实不到位方面。

9.应用分发平台上的APP信息明示不到位。重点整治应用分发平台上未明示APP运行所需权限列表及用途，未明示APP收集、使用用户个人信息的内容、目的、方式和范围等行为。

10.应用分发平台管理责任落实不到位。重点整治APP上架审核不严格、违法违规软件处理不及时和APP提供者、运营者、开发者身份信息不真实、联系方式虚假失效等问题。

四、工作要求

（一）开展检测检查。我部将于即日起组织第三方检测机构对APP、SDK进行技术检测，对应用分发平台的主体责任落实情况进行监督检查。对第一次检查发现存在问题的企业，我部将责令5个工作日内完成整改，对整改不彻底仍然存在问题的，将采取向社会公告、组织下架、行政处罚以及将受到行政处罚的违规主体纳入电信业务经营不良名单或失信名单等措施；对在APP不同版本中反复出现问题的企业，我部将向社会公告，并依法依规开展后续处置工作。

（二）抓好执行落实。各地通信管理局要结合实际开展检查工作，每月15日前将违规线索录入全国APP技术检测平台管理系统，并按照部工作要求开展相关问题处置。相关企业要及时开展自查自纠，对发现的问题立行立改，举一反三，切实有效保护个人信息。APP企业要完善用户权

安证合规集团&北源律师事务所

益保障制度，加强对所集成SDK的管理。应用分发平台要强化平台管理责任，积极配合电信主管部门开展相关监管工作。

（三）推动行业自律。鼓励行业协会组织APP开发运营者、应用分发平台、第三方服务提供者、电信设备生产企业、安全厂商等相关单位，制定行业自律公约和技术检测标准，健全第三方评议机制，强化行业规范。

（四）强化手段建设。中国信息通信研究院要大力推进全国APP技术检测平台管理系统建设，进一步凝聚产业力量，鼓励有条件的企业积极参与平台建设，提升自动化检测水平和能力。各地通信管理局要尽快接入，用好相关技术手段，做到关口前移，及时发现解决问题，不断提升行业治理能力和水平。

（五）畅通投诉渠道。专项整治工作期间，各企业应畅通用户投诉渠道，完善投诉处理服务机制和流程。中国互联网协会应通过互联网信息服务投诉平台（https://ts.isc.org.cn/）或12321举报中心接受群众投诉，及时汇总处理用户反映的相关问题。

工业和信息化部

2020年7月22日

关于开展App违法违规收集使用个人信息专项治理的公告

基本信息：	
【发布机关】中央网络安全和信息化委员会，工业和信息化部，公安部，国家市场监督管理总局	【时效性】 现行有效
	【效力级别】部门工作文件
【发文字号】-	【实施日期】2019.01.23
【发布日期】2019.01.23	

中央网信办 工业和信息化部 公安部 市场监管总局关于开展App违法违规收集使用个人信息专项治理的公告

〔2019年 第1号〕

近年来，移动互联网应用程序（App）得到广泛应用，在促进经济社会发展、服务民生等方面发挥了不可替代的作用。同时，App强制授权、过度索权、超范围收集个人信息的现象大量存在，违法违规使用个人信息的问题十分突出，广大网民对此反应强烈。落实《网络安全法》《消费者权益保护法》的要求，为保障个人信息安全，维护广大网民合法权益，中央网信办、工业和

信息化部、公安部、市场监管总局决定，自2019年1月至12月，在全国范围组织开展App违法违规收集使用个人信息专项治理。现将有关事项公告如下：

一、App运营者收集使用个人信息时要严格履行《网络安全法》规定的责任义务，对获取的个人信息安全负责，采取有效措施加强个人信息保护。遵循合法、正当、必要的原则，不收集与所提供服务无关的个人信息；收集个人信息时要以通俗易懂、简单明了的方式展示个人信息收集使用规则，并经个人信息主体自主选择同意；不以默认、捆绑、停止安装使用等手段变相强迫用户授权，不得违反法律法规和与用户的约定收集使用个人信息。倡导App运营者在定向推送新闻、时政、广告时，为用户提供拒绝接收定向推送的选项。

二、全国信息安全标准化技术委员会、中国消费者协会、中国互联网协会、中国网络空间安全协会，依据法律法规和国家相关标准，编制大众化应用基本业务功能及必要信息规范、App违法违规收集使用个人信息治理评估要点，组织相关专业机构，对用户数量大、与民众生活密切相关的App隐私政策和个人信息收集使用情况进行评估。

三、有关主管部门加强对违法违规收集使用个人信息行为的监管和处罚，对强制、过度收集个人信息，未经消费者同意、违反法律法规规定和双方约定收集、使用个人信息，发生或可能发生信息泄露、丢失而未采取补救措施，非法出售、非法向他人提供个人信息等行为，按照《网络安全法》《消费者权益保护法》等依法予以处罚，包括责令App运营者限期整改；逾期不改的，公开曝光；情节严重的，依法暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照。

四、公安机关开展打击整治网络侵犯公民个人信息违法犯罪专项工作，依法严厉打击针对和利用个人信息的违法犯罪行为。

五、开展App个人信息安全认证，鼓励App运营者自愿通过App个人信息安全认证，鼓励搜索引擎、应用商店等明确标识并优先推荐通过认证的App。

特此公告。

中央网信办 工业和信息化部

公安部 市场监管总局

2019年1月23日

工业和信息化部关于开展APP侵害用户权益专项整治工作的通知

基本信息：	
【发布机关】工业和信息化部	【时效性】 现行有效
【发文字号】工信部信管函〔2019〕337号	【效力级别】 部门工作文件
【发布日期】2019.11.06	【实施日期】2019.10.31

工信部信管函〔2019〕337号

各省、自治区、直辖市通信管理局，中国信息通信研究院、中国互联网协会，各相关单位：

当前，APP违规收集个人信息、过度索权、频繁骚扰、侵害用户权益等问题突出，群众反映强烈，社会关注度高。结合2019年信息通信行业行风建设暨纠风工作安排，我部决定组织开展APP侵害用户权益专项整治行动工作。有关事项通知如下：

一、整治内容

依据《网络安全法》、《电信条例》、《规范互联网信息服务市场秩序若干规定》（工业和信息化部令第20号）、《电信和互联网用户个人信息保护规定》（工业和信息化部令第24号）和《移动智能终端应用软件预置和分发管理暂行规定》（工信部信管〔2016〕407号）等法律法规和规范性文件要求，聚焦人民群众反映强烈和社会高度关注的侵犯用户权益行为，重点对以

下四个方面8类问题开展规范整治工作。

（一）违规收集用户个人信息方面

1.“私自收集个人信息”。即APP未明确告知收集使用个人信息的目的、方式和范围并获得用户同意前，收集用户个人信息。

2.“超范围收集个人信息”。即APP收集个人信息，非服务所必需或无合理应用场景，超范围或超频次收集个人信息，如通讯录、位置、身份证、人脸等。

（二）违规使用用户个人信息方面

3.“私自共享给第三方”。即APP未经用户同意与其他应用共享、使用用户个人信息，如设备识别信息、商品浏览记录、搜索使用习惯、常用软件应用列表等。

4.“强制用户使用定向推送功能”。即APP未向用户告知，或未以显著方式标示，将收集到的用户搜索、浏览记录、使用习惯等个人信息，用于定向推送或精准营销，且未提供关闭该功能的选项。

（三）不合理索取用户权限方面

京汇合规集团及北源律师事务所

5.“不给权限不让用”。即APP安装和运行时，向用户索取与当前服务场景无关的权限，用户拒绝授权后，应用退出或关闭。

6.“频繁申请权限”。即APP在用户明确拒绝权限申请后，频繁申请开启通讯录、定位、短信、录音、相机等与当前服务场景无关的权限，骚扰用户。

7.“过度索取权限”。即APP在用户未使用相关功能或服务时，提前申请开启通讯录、定位、短信、录音、相机等权限，或超出其业务功能或服务外，申请通讯录、定位、短信、录音、相机等权限。

（四）为用户账号注销设置障碍方面

8.“账号注销难”。即APP未向用户提供账号注销服务，或为注销服务设置不合理的障碍。

二、整治对象

本次专项整治工作主要面向两类对象：一是APP服务提供者，主要检查是否存在前述8类问题；二是APP分发服务提供者，含应用商店和基础电信企业营业厅等承担APP分发功能的各类企业，主要检查是否落实《移动智能终端应用软件预置和分发管理暂行规定》（工信部信管〔2016〕407号）等有关要求。

三、工作安排

专项整治工作时间为通知印发之日至2019年12月20日。分三个阶段实施：

（一）企业自查自纠阶段（通知印发之日起至11月10日）。APP服务提供者对照前述8类问题认真开展自查，发现问题及时整改；APP分发服务提供者组织对所分发APP进行全面检查，对存在问题的违规应用软件予以督促整改，拒不改正的应组织予以下架处理。

（二）监督抽查阶段（2019年11月11日至11月30日）。我部将组织第三方检测机构对APP进行技术检测和检查，重点抽测与群众生活密切相关、下载使用量较大的APP产品和分发平台。对群众反映强烈、难以接受、认为不合理的APP，我部将组织电信用户委员会、中国互联网协会以及相关媒体机构开展用户和专家评议。各省、自治区、直辖市通信管理局可根据本地实际情况开展检查工作，并将结果报部（信息通信管理局）。

（三）结果处置阶段（2019年12月1日至12月20日）。我部将对存在问题的APP统一进行通报，依法依规予以处理，具体措施包括责令整改、向社会公告、组织APP下架、停止APP接入服务，以及将受到行政处罚的违规主体纳入电信业务经营不良名单或失信名单等。

四、工作要求

京汇合规集团&北源律师事务所

（一）切实提高思想认识。各单位要坚决贯彻落实以人民为中心的发展思想，切实提高政治站位，高度重视本次专项整治工作，精心组织、周密部署，细化整治措施，着力解决群众最关心最直接最现实的利益问题，务求取得实效。

（二）畅通用户投诉渠道。专项整治工作期间，各企业应畅通用户投诉渠道，完善投诉处理服务机制和流程。中国互联网协会应通过互联网信息服务投诉平台（https://ts.isc.org.cn/）或12321举报中心接受群众投诉，及时汇总处理用户反映的相关问题。

（三）巩固建立长效机制。APP用户量大、影响面广、耦合性强，规范管理工作涉及主体多、链条长，需要企业自律、社会监督和政府监管的协同共治。各单位要以此次专项整治工作为契机，不断总结经验、分析原因、举一反三、巩固成效，为后续规范行业管理奠定基础。

特此通知。

工业和信息化部

2019年10月31日

安证合规集团&北源律师事务所

第六篇 司法解释

最高人民法院关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定

基本信息：	
【发布机关】最高人民法院	【时效性】 现行有效
【发文字号】法释〔2021〕15号	【效力级别】司法解释
【发布日期】2021.07.27	【实施日期】2021.08.21

最高人民法院关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定（2021年6月8日最高人民法院审判委员会第1841次会议通过，自2021年8月1日起施行 法释〔2021〕15号）

为正确审理使用人脸识别技术处理个人信息相关民事案件，保护当事人合法权益，促进数字经济健康发展，根据《中华人民共和国民法典》《中华人民共和国网络安全法》《中华人民共和国消费者权益保护法》《中华人民共和国电子商务法》《中华人民共和国民事诉讼法》等法律的规定，结合审判实践，制定本规定。

第一条 因信息处理者违反法律、行政法规的规定或者双方的约定使用人脸识别技术处理人脸信息、处理基于人脸识别技术生成的人脸信息所引起的民事案件，适用本规定。javascript:void(0);

人脸信息的处理包括人脸信息的收集、存储、使用、加工、传输、提供、公开等。javascript:void(0);

本规定所称人脸信息属于民法典第一千零三十四条规定的“生物识别信息”。javascript:void(0);

第二条 信息处理者处理人脸信息有下列情形之一的，人民法院应当认定属于侵害自然人人格权益的行为：javascript:void(0);

（一）在宾馆、商场、银行、车站、机场、体育场馆、娱乐场所等经营场所、公共场所违反法律、行政法规的规定使用人脸识别技术进行人脸验证、辨识或者分析；javascript:void(0);

（二）未公开处理人脸信息的规则或者未明示处理的目的、方式、范围；javascript:void(0);

（三）基于个人同意处理人脸信息的，未征得自然人或者其监护人的单独同意，或者未按照

安证合规集团&北源律师事务所

法律、行政法规的规定征得自然人或者其监护人的书面同意；javascript:void(0);

（四）违反信息处理者明示或者双方约定的处理人脸信息的目的、方式、范围等；javascript:void(0);

（五）未采取应有的技术措施或者其他必要措施确保其收集、存储的人脸信息安全，致使人脸信息泄露、篡改、丢失；javascript:void(0);

（六）违反法律、行政法规的规定或者双方的约定，向他人提供人脸信息；javascript:void(0);

（七）违背公序良俗处理人脸信息；javascript:void(0);

（八）违反合法、正当、必要原则处理人脸信息的其他情形。javascript:void(0);

第三条 人民法院认定信息处理者承担侵害自然人人格权益的民事责任，应当适用民法典第九百九十八条的规定，并结合案件具体情况综合考量受害人是否为未成年人、告知同意情况以及信息处理的必要程度等因素。javascript:void(0);

第四条 有下列情形之一，信息处理者以已征得自然人或者其监护人同意为由抗辩的，人民法院不予支持：javascript:void(0);

（一）信息处理者要求自然人同意处理其人脸信息才提供产品或者服务的，但是处理人脸信息属于提供产品或者服务所必需的除外；javascript:void(0);

（二）信息处理者以与其他授权捆绑等方式要求自然人同意处理其人脸信息的；javascript:void(0);

（三）强迫或者变相强迫自然人同意处理其人脸信息的其他情形。javascript:void(0);

第五条 有下列情形之一，信息处理者主张其不承担民事责任的，人民法院依法予以支持：javascript:void(0);

（一）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而处理人脸信息的；javascript:void(0);

（二）为维护公共安全，依据国家有关规定在公共场所使用人脸识别技术的；javascript:void(0);

（三）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人脸信息的；javascript:void(0);

（四）在自然人或者其监护人同意的范围内合理处理人脸信息的；javascript:void(0);

安证合规集团&北源律师事务所

（五）符合法律、行政法规规定的其他情形。javascript:void(0);

第六条 当事人请求信息处理者承担民事责任的，人民法院应当依据民事诉讼法第六十四条及《最高人民法院关于适用〈中华人民共和国民事诉讼法〉的解释》第九十条、第九十一条，《最高人民法院关于民事诉讼证据的若干规定》的相关规定确定双方当事人的举证责任。javascript:void(0);

信息处理者主张其行为符合民法典第一千零三十五条第一款规定情形的，应当就此所依据的事实承担举证责任。javascript:void(0);

信息处理者主张其不承担民事责任的，应当就其行为符合本规定第五条规定的情形承担举证责任。javascript:void(0);

第七条 多个信息处理者处理人脸信息侵害自然人人格权益，该自然人主张多个信息处理者按照过错程度和造成损害结果的大小承担侵权责任的，人民法院依法予以支持；符合民法典第一千一百六十八条、第一千一百六十九条第一款、第一千一百七十条、第一千一百七十一条等规定的相应情形，该自然人主张多个信息处理者承担连带责任的，人民法院依法予以支持。javascript:void(0);

信息处理者利用网络服务处理人脸信息侵害自然人人格权益的，适用民法典第一千一百九十五条、第一千一百九十六条、第一千一百九十七条等规定。javascript:void(0);

第八条 信息处理者处理人脸信息侵害自然人人格权益造成财产损失，该自然人依据民法典第一千一百八十二条主张财产损害赔偿的，人民法院依法予以支持。javascript:void(0);

自然人为制止侵权行为所支付的合理开支，可以认定为民法典第一千一百八十二条规定的财产损失。合理开支包括该自然人或者委托代理人对侵权行为进行调查、取证的合理费用。人民法院根据当事人的请求和具体案情，可以将合理的律师费用计算在赔偿范围内。javascript:void(0);

第九条 自然人有证据证明信息处理者使用人脸识别技术正在实施或者即将实施侵害其隐私权或者其他人格权益的行为，不及时制止将使其合法权益受到难以弥补的损害，向人民法院申请采取责令信息处理者停止有关行为的措施的，人民法院可以根据案件具体情况依法作出人格权侵害禁令。javascript:void(0);

第十条 物业服务企业或者其他建筑物管理人以人脸识别作为业主或者物业使用人出入物业服务区域的唯一验证方式，不同意的业主或者物业使用人请求其提供其他合理验证方式的，人民法院依法予以支持。javascript:void(0);

物业服务企业或者其他建筑物管理人存在本规定第二条规定的情形，当事人请求物业服务企

安证合规集团&北源律师事务所

业或者其他建筑物管理人承担侵权责任的，人民法院依法予以支持。javascript:void(0);

第十一条 信息处理者采用格式条款与自然人订立合同，要求自然人授予其无期限限制、不可撤销、可任意转授权等处理人脸信息的权利，该自然人依据民法典第四百九十七条请求确认格式条款无效的，人民法院依法予以支持。javascript:void(0);

第十二条 信息处理者违反约定处理自然人的人脸信息，该自然人请求其承担违约责任的，人民法院依法予以支持。该自然人请求信息处理者承担违约责任时，请求删除人脸信息的，人民法院依法予以支持；信息处理者以双方未对人脸信息的删除作出约定为由抗辩的，人民法院不予支持。javascript:void(0);

第十三条 基于同一信息处理者处理人脸信息侵害自然人人格权益发生的纠纷，多个受害人分别向同一人民法院起诉的，经当事人同意，人民法院可以合并审理。javascript:void(0);

第十四条 信息处理者处理人脸信息的行为符合民事诉讼法第五十五条、消费者权益保护法第四十七条或者其他法律关于民事公益诉讼的相关规定，法律规定的机关和有关组织提起民事公益诉讼的，人民法院应予受理。javascript:void(0);

第十五条 自然人死亡后，信息处理者违反法律、行政法规的规定或者双方的约定处理人脸信息，死者的近亲属依据民法典第九百九十四条请求信息处理者承担民事责任的，适用本规定。javascript:void(0);

第十六条 本规定自2021年8月1日起施行。javascript:void(0);

信息处理者使用人脸识别技术处理人脸信息、处理基于人脸识别技术生成的人脸信息的行为发生在本规定施行前的，不适用本规定。javascript:void(0);

安证合规集团&北源律师事务所

最高人民法院、最高人民检察院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

基本信息:	
【发布机关】最高人民法院，最高人民检察院	【时效性】 现行有效
	【效力级别】司法解释
【发文字号】法释[2017]10号	【实施日期】2017.06.01
【发布日期】2017.05.08	

《最高人民法院、最高人民检察院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》已于2017年3月20日由最高人民法院审判委员会第1712次会议、2017年4月26日由最高人民检察院第十二届检察委员会第63次会议通过，现予公布，自2017年6月1日起施行。

最高人民法院&最高人民检察院

2017年5月8日

法释〔2017〕10号

最高人民法院最高人民检察院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

（2017年3月20日最高人民法院审判委员会第1712次会议、2017年4月26日最高人民检察院第十二届检察委员会

第63次会议通过，自2017年6月1日起施行）

为依法惩治侵犯公民个人信息犯罪活动，保护公民个人信息安全和合法权益，根据《中华人民共和国刑法》《中华人民共和国刑事诉讼法》的有关规定，现就办理此类刑事案件适用法律的若干问题解释如下:

第一条刑法第二百五十三条之一规定的“公民个人信息”,是指以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息，包括姓名、身份证件号码、通信通讯联系方式、住址、账号密码、财产状况、行踪轨迹等。

第二条违反法律、行政法规、部门规章有关公民个人信息保护的规定的，应当认定为刑法第二百五十三条之一规定的“违反国家有关规定”。

第三条向特定人提供公民个人信息，以及通过信息网络或者其他途径发布公民个人信息的，应当认定为刑法第二百五十三条之一规定的“提供公民个人信息”。

未经被收集者同意，将合法收集的公民个人信息向他人提供的，属于刑法第二百五十三条之一规定的“提供公民个人信息”，但是经过处理无法识别特定个人且不能复原的除外。

第四条违反国家有关规定，通过购买、收受、交换等方式获取公民个人信息，或者在履行职责、提供服务过程中收集公民个人信息的，属于刑法第二百五十三条之一第三款规定的“以其他方法非法获取公民个人信息”。

第五条非法获取、出售或者提供公民个人信息，具有下列情形之一的，应当认定为刑法第二百五十三条之一规定的“情节严重”：

（一）出售或者提供行踪轨迹信息，被他人用于犯罪的；

（二）知道或者应当知道他人利用公民个人信息实施犯罪，向其出售或者提供的；

（三）非法获取、出售或者提供行踪轨迹信息、通信内容、征信信息、财产信息五十条以上的；

（四）非法获取、出售或者提供住宿信息、通信记录、健康生理信息、交易信息等其他可能影响人身、财产安全的公民个人信息五百条以上的；

（五）非法获取、出售或者提供第三项、第四项规定以外的公民个人信息五千条以上的；

（六）数量未达到第三项至第五项规定标准，但是按相应比例合计达到有关数量标准的；

（七）违法所得五千元以上的；

（八）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，数量或者数额达到第三项至第七项规定标准一半以上的；

（九）曾因侵犯公民个人信息受过刑事处罚或者二年内受过行政处罚，又非法获取、出售或者提供公民个人信息的；

（十）其他情节严重的情形。

实施前款规定的行为，具有下列情形之一的，应当认定为刑法第二百五十三条之一第一款规定的“情节特别严重”：

（一）造成被害人死亡、重伤、精神失常或者被绑架等严重后果的；

（二）造成重大经济损失或者恶劣社会影响的；

（三）数量或者数额达到前款第三项至第八项规定标准十倍以上的；

（四）其他情节特别严重的情形。

第六条为合法经营活动而非法购买、收受本解释第五条第一款第三项、第四项规定以外的公民个人信息，具有下列情形之一的，应当认定为刑法第二百五十三条之一规定的“情节严重”：

（一）利用非法购买、收受的公民个人信息获利五万元以上的；

（二）曾因侵犯公民个人信息受过刑事处罚或者二年内受过行政处罚，又非法购买、收受公民个人信息的；

（三）其他情节严重的情形。

实施前款规定的行为，将购买、收受的公民个人信息非法出售或者提供的，定罪量刑标准适用本解释第五条的规定。

第七条单位犯刑法第二百五十三条之一规定之罪的，依照本解释规定的相应自然人犯罪的定罪量刑标准，对直接负责的主管人员和其他直接责任人员定罪处罚，并对单位判处罚金。

第八条设立用于实施非法获取、出售或者提供公民个人信息违法犯罪活动的网站、通讯群组，情节严重的，应当依照刑法第二百八十七条之一的规定，以非法利用信息网络罪定罪处罚；同时构成侵犯公民个人信息罪的，依照侵犯公民个人信息罪定罪处罚。

第九条网络服务提供者拒不履行法律、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，致使用户的公民个人信息泄露，造成严重后果的，应当依照刑法第二百八十六条之一的规定，以拒不履行信息网络安全管理义务罪定罪处罚。

第十条实施侵犯公民个人信息犯罪，不属于“情节特别严重”，行为人系初犯，全部退赃，并确有悔罪表现的，可以认定为情节轻微，不起诉或者免予刑事处罚；确有必要判处刑罚的，应当从宽处罚。

第十一条非法获取公民个人信息后又出售或者提供的，公民个人信息的条数不重复计算。

向不同单位或者个人分别出售、提供同一公民个人信息的，公民个人信息的条数累计计算。

对批量公民个人信息的条数，根据查获的数量直接认定，但是有证据证明信息不真实或者重复的除外。

第十二条对于侵犯公民个人信息犯罪，应当综合考虑犯罪的危害程度、犯罪的违法所得数额以及被告人的前科情况、认罪悔罪态度等，依法判处罚金。罚金数额一般在违法所得的一倍以上五倍以下。

第十三条本解释自2017年6月1日起施行。

第七篇 标准等其他文件

信息安全技术 个人信息安全规范（2020）

基本信息：	
【发布机关】全国信息安全标准化技术委员会	【时效性】 现行有效
【标准编号】GB/T 35273-2020	【效力级别】国家标准
【发布日期】2020.03.06	【实施日期】2020.10.01

信息安全技术 个人信息安全规范（2020）

1 范围

本标准规定了开展收集、存储、使用、共享、转让、公开披露、删除等个人信息处理活动应遵循的原则和安全要求。

本标准适用于规范各类组织的个人信息处理活动，也适用于主管监管部门、第三方评估机构等组织对个人信息处理活动进行监督、管理和评估。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 25069—2010 信息安全技术 术语

3 术语和定义

GB/T 25069—2010界定的以及下列术语和定义适用于本文件。

3.1 个人信息 personal information

安证合规集团&北源律师事务所

以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息。

注1：个人信息包括姓名、出生日期、身份证件号码、个人生物识别信息、住址、通信通讯联系方式、通信记录和内容、账号密码、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息等。

注2：关于个人信息的判定方法和类型参见附录 A。

注3：个人信息控制者通过个人信息或其他信息加工处理后形成的信息，例如，用户画像或特征标签，能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的，属于个人信息。

3.2 个人敏感信息 personal sensitive information

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。

注1：个人敏感信息包括身份证件号码、个人生物识别信息、银行账户、通信记录和内容、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息、14岁以下（含）儿童的个人信息等。

注2：关于个人敏感信息的判定方法和类型参见附录 B。

注3：个人信息控制者通过个人信息或其他信息加工处理后形成的信息，如一旦泄露、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，属于个人敏感信息。

3.3 个人信息主体 personal information subject 个人信息所标识或者关联的自然人。

3.4 个人信息控制者 personal information controller

有能力决定个人信息处理目的、方式等的组织或个人。

3.5 收集 collect

获得个人信息的控制权的行为。

注1：包括由个人信息主体主动提供、通过与个人信息主体交互或记录个人信息主体行为等自动采集行为，以及通过共享、转让、搜集公开信息等间接获取个人信息等行为。

注2：如果产品或服务的提供者提供工具供个人信息主体使用，提供者不对个人信息进行访问的，则不属于本标准所称的收集。例如，离线导航软件在终端获取个人信息主体位置信息后，如果不回传至软件提供者，则不属于个人信息主体位置信息的收集。

3.6 明示同意 explicit consent

安证合规集团&北源律师事务所

个人信息主体通过书面、口头等方式主动作出纸质或电子形式的声明，或者自主作出肯定性动作，对其个人信息进行特定处理作出明确授权的行为。

注：肯定性动作包括个人信息主体主动勾选、主动点击“同意”“注册”“发送”“拨打”、主动填写或提供等。

3.7 授权同意 consent

个人信息主体对其个人信息进行特定处理作出明确授权的行为。

注：包括通过积极的行为作出授权（即明示同意），或者通过消极的不作为而作出授权（如信息采集区域内的个人信息主体在被告知信息收集行为后没有离开该区域）。

3.8 用户画像 user profiling

通过收集、汇聚、分析个人信息，对某特定自然人个人特征，如职业、经济、健康、教育、个人喜好、信用、行为等方面作出分析或预测，形成其个人特征模型的过程。

注：直接使用特定自然人的个人信息，形成该自然人的特征模型，称为直接用户画像。使用来源于特

定自然人以外的个人信息，如其所在群体的数据，形成该自然人的特征模型，称为间接用户画像。

3.9 个人信息安全影响评估 personal information security impact assessment

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。

3.10 删除 delete

在实现日常业务功能所涉及的系统中去除个人信息的行为，使其保持不可被检索、访问的状态。

3.11 公开披露 public disclosure

向社会或不特定人群发布信息的行为。

3.12 转让 transfer of control

将个人信息控制权由一个控制者向另一个控制者转移的过程。

3.13 共享 sharing

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。

3.14 匿名化 anonymization

通过对个人信息的技术处理，使得个人信息主体无法被识别或者关联，且处理后的信息不能被复原的过程。

安远合规集团&北京律师事务所

注：个人信息经匿名化处理后所得的信息不属于个人信息。

3.15　去标识化 de-identification

通过对个人信息的技术处理，使其在不借助额外信息的情况下，无法识别或者关联个人信息主体的过程。

注：去标识化建立在个体基础之上，保留了个体颗粒度，采用假名、加密、哈希函数等技术手段替代对个人信息的标识。

3.16　个性化展示 personalized display

基于特定个人信息主体的网络浏览历史、兴趣爱好、消费记录和习惯等个人信息，向该个人信息主体展示信息内容、提供商品或服务的搜索结果等活动。

3.17　业务功能 business function

满足个人信息主体的具体使用需求的服务类型。

注：如地图导航、网络约车、即时通讯、网络社区、网络支付、新闻资讯、网上购物、快递配送、交通票务等。

4 个人信息安全基本原则

个人信息控制者开展个人信息处理活动应遵循合法、正当、必要的原则，具体包括： a) 权责一致——采取技术和其他必要的措施保障个人信息的安全，对其个人信息处理活动对个人信息主体合法权益造成的损害承担责任；

b)目的明确——具有明确、清晰、具体的个人信息处理目的；

c)选择同意——向个人信息主体明示个人信息处理目的、方式、范围等规则，征求其授权同意；

d)最小必要——只处理满足个人信息主体授权同意的目的所需的最少个人信息类型和数量。目的达成后，应及时删除个人信息；

e)公开透明——以明确、易懂和合理的方式公开处理个人信息的范围、目的、规则等，并接受外部监督；

f)确保安全——具备与所面临的安全风险相匹配的安全能力，并采取足够的管理措施和技术手段，保护个人信息的保密性、完整性、可用性；

g)主体参与——向个人信息主体提供能够查询、更正、删除其个人信息，以及撤回授权同意、注销账户、投诉等方法。

5 个人信息的收集

5.1 收集个人信息的合法性

安证合规集团&北源律师事务所

对个人信息控制者的要求包括：

a)不应以欺诈、诱骗、误导的方式收集个人信息；

b)不应隐瞒产品或服务所具有的收集个人信息的功能；

c)不应从非法渠道获取个人信息。

5.2 收集个人信息的最小必要

对个人信息控制者的要求包括：

a)收集的个人信息的类型应与实现产品或服务的业务功能有直接关联；直接关联是指没有上述个人信息的参与，产品或服务的功能无法实现；

b)自动采集个人信息的频率应是实现产品或服务的业务功能所必需的最低频率；

c)间接获取个人信息的数量应是实现产品或服务的业务功能所必需的最少数量。

5.3 多项业务功能的自主选择

当产品或服务提供多项需收集个人信息的业务功能时，个人信息控制者不应违背个人信息主体的自主意愿，强迫个人信息主体接受产品或服务所提供的业务功能及相应的个人信息收集请求。对个人信息控制者的要求包括：

a)不应通过捆绑产品或服务各项业务功能的方式，要求个人信息主体一次性接受并授权同意其未申请或使用的业务功能收集个人信息的请求；

b)应把个人信息主体自主作出的肯定性动作，如主动点击、勾选、填写等，作为产品或服务的特定业务功能的开启条件。个人信息控制者应仅在个人信息主体开启该业务功能后，开始收集个人信息；

c)关闭或退出业务功能的途径或方式应与个人信息主体选择使用业务功能的途径或方式同样方便。个人信息主体选择关闭或退出特定业务功能后，个人信息控制者应停止该业务功能的个人信息收集活动；

d)个人信息主体不授权同意使用、关闭或退出特定业务功能的，不应频繁征求个人信息主体的授权同意；

e)个人信息主体不授权同意使用、关闭或退出特定业务功能的，不应暂停个人信息主体自主选择使用的其他业务功能，或降低其他业务功能的服务质量；

f)不得仅以改善服务质量、提升使用体验、研发新产品、增强安全性等为由，强制要求个人信息主体同意收集个人信息。

5.4 收集个人信息时的授权同意

对个人信息控制者的要求包括：

安证合规集团&北源律师事务所

a)收集个人信息，应向个人信息主体告知收集、使用个人信息的目的、方式和范围等规则，并获得个人信息主体的授权同意；

注1：如产品或服务仅提供一项收集、使用个人信息的业务功能时，个人信息控制者可通过个人信息保护政策的形式，实现向个人信息主体的告知；产品或服务提供多项收集、使用个人信息的业务功能的，除个人信息保护政策外，个人信息控制者宜在实际开始收集特定个人信息时，向个人信息主体提供收集、使用该个人信息的目的、方式和范围，以便个人信息主体在作出具体的授权同意前，能充分考虑对其的具体影响。

注2：符合5.3和 a）要求的实现方法，可参考附录C。

b)收集个人敏感信息前，应征得个人信息主体的明示同意，并应确保个人信息主体的明示同意是其在完全知情的基础上自主给出的、具体的、清晰明确的意愿表示；

c)收集个人生物识别信息前，应单独向个人信息主体告知收集、使用个人生物识别信息的目的、方式和范围，以及存储时间等规则，并征得个人信息主体的明示同意；

注：个人生物识别信息包括个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部识别特征等。

d)收集年满14周岁未成年人的个人信息前，应征得未成年人或其监护人的明示同意；不满14周岁的，应征得其监护人的明示同意； e) 间接获取个人信息时：

1)应要求个人信息提供方说明个人信息来源，并对其个人信息来源的合法性进行确认；

2)应了解个人信息提供方已获得的个人信息处理的授权同意范围，包括使用目的，个人信息主体是否授权同意转让、共享、公开披露、删除等；

3)如开展业务所需进行的个人信息处理活动超出已获得的授权同意范围的，应在获取个人信息后的合理期限内或处理个人信息前，征得个人信息主体的明示同意，或通过个人信息提供方征得个人信息主体的明示同意。

5.5 个人信息保护政策

对个人信息控制者的要求包括：

a)应制定个人信息保护政策，内容应包括但不限于：

1)个人信息控制者的基本情况，包括主体身份、联系方式；

2)收集、使用个人信息的业务功能，以及各业务功能分别收集的个人信息类型。涉及个人敏感信息的，需明确标识或突出显示；

3)个人信息收集方式、存储期限、涉及数据出境情况等个人信息处理规则；

4)对外共享、转让、公开披露个人信息的目的、涉及的个人信息类型、接收个人信息的第三方类型，以及各自的安全和法律责任；

安证合规集团&北源律师事务所

5)个人信息主体的权利和实现机制，如查询方法、更正方法、删除方法、注销账户的方法、撤回授权同意的方法、获取个人信息副本的方法、对信息系统自动决策结果进行投诉的方法等；

6)提供个人信息后可能存在的安全风险，及不提供个人信息可能产生的影响；

7)遵循的个人信息安全基本原则，具备的数据安全能力，以及采取的个人信息安全保护措施，必要时可公开数据安全和个人信息保护相关的合规证明；

8)处理个人信息主体询问、投诉的渠道和机制，以及外部纠纷解决机构及联络方式。

b)个人信息保护政策所告知的信息应真实、准确、完整；

c)个人信息保护政策的内容应清晰易懂，符合通用的语言习惯，使用标准化的数字、图示等，避免使用有歧义的语言；

d)个人信息保护政策应公开发布且易于访问，例如，在网站主页、移动互联网应用程序安装页、附录C中的交互界面或设计等显著位置设置链接；

e)个人信息保护政策应逐一送达个人信息主体。当成本过高或有显著困难时，可以公告的形式发布；

f)在a）所载事项发生变化时，应及时更新个人信息保护政策并重新告知个人信息主体。

注1：组织会习惯性将个人信息保护政策命名为“隐私政策”或其他名称，其内容宜与个人信息保护政策内容保持一致。

注2：个人信息保护政策的内容可参考附录D。

注3：在个人信息主体首次打开产品或服务、注册账户等情形时，宜通过弹窗等形式主动向其展示个人信息保护政策的主要或核心内容，帮助个人信息主体理解该产品或服务的个人信息处理范围和规则，并决定是否继续使用该产品或服务。

5.6 征得授权同意的例外

以下情形中，个人信息控制者收集、使用个人信息不必征得个人信息主体的授权同意：

a)与个人信息控制者履行法律法规规定的义务相关的；

b)与国家安全、国防安全直接相关的；

c)与公共安全、公共卫生、重大公共利益直接相关的；

d)与刑事侦查、起诉、审判和判决执行等直接相关的；

e)出于维护个人信息主体或其他个人的生命、财产等重大合法权益但又很难得到本人授权同意的；

f)所涉及的个人信息是个人信息主体自行向社会公众公开的；

g)根据个人信息主体要求签订和履行合同所必需的；

安证合规集团&北源律师事务所

注：个人信息保护政策的主要功能为公开个人信息控制者收集、使用个人信息范围和规则，不宜将其视为合同。

h)从合法公开披露的信息中收集个人信息的，如合法的新闻报道、政府信息公开等渠道；

i)维护所提供产品或服务的安全稳定运行所必需的，如发现、处置产品或服务的故障；

j)个人信息控制者为新闻单位，且其开展合法的新闻报道所必需的；

k)个人信息控制者为学术研究机构，出于公共利益开展统计或学术研究所必要，且其对外提供学术研究或描述的结果时，对结果中所包含的个人信息进行去标识化处理的。

6 个人信息的存储

6.1 个人信息存储时间最小化

对个人信息控制者的要求包括：

a)个人信息存储期限应为实现个人信息主体授权使用的目的所必需的最短时间，法律法规另有规定或者个人信息主体另行授权同意的除外；

b)超出上述个人信息存储期限后，应对个人信息进行删除或匿名化处理。

6.2 去标识化处理

收集个人信息后，个人信息控制者宜立即进行去标识化处理，并采取技术和管理方面的措施，将可用于恢复识别个人的信息与去标识化后的信息分开存储并加强访问和使用的权限管理。

6.3 个人敏感信息的传输和存储

对个人信息控制者的要求包括：

a) 传输和存储个人敏感信息时，应采用加密等安全措施；

注：采用密码技术时宜遵循密码管理相关国家标准。

b)个人生物识别信息应与个人身份信息分开存储；

c)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：

1)仅存储个人生物识别信息的摘要信息；

2)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；

3)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。

注1：摘要信息通常具有不可逆特点，无法回溯到原始信息。

注2：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。

6.4 个人信息控制者停止运营

当个人信息控制者停止运营其产品或服务时，应：

安证合规集团&北源律师事务所

a)及时停止继续收集个人信息；

b)将停止运营的通知以逐一送达或公告的形式通知个人信息主体；

c)对其所持有的个人信息进行删除或匿名化处理。

7 个人信息的使用

7.1 个人信息访问控制措施

对个人信息控制者的要求包括：

a)对被授权访问个人信息的人员，应建立最小授权的访问控制策略，使其只能访问职责所需的最小必要的个人信息，且仅具备完成职责所需的最少的数据操作权限；

b)对个人信息的重要操作设置内部审批流程，如进行批量修改、拷贝、下载等重要操作；

c)对安全管理人员、数据操作人员、审计人员的角色进行分离设置；

d)确因工作需要，需授权特定人员超权限处理个人信息的，应经个人信息保护责任人或个人信息保护工作机构进行审批，并记录在册；

注：个人信息保护责任人或个人信息保护工作机构的确定见 11.1。

e)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。例如，当收到客户投诉，投诉处理人员才可访问该个人信息主体的相关信息。

