



上海市秀文路898号西子国际中心2号楼3层 邮编：201199

上海市华山路1389弄14号 邮编：200030

电话 (Tel) : 86-21-33883626 传真 (Fax) : 86-21-34127367 网址 (Website) : www.guolinglaw.com

数据安全法律法规汇编

国瓴律师事务所知识产权与数据合规团队

二〇二一年十二月

目 录

一、现行法律.....	1
(一) 中华人民共和国数据安全法.....	1
(二) 中华人民共和国个人信息保护法.....	10
(三) 中华人民共和国网络安全法.....	26
(四) 中华人民共和国电子商务法.....	41
(五) 中华人民共和国密码法.....	57
(六) 中华人民共和国测绘法.....	65
(六) 2021 年全国人民代表大会常务委员会工作报告.....	79
(七) 全国人民代表大会常务委员会关于加强网络信息保护的決定.....	95
(八) 中华人民共和国国民经济和社会发展第十四个五年规划纲要和 2035 年远景目标纲要.....	97
二、行政法规.....	200
(一) 中华人民共和国政府信息公开条例.....	200
(二) 国务院关于进一步推进全国一体化在线政务服务平台建设的指导意见.....	210
(三) 国务院办公厅关于促进和规范健康医疗大数据应用发展的指导意见.....	229
(四) 国务院关于印发促进大数据发展行动纲要的通知.....	236
(五) 国务院关于印发政务信息资源共享管理暂行办法的通知.....	253
(六) 国务院办公厅关于印发进一步深化“互联网+政务服务”推进政务服务“一网、一门、一次”改革实施方案的通知.....	260
(七) 国务院办公厅关于印发科学数据管理办法的通知.....	267
(八) 国务院办公厅关于印发国家政务信息化项目建设管理办法的通知.....	273
(九) 关键信息基础设施安全保护条例.....	281
三、司法解释.....	290
(一) 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.....	290
(二) 最高人民法院关于审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的解释.....	294
(三) 最高人民法院关于人民法院在线办理案件若干问题的规定 (征求意见稿)	298
(四) 最高人民法院、最高人民检察院关于办理非法利用信息网络、帮助信息网络犯罪活动等刑事案件适用法律若干问题的解释.....	308
(五) 最高人民检察院关于印发《检察机关办理侵犯公民个人信息案件指引》的通知.....	315
(六) 最高人民法院、最高人民检察院、公安部关于依法惩处侵害公民个人信息犯罪活动的通知.....	326
(七) 最高人民法院关于审理网络消费纠纷案件适用法律若干问题的规定 (一) (征求意见稿)	329
(八) 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.....	335
四、 部门及部委规章.....	340
(一) 数据安全管理办法 (征求意见稿)	340
(二) 网络数据安全管理办法 (征求意见稿)	347
(三) 儿童个人信息网络保护规定.....	370
(四) 邮政业寄递安全监督管理办法.....	375
(五) 网络安全标准实践指南——移动互联网应用程序(App)个人信息安全防范指引(征求意见稿).....	382
(六) 网络安全标准实践指南——移动互联网应用程序 (App)收集使用个人信息自评估指南.....	507
(七) 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.....	520
(八) 电信和互联网用户个人信息保护规定.....	528
(九) 信息安全技术 个人信息告知同意指南 (征求意见稿)	533
(十) 国家互联网信息办公室关于《网络安全审查办法》 (修订草案征求意见	

稿)》公开征求意见的通知.....	583
(十一) 汽车数据安全若干规定.....	588
(十二) 工业和信息化领域数据安全管理办法(试行)(征求意见稿)	593
(十三) 网络交易监督管理方法(征求意见稿)	607
五、 部门规范性文件.....	625
(一) 交通运输部关于印发《交通运输政务数据共享管理办法》的通知.....	625
(二) 互联网个人信息安全保护指南.....	631
(三) 人口健康信息管理办法(试行)	650
(四) 国家健康医疗大数据标准、安全和服务管理办法(试行)	654
(五) 国家网络空间安全战略.....	661
(六) 国土资源部关于印发促进国土资源大数据应用发展实施意见的通知.....	670
(七) 信息安全技术大数据交易服务安全要求(征求意见稿)	685
(八) 国家知识产权局办公室关于印发加快推进“互联网+政务服务” 工作方案的 通知.....	697
(九) 关于印发《国家知识产权局政府信息公开实施办法(修订)》等文件的 通知.....	711
(十) 人力资源社会保障部办公厅关于加快推进流动人员人事档案信息化建设的 指导意见.....	724
(十一) 国家税务总局关于印发《全面推进政务公开工作实施办法》的通知.....	729
(十二) 教育部办公厅关于印发《教育部机关及直属事业单位教育数据管理办 法》的通知.....	740
(十三) 信息安全技术 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)	748
(十四) 常见类型移动互联网应用程序必要个人信息范围规定.....	758
(十五) 互联网个人信息安全保护指南.....	767
(十六) 信息安全技术 数据出境安全评估指南.....	786
(十七) 车联网(智能网联汽车)网络安全标准体系建设指南(征求意见稿)	842
(十八) 网络数据安全标准体系建设指南(征求意见稿)	854

(十九) APP 违法违规收集使用个人信息自评估指南.....	875
(二十) 中央网信办关于印发《国家网络安全事件应急预案》的通知.....	880
(二十一) 国家互联网信息办公室关于《个人信息和重要数据出境安全评估办法（征求意见稿）》公开征求意见的通知.....	893
(二十二) 工业和信息化部办公厅关于印发《电信和互联网行业提升网络数据安全保护能力专项行动方案》的通知.....	896
(二十三) 交通运输部办公厅关于印发《网络预约出租汽车监督信息交互平台运行管理办法》的通知.....	902
(二十四) 工业和信息化部关于加强车联网网络安全和数据安全工作的通知.....	908
(二十五) 信息安全技术 汽车采集数据的安全要求.....	913
(二十六) 信息安全技术 网络预约汽车服务数据安全指南.....	918
(二十七) 国家地名和区划数据库管理办法（试行）.....	945
(二十八) 交通运输部办公厅关于推进交通运输行业数据资源开放共享的实施意见.....	951
(二十九) 信息安全技术 个人信息安全规范.....	956
(三十) 信息安全技术 大数据安全管理指南.....	1035
(三十一) 个人金融信息保护技术规范.....	1066
(三十二) 公开征求对《工业和信息化领域数据安全风险信息报送与共享工作指引（试行）（征求意见稿）》的意见.....	1102
(三十三) 中国银保监会关于印发监管数据安全管理办法（试行）的通知.....	1114
六、 行业规范.....	1120
(一) 应用商店 App 个人信息收集使用上架审核和管理规范（征求意见稿）	1120
(二) 移动智能端个人信息保护指南（征求意见稿）	1126

一、现行法律

(一) 中华人民共和国数据安全法

(2021年6月10日第十三届全国人民代表大会常务委员会第二十九次会议通过)

目 录

第一章 总 则

第二章 数据安全与发展

第三章 数据安全制度

第四章 数据安全保护义务

第五章 政务数据安全和开放

第六章 法律责任

第七章 附 则

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。

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。

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 政务数据的安全与开放

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。

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。

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，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。

(二) 中华人民共和国个人信息保护法

(2021年8月20日第十三届全国人民代表大会常务委员会第三十次会议通过)

目 录

第一章 总 则

第二章 个人信息处理规则

第一节 一般规定

第二节 敏感个人信息的处理规则

第三节 国家机关处理个人信息的特别规定

第三章 个人信息跨境提供的规则

第四章 个人在个人信息处理活动中的权利

第五章 个人信息处理者的义务

第六章 履行个人信息保护职责的部门

第七章 法律责任

第八章 附 则

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：

- 1、以向境内自然人提供产品或者服务为目的；
- 2、分析、评估境内自然人的行为；
- 3、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。

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：

- 1、取得个人的同意；
- 2、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；
- 3、为履行法定职责或者法定义务所必需；
- 4、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；
- 5、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；
- 6、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；
- 7、法律、行政法规规定的其他情形。

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：

- 1、个人信息处理者的名称或者姓名和联系方式；
- 2、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；
- 3、个人行使本法规定权利的方式和程序；
- 4、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。

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：

- 1、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；

2、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；

3、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；

4、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：

- 1、处理目的已实现、无法实现或者为实现处理目的不再必要；
- 2、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；
- 3、个人撤回同意；
- 4、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；
- 5、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：

- 1、制定内部管理制度和操作规程；
- 2、对个人信息实行分类管理；
- 3、采取相应的加密、去标识化等安全技术措施；
- 4、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；
- 5、制定并组织实施个人信息安全事件应急预案；
- 6、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。

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：

- 1、处理敏感个人信息；
- 2、利用个人信息进行自动化决策；
- 3、委托处理个人信息、向其他个人信息处理者提供个人信息、公开个人信息；
- 4、向境外提供个人信息；
- 5、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：

- 1、个人信息的处理目的、处理方式等是否合法、正当、必要；
- 2、对个人权益的影响及安全风险；
- 3、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：

- 1、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；

- 2、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；
- 3、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：

- 1、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；
- 2、遵循公开、公平、公正的原则，制定平台规则，明确平台内产品或者服务提供者处理个人信息的规范和保护个人信息的义务；
- 3、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；
- 4、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：

1、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；

2、接受、处理与个人信息保护有关的投诉、举报；

3、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；

4、调查、处理违法个人信息处理活动；

5、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：

1、制定个人信息保护具体规则、标准；

2、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；

3、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；

4、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；

5、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：

1、询问有关当事人，调查与个人信息处理活动有关的情况；

2、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；

3、实施现场检查，对涉嫌违法的个人信息处理活动进行调查；

4、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：

1、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。

2、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。

3、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。

4、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。

(三) 中华人民共和国网络安全法

(2016年11月7日第十二届全国人民代表大会常务委员会第二十四次会议通过)

目录

第一章 总 则

第二章 网络安全支持与促进

第三章 网络运行安全

第一节 一般规定

第二节 关键信息基础设施的运行安全

第四章 网络信息安全

第五章 监测预警与应急处置

第六章 法律责任

第七章 附 则

第一章 总 则

第一条 为了保障网络安全，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权益，促进经济社会信息化健康发展，制定本法。

第二条 在中华人民共和国境内建设、运营、维护和使用网络，以及网络安全的监督管理，适用本法。

第三条 国家坚持网络安全与信息化发展并重，遵循积极利用、科学发展、依法管理、确保安全的方针，推进网络基础设施建设和互联互通，鼓励网络技术创新和应用，支持培养网络安全人才，建立健全网络安全保障体系，提高网络安全保护能力。

第四条 国家制定并不断完善网络安全战略，明确保障网络安全的基本要求和主要目标，提出重点领域的网络安全政策、工作任务和措施。

第五条 国家采取措施，监测、防御、处置来源于中华人民共和国境内外的网络安全风险和威胁，保护关键信息基础设施免受攻击、侵入、干扰和破坏，依法惩治网络违法犯罪活动，维护网络空间安全和秩序。

第六条 国家倡导诚实守信、健康文明的网络行为，推动传播社会主义核心价值观，采取措施提高全社会的网络安全意识和水平，形成全社会共同参与促进网络安全的良好环境。

第七条 国家积极开展网络空间治理、网络技术研发和标准制定、打击网络违法犯罪等方面的国际交流与合作，推动构建和平、安全、开放、合作的网络空间，建立多边、民主、透明的网络治理体系。