7.2 个人信息的展示限制

涉及通过界面展示个人信息的（如显示屏幕、纸面），个人信息控制者宜对需展示的个人信息采取去标识化处理等措施，降低个人信息在展示环节的泄露风险。例如，在个人信息展示时，防止内部非授权人员及个人信息主体之外的其他人员未经授权获取个人信息。

7.3 个人信息使用的目的限制

对个人信息控制者的要求包括：

a)使用个人信息时，不应超出与收集个人信息时所声称的目的具有直接或合理关联的范围。因业务需要，确需超出上述范围使用个人信息的，应再次征得个人信息主体明示同意；

注：将所收集的个人信息用于学术研究或得出对自然、科学、社会、经济等现象总体状态的描述，属于与收集目的具有合理关联的范围之内。但对外提供学术研究或描述的结果时，需对结果中所包含的个人信息进行去标识化处理。

b)如所收集的个人信息进行加工处理而产生的信息，能够单独或与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的，应将其认定为个人信息。对其处理应遵循收集个人信息时获得的授权同意范围。

安证合规集团&北源律师事务所

注：加工处理而产生的个人信息属于个人敏感信息的，对其处理需符合对个人敏感信息的要求。

7.4 用户画像的使用限制

对个人信息控制者的要求包括：

a)用户画像中对个人信息主体的特征描述，不应：

1)包含淫秽、色情、赌博、迷信、恐怖、暴力的内容；

2)表达对民族、种族、宗教、残疾、疾病歧视的内容。

b)在业务运营或对外业务合作中使用用户画像的，不应：

1)侵害公民、法人和其他组织的合法权益；

2)危害国家安全、荣誉和利益，煽动颠覆国家政权、推翻社会主义制度，煽动分裂国家、破坏国家统一，宣扬恐怖主义、极端主义，宣扬民族仇恨、民族歧视，传播暴力、淫秽色情信息，编造、传播虚假信息扰乱经济秩序和社会秩序。

c)除为实现个人信息主体授权同意的使用目的所必需外，使用个人信息时应消除明确身份指向性，避免精确定位到特定个人。例如，为准确评价个人信用状况，可使用直接用户画像，而用于推送商业广告目的时，则宜使用间接用户画像。

7.5 个性化展示的使用

对个人信息控制者的要求包括：

a)在向个人信息主体提供业务功能的过程中使用个性化展示的，应显著区分个性化展示的内容和非个性化展示的内容；

注：显著区分的方式包括但不限于：标明“定推”等字样，或通过不同的栏目、版块、页面分别展示等。

b)在向个人信息主体提供电子商务服务的过程中，根据消费者的兴趣爱好、消费习惯等特征向其提供商品或者服务搜索结果的个性化展示的，应当同时向该消费者提供不针对其个人特征的选项；

注：基于个人信息主体所选择的特定地理位置进行展示、搜索结果排序，且不因个人信息主体身份不同展示不一样的内容和搜索结果排序，则属于不针对其个人特征的选项。

c)在向个人信息主体推送新闻信息服务的过程中使用个性化展示的，应：

1)为个人信息主体提供简单直观的退出或关闭个性化展示模式的选项；

2)当个人信息主体选择退出或关闭个性化展示模式时，向个人信息主体提供删除或匿名化定向推送活动所基于的个人信息的选项。

安证合规集团&北京律师事务所

d)在向个人信息主体提供业务功能的过程中使用个性化展示的，宜建立个人信息主体对个性化展示所依赖的个人信息（如标签、画像维度等）的自主控制机制，保障个人信息主体调控个性化展示相关性程度的能力。

7.6 基于不同业务目的所收集个人信息的汇聚融合

对个人信息控制者的要求包括：

a)应遵守7.3的要求；

b)应根据汇聚融合后个人信息所用于的目的，开展个人信息安全影响评估，采取有效的个人信息保护措施。

7.7 信息系统自动决策机制的使用

个人信息控制者业务运营所使用的信息系统，具备自动决策机制且能对个人信息主体权益造成显著影响的（例如，自动决定个人征信及贷款额度，或用于面试人员的自动化筛选等），应：

a) 在规划设计阶段或首次使用前开展个人信息安全影响评估，并依评估结果采取有效的保护个人信息主体的措施；

b) 在使用过程中定期（至少每年一次）开展个人信息安全影响评估，并依评估结果改进保护个人信息主体的措施；

c) 向个人信息主体提供针对自动决策结果的投诉渠道，并支持对自动决策结果的人工复核。

8 个人信息主体的权利

8.1 个人信息查询

个人信息控制者应向个人信息主体提供查询下列信息的方法：

a)其所持有的关于该主体的个人信息或个人信息的类型；

b)上述个人信息的来源、所用于的目的；

c)已经获得上述个人信息的第三方身份或类型。

注：个人信息主体提出查询非其主动提供的个人信息时，个人信息控制者可在综合考虑不响应请求可能对个人信息主体合法权益带来的风险和损害，以及技术可行性、实现请求的成本等因素后，作出是否响应的决定，并给出解释说明。

8.2 个人信息更正

个人信息主体发现个人信息控制者所持有的该主体的个人信息有错误或不完整的，个人信息控制者应为其提供请求更正或补充信息的方法。

8.3 个人信息删除

对个人信息控制者的要求包括：

安证合规集团&北源律师事务所

a)符合以下情形，个人信息主体要求删除的，应及时删除个人信息：

1)个人信息控制者违反法律法规规定，收集、使用个人信息的；

2)个人信息控制者违反与个人信息主体的约定，收集、使用个人信息的。

b)个人信息控制者违反法律法规规定或违反与个人信息主体的约定向第三方共享、转让个人信息，且个人信息主体要求删除的，个人信息控制者应立即停止共享、转让的行为，并通知第三方及时删除；

c)个人信息控制者违反法律法规规定或违反与个人信息主体的约定，公开披露个人信息，且个人信息主体要求删除的，个人信息控制者应立即停止公开披露的行为，并发布通知要求相关接收方删除相应的信息。

8.4 个人信息主体撤回授权同意

对个人信息控制者的要求包括：

a)应向个人信息主体提供撤回收集、使用其个人信息的授权同意的方法。撤回授权同意后，个人信息控制者后续不应再处理相应的个人信息；

b)应保障个人信息主体拒绝接收基于其个人信息推送商业广告的权利。对外共享、转让、公开披露个人信息，应向个人信息主体提供撤回授权同意的方法。

注：撤回授权同意不影响撤回前基于授权同意的个人信息处理。

8.5 个人信息主体注销账户

对个人信息控制者的要求包括：

a)通过注册账户提供产品或服务的个人信息控制者，应向个人信息主体提供注销账户的方法，且方法简便易操作；

b)受理注销账户请求后，需要人工处理的，应在承诺时限内（不超过15个工作日）完成核查和处理；

c)注销过程如需进行身份核验，要求个人信息主体再次提供的个人信息类型不应多于注册、使用等服务环节收集的个人信息类型；

d)注销过程不应设置不合理的条件或提出额外要求增加个人信息主体义务，如注销单个账户视同注销多个产品或服务，要求个人信息主体填写精确的历史操作记录作为注销的必要条件等；

注1：多个产品或服务之间存在必要业务关联关系的，例如，一旦注销某个产品或服务的账户，将会导致其他产品或服务的必要业务功能无法实现或者服务质量明显下降的，需向个人信息主体进行详细说明。

注2：产品或服务没有独立的账户体系的，可采取对该产品或服务账号以外其他个人信息进

安证合规集团&北源律师事务所

行删除，并切断账户体系与产品或服务的关联等措施实现注销。

e)注销账户的过程需收集个人敏感信息核验身份时，应明确对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化处理等；

f)个人信息主体注销账户后，应及时删除其个人信息或匿名化处理。因法律规规定需要留存个人信息的，不能再次将其用于日常业务活动中。

8.6 个人信息主体获取个人信息副本

根据个人信息主体的请求，个人信息控制者宜为个人信息主体提供获取以下类型个人信息副本的方法，或在技术可行的前提下直接将以下类型个人信息的副本传输给个人信息主体指定的第三方：

a)本人的基本资料、身份信息；

b)本人的健康生理信息、教育工作信息。

8.7 响应个人信息主体的请求

对个人信息控制者的要求包括：

a)在验证个人信息主体身份后，应及时响应个人信息主体基于8.1~8.6提出的请求，应在三十天内或法律法规规定的期限内作出答复及合理解释，并告知个人信息主体外部纠纷解决途径；

b)采用交互式页面（如网站、移动互联网应用程序、客户端软件等）提供产品或服务的，宜直接设置便捷的交互式页面提供功能或选项，便于个人信息主体在线行使其访问、更正、删除、撤回授权同意、注销账户等权利；

c)对合理的请求原则上不收取费用，但对一定时期内多次重复的请求，可视情收取一定成本费用；

d)直接实现个人信息主体的请求需要付出高额成本或存在其他显著困难的，个人信息控制者应向个人信息主体提供替代方法，以保障个人信息主体的合法权益；

e)以下情行可不响应个人信息主体基于8.1~8.6提出的请求，包括：

1)与个人信息控制者履行法律法规规定的义务相关的；

2)与国家安全、国防安全直接相关的；

3)与公共安全、公共卫生、重大公共利益直接相关的；

4)与刑事侦查、起诉、审判和执行判决等直接相关的；

5)个人信息控制者有充分证据表明个人信息主体存在主观恶意或滥用权利的；

6)出于维护个人信息主体或其他个人的生命、财产等重大合法权益但又很难得到本人授权同意的；

安证合规集团&北源律师事务所

7)响应个人信息主体的请求将导致个人信息主体或其他个人、组织的合法权益受到严重损害的；

8)涉及商业秘密的。

f)如决定不响应个人信息主体的请求，应向个人信息主体告知该决定的理由，并向个人信息主体提供投诉的途径。

8.8 投诉管理

个人信息控制者应建立投诉管理机制和投诉跟踪流程，并在合理的时间内对投诉进行响应。

9 个人信息的委托处理、共享、转让、公开披露

9.1 委托处理

个人信息控制者委托第三方处理个人信息时，应符合以下要求：

a)个人信息控制者作出委托行为，不应超出已征得个人信息主体授权同意的范围或应遵守5.6所列情形；

b)个人信息控制者应对委托行为进行个人信息安全影响评估，确保受委托者达到11.5的数据安全能力要求；

c) 受委托者应：

1)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；

2)受委托者确需再次委托时，应事先征得个人信息控制者的授权；

3)协助个人信息控制者响应个人信息主体基于8.1~8.6提出的请求；

4)受委托者在处理个人信息过程中无法提供足够的安全保护水平或发生了安全事件的，应及时向个人信息控制者反馈；

5)在委托关系解除时不再存储相关个人信息。

d)个人信息控制者应对受委托者进行监督，方式包括但不限于：

1)通过合同等方式规定受委托者的责任和义务；

2)对受委托者进行审计。

e)个人信息控制者应准确记录和存储委托处理个人信息的情况；

f)个人信息控制者得知或者发现受委托者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，应立即要求受托者停止相关行为，且采取或要求受委托者采取有效补救措施（如更改口令、回收权限、断开网络连接等）控制或消除个人信息面临的安全风险。必要时个人信息控制者应终止与受委托者的业务关系，并要求受委托者及时删除从个人信息控制者获得

安证合规集团&北源律师事务所

的个人信息。

9.2 个人信息共享、转让

个人信息控制者共享、转让个人信息时，应充分重视风险。共享、转让个人信息，非因收购、兼并、重组、破产原因的，应符合以下要求：

a)事先开展个人信息安全影响评估，并依评估结果采取有效的保护个人信息主体的措施；

b)向个人信息主体告知共享、转让个人信息的目的、数据接收方的类型以及可能产生的后果，并事先征得个人信息主体的授权同意。共享、转让经去标识化处理的个人信息，且确保数据接收方无法重新识别或者关联个人信息主体的除外；

c)共享、转让个人敏感信息前，除 b）中告知的内容外，还应向个人信息主体告知涉及的个人敏感信息类型、数据接收方的身份和数据安全能力，并事先征得个人信息主体的明示同意；

d)通过合同等方式规定数据接收方的责任和义务；

e)准确记录和存储个人信息的共享、转让情况，包括共享、转让的日期、规模、目的，以及数据接收方基本情况等；

f)个人信息控制者发现数据接收方违反法律法规要求或双方约定处理个人信息的，应立即要求数据接收方停止相关行为，且采取或要求数据接收方采取有效补救措施（如更改口令、回收权限、断开网络连接等）控制或消除个人信息面临的安全风险；必要时个人信息控制者应解除与数据接收方的业务关系，并要求数据接收方及时删除从个人信息控制者获得的个人信息；

g)因共享、转让个人信息发生安全事件而对个人信息主体合法权益造成损害的，个人信息控制者应承担相应的责任；

h)帮助个人信息主体了解数据接收方对个人信息的存储、使用等情况，以及个人信息主体的权利，例如，访问、更正、删除、注销账户等；

i)个人生物识别信息原则上不应共享、转让。因业务需要，确需共享、转让的，应单独向个人信息主体告知目的、涉及的个人生物识别信息类型、数据接收方的具体身份和数据安全能力等，并征得个人信息主体的明示同意。

9.3 收购、兼并、重组、破产时的个人信息转让

当个人信息控制者发生收购、兼并、重组、破产等变更时，对个人信息控制者的要求包括：

a)向个人信息主体告知有关情况；

b)变更后的个人信息控制者应继续履行原个人信息控制者的责任和义务，如变更个人信息使用目的时，应重新取得个人信息主体的明示同意；

c)如破产且无承接方的，对数据做删除处理。

安证合规集团&北源律师事务所

9.4 个人信息公开披露

个人信息原则上不应公开披露。个人信息控制者经法律授权或具备合理事由确需公开披露时，应符合以下要求：

a)事先开展个人信息安全影响评估，并依评估结果采取有效的保护个人信息主体的措施；

b)向个人信息主体告知公开披露个人信息的目的、类型，并事先征得个人信息主体明示同意；

c)公开披露个人敏感信息前，除 b）中告知的内容外，还应向个人信息主体告知涉及的个人敏感信息的内容；

d)准确记录和存储个人信息的公开披露的情况，包括公开披露的日期、规模、目的、公开范围等；

e)承担因公开披露个人信息对个人信息主体合法权益造成损害的相应责任；

f)不应公开披露个人生物识别信息；

g)不应公开披露我国公民的种族、民族、政治观点、宗教信仰等个人敏感数据的分析结果。

9.5 共享、转让、公开披露个人信息时事先征得授权同意的例外

以下情形中，个人信息控制者共享、转让、公开披露个人信息不必事先征得个人信息主体的授权同意：

a)与个人信息控制者履行法律法规规定的义务相关的；

b)与国家安全、国防安全直接相关的；

c)与公共安全、公共卫生、重大公共利益直接相关的；

d)与刑事侦查、起诉、审判和判决执行等直接相关的；

e)出于维护个人信息主体或其他个人的生命、财产等重大合法权益但又很难得到本人授权同意的；

f)个人信息主体自行向社会公众公开的个人信息；

g)从合法公开披露的信息中收集个人信息的，如合法的新闻报道、政府信息公开等渠道。

9.6 共同个人信息控制者

对个人信息控制者的要求包括：

a) 当个人信息控制者与第三方为共同个人信息控制者时，个人信息控制者应通过合同等形式与第三方共同确定应满足的个人信息安全要求，以及在个人信息安全方面自身和第三方应分别承担的责任和义务，并向个人信息主体明确告知；

b) 如未向个人信息主体明确告知第三方身份，以及在个人信息安全方面自身和第三方应分别承担的责任和义务，个人信息控制者应承担因第三方引起的个人信息安全责任。

安证合规集团&北清律师事务所

注：如个人信息控制者在提供产品或服务的过程中部署了收集个人信息的第三方插件（例如，网站经营者与在其网页或应用程序中部署统计分析工具、软件开发工具包SDK、调用地图API接口），且该第三方并未单独向个人信息主体征得收集个人信息的授权同意，则个人信息控制者与该第三方在个人信息收集阶段为共同个人信息控制者。

9.7 第三方接入管理

当个人信息控制者在其产品或服务中接入具备收集个人信息功能的第三方产品或服务且不适用9.1和9.6时，对个人信息控制者的要求包括：

a)建立第三方产品或服务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；

b)应与第三方产品或服务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；

c)应向个人信息主体明确标识产品或服务由第三方提供；

d)应妥善留存平台第三方接入有关合同和管理记录，确保可供相关方查阅；

e)应要求第三方根据本标准相关要求向个人信息主体征得收集个人信息的授权同意，必要时核验其实现的方式；

f)应要求第三方产品或服务建立响应个人信息主体请求和投诉等的机制，以供个人信息主体查询、使用；

g)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；

h)产品或服务嵌入或接入第三方自动化工具（如代码、脚本、接口、算法模型、软件开发工具包、小程序等）的，宜采取以下措施：

1)开展技术检测确保其个人信息收集、使用行为符合约定要求；

2)对第三方嵌入或接入的自动化工具收集个人信息的行为进行审计，发现超出约定的行为，及时切断接入。

9.8 个人信息跨境传输

在中华人民共和国境内运营中收集和产生的个人信息向境外提供的，个人信息控制者应遵循国家相关规定和相关标准的要求。

10 个人信息安全事件处置

10.1 个人信息安全事件应急处置和报告

对个人信息控制者的要求包括：

安证合规集团&北京律师事务所

a)应制定个人信息安全事件应急预案；

b)应定期（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；

c)发生个人信息安全事件后，个人信息控制者应根据应急响应预案进行以下处置：

1)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；

2)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；

3)按照《国家网络安全事件应急预案》等有关规定及时上报，报告内容包括但不限于：涉及个人信息主体的类型、数量、内容、性质等总体情况，事件可能造成的影响，已采取或将要采取的处置措施，事件处置相关人员的联系方式；

4)个人信息泄露事件可能会给个人信息主体的合法权益造成严重危害的，如个人敏感信息的泄露，按照10.2的要求实施安全事件的告知。

d)根据相关法律法规变化情况，以及事件处置情况，及时更新应急预案。

10.2 安全事件告知

对个人信息控制者的要求包括：

a)应及时将事件相关情况以邮件、信函、电话、推送通知等方式告知受影响的个人信息主体。难以逐一告知个人信息主体时，应采取合理、有效的方式发布与公众有关的警示信息；

b)告知内容应包括但不限于：

1)安全事件的内容和影响；

2)已采取或将要采取的处置措施；

3)个人信息主体自主防范和降低风险的建议；

4)针对个人信息主体提供的补救措施；

5)个人信息保护负责人和个人信息保护工作机构的联系方式。

11 组织的个人信息安全管理要求

11.1 明确责任部门与人员

对个人信息控制者的要求包括：

a)应明确其法定代表人或主要负责人对个人信息安全负全面领导责任，包括为个人信息安全工作提供人力、财力、物力保障等；

b)应任命个人信息保护负责人和个人信息保护工作机构，个人信息保护负责人应由具有相关管理工作经历和个人信息保护专业知识的人员担任，参与有关个人信息处理活动的重要决策直接

安证合规集团&北源律师事务所

向组织主要负责人报告工作；

c)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：

1)主要业务涉及个人信息处理，且从业人员规模大于200人；

2)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；

3)处理超过10万人的个人敏感信息的。

d)个人信息保护负责人和个人信息保护工作机构的职责应包括但不限于：

1)全面统筹实施组织内部的个人信息安全工作，对个人信息安全负直接责任；

2)组织制定个人信息保护工作计划并督促落实；

3)制定、签发、实施、定期更新个人信息保护政策和相关规程；

4)建立、维护和更新组织所持有的个人信息清单（包括个人信息的类型、数量、来源、接收方等）和授权访问策略；

5)开展个人信息安全影响评估，提出个人信息保护的对策建议，督促整改安全隐患；

6)组织开展个人信息安全培训；

7)在产品或服务上线发布前进行检测，避免未知的个人信息收集、使用、共享等处理行为；

8)公布投诉、举报方式等信息并及时受理投诉举报；

9)进行安全审计；

10)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。

e)应为个人信息保护负责人和个人信息保护工作机构提供必要的资源，保障其独立履行职责。

11.2 个人信息安全工程

开发具有处理个人信息功能的产品或服务时，个人信息控制者宜根据国家有关标准在需求、设计、开发、测试、发布等系统工程阶段考虑个人信息保护要求，保证在系统建设时对个人信息保护措施同步规划、同步建设和同步使用。

11.3 个人信息处理活动记录

个人信息控制者宜建立、维护和更新所收集、使用的个人信息处理活动记录，记录的内容可包括：

a）所涉及个人信息的类型、数量、来源（如从个人信息主体直接收集或通过间接获取方式获得）；

b）根据业务功能和授权情况区分个人信息的处理目的、使用场景，以及委托处理、共享、转让、公开披露、是否涉及出境等情况；

安证合规集团&北源律师事务所

c）与个人信息处理活动各环节相关的信息系统、组织或人员。

11.4 开展个人信息安全影响评估

对个人信息控制者的要求包括：

a)应建立个人信息安全影响评估制度，评估并处置个人信息处理活动存在的安全风险；

b)个人信息安全影响评估应主要评估处理活动遵循个人信息安全基本原则的情况，以及个人信息处理活动对个人信息主体合法权益的影响，内容包括但不限于：

1)个人信息收集环节是否遵循目的明确、选择同意、最小必要等原则；

2)个人信息处理是否可能对个人信息主体合法权益造成不利影响，包括是否

会危害人身和财产安全、损害个人名誉和身心健康、导致差别性待遇等；

3)个人信息安全措施的有效性；

4)匿名化或去标识化处理后的数据集重新识别出个人信息主体或与其他数据集汇聚后重新识别出个人信息主体的风险；

5)共享、转让、公开披露个人信息对个人信息主体合法权益可能产生的不利影响；

6)发生安全事件时，对个人信息主体合法权益可能产生的不利影响。

c)在产品或服务发布前，或业务功能发生重大变化时，应进行个人信息安全影响评估；

d)在法律法规有新的要求时，或在业务模式、信息系统、运行环境发生重大变更时，或发生重大个人信息安全事件时，应进行个人信息安全影响评估；

e)形成个人信息安全影响评估报告，并以此采取保护个人信息主体的措施，使风险降低到可接受的水平；

f)妥善留存个人信息安全影响评估报告，确保可供相关方查阅，并以适宜的形式对外公开。

11.5 数据安全能力

个人信息控制者应根据有关国家标准的要求，建立适当的数据安全能力，落实必要的管理和技术措施，防止个人信息的泄漏、损毁、丢失、篡改。

11.6 人员管理与培训

对个人信息控制者的要求包括：

a)应与从事个人信息处理岗位上的相关人员签署保密协议，对大量接触个人敏感信息的人员进行背景审查，以了解其犯罪记录、诚信状况等；

b)应明确内部涉及个人信息处理不同岗位的安全职责，建立发生安全事件的处罚机制；

c)应要求个人信息处理岗位上的相关人员在调离岗位或终止劳动合同时，继续履行保密义务；

d)应明确可能访问个人信息的外部服务人员应遵守的个人信息安全要求，与其签署保密协议，

安证合规集团&北源律师事务所

并进行监督；

e)应建立相应的内部制度和政策对员工提出个人信息保护的指引和要求；

f)应定期（至少每年一次）或在个人信息保护政策发生重大变化时，对个人信息处理岗位上的相关人员开展个人信息安全专业化培训和考核，确保相关人员熟练掌握个人信息保护政策和相关规程。

11.7 安全审计

对个人信息控制者的要求包括：

a)应对个人信息保护政策、相关规程和安全措施的有效性进行审计；

b)应建立自动化审计系统，监测记录个人信息处理活动；

c)审计过程形成的记录应能对安全事件的处置、应急响应和事后调查提供支撑；

d)应防止非授权访问、篡改或删除审计记录；

e)应及时处理审计过程中发现的个人信息违规使用、滥用等情况；

f)审计记录和留存时间应符合法律法规的要求。

附录A

（资料性附录）

个人信息示例

个人信息是指以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息，如姓名、出生日期、身份证件号码、个人生物识别信息、住址、通信通讯联系方式、通信记录和内容、账号密码、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息等。

判定某项信息是否属于个人信息，应考虑以下两条路径：一是识别，即从信息到个人，由信息本身的特殊性识别出特定自然人，个人信息应有助于识别出特定个人。二是关联，即从个人到信息，如已知特定自然人，由该特定自然人在其活动中产生的信息（如个人位置信息、个人通话记录、个人浏览记录等）即为个人信息。符合上述两种情形之一的信息，均应判定为个人信息。

表A.1给出了个人信息举例。

表A.1 个人信息举例

个人基本资料	个人姓名、生日、性别、民族、国籍、家庭关系、住址、个人电话号码、电子邮件地址等

安证合规集团&北源律师事务所

个人身份信息	身份证、军官证、护照、驾驶证、工作证、出入证、社保卡、居住证等
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
网络身份标识信息	个人信息主体账号、IP 地址、个人数字证书等
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，以及与个人身体健康状况相关的信息，如体重、身高、肺活量等
个人教育工作信息	个人职业、职位、工作单位、学历、学位、教育经历、工作经历、培训记录、成绩单等
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
个人通信信息	通信记录和内容、短信、彩信、电子邮件，以及描述个人通信的数据（通常称为元数据）等
联系人信息	通讯录、好友列表、群列表、电子邮件地址列表等
个人上网记录	指通过日志储存的个人信息主体操作记录，包括网站浏览记录、软件使用记录、点击记录、收藏列表等
个人常用设备信息	指包括硬件序列号、设备 MAC 地址、软件列表、唯一设备识别码（如 IMEI/Android ID/IDFA/OpenUDID/GUID/SIM 卡 IMSI 信息等）等在内的描述个人常用设备基本情况的信息
个人位置信息	包括行踪轨迹、精准定位信息、住宿信息、经纬度等

安证合规集团&北源律师事务所

其他信息	婚史、宗教信仰、性取向、未公开的违法犯罪记录等

附录B

（资料性附录）

个人敏感信息判定

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个人敏感信息。可从以下角度判定是否属于个人敏感信息：

泄露：个人信息一旦泄露，将导致个人信息主体及收集、使用个人信息的组织和机构丧失对个人信息的控制能力，造成个人信息扩散范围和用途的不可控。某些个人信息在泄漏后，被以违背个人信息主体意愿的方式直接使用或与其他信息进行关联分析，可能对个人信息主体权益带来重大风险，应判定为个人敏感信息。例如，个人信息主体的身份证复印件被他人用于手机号卡实名登记、银行账户开户办卡等。

非法提供：某些个人信息仅因在个人信息主体授权同意范围外扩散，即可对个人信息主体权益带来重大风险，应判定为个人敏感信息。例如，性取向、存款信息、传染病史等。

滥用：某些个人信息在被超出授权合理界限时使用（如变更处理目的、扩大处理范围等），可能对个人信息主体权益带来重大风险，应判定为个人敏感信息。例如，在未取得个人信息主体授权时，将健康信息用于保险公司营销和确定个体保费高低。

表B.1给出了个人敏感信息举例。

表B.1 个人敏感信息举例

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

安证合规集团&北源律师事务所

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

附录C

（资料性附录）

实现个人信息主体自主意愿的方法（略）

附 录 D

（资料性附录）

个人信息保护政策模板（略）

用性，具体技术要求如下：

a)应建立相应的个人金融信息传输安全策略和规程，采用满足个人金融信息传输安全策略的安全控制措施，如安全通道、数据加密等技术措施。

b)传输个人金融信息前，通信双方应通过有效技术手段进行身份鉴别和认证。

c)通过公共网络传输时，C2、C3类别信息应使用加密通道或数据加密的方式进行传输，保障个人金融信息传输过程的安全；对于C3类别中的支付敏感信息，其安全传输技术控制措施应符合有关行业技术标准与行业主管部门有关规定要求。

d)应根据个人金融信息的不同类别，采用技术手段保证个人金融信息的安全传输；低敏感程度类别的个人金融信息因参与身份鉴别等关键活动导致敏感程度上升的（如，经组合后构成交易授权完整要素的情况），应提升相应的安全传输保障手段。

e)个人金融信息传输的接收方应对接收的信息进行完整性校验。

f)应建立有效机制对个人金融信息传输安全策略进行审核、监控和优化，包括对通道安全配置、密码算法配置、密钥管理等保护措施的管理和监控。

安证合规集团&北源律师事务所

g)应采取有效措施（如个人金融信息传输链路冗余）保证数据传输可靠性和网络传输服务可用性。

6.1.3存储

个人金融信息存储的具体技术要求如下:

a)不应留存非本机构的银行卡磁道数据（或芯片等效信息）、银行卡有效期、卡片验证码（CVN和CVN2）、银行卡密码、网络支付密码等C3类别信息。若确有必要留存的，应取得个人金融信息主体及账户管理机构的授权。

b)应根据个人金融信息的不同类别，采用技术手段保证个人金融信息的存储安全；低敏感程度类别的个人金融信息因参与身份鉴别等关键活动导致敏感程度上升的（如，经组合后构成交易授权完整要素的情况），应提升相应的安全存储保障手段。

c)C3类别个人金融信息应采用加密措施确保数据存储的保密性。

d)受理终端、个人终端及客户端应用软件均不应存储银行卡磁道数据（或芯片等效信息）、银行卡有效期、卡片验证码（CVN和CVN2）、银行卡密码、网络支付密码等支付敏感信息及个人生物识别信息的样本数据、模板，仅可保存完成当前交易所必需的基本信息要素，并在完成交易后及时予以清除。

e)采取必要的技术和管控措施保证个人金融信息存储转移过程中的安全性。

f)应将去标识化、匿名化后的数据与可用于恢复识别个人的信息采取逻辑隔离的方式进行存储，确保去标识化、匿名化后的信息与个人金融信息不被混用。

g)在停止运营时，应依据国家法律法规与行业主管部门有关规定要求，对所存储的个人金融信息进行妥善处置，或移交国家与行业主管部门指定的机构继续保存。

6.1.4使用

6.1.4.1信息展示

提供业务办理与查询等功能的应用软件，对个人金融信息展示具体技术要求如下:

a)依据国家法律法规与行业主管部门有关规定要求，对通过计算机屏幕、客户端应用软件、银行卡受理设备、自助终端设备、纸面（如受理终端打印出的交易凭条等交易凭证）等界面展示的个人金融信息应采取信息屏蔽（或截词）等处理措施，降低个人金融信息在展示环节的泄露风险。

注1：关于信息屏蔽（或截词）的使用方式，参见附录A。

注2：金融业机构柜面打印的凭证依据有关规范执行。

b)处于未登录状态时，不应展示与个人金融信息主体相关的C3类别信息。

安证合规集团&北源律师事务所

c)处于已登录状态时，个人金融信息展示的技术要求如下：

除银行卡有效期外，C3类别信息不应明文展示。

对于银行卡号、手机号码、证件类识别标识或其他识别标识信息等可以直接或组合后确定个人金融信息主体的信息应进行屏蔽展示，或由用户选择是否屏蔽展示，如需完整展示，应进行用户身份验证，并做好此类信息管理，防范此类信息泄露风险。

涉及其他个人金融信息主体的信息时，除以下情况外，宜进行屏蔽展示：

——其他方主动发起的活动包含的信息，此种情况需展示必要的信息以供活动接收方对活动内容进行确认，例如：其他方发起的交易、其他方发起的收付款、保险保费代收。

——与其他方已建立信任关系（间接授权），此时需活动发起方确认发起活动的必要信息的正确性（或活动发起方需接收活动结果信息，并确认活动已正确完成），例如：向其他方收款，其他方已付款；向其他方申请代付，其他方同意付款或者其他方在自己业务应用范围内的联系人。

——其他法律法规要求的情况。

应用软件的后台管理与业务支撑系统，对个人金融信息展示具体技术要求如下：

a)除银行卡有效期外，C3类别信息不应明文展示。

b)应采取技术措施防范个人金融信息在展示过程中泄露或被未经授权的拷贝。

c)后台系统对支付账号、客户法定名称、支付预留手机号码、证件类或其他类识别标识信息等展示宜进行屏蔽处理，如需完整展示，应做好此类信息管理，采取有效措施防范未经授权的拷贝。

d)后台系统不应具备开放式查询能力，应严格限制批量查询。

e)对于确有明文查看需要的业务场景可以保留明文查看权限，后台系统应对所有查询操作进行细粒度的授权与行为审计。

应防止通过散列碰撞等方法推导出完整的数据，若使用“截词”的方式进行部分字段的屏蔽处理，不应用散列代替字段被截词的部分。

6.1.4.2共享和转让

个人金融信息在共享和转让的过程中，应充分重视信息转移或交换过程中的安全风险，具体技术要求如下：

a)在共享和转让前，应开展个人金融信息安全影响评估，并依据评估结果采取有效措施保护个人金融信息主体权益。

b)在共享和转让前，应开展个人金融信息接收方信息安全保障能力评估，并与其签署数据保护责任承诺。

安证合规集团&北源律师事务所

c)支付账号及其等效信息在共享和转让时，除法律法规和行业主管部门另有规定外，应使用支付标记化（按照JR/T0149—2016）技术进行脱敏处理（因业务需要无法使用支付标记化技术时，应进行加密），防范信息泄露风险。

d)应部署信息防泄露监控工具，监控及报告个人金融信息的违规外发行为。

e)应部署流量监控技术措施，对共享、转让的信息进行监控和审计。

f)应根据“业务需要”和“最小权限”原则，对个人金融信息的导出操作进行细粒度的访问控制与全过程审计，应采取两种或两种以上鉴别技术对导出信息操作人员进行身份鉴别。

g)应定期检查或评估信息导出通道的安全性和可靠性。

h)使用外部嵌入或接入的自动化工具（如代码、脚本、接口、算法模型、软件开发工具包等）进行信息共享与转让时，应定期检查或评估信息共享工具、服务组件和共享通道的安全性和可靠性，并留存检查或评估结果记录。

i)应执行严格的审核程序，并准确记录和保存个人金融信息共享和转让情况。记录内容应包括但不限于日期、规模、目的、范围，以及数据接收方基本情况与使用意图等，并应确保对共享和转让的信息及其过程可被追溯。

j)应采取有效技术防护措施，防范信息转移过程中被除信息发送方与接收方之外的其他个人、组织和机构截获和利用。

6.1.4.3公开披露

个人金融信息原则上不得公开披露。金融业机构经法律授权或具备合理事由确需公开披露时，具体技术要求如下:

a)应事先开展个人金融信息安全影响评估，并依据评估结果采取有效的保护个人金融信息主体权益的措施。

b)不应公开披露个人生物识别信息。

c)应准确记录和保存个人金融信息的公开披露情况，包括公开披露的日期、规模、目的、内容、公开范围等。

6.1.4.4委托处理

金融业机构因金融产品或服务的需要，将收集的个人金融信息委托给第三方机构（包含外包服务机构与外部合作机构）处理时，具体技术要求如下:

a)委托行为不应超出已征得个人金融信息主体授权同意的范围或遵循7.1中对于征得授权同意的例外所规定的情形，并准确记录和保存委托处理个人金融信息的情况。

b)C3以及C2类别信息中的用户鉴别辅助信息，不应委托给第三方机构进行处理。转接清算、

安证合规集团&北源律师事务所

登记结算等情况，应依据国家有关法律法规及行业主管部门有关规定与技术标准执行。

c)对委托处理的信息应采用去标识化（不应仅使用加密技术）等方式进行脱敏处理，降低个人金融信息被泄露、误用、滥用的风险。

d)应对委托行为进行个人金融信息安全影响评估，并确保受委托者具备足够的数据安全能力，且提供了足够的安全保护措施。

e)应对第三方机构等受委托者进行监督，方式包括但不限于：

依据7.2.1的要求，通过合同等方式规定受委托者的责任和义务；

依据7.4.2的要求，对受委托者进行安全检查和评估。

f)应对外部嵌入或接入的自动化工具（如代码、脚本、接口、算法模型、软件开发工具包等）开展技术检测，确保其个人金融信息收集、使用行为符合约定要求；并对其收集个人金融信息的行为进行审计，发现超出约定行为及时切断接入。

6.1.4.5加工处理

个人金融信息在加工处理的过程中，具体技术要求如下：

a)应采取必要的技术手段和管理措施，确保在个人金融信息清洗和转换过程中对信息进行保护，对C2、C3类别信息，应采取更加严格的保护措施。

b)应对匿名化或去标识化处理的数据集或其他数据集汇聚后重新识别出个人金融信息主体的风险进行识别和评价，并对数据集采取相应的保护措施。

c)应建立个人金融信息防泄露控制规范和机制，防止个人金融信息处理过程中的调试信息、日志记录等因不受控制的输出而泄露受保护的信息。

d)应具备信息化技术手段或机制，对个人金融信息滥用行为进行有效的识别、监控和预警。

e)应具备完整的个人金融信息加工处理操作记录和管理能力，记录内容包括但不限于日期、时间、主体、事件描述、事件结果等。

6.1.4.6汇聚融合

个人金融信息汇聚融合的技术要求如下：

a)汇聚融合的数据不应超出收集时所声明的使用范围。因业务需要确需超范围使用的，应再次征得个人金融信息主体明示同意。

b)应根据汇聚融合后的个人金融信息类别及使用目的，开展个人金融信息安全影响评估，并采取有效的技术保护措施。

6.1.4.7开发测试

个人金融信息在开发测试过程中的具体技术要求如下：

安证合规集团&北源律师事务所

a)应对开发测试环境与生产环境进行有效隔离。

b)开发环境、测试环境不应使用真实的个人金融信息，应使用虚构的或经过去标识化（不应仅使用加密技术）脱敏处理的个人金融信息，账号、卡号、协议号、支付指令等测试确需信息除外。

6.1.5删除

个人金融信息在删除过程中的具体技术要求如下：

a)应采取技术手段，在金融产品和服务所涉及的系统中去除个人金融信息，使其保持不可被检索和访问。

b)个人金融信息主体要求删除个人金融信息时，金融业机构应依据国家法律法规、行业主管部门有关规定以及与个人金融信息主体的约定予以响应。

6.1.6销毁

个人金融信息在销毁过程中的具体技术要求如下：

a)应建立个人金融信息销毁策略和管理制度，明确销毁对象、流程、方式和要求。

b)应对个人金融信息存储介质销毁过程进行监督与控制，对待销毁介质的登记、审批、介质交接、销毁执行等过程进行监督。

c)销毁过程应保留有关记录，记录至少应包括销毁内容、销毁方式与时间、销毁人签字、监督人签字等内容。

d)存储个人金融信息的介质如不再使用，应采用不可恢复的方式（如消磁、焚烧、粉碎等）对介质进行销毁处理；存储个人金融信息的介质如还需继续使用，不应只采用删除索引、删除文件系统的方式进行信息销毁，应通过多次覆写等方式安全地擦除个人金融信息，确保介质中的个人金融信息不可再被恢复或者以其他形式加以利用。

e)云环境下有关数据清除应依据JR/T0167—2018的9.6执行。

6.2安全运行技术要求

6.2.1网络安全要求

承载与处理个人金融信息的信息系统应符合国家网络安全相关规定与GB/T22239—2019、JR/T0071的要求。存储个人金融信息的数据库应处于金融业机构可控网络内，并进行有效的访问控制。

6.2.2Web应用安全要求

涉及C2、C3类别信息的Web应用的安全技术要求如下：

a)应具备对网站页面篡改、网站页面源代码暴露、穷举登录尝试、重放攻击、SQL注入、跨

站脚本攻击、钓鱼、木马以及任意文件上传、下载等已知漏洞的防范能力。

b)处理个人金融信息相关的Web应用系统与组件上线前应进行安全评估。

c)应具备对处理个人金融信息的系统组件进行实时监测的能力，有效识别和阻止来自内外部的非法访问。

6.2.3客户端应用软件安全要求

与个人金融信息相关的客户端应用软件及应用软件开发工具包（SDK）应符合JR/T0092—2019、JR/T0068—2020客户端应用软件有关安全技术要求，并在上线前进行安全评估。

6.2.4密码技术与密码产品要求

使用的密码技术及产品应符合国家密码管理部门与行业主管部门要求。

7安全管理要求

7.1安全准则

7.1.1收集

个人金融信息收集的方式包括但不限于通过柜面、信息系统、金融自助设备、受理终端、客户端应用软件等渠道获取。金融业机构应遵循合法、正当、必要的原则，向个人金融信息主体明示收集与使用个人金融信息的目的、方式、范围和规则等，获得个人金融信息主体的授权同意，并满足以下要求:

a)收集个人金融信息的基本规则如下:

不应欺诈、诱骗，或以默认授权、功能捆绑等方式误导强迫个人金融信息主体提供个人金融信息;

不应隐瞒金融产品或服务所具有的收集个人金融信息的功能;

不应通过非法渠道间接获取个人金融信息;

不应收集法律法规与行业主管部门有关规定明令禁止收集的个人金融信息。

b)收集个人金融信息应遵循最小化要求，收集个人金融信息的目的应与实现和优化金融产品或服务、防范金融产品或服务的风险有直接关联。直接关联是指无该个人金融信息参与无法实现前述目的。

c)收集个人金融信息时授权同意的具体要求如下:

收集个人金融信息前，应向个人金融信息主体明确告知金融产品或服务需收集的个人金融信息类别，以及收集、使用个人金融信息的规则（如：收集和使用个人金融信息的目的、收集方式、自身的数据安全能力、对外共享、转让、公开披露的规则、投诉与申诉的渠道及响应时限等），并获得个人金融信息主体的明示同意。

安证合规集团&北源律师事务所

间接获取个人金融信息时，应要求个人金融信息提供方说明个人金融信息来源，并对其个人金融信息来源的合法性进行确认；应了解个人金融信息提供方已获得的授权内容，包括使用目的，个人金融信息主体是否授权同意转让、共享、公开披露等情况；因业务需要金融业机构确需超出原授权范围处理个人金融的，应在使用个人金融信息前，征得个人金融信息主体的明示同意。

d)以下情形收集使用个人金融信息无需征得个人金融信息主体的授权同意：

与履行国家法律法规及行业主管部门有关规定的义务相关的；

与国家安全、国防安全直接相关的；

与公共安全、公共卫生、重大公共利益直接相关的；

与犯罪侦查、起诉、审判和判决执行等直接相关的；

出于维护个人金融信息主体或其他主体的生命、财产等重大合法权益但又很难得到本人同意的；

个人金融信息主体自行向社会公众公开的；

根据个人金融信息主体要求签订和履行合同所必需的；

从合法公开披露的信息中收集个人金融信息的，如合法的新闻报道、政府信息公开等渠道；

用于维护所提供的金融产品或服务的安全稳定运行所必需的，例如识别、处置金融产品或服务中的欺诈或被盗用等。

7.1.2存储

个人金融信息的存储时限应满足国家法律法规与行业主管部门有关规定要求，并符合个人金融信息主体授权使用的目的所必需的最短时间要求。超过该期限后，应对收集的个人金融信息进行删除或匿名化处理。

7.1.3使用

个人金融信息在信息展示、共享与转让、公开披露、委托处理、加工处理、汇聚融合等方面，应遵循6.1.4.1—6.1.4.6的要求，并满足以下要求：

a)除法律法规与行业主管部门另有规定或开展金融业务所必需的数据共享与转让（如转接清算等）外，金融业机构原则上不应共享、转让其收集的个人金融信息，确需共享、转让的，应充分重视信息安全风险，具体要求如下：

应向个人金融信息主体告知共享、转让个人金融信息的目的、数据接收方的类型，并事先征得个人金融信息主体明示同意，共享、转让经去标识化处理（不应仅使用加密技术）的个人金融信息，且确保数据接收方无法重新识别个人金融信息主体的除外。

应帮助个人金融信息主体了解数据接收方对个人金融信息的存储、使用等情况，包括个人金

安证合规集团&北海律师事务所

融信息主体的权利，例如访问、更正、删除、注销账户等；在法律法规规定、行业主管部门有关规定及个人金融信息主体约定的范围内，个人金融信息主体行使其个人金融信息控制权利，金融业机构应配合响应其请求。

C3类别信息以及C2类别信息中的用户鉴别辅助信息不应共享、转让。

转接清算、登记结算等情况，应依据国家有关法律法规与行业主管部门有关规定与技术标准执行。

当因收购、兼并、重组、破产等情况，对个人金融信息主体提供金融产品或服务的金融业机构主体变更而发生个人金融信息共享、转让时，具体要求如下：

——金融业机构将其提供的金融产品或服务移交至其他金融业机构的情况，应使用逐一传达（或公告）的方式通知个人金融信息主体。

——承接其金融产品或服务的金融业机构，应对其承接运营的金融产品或服务继续履行个人金融信息保护责任；如变更其在收购、兼并重组过程中获取的个人金融信息使用目的，应重新获得个人金融信息主体明示同意（或授权）。

b)金融业机构原则上不应公开披露其收集的个人金融信息，经法律授权或具备合理理由确需公开披露个人金融信息的，具体要求如下：

应向个人金融信息主体告知公开披露个人金融信息的目的、类别，并事先征得个人金融信息主体的同意，并向其告知涉及的信息内容；

承担因公开披露个人金融信息对个人金融信息主体合法权益造成损害的相应责任；

C3类别信息，以及C2类别信息中的用户鉴别辅助信息不应公开披露。

c)因金融产品或服务的需要，将收集的个人金融信息委托给第三方机构（包含外包服务机构与外部合作机构）处理的，具体要求如下：

依据6.1.4.4开展委托处理工作。

应对第三方机构等受委托者提出如下要求：

——应严格按照金融业机构的要求处理个人金融信息，如因特殊原因受委托者未能按照要求处理个人金融信息，应及时告知金融业机构，并配合金融业机构进行信息安全评估，并采取补救措施以保护个人金融信息的安全，必要时应终止其对个人金融信息的处理；

——未经书面授权，受委托者不应将其处理的个人金融信息再次委托给其他机构进行处理；

——应协助响应个人金融信息主体的请求；

——如受委托者在处理个人金融信息过程中无法提供足够的信息安全保护水平或发生安全事件，应及时告知金融业机构，配合进行信息安全评估与安全事件调查，并采取补救措施以保护个

安证合规集团&北源律师事务所

人金融信息的安全，必要时应终止其对个人金融信息的处理；

——在委托关系解除时（或外包服务终止后），受委托者应按照金融业机构的要求销毁其处理的个人金融信息，并依据双方协商的期限承担后续的个人金融信息保密责任；

——应准确记录和保存委托处理个人金融信息的情况。

d)在中华人民共和国境内提供金融产品或服务过程中收集和产生的个人金融信息，应在境内存储、处理和分析。因业务需要，确需向境外机构（含总公司、母公司或分公司、子公司及其他为完成该业务所必需的关联机构）提供个人金融信息的，具体要求如下：

应符合国家法律法规及行业主管部门有关规定；

应获得个人金融信息主体明示同意；

应依据国家、行业有关部门制定的办法与标准开展个人金融信息出境安全评估，确保境外机构数据安全保护能力达到国家、行业有关部门与金融业机构的安全要求；

应与境外机构通过签订协议、现场核查等方式，明确并监督境外机构有效履行个人金融信息保密、数据删除、案件协查等职责义务。

e)以下情形中，金融业机构共享、转让、公开披露个人金融信息无需征得个人金融信息主体的授权同意：

与履行法律法规及行业主管部门规定的义务相关的；

与国家安全、国防安全直接相关的；

与公共安全、公共卫生、重大公共利益直接相关的；

与犯罪侦查、起诉、审判和判决执行等直接相关的；

出于维护个人金融信息主体或其他主体的生命、财产等重大合法权益但又很难得到本人同意的；

个人金融信息主体自行向社会公众公开的；

从合法公开披露的信息中收集个人金融信息的，如合法的新闻报道、政府信息公开等渠道。

7.2安全策略

7.2.1安全制度体系建立与发布

金融业机构应建立个人金融信息保护制度体系，明确工作职责，规范工作流程。制度体系的管理范畴应涵盖本机构、外包服务机构与外部合作机构，并确保相关制度发布并传达给本机构员工及外部合作方。相关制度应至少包括个人金融信息保护管理规定、日常管理及操作流程、外包服务机构与外部合作机构管理、内外部检查及监督机制、应急处理流程和预案。具体要求如下：

a)制定个人金融信息保护管理规定，提出本机构个人金融信息保护工作方针、目标和原则。

安证合规集团&北源律师事务所

b)开展个人金融信息分类分级管理。应针对不同类别和敏感程度的个人金融信息，实施相应的安全策略和保障措施。

c)建立日常管理及操作流程。应对个人金融信息的收集、传输、存储、使用、删除、销毁等环节提出具体保护要求，制定个人金融信息时效性管理规程，确保符合法律法规和行业主管部门有关规定。

d)建立信息系统分级授权管理机制。应在不影响履行反洗钱等法定义务的前提下，制定本机构人员个人金融信息调取权限与使用范围，并制定专门的授权审批流程。

e)建立个人金融信息脱敏（如屏蔽、去标识、匿名化等）管理规范和制度，应明确不同敏感级别个人金融信息脱敏规则、脱敏方法和脱敏数据的使用限制。

f)依据国家与行业有关标准，建立个人金融信息安全影响评估制度，应定期（至少每年一次）开展个人金融信息安全影响评估。

g)建立外包服务机构与外部合作机构管理制度，包括但不限于：

应对个人金融信息生命周期过程中相关的外包服务机构与外部合作机构进行审查与评估，评估其个人金融信息的保护能力是否达到国家、行业主管部门与金融业机构的要求；应通过协议或合同的方式，约束外包服务机构与外部合作机构不应留存C2、C3类别信息；对于C2类别信息中的支付账号等信息，若因清分清算、差错处理等业务需要确需留存，金融业机构应明确其保密义务与保密责任，并应根据安全要求落实安全控制措施，并将有关资料留档备查；对可能访问个人金融信息的外包服务机构、外部合作机构及其人员，金融业机构应要求外包服务机构与外部合作机构向有关人员传达个人金融信息保护安全要求，与其签署保密协议，并对协议履行情况进行监督。

不应将存储个人金融信息的数据库交由外部合作机构运维。

应定期对外包服务机构与外部合作机构的个人金融信息保护措施落实情况进行确认，确认的方式包括但不限于外部信息安全评估、现场检查等。

国家法律法规与行业主管部门另有规定的，按照相关要求执行。

h)建立个人金融信息安全检查及监督机制。应建立个人金融信息安全日常检查机制和工作流程、定期评估个人金融信息管理方面存在的不足，及时调整检查机制和工作流程。

i)应将个人金融信息泄露等相关事件处理纳入机构信息安全事件应急处置工作机制，制定专门的流程和预案。定期评估应急处理流程和预案，及时保障、有效应对个人金融信息安全事件，降低安全事件造成的损失及不利影响。

j)建立个人金融信息投诉与申诉处理程序，明确投诉与申诉受理部门、处理程序，对个人金

安证合规集团&北海律师事务所

融信息主体要求更正或删除金融业机构收集其个人金融信息的情况，应受理、核实，并依据国家与行业主管部门要求予以处理。

k)明确个人金融信息共享、存储、使用和销毁的期限，具备个人金融信息存储时效性的控制能力。

7.2.2组织架构岗位设置

组织架构及岗位设置具体要求如下：

a)应建立个人金融信息保护组织架构，明确机构各层级内设部门与相关岗位个人金融信息保护职责与总体要求。

b)应明确个人金融信息保护责任人和个人金融信息保护责任机构，并履行以下工作职责：

负责制定和管理本机构个人金融信息安全管理制度；

制定、实施、定期更新隐私政策和相关规程；

监督本机构内部，以及本机构与外部合作方个人金融信息安全管理；

开展信息安全管理内部审计、分析处理信息安全相关事件；

组织开展个人金融信息安全影响评估，提出个人金融信息保护的对策建议；

组织在金融产品或服务上线发布前进行技术检测，避免未知（与金融产品或服务功能及隐私政策不符）的个人金融信息收集、使用、共享等处理行为；

公布投诉与申诉方式等信息并及时受理个人金融信息有关的投诉、申诉。

c)应明确在提供金融产品和服务的过程中知悉个人金融信息的岗位，并针对相关岗位明确其个人金融信息安全管理责任与保密责任，如不得未经授权的复制、存储、使用个人金融信息，不得向他人出售或者以其他形式未经授权的共享、转让、披露个人金融信息等。

7.2.3人员管理

对涉及个人金融信息相关人员的安全管理，具体要求如下：

a)录用员工前，应进行必要的背景调查，并与所有可访问个人金融信息的员工签署保密协议，或在劳动合同中设置保密条款。

b)应定期开展内外部个人金融信息保护培训与意识教育活动，并保留相关记录。

c)在发生人员调离岗位时，应立即调整和完成相关人员的个人金融信息访问、使用等权限的配置，并明确有关人员后续的个人金融信息保护管理权限和保密责任；若有关人员调整后的岗位不涉及个人金融信息的访问与处理的，应明确其继续履行有关信息的保密义务要求。

d)与员工终止劳动合同时，应立即终止并收回其对个人金融信息的访问权限，并明确其继续履行有关信息的保密义务要求。

安证合规集团&北京律师事务所

e)系统开发人员、系统测试人员与运维人员之间不应相互兼岗。

f)应定期（至少每年一次）或在隐私政策发生重大变化时，对个人金融信息处理岗位上的相关人员开展个人金融信息安全专业化培训和考核，确保相关人员熟练掌握隐私政策和相关规程。

7.3访问控制

加强个人金融信息访问控制管理，具体要求如下:

a)应根据“业务需要”和“最小权限”原则，进行个人金融信息相关的权限管理，严格控制和分配访问、使用个人金融信息的权限。

b)对于可访问和处理个人金融信息的系统应设置基于角色的访问控制策略，禁止账户共用。

c)传输、处理、存储个人金融信息的系统默认用户权限应为“拒绝所有访问”。

d)对个人金融信息使用的权限管理应设置权限指派、回收、过期处理等安全功能。

e)对存储或处理个人金融信息的系统或设备进行远程访问时，应通过专线、VPN等方式访问，个人金融信息不应在远程访问设备上留存。

f)应对生产网络、开发测试网络、办公网络以及相关非生产网络进行访问控制。

g)应对个人金融信息访问与个人金融信息的增删改查等操作进行记录，并保证操作日志的完整性、可用性及可追溯性，操作日志包括但不限于业务操作日志、系统日志等；系统运维管理类日志不应记录个人金融信息。

h)应对存储个人金融信息的数据库及操作日志实施严格的用户授权与访问控制。

i)存储或处理个人金融信息的相关物理设备或介质应在获得审批授权后方可移入或移出机房受控区域，留存有C2、C3类别信息的物理设备或介质移入或移出区域应具有同等的安全保障措施。

7.4安全监测与风险评估

7.4.1监控与审计

监控与审计具体要求如下:

a)应识别并记录包括但不限于管理员用户、业务用户对个人金融信息的访问。

b)应对个人金融信息数据交换网络流量进行安全监控和分析，并存储匹配安全规则的数据，以备事件溯源。

c)日志文件和匹配规则的数据应至少保存6个月，应定期对所有系统组件日志进行审计，包括但不限于存储、处理或传输个人金融信息的系统组件日志、执行安全功能的系统组件日志（如防火墙、入侵检测系统、验证服务器等）、安全事件日志等。

d)应采取技术手段对个人金融信息全生命周期进行安全风险识别和管控，如恶意代码检测、异常流量监测、用户行为分析等。

安证合规集团&北源律师事务所

7.4.2安全检查和评估

金融业机构应对个人金融信息生命周期全过程进行安全检查和评估，范围包括金融业机构以及与其合作的第三方机构（包含外包服务机构与外部合作机构）。

个人金融信息的安全检查和评估具体要求如下:

a)应依据制定的个人金融信息安全影响评估制度，在个人金融信息委托处理、共享与转让、公开披露等过程中，执行个人金融信息安全影响评估活动，并将评估报告归档保存。个人金融信息安全影响评估可由金融业机构自行组织开展，也可委托外部安全评估机构执行。

b)应每年至少开展一次对涉及收集、存储、传输、使用个人金融信息的信息系统进行安全检查或安全评估，包括但不限于以下方式及其组合:

对信息系统进行信息安全评估、漏洞扫描和渗透测试，并及时采取补救措施;

在信息系统组件或运行环境发生重大变更（或发现新的高安全等级威胁和漏洞）时，重新进行信息安全风险评估;

将个人金融信息保护纳入金融业机构内部安全审计工作，定期开展安全审计，形成审计报告，并根据审计结果完善制度、流程。

c)对于个人金融信息中的支付信息部分，应采取自行评估或委托外部机构进行检查评估，金融业机构以及与其合作的第三方机构应每年至少开展一次支付信息安全合规评估，对评估过程中发现的问题及时采取补救措施并形成报告存档备查。

d)出现个人金融信息泄露事件，造成一定经济损失（或社会影响）时，应及时委托外部安全评估机构重新进行相关安全评估与检查活动，并将结果报送行业主管部门。

7.5安全事件处置

安全事件处置具体要求如下:

a)应制定个人金融信息安全事件应急预案，明确安全事件处置流程和岗位职责。

b)应定期组织内部相关人员进行个人金融信息保护应急预案相关培训和应急演练。

c)发生个人金融信息遗失、损毁、泄露或被篡改等安全事件后，应及时采取必要措施进行处置，控制事态发展，消除安全隐患，并及时告知受影响的个人金融信息主体，告知的内容应符合GB/T35273—2017关于安全事件告知内容的规定，告知的方式包括但不限于:

以邮件、信函、电话、推送消息等方式及时告知受影响的个人金融信息主体;

难以逐一告知个人金融信息主体时，应采取合理、有效的方式发布与公众有关的警示信息。

d)发现因系统漏洞或人为原因造成个人金融信息泄露时，应立即采取有效措施防止风险扩大，并向行业主管部门报告。

安证合规集团&北源律师事务所

e)应记录事件内容，分析和鉴定事件产生的原因，评估事件可能造成的影响，制定补救措施，并按国家与行业主管部门规定及时进行报告。

f)应建立投诉与申诉管理机制，包括跟踪流程，并在规定的时间内，对投诉、申诉进行响应。

g)根据相关法律法规与行业主管部门有关规定的变化情况以及事件处置情况，及时评估并更新应急预案。

信息安全技术 个人信息去标识化指南

基本信息：	
【发布机关】国家市场监督管理总局、国家标准化管理委员会	【时效性】 现行有效
	【效力级别】国家标准
【标准编号】GB/T 37964-2019	【实施日期】2020.03.01
【发布日期】2019.08.30	

信息安全技术　个人信息去标识化指南

1　范围

本标准描述了个人信息去标识化的目标和原则，提出了去标识化过程和管理措施。

本标准针对微数据提供具体的个人信息去标识化指导，适用于组织开展个人信息去标识化工作，也适用于网络安全相关主管部门、第三方评估机构等组织开展个人信息安全监督管理、评估等工作。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 25069—2010 信息技术　安全技术　术语

3　术语和定义

GB/T 25069—2010中界定的以及下列术语和定义适用于本文件。

3.1

个人信息　personal information

以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息。

[GB/T 35273-2017，定义3.1]

安证合规集团&北源律师事务所

3.2

个人信息主体　personal data subject

个人信息所标识的自然人。

[GB/T 35273-2017，定义3.3]

3.3

去标识化　de-identification

通过对个人信息的技术处理，使其在不借助额外信息的情况下，无法识别个人信息主体的过程。

[GB/T 35273-2017，定义3.14]

注：去除标识符与个人信息主体之间关联性。

3.4

微数据　microdata

一个结构化数据集，其中每条（行）记录对应一个个人信息主体，记录中的每个字段（列）对应一个属性。

3.5

聚合数据　aggregate data

表征一组个人信息主体的数据，比如各种统计值的集合。

注：例如各种统计值的集合。

3.6

标识符　identifier

微数据中的一个或多个属性，可以实现对个人信息主体的唯一识别。

注：标识符分为直接标识符和准标识符。

3.7

直接标识符　direct identifier

微数据中的属性，在特定环境下可以单独识别个人信息主体。例如：姓名、地址、电子邮件地址、电话号码、传真号码、信用卡号码、车牌号码、车辆识别号码、社会保险号码、健康卡号码、病历号码、设备标识符、生物识别码、互联网协议（IP）地址号和网络通用资源定位符（URL）等。

注1：特定环境指个人信息使用的具体场景。比如，在一个具体的学校，通过学号可以直接识别出一个具体的学生。

安证合规集团&北源律师事务所

注2：常见的直接标识符有：姓名、身份证号、护照号、驾照号、地址、电子邮件地址、电话号码、传真号码、银行卡号 、车牌号码、车辆识别号码、社会保险号码、健康卡号码、病历号码、设备标识符、生物识别码、互联网议(IP)地址号和网络通用资源定位符(URL) 等。

3.8

准标识符　quasi-identification

微数据中的属性，结合其它属性可唯一识别个人信息主体。

注：常见的准标识符有：性别、出生日期或年龄、事件日期（例如入院、手术、出院、访问）、地点（例如邮政编码、建筑名称、地区）、族裔血统、出生国、语言、原住民身份、可见的少数民族地位、职业、婚姻状况、受教育水平、上学年限、犯罪历史、总收入和宗教信仰等。

3.9

重标识　re-identification

把去标识化的数据集重新关联到原始个人信息主体或一组个人信息主体的过程。

3.10

敏感属性　sensitive attribute

数据集中需要特别保护的属性，在潜在的重标识攻击期间需要防止其值与任何一个个人信息主体相关联。

注：在潜在的重标识攻击期间需要防止其值与任何一个个人信息主体相关联。

3.11

有用性　usefulness

数据对于应用有着具体含义、具有使用意义的特性。

注：去标识化数据应用广泛，每种应用将要求去标识化数据具有某些特性以达到应用目的，因此在去标识化后，需要保证对这些特性的保留。

3.12

完全公开共享　completely public sharing

数据一旦发布，很难召回，一般通过互联网直接公开发布。

注：同英文术语 The Release and Forget Model

3.13

受控公开共享　controlled public sharing

通过数据使用协议对数据的使用进行约束。

注1：例如通过协议禁止信息接方发起对数据集中个体的重标识攻击，禁止信息接收方关联

安证合规集团&北源律师事务所

到外部数据集或信息，禁止信息接收方未经许可共享数据集。

注2：同英文术语 The Data Use Agreement Model。

3.14

领地公开共享　enclave public sharing

在物理或者虚拟的领地范围内共享，数据不能流出到领地范围外。

注2：同英文术语 The Enclave Model。

3.15

去标识化技术　de-identification technique

在物理或者虚拟的领地范围内共享，数据不能流出到领地范围外。

注2：同英文术语 The Enclave Model。

3.16

去标识化模型　de-identification model

在物理或者虚拟的领地范围内共享，数据不能流出到领地范围外。

注2：同英文术语 The Enclave Model。

4　去标识化概述

4.1　去标识化目标

去标识化目标包括：

a)对直接标识符和准标识符进行删除或变换，避免攻击者根据这些属性直接识别或者结合其它信息识别出原始个人信息主体；

b)控制重标识的风险，根据可获得的数据情况和应用场景选择合适的模型和技术，将重标识的风险控制在可接受范围内，确保重标识风险不会随着新数据发布而增加，确保数据接收方之间的潜在串通不会增加重标识风险；

c)在控制重标识风险的前提下，结合业务目标和数据特性，选择合适的去标识化模型和技术，确保去标识化后的数据集尽量满足其预期目的（有用）。

4.2　去标识化原则

对数据集进行去标识化，应遵循以下原则：

a)合规：应满足我国法律法规和标准规范对个人信息安全保护的有关规定，并持续跟进有关法律法规和标准规范。

b)个人信息安全保护优先：应根据业务目标和安全保护要求，对个人信息进行恰当的去标识化处理，在保护个人信息安全的前提下确保去标识化后的数据具有应用价值。

安证合规集团&北源律师事务所

c)技术和管理相结合：根据工作目标制定适当的策略，选择适当的模型和技术，综合利用技术和管理两方面措施实现最佳效果。包括设定具体的岗位，明确相应职责；对去标识化过程中形成的辅助信息（比如密钥，映射表等）采取有效的安全防护措施等。

d)充分应用软件工具：针对大规模数据集的去标识化工作，应考虑使用软件工具提高去标识化效率、保证有效性。

e)持续改进：在完成去标识化工作后须进行评估和定期重评估，对照工作目标，评估工作效果（包括重标识风险和有用性）与效率，持续改进方法、技术和工具。并就相关工作进行文档记录。

4.3　重标识风险

4.3.1　重标识方法

常见的用于重标识的方法如下：

a)隔离：基于是否能唯一确定一个个人信息主体，将属于一个个人信息主体的记录隔离出来；

b)关联：将不同数据集中关于相同个人信息主体的信息关联；

c)推断：通过其它属性的值以一定概率推断出一个属性的值。

4.3.2　重标识攻击

重标识攻击包括：

a)重标识一条记录属于一个特定个人信息主体；

b)重标识一条特定记录的个人信息主体；

c)尽可能多的将记录和其对应的个人信息主体关联；

d)判定一个特定的个人信息主体在数据集中是否存在；

e)推断和一组其它属性关联的敏感属性。

4.4　去标识化影响

对数据集进行去标识化，会改变原始数据集，可能影响数据有用性。业务应用使用去标识化后的数据集时应充分认识到这一点，并考虑数据集变化可能带来的影响。

4.5　不同公开共享类型对去标识化的影响

在开展去标识化工作之前需要根据应用需求确定数据的公开共享类型，不同公开共享类型可能引发的重标识风险和对去标识化的要求如表1所示。

表1 不同公开共享类型对去标识化的影响

公开共享类型	可能的重标识风险	对去标识化的要求
完全公开共享	高	高

安证合规集团&北京律师事务所

受控公开共享	中	中
领地公开共享	低	低

5 去标识化过程

5.1 概述

去标识化过程通常可分为确定目标、识别标识、处理标识以及验证批准等步骤，并在上述各步骤的实施过程中和完成后进行有效的监控和审查。如图1所示。

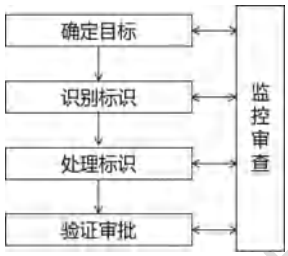

图1 去标识化过程

5.2 确定目标

5.2.1 概述

确定目标步骤包括确定去标识化对象、建立安全目标和制定工作计划等内容。

5.2.2 确定去标识化对象

确定去标识化对象，指确定需要去标识化的数据集范围。在目标数据集中存在标识符时，宜根据以下要素确定哪些数据属于去标识化对象：

a)法规标准。了解国家、地区或行业的相关政策、法律、法规和标准，待采集或发布数据是否涉及去标识化相关要求。

b)组织策略。了解数据是否属于组织列入的重要数据或敏感数据范畴，数据应用时是否存在去标识化的要求。

c)数据来源。了解这些数据采集时是否做过去标识化相关承诺。

d)业务背景。了解数据来源相关信息系统的业务特性，了解业务内容和业务流程，披露数据是否涉及重标识风险。

e)数据用途。了解待发布数据的用途，是否存在重标识风险。

f)关联情况。了解数据披露历史和去标识化历史情况，待披露数据是否和历史数据存在关联关系。

5.2.3 建立安全目标

建立安全目标，具体包括确定重标识风险不可接受程度以及数据有用性最低要求。需要考虑

安证合规集团&北源律师事务所

的因素包括：

a)数据用途。了解数据去标识化后的用途，涉及到业务系统的功能和特性。

b)数据来源。了解数据获取时的相关承诺，以及涉及哪些个人信息。

c)公开共享类别。若为数据发布实施个人信息去标识化，需了解数据是完全公开共享、受控公开共享还是领地公开共享，以及对数据在浏览和使用方面的安全保护措施。

d)去标识化模型和技术。了解数据适用的保护或去标识化标准，以及可能采用的去标识化模型和技术。

e)风险级别。了解数据属性和业务特性，拟采用的重标识风险评估模型及设定的风险级别。

5.2.4　制定工作计划

制定个人信息去标识化的实施计划，包括去标识化的目的、安全目标、数据对象、公开共享方式、实施团队、实施方案、利益相关方、应急措施以及进度安排等，形成去标识化实施计划书。

确定相关内容后，去标识化实施计划书应得到组织最高管理层的批准和支持。

5.3　识别标识

5.3.1　概述

识别标识符的方法包括查表识别法、规则判定法和人工分析法。

5.3.2　查表识别法

查表识别法指预先建立元数据表格，存储需去标识化的直接标识符和准标识符名称，在识别标识数据时，将待识别数据的各个属性名称或字段名称，逐个与元数据表中记录进行对比，以此识别出标识数据。

建立的标识符元数据表，应包括标识符名称、含义、格式要求、常用数据类型、常用字段名字等内容。

查表识别法适用于数据集格式和属性已经明确的去标识化场景，如采用关系型数据库，在表结构中已经明确姓名、身份证号等标识符字段。

5.3.3　规则判定法

规则判定法是指通过建立自动化程序，分析数据集规律，从中自动发现需去标识化的直接标识符和准标识符。

组织可分析业务特点，总结可能涉及到直接标识符和准标识符的数据格式和规律，确立相关标识符识别规则，然后通过运行程序，自动化地从数据集中识别出标识符。如可依据GB 11643—1999《公民身份号码》建立身份证号码识别规则，并通过自动化程序在数据集中自动发现存在的身份证号码数据。

安证合规集团&北源律师事务所

组织识别标识数据宜先采用查表识别法，并根据数据量大小和复杂情况，结合采用规则判定法。规则判定法在某些情况下有助于发现查表识别法不能识别出的标识符，如标识符处于下面情况时：

a)业务系统存储数据时未采用常用的字段名称，如使用“备注”字段存储身份证号；

b)数据中存在混乱或错误情况，如该“备注”字段前100条记录的值为空，而后10000条记录的值为用户身份证号码。

规则判定法不仅仅适用于结构化数据应用场景，也适用于某些半结构化和非结构化数据应用场景，如对于非结构化存储的司法判决书，可以通过建立身份证号识别规则和开发程序，从司法判决书中自动识别出所有的身份证号。

5.3.4　人工分析法

人工分析法是通过人工发现和确定数据集中的直接标识符和准标识符。

组织可在对业务处理、数据集结构、相互依赖关系和对数据集之外可用数据等要素分析的基础上，综合判断数据集重标识风险后，直接指定数据集中需要去标识化的直接标识符和准标识符。

人工分析法在结构化、半结构化和非结构化数据应用场景下都可使用。但考虑到工作量和复杂程度等因素，人工分析法更适用于数据结构简单的数据集。同时，在下列场景时，人工分析法具有明显的优势：

a)数据集中的多个不同数据子集之间存在关联、引用关系时，如通过数据挖掘算法，可联合分析数据集中多个非常见标识符属性后识别出唯一的用户身份；

b)数据集中有特别含义的数据，或者数据具有特殊值、容易引起注意的值，从而可能被用来重标识时，如超出常人的身高、独特的地理坐标、罕见的病因等。

相比较于查表识别法和规则判定法，人工分析法能够更加准确地识别出标识符。

5.4　处理标识

5.4.1　概述

处理标识步骤分为预处理、选择模型技术、实施去标识化三个阶段工作。

5.4.2　预处理

预处理是在对数据集正式实施去标识化前的准备过程。一般地，预处理是对数据集施加某种变化，使其有利于后期进行处理。

预处理阶段工作可参考如下方法进行：

a)形成规范化，或满足特定格式要求的数据；

b)对数据抽样，减小数据集的规模；

安证合规集团&北京律师事务所

c)增加或扰乱数据，改变数据集的真实性。

组织应根据数据集的实际情况选择预处理措施，或选择不预处理。

5.4.3 选择模型技术

不同类型的数据需要采用不同的去标识化技术，所以在去标识化的早期阶段，重要的一步是确定数据的类型和业务特性，选择合适的去标识化模型和技术。选择的参考因素包括如下方面：

a)是否需要对重标识风险进行量化；

b)聚合数据是否够用；

c)数据是否可删除；

d)是否需要保持唯一性；

e)是否需要满足可逆性；

f)是否需要保持原有数据值顺序；

g)是否需要保持原有数据格式，如数据类型、长度等保持不变；

h)是否需要保持统计特征，如平均值、总和值、最大值、最小值等；

i)是否需要保持关系型数据库中的实体完整性、参照完整性或用户自定义完整性；

j)是否可以更改数据类型，比如在针对字符串类型的“性别”（男/女）进行去标识化时，是否可以变成数字类型表示（1/0）；

k)是否需要满足至少若干个属性值相同，以加强数据的不可区分性；

l)是否可以对属性值实施随机噪声添加，对属性值做小变化；

m)去标识化的成本约束。

附录A和附录B分别给出了常见的去标识化技术和模型，针对这些技术和模型的特点以及选择方法可参考附录C，附录D给出了去标识化面临的风险。

5.4.4 实施去标识化

根据选择的去标识化模型和技术，对数据集实施操作。主要工作包括：

a)若存在多个需要去标识化的标识符，则根据数据特点和业务特性设定去标识化的顺序；

b)依次选择相应的工具或程序；

c)设置工具或程序的属性和参数，如设置数据源、用户名/口令、算法参数等；

d)依次执行去标识化工具或程序，获得结果数据集。

5.5 验证审批

5.5.1 验证结果含义

对数据集去标识化后进行验证，以确保生成的数据集在重标识风险和数据有用性方面都符合

安证合规集团&北源律师事务所

预设的目标。在验证满足目标过程中，需对去标识化后重标识风险进行评估，计算出实际风险，与预期可接受风险阈值进行比较，若风险超出阈值，需继续进行调整直到满足要求。由于重标识技术和重标识攻击的能力在迅速演变，需要由内部专业人员或权威的外部组织定期展开验证评估。

5.5.2　验证个人信息安全

验证去标识化数据满足个人信息安全保护要求的方法包括：

a)检查生成的数据文件，以确保文件数据或元数据中不包含直接标识符和准标识符；

b)检查生成的数据文件，以确保所得数据符合既定目标要求；

c)评估去标识化软件所使用的默认假设；

d)进行有动机的入侵者测试，看看是否有具备合格能力的外部人员可以使用公开的数据集执行重标识；

e)让团队利用内部数据进行有针对性的入侵者测试，模拟违规者或敌对内幕人士可能发生的情况。

这些方法不能保证去标识化后的数据满足个人信息安全保护的要求，但它们可以作为整个组织风险评估的一部分。可证明的个人信息安全保护应依赖于形式化方法，比如用于规划组织数据发布的差分隐私方法。通过使用经过验证的去标识化软件，可以大大简化验证去标识化数据的个人信息安全保护。

5.5.3　验证数据有用性

去标识化降低了数据质量和生成数据集的有用性。因此，需要考虑去标识化后的数据集对于预期的应用仍然有用。

存在一些方法用于验证数据有用性。例如，内部人员可对原始数据集和去标识化的数据集执行统计计算，并对结果进行比较，以查看去标识化后是否导致不可接受的更改。组织可让可信的外部人员检查去标识化数据集，以确定数据能被用于预期目的。

5.5.4　评审批准去标识化工作

在完成处理标识和验证结果后，组织管理层应依据数据发布共享用途、重标识风险、数据有用性最低要求等因素，以及验证结果、去标识化各步骤实施过程中的监控审查记录等因素，做出是否认可数据去标识化结果的决定。

审批由组织高级管理层来执行。

5.6　监控审查

5.6.1　监控审查去标识化各步骤实施过程

应确保去标识化的每一步骤均实现了预定目标。

安证合规集团&北海律师事务所

在去标识化的各个步骤中，为有效完成去标识化任务，需在确定目标步骤撰写去标识化工作方案，明确各步骤要完成的工作，并在识别标识、处理标识、验证结果阶段记录工作过程和结果，形成文档。

组织管理层在去标识化的各个步骤完成时，对该阶段记录文档进行审查，检查输出文档是否齐全和内容完备，及时发现已经出现或可能出现的错误或偏差，并采取适当控制措施，监督各步骤执行过程得到完整和有效地执行。

监控审查过程也应记录到文档中，记录内容至少包括监控审查对象、时间、过程、结果和措施等内容。

5.6.2　持续监控去标识化效果

持续监控是指数据在去标识化、批准同意交付用户后，宜根据情况变化或定期进行去标识化数据的重标识风险评估，并与预期可接受风险阈值进行比较，以保障个人信息安全性。

情况发生变化是指重标识风险的相关要素发生变化，相关要素包括但不限于：

a)去标识化数据使用者；

b)目标信息系统；

c)目标信息安全环境；

d)新增去标识化数据。

此外，即使各种要素均未发生变化，只要去标识化数据仍然可以被目标用户访问，也需定期对数据进行重标识风险评估。这是由于重标识技术以及重标识攻击能力都在迅速演变，所以要通过重标识风险评估，检查先前的去标识化数据是否仍然安全。

6　角色职责与人员管理

6.1　角色职责

个人信息去标识化工作相关的主要角色包括规划管理者、执行者、监督者。

a)规划管理者

在组织中，规划管理者对个人信息去标识化工作负总责，具体职责包括：规划个人信息去标识化策略，建立相关的规范制度和监控审计机制，宣贯去标识化政策和制度，认可和批准去标识化工作的结果，和上级主管部门、监管机构进行沟通，与外部技术单位进行合作和交流。

b)执行者

执行者负责去标识化业务的具体执行，主要职责包括：依据数据共享场景，提出个人信息去标识化需求；识别个人信息安全风险，制定去标识化工作计划；执行去标识化工作，记录工作情况；申请审批去标识化结果。