第八条 国家网信部门负责统筹协调网络安全工作和相关监督管理工作。国务院电信主管部门、公安部门和其他有关机关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网络安全保护和监督管理工作。

县级以上地方人民政府有关部门的网络安全保护和监督管理职责，按照国家有关规定确定。

第九条 网络运营者开展经营和服务活动，必须遵守法律、行政法规，尊重社会公德，遵守商业道德，诚实信用，履行网络安全保护义务，接受政府和社会的监督，承担社会责任。

第十条 建设、运营网络或者通过网络提供服务，应当依照法律、行政法规的规定和国家标准的强制性要求，采取技术措施和其他必要措施，保障网络安全、稳定运行，有效应对网络安全事件，防范网络违法犯罪活动，维护网络数据的完整性、保密性和可用性。

第十一条 网络相关行业组织按照章程，加强行业自律，制定网络安全行为规范，指导会员加强网络安全保护，提高网络安全保护水平，促进行业健康发展。

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。

第十三条 国家支持研究开发有利于未成年人健康成长的网络产品和服务，依法惩治利用网络从事危害未成年人身心健康的活动，为未成年人提供安全、健康的网络环境。

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。

第二章 网络安全支持与促进

第十五条 国家建立和完善网络安全标准体系。国务院标准化行政主管部门和国务院其他有关部门根据各自的职责，组织制定并适时修订有关网络安全管理以及网络产品、服务和运行安全的国家标准、行业标准。

国家支持企业、研究机构、高等学校、网络相关行业组织参与网络安全国家标准、行业标准的制定。

第十六条 国务院和省、自治区、直辖市人民政府应当统筹规划，加大投入，扶持重点网络安全技术产业和项目，支持网络安全技术的研究开发和应用，推广安全可信的网络产品和服务，保护网络技术知识产权，支持企业、研究机构和高等学校等参与国家网络安全技术创新项目。

第十七条 国家推进网络安全社会化服务体系建设，鼓励有关企业、机构开展网络安全认证、检测和风险评估等安全服务。

第十八条 国家鼓励开发网络数据安全保护和利用技术，促进公共数据资源开放，推动技术创新和经济社会发展。

国家支持创新网络安全管理方式，运用网络新技术，提升网络安全保护水平。

第十九条 各级人民政府及其有关部门应当组织开展经常性的网络安全宣传教育，并指导、督促有关单位做好网络安全宣传教育工作。

大众传播媒介应当有针对性地面向社会进行网络安全宣传教育。

第二十条 国家支持企业和高等学校、职业学校等教育培训机构开展网络安全相关教育与培训，采取多种方式培养网络安全人才，促进网络安全人才交流。

第三章 网络运行安全

第一节 一般规定

第二十一条 国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：

- 1、制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安

全保护责任；

2、采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施；

3、采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；

4、采取数据分类、重要数据备份和加密等措施；

5、法律、行政法规规定的其他义务。

第二十二条 网络产品、服务应当符合相关国家标准的强制性要求。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。

第二十三条 网络关键设备和网络安全专用产品应当按照相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求后，方可销售或者提供。国家网信部门会同国务院有关部门制定、公布网络关键设备和网络安全专用产品目录，并推动安全认证和安全检测结果互认，避免重复认证、检测。

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。

第二十五条 网络运营者应当制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险；在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告。

第二十六条 开展网络安全认证、检测、风险评估等活动，向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息，应当遵守国家有关规定。

第二十七条 任何个人和组织不得从事非法侵入他人网络、干扰他人网络正常功能、窃取网络数据等危害网络安全的活动；不得提供专门用于从事侵入网络、干扰网络正常功能及防护措施、窃取网络数据等危害网络安全活动的程序、工具；明知他人从事危害网络安全的活动的，不得为其提供技术支持、广告推广、支付结算等帮助。

第二十八条 网络运营者应当为公安机关、国家安全机关依法维护国家安全和侦查犯罪的活动提供技术支持和协助。

第二十九条 国家支持网络运营者之间在网络安全信息收集、分析、通报和应急处置等方面进行合作，提高网络运营者的安全保障能力。

有关行业组织建立健全本行业的网络安全保护规范和协作机制，加强对网络安全风险的分析评估，定期向会员进行风险警示，支持、协助会员应对网络安全风险。

第三十条 网信部门和有关部门在履行网络安全保护职责中获取的信息，只能用于维护网络安全的需要，不得用于其他用途。

第二节 关键信息基础设施的运行安全

第三十一条 国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。关键信息基础设施的具体范围和安全保护办法由国务院制定。

国家鼓励关键信息基础设施以外的网络运营者自愿参与关键信息基础设施保护体系。

第三十二条 按照国务院规定的职责分工，负责关键信息基础设施安全保护工作的部门分别编制并组织实施本行业、本领域的关键信息基础设施安全规划，指导和监督关键信息基础设施运行安全保护工作。

第三十三条 建设关键信息基础设施应当确保其具有支持业务稳定、持续运行的性能，并保证安全技术措施同步规划、同步建设、同步使用。

第三十四条 除本法第二十一条的规定外，关键信息基础设施的运营者还应当履行下列安全保护义务：

- 1、设置专门安全管理机构和安全管理负责人，并对该负责人和关键岗位的人员进行安全背景审查；
- 2、定期对从业人员进行网络安全教育、技术培训和技能考核；
- 3、对重要系统和数据库进行容灾备份；
- 4、制定网络安全事件应急预案，并定期进行演练；
- 5、法律、行政法规规定的其他义务。

第三十五条 关键信息基础设施的运营者采购网络产品和服务，可能影响国家安全的，应当通过国家网信部门会同国务院有关部门组织的国家安全审查。

第三十六条 关键信息基础设施的运营者采购网络产品和服务，应当按照规定与提供者签订安全保密协议，明确安全和保密义务与责任。

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。

第三十八条 关键信息基础设施的运营者应当自行或者委托网络安全服务机构对其网络的安全性和可能存在的风险每年至少进行一次检测评估，并将检测

评估情况和改进措施报送相关负责关键信息基础设施安全保护工作的部门。

第三十九条 国家网信部门应当统筹协调有关部门对关键信息基础设施的安全保护采取下列措施:

- 1、对关键信息基础设施的安全风险进行抽查检测,提出改进措施,必要时可以委托网络安全服务机构对网络存在的安全风险进行检测评估;
- 2、定期组织关键信息基础设施的运营者进行网络安全应急演练,提高应对网络安全事件的水平和协同配合能力;
- 3、促进有关部门、关键信息基础设施的运营者以及有关研究机构、网络安全服务机构等之间的网络安全信息共享;
- 4、对网络安全事件的应急处置与网络功能的恢复等,提供技术支持和协助。

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。

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。

第四十六条 任何个人和组织应当对其使用网络的行为负责，不得设立用于实施诈骗，传授犯罪方法，制作或者销售违禁物品、管制物品等违法犯罪活动的网站、通讯群组，不得利用网络发布涉及实施诈骗，制作或者销售违禁物品、管制物品以及其他违法犯罪活动的信息。

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。

第五章 监测预警与应急处置

第五十一条 国家建立网络安全监测预警和信息通报制度。国家网信部门应当统筹协调有关部门加强网络安全信息收集、分析和通报工作，按照规定统一发布网络安全监测预警信息。

第五十二条 负责关键信息基础设施安全保护工作的部门，应当建立健全本行业、本领域的网络安全监测预警和信息通报制度，并按照规定报送网络安全监测预警信息。

第五十三条 国家网信部门协调有关部门建立健全网络安全风险评估和应急工作机制，制定网络安全事件应急预案，并定期组织演练。

负责关键信息基础设施安全保护工作的部门应当制定本行业、本领域的网络安全事件应急预案，并定期组织演练。

网络安全事件应急预案应当按照事件发生后的危害程度、影响范围等因素对网络安全事件进行分级，并规定相应的应急处置措施。

第五十四条 网络安全事件发生的风险增大时，省级以上人民政府有关部门应当按照规定的权限和程序，并根据网络安全风险的特点和可能造成的危害，采取下列措施：

- 1、要求有关部门、机构和人员及时收集、报告有关信息，加强对网络安全风险的监测；
- 2、组织有关部门、机构和专业人员，对网络安全风险信息进行分析评估，预测事件发生的可能性、影响范围和危害程度；
- 3、向社会发布网络安全风险预警，发布避免、减轻危害的措施。

第五十五条 发生网络安全事件，应当立即启动网络安全事件应急预案，对

网络安全事件进行调查和评估，要求网络运营者采取技术措施和其他必要措施，消除安全隐患，防止危害扩大，并及时向社会发布与公众有关的警示信息。

第五十六条 省级以上人民政府有关部门在履行网络安全监督管理职责中，发现网络存在较大安全风险或者发生安全事件的，可以按照规定的权限和程序对该网络的运营者的法定代表人或者主要负责人进行约谈。网络运营者应当按照要求采取措施，进行整改，消除隐患。

第五十七条 因网络安全事件，发生突发事件或者生产安全事故的，应当依照《中华人民共和国突发事件应对法》、《中华人民共和国安全生产法》等有关法律、行政法规的规定处置。

第五十八条 因维护国家和社会公共秩序，处置重大突发社会安全事件的需要，经国务院决定或者批准，可以在特定区域对网络通信采取限制等临时措施。

第六章 法律责任

第五十九条 网络运营者不履行本法第二十一条、第二十五条规定的网络安全保护义务的，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，处一万元以上十万元以下罚款，对直接负责的主管人员处五千元以上五万元以下罚款。

关键信息基础设施的运营者不履行本法第三十三条、第三十四条、第三十六条、第三十八条规定的网络安全保护义务的，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，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。

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：

- 1、设置恶意程序的；

2、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；

3、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，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。

第六十二条 违反本法第二十六条规定，开展网络安全认证、检测、风险评估等活动，或者向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息的，由有关主管部门责令改正，给予警告；拒不改正或者情节严重的，处一万元以上十万元以下罚款，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五千元以上五万元以下罚款。

第六十三条 违反本法第二十七条规定，从事危害网络安全的活动，或者提供专门用于从事危害网络安全活动的程序、工具，或者为他人从事危害网络安全的活动提供技术支持、广告推广、支付结算等帮助，尚不构成犯罪的，由公安机关没收违法所得，处五日以下拘留，可以并处五万元以上五十万元以下罚款；情节较重的，处五日以上十五日以下拘留，可以并处十万元以上一百万元以下罚款。

单位有前款行为的，由公安机关没收违法所得，处十万元以上一百万元以下罚款，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。

违反本法第二十七条规定，受到治安管理处罚的人员，五年内不得从事网络管理和网络运营关键岗位的工作；受到刑事处罚的人员，终身不得从事网络管理和网络运营关键岗位的工作。

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。

第六十五条 关键信息基础设施的运营者违反本法第三十五条规定，使用未经安全审查或者安全审查未通过的网络产品或者服务的，由有关主管部门责令停止使用，处采购金额一倍以上十倍以下罚款；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。

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。

第六十七条 违反本法第四十六条规定，设立用于实施违法犯罪活动的网站、通讯群组，或者利用网络发布涉及实施违法犯罪活动的信息，尚不构成犯罪的，由公安机关处五日以下拘留，可以并处一万元以上十万元以下罚款；情节严重的，处五日以上十五日以下拘留，可以并处五万元以上五十万元以下罚款。关闭用于实施违法犯罪活动的网站、通讯群组。

单位有前款行为的，由公安机关处十万元以上五十万元以下罚款，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。

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：

- 1、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；
- 2、拒绝、阻碍有关部门依法实施的监督检查的；
- 3、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。

第七十二条 国家机关政务网络的运营者不履行本法规定的网络安全保护义务的，由其上级机关或者有关机关责令改正；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。

第七十三条 网信部门和有关部门违反本法第三十条规定，将在履行网络安全保护职责中获取的信息用于其他用途的，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。

网信部门和有关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。

第七十五条 境外的机构、组织、个人从事攻击、侵入、干扰、破坏等危害中华人民共和国的关键信息基础设施的活动，造成严重后果的，依法追究法律责任；国务院公安部门和有关部门并可以决定对该机构、组织、个人采取冻结财产或者其他必要的制裁措施。

第七章 附 则

第七十六条 本法下列用语的含义：

1、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。

2、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。

3、网络运营者，是指网络的所有者、管理者和网络服务提供者。

4、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。

5、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。

第七十七条 存储、处理涉及国家秘密信息的网络的运行安全保护，除应当遵守本法外，还应当遵守保密法律、行政法规的规定。

第七十八条 军事网络的安全保护，由中央军事委员会另行规定。

第七十九条 本法自2017年6月1日起施行。

(四) 中华人民共和国电子商务法

(2018年8月31日第十三届全国人民代表大会常务委员会第五次会议通过)

目录

第一章 总 则

第二章 电子商务经营者

第一节 一般规定

第二节 电子商务平台经营者

第三章 电子商务合同的订立与履行

第四章 电子商务争议解决

第五章 电子商务促进

第六章 法律责任

第七章 附 则

第一章 总 则

第一条 为了保障电子商务各方主体的合法权益，规范电子商务行为，维护市场秩序，促进电子商务持续健康发展，制定本法。

第二条 中华人民共和国境内的电子商务活动，适用本法。

本法所称电子商务，是指通过互联网等信息网络销售商品或者提供服务的经营活动。

法律、行政法规对销售商品或者提供服务有规定的，适用其规定。金融类产品和服务，利用信息网络提供新闻信息、音视频节目、出版以及文化产品等内容方面的服务，不适用本法。

第三条 国家鼓励发展电子商务新业态，创新商业模式，促进电子商务技术研发和推广应用，推进电子商务诚信体系建设，营造有利于电子商务创新发展的市场环境，充分发挥电子商务在推动高质量发展、满足人民日益增长的美好生活需要、构建开放型经济方面的重要作用。

第四条 国家平等对待线上线下商务活动，促进线上线下融合发展，各级人民政府和有关部门不得采取歧视性的政策措施，不得滥用行政权力排除、限制市场竞争。

第五条 电子商务经营者从事经营活动，应当遵循自愿、平等、公平、诚信的原则，遵守法律和商业道德，公平参与市场竞争，履行消费者权益保护、环境保护、知识产权保护、网络安全与个人信息保护等方面的义务，承担产品和服务质量责任，接受政府和社会的监督。

第六条 国务院有关部门按照职责分工负责电子商务发展促进、监督管理等工作。县级以上地方各级人民政府可以根据本行政区域的实际情况，确定本行政区域内电子商务的部门职责划分。

第七条 国家建立符合电子商务特点的协同管理体系，推动形成有关部门、电子商务行业组织、电子商务经营者、消费者等共同参与的电子商务市场治理体系。

第八条 电子商务行业组织按照本组织章程开展行业自律，建立健全行业规范，推动行业诚信建设，监督、引导本行业经营者公平参与市场竞争。

第二章 电子商务经营者

第一节 一般规定

第九条 本法所称电子商务经营者，是指通过互联网等信息网络从事销售商品或者提供服务的经营活动的自然人、法人和非法人组织，包括电子商务平台经营者、平台内经营者以及通过自建网站、其他网络服务销售商品或者提供服务的电子商务经营者。

本法所称电子商务平台经营者，是指在电子商务中为交易双方或者多方提供网络经营场所、交易撮合、信息发布等服务，供交易双方或者多方独立开展交易活动的法人或者非法人组织。

本法所称平台内经营者，是指通过电子商务平台销售商品或者提供服务的电子商务经营者。

第十条 电子商务经营者应当依法办理市场主体登记。但是，个人销售自产农副产品、家庭手工业产品，个人利用自己的技能从事依法无须取得许可的便民劳务活动和零星小额交易活动，以及依照法律、行政法规不需要进行登记的除外。

第十一条 电子商务经营者应当依法履行纳税义务，并依法享受税收优惠。

依照前条规定不需要办理市场主体登记的电子商务经营者在首次纳税义务发生后，应当依照税收征收管理法律、行政法规的规定申请办理税务登记，并如实申报纳税。

第十二条 电子商务经营者从事经营活动，依法需要取得相关行政许可的，应当依法取得行政许可。

第十三条 电子商务经营者销售的商品或者提供的服务应当符合保障人身、财产安全的要求和环境保护要求，不得销售或者提供法律、行政法规禁止交易的商品或者服务。

第十四条 电子商务经营者销售商品或者提供服务应当依法出具纸质发票或者电子发票等购货凭证或者服务单据。电子发票与纸质发票具有同等法律效力。

第十五条 电子商务经营者应当在其首页显著位置，持续公示营业执照信息、与其经营业务有关的行政许可信息、属于依照本法第十条规定的不需要办理市场主体登记情形等信息，或者上述信息的链接标识。

前款规定的信息发生变更的，电子商务经营者应当及时更新公示信息。

第十六条 电子商务经营者自行终止从事电子商务的，应当提前三十日在首页显著位置持续公示有关信息。

第十七条 电子商务经营者应当全面、真实、准确、及时地披露商品或者服务信息，保障消费者的知情权和选择权。电子商务经营者不得以虚构交易、编造用户评价等方式进行虚假或者引人误解的商业宣传，欺骗、误导消费者。

第十八条 电子商务经营者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的搜索结果的，应当同时向该消费者提供不针对其个人特征的选项，尊重和平等保护消费者合法权益。

电子商务经营者向消费者发送广告的，应当遵守《中华人民共和国广告法》的有关规定。

第十九条 电子商务经营者搭售商品或者服务，应当以显著方式提请消费者注意，不得将搭售商品或者服务作为默认同意的选项。

第二十条 电子商务经营者应当按照承诺或者与消费者约定的方式、时限向消费者交付商品或者服务，并承担商品运输中的风险和责任。但是，消费者另行选择快递物流服务提供者的除外。

第二十一条 电子商务经营者按照约定向消费者收取押金的，应当明示押金退还的方式、程序，不得对押金退还设置不合理条件。消费者申请退还押金，符合押金退还条件的，电子商务经营者应当及时退还。

第二十二条 电子商务经营者因其技术优势、用户数量、对相关行业的控制

能力以及其他经营者对该电子商务经营者在交易上的依赖程度等因素而具有市场支配地位的，不得滥用市场支配地位，排除、限制竞争。

第二十三条 电子商务经营者收集、使用其用户的个人信息，应当遵守法律、行政法规有关个人信息保护的规定。

第二十四条 电子商务经营者应当明示用户信息查询、更正、删除以及用户注销的方式、程序，不得对用户信息查询、更正、删除以及用户注销设置不合理条件。

电子商务经营者收到用户信息查询或者更正、删除的申请，应当在核实身份后及时提供查询或者更正、删除用户信息。用户注销的，电子商务经营者应当立即删除该用户的信息；依照法律、行政法规的规定或者双方约定保存的，依照其规定。

第二十五条 有关主管部门依照法律、行政法规的规定要求电子商务经营者提供有关电子商务数据信息的，电子商务经营者应当提供。有关主管部门应当采取必要措施保护电子商务经营者提供的数据信息的安全，并对其中的个人信息、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。

第二十六条 电子商务经营者从事跨境电子商务，应当遵守进出口监督管理的法律、行政法规和国家有关规定。

第二节 电子商务平台经营者

第二十七条 电子商务平台经营者应当要求申请进入平台销售商品或者提供服务的经营者提交其身份、地址、联系方式、行政许可等真实信息，进行核验、登记，建立登记档案，并定期核验更新。

电子商务平台经营者为进入平台销售商品或者提供服务的非经营用户提供服务的，应当遵守本节有关规定。

第二十八条 电子商务平台经营者应当按照规定向市场监督管理部门报送平台内经营者的身份信息，提示未办理市场主体登记的经营者依法办理登记，并配合市场监督管理部门，针对电子商务的特点，为应当办理市场主体登记的经营

者办理登记提供便利。

电子商务平台经营者应当依照税收征收管理法律、行政法规的规定，向税务部门报送平台内经营者的身份信息和与纳税有关的信息，并应当提示依照本法第十条规定不需要办理市场主体登记的电子商务经营者依照本法第十一条第二款的规定办理税务登记。

第二十九条 电子商务平台经营者发现平台内的商品或者服务信息存在违反本法第十二条、第十三条规定情形的，应当依法采取必要的处置措施，并向有关主管部门报告。

第三十条 电子商务平台经营者应当采取技术措施和其他必要措施保证其网络安全、稳定运行，防范网络违法犯罪活动，有效应对网络安全事件，保障电子商务交易安全。

电子商务平台经营者应当制定网络安全事件应急预案，发生网络安全事件时，应当立即启动应急预案，采取相应的补救措施，并向有关主管部门报告。

第三十一条 电子商务平台经营者应当记录、保存平台上发布的商品和服务信息、交易信息，并确保信息的完整性、保密性、可用性。商品和服务信息、交易信息保存时间自交易完成之日起不少于三年；法律、行政法规另有规定的，依照其规定。

第三十二条 电子商务平台经营者应当遵循公开、公平、公正的原则，制定平台服务协议和交易规则，明确进入和退出平台、商品和服务质量保障、消费者权益保护、个人信息保护等方面的权利和义务。

第三十三条 电子商务平台经营者应当在其首页显著位置持续公示平台服务协议和交易规则信息或者上述信息的链接标识，并保证经营者和消费者能够便利、完整地阅览和下载。

第三十四条 电子商务平台经营者修改平台服务协议和交易规则，应当在其首页显著位置公开征求意见，采取合理措施确保有关各方能够及时充分表达意见。修改内容应当至少在实施前七日予以公示。

平台内经营者不接受修改内容，要求退出平台的，电子商务平台经营者不得阻止，并按照修改前的服务协议和交易规则承担相关责任。

第三十五条 电子商务平台经营者不得利用服务协议、交易规则以及技术等手段，对平台内经营者在平台内的交易、交易价格以及与其他经营者的交易等进行不合理限制或者附加不合理条件，或者向平台内经营者收取不合理费用。

第三十六条 电子商务平台经营者依据平台服务协议和交易规则对平台内经营者违反法律、法规的行为实施警示、暂停或者终止服务等措施的，应当及时公示。

第三十七条 电子商务平台经营者在其平台上开展自营业务的，应当以显著方式区分标记自营业务和平台内经营者开展的业务，不得误导消费者。

电子商务平台经营者对其标记为自营的业务依法承担商品销售者或者服务提供者的民事责任。

第三十八条 电子商务平台经营者知道或者应当知道平台内经营者销售的商品或者提供的服务不符合保障人身、财产安全的要求，或者有其他侵害消费者合法权益行为，未采取必要措施的，依法与该平台内经营者承担连带责任。