安证合规集团&北源律师事务所

c)监督者

监督者的主要职责是监督去标识化丁作情况、审计该业务执行过程，保证业务合规、安全风险 可控。

6.2 人员管理

组织应整体规划个人信息去标识化有关的工作任务和职责，做到有效保护个人信息安全、确保个人信息去标识化工作顺利开展。在人员管理方面还应考虑如下因素：

a)提炼对个人信息去标识化工作岗位需求，包括技术能力需求和安全保密需求；

b)个人信息去标识化工作岗位招聘时应按照相关法律、法规、道德规范和相应的工作岗位需求，对应聘人员进行考察；

c)与个人信息去标识化工作岗位人员工作合同或补充文档中，应明确其理解工作职责和要承担的安全保密需求；

d)组织应定期开展业务和安全培训，确保执行去标识化操作的个人接受充分和最新的培训，保证岗位人员达到培训要求，持续拥有适当的技能，能够按要求执行个人信息去标识化的相关工作；

e)个人信息去标识化工作岗位人员离职时，应依据其涉及数据重要程度，在离职保密协议中增加适当的保密要求条款。

附 录 A

（资料性附录）

常用去标识化技术（略）

附 录 B

（资料性附录）

常用去标识化模型（略）

附 录 C

（资料性附录）

去标识化模型和技术的选择（略）

附 录 D

（资料性附录）

去标识化面临的挑战（略）

安证合规集团&北源律师事务所

信息安全技术 个人信息安全影响评估指南

基本信息：	
【发布机关】国家市场监督管理总局、国家标准化管理委员会	【时效性】尚未生效
	【效力级别】国家标准
【标准编号】GB/T 39335-2020	【实施日期】2021.06.01
【发布日期】2020.11.19	

安证合规集团&北源律师事务所

信息安全技术 个人信息安全影响评估指南

1 范围

本标准规定了个人信息安全影响评估的基本原理和实践流程。

本标准适用于各类组织自行开展个人信息安全影响评估工作，同时可为国家主管监管部门、第三方测评机构等开展个人信息安全监管、检查、评估等工作提供参考。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 20984 信息安全技术 信息安全风险评估规范

GB/T 25069-2010 信息安全技术 术语

GB/T 35273-2020 信息安全技术 个人信息安全规范

3 术语

GB/T 25069-2010、GB/T 35273-2020确立的以及下列术语适用于本标准。

3.1

个人信息 personal information

以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然

人活动情况的各种信息。

［GB/T 35273-2020，定义3. 1 ］

3.2

个人敏感信息 personal sensitive information

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。

［GB/T 35273-2020，定义3.2］

3.3

个人信息主体 personal information subject

个人信息所标识或者关联的自然人。

［GB/T 35273-2020，定义3.3］

3.4

个人信息安全影响评估 personal information security impact assessment

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。

4 评估基本原理和框架

4.1 概述

个人信息安全影响评估旨在发现、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。

4.2 开展评估的价值

实施个人信息安全影响评估，能够有效加强对个人信息主体权益的保护，有利于组织对外展示其保护个人信息安全的努力，提升透明度，增进个人信息主体对其的信任。包括：

a） 在开展个人信息处理前，组织可通过影响评估，识别可能导致个人信息主体权益遭受损害的风险，并据此采用适当的个人信息安全控制措施。

b） 对于正在开展的个人信息处理，组织可通过影响评估，综合考虑内外部因素的变化情况，持续修正已采取的个人信息安全控制措施，确保对个人合法权益不利影响的风险处于总体可控的状态。

c） 个人信息安全影响评估及其形成的记录文档，可帮助组织在政府、相关机构或商业伙伴的调查、执法、合规性审计等中，证明其遵守了个人信息保护与数据安全等方面的法律、法规和标准的要求。

d） 在发生个人信息安全事件时，个人信息安全影响评估及其形成的记录文档，可用于证明组织已经主动评估风险并采取一定的安全保护措施，有助于减轻、甚至免除组织相关责任和名

安证合规集团&北源律师事务所

誉损失。

e） 组织可通过个人信息安全影响评估，加强对员工的个人信息安全教育。参与评估之中，员工能熟悉各种个人信息安全风险，增强处置风险的能力。

f） 对合作伙伴，组织通过评估的实际行动表明其严肃对待个人信息安全保护，并引导其能够采取适当的安全控制措施，以达到同等或类似的安全保护水平。

4.3 评估报告的用途

个人信息安全影响评估报告的内容主要包括：评估所覆盖的业务场景、业务场景所涉及的具体的个人信息处理活动、负责及参与的部门和人员、已识别的风险、已采用及拟采用的安全控制措施清单、剩余风险等。

因此，个人信息安全影响评估报告的用途包括但不限于：

a） 对于个人信息主体，评估报告可确保个人信息主体了解其个人信息被如何处理、如何保护，并使个人信息主体能够判断是否有剩余风险尚未得到处置。

b） 对于开展影响评估的组织，评估报告的用途可能包括：

1） 在产品、服务或项目的规划阶段，用于确保在产品或服务的设计中充分考虑并实现个人信息的保护要求（例如，安全机制的可实现性、可行性、可追踪性等）；

2） 在产品、服务或项目的运营过程中，用于判断运营的内外部因素（例如运营团队的变动、互联网安全环境、信息共享的第三方安全控制能力等）、法律法规是否发生实质变更，是否需要对影响评估结果进行审核和修正；

3） 用于建立责任制度，监督发现存在安全风险的个人信息处理活动是否已采取安全保护措施，改善或消除已识别的风险；

4） 用于提升内部员工的个人信息安全意识。

c） 对于主管监管部门，要求组织提供个人信息安全影响评估报告，可督促组织开展评估并采取有效的安全控制措施。在处理个人信息安全相关投诉、调查个人信息安全事件等时，主管监管部门可通过影响评估报告了解相关情况，或将报告作为相关证据。

d） 对千开展影响评估的组织的合作伙伴，用千整体了解其在业务场景中的角色和作用，以及其应具体承担的个人信息保护工作和责任。

4.4 评估责任主体

组织指定个人信息安全影响评估的责任部门或责任人员，由其负责个人信息安全影响评估工作流程的制定、实施、改进，并对个人信息安全影响评估工作结果的质量负责。该责任部门或人员具有独立性，不受到被评估方的影响。通常，组织内部牵头执行个人信息安全影响评估工作的

安证合规集团&北源律师事务所

部门为法务部门、合规部门或信息安全部门。

组织内的责任部门可根据部门的具体能力配备情况，选择自行开展个人信息安全影响评估工作，或聘请外部独立第三方来承担具体的个人信息安全影响评估工作。

对千具体的产品、服务或项目，由相应的产品、服务或项目负责人确保个人信息安全影响评估活动的开展和顺利进行，并给予相应支持。

当由组织自行进行个人信息安全影响评估时，主管监管部门和客户可要求独立审计来核证影响评估活动的合理性和完备性。同时，该组织允许主管监管部门对影响评估流程以及相关信息系统或程序进行取证。

4.5 评估基本原理

个人信息安全影响评估的基本原理如图 1 。

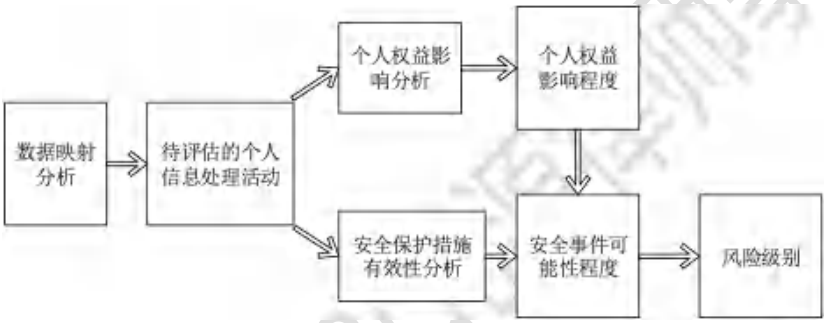

图1 评估原理示意图

4.6 评估实施需考虑的要素

4.6.1 评估规模

个人信息安全影响评估的规模往往取决于受到影响的个人信息主体范围、数量和受影响的程度。

通常，组织在实施该类个人信息安全影响评估时，个人信息的类型、敏感程度、数量，涉及个人信息主体的范围和数量，以及能访问个人信息的人员范围等，都会成为影响评估规模的重要因素。

4.6.2 评估方法

评估实施过程中采用的基本评估方法，包括但不限于以下三种：

a） 访谈：指评估人员对相关人员进行谈话，以对信息系统中个人信息的处理、保护措施设计和实施情况进行了解、分析和取证的过程。访谈的对象包括产品经理、研发工程师、个人信息保护负责人、法务负责人员、系统架构师、安全管理员、运维人员、人力资源人员和系统用户等。

b） 检查：指评估人员通过对管理制度、安全策略和机制、合同协议、安全配置和设计文

安证合规集团&律师事务所

档、运行记录等进行观察、查验、分析，以便理解、分析或取得证据的过程。检查的对象为规范、机制和活动，如个人信息保护策略规划和程序、系统的设计文档和接口规范、应急规划演练结果、事件响应活动、技术手册和用户／管理员指南、信息系统的硬件／软件中信息技术机制的运行等。

c） 测试：指评估人员通过人工或自动化安全测试工具进行技术测试，获得相关信息，并进行分析以便获取证据的过程。测试的对象为安全控制机制，如访问控制、身份识别和验证、安全审计机制、传输链路和保存加密机制、对重要事件进行持续监控、测试事件响应能力以及应急规划演练能力等。

4.6.3 评估工作形式

从实施主体来区分，个人信息安全影响评估分为自评估和检查评估两种形式。

自评估是指组织自行发起对其个人信息处理行为的评估，自评估可以由本组织指定专门负责评估、审计的岗位或角色开展，也可以委托外部专业组织开展评估工作。

检查评估是指组织的上级组织发起的个人信息安全影响评估工作。上级组织是对组织有直接领导关系或负有监督管理责任的组织。检查评估也可以委托外部专业组织开展评估。

在确定评估规模，选定评估方法、评估工作形式后，评估实施的具体流程可参照第 5 漳内容。

5 评估实施流程

5.1 评估必要性分析

5.1.1 概述

个人信息安全影响评估可用于合规差距分析，也可以用于合规之上、进一步提升自身安全风险管理能力和安全水平的目的。因此启动个人信息安全影响评估的必要性，取决于组织的个人信息安全目标，组织可根据实际的需求选取需要启动评估的业务场景。

5.1.2 合规差距评估

5.1.2.1 概述

当组织定义的个人信息安全目标为符合相关法律、法规或标准的基线要求时，则个人信息安全影响评估主要目的在于识别待评估的具体个人信息处理活动已采取的安全控制措施，与相关法律、法规或标准的具体要求之间的差距，例如在某业务场景中与第三方共享个人信息，是否取得了个人信息主体的明示同意。

5.1.2.2 整体合规分析

组织可根据所适用的个人信息保护相关法律、法规、政策及标准，分析特定产品或服务所涉及的全部个人信息处理活动与所适用规则的差距。区评估方式的应用场景包括但不限于以下情形：

a） 产品或服务的年度整体评估；

安注合规集团&北清律师事务所

b） 新产品或新服务（不限技术平台）设计阶段评估；

c） 新产品或新服务（不限技术平台）上线初次评估；

d） 法律法规、政策、标准等出现重大变化时重新评估；

e） 业务模式、互联网安全环境、外部环境等发生重大变化的重新评估；

f） 发生重大个人信息安全事件后重新评估；

g） 发生收购、兼并、重组等情形开展评估。

5.1.2.3 局部合规分析

组织可根据所适用的个人信息保护相关法律、法规、政策及标准，对特定产品或服务所涉及的部分个人信息处理活动与所适用规则的差距进行分析。该评估方式的应用场景包括但不限于以下情形：

a） 新增功能需要收集新的个人信息类型时的评估；

b） 法律、法规、政策、标准出现部分变化时的评估；

c） 业务模式、信息系统、运行环境等发生变化时评估。

5.1.2.4 评估性合规要求分析

部分个人信息保护相关的法律、法规、标准的规定提出了评估性合规要求。这类规定并没有针对特定的个人信息处理活动提出明确、具体的安全控制措施，而是要求组织针对特定个人信息处理活动，专门开展风险评估，并采取与风险程度相适应的安全控制措施，将对个人信息主体合法权益不利影响的风险降低到可接受的程度，才符合其规定。

评估性合规要求往往针对的是对个人权益有重大影响的个人信息处理活动，例如处理个人敏感信息、使用自动化决策方式处理个人信息、委托处理个人信息、向第三方转让或共享个人信息、公开披露个人信息、向境外转移个人信息等。

针对此类规定，组织可使用本指南提供的个人信息安全影响评估方法进行评估，保证个人信息处理活动的安全风险可控，以符合相应的法律、法规、标准的要求。

注：评估性合规要求分析示例及具体评估要点可参考附录 A。

5.1.3 尽责性风险评估

出于审慎经营、声誉维护、品牌建立等目的，组织往往选取可能对个人合法权益产生高风险的个人信息处理活动，开展尽责性风险评估。此种风险评估的目标，是在符合相关法律、法规和标准的基线要求之上，尽可能降低对个人信息主体合法权益的不利影响。

注：高风险个人信息处理活动示例可参考附录 B。

组织可使用本标准提供的个人信息安全影响评估方法，对高风险个人信息处理活动进行评估，

安证合规集团&北源律师事务所

进一步降低个人信息处理活动的安全风险。

5.2 评估准备工作

5.2.1 组建评估团队

组织确认并任命负责进行个人信息安全影响评估的人员（评估人）。此外，组织还要指定人员负责签署评估报告。

评估人明确规定个人信息安全影响评估报告的提交对象、个人信息安全影响评估的时间段、是否会公布评估报告或其摘要。

如有必要评估人需申请团队支持，例如由技术部门、相关业务部门及法律部门的代表构成的团队。

组织内部个人信息安全影响评估需要组织管理层给予长期支持。

管理层需为个人信息安全影响评估团队配置必要资源。

5.2.2 制定评估计划

计划需清楚规定完成个人信息安全影响评估报告所进行的工作、评估任务分工、评估计划表。此外，计划还需考虑到待评估场景中止或撤销的情况。具体操作时考虑以下方面：

a） 人员、技能、经验及能力；

b） 执行各项任务所需时间；

c） 进行评估每一步骤所需资源，如自动化的评估工具等。

注：涉及的场景复杂、耗用资源多时，建议对原有方案进行更新迭代，针对常规评估活动或涉及待评估场景复杂度

低等情形时，可沿用原有计划或简化该步骤。

如涉及相关方咨询，计划需说明在何种情况下需要咨询相关方、将咨询哪些人员以及具体的咨询方式（例如通过公众意见调查、研讨会、焦点小组、公众听证会、线上体验等等）。

5.2.3 确定评估对象和范围

从以下三个方面描述评估的对象和范围：

a） 描述系统基本信息，包括但不限于：

1） 处理个人信息的目的和类型；

2） 对支撑当前或未来业务流程的信息系统的描述；

3） 履行信息系统管理职责的部门或相关人员，以及其职责或履行水平；

4） 关于个人信息处理方式、处理范围的说明、有权访问个人信息的角色等；

5） 如预计委托第三方处理，或与第三方共享、转让信息系统的个人信息，说明上述第三

安证合规集团&北源律师事务所

方身份、第三方接入信息系统的情况等。

b） 描述系统设计信息，包括但不限于：

1） 功能（或逻辑）结构概览；

2） 物理结构概览；

3） 包含个人信息的信息系统数据库、表格和字段的清单和结构；

4） 按组件和接口划分的数据流示意图；

5） 个人信息生命周期的数据流示意图，例如个人信息的收集、存储、使用和共享等；

6） 描述通知个人信息主体的时间节点以及取得个人信息主体同意的时间节点和工作流程图；

7） 可对外传输个人信息的接口清单；

8） 个人信息处理过程中的安全措施。

c） 描述处理流程和程序信息，包括但不限于：

1） 信息系统的身份与用户管理概念；

2） 操作概念，包括信息系统或其中部分结构采用现场运行、外部托管，或云外包的方式；

3） 支持概念，包括列示可访问个人信息的第三方范围、其所拥有的个人信息访问权限、其可访问个人信息的位置等；

4） 记录概念，包括已登入信息的保存计划；

5） 备份与恢复计划；

6） 元数据的保护与管理；

7） 数据保存与删除计划及存储介质的处置。

5.2.4 制定相关方咨询计划

相关方包括但不限于：

——员工，例如人力资源、法律、信息安全、财务、业务运营职能、通信与内部审计（尤其是在监管环境下）相关人员；

——个人信息主体和消费者代表；

——分包商和业务合作伙伴；

——系统开发和运维人员；

——对于评估有相应担忧的其他组织人员。

为保证评估流程的透明，实现降低安全风险的目标，评估人需详细确认进入评估程序的内部或外部相关方。相关方与待评估的个人信息处理活动具有直接的利益关系，相关方可以是拥有或

安证合规集团&北源律师事务所

可能获取个人信息访问权限的组织或个人。

评估人需确认相关方的分类，然后具体确认各类相关方中的特定组织或个人。如果相关方为个人，则该个人宜尽可能具有代表性。

个人信息的范围与规模，以及业务重要性、成本收益等因素，对于确定恰当的相关方非常重要。如对大型个人信息处理活动进行评估，则可能存在较多相关方。在这种情况下，社会团体（如消费者权益保护组织）可能被确认为相关方。相反，一些小型评估，可能不需要确认宽泛的相关方清单。

制定咨询计划需明确不同的相关方所受的影响、后果（如果已知）、以及所采取的用于降低不利影响的安全控制措施等相关问题计划中还包含咨询范围及计划表。

咨询计划的目标包括但不限于:

a）确定相关方的数量与范围;

b）相关方参与识别并评估个人权益影响及安全风险的具体方式;

注：相关方的反溃点见所提出的问题可能与主观风险认识有关、而非客观实际风险，但不能忽略这些意见，组织可将这些意见放在更广泛的相关方管理问题中进行处理，为交流活动提供帮助。

c）就评估报告咨询相关方意见以确认报告是否充分反映他们对有关问题的关注。

组织在开展个人信息安全影响评估时，可以督促适当的相关方（主要包括分包商和业务合作伙伴）开展个人信息安全影响评估。适当的相关方有义务开展个人信息安全影响评估，或者配合组织开展个人信息安全影响评估，组织可以引用相关方的个人信息安全影响i平估报告作为咨询结果。

5. 3数据映射分析

组织在针对个人信息处理过程进行全面的调研后，形成清晰的数据清单及数据映射图表。

数据映射分析阶段需结合个人信息处理的具体场景。调研内容包括个人信息收集、存储、使用、转让、共享、删除等环节涉及的个人信息类型、处理目的、具体实现方式等.以及个人信息处理过程涉及的资源（如内部信息系统）和相关方（如个人信息处理者、平台经营者、外部服务供应商、云服务商等第三方）。调研过程中尽可能考虑已下线系统、系统数据合并、企业收购、并购及全球化扩张等情况。

梳理数据映射分析的结果时，根据个人信息的类型、敏感程度、收集场景、处理方式、涉及相关方等要素，对个人信息处理活动进行分类，并描述每类个人信息处理活动的具体情形，便于后续分类进行 影响分析和风险评价。

安证合规集团&北源律师事务所

注：开展数据映射分析，可参考附录C中表C. 1和表C.2.

5. 4风险源识别

风险源识别是为了分析个人信息处理活动面临哪些威胁源，是否缺乏足够的安全措施，导致存在脆弱性而引发安全事件“决定个人信息安全事件发生的要素很多，就威胁源而言，有内部威胁源，也有外部威胁源，有恶意人员导致的数据被窃取等事件，也有非恶意人员无意中导致的数据泄露等事件；就脆弱性而言，有物理环境影响导致的数据毁损，有技术因素导致的数据泄露、篡改、丢失等事件，也有管理不当引起的滥用等事件。

GB/T 20984中所描述的威胁识别和脆弱性识别方法均可用于对个人信息安全事件的分析过程。为进一步简化个人信息安全事件可能性的分析过程，将与个人信息安全事件可能性相关的要素归纳为以下四个方面：

a）网络环境和技术措施。评估时关注的要素包括但不限于：

1）处理个人信息的信息系统所处网络环境为内部网络还是互联网，不同的网络环境其面临的威胁源不同，连接互联网的信息系统面临的风险更高；

2）处理个人信息的信息系统与其他系统的交互方式，比如是否采用网络接口进行数据交互，是否嵌入可收集个人信息的第三方代码、插件等，通常情况下数据交互越多，需采取更加 全面的安全措施防止信息泄露、窃取等风险；

3）个人信息处理过程中是否实施严格的身份鉴别、访问控制等措施：

4）是否在网络边界部署了边界防护设备,配赏了严格的边界防护策略，实施了数据防泄露技术措施；

5）是否监测和记录网络运行状态，是否标记、分析个人信息在内部或与第三方交互时的状态,及时发现异常流量和违规使用情况；

6）是否采取了防范病毒和木马后门攻击、端口扫描、拒绝服务攻击等网络入侵行为的技术措施；

7）是否采用加密传输、加密存储等措施对个人敏感信息进行额外保护；

8）是否对个人信息收集、保存、传输、使用、共享等各阶段的个人信息处理活动进行审计，并对异常操作行为进行报警；

9）是否建立了完备的网络安全事件预警、应急处置、报告机制；

10）是否对信息系统进行定期安全检查、评估、渗透测试，并及时进行补丁更新和安全加固；

11）是否对数据存储介质加强安全管理.是否具备对数据进行备份和恢复的能力。

12）其他必要的网络安全技术保障措施。

安证合规集团&北源律师事务所

注：如果组织参照其他网络安全、数据安全相关国家标准建立成熟的安全防护体系，可基于其已有基础进行分析评估。

b）个人信息处理流程。评估时关注的要素包括但不限于：

1）个人敏感信息的判定是否准确；

2）收集个人信息的目的是否正当、合法；

3）从第三方获得的数据是否得到正式的处理授权；

4）告知方式和告知的内容是否友好可达，是否所有的处理活动都征得了用户同意；

5）是否定义了个人信息最小元素集，是否超范围收集了个人信息；

6）变更个人信息使用目的是否对个人信息主体产生影响；

7）是否提供便捷有效的个体参与的机制，包括查询、更正、删除、撤回同意、注销账号等；

8）接收个人信息的第三方是否会变更目的使用个人信息；

9）个人信息的保存时间是否最小化，超出期限的删除等机制是否合理；

10）是否对用户画像机制进行限制，避免精确定位到特定个人；

11）是否为个性化展示提供用户可控制、可退出或关闭的机制；

12）匿名化机制是否有效，去标识化后的个人信息是否能够被关联分析等，导致可重新识别个人信息主体身份；

13）是否提供及时有效的安全事件通知机制和应急处置机制；

14）是否提供有效的投诉和维权渠道等；

15）是否未经用户同意向第三方共享、转让个人信息；

16）是否散播不准确的数据或不完整的误导性数据；

17）是否诱导或强迫个人提供过多个人信息；

18）是否过多地追踪或监视个人行为；

19）是否无根据地限制个人控制其个人信息的行为等；

20）其他个人信息处理流程的规范性。

注：对个人信息处理流程规范性的分析可参照GB/T 35273-2020相应内容。

c）参与人员与第三方。评估时关注的要素包括但不限于：

1）是否任命个人信息保护负责人或个人信息保护工作机构.个人信息保护负责人是否由具有相关管理工作经历和个人信息保护专业知识的人员担任；

2）是否依据业务安全需求，制定并执行个人信息安全管理的方针和策略；

3）是否制定涉及个人信息处理各环节的安全管理制度，并提出具体的安全管理要求；

安证合规集团&北源律师事务所

4）是否与从事冬人信息处理岗位上的相关人员签署保密协议，并对大量接触个人敏感信息的人员进行背景审查；

5）是否明确内部涉及个人信息处理不同岗位的安全职责，并建立发生安全事件的处罚、问责机制；

6）是否对个人信息处理岗位上的相关人员开展个人信息安全专业化培训和考核，并确保相关人员熟练掌握隐私政策和相关规程；

7）是否明确可能访问个人信息的外部服务人员需遵守的个人信息安全要求，并进行监督；

8）是否与第三方签署有约束力的合同等文件，约定个人信息传输至第三方后的处理目的、方式、数据留存期限、超出期限后的处理方式；

9）是否对第三方处理个人信息的行为进行定期检查、审计，确保其严格执行合同等约定；

10）其他方面的必要措施。

注：如果组织参照其他网络安全、数据安全相关国家标准建立成熟的安全管理体系可基于其已有基础进行分析评估.

d）业务特点和规模及安全态势。评估时关注的要素包括但不限于：

1）业务对个人信息处理的依赖性；

2）业务处理或可能处理个人信息的数量、频率、用户规模、用户峰值等；

3）是否曾经发生过个人信息泄露、篡改、毁损、丢失等事件；

4）个人信息保护相关执法监管动态；

5）近期内遭受网络攻击或发生安全事件的情况；

6）近期收到过或公开发布的安全相关的警示信息。

组织在对以上维度的相应内容进行充分了解后，通过调研访谈、查阅支撑性文档、功能检查、技术测试等方式，识别已采取的措施与当前的状态。针对5.5中对个人权益影响分析的不同维度，从以上四方面对安全事件发生的可能性等级进行综合评价。

注：安全事件可能性等级评估可参考附录D中D.I.

5. 5个人权益影响分析

5.5.1个人权益维度

个人权益影响分析指分析特定的个人信息处理活动是否会对个人信息主体合法权益产生影响，以及可能产生何种影响。个人权益影响概括可分为“限制个人自主决定权”“引发差别性待遇”“个人名誉受损或遭受精神压力”“人身财产受损”四个维度：

a）限制个人自主决定权。例如被强迫执行不愿执行的换作、缺乏相关知识或缺少相关渠道

安证合规集团&北源律师事务所

更正个人信息、无法选择拒绝个性化广告的推送、被蓄意推送影响个人价值观判断的资讯等;

b）引发差别性待遇。例如因疾病、婚史、学籍等信息泄露造成的针对个人权利的歧视；因个人消费习惯等信息的滥用而对个人公平交易权造成损害等;

c）个人名誉受损或遭受精神压力。例如被他人冒用身份、公开不愿为人知的习惯、经历等，被频繁骚扰、监视追踪等;

d）人身财产受损。例如引发人身伤害、资金账户被盗、遭受诈骗、勒索等。

5. 5. 2个人权益影响分析过程

组织可根据数据映射分析结果及确定需要评估的个人信息处理活动，结合相关法律、法规、标准的要求或组织自定义的个人信息安全目标，分析个人信息处理活动全生命周期或特定处理行为对个人权 益可能产生的影响，以及个人信息泄露、毁损、丢失、滥用等对个人权益可能产生的影响，以审视是否 存在侵害个人信息主体权益的风险。

个人权益影响分析过程一般包含对个人信息敏感程度分析、个人信息处理活动特点分析、个人信息 处理活动问题分析以及影响程度分析四个阶段:

a）在个人信息敏感程度分析阶段，组织可参照国家有关法律、法规、标准，依据数据映射分析结果，分析个人信息的敏感程度对个人权益可能产生的影响。例如健康生理信息的泄露、滥用等可能会对个人生理、心理产生较严重的影响;

b）在个人信息处理活动特点分析阶段，组织可参照与国家有关法律、法规、标准，依据数据映射分析结果，分析个人信息处理活动是否涉及限制个人自主决定权、引发差别性待遇、个人名誉受损或遭受精神压力、人身财产受损等。例如公开披露个人经历的行为可能会对个人声誉产生影响;

c）在个人信息处理活动问题分析阶段，组织可参照与国家有关法律、法规、标准.依据数据映射分析结果，分析个人信息处理活动可能存在的弱点、差距和问题，其中5.4 b）中的对个人信息流程规范性的分析结果可以支撑该阶段的分析过程，对问题严重程度的分析有助于分析个人权益的影响程度:

d）在个人权益影响程度分析阶段，组织可结合前几个阶段的分析结果，综合分析个人信息处理活动对个人权益可能造成的影响，及其严重程度。

注：个人权益影响程度评估可参考附录D中D. 2.

5.6安全风险综合分析

进行安全风险综合分析时，可参照4. 5中的基本原理，采取以下步骤:

a）参照5.4,分析已实施的安全措施、相关方、处理规模等要素，评价安全事件发生的可能性

安证合规集团&北源律师事务所

等级：

b）参照5.5,分析可能发生的安全事件会对个人权益产生何种影响，并评价对个人权益影响的程度等级：

c）综合考虑安全事件可能性和个人权益影响程度两个要素，综合分析得出个人信息处理活动的安全风险等级。

注：安全风险分析的具体过程和风险等级的判定可参考咐录D中D.3,安全风险分析的具体过程可参考使用附录C中表 C. 3、表C.4和表C.5.

在完成针对特定个人信息处理活动影响评估之后，组织可综合针对所有相关个人信息处理活动的评估结果，形成对整个评估对象（如业务部门、具体项目、具体合作等）的风险等级。

5. 7评估报告

评估报告的内容通常包括：个人信息保护专员的审批页面、评估报告适用范围、实施评估及撰写报告的人员信息、参考的法律、法规和标准、个人信息影响评估对象（明确涉及的个人敏感信息）、评估内容、涉及的相关方等，以及个人权益影响分析结果，安全保护措施分析结果、安全事件发生的可能性分析结果、风险判定的准则、合规性分析结果、风险分析过程及结果、风险处置建议等。

5. 8风险处置和持续改进

根据评估结果，组织可选取并实施相应的安全控制措施进行风险处置通常情况下，可根据风险的等级，采取立即处置、限期处置、权衡影响和成本后处置，接受风险等处置方式。

组织需持续跟踪风险处置的落实情况，评估剩余风险，将风险控制在可接受的范围内。此外，还可 将评估结果用于下一次个人信息安全影响评估工作。

5 9制定报告发布策略

为促进自身持续提升人人信息保护水平、配合监管活动、增加客户信任，组织可制定个人信息安全影响评估报告发布策略。选择公开发布的个人信息安全影响评估报告可以在已有评估报告基础上予以简化，但其内容通常不少于以下方面：

a）收集和处理个人信息的类型和必要性；

b）收集和处理的个人信息类型（个人敏感信息需单独强调）；

c）个人信息处理的例外情况（法律法规规定等）；

d）合规性分析的概况：

e）评估过程和结果概况；

f）已实施和将要实施的风险处置措施概况：

安证合规集团&北源律师事务所

g）对个人信息主体的建议；

h）实施评估责任部门和人员的联系方式和解答疑问的渠道等。

附录A

（资料性附录）

评估性合规的示例及评估要点

A.1 概述

常见的个人信息相关法律、法规、标准中评估性合规要求，包括处理个人敏感信息、使用自动化决策方式处理个人信息、委托处理个人信息、向第三方转让或共享个人信息、公开披露个人信息、向境外转移个人信息、个人信息处理目的变更评估、个人信息匿名化和去标识化效果评估，以及确定个人信息安全事件处置方案的评估等，其中部分评估要点示例如下。

A.2 个人信息出境安全评估

个人信息出境场景的评估可参照有关国家标准执行。

A.3 个人信息处理目的变更前的影响评估

分析个人信息处理活动的影响时，需要考虑多种因素，以评估“与收集个人信息时所声称的目的具有直接或合理关联的范围”的影响为例，如果新设目的与原目的有直接或合理的关联，且不会为个人权 益带来额外影响，无需再次告知个人信息主体并征得其明示同意。判断时是否有直接或合理的关联，至少需要考虑如下因素：

——个人信息主体对原先目的、组织处理个人信息方式和方法的合理性的理解程度；

——个人信息收集时的场景，包括个人信息主体和组织之间的关系、产品或服务的范围及使用的商标和名称、个人信息主体使用产品或服务的方式、产品或服务为个人信息主体提供的便利等；

——特定场景中可合理预期的个人信息处理方式，如常规商业运营中，可预见到的将被使用的个人 信息的类型，与个人信息主体之间直接互动的范围、频率、性质、历史，以及为提供产品或服务，或改进或推广产品或服务，可预见到的将被使用的个人信息的类型。

——如将所收集的个人信息用于学术研究或得出对自然、科学、社会、经济等现象总体状态的描述，属于与收集目的具有合理关联的范围之内。但对外提供学术研究或描述的结果时，需对结果中所包含的个人信息进行去标识化处理，否则在对目的变更后的影响评估中可能会得出存在高风险的判断。

A.4 个人信息匿名化和去标识化效果评估

匿名化和去标识化对个人信息进行了技术处理，使其在不借助额外信息的情况下，无法识别

安证合规集团&北源律师事务所

个人信息主体。但数据接收方可能会借助于额外的信息以及技术手段，进行重标识攻击，从而将去标识化的数据集归因到原始个人信息主体或一组个人信息主体。

常见的用于重标识的方法如下：

——筛选：基于是否能唯一确定一个个人信息主体，将属于一个个人信息主体的记录筛选出来；

——关联：将不同数据集中关于相同个人信息主体的信息关联；

——推断：通过其它属性的值以一定概率推断出一个属性的值。

评估个人信息匿名化和去标识化效果时，可充分考虑以下要素：

——个人信息匿名化和去标识化过程的规范性，所采用技术的通用性；

——匿名化后的个人信息是否为统计型结果；

——去标识化后的个人信息是否能够达到使用目的；

——匿名化和去标识化后的个人信息使用场景；

——如委托第三方进行去标识化或匿名化时，需评估其采用的方案及数据安全保障能力；

——能否在公开渠道或数据交易组织获得类似的个人信息；

——未经去标识化或匿名化处理保留的个人信息类型和内容的特殊性。

A.5 个人信息委托处理、转让、共享或公开披露前的影响评估

在对个人信息进行委托处理、转让、共享和公开披露前，开展个人信息安全影响评估，评估的内容包括但不限于以下方面：

——个人信息的类型、数量、敏感程度等；

——是否向个人信息主体告知了转让、共享、公开披露的基本情况，并征得个人信息主体的明示授权同意；

——数据发送方的安全管理保障和安全技术保障能力；

——数据接收方的安全管理保障和安全技术保障能力（不包括公开披露）；

——数据接收方可能会开展的个人信息处理活动，或公开披露的个人信息可能会被使用的个人信息处理场景；

——个人信息是否进行过去标识化处理；

——发生个人信息安全事件后的补救措施；

——数据接收方所能响应个人信息主体的请求的范围，如：访问、更正、删除等。

A.6 确定个人信息安全事件处置方案的评估

发生个人信息安全事件后，组织需及时评估事件可能造成的影响，并采取必要措施控制事态，

安证合规集团&北京律师事务所

消除隐患。评估影响时，可充分考虑以下因素：

——个人信息的类型、数量、敏感程度、涉及的个人信息主体数量等；

——发生事件的信息系统状况，对其他互联系统的影响；

——已采取或将要采取的处置措施及措施的有效性；

——对个人信息主体权益造成的直接影响和长期影响；

——向个人信息主体告知事件的方式和内容；

——是否达到《国家网络安全事件应急预案》等有关规定的上报要求。

A.7 使用自动化决策方式处理个人信息的评估

组织在设计、采用自动化决策方式处理个人信息时，如自动决定个人征信及贷款额度，或用于面试 人员的自动化筛选等，需充分考虑对个人权益产生的不利影响，并在在规划设计阶段或首次使用前开展个人信息安全影响评估，评估考虑的要素包括：

——是否向用户说明了自动化决策的基本原理或运行机制；

——是否定期对自动化决策的效果进行评价；

——是否对自动化决策使用的数据源、算法等持续优化；

——是否向用户提供针对自动化决策结果的投诉渠道；

——是否支持对自动化决策结果的人工复核。

附录B

（资料性附录）

高风险的个人信息处理活动示例

个人信息处理活动自身可能涉及对个人信息主体权益影响及相应风险较高的情况下，需开展个人 信息安全影响评估，可能产生高风险的个人信息处理活动及场景示例见表A. 1。

表B. 1高风险的个人信息处理活动及场景示例

个人信息处理活动	场景示例
a）数据处理涉及对个人信息主体的评 价或评分，特别是对个人信息主体的工作表现、经济状况、健康状况、偏好 或兴趣的评估或预测：	示例1：对个人信息主体使用社交网络和其他应用程序的行为进行分析，以便向其发送商业信息或垃圾邮件。 示例2:：银行或其他金融组织在提供贷款前使用人工智能算法对个人信息 主体进行信用评估，数据处理可能涉及与信用评估没有直接关联的个人信息。 示例3：保险公司通过分析香烟、酒精、极限运动、驾驶等偏好数

	据，评估个人信息主体的生活方式、健康状况等，据此作出保费设置的决策。
b）使用个人信息进行自动分析给出司 法裁定或其他对个人有重大影响的决定:	示例1：在设置有分段测速或电子收费的道路，建设有用于流量、道路违 规等行为的检测系统，特别是能墟自动识别车辆的系统，对驾驶员及其驾驶行为进行详细的记录和监督，并给出是否违法的判断。 示例2：电商平台监控用户购物行为，进行用户画像，分析用户的购买偏好和购买能力，设置针对用户特定偏好的营销计划。
C）系统性的监控分析个人或个人信息，如在公共区域监控、采集个人信息等，但仅在涉及违规事件分析时才使用的视频监测系统除外;	示例1:大规模公共空间监测系统，用于人员追踪并且能够收集超出提供服务范围的个人信息。 示例2：设置在工作场所的 IT 监测系统，监控员工的电子邮件、所使用的应用程序等，用于分析员工工作时间及使用工具（如电子邮件、互联网）的情况.
d）收集的个人敏感信息数量、比较多、收集频率要求高、与个人经历、思想观点、健康、财务状况等密切相关;	示例1:通过智能手表、手环、制服、头鼓或其它移动设备持续收集或监控个人信息主体的活动、健康相关数据。 示例2：通过健身手环或智能手机中的传感器持续收集或监控用户运动、健康相关数据，通过数据分析和处理提供定制化的健身建议或改善训练流 程的服务。
e）数据处理的规模较大，如涉及100万人以上、持续时间久、在某个特定群体 的占比超过50%、涵盖的地理区域广泛或较集中等:	示例1：社交网络、在线浏览器、有线电视订阅服务大规模收集用户浏览网站、购买记录、观看记录、收听记录等数据. 示例2：百货商店、购物中心或其他类似营业场所中，通过收集路人和顾客的 GPS、蓝牙或移动通信信号，对客流情况进行监测，跟踪顾客的购物路线和购物习惯.