对关系消费者生命健康的商品或者服务，电子商务平台经营者对平台内经营者的资质资格未尽到审核义务，或者对消费者未尽到安全保障义务，造成消费者损害的，依法承担相应的责任。

第三十九条 电子商务平台经营者应当建立健全信用评价制度，公示信用评价规则，为消费者提供对平台内销售的商品或者提供的服务进行评价的途径。

电子商务平台经营者不得删除消费者对其平台内销售的商品或者提供的服务的评价。

第四十条 电子商务平台经营者应当根据商品或者服务的价格、销量、信用等以多种方式向消费者显示商品或者服务的搜索结果；对于竞价排名的商品或者服务，应当显著标明“广告”。

第四十一条 电子商务平台经营者应当建立知识产权保护规则，与知识产权

权利人加强合作，依法保护知识产权。

第四十二条 知识产权权利人认为其知识产权受到侵害的，有权通知电子商务平台经营者采取删除、屏蔽、断开链接、终止交易和服务等必要措施。通知应当包括构成侵权的初步证据。

电子商务平台经营者接到通知后，应当及时采取必要措施，并将该通知转送平台内经营者；未及时采取必要措施的，对损害的扩大部分与平台内经营者承担连带责任。

因通知错误造成平台内经营者损害的，依法承担民事责任。恶意发出错误通知，造成平台内经营者损失的，加倍承担赔偿责任。

第四十三条 平台内经营者接到转送的通知后，可以向电子商务平台经营者提交不存在侵权行为的声明。声明应当包括不存在侵权行为的初步证据。

电子商务平台经营者接到声明后，应当将该声明转送发出通知的知识产权权利人，并告知其可以向有关主管部门投诉或者向人民法院起诉。电子商务平台经营者在转送声明到达知识产权权利人后十五日内，未收到权利人已经投诉或者起诉通知的，应当及时终止所采取的措施。

第四十四条 电子商务平台经营者应当及时公示收到的本法第四十二条、第四十三条规定的通知、声明及处理结果。

第四十五条 电子商务平台经营者知道或者应当知道平台内经营者侵犯知识产权的，应当采取删除、屏蔽、断开链接、终止交易和服务等必要措施；未采取必要措施的，与侵权人承担连带责任。

第四十六条 除本法第九条第二款规定的服务外，电子商务平台经营者可以按照平台服务协议和交易规则，为经营者之间的电子商务提供仓储、物流、支付结算、交收等服务。电子商务平台经营者为经营者之间的电子商务提供服务，应当遵守法律、行政法规和国家有关规定，不得采取集中竞价、做市商等集中交易方式进行交易，不得进行标准化合约交易。

第三章 电子商务合同的订立与履行

第四十七条 电子商务当事人订立和履行合同，适用本章和《中华人民共和国民法总则》《中华人民共和国合同法》《中华人民共和国电子签名法》等法律的规定。

第四十八条 电子商务当事人使用自动信息系统订立或者履行合同的行为对使用该系统的当事人具有法律效力。

在电子商务中推定当事人具有相应的民事行为能力。但是，有相反证据足以推翻的除外。

第四十九条 电子商务经营者发布的商品或者服务信息符合要约条件的，用户选择该商品或者服务并提交订单成功，合同成立。当事人另有约定的，从其约定。

电子商务经营者不得以格式条款等方式约定消费者支付价款后合同不成立；格式条款等含有该内容的，其内容无效。

第五十条 电子商务经营者应当清晰、全面、明确地告知用户订立合同的步骤、注意事项、下载方法等事项，并保证用户能够便利、完整地阅览和下载。

电子商务经营者应当保证用户在提交订单前可以更正输入错误。

第五十一条 合同标的为交付商品并采用快递物流方式交付的，收货人签收时间为交付时间。合同标的为提供服务的，生成的电子凭证或者实物凭证中载明的时间为交付时间；前述凭证没有载明时间或者载明时间与实际提供服务时间不一致的，实际提供服务的时间为交付时间。

合同标的为采用在线传输方式交付的，合同标的进入对方当事人指定的特定系统并且能够检索识别的时间为交付时间。

合同当事人对交付方式、交付时间另有约定的，从其约定。

第五十二条 电子商务当事人可以约定采用快递物流方式交付商品。

快递物流服务提供者应当遵守法律、行政法规，并应当符合承诺的服务规范和时限。快递物流服务提供者在交付商品时，应

当提示收货人当面查验；交由他人代收的，应当经收货人同意。

快递物流服务提供者应当按照规定使用环保包装材料，实现包装材料的减量化和再利用。

快递物流服务提供者在提供快递物流服务的同时，可以接受电子商务经营者的委托提供代收货款服务。

第五十三条 电子商务当事人可以约定采用电子支付方式支付价款。

电子支付服务提供者电子商务提供电子支付服务，应当遵守国家规定，告知用户电子支付服务的功能、使用方法、注意事项、相关风险和收费标准等事项，不得附加不合理交易条件。电子支付服务提供者应当确保电子支付指令的完整性、一致性、可跟踪稽核和不可篡改。

电子支付服务提供者应当向用户免费提供对账服务以及最近三年的交易记录。

第五十四条 电子支付服务提供者提供电子支付服务不符合国家有关支付安全管理要求，造成用户损失的，应当承担赔偿责任。

第五十五条 用户在发出支付指令前，应当核对支付指令所包含的金额、收款人等完整信息。

支付指令发生错误的，电子支付服务提供者应当及时查找原因，并采取相关措施予以纠正。造成用户损失的，电子支付服务提供者应当承担赔偿责任，但能够证明支付错误非自身原因造成的除外。

第五十六条 电子支付服务提供者完成电子支付后，应当及时准确地向用户提供符合约定方式的确认支付的信息。

第五十七条 用户应当妥善保管交易密码、电子签名数据等安全工具。用户发现安全工具遗失、被盗用或者未经授权的支付的，应当及时通知电子支付服务提供者。

未经授权的支付造成的损失，由电子支付服务提供者承担；电子支付服务提

供者能够证明未经授权的支付是因用户的过错造成的，不承担责任。

电子支付服务提供者发现支付指令未经授权，或者收到用户支付指令未经授权的通知时，应当立即采取措施防止损失扩大。电子支付服务提供者未及时采取措施导致损失扩大的，对损失扩大部分承担责任。

第四章 电子商务争议解决

第五十八条 国家鼓励电子商务平台经营者建立有利于电子商务发展和消费者权益保护的商品、服务质量担保机制。

电子商务平台经营者与平台内经营者协议设立消费者权益保证金的，双方应当就消费者权益保证金的提取数额、管理、使用和退还办法等作出明确约定。

消费者要求电子商务平台经营者承担先行赔偿责任以及电子商务平台经营者赔偿后向平台内经营者的追偿，适用《中华人民共和国消费者权益保护法》的有关规定。

第五十九条 电子商务经营者应当建立便捷、有效的投诉、举报机制，公开投诉、举报方式等信息，及时受理并处理投诉、举报。

第六十条 电子商务争议可以通过协商和解，请求消费者组织、行业协会或者其他依法成立的调解组织调解，向有关部门投诉，提请仲裁，或者提起诉讼等方式解决。

第六十一条 消费者在电子商务平台购买商品或者接受服务，与平台内经营者发生争议时，电子商务平台经营者应当积极协助消费者维护合法权益。

第六十二条 在电子商务争议处理中，电子商务经营者应当提供原始合同和交易记录。因电子商务经营者丢失、伪造、篡改、销毁、隐匿或者拒绝提供前述资料，致使人民法院、仲裁机构或者有关机关无法查明事实的，电子商务经营者应当承担相应的法律责任。

第六十三条 电子商务平台经营者可以建立争议在线解决机制，制定并公示争议解决规则，根据自愿原则，公平、公正地解决当事人的争议。

第五章 电子商务促进

第六十四条 国务院和省、自治区、直辖市人民政府应当将电子商务发展纳入国民经济和社会发展规划，制定科学合理的产业政策，促进电子商务创新发展。

第六十五条 国务院和县级以上地方人民政府及其有关部门应当采取措施，支持、推动绿色包装、仓储、运输，促进电子商务绿色发展。

第六十六条 国家推动电子商务基础设施和物流网络建设，完善电子商务统计制度，加强电子商务标准体系建设。

第六十七条 国家推动电子商务在国民经济各个领域的应用，支持电子商务与各产业融合发展。

第六十八条 国家促进农业生产、加工、流通等环节的互联网技术应用，鼓励各类社会资源加强合作，促进农村电子商务发展，发挥电子商务在精准扶贫中的作用。

第六十九条 国家维护电子商务交易安全，保护电子商务用户信息，鼓励电子商务数据开发应用，保障电子商务数据依法有序自由流动。

国家采取措施推动建立公共数据共享机制，促进电子商务经营者依法利用公共数据。

第七十条 国家支持依法设立的信用评价机构开展电子商务信用评价，向社会提供电子商务信用评价服务。

第七十一条 国家促进跨境电子商务发展，建立健全适应跨境电子商务特点的海关、税收、进出境检验检疫、支付结算等管理制度，提高跨境电子商务各环节便利化水平，支持跨境电子商务平台经营者等为跨境电子商务提供仓储物流、报关、报检等服务。

国家支持小型微型企业从事跨境电子商务。

第七十二条 国家进出口管理部门应当推进跨境电子商务海关申报、纳税、检验检疫等环节的综合服务和监管体系建设，优化监管流程，推动实现信息共享、

监管互认、执法互助，提高跨境电子商务服务和监管效率。跨境电子商务经营者可以凭电子单证向国家进出口管理部门办理有关手续。

第七十三条 国家推动建立与不同国家、地区之间跨境电子商务的交流合作，参与电子商务国际规则的制定，促进电子签名、电子身份等国际互认。

国家推动建立与不同国家、地区之间的跨境电子商务争议解决机制。

第六章 法律责任

第七十四条 电子商务经营者销售商品或者提供服务，不履行合同义务或者履行合同义务不符合约定，或者造成他人损害的，依法承担民事责任。

第七十五条 电子商务经营者违反本法第十二条、第十三条规定，未取得相关行政许可从事经营活动，或者销售、提供法律、行政法规禁止交易的商品、服务，或者不履行本法第二十五条规定的信息提供义务，电子商务平台经营者违反本法第四十六条规定，采取集中交易方式进行交易，或者进行标准化合约交易的，依照有关法律、行政法规的规定处罚。

第七十六条 电子商务经营者违反本法规定，有下列行为之一的，由市场监督管理部门责令限期改正，可以处一万元以下的罚款，对其中的电子商务平台经营者，依照本法第八十一条第一款的规定处罚：

- 1、未在首页显著位置公示营业执照信息、行政许可信息、属于不需要办理市场主体登记情形等信息，或者上述信息的链接标识的；
- 2、未在首页显著位置持续公示终止电子商务的有关信息的；
- 3、未明示用户信息查询、更正、删除以及用户注销的方式、程序，或者对用户信息查询、更正、删除以及用户注销设置不合理条件的。