表 **B. 1** （续）

个人信息处理活动	场景示例

f）对不同处理活动的数据集进行匹配和合并，并应用于业务：	示例1:基于防欺诈或风险管控目的，电商平台合并处理不同来源的数据集，以便根据分析或测试结果显示的风险值采取相应管控措施。 示例2：电商平台、零售商店通过分析顾客的购物、优惠券使用等行为数据，结合顾客的信用数据、第三方和社交网络数据等，获得提高销售额的营销策略。
g）数据处理涉及弱势群体的，如未成年人、病人、老年人、低收入人群等：	示例1:能够连接网络的智能玩具收集儿童玩耍的音频、视频数据，或收集儿童的年龄、性别、位置等信息。 示例2：在远程医疗场景中，医生通过网站或应用程序与患者进行视频通话，通过各类传感器收集分析患者的血糖、血氧等健康数据。
h）创新型技术或解决方案的应用，如生物特征识别、物联网、人工智能等；	示例1：通过人工智能提供客户服务或支持呼叫中心利用人工智能技术处理呼叫者的音频数据，自动评估呼叫者的心情，并根据评估结果确定与呼叫者的沟通方式或向呼叫者提供的建议。 示例2：健身俱乐部、酒店等入口控制系统，拍纹支付或刷脸支付等支付程序，通过收集和处理个人信息主体的个人生物识别信息，判断是否拥有进入某些区域、使用某些功能的权限。
1）处理个人信息可能导致个人信息主体无法行使权利、使用服务或得到合同保障等。	示例1:提供贷款、信贷、分期付款销售的实体通过收集、处理包含有债务人或类似个人信息主体的数据库信息，针对潜在客户制定信贷决策。

判断个人信息处理活动是否与上述场景相关，需考虑贯穿数据映射分析、合规差距分析等过程，一旦涉及上述情形，可针对以上场景评估影响和风险，同时重视个人信息主体代表等相关方的咨询意见,保障评估的准确性。

附录C

（资料性附录）

个人信息安全影响评估常用工具表

以下工具表（表C.1-表C.5）均为资料性工具，供组织进行评估时选取参考。工具表以个人信息处理活动/场景/特性或组件为维度，各表可基于此项进行整合或分开处理。建议组织采取IT化/自动化处理方式进行影响评估。

表C. 1基于处理活动/场景/特性或蛆件的个人信息映射表

个人信息处理活动/场景/特性或组件	个人信息类型[1]	个人信息主体	个人信息收集、处理的目的	个人信息处理的合法事由	个人信息控制者[2]	个人信息处理者[3]	是否涉及跨境转移[4]	是否涉及第三方共享[5]
处理活动 A								
处理活动 B								
处理活动 C								

表C.2个人信息生命周期安全管理

个人信息处理活动/场景/特性或组件	相关个人信息项	收集来源	收集方式	存储方式/加密措施	传输方式/加密措施	存储期艰	删除/匿名化方式
处理活动A[6]							
处理活动 B							
处理活动 C							

表C. 3安全事件可能性分析表

个人信息处理活动/场景/'特性或组件	风险源维度	产生风险的原因/存在的问此	相关证据	安全事件发生可能性
处理活动A	网络环境和技术措施			

	个人信息处理流程			
	参与人员与第三方			
	业务特点和规模及安全态势			
处理活动B				

表C. 4安全风险评估及整改措施表

个人信息处理活动/场景/或组件	风险源维度	产生风险的原因/存在的问题	安全事件发生可能性等级	对个人权益产生的影响维度	影响程度	风险描述及等级	相关责任方与风险处置建议	整改效果验证及归档情况
处理活动 A	网络环境和技术措施			限制个人自主决定权				
				引发差别性待遇				
				个人名誉受损或遭受精神压力				
				人身财产受损				
	个人信息处理流程							
	参与人员与第三方							

	业务特点和堺模及安全态势							
处理活动 B								

注：评估过程中仅需体现识别出的风险源维度及对个人权益产生的影响维度，可不体现本标准所列举所有维度。

组织针对特定个人信息处理活动开展具体的风险分析时，可参考表C.5简化评估过程，首先，从识别的风险源维度出发，分析可能发生的安全事件及其可能性，同时，按照影响程度类型，分析对个人信息主体权益的影响程度，如果两者存在交叉，则可参考表D.5得出风险等级，并简要说明存在风险的原因。

表C.5特定个人信息处理活动的安全风险评估表

影响方面	限制个人自主决定权		引发差别性待遇		名誉受损或精神压力		人身财产受损	
	风险等级	原因说明	风险等级	原因说明	风险等级	原因说明	风险等级	原因说明
网络环境和技术措施								
个人信息处理流程								
参与人员与第三方								
业务特点和规模及								

安全态势								

附录 D

（资料性附录）

个人信息安全影响评估参考方法

D. 1评估安全事件发生的可能性

安全事件可能性等级评价可采用定性、半定量和定量的方式。安全事件可能性等级判定准则见表D1.

表D. 1安全事件可能性等级判定准则

可能性描述	可能性等级
采取的措施严重不足，个人信息处理行为极不规范，安全事件的发生几乎不可避免	很高
采取的措施存在不足，个人信息处理行为不规范，安全事件曾经发生过或已经在类似场景下被证实发生过	高
采取了一定的措施，个人信息处理行为遵循了基本的规范性原则，安全事件在同行业、领域被证实发生过	中
采取了较有效的措施个人信息处理行为遵循了规范性最佳实践，安全事件还未被证实发生过	低

以定性方式为例，可从“网络环境和技术措施”、“处理流程规范性”、“参与人员与第三方”、“安全态势及业务特点”等方面，依据本标准表D.1的判定准则，对安全事件可能性等级进行评价。可能性等级分为“很高”、“高”、“中”、“低”四个等级，安全事件可能性判定可参考表D.2。

表D. 2可能性判定表

可能性描述	可能性等级
网络环境与互联网及大最信息系统有交互现象，基本上未采取安全措施保护个人信息安全。	很高
该个人信息处理行为为常态、不间断的业务行为，该行为已经对个人主体的权益造成了影响，或收到了大最相关的投诉，并引起了社会关注。	

任意人员可接触到个人信息,对第三方处理个人信息的范度无任何限制或已出现第三方滥用个人信息的情形。	
威胁引发的相关安全事件已经被本组织发现，或已收到监管部门发出的相关风险警报。	
网络环境与互联网及其他信息系统有较多交互现象，采取的安全措施不够全面。	高
该个人信息处理行为为常态、不间断的业务行为，个人信息处理行为不规范，且收到了相关的投诉	
对处理个人信息相关人员的管理松散，管理制度无落实的记录，未对第三方处理个人信息的范围提出相关要求。	
威胁引发的相关安全事件曾经在组织内部发生过，或已在合作方中发生，或收到过权威组织发出的相关风险预警信息，或处理个人信息的规模超过1000万人。	

表D.2 （续）

可能性描述	可能性等级
网络环境与互联网及其他信息系统有交互现象，采取了一定的安全措施。	
该个人信息处理行为为常态业务行为，个人信息处理行为规范性欠缺，且合作伙伴或同领域 其他组织收到过相关的投诉。	
有相关的管理制度，对人员提出了管理要求，对第三方处理个人信息的范围提出限制条件. 但相应的管理和监督效果不明.	中
威胁引发的相关安全事件已经被同领域其他组织发现，或在专业组织相关报告中被证实已出 现，或处理个人信息的规模超过100万人。	
网络环境比较独立，交互少，或采取了有效的措施保护个人信息安全。	
该个人信息处理行为非常态业务行为，个人侑息处理行为符合规范，几乎没有出现关于该行 为的投诉0	低
有完善的管理机制，对人员的管理和审核比较严格，与第三方合作时提出有效的约束条件并 进行监督，	
威胁引发的安全事件仅被专业组织所预测.	

评估过程中，可根据事件自身的性质估计和经验数据评估其可能性，再根据组织所实施的针对性安 全控制措施、相关事件处置经验对可能性进行修正。比如，个人信息处理的规模超过1000万人，但有 完备的、针对性的个人信息保护措施和应急机制.或者已具备类似事件处置的经验，并得到了个人信息 主体的认同，则安全可能性等级可降低一A级别。在进行修正时需要具体说明修正的理由，必要时可咨 询外部专业组织保证修正过程的合理性。

D.2 评估个人信息、主体权益影响程度

个人权益影响程度评价可采用定性、半定量和定量的方式。个人权益影响程度判定准则见表D.3。

表D. 3个人权益影响程度判定准则

影响描述	影响程度
个人信息主体可能会遭受重大的、不可消除的、可能无法克服的影响。如遭受无法承担的债务、失去工作能力、导致长期的心理或生理疾病、导致死亡等	严重
个人信息主体可能遭受重大影响，个人信息主体克服难度高.消除影响代价大如遭受诈骗、资金被盗用、被银行列入黑名单、信用评分受损、名誉受损、造成歧视、被解雇、被法院传唤、健康状况恶化等.	高
个人信息主体可能会遭受较严重的困扰，且克服困扰存在一定的准度。如付出额外成本、无法使用所提供的服务、造成误鲜、产生害怕和紧张的情绪、导致较小的生理疾病等。	中
个人信息主体可能会遭受一定程度的困扰，但尚可以克服，如被占用额外的时间、被打扰、产生厌烦和恼怒情緒等。	低

以定性方式为例，可从"限制个人自主决定权”、"引发差别性待遇”、"个人名誉受损和遭受精神压 力”、“人身财产受损”四个维度，依据表D.3的判定准则，对个人信息主体的权益进行影响程度评价。 影响程度分为“严重”、“高”、“中”、“低”四个等级，影响程度判定可参考表D.4。

表D.4影响程度判定表

影响类别	影响描述	影响程度
限制个人自主决定权	例如个人人身自由受限。	严重
	例如被强迫执行违反个人意愿的操作、被蓄意推送消息影响个人价值	高

	观判断、可能引发个人人身自由受限。	
	例如缺乏相关知识或缺少相关渠道更正个人信息、为使用应提供的产品或服务而付出额外的成本等。	中
	例如被占用额外的时同	低
引发差别性待遇	例如因信息淅露造成歧视性对待以致被用人单位解除劳动关系。	严重
	例如造成对个人合法权利的歧视性待遇、造成对个人公平交易圾的损害（无法全部或部分使用所提供的产品或服务）。	高
	例如造成误解、为使用所提供的产品或服务而需付出额外的成本（包含资金成本、时间成本等）。	中
	例如耗费额外的时间获取公平的服务或取得相应的资格等.	低
个人名誉受损和遭受精神压力	例如名誉受损以致长期无法获得财务收入、导致长期的心理或生理疾病以至于失去工作能力、导致死亡等。	严重
	例如名誉受损以致被用人单位解除劳动关系、导致心理或生理疾病以致健康遭受不可逆的损害等。	高
	例如造成误解、名誉受损（通过澄清可全部或部分恢复）、产生害怕和紧张的情绪、导致心理或生理疾病（通过治疗或纠正措施，短期可痊愈）等。	中
	例如被频繁打扰、产生厌烦和恼怒情绪等.	低
人身财产受损	例如造成重伤、遭憂无法承担的债务等.	严重
	例如造成轻伤、瀆受金融诈骗、资金被盗用、征信信息受损等。	高
	例如造成轻微伤、社会信用受损，为获取金隸产品或服务，或挽回损失需付出额外的成本等。	中
	例如因个人信息更正而需执行额外的流程（或提供額外的证明性材料）等。	低

评估过程中.可先分析个人信息姓理活动对某一个个人信息主体造成的影响程度，再根据处理活动的规模、特点、外部环境、个人信息去标识化、群体性特征等要素修正影响等级。比如，个人信息处理活动涉及典型的个人敏感信息，如健康状况等，且达到一定的数量（如50万人），则影响程度可上升一个级别；如果受影响个人信息主体群体抗财务风险能力差、心理承受能力差等情形。如未成年人、学生、老年人等.则影响程度可上升一个级别；如果个人信息经去标识化后已

确认降低敏感程度的，影响程度可降低一个级别。在进行修正时需要具体说明修正的理由，必要时可咨询外部专业组织保证修正过程的合理性。

此外，从组织实践角度出发，可以进一步将个人信息主体权益的影响映射到对组织的影响，以促进组织进一步认识到其中的风险。比如，可根据个人权益受损对组织付出的成本进行评价。成本一般包括：违规成本（如监管处罚、诉讼费用、整改费用等）、直接的业务损失（如流失客户减少了业务收入等）、名誉损失（如品牌形象受损、客户信任受损等）、内部企业文化损失（如企业执行力受损、价值观冲突引起员工积极性下降等）等，以上方面还可以进行初步的半定量或定最分析（比如处罚的案例与罚金等），以促进组织充分重视个人信息保护工作，积极改进，降低个人信息处理过程对个人权益的影响。

D. 3个人信息安全风险综合评估

综合分析个人权益影响程度和安全事件可能性两个要素，得出风险等级，并给出相应的改进建议， 最终形成评估报告。风险等级可分为：严重、高、中、低四个等级。以定性分析为例，可参考表D.5。

组织可以根据自身业务特点和内部风险管理策略，设计科学、合理的风险等级判定表，并设定何种 等级风险为不可接受的风险，但注意保证风险等级判定表不得随意变更或修订，必要时可咨询外部专业 组织保证风险等级判定表的合理性。

表 D.5 风险等级判定表

风险等级		可能性级别			
		低	中	高	很高
影响级别	严重	中	高	[illegible]	[illegible]
	高	中	中	高	[illegible]
	中	低	中	中	高
	低	低	低	中	中

安证[illegible]

信息安全技术 移动智能终端个人信息保护技术要求

基本信息:	
【发布机关】中华人民共和国国家质量监督检验检疫总局、中国国家标准化管理委员会	【时效性】 现行有效 【效力级别】国家标准
【标准编号】GB/T 34978-2017	【实施日期】2018.05.01
【发布日期】2017.11.01	

安证合规集团&北源律师事务所

信息安全技术 移动智能终端个人信息保护技术要求

1范围

本标准规定了移动智能终端的个人信息分类及个人信息的保护原则和技术要求。

本标准适用于指导公共及商业用途的移动智能终端进行个人信息的处理，其他有关各方也可参照使用。

2规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件最新版本（包括所有的修改单）适用于本文件。

GB/Z 28828-2012信息安全技术 公共及商用服务信息系统个人信息保护指南

3术语、定义和缩略语

3.1术语和定义

下列术语和定义适用于本文件。

3.1.1

移动智能终端 smart mobile terminal

能够接入移动通信网，具有能够提供应用程序开发接口的开放操作系统，并能够安装和运行第三方应用软件的手持或便携设备。

3.1.2

移动智能终端应用程序 smart mobile terminal application

安装在移动智能终端设备上能够利用移动智能终端设备上操作系统提供的开发接口，实现某项或某几项特定任务的计算机程序。

3.1.3

移动智能终端个人信息 smart mobile terminal personal information

即为移动智能终端中操作系统或应用软件所处理、与移动智能终端用户相关，且能够单独或通过与其他信息相结合使用，从而识别该移动智能终端用户的数据信息。

3.1.4

个人信息主体 subject of personal information

个人信息指向的自然人。

3.1.5

明示同意 expressed consent

个人信息主体明确授权同意，并保留证据。

3.2缩略语

下列缩略语适用于本义件。

API：应用程序编程接口 (Application Programming Interface)

IMEI：国际移动设备身份码(International Mobile Equipment Identity)

UDIDs：唯一设备识别符(Unique Device Identifier)

4移动智能终端个人信息分类

4.1概述

移动智能终端个人信息主要包含通信信息、日志信息、账户信息、金融支付信息、传感采集信息、设备信息和文件信息共七大类别，涉及了包括移动智能终端设备系统固有、用户存储及应用程序生成等各类个人信息数据。

4.2个人信息分类

4.2.1通信信息是指移动智能终端用户用于发起或接受通信以及在通信过程中所产生的数据信息。包括通讯录、通讯记录、短信、彩信、邮件、即时通信消息等。

4.2.2日志信息是指移动智能终端用户通过使用应用程序而记录的与时间相关的事件信息.或由应用程序产生的以时间为检索条件的使用记录或缓存数据。

4.2.3账户信息是指移动智能终端应用程序在注册或登录时需要填写的信息，以及移动智能终端中各 应用程序所存储的个人账号相关信息。

4.2.4金融支付信息是指移动智能终端用户借助终端参与金融交易或支付活动而产生的数据信息。包括交易验证码、动态口令等。

4.2.5传感采集信息是指利用移动智能终端传感器设备所采集到的、能反映移动智能终端设备用户的 周边环境和身份特征的数据信息。包括地理位置信息、指纹信息等。

4.2.6设备信息是指可标识移动智能终端唯一性的数据信息。包括1MEI、UDID等。

安证合规集团&北源律师事务所

4.2.7文件信息是指存储在移动智能终端设备存储介质中的数据信息。包括照片、音频、视频、文本等各种类型文件数据。

5移动智能终端个人信息保护原则

在对移动智能终端个人信息进行处理时，一般应按GB/Z 28828-2012中4.2的要求。遵循其目的明确、最少够用、公开告知、个人同意、质量保证、安全保障、诚信履行和责任明确八项原则合理的利用个 人信息。

6移动智能终端个人信息保护技术要求

6.1概述

在移动智能终端个人信息的处理过程中可分为收集、加工、转移和删除四个主要环节。对个人信息的保护贯穿于四个阶段中:

a)收集阶段是指移动智能终端系统和应用程序对设备中个人信息的提取和记录。

1))加工阶段是指移动智能终端系统和应用程序对收集到的个人信息进行的操作处理，如录入、存储、修改、标注等。

c)转移阶段是指移动智能终端系统和应用程序对收集和处理的个人信息进行发送和传输,从而将个人信息转移复制到其他信息系统。

d）删除阶段指使移动智能终端个人信息在收集、加工处理和传输存储过程结束后个人信息不再可用时应删除相应数据。

6.2个人信息收集阶段

6.2.1移动智能终端操作系统应对系统资源的调用进行监控、保护和提醒，确保涉及收集个人信息的行为总是在受控的状态下，不会造成出现用户不可控的行为的执行。

6.2.2移动智能终端系统和应用程序.在通过调用操作系统或其他安装的第三方软件系统提供的API 接口收集个人信息时，应告知用户，让用户知晓当前操作会收集个人信息的种类，以及收集的个人信息的用途。

6.2.3在收集个人信息过程中，移动智能终端系统和应用程序只应收集能够达到已告知目的的最少信息。

6.2.4持续收集个人信息时，应允许移动智能终端用户配置、调整或关闭个人信息收集功能。

6.2.5移动智能终端系统和应用程序不应该采取隐蔽手段或以间接方式收集个人信息。

6.2.6收集涉及个人敏感信息和身份特征的个人信息数据时应采用明示同意的告知许可方式。

6.2.7收集阶段的告知提醒.应明确一个时间有效期，包括一段时间或长期等。

6.2.8个人信息收集方在收集阶段进行告知提醒时，应提供对个人信息进行全过程安全保护的

安证合规集团&北源律师事务所

证据。

6.3个人信息加工阶段

6.3.1移动智能终端系统和应用程序在对个人信息进行加工处理时,应告知加工目的、方法或手段。

6.3.2不对收集阶段告知范围以外的个人信息数据进行加工处理。

6.3.3保证个人信息在加工处理过程中的安全性，在整个过程中个人信息不应被三方无关人员或组织获知，过程数据和结果数据都应加密处理，且加密处理方式和强度应符合公共或商用标准。

6.3.4移动智能终端系统和应用程序对个人信息进行加工处理时，应保证系统稳定运行，不造成个人信息的损毁、泄露和丢失等,加工过程完毕时应进行数据完整性和正确性检查。

6.3.5移动智能终端中个人信息加工处理过程应可控，移动智能终端设备用户可配置、调整或关闭加工过程。

6.3.6移动智能终端系统和应用程序的设计者或开发者不应该在加工过程中采取隐蔽手段挖掘和分析归纳用户的身份特征数据。

6.4个人信息转移阶段

6.4.1移动智能终端系统和应用程序在进行个人信息数据传输转移时,应告知移动智能终端设备用户当前个人信息转移的目的、转移信息的获得者、转移数据的使用范围。

6.4.2不对收集阶段告知范围以外的个人信息数据进行转移处理。

6.4.3基于最少够用的原则，对于在本地加工处理能满足功能需求的个人信息数据，则不需要进行数据的传输转移。

6.4.4通讯数据和环境数据类等涉及个人敏感信息或身份特征的个人信息，经移动智能终端设备用户同意授权后才可转移。

6.4.5个人信息的数据转移过程应保证所转移数据的安全性、完整性及正确性，转移或转存的个人信息数据其过程和结果都应进行加密处理，且加密处理方式和强度应符合公共或商用标准。

6.4.6个人信息数据的转移过程应要控，移动智能终端设备用户可对当前转移操作进行配置、调整或关闭操作。

6.5个人信息删除阶段

6.5.1移动智能终端系统和应用程序对收集、加工、转移阶段所使用的个人信息的缓存数据，应该提供自动删除或者手动删除功能。

6.5.2移动智能终端系统和应用程序提供的删除功能应该具备数据彻底删除能力，以保证被删除的个人信息数据不可被恢复。

安证合规集团&北源律师事务所

6.5.3移动智能终端设备遗失或被盗时，移动智能终端系统和应用程序应确保原设备中的个人信息数据可以被远程销毁。

信息安全技术 个人信息告知同意指南

基本信息：	
【发布机关】全国信息安全标准化技术委员会	【时效性】 -
【标准编号】-	【效力级别】-
【发布日期】2020.01.20	【实施日期】-

信息安全技术 个人信息告知同意指南

1 适用范围

本标准为网络运营者个人信息处理告知的内容、结构及征得个人信息主体同意收集、使用、对外提供个人信息的方式提供指导。

本标准适用于规范网络运营者在网络环境中进行个人信息告知同意的情形。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 25069-2010 信息安全技术 术语

GB/T 35273-2017 信息安全技术 个人信息安全规范

3 术语和定义

GB/T 35273-2017 《信息安全技术 个人信息安全规范》和GB/T 20984-2007 《信息安全技术 信息 安全风险评估规范》中的术语和定义,以及下列术语和定义适用于本文件。

3.1

个人信息 personal information

以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息。

注1：个人信息包括姓名、出生日期、身份证件号码、个人生物识别信息、住址、通信通讯联系方式、通信记录和内容、账号密码、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息等。

安证合规集团&北源律师事务所

3.2

个人敏感信息　personal sensitive information

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。

注1：个人敏感信息包括身份证件号码、个人生物识别信息、银行账号、通信记录和内容、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息、14岁以下（含）儿童的个人信息等。

3.3

个人信息主体　personal information subject

个人信息所标识或者关联的自然人。

3.4

个人信息控制者　personal information controller

有权决定个人信息处理目的、方式等的组织或个人。

3.5

告知 notice

将与个人信息处理活动相关信息提供给个人信息主体，使其了解个人信息处理活动的有关规则。

3.6

授权同意　consent

个人信息主体对其个人信息进行特定处理作出明确授权的行为，包括通过积极的行为作出授权（即明示同意），或者通过消极的不作为而作出授权。

注1：例如信息采集区域内的个人信息主体在被告知信息收集行为后没有离开该区域；

注2：例如个人信息主体未自行拒绝使用产品或服务，且产品或服务可通过公开可访问的隐私政策等文件了解收集使用个人信息规则。

3.7

明示同意　explicit consent

个人信息主体通过书面、口头等方式主动作出纸质或电子形式的声明，或者自主作出肯定性动作，对其个人信息进行特定处理作出明确授权的行为。

注：肯定性动作包括个人信息主体主动勾选、主动点击“同意”“注册”“发送”“拨打”、主动填写或提供等。

安证合规集团&北源律师事务所

3.8

对外提供 external provision

个人信息控制者通过共享、转让、公开披露等方式将个人信息传输或披露给第三方的过程。

3.9

告知同意界面 notice consent interface

个人信息告知同意界面通常包括移动和PC端交互式界面、IoT终端、海报、签字页等。

4 缩略语

PC个人电脑 Personal Computer

SDK软件工具开发包 Software Development Kit

IoT物联网 Internet of Things

AI人工智能 Artificial Intelligence

API应用程序接口 Application Programming Interface

5 告知同意的适用情形

5.1 收集使用个人信息时的告知同意

收集个人信息时，需向个人信息主体告知收集、使用个人信息的类型、目的、方式和范围，并征得个人信息主体的明示同意，收集个人信息包括但不限于以下情形；

a)个人信息主体主动填写、选择、上传等主动提供个人信息的；

b)个人信息控制者通过智能终端、API、SDK、IoT设备、浏览器、传感器等自动采集个人信息的；

c)个人信息控制者通过与用户交互记录个人信息主体行为的；

d)个人信息控制者从第三方间接接受、查询等方式间接获取的；

e)个人信息控制者从非完全公开渠道搜集个人信息的；

f)个人信息控制者从个人信息主体关联身份或账号收集个人信息的；

g)个人信息控制者使用大数据、AI等技术分析、关联和生成个人信息的。

5.2 使用目的变更时的告知同意

个人信息控制者也业务需要需变更使用目的的，需向个人信息主体告知涉及的个人信息类型、变更原因、变更后的处理目的，并再次征得个人信息主体的明示同意。使用目的变更包括但不限于以下情形：

a)个人信息控制者收集个人信息后，超出原有授权范围应用于新的业务场景的；

b)个人信息控制者间接获取个人信息后，进行加工处理形成新的个人信息并用于其他目的；

安证合规集团&北源律师事务所

c)个人信息控制者所提供的产品或服务基于业务扩展而增加的新的功能，该新增功能收集使用个人信息都超出原授权范围的；

d)个人信息控制者进行收购、兼并等，将获取的个人信息超出原有授权范围使用的；

e)个人信息控制者收集后涉及重大处理规则变化的，例如需要将个人信息传输到境外进行处理的。

5.3 对外提供个人信息时的告知同意

个人信息控制者对外提供个人信息时，需向个人信息主体告知个人信息类型、目的、接收方等，并事先征得个人信息主体的明示同意。对外提供个人信息包括但不限于以下情形：

a)个人信息控制者应业务所需向第三方共享个人信息；

b)个人信息控制者应业务变更等原因，向第三方转让个人信息，且不再保留个人信息；

c)个人信息控制者以不定向方式向公众公开披露个人信息；

d)其他个人信息控制者对外提供个人信息的情形，但个人信息控制者向接受其委托、为其提供个人信息处理服务的情形除外。

5.4 告知同意的其他情形

以下情形，需要对个人信息主体告知原因、目的、处理方式、可能产生的影响等：

a)涉及个人信息出境的情形；

b)个人信息处理规则，如隐私政策，内容发生对个人信息主体权益产生影响的实质性变化时；

c)个人信息主体撤回授权同意时；

d)个人信息主体注销账号时；

e)对个人信息进行汇聚融合，且可能对个人信息主体权益产生影响时；

f)发生个人信息安全事件，且可能对个人信息主体合法权益造成侵害时。

6 免于告知同意的情形

6.1 收集使用个人信息时免于告知同意的情形

以下情形中，个人信息控制者收集、使用个人信息的，需以适当方式告知个人信息主体目的，但无需征得个人信息主体的明示同意：

a)与个人信息控制者履行法律法规规定的强制性义务相关的，例如为履行相关法律法规规定的反洗钱监管要求，收集实名身份信息及相关交易记录；

b)与国家安全、国防安全直接相关的；

c)与公共安全、公共卫生、公共网络安全、网络环境治理、重大公共利益直接相关的，例如为加强口岸防控人感染特定流感疫情，对疑似病例人员采样进行病原体监测，详细登记其个人信

安证合规集团&北源律师事务所

息、联系方式等；

d)与犯罪侦查直接相关的，例如为侦查刑事案件，收集、使用犯罪嫌疑人的指纹、DNA等生物信息、通话记录、上网记录等；

e)出于维护个人信息主体或其他个人的生命、财产等重大合法权益但又很难得到本人同意的，例如因患者陷入严重昏迷无法取得本人同意，医生为救助患者必须检测其血型以向其输血；

f)所涉及的个人信息是个人信息主体自行向不特定社会公众公开的，例如收集、使用用户在开放式社交平台上自行向所有平台用户公开的本人学历背景、就职单位等个人信息；

g)与商业或职务行为直接相关的个人信息，例如企业依法注册登记、备案的法定代表人、股东、监事、高管的个人信息，个体工商户依法登记、备案的个人信息等；

h)为履行或签订个人信息主体与个体信息控制者之间的合同所必需的，如，购物网站为实现其基本功能寄送用户网购的商品而收集、使用用户的姓名、住址和联系电话，网络租房平台为实现其基本功能与用户签订租房合同，收集用户的实名信息、手机号码等个人信息；

i)用于维护所提供的产品或服务安全、质量和稳定运行以及防范危害运营安全行为所必需的。例如某软件为确保产品或服务的安全稳定运行，收集用户的设备类型、网络运行日志、崩溃报告等日志信息用于分析和改善软件运行情况；或者防止恶意注册、批量点击等危害运营安全活动，收集用户设备信息、日志信息、网络接入情况等信息。

j)个人信息控制者为学术研究机构，出于公共利益开展统计或学术研究所科研机构必要，且其对外提供学术研究或描述的结果时，对结果中所包含的个人信息进行去标识化处理的，例如某学术研究机构为调查研究某公共政策对不同性别、不同年龄、不同地区的人群的影响情况，收集、使用被调查人员的性别、年龄、地区等个人信息，但在提供研究成果时对所包含的个人信息进行去标识化处理；

k)个人信息控制者为新闻单位且其在开展合法的新闻报道所必需的，例如某报社为报道某大学志愿者在贫困山区支教的情况，收集、使用了志愿者的姓名、在读学校等个人信息等；

l)从合法公开披露的信息中收集个人信息的，如合法的新闻报道、政府信息公开等渠道，例如国家审计署网站公告的移送违纪违法问题线索的查处情况等；

m)与个人信息主体求职、就业直接相关的，例如用人单位收集个人信息主体投递的包含姓名、联系电话、学历背景、工作经验等个人信息的简历；

n)法律法规规定的其他情形，例如酒店、航空公司等按照相关法律法规规定收集旅客的实名身份信息等。

o)专为未成年人提供服务的产品或应用，为保障未成年人的合法权益（例如：教育应用为保

安证合规集团&北源律师事务所

障教学过程中教师不侵犯儿童合法权益而对教学视频进行抽检），在充分告知监护人的前提下，可以豁免征求同意。

p)收集已进行匿名化处理的个人信息，该个人信息无法单独识别到个人身份（不具有可识别性的信息）；

q)个人信息控制者因被收购、兼并、重组、分拆等主体变更导致向继受者提供或者转移个人信息的情形；

r)法律法规规定的其他情形。

注：个人信息控制者在以上情形中收集使用个人信息的，应该告知信息主体收集使用其个人信息的情形。

6.2 使用目的变更时免于告知同意的情形

以下情形中，可以综合考虑变更个人信息使用目的对个人信息主体造成的影响，在不会对个人权益带来额外影响的前提下，决定是否采取明示同意的方式：

a)新设目的与原先授权目的有直接或合理的关联，个人信息控制者采取类似的处理规则和安全保护措施；

b)服务升级、改造后使用个人信息的频率、用户画像计算和展现方式、与个人信息主体的互动方式发生调整的；

c)将所收集的个人信息用于学术研究或得出对自然、科学、社会、经济等现象总体状态的描述，且使用对外提供学术研究或描述的结果时，对个人信息进行去标识化处理的；

d)经个人信息安全影响评估后无高风险，且以合理方式披露评估结果的。

6.3 对外提供个人信息时免于告知同意的情形

个人信息控制者共享、转让、公开披露个人信息时，需以适当方式告知用户目的，但无需征得个人信息主体的明示同意：

a)与国家安全、国防安全直接相关的；

b)与公共安全、公共卫生、重大公共利益直接相关的，例如在发生大规模地质灾害的紧急情况下，向有关人员的亲属、行政机关和救援部队提供受灾人群、伤亡人员的个人信息；

c)与犯罪侦查直接相关的，例如金融机构为配合公安机关调查某金融犯罪，依据有效法律文书向公安机关提供嫌疑人交易流水信息；

d)出于维护个人信息主体或其他个人的生命、财产等重大合法权益但又很难得到本人同意的，例如因个人信息主体陷入昏迷无法取得同意，医院甲向拟为患者实施紧急抢救的医院乙提供包括药物过敏史在内的病史信息等个人信息，以帮助医院乙的医生进行手术抢救；

安证合规集团&北源律师事务所

e)个人信息主体自行向不特定社会公众公开的个人信息，例如用户在开放式社交平台上自行向所有平台用户公开的本人昵称、头像等个人信息；

f)对外提供已进行去标识化处理的个人信息，该个人信息无法单独识别到个人身份，且经个人信息安全影响评估后接收方不可识别个人身份的；

g)个人信息控制者因被收购、兼并、重组、分拆等主体变更导致向数据接受者转让个人信息，且数据接收者承诺将继续履行安全义务的；

h)法律法规规定的其他情形。

7 告知同意的基本原则

7.1 告知的基本原则

个人信息控制者在实施告知同意时需考虑以下基本原则，保证告知过程切实有效：

a)公开透明——公布收集、使用个人信息的范围、目的，不隐瞒产品或服务所收集的个人信息及其使用目的，不采取故意遮挡、隐藏等方式诱导个人信息主体略过告知内容；

b)逐一传达——向个人信息主体逐一告知相关内容，有显著困难时也可采取公告方式；

c)同步实时——当涉及具体业务功能收集、使用等个人信息处理场景时，或触发个人信息收集行为时，对个人信息主体进行即时告知；

d)真实准确——反映产品或服务真实、准确的个人信息收集使用范围、目的；

e)具体明确——告知个人信息的类型、目的等内容需结合实际业务场景，不使用格式化条款；

f)清晰易懂——告知文本符合个人信息主体的语言习惯（如简体中文），使用标准化语言、数字、图示等，避免使用有歧义的语言。

7.2 同意的基本原则

个人信息控制者在实施告知同意时需考虑以下基本原则，保证征得同意过程切实有效：

a)告知一致——征得同意的授权范围与所告知内容相一致；

b)自主选择——主动向个人信息主体展示征得同意的选项，支持其自行做出选择，不给出同意时，仅影响当前服务类型的正常使用；

c)时机恰当——在个人信息收集行为发生前，且同步传达告知内容时，征得个人信息主体同意，以增进个人信息主体对业务功能与所收集的个人信息之间关联性的理解；

d)分类独立——区分产品或服务的服务类型后，分别征得个人信息主体同意，不采用捆绑方式强迫个人信息主体一次性接受或拒绝所有可能收集的个人信息。

7.3 告知同意需考虑的要素

个人信息控制者在实施告知同意时还可以考虑以下要素，优化告知同意的方案和机制：

安证合规集团&北清律师事务所

a)友好展示——使用友好、生动、形象的方式编辑告知内容（如使用插图、漫画等），优化告知内容风格及其组织形式，以促进个人信息主体理解；

b)适应载体——告知内容、展示形式、征得同意的方式等可以根据告知载体的类型、界面特点进行适应性设计，如适宜的字体大小、额外的震动和语音提示等；

c)考虑影响——确定告知内容的详细程度和个人信息主体给出“肯定性动作”进行同意的明确程度时，可根据个人信息处理活动对个人权益影响程度进行权衡，包括对个人信息主体使用服务过程的用户体验等因素；

d)区分阶段——根据个人信息主体使用产品和服务业务功能的范围和个人信息处理阶段，结合隐私政策、用户协议、提示语句等不同文本的性质和展示效果，设置具体的告知同意方案；

e)兼顾差异——充分考虑复杂多样的网络条件、技术差异，个人信息主体的理解能力、水平（例如儿童或残障人士）等，使用可以广泛适用或针对特定群体的告知同意解决方案。

8 告知

8.1 告知的内容

8.1.1 一般的告知内容

个人信息控制者向个人信息主体告知的内容包括：

a)个人信息控制者基本情况：

1)个人信息控制者注册名称、注册地址、常用办公地点和相关负责人的联系方式等。

b)个人信息的收集、使用：

1)至少包括基本功能运行所必要收集的个人信息类型；

注：所必要收集的个人信息是指收集的个人信息与业务功能之间具有直接的关联关系，该业务功能仅能在收集、使用该个人信息的条件下得以实现。

2)收集的具体个人信息范围，包括图片信息、影像信息、音频信息、文本信息等；

3)不得将敏感数据与一般信息混淆在一起进行告知。收集的个人信息涉及个人敏感信息的，明确标识或突出显示；

4)收集、使用个人信息的目的，以及目的所涵盖的各个业务功能，例如将个人信息用于推送商业广告，将个人信息用于形成直接用户画像及其用途等。针对用户画像、广告目的应与其他目的区分进行告知；

5)不同信息有不同目的时，分别进行详细说明；同一信息有多个目的，按照信息对用户的影响程度排序，对用户影响最严重的优先进行说明。

6)提供个人信息后可能存在的安全风险，及不提供个人信息可能产生的影响；

安证合规集团&北源律师事务所

7)提供个人信息后能够获取的权益，例如个人信息主体可以享受更加有针对性的服务，个人信息控制者可以确保在某些特殊情况下为个人信息主体提供更安全的产品和服务等；

8)提供告知中应遵循的个人信息的使用权利和义务，及用户授权选项；

9)个人信息的收集方式、收集频率、收集的时间。例如，应用软件告知用户收集信息的时间长度，如单次，一段时间或长期。

c)存储：

1)个人信息存放地域，以及涉及数据出境时的个人信息处理规则；

2)个人信息保存期限，包括注销账号前保存期限及注销账号后的保存期限，以及保存期限届满后的处理规则；

3)采取的各种存储安全技术措施，例如身份验证、访问控制、完整性保护、加密、病毒防护等。

d)对外提供（包括对外共享、转让、公开披露）：

1)对外共享：应用软件告知用户收集到的个人信息是否会向第三方公司进行共享。如共享，则应告知用户对第三方的审核要求，如第三方公司收集实施者、收集内容、使用目的、收集时间、保护措施，以及所承担的相应法律责任。

2)转让：应用软件告知用户个人信息是否会进行转让。如转让，则告知转让方名称、联系方式、转让目的、转让内容、以及转让方所承担的相应法律责任等。

3)公开披露：应用软件告知用户收集到的个人信息是否会进行公开披露。如公开披露则应告知公开披露的对象，公开披露的时间，公开披露的影响等；

e)个人信息主体的相关权利及实现方法：

1)个人信息主体的权利和实现机制，如查询方法、更正方法、删除方法、注销账户的方法、撤回同意的方法、获取个人信息副本的方法、约束信息系统自动决策的方法等；

2)处理个人信息主体询问、投诉的渠道和机制，以及外部纠纷解决机构及联络方式；

3)个人信息主体可以再次查看告知内容的方法和路径。

f)其他：

1)本告知遵循的相关国家法律法规和政策；

2)遵循的个人信息安全基本原则，具备的数据安全能力、安全组织、安全流程，必要时可公开数据安全和个人信息保护相关的合规证明；

3)涉及SDK等外部代码的引用：应用软件是否存在SDK等外部代码的引用，以及SDK等外部代码收集处理个人信息的情况。

安证合规集团&北清律师事务所

8.1.2 额外的告知内容

a)个人信息控制者逐一告知扩展功能所需收集的信息时，告知内容包括：

1)个人信息收集目的以及个人信息类型；

2)个人信息使用、存储、对外提供、个人信息主体相关权利及实现方法与公示的个人信息处理基本规则相同的，适用基本规则。与个人信息处理基本规则有所不同的，予以特殊说明。

b)个人信息处理基本规则或者某项个人信息的处理活动发生重要变化时，告知内容包括：：

个人信息控制者在业务功能开启前、收集使用的目的发生变化、收集使用的个人信息范围发生变化、停止收集个人信息等特殊情况下应告知的内容包括：

1)在基本业务功能开启前（如个人信息主体初始安装、首次使用、注册账号等），应向个人信息主体告知基本业务功能所必要收集的个人信息类型，以及个人信息主体拒绝提供或拒绝同意收集将带来的影响；