电子商务平台经营者对违反前款规定的平台内经营者未采取必要措施的，由市场监督管理部门责令限期改正，可以处二万元以上十万元以下的罚款。

第七十七条 电子商务经营者违反本法第十八条第一款规定提供搜索结果，或者违反本法第十九条规定搭售商品、服务的，由市场监督管理部门责令限期改

正，没收违法所得，可以并处五万元以上二十万元以下的罚款；情节严重的，并处二十万元以上五十万元以下的罚款。

第七十八条 电子商务经营者违反本法第二十一条规定，未向消费者明示押金退还的方式、程序，对押金退还设置不合理条件，或者不及时退还押金的，由有关主管部门责令限期改正，可以处五万元以上二十万元以下的罚款；情节严重的，处二十万元以上五十万元以下的罚款。

第七十九条 电子商务经营者违反法律、行政法规有关个人信息保护的规定，或者不履行本法第三十条和有关法律、行政法规规定的网络安全保障义务的，依照《中华人民共和国网络安全法》等法律、行政法规的规定处罚。

第八十条 电子商务平台经营者有下列行为之一的，由有关主管部门责令限期改正；逾期不改正的，处二万元以上十万元以下的罚款；情节严重的，责令停业整顿，并处十万元以上五十万元以下的罚款：

- 1、不履行本法第二十七条规定的核验、登记义务的；
- 2、不按照本法第二十八条规定向市场监督管理部门、税务部门报送有关信息的；
- 3、不按照本法第二十九条规定对违法情形采取必要的处置措施，或者未向有关主管部门报告的；
- 4、不履行本法第三十一条规定的商品和服务信息、交易信息保存义务的。

法律、行政法规对前款规定的违法行为的处罚另有规定的，依照其规定。

第八十一条 电子商务平台经营者违反本法规定，有下列行为之一的，由市场监督管理部门责令限期改正，可以处二万元以上十万元以下的罚款；情节严重的，处十万元以上五十万元以下的罚款：

- 1、未在首页显著位置持续公示平台服务协议、交易规则信息或者上述信息的链接标识的；
- 2、修改交易规则未在首页显著位置公开征求意见，未按照规定的时间提前

公示修改内容，或者阻止平台内经营者退出的；

3、未以显著方式区分标记自营业务和平台内经营者开展的业务的；

4、未为消费者提供对平台内销售的商品或者提供的服务进行评价的途径，或者擅自删除消费者的评价的。

电子商务平台经营者违反本法第四十条规定，对竞价排名的商品或者服务未显著标明“广告”的，依照《中华人民共和国广告法》的规定处罚。

第八十二条 电子商务平台经营者违反本法第三十五条规定，对平台内经营者在平台内的交易、交易价格或者与其他经营者的交易等进行不合理限制或者附加不合理条件，或者向平台内经营者收取不合理费用的，由市场监督管理部门责令限期改正，可以处五万元以上五十万元以下的罚款；情节严重的，处五十万元以上二百万元以下的罚款。

第八十三条 电子商务平台经营者违反本法第三十八条规定，对平台内经营者侵害消费者合法权益行为未采取必要措施，或者对平台内经营者未尽到资质资格审核义务，或者对消费者未尽到安全保障义务的，由市场监督管理部门责令限期改正，可以处五万元以上五十万元以下的罚款；情节严重的，责令停业整顿，并处五十万元以上二百万元以下的罚款。

第八十四条 电子商务平台经营者违反本法第四十二条、第四十五条规定，对平台内经营者实施侵犯知识产权行为未依法采取必要措施的，由有关知识产权行政部门责令限期改正；逾期不改正的，处五万元以上五十万元以下的罚款；情节严重的，处五十万元以上二百万元以下的罚款。

第八十五条 电子商务经营者违反本法规定，销售的商品或者提供的服务不符合保障人身、财产安全的要求，实施虚假或者引人误解的商业宣传等不正当竞争行为，滥用市场支配地位，或者实施侵犯知识产权、侵害消费者权益等行为的，依照有关法律的规定处罚。

第八十六条 电子商务经营者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。

第八十七条 依法负有电子商务监督管理职责的部门的工作人员，玩忽职守、滥用职权、徇私舞弊，或者泄露、出售或者非法向他人提供在履行职责中所知悉的个人信息、隐私和商业秘密的，依法追究法律责任。

第八十八条 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。

第七章 附 则

第八十九条 本法自2019年1月1日起施行。

(五) 中华人民共和国密码法

(2019年10月26日第十三届全国人民代表大会常务委员会第十四次会议通过)

目 录

第一章 总 则

第二章 核心密码、普通密码

第三章 商用密码

第四章 法律责任

第五章 附 则

第一章 总 则

第一条 为了规范密码应用和管理，促进密码事业发展，保障网络与信息安全，维护国家和社会公共利益，保护公民、法人和其他组织的合法权益，制定本法。

第二条 本法所称密码，是指采用特定变换的方法对信息等进行加密保护、安全认证的技术、产品和服务。

第三条 密码工作坚持总体国家安全观，遵循统一领导、分级负责，创新发展、服务大局，依法管理、保障安全的原则。

第四条 坚持中国共产党对密码工作的领导。中央密码工作领导机构对全国密码工作实行统一领导，制定国家密码工作重大方针政策，统筹协调国家密码重大事项和重要工作，推进国家密码法治建设。

第五条 国家密码管理部门负责管理全国的密码工作。县级以上地方各级密码管理部门负责管理本行政区域的密码工作。

国家机关和涉及密码工作的单位在其职责范围内负责本机关、本单位或者本系统的密码工作。

第六条 国家对密码实行分类管理。

密码分为核心密码、普通密码和商用密码。

第七条 核心密码、普通密码用于保护国家秘密信息，核心密码保护信息的最高密级为绝密级，普通密码保护信息的最高密级为机密级。

核心密码、普通密码属于国家秘密。密码管理部门依照本法和有关法律、行政法规、国家有关规定对核心密码、普通密码实行严格统一管理。

第八条 商用密码用于保护不属于国家秘密的信息。

公民、法人和其他组织可以依法使用商用密码保护网络与信息安全。

第九条 国家鼓励和支持密码科学技术研究和应用，依法保护密码领域的知识产权，促进密码科学技术进步和创新。

国家加强密码人才培养和队伍建设，对在密码工作中作出突出贡献的组织和个人，按照国家有关规定给予表彰和奖励。

第十条 国家采取多种形式加强密码安全教育，将密码安全教育纳入国民教育体系和公务员教育培训体系，增强公民、法人和其他组织的密码安全意识。

第十一条 县级以上人民政府应当将密码工作纳入本级国民经济和社会发展规划，所需经费列入本级财政预算。

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。

第二章 核心密码、普通密码

第十三条 国家加强核心密码、普通密码的科学规划、管理和使用，加强制度建设，完善管理措施，增强密码安全保障能力。

第十四条 在有线、无线通信中传递的国家秘密信息，以及存储、处理国家秘密信息的信息系统，应当依照法律、行政法规和国家有关规定使用核心密码、普通密码进行加密保护、安全认证。

第十五条 从事核心密码、普通密码科研、生产、服务、检测、装备、使用和销毁等工作的机构（以下统称密码工作机构）应当按照法律、行政法规、国家有关规定以及核心密码、普通密码标准的要求，建立健全安全管理制度，采取严格的保密措施和保密责任制，确保核心密码、普通密码的安全。

第十六条 密码管理部门依法对密码工作机构的核心密码、普通密码工作进行指导、监督和检查，密码工作机构应当配合。

第十七条 密码管理部门根据工作需要会同有关部门建立核心密码、普通密码的安全监测预警、安全风险评估、信息通报、重大事项会商和应急处置等协作机制，确保核心密码、普通密码安全管理的协同联动和有序高效。

密码工作机构发现核心密码、普通密码泄密或者影响核心密码、普通密码安全的重大问题、风险隐患的，应当立即采取应对措施，并及时向保密行政管理部门、密码管理部门报告，由保密行政管理部门、密码管理部门会同有关部门组织开展调查、处置，并指导有关密码工作机构及时消除安全隐患。

第十八条 国家加强密码工作机构建设，保障其履行工作职责。

国家建立适应核心密码、普通密码工作需要的人员录用、选调、保密、考核、培训、待遇、奖惩、交流、退出等管理制度。

第十九条 密码管理部门因工作需要，按照国家有关规定，可以提请公安、交通运输、海关等部门对核心密码、普通密码有关物品和人员提供免检等便利，有关部门应当予以协助。

第二十条 密码管理部门和密码工作机构应当建立健全严格的监督和安全审查制度，对其工作人员遵守法律和纪律等情况进行监督，并依法采取必要措施，定期或者不定期组织开展安全审查。

第三章 商用密码

第二十一条 国家鼓励商用密码技术的研究开发、学术交流、成果转化和推广应用，健全统一、开放、竞争、有序的商用密码市场体系，鼓励和促进商用密码产业发展。

各级人民政府及其有关部门应当遵循非歧视原则，依法平等对待包括外商投资企业在内的商用密码科研、生产、销售、服务、进出口等单位（以下统称商用密码从业单位）。国家鼓励在外商投资过程中基于自愿原则和商业规则开展商用密码技术合作。行政机关及其工作人员不得利用行政手段强制转让商用密码技术。

商用密码的科研、生产、销售、服务和进出口，不得损害国家安全、社会公共利益或者他人合法权益。

第二十二条 国家建立和完善商用密码标准体系。

国务院标准化行政主管部门和国家密码管理部门依据各自职责，组织制定商

用密码国家标准、行业标准。

国家支持社会团体、企业利用自主创新技术制定高于国家标准、行业标准相关技术要求的商用密码团体标准、企业标准。

第二十三条 国家推动参与商用密码国际标准化活动，参与制定商用密码国际标准，推进商用密码中国标准与国外标准之间的转化运用。

国家鼓励企业、社会团体和教育、科研机构等参与商用密码国际标准化活动。

第二十四条 商用密码从业单位开展商用密码活动，应当符合有关法律、行政法规、商用密码强制性国家标准以及该从业单位公开标准的技术要求。

国家鼓励商用密码从业单位采用商用密码推荐性国家标准、行业标准，提升商用密码的防护能力，维护用户的合法权益。

第二十五条 国家推进商用密码检测认证体系建设，制定商用密码检测认证技术规范、规则，鼓励商用密码从业单位自愿接受商用密码检测认证，提升市场竞争力。

商用密码检测、认证机构应当依法取得相关资质，并依照法律、行政法规的规定和商用密码检测认证技术规范、规则开展商用密码检测认证。

商用密码检测、认证机构应当对其在商用密码检测认证中所知悉的国家秘密和商业秘密承担保密义务。

第二十六条 涉及国家安全、国计民生、社会公共利益的商用密码产品，应当依法列入网络关键设备和网络安全专用产品目录，由具备资格的机构检测认证合格后，方可销售或者提供。商用密码产品检测认证适用《中华人民共和国网络安全法》的有关规定，避免重复检测认证。

商用密码服务使用网络关键设备和网络安全专用产品的，应当经商用密码认证机构对该商用密码服务认证合格。

第二十七条 法律、行政法规和国家有关规定要求使用商用密码进行保护的关键信息基础设施，其运营者应当使用商用密码进行保护，自行或者委托商用密

码检测机构开展商用密码应用安全性评估。商用密码应用安全性评估应当与关键信息基础设施安全检测评估、网络安全等级测评制度相衔接，避免重复评估、测评。

关键信息基础设施的运营者采购涉及商用密码的网络产品和服务，可能影响国家安全的，应当按照《中华人民共和国网络安全法》的规定，通过国家网信部门会同国家密码管理部门等有关部门组织的国家安全审查。

第二十八条 国务院商务主管部门、国家密码管理部门依法对涉及国家安全、社会公共利益且具有加密保护功能的商用密码实施进口许可，对涉及国家安全、社会公共利益或者中国承担国际义务的商用密码实施出口管制。商用密码进口许可清单和出口管制清单由国务院商务主管部门会同国家密码管理部门和海关总署制定并公布。

大众消费类产品所采用的商用密码不实行进口许可和出口管制制度。

第二十九条 国家密码管理部门对采用商用密码技术从事电子政务电子认证服务的机构进行认定，会同有关部门负责政务活动中使用电子签名、数据电文的管理。

第三十条 商用密码领域的行业协会等组织依照法律、行政法规及其章程的规定，为商用密码从业单位提供信息、技术、培训等服务，引导和督促商用密码从业单位依法开展商用密码活动，加强行业自律，推动行业诚信建设，促进行业健康发展。

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。

第三十三条 违反本法第十四条规定，未按照要求使用核心密码、普通密码的，由密码管理部门责令改正或者停止违法行为，给予警告；情节严重的，由密码管理部门建议有关国家机关、单位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或者处理。

第三十四条 违反本法规定，发生核心密码、普通密码泄密案件的，由保密行政管理部门、密码管理部门建议有关国家机关、单位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或者处理。

违反本法第十七条第二款规定，发现核心密码、普通密码泄密或者影响核心密码、普通密码安全的重大问题、风险隐患，未立即采取应对措施，或者未及时报告的，由保密行政管理部门、密码管理部门建议有关国家机关、单位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或者处理。

第三十五条 商用密码检测、认证机构违反本法第二十五条第二款、第三款规定开展商用密码检测认证的，由市场监督管理部门会同密码管理部门责令改正或者停止违法行为，给予警告，没收违法所得；违法所得三十万元以上的，可以并处违法所得一倍以上三倍以下罚款；没有违法所得或者违法所得不足三十万元的，可以并处十万元以上三十万元以下罚款；情节严重的，依法吊销相关资质。

第三十六条 违反本法第二十六条规定，销售或者提供未经检测认证或者检测认证不合格的商用密码产品，或者提供未经认证或者认证不合格的商用密码服务的，由市场监督管理部门会同密码管理部门责令改正或者停止违法行为，给予警告，没收违法产品和违法所得；违法所得十万元以上的，可以并处违法所得一倍以上三倍以下罚款；没有违法所得或者违法所得不足十万元的，可以并处三万元以上十万元以下罚款。

第三十七条 关键信息基础设施的运营者违反本法第二十七条第一款规定，

未按照要求使用商用密码，或者未按照要求开展商用密码应用安全性评估的，由密码管理部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。

关键信息基础设施的运营者违反本法第二十七条第二款规定，使用未经安全审查或者安全审查未通过的产品或者服务的，由有关主管部门责令停止使用，处采购金额一倍以上十倍以下罚款；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。

第三十八条 违反本法第二十八条实施进口许可、出口管制的规定，进出口商用密码的，由国务院商务主管部门或者海关依法予以处罚。

第三十九条 违反本法第二十九条规定，未经认定从事电子政务电子认证服务的，由密码管理部门责令改正或者停止违法行为，给予警告，没收违法产品和违法所得；违法所得三十万元以上的，可以并处违法所得一倍以上三倍以下罚款；没有违法所得或者违法所得不足三十万元的，可以并处十万元以上三十万元以下罚款。

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。

第五章 附 则

第四十二条 国家密码管理部门依照法律、行政法规的规定，制定密码管理规章。

第四十三条 中国人民解放军和中国人民武装警察部队的密码工作管理办法，由中央军事委员会根据本法制定。

第四十四条 本法自2020年1月1日起施行。

(六) 中华人民共和国测绘法

(1992 年 12 月 28 日第七届全国人民代表大会常务委员会第二十九次会议通过 2002 年 8 月 29 日第九届全国人民代表大会常务委员会第二十九次会议第一次修订 2017 年 4 月 27 日第十二届全国人民代表大会常务委员会第二十七次会议第二次修订)

目录

第一章 总则

第二章 测绘基准和测绘系统

第三章 基础测绘

第四章 界线测绘和其他测绘

第五章 测绘资质资格

第六章 测绘成果

第七章 测量标志保护

第八章 监督管理

第九章 法律责任

第十章 附则

第一章 总 则

第一条 为了加强测绘管理，促进测绘事业发展，保障测绘事业为经济建设、国防建设、社会发展和生态保护服务，维护国家地理信息安全，制定本法。

第二条 在中华人民共和国领域和中华人民共和国管辖的其他海域从事测绘活动，应当遵守本法。

本法所称测绘，是指对自然地理要素或者地表人工设施的形状、大小、空间位置及其属性等进行测定、采集、表述，以及对获取的数据、信息、成果进行处理和提供的活动。

第三条 测绘事业是经济建设、国防建设、社会发展的基础性事业。各级人民政府应当加强对测绘工作的领导。

第四条 国务院测绘地理信息主管部门负责全国测绘工作的统一监督管理。国务院其他有关部门按照国务院规定的职责分工，负责本部门有关的测绘工作。

县级以上地方人民政府测绘地理信息主管部门负责本行政区域测绘工作的统一监督管理。县级以上地方人民政府其他有关部门按照本级人民政府规定的职责分工，负责本部门有关的测绘工作。

军队测绘部门负责管理军事部门的测绘工作，并按照国务院、中央军事委员会规定的职责分工负责管理海洋基础测绘工作。

第五条 从事测绘活动，应当使用国家规定的测绘基准和测绘系统，执行国家规定的测绘技术规范和标准。

第六条 国家鼓励测绘科学技术的创新和进步，采用先进的技术和设备，提高测绘水平，推动军民融合，促进测绘成果的应用。国家加强测绘科学技术的国际交流与合作。

对在测绘科学技术的创新和进步中做出重要贡献的单位和个人，按照国家有关规定给予奖励。

第七条各级人民政府和有关部门应当加强对国家版图意识的宣传教育，增强公民的国家版图意识。新闻媒体应当开展国家版图意识的宣传。教育行政部门、学校应当将国家版图意识教育纳入中小学教学内容，加强爱国主义教育。

第八条外国的组织或者个人在中华人民共和国领域和中华人民共和国管辖的其他海域从事测绘活动，应当经国务院测绘地理信息主管部门会同军队测绘部门批准，并遵守中华人民共和国有关法律、行政法规的规定。

外国的组织或者个人在中华人民共和国领域从事测绘活动，应当与中华人民共和国有关部门或者单位合作进行，并不得涉及国家秘密和危害国家安全。

第二章 测绘基准和测绘系统

第九条国家设立和采用全国统一的大地基准、高程基准、深度基准和重力基准，其数据由国务院测绘地理信息主管部门审核，并与国务院其他有关部门、军队测绘部门会商后，报国务院批准。

第十条国家建立全国统一的大地坐标系统、平面坐标系统、高程系统、地心坐标系统和重力测量系统，确定国家大地测量等级和精度以及国家基本比例尺地图的系列和基本精度。具体规范和要求由国务院测绘地理信息主管部门会同国务院其他有关部门、军队测绘部门制定。

第十一条因建设、城市规划和科学研究的需要，国家重大工程项目和国务院确定的大城市确需建立相对独立的平面坐标系统的，由国务院测绘地理信息主管部门批准；其他确需建立相对独立的平面坐标系统的，由省、自治区、直辖市人民政府测绘地理信息主管部门批准。

建立相对独立的平面坐标系统，应当与国家坐标系统相联系。

第十二条国务院测绘地理信息主管部门和省、自治区、直辖市人民政府测绘地理信息主管部门应当会同本级人民政府其他有关部门，按照统筹建设、资源共享的原则，建立统一的卫星导航定位基准服务系统，提供导航定位基准信息公共服务。

第十三条建设卫星导航定位基准站的，建设单位应当按照国家有关规定报国务院测绘地理信息主管部门或者省、自治区、直辖市人民政府测绘地理信息主管部门备案。国务院测绘地理信息主管部门应当汇总全国卫星导航定位基准站建设备案情况，并定期向军队测绘部门通报。

本法所称卫星导航定位基准站，是指对卫星导航信号进行长期连续观测，并通过通信设施将观测数据实时或者定时传送至数据中心的地面固定观测站。

第十四条卫星导航定位基准站的建设和运行维护应当符合国家标准和要求，不得危害国家安全。

卫星导航定位基准站的建设和运行维护单位应当建立数据安全保障制度，并遵守保密法律、行政法规的规定。

县级以上人民政府测绘地理信息主管部门应当会同本级人民政府其他有关部门，加强对卫星导航定位基准站建设和运行维护的规范和指导。

第三章 基础测绘

第十五条基础测绘是公益性事业。国家对基础测绘实行分级管理。

本法所称基础测绘，是指建立全国统一的测绘基准和测绘系统，进行基础航空摄影，获取基础地理信息的遥感资料，测制和更新国家基本比例尺地图、影像图和数字化产品，建立、更新基础地理信息系统。

第十六条国务院测绘地理信息主管部门会同国务院其他有关部门、军队测绘部门组织编制全国基础测绘规划，报国务院批准后组织实施。

县级以上地方人民政府测绘地理信息主管部门会同本级人民政府其他有关部门，根据国家和上一级人民政府的基础测绘规划及本行政区域的实际情况，组织编制本行政区域的基础测绘规划，报本级人民政府批准后组织实施。

第十七条军队测绘部门负责编制军事测绘规划，按照国务院、中央军事委员会规定的职责分工负责编制海洋基础测绘规划，并组织实施。

第十八条县级以上人民政府应当将基础测绘纳入本级国民经济和社会发展规划，将基础测绘工作所需经费列入本级政府预算。

国务院发展改革部门会同国务院测绘地理信息主管部门，根据全国基础测绘规划编制全国基础测绘年度计划。

县级以上地方人民政府发展改革部门会同本级人民政府测绘地理信息主管部门，根据本行政区域的基础测绘规划编制本行政区域的基础测绘年度计划，并分别报上一级部门备案。

第十九条基础测绘成果应当定期更新，经济建设、国防建设、社会发展和生态环境保护急需的基础测绘成果应当及时更新。

基础测绘成果的更新周期根据不同地区国民经济和社会发展的需要确定。

第四章 界线测绘和其他测绘

第二十条中华人民共和国国界线的测绘，按照中华人民共和国与相邻国家缔结的边界条约或者协定执行，由外交部组织实施。中华人民共和国地图的国界线标准样图，由外交部和国务院测绘地理信息主管部门拟定，报国务院批准后公布。

第二十一条行政区域界线的测绘，按照国务院有关规定执行。省、自治区、直辖市和自治州、县、自治县、市行政区域界线的标准画法图，由国务院民政部门 and 国务院测绘地理信息主管部门拟定，报国务院批准后公布。

第二十二条县级以上人民政府测绘地理信息主管部门应当会同本级人民政府不动产登记主管部门，加强对不动产测绘的管理。

测量土地、建筑物、构筑物 and 地面其他附着物的权属界址线，应当按照县级以上人民政府确定的权属界线的界址点、界址线或者提供的有关登记资料和附图进行。权属界址线发生变化的，有关当事人应当及时进行变更测绘。