2)在扩展业务功能开启前，应向个人信息主体逐一告知所提供扩展业务功能及所必要收集的个人信息；

3)收集使用个人信息的目的发生变更、收集使用个人信息的范围发生变化时，应向个人信息主体告知变化的具体内容，并重新征得个人信息主体的明示同意；

4)在某些业务功能停止运营之后，应及时向个人信息主体告知已停止继续收集相关个人信息，采取的对个人信息删除或匿名化等措施，以保证个人信息主体可以终止同意授予。

8.2 告知的方式

个人信息控制者将与个人信息处理有关的规则等内容告知个人信息主体的方式应结合自身产品或服务特点，基于本标准第7.1和7.3中的原则，选择适当的告知方式，具体包括：

a)个人信息控制者就个人信息处理活动制定基本规则，例如专门、单独的隐私政策或文本协议，并以易于访问的方式公开展示；

b)在基本业务功能开启前（如个人信息主体初始安装、首次使用、注册账号等），向个人信息主体告知个人信息控制者的个人信息收集使用规则（包括基本业务功能所必要收集的个人信息类型，个人信息主体拒绝提供或拒绝同意收集将带来的影响）；

c)个人信息控制者可以将隐私政策的完整版链接置于基本业务功能开启时告知相关的交互界面或设计中；

d)在扩展功能开启前，向个人信息主体逐一告知所提供扩展业务功能及所必要收集的个人信息；当逐一告知某项功能收集的个人信息时，如果产品展示出的功能或者产品名称能够明示个人信息收集目的、使用用途的，可以不予以单独说明；

安证合规集团&北源律师事务所

e)收集个人信息时，宜采用交互式界面进行告知，例如弹窗、文字说明、填写框、提示条、提示音等类似方式；

f)使用目的变更、对外提供个人信息、个人信息处理规则发生变化时，宜使用弹窗、浮窗、短信、邮件、消息推送等显著方式进行告知；

g)可以通过邮件、短信的方式告知临时性的个人信息处理行为。如，产品或服务停止运营、发生个人信息安全事件、间接获取到个人信息等；

h)当涉及可能对个人权益产生重大影响的个人信息收集、使用行为时，可选择电话方式告知；

i)当逐一向个人信息主体告知成本过高或者有显著困难时，可以以公告的形式发布；

j)可通过图标、文字、应用名称、动画、音/视频等多种形式编辑告知内容。

8.3 告知的展示

8.3.1 告知的展现形式

个人信息控制者应当以便于个人信息主体立即阅读的方式展现告知内容，且内容简洁、主次分明。此外，还应当根据环境与情景的不同进行调整，优化告知内容的展现形式，具体如下：

a)PC端可以采取弹出窗口和下拉列表的方式展示告知内容；

b)移动端由于设备屏幕较小、显示容量受限，可以采用多层次的告知同意模式，通过以简短内容（可包含文字和图示）告知关键内容，同时提供完整版告知内容的链接；

c)IoT设备可以在连接互联网时通过绑定该设备的移动端程序展示告知内容，如果设备配备显示屏且足以展示告知内容的，也可以在自带的显示屏上进行展示；

d)书面等方式告知时，可将核心告知内容布置于签字确认区域附近。

8.3.2 告知内容的展示形式

告知内容展示需以个人信息主体视角的用户体验和权益保障为中心，包括：

a)收集的个人信息涉及个人敏感信息的，需明确标识或突出显示；

b)个人信息处理规则等告知内容发生重大变化的部分，需明确标识或突出显示；

c)将对个人信息主体产生重要的或易于引起异议或争端的内容靠前推送，以便用户自行理解并支持其后续关于同意的判断；

d)针对特殊群体，提供除文本外的图片、语音或视频等对告知内容进行阐述。

8.4 告知的适当性

8.4.1 告知的适当时机

个人信息控制者应当在个人信息收集之前或收集之时及停止收集之后向个人信息主体告知。如果告知的时间点和收集个人信息的时间点相差很大，建议个人信息控制者在进一步收集个人信

息之前再次告知，以便个人信息主体意识到告知与个人信息收集之间的关系。例如，针对不同场景下的个人信息收集的情况应及时向个人信息主体告知。在停止收集个人信息之后，也应及时告知，以保证个人信息主体的知情权。

应用软件的告知时机与频率应与用户体验感及舒适度相平衡。告知的时机包括：

a)下载安装前：应用软件在下载安装前，宜通过应用软件主页或下载页面等方式告知用户应用软件在运行使用过程中需收集处理的个人信息。

b)首次使用前：应用软件在首次运行时，应告知用户需收集处理的个人信息。

c)信息收集前：应用软件收集个人信息前，应告知用户需收集处理的个人信息。

d)信息变更前：当收集处理的内容、使用目的、保护方式、信息共享等发生重大变更时，应重新告知用户。

e)信息转让前：应用软件在信息转移前，应告知用户进行转让操作的个人信息。

f)应用软件卸载前：应用软件在进行卸载前，应告知用户个人信息存储/删除情况。注销账户时：用户在注销账户时，应用软件应告知用户个人信息存储/删除情况。

g)应用软件停止运营时：应用软件停止运营时，应告知用户个人信息的处理情况。

h)安全事件发生时：应用软件发生安全事件时，应告知用户个人信息面临的风险情况。

i)间接获取个人信息时：应用软件在间接获取个人信息时，如开展业务需进行的个人信息处理活动超出用户授权范围，应在获取个人信息后的合理期限内或处理个人信息前，明确告知用户，并征求用户同意。

j)通过其他载体收集个人信息时：应用软件应告知用户收集处理的个人信息情况。

注：个人信息控制者处理活动发生变更需要征得个人信息主体的授权同意的，应当考虑个人信息主体是否可以查阅同意内容的历史记录，以及之前的同意至再次征求同意经历了多长时间。如果个人信息主体可以随时查阅其历史同意内容，或距上次告知时间较短，个人信息控制者可以选择仅告知变更内容，并征得个人信息主体对变更内容的授权同意。否则，个人信息控制者在告知变更内容并征得个人信息主体对变更内容的授权同意之外，还可以确认个人信息主体授权同意原始内容。

8.4.3 告知的适当频率

个人信息控制者应当以适当的频率或时间间隔确认现有的同意或征得个人信息主体的新同意。个人信息控制者应当避免告知的频率过低，导致告知的内容与时机情况不符；同时避免告知的频率过高对个人信息主体造成不必要的打扰。

8.4.4 告知的适当位置

安证合规集团&北源律师事务所

个人信息控制者应当在个人信息主体习惯性访问的位置进行告知，包括：

a)在用户注册页面、登录页面、移动互联网应用程序启动页、社交媒体首页等显著位置显示个人信息收集处理规则；

b)采取浮窗、弹窗等方式告知时，优先选取网站、移动互联网应用程序主界面；

c)在网站、应用程序交互式界面展示隐私政策时，不宜藏匿太深，如打开主界面起，多于4次点击、滑动等才能访问到隐私政策；

d)需要用户主动填写提交个人信息的，可以在填写或选择框中使用灰色字体简述目的等内容。

9 同意

9.1 同意模式选择

个人信息控制者征得同意时，需优先采用明示同意的方式，确保个人信息主体在理解收集目的和相关处理规则的基础上自主给出的、具体的、清晰明确的意愿表示，且尽量避免采取授权同意的机制，以致个人信息主体忽略对个人信息处理规则的关注。明示同意的模式主要包括：

a)设置交互式界面，由个人信息主体做出主动勾选、主动点击“同意”“下一步”“继续”、滑动滑块、主动发送等动作表示意愿；

b)由个人信息主体主动填写、输入个人信息表示意愿；

c)由个人信息主体开启可收集个人信息的API、权限表示意愿；

d)个人信息主体通过纸质或电子的书面声明、签字确认表示意愿；

e)个人信息主体通过电子签名方式表示意愿；

f)个人信息主体通过电话录音、视频录像等方式表示意愿；

个人信息控制者可结合产品或服务的特点，可能多个人信息主体造成影响的程度等因素，选择上述同意模式中的一种或几种。如收集个人信息可能对个人信息主体权益造成重大财产损失的，可在交互式界面执行“下一步”“同意”等操作基础上，进一步采取电话回访、签字确认等方式。

存在以下情形且经个人信息影响评估后无高风险，可考虑采用授权同意模式：

a)产品或服务的业务场景网络等环境条件受限；

b)产品或服务的展示界面和展示方式受限；

c)基于最小必要考虑，为实现业务功能仅收集无法直接关联到个人身份的个人信息；

d)执行同意需要付出大额成本才可以实现；

e)告知后执行同意可能对个人信息主体使用产品或服务的良好习惯带来削减；

f)告知后执行同意可能影响业务运营安全的；

g)需告知的目的等内容有助于保护个人信息主体权益；

安证合规集团&北源律师事务所

h)需告知的目的等内容为本标准第6章直接相关的。

9.2 同意机制设计

个人信息控制者设计同意机制时需注重以下方面：

a)个人信息控制者应当以个人信息主体能够清楚理解的方式设计同意机制，在同意界面清晰地、明确地向个人信息主体展示如何给予同意，使个人信息主体能够清楚地、无疑问的操作以表达授权同意；

b)个人信息控制者在展示告知内容的同一页面征得个人信息主体的同意；

注：若告知内容与征得同意不在同一页面，个人信息主体可能会对同意的内容产生困惑。若无法在同一页面进行告知并征得同意，应当采取进一步措施确保个人信息主体了解其同意的内容。

c)个人信息控制者应当避免选取模棱两可的同意机制，必须确保个人信息主体授权同意的行为可以与其它行为区分开来，使个人信息主体授权同意的意图毋庸置疑（例如，仅继续正常浏览网站不构成个人信息主体明示同意个人信息处理）；

d)个人信息控制者应当将个人信息处理的同意与其它同意区分开来，更不得将其隐匿在其它事项中并使得个人信息主体接受（例如，个人信息主体接受一般性的服务条款不构成个人信息主体同意个人信息处理；

e)个人信息控制者应当使个人信息主体能够就必须收集的个人信息和选择收集的个人信息分别授权同意。

9.3 同意的变更与撤回

9.3.1 同意的变更

个人信息控制者应当设立便捷的机制使个人信息主体能够变更其授权同意。如果个人信息主体无法变更同意，个人信息控制者需向个人信息主体解释造成这种情况的原因。

9.3.2 同意的撤回

个人信息控制者应当设立便捷机制使个人信息主体能够随时撤回其授权同意，并注意以下几点：

a)授权同意的撤回不应影响在撤回前基于授权同意作出的数据处理；

b)个人信息主体在作出授权同意之前，个人信息控制者应告知其拥有授权同意撤回的权利，且撤回同意的操作容易程度应当授予同意等同；

c)如果个人信息主体无法撤回同意，个人信息控制者应当向个人信息主体解释造成该情况的原因；

d)个人信息控制者在实施同意撤回动作之前，应确认请求提出者为个人信息主体本人或有权

安证合规集团&北源律师事务所

处理者。

9.4 告知同意的证据留存

个人信息控制者需按照如下要求留存告知同意的证据：

a)个人信息控制者应当留存个人信息主体初次选择同意特定个人信息处理活动以及后续变更或撤回同意的证据；

b)告知同意证据内容主要包括：时间，事项，目的等，针对可能产生高风险的个人信息收集行为，还需留存具体的告知同意；

c)个人信息控制者可以根据自身情况灵活选择证据留存的方式。例如，在网络环境中，个人信息控制者可以留存当时个人信息主体授权同意的页面、告知同意的工作流程、个人信息主体同意行为的记录（如日志）以及提供给个人信息主体的告知内容；

d)只要有关的个人信息处理活动持续存在，个人信息控制者证明告知同意的义务就持续存在；在处理活动结束后，证据留存不应超过履行法律义务、提起或应对诉讼、纠纷的必要限度，例如以诉讼时效为限；

e)对于授权同意证据的留存，需避免因证据留存导致产生收集额外个人信息的情形。

附 录 A

（资料性附录）

未成年人个人信息的告知同意

收集使用年满14周岁的未成年人的个人信息前，宜将个人信息使用规则等信息告知该未成年人或其监护人，并征得该未成年人或其监护人的明示同意;收集不满14周岁的未成年人的个人信息前，应将个人信息使用规则等信息告知该未成年人的监护人，并征得其监护人的明示同意。

A.1 告知的内容

收集使用未成年人个人信息的告知，除本标准8.1中的相关信息外，还可以包含下列信息：

a)未成年人个人信息的敏感性与注意事项；

b)针对未成年人个人信息的敏感性所采取的特别的安全保障措施；

c)监护人更正、管理未成年人个人信息的方式和途径；

d)监护人正确履行监护职责，教育引导儿童增强个人信息保护意识和能力的方式；

e)若涉及幼儿园、学校等决定采用自动化设备收集未成年人个人信息的，可以说明采取此类措施的正当性、合法性与必要性，有必要时可提供相关的个人信息安全影响评估报告的全文或摘要，与监护人进行集体沟通的，可以告知沟通的总体情况与结论。

A.2 告知同意的方式

安证合规集团&北源律师事务所

A.2.1 核验未成年人和监护人身份的方式

个人信息控制者应采取合理措施核验个人信息主体的年龄，区分个人信息主体为不满14周岁的未成年人、已满14周岁的未成年人以及成年人的情形。若个人信息主体为不满14周岁的未成年人，则应当继续采取合理措施核验该未成年人监护人的身份；若个人信息主体为已满14周岁的未成年人，则宜继续采取合理措施核验该未成年人监护人的身份。

核验的方式宜充分考虑不同的产品或服务在受众群体上的本质差异，如果对所有的产品或服务都采取同一核实方式，可能会对用户造成打扰，例如，对于有关个人所得税查询的产品或服务而言，如果一味地要求个人信息主体进行严格的身份验证，则很可能会招来个人信息主体的不满。因此，对于不同的产品或服务宜采取不同强度的核验方式。

a)核验未成年人身份的方式

1)未成年人非为主要受众群体的产品或服务：未成年人几乎不会使用手机银行、租房等产品或服务， 此时宜采用验证强度较低的方式进行核实，例如通过弹窗询问个人信息主体是否已年满14周岁、要求个人信息主体声明其已年满14周岁等。

2)未成年人为主要受众群体的产品或服务：对于未成年人而言，有关游戏、社交以及教育等产品或服务是他们使用可能性较大的。此时宜采用验证强度较高的方式进行核验，例如要求个人信息主体输入生日信息（精确到年月日）、身份证号，或采取其他合理的方式进行身份验证，但上述措施不应超过必要限度（例如不应要求未成年人上传其手持身份证的照片）。

b)核验监护人身份的方式

1)若根据以上方式核验个人信息主体的身份为未成年人的，宜继续采取合理措施核验监护人的身份，合理措施包括短信验证、电话验证、邮箱验证、超链接验证等。

i.终端或应用仅单独面向未成年人的：核验的方式可采取短信验证、电话验证、邮箱验证等合理措施进行。例如通过让该未成年人输入监护人的手机号码，将验证监护人身份的内容发送至监护人的手机上，监护人可通过回复特定字段以表示是否为该未成年人的监护人。

注1：短信内容可参照：尊敬的用户您好！这里是xxxx，根据国家有关未成年人个人信息保护的要求，收集使用年满14周岁的未成年人的个人信息前，宜征得该未成年人或其监护人的明示同意;收集不满14周岁的未成年人的个人信息前，应征得其监护人的明示同意。若您是xxx的监护人，请回复“1”，若不是请回复“2”。本条短信5分钟内容有效。

ii.若产品或服务为未成年人和监护人提供了不同终端或应用界面的，核验的方式可直接在监护人终端或应用界面中完成。例如在未成年人的终端或应用界面提示为满足国家有关未成年人个人信息保护的要求，需要该未成年人将有关产品或服务的个人信息使用规则等信息告知其监护人，

安证合规集团&北源律师事务所

此时该未成年人的终端或应用界面上已生成用于分享给其监护人的超链接或二维码。未成年人可分享超链接或二维码至其监护人，其监护人打开该超链接或扫一扫该二维码之后可以下载或进入监护人专门的终端或应用，该监护人可在该终端或应用界面上确认其是否为该未成年人的监护人。

A.2.2 告知的方式

终端或应用仅单独面向未成年人的，宜使用未成年人可理解的方式进行告知，并在协议或交互界面中重点说明收集、使用未成年人信息的情况和敏感性，可参考身份核验的合理措施向其监护人进行告知，即在核验其为未成年人身份后，继续核验其监护人身份时，可将相关需要告知的信息采用短信、电子邮件的方式向其监护人告知。

注2：短信内容可参照：尊敬的家长您好！这里是xxxx，根据国家有关未成年人个人信息保护的要求，收集使用年满14周岁的未成年人的个人信息前，宜向该未成年人或其监护人告知个人信息使用规则等信息，并征得该未成年人或其监护人的明示同意;收集不满14周岁的未成年人的个人信息前，应向该未成年人的监护人告知个人信息使用规则等信息，并征得其监护人的明示同意。您的孩子正在试图使用我们提供的xxxx产品或服务，有关该产品或服务的个人信息使用规则等信息请您点击xxxx（超链接方式）进行了解。

若产品或服务为未成年人和监护人提供了不同终端或应用界面的，可以根据角色分别制定告知方案。未成年人端可以通过简明、易于理解的形式展示其在使用产品或服务过程中可能遇到的个人信息问题，并加以注意；监护人端可以通过弹窗、提示框、文字说明等形式详细说明未成年人信息收集、使用的情况，并重点提示未成年人个人信息的敏感性。例如在未成年人的终端或应用界面提示为满足国家有关未成年人个人信息保护的要求，需要该未成年人将有关产品或服务的个人信息使用规则等信息告知其监护人，此时该未成年人的终端或应用界面上已生成用于分享给其监护人的超链接或二维码。未成年人可分享超链接或二维码至其监护人，其监护人打开该超链接或扫一扫该二维码之后可以下载或进入监护人专门的终端或应用，该监护人可在该终端或应用界面上查询相应需要告知的内容。

若涉及幼儿园、中小学校、社会教育培训机构、儿童游乐场等公共场合场景下收集未成年人个人信息的，可以通过信件、公示、签署协议、即时通讯工具等方式告知未成年人监护人个人信息使用规则等信息。告知的方式可参考附录D。

注3：幼儿园、学校决定采用自动化设备收集未成年人信息（例如：为检验教学质量而采取监控设备、采用电子课程应用软件布置教学作业、采用物联网设备辅助教学等），一旦投入建设或进行采购，则监护人便难以做出有效反对。因此在决定采用自动化设备前，宜开展个人信息安全影响评估并与监护人进行集体沟通协商，根据协商结果做出最终决定。

安证合规集团&北源律师事务所

A.2.3 同意的方式

终端或应用仅单独面向未成年人的，可参考向未成年人的监护人进行告知的方式，并在告知时同时征求监护人的同意，即在将相关需要告知的信息采用短信、电子邮件的方式向其监护人告知时同时提供同意和拒绝的选项。

注4：短信内容可参照：尊敬的家长您好！这里是xxxx，根据国家儿童人个人信息保护的要求，收集使用年满14周岁的未成年人的个人信息前，应向该未成年人或其监护人告知个人信息使用规则等信息，并征得该未成年人或其监护人的明示同意;收集不满14周岁的未成年人的个人信息前，应向该未成年人的监护人告知个人信息使用规则等信息，并征得其监护人的明示同意。您的孩子正在试图使用我们提供的xxxx产品或服务，有关该产品或服务的个人信息使用规则等信息请您点击xxxxx（超链接方式）进行了解。若您同意您的孩子使用该产品或服务，请回复“TY”，若不是请回复“NO”。本条短信5分钟内容有效。

若产品或服务为未成年人和监护人提供了不同终端或应用界面的，可在向监护人告知个人信息使用规则等信息时同时征求监护人的同意。例如在监护人断通过弹窗展示授权页面，让监护人选择“同意”或“拒绝”。

若涉及幼儿园、中小学校、社会教育培训机构、儿童游乐场等单位收集未成年人个人信息的，可以在通过信件、公示、签署协议、即时通讯工具等方式告知未成年人监护人个人信息使用规则等信息时，征求其监护人的同意。同意的方式可参考附录D。

注5：幼儿园、学校为根据法律法规要求和必要的教学管理所需而收集未成年人信息的（例如：学籍信息、考勤信息、考试成绩等），可以免于征求同意，属于本标准6.1中收集使用个人信息时免于告知同意的情形。

附 录 B

（资料性附录）

SDK收集使用个人信息场景下的告知同意

SDK 是 Software Development Kit 的缩写，即“软件开发工具包”。简单来看，它是辅助开发某一类应用软件的相关文档、范例和工具的集合。对 App 来说，为了提高开发效率，可以将某项功能交给第三方来开发，第三方服务提供商将服务封装为工具包（即 SDK）供开发者使用。目前，SDK 类型主要包括：第三方登录分享类、支付类、推送类、广告类、数据统计分析类、地图类、风控插件以及一些基础库等。

SDK 提供者指开发并运营SDK的组织或个人。SDK 集成者指集成SDK并使用其功能的组织或个人。

安证合规集团&北源律师事务所

B.1 告知的内容

涉及集成和使用第三方SDK的移动应用，告知中还应包含以下内容：

a)使用的第三方SDK组件列表或组件类别示例，各组件提供的公司主体及各组件的下述相关信息；

b)第三方SDK的启动/加载方式，如自动/手动启动、同步/异步加载等；

c)第三方SDK是否进行了数据采集以及采集的主要数据，包括采集时间、采集数据字段；

d)如果第三方SDK进行了数据采集，是否允许用户进行关闭或限制；

e)如果第三方SDK进行了数据采集，是否对采集数据的传输进行了加密；

f)如果第三方SDK进行了数据采集，后台对采集数据的主要安全防护策略以及是否进行了安全测试；

B.2 告知同意的适用情形

B.2.1 一般的告知情形/收集使用个人信息时的告知同意

收集使用个人信息的告知同意情形原则上同标准5.1要求。对于SDK本身存在个收集个人信息的情况，应将所采集的个人信息类型及采集使用的目的告知个人信息主体。为此，SDK提供者应将SDK收集个人信息的全部情况（参考GB/T 35273 5.3）先行告知SDK集成者，SDK集成者依据标准所适用的情形，针对涉及个人信息采集的情况，采取适宜的方式进行个人信息采集的告知同意，SDK提供者应提供必要的配合。SDK收集用户个人信息前，应当自行或通过宿主应用软件征得用户同意，否则宿主APP应停止集成该SDK，SDK提供者应停止采集处理行为。根据SDK的功能不同，具体情况可以分为：

a)当SDK提供者不是个人信息控制者时（即提供的SDK为功能性SDK，所采集的个人信息全部为宿主APP控制），SDK提供者应保证宿主APP服务提供者知晓SDK采集个人信息的功能和范围；宿主APP服务提供者应在SDK收集个人信息前向个人信息主体告知并应征得个人信息主体同意。

b)当SDK提供者仅从宿主APP间接获取个人信息时，宿主APP服务提供者应向个人信息主体告知信息对外提供情况并应征得个人信息主体同意（标准主体5.3）。

c)当SDK提供者是直接个人信息控制者时（即SDK提供者通过SDK直接采集个人信息，宿主APP不能控制收集到的个人信息），SDK提供者应首先向宿主APP服务提供者告知所采集的个人信息类型及采集使用的目的，范围等。宿主APP服务提供者同意后方可集成SDK，SDK提供者应通过SDK本身或通过宿主APP，在收集个人信息前向个人信息主体告知并应征得个人信息主体同意。例如， SDK提供者通过单独用户界面的交互形式征得个人信息主体同意。

安证合规集团&北源律师事务所

注：如电商网站的支付SDK，点击支付SDK服务商的图标后会跳转/展示到SDK对应的页面上进行登录以及支付，在此场景下支付SDK独立收集并处理支付相关的个人信息，支付SDK宜在用户注册或使用服务时告知用户，展示第9.1条的告知内容，并征得用户的同意。

d)当SDK提供者与宿主APP服务提供者同是个人信息控制者时（即SDK提供者通过SDK直接采集个人信息，宿主APP服务提供者同时也可以控制收集到的个人信息），SDK提供者应首先向宿主APP服务提供者告知所采集的个人信息类型及采集使用的目的、范围等。宿主APP服务提供者同意后方可集成SDK，宿主APP服务提供者和SDK提供者各自或共同说明收集个人信息情况，并应征得个人信息主体同意。

B.2.1 使用目的变更时的告知同意

如存在SDK相关信息重大变更的情况，则应更新告知，并重新征得用户同意。

B.3 免于告知同意的情形

a)当SDK提供者不是直接的个人信息控制者时，宿主APP服务提供者应对个人信息主体负有有效告知同意义务。告知同意的例外适用标准主体6.1部分.

b)当SDK提供者不是直接的个人信息控制者但后续通过宿主APP服务提供者的提供而成为个人信息控制者时，SDK集成者应对个人信息主体负有有效告知同意义务。告知同意的例外适用标准主体6.3部分.

c)当SDK提供者是直接的个人信息控制者时，SDK提供者对于宿主APP服务提供者的告知同意例外适用于标准主体6.1和6.3部分；宿主APP服务提供者基于被告知的信息，对个人信息主体告知同意的例外适用于标准主体6.1和6.3部分。

附 录 C

（资料性附录）

IoT场景下的告知同意

IoT是internet of things的缩写，中文为“物联网”。物联网是指通过“随时”和“随地”连接任何事物而创建的一个全新的、动态的网络。

C.1 告知的内容

参考8.1.1节中所列的告知内容。

C.2 告知同意的方式

C.2.1 智慧生活的告知同意方式

C.2.1.1 告知同意方式

智慧生活设备是围绕用户家居生活的各种设备，包括照明设备、家用电器、各类传感器、监

安证合规集团&北源律师事务所

控摄像头等，智慧生活设备可以连接到云，由云端提供管理和服务，并通过控制设备，如手机、音箱等对其进行控制。

智慧生活设备收集个人信息的告知同意包括以下方式：

a)弱界面交互的产品，其告知内容通过建立连接设备上的web UI上展示，并获得用户的同意；如无线路由器、CPE（用户驻地设备）。

b)若App在与智慧生活设备绑定前就已经开始收集个人信息的，应当通过该App进行告知同意。

c)智慧生活设备在注册到智慧生活平台前，对于所收集的个人信息可通过与平台直接相连的APP告知用户，并获得用户同意。

d)智慧生活平台提供对智慧生活设备管理和服务，为实现对智慧生活设备的管理和服务，智慧生活平台需要收集注册到智慧生活平台上的设备的相关信息，在收集该信息前，通过与平台直接相连的APP告知用户所收集的个人信息，并征得用户同意。

智慧生活设备向第三方分享、从第三方获得个人信息的告知同意包括：

a)为实现智慧生平平台和三方平台之间的互联，当用户授权三方账号登陆时，应向用户展示智慧生活平台从三方平台获得的用户设备等信息，并获得用户同意。

此外，产品所提供的服务若跳转到由第三方提供的服务界面，还应告知用户该服务由第三方提供。

C.2.1.1 告知的时机

智慧生活设备或服务收集用户个人信息前，应该告知用户所收集的个人信息并获得用户同意。

C.2.2 运动健康的告知同意方式

C.2.2.1告知同意方式

运动健康指为用户提供运动指导和健康服务的产品或服务，运动健康设备包括智能手表、智能手环、耳机等穿戴设备和健康管理设备，如体脂秤、血压计、健身设备等。

运动健康场景收集个人信息的告知同意包括：

a)运动健康设备多为没有屏幕或屏幕尺寸受限的设备，与运动健康设备相关的个人信息处理在提供运动健康服务的APP上实现告知同意。

b)用户通过提供运动健康服务的APP绑定运动健康设备前，应告知用户的运动数据、健康数据等个人信息同步到提供运动健康服务的APP；若存在设备间数据同步，则应告知用户在设备间分享的数据类型，并告知用户解除绑定方式。

c)运动健康平台收集用户的个人资料、运动信息、健康信息等个人信息应在收集信息前明确告知用户，并获得用户同意。

安证合规集团&北京律师事务所

运动健康场景向第三方分享个人信息的告知同意包括：

d)用户使用运动健康服务，其个人数据可以共享给第三方，以使用户使用三方应用提供的运动健康服务，在数据共享前应告知用户，并得到用户授权，并告知用户取消授权的方式。

C.2.2.2 告知的时机

用户首次使用运动健康服务、绑定运动健康设备、或使用三方运动健康提供服务时，告知用户。

C.2.3 智能音箱的告知同意方式

智能音箱是指可连接网络实现播报新闻、播放音乐、互动聊天以及可能包含控制其他智能家庭设备的功能，可能采用语音的方式操控的音箱。

C.2.3.1. 告知同意方式

智能音箱收集个人信息的告知同意包括以下方式：

a)若智能音箱配备显示屏且足以展示告知内容的，可以在自带的显示屏上进行展示并获得用户同意。

b)若智能音箱不配备显示屏，或者为了更好的阅读体验，可以在其他终端展示，并通过（在屏幕直接显示或在印刷包装上）提供二维码、短链接（URL）等方式引导个人信息主体访问，或者采用语音播报提示重要内容，并获得用以同意，但应避免在此过程中收集个人信息。

c)若智能音箱可以绑定APP，可以通过绑定该设备的APP展示告知内容，并通过APP获得用户同意。

d)若绑定该智能音箱的APP收集不同于智能音箱收集的个人信息，应当在APP启动或账号登录时向用户展示告知内容，并通过APP获得用户同意。

e)若智能音箱以及APP收集的个人信息均通过APP展示告知内容的，则宜在告知内容上区分智能音箱及APP分别收集的个人信息类型和个人信息处理规则，并通过APP获得用户同意。

智能音箱向第三方分享、从第三方获得个人信息的告知同意包括：

a)当智能音箱其他智能家居设备的控制中枢，且该设备由其他数据控制者处理个人信息，则智能音箱在向其他控制者传输或者获取其他数据控制者收集的个人信息前（比如智能音箱需要将用户操作其他设备的指令传输给该其他设备实现操作，而该其他设备操作后需要返回操作结果等给智能音箱进而播报给用户），应当告知用户并获得用户同意。

C.2.3.1告知的时机

对于允许多人使用且能区分用户的设备，须在每个用户首次使用时获得同意。

C.2.4 告知的形式

安汇合规集团&北源律师事务所

告知的形式参考8.2节，包括隐私声明、隐私通知等。具体形式可以为弹窗询问、开关、链接、文字展示等。注意展示的字体、行距等足以让用户可清晰阅读。

附 录 D

（资料性附录）

公共场合场景下的告知同意

公共空间是指向不特定的社会公众开放的、供公共使用和活动的场所，包括市政道路、建筑物、公园、广场、绿地、滨水区域等开放式空间，也包括政府机关或企事业单位管理的机场、火车站、学校、图书馆、商场、餐饮娱乐产所、公共交通工具等非开放式空间。

D.1 告知的内容

a)建议个人信息控制者在产品PC端、移动端与公共场所的问讯处、柜台、管理办公室等处同时提供完整隐私政策或条款文本，供个人信息主体需要时查阅，内容宜包括本指南8.1建议的告知内容。

b)商场等公共场所收集未成年人个人信息的告知参照附录A。

c)在不特定人群进入的公共场所收集人脸等个人敏感信息的，应当符合法律法规的相关规定，并明确标识信息采集设备的性质和目的。

d)在特定人进入的场所采集人脸特征等个人敏感信息的，应当明确标识信息采集设备的性质和目的，并征得信息主体或其合法监护人的授权同意，依据法律法规和相关约定的情况除外。

e)在学校场景下采用人脸识别或者脑电波检测等技术收集人脸、脑电波等个人敏感信息的，应当明确标识信息采集设备的性质和目的并征得信息主体或其合法监护人的授权同意，并为信息主体提供拒绝的路径和方式。

f)在新零售场景下采用刷脸登陆、刷脸支付等技术时收集人脸等个人敏感信息的，应当明确标识信息采集设备的性质和目的并征得信息主体或其合法监护人的授权同意，并为信息主体提供其他登陆或支付的路径和方式，依据法律法规和相关约定的情况除外。

注：收集人脸信息仅用于与设备本地已存储的人脸信息进行比对或进行本地化处理而没有回传服务器的，不属于人脸信息的收集行为。

D.2 告知同意的方式

a)在汽车站、火车站、地铁站、机场、商场等公共场所收集个人信息时，建议个人信息控制者以显著方式向个人信息主体进行展示告知。公共场所张贴告知内容宜简短易懂，效果宜显著醒目，同时告知获取更多相关信息的途径。方式包括但不限于：

1)在汽车站、火车站、地铁站、机场、商场、店铺入口显著处张贴告知，例如：本地铁站安

安证合规集团&北清律师事务所

装有人脸识别系统，用于进行人群分流安检，我们承诺会保护您的人脸等信息安全，详情可向询问台咨询或扫描二维码。又如：本商场安装有人脸识别系统，以便进行客流分析或进行个性化推荐。我们承诺会保护您的人脸等信息安全，详情可向询问台咨询或扫描二维码。

2)在摄像头安装显著处张贴告知，例如：此处摄像头用于人脸识别，以便实现XXX目的。我们承诺会保护您的人脸等信息安全，详情可咨询收银台或扫描二维码。

3)在人脸识别购物柜显著处张贴告知，例如：此购物柜使用人脸识别支付，我们承诺会保护您的人脸等信息安全，详情可扫描二维码。

4)在商场或柜台导购导引时告知，例如：您成为我们的会员需要收集您的生日和地址，用于给您寄送赠品。我们不会泄露您的个人信息，具体信息您可以查询我们官网的隐私政策。

5)在顾客于柜台交易支付页面显著处张贴或者弹窗告知隐私政策。

b)当个人信息主体拒绝在公共场所收集其个人信息时，建议相关公共场所提供不收集个人信息的选择方案，例如，不参与分流安检的通道；不成为会员的购买方式；不通过人脸识别的支付方式等。

c)公共场所收集未成年人个人信息的告知参照附录A。

d)公共场所出于公共安全等原因由公权力安装摄像头或查询、向外提供个人信息参照本指南6.1与6.3相关条款。

D.3 免于告知同意的情形

个人信息控制者在公共空间收集个人信息的，以下情形属于“收集使用个人信息的告知同意例外”中所列的特殊情形，无需征得个人信息主体的明示同意:

a)信息主体自行公开的信息，但信息主体明确拒绝或者处理该信息侵害其它重大利益的除外。

b)与个人信息控制者履行法律法规规定的强制性义务相关的；

c)与国家安全、国防安全直接相关的；

d)与公共安全、公共卫生、重大公共利益直接相关的，例如在公共场所接入安防监控系统，并将监控系统与公安等监管部门对接；

e)所涉及的个人信息是个人信息主体自行向社会公众公开的，例如收集、使用用户在公共空间自行向公众公开的本人姓名、电话、照片等个人信息；

f)为履行或签订个人信息主体与个体信息控制者之间的合同所必要的，例如乘坐公交时，公交记录的用户刷卡时间、刷卡人ID、刷卡方式、乘车地点和下车地点等；

g)法律法规规定的其他情形。

注：个人信息控制者在公共空间收集个人信息，但在收集前难以取得个人信息主体明示同意

安证合规集团&北源律师事务所

的，如果数据处理不以“识别信息主体身份”为目的且不会对个人信息主体合法权益产生不利影响的，可以不经用户明示同意，但应当向个人信息主体提供了解其具体数据处理目的和方式的途径，并向用户提供撤回同意的渠道。例如，商场运营者出于优化商户管理、活动管理等合法正当目的，会基于商城内部署监控系统，统计和分析商场的人流量等。个人信息控制者基于上述场景收集完数据后，如果希望将收集的数据用于识别特定信息主体身份（例如收集人脸识别数据用于课堂情况监测或个性化推荐），应当就该等数据处理目的取得该信息主体的明示同意。

附 录 E

（资料性附录）

个性化推荐场景下的告知同意

个性化推荐是指个人信息控制者利用用户数据和算法推送新闻信息、商业广告等向个人信息主体提供的一种。个人信息控制者不得以提供个性化推荐为由，误导个人信息主体同意其收集个人信息。

个人信息控制者在提供个性化推荐时，应当以明显方式标明“个性化推荐”字样，并为用户提供关闭个性化推荐的功能；用户选择关闭个性化推荐的功能时，应当停止个性化推荐，并删除已经收集的设备识别码等用户数据和个人信息。

个人信息控制者提供个性化推荐服务应遵守法律、行政法规，尊重社会公德、商业道德、公序良俗，诚实守信，严禁歧视、欺诈等行为。

F.1 告知的内容

向个人信息主体告知个性化推荐的内容，除本标准9.1中的相关信息外，还可以包含下列信息：

a)个性化推荐功能是否会对个人信息主体的权益或自主决策造成影响；

b)个性化推荐功能的原理或实现方式；

c)个性化推荐功能的提供方；

d)告知管理个性化推荐功能的方式；

e)如提供采用非个性化推荐的同类功能，可以告知进入或开启该功能的方式。

F.2 告知同意的方式

向个人信息主体提供个性化推荐功能或服务，可以通过下列方式向个人信息主体告知个性化推荐功能或服务收集、使用个人信息的情况：

a)在首次开启或进入相关界面时，可以通过交互设计（弹窗、文字说明、提示条、提示框、提示音）等方式向个人信息主体进行告知；

b)个人信息主体主动提交的信息被用于个性化推荐的，在首次填写时可以采用即时告知的方

安证合规集团&北清律师事务所

式告知；

c)以个性化推荐为核心业务模式的（例如：资讯浏览、视频播放、社区论坛），可以在首次使用前采取弹窗等显著提示的方式告知；

d)功能或服务采用个性化推荐的，可以在功能开启或进入时，通过提示框等方式即时告知；

e)提供程序化广告功能的，可以在专门设置页面或可访问的文档中告知程序化广告的推荐原理。

注：若涉及未成年人的个人信息的，可参照附录A。

征求个人信息主体同意，宜同时提供非个性化推荐的同类功能（例如：根据热度、地区、时间流等自然排序的资讯模块）。

附 录 F

（资料性附录）

互联网金融场景下的告知同意

互联网金融场景下的告知同意主要涉及三类场景：

金融借贷，是指为用户提供从金融机构进行个人消费贷款服务，包括授信、借款、还款与交易记录等功能，这里的金融机构是指有放贷资质的银行、消费金融公司、小贷公司等在网络上提供借贷服务的机构。

助贷业务，是指金融科技机构通过自有系统或渠道筛选目标客群，在完成自有风控流程后，将较为优质的客户输送给持牌金融机构、类金融机构，经持牌金融机构、类金融机构风控终审后，完成发放贷款的一种业务。

金融机构线上业务，是指金融服务机构通过网络提供金融服务，为用户提供从金融机构进行存款、保险及投资理财服务，包括账户开户、存款、交易、认购、赎回、投保、理赔、分红、交易记录、查询与客服等功能，具有银行、保险、理财、投资等资质在网络上提供服务的金融机构及金融中介机构（统称“金融服务机构”）。

G.1告知的内容

G.1.1 收集使用个人信息的告知

a)金融机构收集法律法规要求的个人信息和实现服务所需的个人信息时，应将所采集的个人信息类型及采集使用的目的告知个人信息主体，并通过个人信息主体对信息收集主动做出肯定性动作征得其明示同意。

1)当金融机构出于向个人信息主体提供授信、借款、还款、交易记录等产品或服务而收集使用个人信息时，应当在实名认证、绑定银行账户信息、获取个人征信信息、紧急联系人信息、借

安证合规集团&北源律师事务所

贷交易记录等基本功能开启前，向个人信息主体告知基本业务功能所必要收集的个人信息类型，包括网络日志、手机号码、身份证件信息、账户信息、银行账户信息、个人征信信息、紧急联系人信息、借贷交易记录等。并向个人信息主体说明拒绝提供或拒绝同意收集将带来的影响，并通过个人信息主体对信息收集主动做出肯定性动作（如勾选、点击“同意”或“下一步”等）征得其明示同意；

2)当金融机构出于向个人信息主体提供产品或服务的扩展业务，包括但不限于基于定位的扩展功能、基于相机的扩展功能、基于通讯录的扩展功能、基于日历的扩展功能、基于麦克风的扩展功能，收集使用个人信息时，应当在扩展业务功能开启前，向个人信息主体注意告知所提供扩展业务功能及所必要收集的个人信息，并允许个人信息主体对扩展业务功能逐项选择同意。

b)助贷机构收集使用个人信息的告知：

1)当助贷机构出于向个人信息主体提供产品或服务的基本业务功能（产品推荐、借款申请、初步信审、资金匹配、还款管理等）的目的收集使用个人信息时，应当在基本业务功能开启前向个人信息主体告知基本业务功能所必要收集的个人信息类型，以及个人信息主体拒绝提供或拒绝同意收集将带来的影响，并通过个人信息主体对信息收集主动做出肯定性动作（如勾选、点击“同意”或“下一步”等）征得其明示同意；

2)当个人信息控制者出于向个人信息主体提供产品或服务的扩展业务功能的目的收集使用个人信息时，应当在扩展业务功能（社区论坛、邀请分享、会员积分等）开启前，向个人信息主体注意告知所提供扩展业务功能及所必要收集的个人信息，并允许个人信息主体对扩展业务功能逐项选择同意。

c)金融服务机构通过网络上提供金融服务的，应在主动收集客户信息、间接收取客户信息、客户主动提供信息、对外提供等实现业务所需信息前，告知客户收集使用个人金融信息的目的、范围及用途。

1)必要信息是指金融机构为客户提供金融服务、业务实名制所需要的最小化身份信息，如姓名、性别、国籍、证件号、联系号码；额外信息是指金融机构为履行反洗钱和反恐融资义务所需除个人实名制信息之外的信息，包括但不限于职业、婚姻状况、家庭状况、住所、工作单位、照片、收入、动产及不动产、纳税公积金、账户状况、信用状况等含身份、财产、账户、信用、交易信息。

2)存款、保险及投资理财属于金融机构基本职能，虽然基于反洗钱要求应对客户进行尽职调查，但不能以反洗钱为由无限扩大客户信息的获取范围及获取种类，针对可通过交叉验证或已经通过有效实名认证的网络客户，由于具体交易场景和目的相一致，可经客户同意直接获取或经客

安证合规集团&北源律师事务所

户授权同意间接获取必要的客户姓名、性别、证件号码后向客户提供金融服务；但因合理怀疑客户从事洗钱或恐怖融资等犯罪活动相关时，需收集其他信息的应逐项、清晰告知客户，并获得客户的明确同意。

G.1.2 对外提供个人信息的告知

a)金融机构向与其存在业务关系的第三方提供个人信息的，应当事先明确告知信息主体第三方的姓名或者名称，第三方收集、处理、使用个人信息的特定的用途，范围和可能产生的后果等，并取得信息主体的明示同意。

注：金融机构将收集的个人信息委托给外包服务供应商或者外部合作机构处理的，应当事先取得个人信息主体的明示同意，并充分审查、评估外包服务供应商或者外部合作机构保护个人信息的能力，将其作为选择评估的重要指标。

b)金融机构在评估个人信息保护及信息安全风险程度较低的情况下，通过协议方式委托第三方服务商对信息进行使用及处理，如计算机系统外包服务、科技外包服务商、广告服务、云服务、债务追讨、司法诉讼、法律及财务专业咨询机构、第三方SDK/API、小程序等。

1)固定类型的委托外包服务可在隐私政策或服务合同内予以列明，清晰告知客户；

2)不固定类型的委托外包服务可在具体应用场景予以说明，显著标示、提示第三方服务商名称。

注：委托第三方处理信息之前，应充分审查、评估第三方服务商保护个人金融信息的能力，通过委托处理协议约定职责和义务，对外部供应商、外部合作机构进行监督，并约定第三方服务商不得转委托。金融机构对委托机构及信息安全义务承担首要责任，不因委托而转移、减免。

G.2 告知同意的适当性

助贷业务告知同意的适当时机：可以在借款客户选择“申请借款”、“立即申请”、“立即借款”等类似表述后，并在借款申请的基本业务功能开启前，向个人信息主体告知基本业务功能所必要收集的个人信息类型，以及个人信息主体拒绝提供或拒绝同意收集将带来的影响。

注：这样操作告知的时间点和收集个人信息的时间点相差时间适当，且明确知道该客户具备借款意图后（非游客状态）向其告知较为合适，同时避免对无借款意图的客户造成不必要的打扰。

G.3 免于告知同意的情形

以下情形中，个人信息控制者共享、转让、公开披露个人信息，无需事先征得个人信息主体的授权同意：

a)提供给中国人民银行个人征信中心或经其批准设立的合法征信机构；

b)提供给中国互联网金融协会及其他合法成立的行业协会；

安证合规集团&北源律师事务所

c)基于非营利性科研目的的提供给科研机构（例如：高等院校、研究所等）；

除以上内容，互联网金融场景下个人信息告知的内容、方式、展示、适当性，同意模式与实现形式等，可遵循指南的一般规定。

附 录 G

（资料性附录）

车载场景下的告知同意

车载场景是指以车载终端作为载体，通过网络连接实现人车交互及系统服务的各种应用场景，包括信息娱乐系统、交通信息管理系统、应急救援系统等。车载场景随着网络技术、大数据算法能力、AI技术等的发展有所变化，可能会出现更多的融合模式。

H.1 告知

H.1.1告知的内容

在车载场景下，除本标准第8.1中的相关信息外，还可以包含以下内容：

a)车载系统、应用服务的内容、使用说明、性能、标准及相关服务的提供者的详细信息；

b)车辆销售商、车载系统服务商、车载应用服务商在提供服务时对于个人信息的收集及共享情况；

c)车辆所有人、驾驶员及其他个人信息主体查询各个人信息控制者隐私政策的方式和途径；

d)车辆所有人、驾驶员及其他个人信息主体查询、管理个人信息的方式和途径；

e)车辆内通过自动化设备及车载系统采集驾驶员及乘车人个人信息的，可以通过功能介绍及说明书等向个人信息主体说明采取此类措施的正当性、合法性与必要性。

H.1.2告知的方式

车载场景下选择个人信息处理有关的规则等内容的告知方式时，除本标准8.2的相关内容外，宜充分考虑车辆驾驶场景的特殊性，依据道路交通安全法律法规、国家及行业标准的相关规定，选择适当的告知方式。在进行告知及与个人信息主体交互时，不宜在行车场景下设置任何可能干扰驾驶的产品方案。

车载场景下选择的适当的告知方式，可以包括：

a)在车辆使用说明书或销售协议中对于车载系统及应用服务进行介绍，并将服务相关的个人信息控制者、个人信息处理活动及个人信息控制者就个人信息处理活动制定的基本规则或查看规则的具体路径和方式进行告知；

b)车辆生产商及车载系统服务提供商宜在系统控制层面为各个人信息控制者提供向个人信息主体告知个人信息处理活动制定的基本规则的交互界面或可行设计，个人信息控制者通过前述交

安证合规集团&北源律师事务所

互页面或可行设计向用户展示隐私政策等个人信息处理活动的规则；

c)存在车机互联或账号设定等交互的产品，可以选择将告知内容通过建立连接的移动设备进行展示；

d)提供服务时如手机人脸、指纹等个人敏感信息时，宜在交互过程中向个人信息主体明示收集信息的目的，可以采用语音提示方式引起个人信息主体的注意。

注1：如信息仅用于或存储在车载终端没有回传服务器，不属于个人信息的收集行为。

H.1.3告知的展示

车载场景下选择告知展示的形式时，宜结合车辆具体性能、车载系统的安装位置等合理设置。基于车内环境、驾驶场景等因素，可以采取如下方式：

a)提供网页、二维码等渠道方便个人信息主体在非车内及汽车启动场景下阅读；

b)提供语音、视频等方式，在保证行车安全的场景下，根据个人信息主体的选择对告知内容进行展示；

c)对于个人信息主体产生重要的或易于引起异议或争端的内容，宜在销售过程中进行功能介绍及信息收集相关说明，以便车辆购买人理解并作出判断。

H.2 同意

H.2.1同意模式的选择

车载场景下选择合适的同意模式时，除本标准9 的相关规定外，宜对车辆购买者、车辆驾驶员、乘车人的不同特点进行考虑，在可能的情况下，结合服务场景和个人信息处理活动的特性，采用不同的同意模式：

a)车载服务或服务中的个人信息处理活动可能对车辆购买者权益造成重大影响时，车辆生产商、销售商宜在销售前向车辆购买者充分、完整的介绍功能、服务及信息收集情况。同时，可在销售协议设置相关条款，车辆购买者在采购协议签署中完成明示同意；

b)向驾驶员征求同意时不宜以可能干扰驾驶的方式进行，且不宜将驾驶行为和个人信息处理活动进行绑定；

c)在个人信息主体使用语音交互、人脸识别等功能时，个人信息主体使用服务即可视为其同意个人信息控制者收集其个人信息的行为。同时，个人信息控制者宜为个人信息主体提供撤回同意或删除已收集个人信息的路径和方式，依据法律法规和相关约定或超出技术能力和合理成本的情况除外；

d)对于个人信息的收集如无法隔离不同个人信息主体时，可以采用代为授权或默示同意方式。同时，为个人信息主体提供撤回同意或删除已收集信息的路径和方式，依据法律法规和相关约定

安证合规集团&北源律师事务所

或超出技术能力和合理成本的情况除外。

附 录 H

（资料性附录）

网上购物场景下的告知同意

I.1告知的内容

a)收集用户手机号码:至少应明确说明收集信息用途。建议通过输入框背景文字等方式提示用户，引导其主动输入手机号码，避免直接从第三方处收集其手机号码。

b)收集用户与网络产品与服务之间通信内容:至少应明确说明收集信息用途。例如，在用户拨通客服电话时提示用户：“为了保证服务质量，您的本次通话可能会被录音。”

c)收集用户身份证件信息:由于其与用户人身与财产安全高度相关，应明确说明收集信息用途、安全保障措施和拒绝提供或拒绝同意将带来的影响。

d)收集用户生物识别特征信息:由于其与用户人身与财产安全高度相关，应明确说明收集信息用途、安全保障措施和拒绝提供或拒绝同意将带来的影响。同时，应当增加“关闭”此类应用的功能。

I.2 告知同意的方式

I.2.1 隐私权政策的展示

隐私权政策应当有明确的生效日期和版本信息，内容公开发布且易于访问，例如，web网站主页、移动应用程序安装页等显著位置设置链接。

a)固定位置展示

1)web网站主页页尾处应设置专门的隐私权政策链接，确保用户可以随时访问隐私权政策内容。网页中应当采用侧边栏、目录树等便于用户阅读的形式。

2)应用程序应在其APP中设置专门的隐私权政策链接，确保用户可以随时访问隐私权政策内容。推荐在APP中设置专门的“隐私”板块集中展示政策与相关控制措施。

b)历史版本展示

1)网络产品与服务的隐私权政策在变更时，应确保其历史版本也可在web网站或应用程序中的适当位置可公开访问。例如，淘宝网规则-协议专区中可查询淘宝网历史版本的隐私权政策。

I.2.2 告知同意的时机

a)注册账号时同意隐私权政策：在用户注册账号时，以弹窗等形式向用户展示隐私条款核心内容，核心内容简洁、精炼、易阅读；核心内容下方提供完整的隐私条款链接，并通过用户主动作出勾选“同意”的形式征得用户同意。

安证合规集团&北源律师事务所

1)用户在web网站注册账号，网页应弹出浮框提示用户阅读包括隐私权政策在内的协议，并引导用户点击同意。

2)用户在应用程序注册账号时，若属于综合类、复杂场景的应用程序，应用程序应弹出浮框提示用户阅读包括隐私权政策在内的协议，并引导用户点击同意。

3)用户在应用程序注册账号时，若属于垂直类、场景相对单一的应用程序，可以在注册页明确提示用户阅读包括隐私权政策在内的协议，并引导用户同意协议并注册。

b)隐私权政策重大变更的同意

1)隐私权政策发生重大变更，在网页端用户登录时应提示协议更新。

2)隐私权政策发生重大变更，在用户首次进入应用程序时应提示用户并取得同意。

c)使用其他账号登录时同意隐私权政策

1)当在本网络产品与服务的账号之外，提供使用其他网络产品与服务账号登录的功能时，应引导提示用户阅读并同意本网络产品与服务的隐私权政策。

2)当使用其他网络产品与服务的账号登录功能时，应在为用户提供信息发布功能前，要求用户绑定手机号码，确保符合法律关于实名制的要求。

d)用户首次进入应用程序时同意隐私权政策。用户首次进入应用程序时（APP新安装或者更新安装），可在用户打开APP时提示用户阅读隐私权政策，并简要说明APP收集使用信息的基本情况。

个人金融信息保护技术规范

基本信息:

【发布机关】全国人民代表大会	【时效性】-
【发文字号】JR/T 0171-2020	【效力级别】国家标准
【发布日期】2020.02.13	【实施日期】2020.02.13

个人金融信息保护技术规范

1范围

本标准规定了个人金融信息在收集、传输、存储、使用、删除、销毁等生命周期各环节的安全防护要求，从安全技术和安全管理两个方面，对个人金融信息保护提出了规范性要求。

本标准适用于提供金融产品和服务的金融业机构，并为安全评估机构开展安全检查与评估工

安汇合规集团&北源律师事务所

作提供参考。

2规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T22239—2019信息安全技术网络安全等级保护基本要求

GB/T25069—2010信息安全技术术语

GB/T31186.2—2014银行客户基本信息描述规范第2部分：名称

GB/T31186.3—2014银行客户基本信息描述规范第3部分：识别标识

GB/T35273—2017信息安全技术个人信息安全规范

JR/T0068—2020网上银行系统信息安全通用规范

JR/T0071金融行业信息系统信息安全等级保护实施指引

JR/T0092—2019移动金融客户端应用软件安全管理规范

JR/T0149—2016中国金融移动支付支付标记化技术规范

JR/T0167—2018云计算技术金融应用规范安全技术要求

3术语和定义

GB/T25069—2010、GB/T35273—2017界定的以及下列术语和定义适用于本文件。

3.1金融业机构

本标准中的金融业机构是指由国家金融管理部门监督管理的持牌金融机构,以及涉及个人金融信息处理的相关机构。

3.2个人金融信息

金融业机构通过提供金融产品和服务或者其他渠道获取、加工和保存的个人信息。

注1：本标准中的个人金融信息包括账户信息、鉴别信息、金融交易信息、个人身份信息、财产信息、借贷信息及其他反映特定个人某些情况的信息。

注2：改写GB/T35273—2017，定义3.1。

3.3支付敏感信息

支付信息中涉及支付主体隐私和身份识别的重要信息。

注：支付敏感信息包括但不限于银行卡磁道数据或芯片等效信息、卡片验证码、卡片有效期、银行卡密码、网络支付交易密码等用于支付鉴权的个人金融信息。

3.4个人金融信息主体

安证合规集团&北源律师事务所

个人金融信息所标识的自然人。

注：改写GB/T35273—2017，定义3.3。

3.5个人金融信息控制者

有权决定个人金融信息处理目的、方式等的机构。

注：改写GB/T35273—2017，定义3.4。

3.6收集

获得个人金融信息的控制权的行为。

注1：收集行为包括由个人金融信息主体主动提供、通过与个人金融信息主体交互或记录个人金融信息主体行为等自动采集行为，以及通过共享、转让、搜集公开信息等间接获取个人金融信息等行为。

注2：如金融产品或服务提供者提供工具供个人金融信息主体使用，提供者不对个人金融信息进行访问的，则不属于本标准所称的收集。例如手机银行客户端应用软件在终端获取用户指纹特征信息用于本地鉴权后，指纹特

征信息不回传至提供者，则不属于用户指纹特征信息的收集行为。

注3：改写GB/T35273—2017，定义3.5。

3.7公开披露

向社会或不特定群体发布信息的行为。

[GB/T35273—2017，定义3.10]

3.8转让

将个人金融信息控制权由一个控制者向另一个控制者转移的过程。

注：改写GB/T35273—2017，定义3.11。

3.9共享

个人金融信息控制者向其他控制者提供个人金融信息，且双方分别对个人金融信息拥有独立控制权的过程。

注：改写GB/T35273—2017，定义3.12。

3.10个人金融信息安全影响评估

针对个人金融信息处理活动，检验其合法合规程度，判断其对个人金融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金融信息主体的各项措施有效性的过程。

注：改写GB/T35273—2017，定义3.8。

3.11支付账号

安证合规集团&北源律师事务所

具有金融交易功能的银行账户、非银行支付机构支付账户及银行卡卡号。

注：改写JR/T0149—2016，定义3.1。

3.12支付标记

作为支付账号等原始交易要素的替代值，用于完成特定场景支付交易。

[JR/T0149—2016，定义3.2]

3.13磁道数据

一磁、二磁和三磁定义的必备或可选的数据元。

注：磁道数据可以在物理卡的磁条上，也可以被包含在集成电路或者其他媒介上。

[JR/T0061—2011，定义3.20]

3.14卡片验证码

对磁条信息合法性进行验证的代码。

[JR/T0061—2011，定义8.7]

3.15卡片验证码2

在邮购或电话订购等非面对面交易中对银行卡卡片合法性进行验证的代码。

[JR/T0061—2011，定义8.8]

3.16动态口令

基于时间、事件等方式动态生成的一次性口令。

[GM/Z0001—2013，定义2.15]

3.17短信动态密码

短信验证码SMScode

后台系统以手机短信形式发送到用户绑定手机上的随机数，用户通过回复该随机数进行身份认证。

[JR/T0088.1—2012，定义2.44]

3.18客户法定名称

在法律上认可的客户名称。

注1：客户法定名称一般记录在国家授权部门颁发给客户的证件上，本标准客户主要指自然人客户。

注2：改写GB/T31186.2—2014，定义3.2。

3.19证件类识别标识

由国家法定有权部门颁发，能够唯一确定客户的且具有法律效力的标识。

安证合规集团&北源律师事务所

注1：证件类识别标识是外源性数据。外源性数据意味着数据的使用者不是数据的所有者，数据在产生、变更、废止后可能不为数据的使用者所知悉。

注2：本标准的使用者因本身业务需求而产生的内部证件类标识，不应在使用者外部使用，也不具有法律效力。注3：改写GB/T31186.3—2014，定义3.2。

3.20未经授权的查看

未得到信息的所有者或有权授权人授权对信息的查看。

注1：未经授权的查看可能是善意的，也可能是恶意的；信息处理者无意泄露的未经授权的查看为信息泄露事件；

攻击者通过使相关安全措施无效的措施有意获取的未经授权的查看为信息窃取事件。

注2：非法查看是对未经授权的查看的一种不严谨但在特定的语境下并无二义性的提法。

3.21未经授权的变更

未得到信息的所有者或有权授权人授权对信息的变更。

注1：未经授权的变更典型地分为未经授权的增加（即增加全新的内容）、未经授权的更改（即修改现有的内容）或未经授权的删除（即删除原有的内容）三种情况，也可能是三种情况的组合。

注2：未经授权的变更可能是善意的，也可能是恶意的；往往表现为信息篡改事件、信息假冒事件、信息丢失事件等。

注3：非法变更是对未经授权的变更的一种不严谨但在特定的语境下并无二义性的提法。

3.22明示同意

个人金融信息主体通过书面声明或主动作出肯定性动作，对其个人金融信息进行特定处理作出明确授权的行为。

注1：肯定性动作包括个人金融信息主体主动作出声明（电子或纸质形式）、主动勾选、主动点击“同意”“注册”“发送”“拨打”、主动填写或提供等。

注2：改写GB/T35273—2017，定义3.6。

3.23匿名化

通过对个人金融信息的技术处理，使得个人金融信息主体无法被识别，且处理后的信息不能被复原的过程。

注1：个人金融信息经匿名化处理后所得的信息不属于个人金融信息。

注2：改写GB/T35273—2017，定义3.13。

3.24去标识化

安证合规集团&北京律师事务所

通过对个人金融信息的技术处理，使其在不借助额外信息的情况下，无法识别个人金融信息主体的过程。

注1：去标识化仍建立在个体基础之上，保留了个体颗粒度，采用假名、加密、加盐的哈希函数等技术手段替代对个人金融信息的标识。

注2：改写GB/T35273—2017，定义3.14。

3.25删除

在金融产品和服务所涉及的系统中去除个人金融信息的行为，使其保持不可被检索、访问的状态。注：改写GB/T35273—2017，定义3.9。

4个人金融信息概述

4.1个人金融信息内容

个人金融信息包括账户信息、鉴别信息、金融交易信息、个人身份信息、财产信息、借贷信息和其他反映特定个人金融信息主体某些情况的信息，具体如下：

a)账户信息指账户及账户相关信息，包括但不限于支付账号、银行卡磁道数据（或芯片等效信息）、银行卡有效期、证券账户、保险账户、账户开立时间、开户机构、账户余额以及基于上述信息产生的支付标记信息等。

b)鉴别信息指用于验证主体是否具有访问或使用权限的信息，包括但不限于银行卡密码、预付卡支付密码；个人金融信息主体登录密码、账户查询密码、交易密码；卡片验证码（CVN和CVN2）、动态口令、短信验证码、密码提示问题答案等。

c)金融交易信息指个人金融信息主体在交易过程中产生的各类信息，包括但不限于交易金额、支付记录、透支记录、交易日志、交易凭证；证券委托、成交、持仓信息；保单信息、理赔信息等。

d)个人身份信息指个人基本信息、个人生物识别信息等：

个人基本信息包括但不限于客户法定名称、性别、国籍、民族、职业、婚姻状况、家庭状况、收入情况、身份证和护照等证件类信息、手机号码、固定电话号码、电子邮箱、工作及家庭地址，以及在提供产品和服务过程中收集的照片、音视频等信息；

个人生物识别信息包括但不限于指纹、人脸、虹膜、耳纹、掌纹、静脉、声纹、眼纹、步态、笔迹等生物特征样本数据、特征值与模板。

e)财产信息指金融业机构在提供金融产品和服务过程中，收集或生成的个人金融信息主体财产信息，包括但不限于个人收入状况、拥有的不动产状况、拥有的车辆状况、纳税额、公积金存缴金额等。

安证合规集团&北源律师事务所

f)借贷信息指个人金融信息主体在金融业机构发生借贷业务产生的信息，包括但不限于授信、信用卡和贷款的发放及还款、担保情况等。

g)其他信息：

对原始数据进行处理、分析形成的，能够反映特定个人某些情况的信息，包括但不限于特定个人金融信息主体的消费意愿、支付习惯和其他衍生信息；

在提供金融产品与服务过程中获取、保存的其他个人信息。

4.2个人金融信息类别

根据信息遭到未经授权的查看或未经授权的变更后所产生的影响和危害，将个人金融信息按敏感程度从高到低分为C3、C2、C1三个类别。具体如下：

a)C3类别信息主要为用户鉴别信息。该类信息一旦遭到未经授权的查看或未经授权的变更，会对个人金融信息主体的信息安全与财产安全造成严重危害，包括但不限于：

银行卡磁道数据（或芯片等效信息）、卡片验证码（CVN和CVN2）、卡片有效期、银行卡密码、网络支付交易密码；

账户（包括但不限于支付账号、证券账户、保险账户）登录密码、交易密码、查询密码；

用于用户鉴别的个人生物识别信息。

b)C2类别信息主要为可识别特定个人金融信息主体身份与金融状况的个人金融信息，以及用于金融产品与服务的关键信息。该类信息一旦遭到未经授权的查看或未经授权的变更，会对个人金融信息主体的信息安全与财产安全造成一定危害，包括但不限于：

支付账号及其等效信息，如支付账号、证件类识别标识与证件信息（身份证、护照等）、手机号码。

账户（包括但不限于支付账号、证券账户、保险账户）登录的用户名。

用户鉴别辅助信息，如动态口令、短信验证码、密码提示问题答案、动态声纹密码；若用户鉴别辅助信息与账号结合使用可直接完成用户鉴别，则属于C3类别信息。

直接反映个人金融信息主体金融状况的信息，如个人财产信息（包括网络支付账号余额）、借贷信息。

用于金融产品与服务的关键信息，如交易信息（如交易指令、交易流水、证券委托、保险理赔）等。

用于履行了解你的客户（KYC）要求，以及按行业主管部门存证、保全等需要，在提供产品和服务过程中收集的个人金融信息主体照片、音视频等影像信息。

其他能够识别出特定主体的信息，如家庭地址等。

安证合规集团&北源律师事务所

c)C1类别信息主要为机构内部的信息资产，主要指供金融业机构内部使用的个人金融信息。该类信息一旦遭到未经授权的查看或未经授权的变更，可能会对个人金融信息主体的信息安全与财产安全造成一定影响，包括但不限于：

账户开立时间、开户机构；

基于账户信息产生的支付标记信息；

C2和C3类别信息中未包含的其他个人金融信息。

个人金融信息主体因业务需要（如贷款）主动提供的有关家庭成员信息（如身份证号码、手机号码、财产信息等），应依据C3、C2、C1敏感程度类别进行分类，并实施针对性的保护措施。

两种或两种以上的低敏感程度类别信息经过组合、关联和分析后可能产生高敏感程度的信息。同一信息在不同的服务场景中可能处于不同的类别，应依据服务场景以及该信息在其中的作用对信息的类别进行识别，并实施针对性的保护措施。

4.3个人金融信息生命周期

个人金融信息生命周期指对个人金融信息进行收集、传输、存储、使用、删除、销毁等处理的整个过程，各环节描述如下：

a)收集：对个人金融信息主体各类信息进行获取和记录的过程。

b)传输：个人金融信息在终端设备、信息系统内或信息系统间传递的过程。

c)存储：个人金融信息在终端设备、信息系统内保存的过程。

d)使用：对个人金融信息进行展示、共享和转让、公开披露、委托处理、加工处理等操作的过程。

e)删除：使个人金融信息不可被检索、访问的过程。

f)销毁：对个人金融信息进行清除，使其不可恢复的过程。

5安全基本原则

金融业机构应遵循GB/T35273—2017的要求，以“权责一致、目的明确、选择同意、最少够用、公开透明、确保安全、主体参与”的原则，设计并实施覆盖个人金融信息全生命周期的安全保护策略。

6安全技术要求

6.1生命周期技术要求

6.1.1收集

应根据信息类别确定个人金融信息收集方案。具体技术要求如下：

安证合规集团&北源律师事务所

a)不应委托或授权无金融业相关资质的机构收集C3、C2类别信息。

b)应确保收集信息来源的可追溯性。

c)应采取技术措施（如弹窗、明显位置URL链接等），引导个人金融信息主体查阅隐私政策，并获得其明示同意后，开展有关个人金融信息的收集活动。

d)对于C3类别信息，通过受理终端、客户端应用软件、浏览器等方式收集时，应使用加密等技术措施保证数据的保密性，防止其被未授权的第三方获取。

e)通过受理终端、客户端应用软件与浏览器等方式引导用户输入（或设置）银行卡密码、网络支付密码时，应采取展示屏蔽等措施防止密码明文显示，其他密码类信息宜采取展示屏蔽措施。

f)在网络支付业务系统中，应采取具有信息输入安全防护、即时数据加密功能的安全控件对支付敏感信息的输入进行安全保护，并采取有效措施防止合作机构获取、留存支付敏感信息。

g)在停止提供金融产品或服务时，应及时停止继续收集个人金融信息的活动。

6.1.2传输

个人金融信息传输过程的参与方应保证信息在传输过程中的保密性、完整性和可用性，具体技术要求如下:

a)应建立相应的个人金融信息传输安全策略和规程，采用满足个人金融信息传输安全策略的安全控制措施，如安全通道、数据加密等技术措施。

b)传输个人金融信息前，通信双方应通过有效技术手段进行身份鉴别和认证。

c)通过公共网络传输时，C2、C3类别信息应使用加密通道或数据加密的方式进行传输，保障个人金融信息传输过程的安全；对于C3类别中的支付敏感信息，其安全传输技术控制措施应符合有关行业技术标准与行业主管部门有关规定要求。

d)应根据个人金融信息的不同类别，采用技术手段保证个人金融信息的安全传输；低敏感程度类别的个人金融信息因参与身份鉴别等关键活动导致敏感程度上升的（如，经组合后构成交易授权完整要素的情况），应提升相应的安全传输保障手段。

e)个人金融信息传输的接收方应对接收的信息进行完整性校验。

f)应建立有效机制对个人金融信息传输安全策略进行审核、监控和优化，包括对通道安全配置、密码算法配置、密钥管理等保护措施的管理和监控。

g)应采取有效措施（如个人金融信息传输链路冗余）保证数据传输可靠性和网络传输服务可用性。

6.1.3存储

个人金融信息存储的具体技术要求如下:

安证合规集团&北源律师事务所

a)不应留存非本机构的银行卡磁道数据（或芯片等效信息）、银行卡有效期、卡片验证码（CVN和CVN2）、银行卡密码、网络支付密码等C3类别信息。若确有必要留存的，应取得个人金融信息主体及账户管理机构的授权。

b)应根据个人金融信息的不同类别，采用技术手段保证个人金融信息的存储安全；低敏感程度类别的个人金融信息因参与身份鉴别等关键活动导致敏感程度上升的（如，经组合后构成交易授权完整要素的情况），应提升相应的安全存储保障手段。

c)C3类别个人金融信息应采用加密措施确保数据存储的保密性。

d)受理终端、个人终端及客户端应用软件均不应存储银行卡磁道数据（或芯片等效信息）、银行卡有效期、卡片验证码（CVN和CVN2）、银行卡密码、网络支付密码等支付敏感信息及个人生物识别信息的样本数据、模板，仅可保存完成当前交易所必需的基本信息要素，并在完成交易后及时予以清除。

e)采取必要的技术和管控措施保证个人金融信息存储转移过程中的安全性。

f)应将去标识化、匿名化后的数据与可用于恢复识别个人的信息采取逻辑隔离的方式进行存储，确保去标识化、匿名化后的信息与个人金融信息不被混用。

g)在停止运营时，应依据国家法律法规与行业主管部门有关规定要求，对所存储的个人金融信息进行妥善处置，或移交国家与行业主管部门指定的机构继续保存。

6.1.4使用

6.1.4.1信息展示

提供业务办理与查询等功能的应用软件，对个人金融信息展示具体技术要求如下:

a)依据国家法律法规与行业主管部门有关规定要求，对通过计算机屏幕、客户端应用软件、银行卡受理设备、自助终端设备、纸面（如受理终端打印出的交易凭条等交易凭证）等界面展示的个人金融信息应采取信息屏蔽（或截词）等处理措施，降低个人金融信息在展示环节的泄露风险。

注1：关于信息屏蔽（或截词）的使用方式，参见附录A。

注2：金融业机构柜面打印的凭证依据有关规范执行。

b)处于未登录状态时，不应展示与个人金融信息主体相关的C3类别信息。

c)处于已登录状态时，个人金融信息展示的技术要求如下:

除银行卡有效期外，C3类别信息不应明文展示。

对于银行卡号、手机号码、证件类识别标识或其他识别标识信息等可以直接或组合后确定个人金融信息主体的信息应进行屏蔽展示，或由用户选择是否屏蔽展示，如需完整展示，应进行用

安证合规集团&北京律师事务所

户身份验证，并做好此类信息管理，防范此类信息泄露风险。

涉及其他个人金融信息主体的信息时，除以下情况外，宜进行屏蔽展示：

——其他方主动发起的活动包含的信息，此种情况需展示必要的信息以供活动接收方对活动内容进行确认，例如：其他方发起的交易、其他方发起的收付款、保险保费代收。

——与其他方已建立信任关系（间接授权），此时需活动发起方确认发起活动的必要信息的正确性（或活动发起方需接收活动结果信息，并确认活动已正确完成），例如：向其他方收款，其他方已付款；向其他方申请代付，其他方同意付款或者其他方在自己业务应用范围内的联系人。

——其他法律法规要求的情况。

应用软件的后台管理与业务支撑系统，对个人金融信息展示具体技术要求如下：

a)除银行卡有效期外，C3类别信息不应明文展示。

b)应采取技术措施防范个人金融信息在展示过程中泄露或被未经授权的拷贝。

c)后台系统对支付账号、客户法定名称、支付预留手机号码、证件类或其他类识别标识信息等展示宜进行屏蔽处理，如需完整展示，应做好此类信息管理，采取有效措施防范未经授权的拷贝。

d)后台系统不应具备开放式查询能力，应严格限制批量查询。

e)对于确有明文查看需要的业务场景可以保留明文查看权限，后台系统应对所有查询操作进行细粒度的授权与行为审计。

应防止通过散列碰撞等方法推导出完整的数据，若使用“截词”的方式进行部分字段的屏蔽处理，不应用散列代替字段被截词的部分。

6.1.4.2共享和转让

个人金融信息在共享和转让的过程中，应充分重视信息转移或交换过程中的安全风险，具体技术要求如下：

a)在共享和转让前，应开展个人金融信息安全影响评估，并依据评估结果采取有效措施保护个人金融信息主体权益。

b)在共享和转让前，应开展个人金融信息接收方信息安全保障能力评估，并与其签署数据保护责任承诺。

c)支付账号及其等效信息在共享和转让时，除法律法规和行业主管部门另有规定外，应使用支付标记化（按照JR/T0149—2016）技术进行脱敏处理（因业务需要无法使用支付标记化技术时，应进行加密），防范信息泄露风险。

d)应部署信息防泄露监控工具，监控及报告个人金融信息的违规外发行为。

e)应部署流量监控技术措施，对共享、转让的信息进行监控和审计。

f)应根据“业务需要”和“最小权限”原则，对个人金融信息的导出操作进行细粒度的访问控制与全过程审计，应采取两种或两种以上鉴别技术对导出信息操作人员进行身份鉴别。

g)应定期检查或评估信息导出通道的安全性和可靠性。

h)使用外部嵌入或接入的自动化工具（如代码、脚本、接口、算法模型、软件开发工具包等）进行信息共享与转让时，应定期检查或评估信息共享工具、服务组件和共享通道的安全性和可靠性，并留存检查或评估结果记录。

i)应执行严格的审核程序，并准确记录和保存个人金融信息共享和转让情况。记录内容应包括但不限于日期、规模、目的、范围，以及数据接收方基本情况与使用意图等，并应确保对共享和转让的信息及其过程可被追溯。

j)应采取有效技术防护措施，防范信息转移过程中被除信息发送方与接收方之外的其他个人、组织和机构截获和利用。

6.1.4.3公开披露

个人金融信息原则上不得公开披露。金融业机构经法律授权或具备合理事由确需公开披露时，具体技术要求如下:

a)应事先开展个人金融信息安全影响评估，并依据评估结果采取有效的保护个人金融信息主体权益的措施。

b)不应公开披露个人生物识别信息。

c)应准确记录和保存个人金融信息的公开披露情况，包括公开披露的日期、规模、目的、内容、公开范围等。

6.1.4.4委托处理

金融业机构因金融产品或服务的需要，将收集的个人金融信息委托给第三方机构（包含外包服务机构与外部合作机构）处理时，具体技术要求如下:

a)委托行为不应超出已征得个人金融信息主体授权同意的范围或遵循7.1中对于征得授权同意的例外所规定的情形，并准确记录和保存委托处理个人金融信息的情况。

b)C3以及C2类别信息中的用户鉴别辅助信息，不应委托给第三方机构进行处理。转接清算、登记结算等情况，应依据国家有关法律法规及行业主管部门有关规定与技术标准执行。

c)对委托处理的信息应采用去标识化（不应仅使用加密技术）等方式进行脱敏处理，降低个人金融信息被泄露、误用、滥用的风险。

d)应对委托行为进行个人金融信息安全影响评估，并确保受委托者具备足够的数据安全能力，

安证合规集团&北源律师事务所

且提供了足够的安全保护措施。

e)应对第三方机构等受委托者进行监督，方式包括但不限于：

依据7.2.1的要求，通过合同等方式规定受委托者的责任和义务；

依据7.4.2的要求，对受委托者进行安全检查和评估。

f)应对外部嵌入或接入的自动化工具（如代码、脚本、接口、算法模型、软件开发工具包等）开展技术检测，确保其个人金融信息收集、使用行为符合约定要求；并对其收集个人金融信息的行为进行审计，发现超出约定行为及时切断接入。

6.1.4.5加工处理

个人金融信息在加工处理的过程中，具体技术要求如下：

a)应采取必要的技术手段和管理措施，确保在个人金融信息清洗和转换过程中对信息进行保护，对C2、C3类别信息，应采取更加严格的保护措施。

b)应对匿名化或去标识化处理的数据集或其他数据集汇聚后重新识别出个人金融信息主体的风险进行识别和评价，并对数据集采取相应的保护措施。

c)应建立个人金融信息防泄露控制规范和机制，防止个人金融信息处理过程中的调试信息、日志记录等因不受控制的输出而泄露受保护的信息。

d)应具备信息化技术手段或机制，对个人金融信息滥用行为进行有效的识别、监控和预警。

e)应具备完整的个人金融信息加工处理操作记录和管理能力，记录内容包括但不限于日期、时间、主体、事件描述、事件结果等。

6.1.4.6汇聚融合

个人金融信息汇聚融合的技术要求如下：

a)汇聚融合的数据不应超出收集时所声明的使用范围。因业务需要确需超范围使用的，应再次征得个人金融信息主体明示同意。

b)应根据汇聚融合后的个人金融信息类别及使用目的，开展个人金融信息安全影响评估，并采取有效的技术保护措施。

6.1.4.7开发测试

个人金融信息在开发测试过程中的具体技术要求如下：

a)应对开发测试环境与生产环境进行有效隔离。

b)开发环境、测试环境不应使用真实的个人金融信息，应使用虚构的或经过去标识化（不应仅使用加密技术）脱敏处理的个人金融信息，账号、卡号、协议号、支付指令等测试确需信息除外。