第二十三条城乡建设领域的工程测量活动，与房屋产权、产籍相关的房屋面积的测量，应当执行由国务院住房城乡建设主管部门、国务院测绘地理信息主管部门组织编制的测量技术规范。

水利、能源、交通、通信、资源开发和其他领域的工程测量活动，应当执行国家有关的工程测量技术规范。

第二十四条建立地理信息系统，应当采用符合国家标准的基础地理信息数据。

第二十五条县级以上人民政府测绘地理信息主管部门应当根据突发事件应对工作需要，及时提供地图、基础地理信息数据等测绘成果，做好遥感监测、导航定位等应急测绘保障工作。

第二十六条县级以上人民政府测绘地理信息主管部门应当会同本级人民政府其他有关部门依法开展地理国情监测，并按照国家有关规定严格管理、规范使用地理国情监测成果。

各级人民政府应当采取有效措施，发挥地理国情监测成果在政府决策、经济社会发展和社会公众服务中的作用。

第五章 测绘资质资格

第二十七条国家对从事测绘活动的单位实行测绘资质管理制度。

从事测绘活动的单位应当具备下列条件，并依法取得相应等级的测绘资质证书，方可从事测绘活动：

- （一）有法人资格；
- （二）有与从事的测绘活动相适应的专业技术人员；
- （三）有与从事的测绘活动相适应的技术装备和设施；

（四）有健全的技术和质量保证体系、安全保障措施、信息安全保密管理制度以及测绘成果和资料档案管理制度。

第二十八条国务院测绘地理信息主管部门和省、自治区、直辖市人民政府测绘地理信息主管部门按照各自的职责负责测绘资质审查、发放测绘资质证书。具体办法由国务院测绘地理信息主管部门商国务院其他有关部门规定。

军队测绘部门负责军事测绘单位的测绘资质审查。

第二十九条测绘单位不得超越资质等级许可的范围从事测绘活动，不得以其他测绘单位的名义从事测绘活动，不得允许其他单位以本单位的名义从事测绘活动。

测绘项目实行招投标的，测绘项目的招标单位应当依法在招标公告或者投标邀请书中对测绘单位资质等级作出要求，不得让不具有相应测绘资质等级的单位中标，不得让测绘单位低于测绘成本中标。

中标的测绘单位不得向他人转让测绘项目。

第三十条从事测绘活动的专业技术人员应当具备相应的执业资格条件。具体办法由国务院测绘地理信息主管部门会同国务院人力资源社会保障主管部门规定。

第三十一条测绘人员进行测绘活动时，应当持有测绘作业证件。

任何单位和个人不得阻碍测绘人员依法进行测绘活动。

第三十二条测绘单位的测绘资质证书、测绘专业技术人员的执业证书和测绘人员的测绘作业证件的式样，由国务院测绘地理信息主管部门统一规定。

第六章 测绘成果

第三十三条国家实行测绘成果汇交制度。国家依法保护测绘成果的知识产权。

测绘项目完成后，测绘项目出资人或者承担国家投资的测绘项目的单位，应当向国务院测绘地理信息主管部门或者省、自治区、直辖市人民政府测绘地理信息主管部门汇交测绘成果资料。属于基础测绘项目的，应当汇交测绘成果副本；属于非基础测绘项目的，应当汇交测绘成果目录。负责接收测绘成果副本和目录的测绘地理信息主管部门应当出具测绘成果汇交凭证，并及时将测绘成果副本和目录移交给保管单位。测绘成果汇交的具体办法由国务院规定。

国务院测绘地理信息主管部门和省、自治区、直辖市人民政府测绘地理信息主管部门应当及时编制测绘成果目录，并向社会公布。

第三十四条县级以上人民政府测绘地理信息主管部门应当积极推进公众版测绘成果的加工和编制工作，通过提供公众版测绘成果、保密技术处理等方式，促进测绘成果的社会化应用。

测绘成果保管单位应当采取措施保障测绘成果的完整和安全，并按照国家有关规定向社会公开和提供利用。

测绘成果属于国家秘密的，适用保密法律、行政法规的规定；需要对外提供的，按照国务院和中央军事委员会规定的审批程序执行。

测绘成果的秘密范围和秘密等级，应当依照保密法律、行政法规的规定，按照保障国家秘密安全、促进地理信息共享和应用的原则确定并及时调整、公布。

第三十五条使用财政资金的测绘项目和涉及测绘的其他使用财政资金的项目，有关部门在批准立项前应当征求本级人民政府测绘地理信息主管部门的意见；有适宜测绘成果的，应当充分利用已有的测绘成果，避免重复测绘。

第三十六条基础测绘成果和国家投资完成的其他测绘成果，用于政府决策、国防建设和公共服务的，应当无偿提供。

除前款规定情形外，测绘成果依法实行有偿使用制度。但是，各级人民政府及有关部门和军队因防灾减灾、应对突发事件、维护国家安全等公共利益的需要，可以无偿使用。

测绘成果使用的具体办法由国务院规定。

第三十七条中华人民共和国领域和中华人民共和国管辖的其他海域的位置、高程、深度、面积、长度等重要地理信息数据，由国务院测绘地理信息主管部门审核，并与国务院其他有关部门、军队测绘部门会商后，报国务院批准，由国务院或者国务院授权的部门公布。

第三十八条地图的编制、出版、展示、登载及更新应当遵守国家有关地图编制标准、地图内容表示、地图审核的规定。

互联网地图服务提供者应当使用经依法审核批准的地图，建立地图数据安全管理制度，采取安全保障措施，加强对互联网地图新增内容的核校，提高服务质量。

县级以上人民政府和测绘地理信息主管部门、网信部门等有关部门应当加强对地图编制、出版、展示、登载和互联网地图服务的监督管理，保证地图质量，维护国家主权、安全和利益。

地图管理的具体办法由国务院规定。

第三十九条测绘单位应当对完成的测绘成果质量负责。县级以上人民政府测绘地理信息主管部门应当加强对测绘成果质量的监督管理。

第四十条国家鼓励发展地理信息产业，推动地理信息产业结构调整和优化升级，支持开发各类地理信息产品，提高产品质量，推广使用安全可信的地理信息技术和设备。

县级以上人民政府应当建立健全政府部门间地理信息资源共建共享机制，引导和支持企业提供地理信息社会化服务，促进地理信息广泛应用。

县级以上人民政府测绘地理信息主管部门应当及时获取、处理、更新基础地理信息数据，通过地理信息公共服务平台向社会提供地理信息公共服务，实现地理信息数据开放共享。

第七章 测量标志保护

第四十一条任何单位和个人不得损毁或者擅自移动永久性测量标志和正在使用中的临时性测量标志，不得侵占永久性测量标志用地，不得在永久性测量标志安全控制范围内从事危害测量标志安全和使用效能的活动。

本法所称永久性测量标志，是指各等级的三角点、基线点、导线点、军用控制点、重力点、天文点、水准点和卫星定位点的觇标和标石标志，以及用于地形测图、工程测量和形变测量的固定标志和海底大地点设施。

第四十二条永久性测量标志的建设单位应当对永久性测量标志设立明显标记，并委托当地有关单位指派专人负责保管。

第四十三条进行工程建设，应当避开永久性测量标志；确实无法避开，需要拆迁永久性测量标志或者使永久性测量标志失去使用效能的，应当经省、自治区、直辖市人民政府测绘地理信息主管部门批准；涉及军用控制点的，应当征得军队测绘部门的同意。所需迁建费用由工程建设单位承担。

第四十四条测绘人员使用永久性测量标志，应当持有测绘作业证件，并保证测量标志的完好。

保管测量标志的人员应当查验测量标志使用后的完好状况。

第四十五条县级以上人民政府应当采取有效措施加强测量标志的保护工作。

县级以上人民政府测绘地理信息主管部门应当按照规定检查、维护永久性测量标志。

乡级人民政府应当做好本行政区域内的测量标志保护工作。

第八章 监督管理

第四十六条县级以上人民政府测绘地理信息主管部门应当会同本级人民政府其他有关部门建立地理信息安全管理和技术防控体系，并加强对地理信息安全的监督管理。

第四十七条地理信息生产、保管、利用单位应当对属于国家秘密的地理信息的获取、持有、提供、利用情况进行登记并长期保存，实行可追溯管理。

从事测绘活动涉及获取、持有、提供、利用属于国家秘密的地理信息，应当遵守保密法律、行政法规和国家有关规定。

地理信息生产、利用单位和互联网地图服务提供者收集、使用用户个人信息的，应当遵守法律、行政法规关于个人信息保护的规定。

第四十八条县级以上人民政府测绘地理信息主管部门应当对测绘单位实行信用管理，并依法将其信用信息予以公示。

第四十九条县级以上人民政府测绘地理信息主管部门应当建立健全随机抽查机制，依法履行监督检查职责，发现涉嫌违反本法规定行为的，可以依法采取下列措施：

（一）查阅、复制有关合同、票据、账簿、登记台账以及其他有关文件、资料；

（二）查封、扣押与涉嫌违法测绘行为直接相关的设备、工具、原材料、测绘成果资料等。

被检查的单位和个人应当配合，如实提供有关文件、资料，不得隐瞒、拒绝和阻碍。

任何单位和个人对违反本法规定的行为，有权向县级以上人民政府测绘地理信息主管部门举报。接到举报的测绘地理信息主管部门应当及时依法处理。

第九章 法律责任

第五十条违反本法规定，县级以上人民政府测绘地理信息主管部门或者其他有关部门工作人员利用职务上的便利收受他人财物、其他好处或者玩忽职守，对不符合法定条件的单位核发测绘资质证书，不依法履行监督管理职责，或者发现违法行为不予查处的，对负有责任的领导人员和直接责任人员，依法给予处分；构成犯罪的，依法追究刑事责任。

第五十一条违反本法规定，外国的组织或者个人未经批准，或者未与中华人民共和国有关部门、单位合作，擅自从事测绘活动的，责令停止违法行为，没收违法所得、测绘成果和测绘工具，并处十万元以上五十万元以下的罚款；情节严重的，并处五十万元以上一百万元以下的罚款，限期出境或者驱逐出境；构成犯罪的，依法追究刑事责任。

第五十二条违反本法规定，未经批准擅自建立相对独立的平面坐标系统，或者采用不符合国家标准的基础地理信息数据建立地理信息系统的，给予警告，责令改正，可以并处五十万元以下的罚款；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。

第五十三条违反本法规定，卫星导航定位基准站建设单位未报备案的，给予警告，责令限期改正；逾期不改正的，处十万元以上三十万元以下的罚款；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。

第五十四条违反本法规定，卫星导航定位基准站的建设和运行维护不符合国家标准、要求的，给予警告，责令限期改正，没收违法所得和测绘成果，并处三十万元以上五十万元以下的罚款；逾期不改正的，没收相关设备；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。

第五十五条违反本法规定，未取得测绘资质证书，擅自从事测绘活动的，责令停止违法行为，没收违法所得和测绘成果，并处测绘约定报酬一倍以上二倍以下的罚款；情节严重的，没收测绘工具。

以欺骗手段取得测绘资质证书从事测绘活动的，吊销测绘资质证书，没收违法所得和测绘成果，并处测绘约定报酬一倍以上二倍以下的罚款；情节严重的，没收测绘工具。

第五十六条违反本法规定，测绘单位有下列行为之一的，责令停止违法行为，没收违法所得和测绘成果，处测绘约定报酬一倍以上二倍以下的罚款，并可以责令停业整顿或者降低测绘资质等级；情节严重的，吊销测绘资质证书：