安证合规集团&北源律师事务所

6.1.5删除

个人金融信息在删除过程中的具体技术要求如下:

a)应采取技术手段，在金融产品和服务所涉及的系统中去除个人金融信息，使其保持不可被检索和访问。

b)个人金融信息主体要求删除个人金融信息时，金融业机构应依据国家法律法规、行业主管部门有关规定以及与个人金融信息主体的约定予以响应。

6.1.6销毁

个人金融信息在销毁过程中的具体技术要求如下:

a)应建立个人金融信息销毁策略和管理制度，明确销毁对象、流程、方式和要求。

b)应对个人金融信息存储介质销毁过程进行监督与控制，对待销毁介质的登记、审批、介质交接、销毁执行等过程进行监督。

c)销毁过程应保留有关记录，记录至少应包括销毁内容、销毁方式与时间、销毁人签字、监督人签字等内容。

d)存储个人金融信息的介质如不再使用，应采用不可恢复的方式（如消磁、焚烧、粉碎等）对介质进行销毁处理；存储个人金融信息的介质如还需继续使用，不应只采用删除索引、删除文件系统的方式进行信息销毁，应通过多次覆写等方式安全地擦除个人金融信息，确保介质中的个人金融信息不可再被恢复或者以其他形式加以利用。

e)云环境下有关数据清除应依据JR/T0167—2018的9.6执行。

6.2安全运行技术要求

6.2.1网络安全要求

承载与处理个人金融信息的信息系统应符合国家网络安全相关规定与GB/T22239—2019、JR/T0071的要求。存储个人金融信息的数据库应处于金融业机构可控网络内，并进行有效的访问控制。

6.2.2Web应用安全要求

涉及C2、C3类别信息的Web应用的安全技术要求如下:

a)应具备对网站页面篡改、网站页面源代码暴露、穷举登录尝试、重放攻击、SQL注入、跨站脚本攻击、钓鱼、木马以及任意文件上传、下载等已知漏洞的防范能力。

b)处理个人金融信息相关的Web应用系统与组件上线前应进行安全评估。

c)应具备对处理个人金融信息的系统组件进行实时监测的能力，有效识别和阻止来自内外部的非法访问。

安证合规集团&北源律师事务所

6.2.3客户端应用软件安全要求

与个人金融信息相关的客户端应用软件及应用软件开发工具包（SDK）应符合JR/T0092—2019、JR/T0068—2020客户端应用软件有关安全技术要求，并在上线前进行安全评估。

6.2.4密码技术与密码产品要求

使用的密码技术及产品应符合国家密码管理部门与行业主管部门要求。

7安全管理要求

7.1安全准则

7.1.1收集

个人金融信息收集的方式包括但不限于通过柜面、信息系统、金融自助设备、受理终端、客户端应用软件等渠道获取。金融业机构应遵循合法、正当、必要的原则，向个人金融信息主体明示收集与使用个人金融信息的目的、方式、范围和规则等，获得个人金融信息主体的授权同意，并满足以下要求：

a)收集个人金融信息的基本规则如下：

不应欺诈、诱骗，或以默认授权、功能捆绑等方式误导强迫个人金融信息主体提供个人金融信息；

不应隐瞒金融产品或服务所具有的收集个人金融信息的功能；

不应通过非法渠道间接获取个人金融信息；

不应收集法律法规与行业主管部门有关规定明令禁止收集的个人金融信息。

b)收集个人金融信息应遵循最小化要求，收集个人金融信息的目的应与实现和优化金融产品或服务、防范金融产品或服务的风险有直接关联。直接关联是指无该个人金融信息参与无法实现前述目的。

c)收集个人金融信息时授权同意的具体要求如下：

收集个人金融信息前，应向个人金融信息主体明确告知金融产品或服务需收集的个人金融信息类别，以及收集、使用个人金融信息的规则（如：收集和使用个人金融信息的目的、收集方式、自身的数据安全能力、对外共享、转让、公开披露的规则、投诉与申诉的渠道及响应时限等），并获得个人金融信息主体的明示同意。

间接获取个人金融信息时，应要求个人金融信息提供方说明个人金融信息来源，并对其个人金融信息来源的合法性进行确认；应了解个人金融信息提供方已获得的授权内容，包括使用目的，个人金融信息主体是否授权同意转让、共享、公开披露等情况；因业务需要金融业机构确需超出

安证合规集团&北源律师事务所

原授权范围处理个人金融的，应在使用个人金融信息前，征得个人金融信息主体的明示同意。

d)以下情形收集使用个人金融信息无需征得个人金融信息主体的授权同意：

与履行国家法律法规及行业主管部门有关规定的义务相关的；

与国家安全、国防安全直接相关的；

与公共安全、公共卫生、重大公共利益直接相关的；

与犯罪侦查、起诉、审判和判决执行等直接相关的；

出于维护个人金融信息主体或其他主体的生命、财产等重大合法权益但又很难得到本人同意的；

个人金融信息主体自行向社会公众公开的；

根据个人金融信息主体要求签订和履行合同所必需的；

从合法公开披露的信息中收集个人金融信息的，如合法的新闻报道、政府信息公开等渠道；

用于维护所提供的金融产品或服务的安全稳定运行所必需的，例如识别、处置金融产品或服务中的欺诈或被盗用等。

7.1.2存储

个人金融信息的存储时限应满足国家法律法规与行业主管部门有关规定要求，并符合个人金融信息主体授权使用的目的所必需的最短时间要求。超过该期限后，应对收集的个人金融信息进行删除或匿名化处理。

7.1.3使用

个人金融信息在信息展示、共享与转让、公开披露、委托处理、加工处理、汇聚融合等方面，应遵循6.1.4.1—6.1.4.6的要求，并满足以下要求：

a)除法律法规与行业主管部门另有规定或开展金融业务所必需的数据共享与转让（如转接清算等）外，金融业机构原则上不应共享、转让其收集的个人金融信息，确需共享、转让的，应充分重视信息安全风险，具体要求如下：

应向个人金融信息主体告知共享、转让个人金融信息的目的、数据接收方的类型，并事先征得个人金融信息主体明示同意，共享、转让经去标识化处理（不应仅使用加密技术）的个人金融信息，且确保数据接收方无法重新识别个人金融信息主体的除外。

应帮助个人金融信息主体了解数据接收方对个人金融信息的存储、使用等情况，包括个人金融信息主体的权利，例如访问、更正、删除、注销账户等；在法律法规规定、行业主管部门有关规定及个人金融信息主体约定的范围内，个人金融信息主体行使其个人金融信息控制权利，金融业机构应配合响应其请求。

安证合规集团&北源律师事务所

C3类别信息以及C2类别信息中的用户鉴别辅助信息不应共享、转让。

转接清算、登记结算等情况，应依据国家有关法律法规与行业主管部门有关规定与技术标准执行。

当因收购、兼并、重组、破产等情况，对个人金融信息主体提供金融产品或服务的金融业机构主体变更而发生个人金融信息共享、转让时，具体要求如下：

——金融业机构将其提供的金融产品或服务移交至其他金融业机构的情况，应使用逐一传达（或公告）的方式通知个人金融信息主体。

——承接其金融产品或服务的金融业机构，应对其承接运营的金融产品或服务继续履行个人金融信息保护责任；如变更其在收购、兼并重组过程中获取的个人金融信息使用目的，应重新获得个人金融信息主体明示同意（或授权）。

b)金融业机构原则上不应公开披露其收集的个人金融信息，经法律授权或具备合理理由确需公开披露个人金融信息的，具体要求如下：

应向个人金融信息主体告知公开披露个人金融信息的目的、类别，并事先征得个人金融信息主体的同意，并向其告知涉及的信息内容；

承担因公开披露个人金融信息对个人金融信息主体合法权益造成损害的相应责任；

C3类别信息，以及C2类别信息中的用户鉴别辅助信息不应公开披露。

c)因金融产品或服务的需要，将收集的个人金融信息委托给第三方机构（包含外包服务机构与外部合作机构）处理的，具体要求如下：

依据6.1.4.4开展委托处理工作。

应对第三方机构等受委托者提出如下要求：

——应严格按照金融业机构的要求处理个人金融信息，如因特殊原因受委托者未能按照要求处理个人金融信息，应及时告知金融业机构，并配合金融业机构进行信息安全评估，并采取补救措施以保护个人金融信息的安全，必要时应终止其对个人金融信息的处理；

——未经书面授权，受委托者不应将其处理的个人金融信息再次委托给其他机构进行处理；

——应协助响应个人金融信息主体的请求；

——如受委托者在处理个人金融信息过程中无法提供足够的信息安全保护水平或发生安全事件，应及时告知金融业机构，配合进行信息安全评估与安全事件调查，并采取补救措施以保护个人金融信息的安全，必要时应终止其对个人金融信息的处理；

——在委托关系解除时（或外包服务终止后），受委托者应按照金融业机构的要求销毁其处理的个人金融信息，并依据双方协商的期限承担后续的个人金融信息保密责任；

安证合规集团&北源律师事务所

——应准确记录和保存委托处理个人金融信息的情况。

d)在中华人民共和国境内提供金融产品或服务过程中收集和产生的个人金融信息，应在境内存储、处理和分析。因业务需要，确需向境外机构（含总公司、母公司或分公司、子公司及其他为完成该业务所必需的关联机构）提供个人金融信息的，具体要求如下：

应符合国家法律法规及行业主管部门有关规定；

应获得个人金融信息主体明示同意；

应依据国家、行业有关部门制定的办法与标准开展个人金融信息出境安全评估，确保境外机构数据安全保护能力达到国家、行业有关部门与金融业机构的安全要求；

应与境外机构通过签订协议、现场核查等方式，明确并监督境外机构有效履行个人金融信息保密、数据删除、案件协查等职责义务。

e)以下情形中，金融业机构共享、转让、公开披露个人金融信息无需征得个人金融信息主体的授权同意：

与履行法律法规及行业主管部门规定的义务相关的；

与国家安全、国防安全直接相关的；

与公共安全、公共卫生、重大公共利益直接相关的；

与犯罪侦查、起诉、审判和判决执行等直接相关的；

出于维护个人金融信息主体或其他主体的生命、财产等重大合法权益但又很难得到本人同意的；

个人金融信息主体自行向社会公众公开的；

从合法公开披露的信息中收集个人金融信息的，如合法的新闻报道、政府信息公开等渠道。

7.2安全策略

7.2.1安全制度体系建立与发布

金融业机构应建立个人金融信息保护制度体系，明确工作职责，规范工作流程。制度体系的管理范畴应涵盖本机构、外包服务机构与外部合作机构，并确保相关制度发布并传达给本机构员工及外部合作方。相关制度应至少包括个人金融信息保护管理规定、日常管理及操作流程、外包服务机构与外部合作机构管理、内外部检查及监督机制、应急处理流程和预案。具体要求如下：

a)制定个人金融信息保护管理规定，提出本机构个人金融信息保护工作方针、目标和原则。

b)开展个人金融信息分类分级管理。应针对不同类别和敏感程度的个人金融信息，实施相应的安全策略和保障措施。

c)建立日常管理及操作流程。应对个人金融信息的收集、传输、存储、使用、删除、销毁等

安证合规集团&北源律师事务所

环节提出具体保护要求，制定个人金融信息时效性管理规程，确保符合法律法规和行业主管部门有关规定。

d)建立信息系统分级授权管理机制。应在不影响履行反洗钱等法定义务的前提下，制定本机构人员个人金融信息调取权限与使用范围，并制定专门的授权审批流程。

e)建立个人金融信息脱敏（如屏蔽、去标识、匿名化等）管理规范和制度，应明确不同敏感级别个人金融信息脱敏规则、脱敏方法和脱敏数据的使用限制。

f)依据国家与行业有关标准，建立个人金融信息安全影响评估制度，应定期（至少每年一次）开展个人金融信息安全影响评估。

g)建立外包服务机构与外部合作机构管理制度，包括但不限于：

应对个人金融信息生命周期过程中相关的外包服务机构与外部合作机构进行审查与评估，评估其个人金融信息的保护能力是否达到国家、行业主管部门与金融业机构的要求；应通过协议或合同的方式，约束外包服务机构与外部合作机构不应留存C2、C3类别信息；对于C2类别信息中的支付账号等信息，若因清分清算、差错处理等业务需要确需留存，金融业机构应明确其保密义务与保密责任，并应根据安全要求落实安全控制措施，并将有关资料留档备查；对可能访问个人金融信息的外包服务机构、外部合作机构及其人员，金融业机构应要求外包服务机构与外部合作机构向有关人员传达个人金融信息保护安全要求，与其签署保密协议，并对协议履行情况进行监督。

不应将存储个人金融信息的数据库交由外部合作机构运维。

应定期对外包服务机构与外部合作机构的个人金融信息保护措施落实情况进行确认，确认的方式包括但不限于外部信息安全评估、现场检查等。

国家法律法规与行业主管部门另有规定的，按照相关要求执行。

h)建立个人金融信息安全检查及监督机制。应建立个人金融信息安全日常检查机制和工作流程、定期评估个人金融信息管理方面存在的不足，及时调整检查机制和工作流程。

i)应将个人金融信息泄露等相关事件处理纳入机构信息安全事件应急处置工作机制，制定专门的流程和预案。定期评估应急处理流程和预案，及时保障、有效应对个人金融信息安全事件，降低安全事件造成的损失及不利影响。

j)建立个人金融信息投诉与申诉处理程序，明确投诉与申诉受理部门、处理程序，对个人金融信息主体要求更正或删除金融业机构收集其个人金融信息的情况，应受理、核实，并依据国家与行业主管部门要求予以处理。

k)明确个人金融信息共享、存储、使用和销毁的期限，具备个人金融信息存储时效性的控制

安证合规集团&北京律师事务所

能力。

7.2.2组织架构岗位设置

组织架构及岗位设置具体要求如下:

a)应建立个人金融信息保护组织架构，明确机构各层级内设部门与相关岗位个人金融信息保护职责与总体要求。

b)应明确个人金融信息保护责任人和个人金融信息保护责任机构，并履行以下工作职责:

负责制定和管理本机构个人金融信息安全管理制度;

制定、实施、定期更新隐私政策和相关规程;

监督本机构内部，以及本机构与外部合作方个人金融信息安全管理;

开展信息安全管理内部审计、分析处理信息安全相关事件;

组织开展个人金融信息安全影响评估，提出个人金融信息保护的对策建议;

组织在金融产品或服务上线发布前进行技术检测，避免未知（与金融产品或服务功能及隐私政策不符）的个人金融信息收集、使用、共享等处理行为;

公布投诉与申诉方式等信息并及时受理个人金融信息有关的投诉、申诉。

c)应明确在提供金融产品和服务的过程中知悉个人金融信息的岗位，并针对相关岗位明确其个人金融信息安全管理责任与保密责任，如不得未经授权的复制、存储、使用个人金融信息，不得向他人出售或者以其他形式未经授权的共享、转让、披露个人金融信息等。

7.2.3人员管理

对涉及个人金融信息相关人员的安全管理，具体要求如下:

a)录用员工前，应进行必要的背景调查，并与所有可访问个人金融信息的员工签署保密协议，或在劳动合同中设置保密条款。

b)应定期开展内外部个人金融信息保护培训与意识教育活动，并保留相关记录。

c)在发生人员调离岗位时，应立即调整和完成相关人员的个人金融信息访问、使用等权限的配置，并明确有关人员后续的个人金融信息保护管理权限和保密责任；若有关人员调整后的岗位不涉及个人金融信息的访问与处理的，应明确其继续履行有关信息的保密义务要求。

d)与员工终止劳动合同时，应立即终止并收回其对个人金融信息的访问权限，并明确其继续履行有关信息的保密义务要求。

e)系统开发人员、系统测试人员与运维人员之间不应相互兼岗。

f)应定期（至少每年一次）或在隐私政策发生重大变化时，对个人金融信息处理岗位上的相关人员开展个人金融信息安全专业化培训和考核，确保相关人员熟练掌握隐私政策和相关规程。

安证合规集团&北京律师事务所

7.3访问控制

加强个人金融信息访问控制管理，具体要求如下：

a)应根据“业务需要”和“最小权限”原则，进行个人金融信息相关的权限管理，严格控制和分配访问、使用个人金融信息的权限。

b)对于可访问和处理个人金融信息的系统应设置基于角色的访问控制策略，禁止账户共用。

c)传输、处理、存储个人金融信息的系统默认用户权限应为“拒绝所有访问”。

d)对个人金融信息使用的权限管理应设置权限指派、回收、过期处理等安全功能。

e)对存储或处理个人金融信息的系统或设备进行远程访问时，应通过专线、VPN等方式访问，个人金融信息不应在远程访问设备上留存。

f)应对生产网络、开发测试网络、办公网络以及相关非生产网络进行访问控制。

g)应对个人金融信息访问与个人金融信息的增删改查等操作进行记录，并保证操作日志的完整性、可用性及可追溯性，操作日志包括但不限于业务操作日志、系统日志等；系统运维管理类日志不应记录个人金融信息。

h)应对存储个人金融信息的数据库及操作日志实施严格的用户授权与访问控制。

i)存储或处理个人金融信息的相关物理设备或介质应在获得审批授权后方可移入或移出机房受控区域，留存有C2、C3类别信息的物理设备或介质移入或移出区域应具有同等的安全保障措施。

7.4安全监测与风险评估

7.4.1监控与审计

监控与审计具体要求如下：

a)应识别并记录包括但不限于管理员用户、业务用户对个人金融信息的访问。

b)应对个人金融信息数据交换网络流量进行安全监控和分析，并存储匹配安全规则的数据，以备事件溯源。

c)日志文件和匹配规则的数据应至少保存6个月，应定期对所有系统组件日志进行审计，包括但不限于存储、处理或传输个人金融信息的系统组件日志、执行安全功能的系统组件日志（如防火墙、入侵检测系统、验证服务器等）、安全事件日志等。

d)应采取技术手段对个人金融信息全生命周期进行安全风险识别和管控，如恶意代码检测、异常流量监测、用户行为分析等。

7.4.2安全检查和评估

金融业机构应对个人金融信息生命周期全过程进行安全检查和评估，范围包括金融业机构以及与其合作的第三方机构（包含外包服务机构与外部合作机构）。

安证合规集团&北源律师事务所

个人金融信息的安全检查和评估具体要求如下：

a)应依据制定的个人金融信息安全影响评估制度，在个人金融信息委托处理、共享与转让、公开披露等过程中，执行个人金融信息安全影响评估活动，并将评估报告归档保存。个人金融信息安全影响评估可由金融业机构自行组织开展，也可委托外部安全评估机构执行。

b)应每年至少开展一次对涉及收集、存储、传输、使用个人金融信息的信息系统进行安全检查或安全评估，包括但不限于以下方式及其组合：

对信息系统进行信息安全评估、漏洞扫描和渗透测试，并及时采取补救措施；

在信息系统组件或运行环境发生重大变更（或发现新的高安全等级威胁和漏洞）时，重新进行信息安全风险评估；

将个人金融信息保护纳入金融业机构内部安全审计工作，定期开展安全审计，形成审计报告，并根据审计结果完善制度、流程。

c)对于个人金融信息中的支付信息部分，应采取自行评估或委托外部机构进行检查评估，金融业机构以及与其合作的第三方机构应每年至少开展一次支付信息安全合规评估，对评估过程中发现的问题及时采取补救措施并形成报告存档备查。

d)出现个人金融信息泄露事件，造成一定经济损失（或社会影响）时，应及时委托外部安全评估机构重新进行相关安全评估与检查活动，并将结果报送行业主管部门。

7.5安全事件处置

安全事件处置具体要求如下：

a)应制定个人金融信息安全事件应急预案，明确安全事件处置流程和岗位职责。

b)应定期组织内部相关人员进行个人金融信息保护应急预案相关培训和应急演练。

c)发生个人金融信息遗失、损毁、泄露或被篡改等安全事件后，应及时采取必要措施进行处置，控制事态发展，消除安全隐患，并及时告知受影响的个人金融信息主体，告知的内容应符合GB/T35273—2017关于安全事件告知内容的规定，告知的方式包括但不限于：

以邮件、信函、电话、推送消息等方式及时告知受影响的个人金融信息主体；

难以逐一告知个人金融信息主体时，应采取合理、有效的方式发布与公众有关的警示信息。

d)发现因系统漏洞或人为原因造成个人金融信息泄露时，应立即采取有效措施防止风险扩大，并向行业主管部门报告。

e)应记录事件内容，分析和鉴定事件产生的原因，评估事件可能造成的影响，制定补救措施，并按国家与行业主管部门规定及时进行报告。

f)应建立投诉与申诉管理机制，包括跟踪流程，并在规定的时间内，对投诉、申诉进行响应。

安证合规集团&北源律师事务所

g)根据相关法律法规与行业主管部门有关规定的变化情况以及事件处置情况，及时评估并更新应急预案。

移动互联网应用程序（App）收集使用个人信息自评估指南

基本信息：	
【发布机关】信安标委	【时效性】 现行有效
【发文字号】信安秘字[2020]40号	【效力级别】指引性文件
【发布日期】2020.07	【实施日期】-

移动互联网应用程序（App）收集使用个人信息自评估指南

评估点一：是否公开收集使用个人信息的规则

1.1 是否公开隐私政策等收集使用规则

a) 隐私政策通过弹窗、文本链接、附件、常见问题（FAQs）等界面或形式展示。

b) 隐私政策中包含收集使用个人信息规则的相关内容。

c) 隐私政策文本链接有效，文本可正常显示。

d) 如存在涉及收集使用儿童个人信息相关业务功能的，需制定针对儿童的个人信息保护规则。

注1：详见2019年国家互联网信息办公室令（第4号）《儿童个人信息网络保护规定》。

注2：例如收集不满十四周岁的未成年人个人信息的教育类App，需制定针对儿童的个人信息保护规则。

1.2 是否提示用户阅读隐私政策等收集使用规则

a)在App首次运行或用户注册时主动提示用户阅读隐私政策。

注：例如可采用通过弹窗、突出链接等主动方式提示用户阅读隐私政策。

b)避免使用不明显的方式展示隐私政策链接，导致用户不易发现隐私政策。

注：例如采用与背景颜色相近的字体、刻意缩小字号、弹出键盘遮挡、置于边缘等为不明显方式展示隐私政策链接。

1.3 隐私政策等收集使用规则是否易于访问

a)用户进入主功能界面后，通过4次（含）以内的点击等操作，能够访问到隐私政策。

b)尽可能在界面的固定路径展示隐私政策（或其链接），以便用户随时访问和获取，避免仅

安证合规集团&北源律师事务所

在注册/登录界面展示隐私政策链接，或只能以咨询客服等方式查找隐私政策等情形。

注1：例如通过“我--设置--关于”或者“我的--设置--隐私”等用户熟悉路径展示隐私政策，不频繁变更展示隐私政策的路径。

注2：在首次展示隐私政策时，宜说明查找隐私政策的方法、路径。

c) 隐私政策以单独成文的形式发布，而不是作为用户协议、用户须知等文件中的一部分存在。

注：如果因展示条件等特殊原因使用用户协议、用户须知等文件描述个人信息收集使用规则，则尽可能显著标识并以连续篇幅呈现。

1.4 隐私政策等收集使用规则是否易于阅读

a) 隐私政策文本文字显示方式不会造成阅读困难。

注1：例如可采取与App其他界面等同的样式。

注2：例如文本字号过小、颜色与背景色相近、行间距过密、字迹模糊、列宽大于手机屏幕等易造成阅读困难。

b) 提供简体中文版隐私政策。

c) 隐私政策内容使用标准化的数字、图示，采用通用的语言习惯，避免误用概念、术语或存在有歧义的语句等。

1.5 公开的收集使用规则是否完整

a) 对App运营者基本情况进行描述，至少包括组织名称、注册地址或常用办公地址、个人信息保护工作机构或相关负责人联系方式。

b) 说明隐私政策的发布、生效或更新日期。

c) 说明收集使用个人信息的目的、方式、范围。

注：详见本《实践指南》2.1节。

d) 对个人信息存放地域（境内、境外哪个国家或地区）、存储期限（法律规定范围内最短期限或明确的期限）、超期处理方式进行说明。

e) 如果将个人信息用于用户画像、个性化展示等，说明其应用场景和可能对用户权益产生的影响。

注：如部分业务功能不涉及用户画像、个性化展示，可在规则中明确说明。

f) 如果存在个人信息出境情形，说明出境个人信息类型并显著标识。

注：例如可采用字体加粗、标星号、下划线、斜体、不同颜色等显著标识方式。

g) 对个人信息保护方面采取的措施和具备的能力进行说明。

h) 如果存在个人信息对外共享、转让、公开披露的情况，说明以下内容：①对外共享、转

安证合规集团&北源律师事务所

让、公开披露个人信息的目的；②涉及的个人信息类型；③接收方类型或身份。

i) 对以下用户权利和相关操作方法进行说明：①个人信息查询；②个人信息更正；③个人信息删除；④用户账号注销；⑤撤回已同意的授权。

j) 至少说明以下一种投诉、举报渠道：①电子邮件；②电话；③在线客服；④在线表单；⑤即时通信账号。

注：本节相关定义和内容可参考GB/T 35273-2020《信息安全技术 个人信息安全规范》5.5节。

评估点二：是否明示收集使用个人信息的目的、方式和范围

2.1 是否逐一列出收集使用个人信息的目的、方式、范围等

a) 完整、清晰、区分说明各业务功能所收集的个人信息。宜根据用户使用习惯逐项说明各业务功能收集个人信息的目的、类型、方式，避免使用“等、例如”等方式不完整列举。

注：业务功能通常是指App为面向用户的具体使用需求所提供的一类完整的服务类型，如地图导航、网络约车、即时通信、网络支付、新闻资讯、网上购物、短视频、快递物流、餐饮外卖、交通票务、婚恋相亲、房屋租售、求职招聘、网络借贷等。

b) 使用Cookie等同类技术（包括脚本、Clickstream、Web 信标、Flash Cookie、内嵌 Web 链接等）收集个人信息时，简要说明相关机制，以及收集个人信息的目的、类型。

c) 如嵌入的第三方代码、插件（如SDK）收集个人信息，说明第三方代码、插件的类型或名称，及收集个人信息的目的、类型、方式。

注：例如可采用隐私政策、弹窗提示、文字备注、文本链接等方式说明。

2.2 收集使用个人信息的目的、方式、范围发生变化时是否通知用户

a) 收集使用个人信息的目的、方式和范围发生变化时，以适当方式通知用户。

注：例如可采用更新隐私政策等收集使用规则并以推送消息、邮件、弹窗、红点提示等方式提醒用户阅读发生变化的条款。

2.3 是否同步告知申请打开权限和要求提供个人敏感信息的目的

a) 在申请打开可收集个人信息权限时，通过显著方式同步告知用户其目的，对目的的描述明确、易懂。

注1：常见可收集个人信息权限类型有：

iOS系统:定位、通讯录、日历、提醒事项、照片、麦克风、相机、健康等；

Android系统:日历、通话记录、相机、通讯录、位置、麦克风、电话、传感器、短信、存储等。

注2：例如可采用弹窗提示、用途描述等显著方式告知。

安证合规集团&北源律师事务所

b) 在要求用户提供个人敏感信息时，通过显著方式同步告知用户其目的，对目的的描述明确、易懂。

注1：个人敏感信息定义见GB/T 35273-2020《信息安全技术 个人信息安全规范》3.2节。

注2：例如可采用弹窗提示、用途描述等显著方式告知。

2.4 收集使用规则是否易于理解

a) 有关收集使用规则的内容需简练、结构清晰、重点突出。

注：例如使用晦涩难懂的词语、冗长繁琐的篇幅、大量专业术语、逻辑结构混乱等易造成用户难以理解。

评估点三：是否征得用户同意后才收集使用个人信息

3.1 收集个人信息或打开可收集个人信息权限前是否征得用户同意

a) 收集个人信息前提供可由用户自主作出同意或不同意的选项。

注：例如提供“退出”“上一步”“关闭”“取消”的按钮等方式供用户作出不同意的选项。

b) 未征得用户同意前，不收集个人信息或打开可收集个人信息权限。

注1：例如用户首次使用App时，在未得知收集个人信息的目的并作出同意前，App就开始收集个人信息的行为属于未征得用户同意收集个人信息。

注2：相关定义和内容可参考GB/T 35273-2020《信息安全技术 个人信息安全规范》5.4节。

c) 未征得用户同意前，不利用Cookie等同类技术或通过调用可收集用户个人信息的权限、接口等方式收集个人信息。

3.2 用户明确表示不同意收集后是否仍收集个人信息

a) 用户通过拒绝提供个人信息、不同意收集使用规则、拒绝提供或关闭权限等操作，明确表示不同意收集某类个人信息后，不以任何形式收集该类个人信息或打开该类可收集个人信息权限。

3.3 用户明确表示不同意收集后是否频繁征求用户同意、干扰用户正常使用

a) 用户明确表示不同意收集后，不在每次重新打开App、或使用某一业务功能时，向用户频繁询问（如48小时内询问超过一次）是否同意收集该类个人信息。

b) 用户明确表示不同意打开某类可收集个人信息权限后，不在每次重新打开App、或使用某一业务功能时，向用户频繁询问（如48小时内询问超过一次）是否同意打开该类可收集个人信息权限。

注：为支持App正常运行，或用户主动选择使用的某一具体功能触发征得同意的动作，不属于频繁干扰情形。例如用户拒绝授权“相机”权限后的48小时内，主动选择使用拍摄、扫码等功能时，App再次申请打开该权限的情形不属于频繁干扰。

安恒合规集团&北源律师事务所

3.4 实际收集的个人信息是否超出用户授权范围

a) 收集使用个人信息的过程需与其所声明的隐私政策等收集使用规则保持一致。实际收集的个人信息类型、申请打开可收集使用个人信息的权限等与隐私政策等收集使用规则中相关内容一致，不超出隐私政策等收集使用规则所述范围。

3.5 是否以默认选择同意隐私政策等非明示方式征求用户同意

a) 在首次运行、用户注册等时，可通过弹窗、突出链接等明示方式提醒用户阅读隐私政策后征求用户同意，不采用默认勾选隐私政策等非明示方式。

b) 通过设置“下一步”“注册”“登录即代表同意”等方式征求用户同意的情形，除以显著方式展示隐私政策等收集使用规则外，还需明确执行上述动作与同意隐私政策之间的逻辑关系，以达到主动提醒用户主动阅读隐私政策后征求用户同意的效果。

注：隐私政策等收集使用规则未发生变化时无需反复征求用户同意。如App更新后，隐私政策无变化时，无需再次征求用户同意隐私政策。

3.6 是否未经用户同意更改其设置的可收集个人信息权限状态

a) 未经用户同意，不私自更改用户设置的可收集个人信息权限和收集使用个人信息相关功能的状态。

注：例如未经用户同意，在更新升级后，将用户设置的可收集个人信息权限恢复到默认状态，或将用户已关闭的使用通讯录匹配好友等功能重新打开。

3.7 存在定向推送信息情形的是否提供非定向推送信息的选项

a) 存在利用用户个人信息和算法定向推送信息情形时（包括利用个人信息和个性化推荐算法等推送新闻和信息、展示商品、推送广告等），需为用户提供拒绝接收定向推送信息，或停止、退出、关闭相应功能的机制，或不基于个人信息和个性化推荐算法等推送的模式、选项。

注：相关定义和内容可参考GB/T 35273-2020《信息安全技术 个人信息安全规范》7.5节。

3.8 是否以不正当方式误导用户同意收集个人信息

a) 明示收集使用个人信息的目的需真实、准确。不故意欺瞒、掩饰收集使用个人信息的真实目的，不诱骗用户同意收集个人信息或打开可收集个人信息权限。

注：例如App提示用户打开通讯录权限以参与红包、金币、抽奖等活动。事实上，通讯录权限与上述活动之间毫无关联，App诱骗用户打开通讯录权限后，立即上传用户通讯录信息，并将该类信息用于发送商业广告或其它目的。

3.9 是否向用户提供撤回同意收集个人信息的途径、方式

a) 向用户提供撤回同意收集个人信息的途径、方式，并在隐私政策等收集使用规则中予以明

安证合规集团&北清律师事务所

确。

b) 如用户拒绝或撤回特定业务功能收集个人信息的同意时，除非用户拒绝或撤回的个人信息是其他业务功能所必需，否则不暂停其他业务功能，或降低其他业务功能的服务质量。

c) 如用户拒绝或关闭可收集个人信息权限时，不影响用户正常使用与该权限无关的业务功能，除非该权限是保证App正常运行所必需。

注1：相关定义和内容可参考GB/T 35273-2020《信息安全技术 个人信息安全规范》8.4节。

注2：如用户需要撤回对同意App收集使用其所有个人信息的授权，可采取注销账号等方式执行。

3.10 是否违反其所声明的收集使用规则

a) 开展个人信息处理活动需严格遵循所公开的隐私政策等收集使用规则，并遵守与用户的约定；如个人信息使用目的、方式、范围等发生变化的，需再次征得用户同意。

评估点四：是否遵循必要原则，仅收集与其提供的服务相关的个人信息

4.1 是否收集与业务功能无关的个人信息

a) 不收集与业务功能无关的个人信息。

b) 不申请打开与业务功能无关的可收集个人信息权限。

4.2 用户是否可拒绝收集非必要信息或打开非必要权限

a) 收集与业务功能相关但非必要的个人信息或申请打开相关但非必要的可收集个人信息权限时，需由用户自主选择同意，如用户不同意，不影响其使用现有业务功能或相关服务。

b) 不将同意收集其他业务功能所需的个人信息或同意打开其他业务功能所需的可收集个人信息权限，作为用户使用当前业务功能的前提条件。

c) 如提供无需注册即可使用的服务模式（如仅浏览、游客模式），当用户拒绝同意该类服务模式以外的个人信息收集行为时，不影响其使用仅浏览等功能。

注1：必要信息指与业务功能直接相关的个人信息，缺少该个人信息则无法提供最基本的服务。必要信息范围可参考《信息安全技术 移动互联网应用程序（App）收集个人信息基本规范》，如果服务类型不在该标准内，则可根据其业务特点，参考该标准相关定义和理念自行分析。

注2：相关内容和实践案例可参考GB/T 35273-2020《信息安全技术 个人信息安全规范》5.3节及其附录C。

4.3 是否以非正当方式强迫收集用户个人信息

a) 根据用户主动填写、点击、勾选等自主行为，作为各个业务功能收集使用个人信息的前提条件。

安证合规集团&北源律师事务所

b) 新增业务功能申请收集的个人信息超出用户原有同意范围时，不因用户拒绝新增业务功能收集个人信息的请求，拒绝提供原有业务功能，新增业务功能取代原有业务功能的除外。

c) 不仅以改善服务质量、提升使用体验、研发新产品、定向推送信息、增强安全性等为由，强制要求个人信息主体同意收集个人信息。

d) 不以捆绑方式强制要求用户一次性同意打开多个可收集个人信息权限。

注：例如将安卓版App的targetSdkVersion值设置低于23，通过声明机制，在安装App时要求用户一次性同意打开多个可收集个人信息权限属于捆绑方式。

4.4 收集个人信息的频度是否超出业务功能实际需要

a) 收集个人信息的频度不超出业务功能实际需要，在用户使用某业务功能过程中，仅收集与当前业务功能相关的个人信息。

b) 在App未打开或处于后台运行状态时，不收集用户个人信息，除非业务功能需要后台运行时继续提供服务，如导航功能等。

注：在用户主动关闭App后，未经用户同意不采用自启动、关联启动方式收集个人信息。

c) 接入第三方应用时，不私自截留第三方应用收集的个人信息。

注：例如信息查询类App，在用户向第三方应用提交相关个人信息时，截留用户个人信息并上传至其后端服务器的行为属于私自截留个人信息。

评估点五：是否经用户同意后才向他人提供个人信息

5.1 向他人提供个人信息前是否征得用户同意

a) 如存在从客户端直接向第三方发送个人信息的情形，包括通过客户端嵌入第三方代码、插件（如SDK）等方式向第三方发送个人信息的情形，需事先征得用户同意，经匿名化处理的除外。

b) 如个人信息传输至服务器后，App运营者向第三方提供其收集的个人信息，需事先征得用户同意，经匿名化处理的除外。

c) 如向第三方传输的个人信息类型、接收数据的第三方身份等发生变更的，需以适当方式通知用户，并征得用户同意。

注：“匿名化”的定义可参考GB/T 35273-2020《信息安全技术 个人信息安全规范》3.14节。

5.2 向接入的第三方应用提供个人信息前是否经用户同意

a) 如App接入第三方应用，当用户使用第三方应用时，需在征得用户同意后，再向第三方应用提供个人信息；当用户获知应用为第三方提供后，自行以主动填写等方式向第三方直接授权的除外。

b) App运营者宜对于接入的第三方应用收集个人信息的合法、正当、必要性等方面进行审核，

明确标识相关业务功能为第三方提供，并提醒用户关注第三方应用收集使用个人信息的规则。

注：第三方接入管理相关内容可参考GB/T 35273-2020《信息安全技术 个人信息安全规范》9.7节。

评估点六：是否提供删除或更正个人信息功能，或公布投诉、举报方式等信息

6.1 是否提供有效的注销用户账号功能

a) 提供有效的注销账号途径，并在用户注销账号后，及时删除其个人信息或进行匿名化处理。

注：例如可提供在线操作、客服电话、电子邮件等注销账号的途径。

b) 受理注销账号请求后，在承诺时限内（承诺时限不得超过15个工作日，无承诺时限的，以15个工作日为限）完成核查和处理。

c) 注销账号的过程简单易操作，不设置不必要或不合理的注销条件。

注：不必要或不合理的注销条件相关内容可参考GB/T 35273-2020《信息安全技术 个人信息安全规范》8.5节。

6.2 是否提供有效的更正或删除个人信息途径

a) 提供有效的查询、更正、删除个人信息的途径。

注：隐私政策中注明的，经证实无法完成相关操作的，视为无效途径。

b) 无法通过在线操作方式及时响应个人信息查询、更正、删除请求的，在承诺时限内（承诺时限不超过15个工作日，无承诺时限的，以15个工作日为限）完成核查和处理。

c) 查询、更正和删除个人信息的过程简单易操作，不设置不必要或不合理的条件。

d) 用户更正、删除个人信息等操作完成时，后台需及时执行完成相关操作。

6.3 是否建立并公布个人信息安全投诉、举报渠道

a) 建立并公布可受理个人信息安全问题相关的投诉、举报渠道。

注：例如可采取电子邮件、电话、在线客服、在线表单、即时通讯账号等受理方式。

b) 妥善受理用户关于个人信息相关的投诉、举报，并在承诺时限内（承诺时限不超过15个工作日，无承诺时限的，以15个工作日为限）受理并处理。

安证合规集团&北源律师事务所