- (一) 超越资质等级许可的范围从事测绘活动；
- (二) 以其他测绘单位的名义从事测绘活动；
- (三) 允许其他单位以本单位的名义从事测绘活动。

第五十七条违反本法规定，测绘项目的招标单位让不具有相应资质等级的测绘单位中标，或者让测绘单位低于测绘成本中标的，责令改正，可以处测绘约定报酬二倍以下的罚款。招标单位的工作人员利用职务上的便利，索取他人财物，或者非法收受他人财物为他人谋取利益的，依法给予处分；构成犯罪的，依法追究刑事责任。

第五十八条违反本法规定，中标的测绘单位向他人转让测绘项目的，责令改正，没收违法所得，处测绘约定报酬一倍以上二倍以下的罚款，并可以责令停业整顿或者降低测绘资质等级；情节严重的，吊销测绘资质证书。

第五十九条违反本法规定，未取得测绘执业资格，擅自从事测绘活动的，责令停止违法行为，没收违法所得和测绘成果，对其所在单位可以处违法所得二倍以下的罚款；情节严重的，没收测绘工具；造成损失的，依法承担赔偿责任。

第六十条违反本法规定，不汇交测绘成果资料的，责令限期汇交；测绘项目出资人逾期不汇交的，处重测所需费用一倍以上二倍以下的罚款；承担国家投资的测绘项目的单位逾期不汇交的，处五万元以上二十万元以下的罚款，并处暂扣测绘资质证书，自暂扣测绘资质证书之日起六个月内仍不汇交的，吊销测绘资质证书；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。

第六十一条违反本法规定，擅自发布中华人民共和国领域和中华人民共和国管辖的其他海域的重要地理信息数据的，给予警告，责令改正，可以并处五十万元以下的罚款；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。

第六十二条违反本法规定，编制、出版、展示、登载、更新的地图或者互联网地图服务不符合国家有关地图管理规定的，依法给予行政处罚、处分；构成犯罪的，依法追究刑事责任。

第六十三条违反本法规定，测绘成果质量不合格的，责令测绘单位补测或者重测；情节严重的，责令停业整顿，并处降低测绘资质等级或者吊销测绘资质证书；造成损失的，依法承担赔偿责任。

第六十四条违反本法规定，有下列行为之一的，给予警告，责令改正，可以并处二十万元以下的罚款；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；造成损失的，依法承担赔偿责任；构成犯罪的，依法追究刑事责任：

- （一）损毁、擅自移动永久性测量标志或者正在使用中的临时性测量标志；
- （二）侵占永久性测量标志用地；

(三) 在永久性测量标志安全控制范围内从事危害测量标志安全和使用效能的活动;

(四) 擅自拆迁永久性测量标志或者使永久性测量标志失去使用效能, 或者拒绝支付迁建费用;

(五) 违反操作规程使用永久性测量标志, 造成永久性测量标志毁损。

第六十五条违反本法规定, 地理信息生产、保管、利用单位未对属于国家秘密的地理信息的获取、持有、提供、利用情况进行登记、长期保存的, 给予警告, 责令改正, 可以并处二十万元以下的罚款; 泄露国家秘密的, 责令停业整顿, 并处降低测绘资质等级或者吊销测绘资质证书; 构成犯罪的, 依法追究刑事责任。

违反本法规定, 获取、持有、提供、利用属于国家秘密的地理信息的, 给予警告, 责令停止违法行为, 没收违法所得, 可以并处违法所得二倍以下的罚款; 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; 造成损失的, 依法承担赔偿责任; 构成犯罪的, 依法追究刑事责任。

第六十六条本法规定的降低测绘资质等级、暂扣测绘资质证书、吊销测绘资质证书的行政处罚, 由颁发测绘资质证书的部门决定; 其他行政处罚, 由县级以上人民政府测绘地理信息主管部门决定。

本法第五十一条规定的限期出境和驱逐出境由公安机关依法决定并执行。

第十章 附 则

第六十七条军事测绘管理办法由中央军事委员会根据本法规定。

第六十八条本法自 2017 年 7 月 1 日起施行。

(六) 2021年全国人民代表大会常务委员会工作报告

——2021年3月8日在第十三届全国人民代表大会第四次会议上

全国人民代表大会常务委员会委员长 栗战书

各位代表：

受全国人大常委会委托，我向大会报告工作，请予审议。

十三届全国人大三次会议以来的主要工作

2020年是新中国历史上极不平凡的一年，以习近平同志为核心的党中央，从容应对世所罕见的风险挑战，统筹推进“五位一体”总体布局，协调推进“四个全面”战略布局，在危机中育先机，于变局中开新局，疫情防控取得重大战略成果，全面建成小康社会取得伟大历史性成就，决战脱贫攻坚取得全面胜利，交出了一份人民满意、世界瞩目、可以载入史册的答卷，中华民族伟大复兴向前迈出了新的一大步！党和国家事业取得新的重大进展，必将激励我们以更加昂扬的姿态奋进在全面建设社会主义现代化国家的伟大征程上！

面对错综复杂的国际形势、艰巨繁重的改革发展稳定任务，在以习近平总书记为核心的党中央坚强领导下，全国人大常委会坚持以习近平新时代中国特色社会主义思想为指导，深入贯彻习近平法治思想，履职尽责、积极作为，为推动重大工作部署、应对重大风险挑战、维护国家安全提供法律保障，有效发挥了国家权力机关的职能作用。十三届全国人大三次会议以来的10个月，常委会认真行使立法权、监督权、决定权、任免权，制定法律9件，修改法律13件，作出有关法律问题和重大问题的决定8件，正在审议的法律案23件；听取审议35个报告，检查1个决定和6部法律实施情况，进行专题询问2次，开展专题调研6项，作出决议1项；决定批准或加入条约7件；审议通过39个任免案，依法任免国家工作人员259人次。

常委会工作最为显著的特点是紧跟党中央重大决策部署，紧贴人民群众美好生活对法治建设的呼声期盼，紧扣国家治理体系和治理能力现代化提出的法律需求实际，加强立法和法律监督，努力使各项工作更好围绕中心和全局、更好服务国家和人民。例如：强化野生动物保护法律制度，及时作出关于全面禁止野生动

物非法交易和食用的决定，接着就这一决定和野生动物保护法开展执法检查，随后启动野生动物保护法的修改；强化公共卫生法治保障，及时制定专项立法修法工作计划，成立专班分批推进30部法律的制定和修改工作；坚决维护香港特别行政区宪制秩序，根据香港形势发展对法律的需求，及时制定香港特别行政区维护国家安全法，听取审议国务院关于修改完善香港选举制度和有关建议的报告，形成关于完善香港选举制度的决定草案，并提请大会审议；助力脱贫攻坚战，加快推进“三农”立法工作，围绕脱贫攻坚听取审议专项工作报告、开展专题调研；持续助力打好污染防治攻坚战，用3年时间完成污染防治领域最为重要的大气污染防治法、水污染防治法、土壤污染防治法实施情况的检查，特别是土壤污染防治法实施一年半即跟进执法检查，有力推动了土壤污染防治工作；用法治力量推动优化营商环境，检查了反不正当竞争法实施情况，开展优化营商环境专项备案审查，今年还将修改反垄断法；为适应国家新一轮高水平对外开放提供法律支撑，审议海南自由贸易港法草案，及时制定出口管制法，修改专利法；积极回应社会治理领域热点问题，社区矫正法出台之后，紧接着通过[刑法修正案（十一）](#)，修改未成年人保护法和预防未成年人犯罪法等等。这些工作，落实了党中央对人大工作的新要求，回应了人民群众的新期待，为新时代全面依法治国提供了法律支持和保障。

一、加强宪法实施和监督，维护国家法治统一

全面贯彻实施宪法是全面依法治国、建设社会主义法治国家的首要任务和基础性工作。常委会认真履行推动宪法实施、加强宪法监督的法定职责，维护宪法尊严和权威。

完善宪法相关法律制度。修改国旗法、国徽法，更好维护国家形象、弘扬爱国主义精神，让捍卫国旗和国徽的尊严成为人们的自觉行动。修改选举法，适当增加县乡两级人大代表名额，夯实人民代表大会制度基础。适应深化国家监察体制改革需要，制定公职人员政务处分法，审议监察官法草案。全国人大组织法、全国人大议事规则制定30多年来，进行首次修改，提交大会审议的修正草案，全面贯彻坚持党的领导政治原则，充分吸收人民代表大会制度实践的新经验、新成果，围绕人大组织制度、工作机制、运行模式，对大会主席团、委员长会议的职

权和工作程序进行完善，充分反映党和国家机构改革后机构设置及其职能发生的新变化。经过全体代表的共同努力，一定能把这两部法律修改好，成为全国人大及其常委会依法履职、确保人大工作高效运行的程序法，成为实现坚持党的领导、人民当家作主、依法治国有机统一的保障法。

维护香港特别行政区宪制秩序、法治秩序。2019年发生“修例风波”，香港法治和社会秩序遭遇严重冲击，“一国两制”受到严重挑战。十三届全国人大三次会议作出关于建立健全香港特别行政区维护国家安全的法律制度和执行机制的决定后，常委会迅速行动，于去年6月连续召开两次会议，审议通过香港特别行政区维护国家安全法，并决定将其列入香港基本法附件三，由香港特别行政区在当地公布实施，扭转了香港在国家安全领域长期“不设防”的严峻局面。去年8月、11月，先后通过关于香港第六届立法会继续履行职责的决定、关于香港立法会议员资格问题的决定，本次大会将作出关于完善香港特别行政区选举制度的决定，之后常委会将根据这一决定修改完善相关法律，打出一套法律的“组合拳”。人大将坚定不移依法维护国家主权、安全、发展利益，切实履行法定职责，为维护香港宪制秩序、打击“港独”势力、确保爱国者治港、保持香港长期繁荣稳定提供法律保障！

大力弘扬宪法精神。根据党中央决策部署，落实宪法规定，作出关于授予国家勋章和国家荣誉称号的决定，习近平主席签署主席令，授予钟南山共和国勋章，授予张伯礼、张定宇、陈薇“人民英雄”国家荣誉称号，表彰他们的崇高品质和卓越功绩。举办6次宪法宣誓仪式，任命和决定任命的23位国家工作人员庄严宣誓，引导和教育国家工作人员树立宪法意识，恪守宪法原则，履行宪法使命。开展国家宪法日活动，召开第7个国家宪法日座谈会，推动全社会形成尊崇宪法、学习宪法、遵守宪法、维护宪法、运用宪法的良好氛围。

做好合宪性审查和备案审查工作。回应涉及宪法有关问题的关切，确保法律法规和政策举措符合宪法规定、宪法精神。2020年共收到报送备案的行政法规、地方性法规、自治条例和单行条例、经济特区法规、司法解释、特别行政区法律1310件，逐件进行主动审查。围绕疫情防控、野生动物保护、民法典实施、食品药品安全、优化营商环境等五个方面开展专项审查和集中清理，发现需要修改或

废止的规范性文件3372件，督促有关方面及时予以纠正。做好依申请审查和移送审查，共收到公民、组织提出的审查建议5146件，对属于常委会审查范围的3378件逐一进行研究，提出处理意见，其他建议分别移送有关机关处理。收到有关部门移送审查的地方性法规58件，督促制定机关修改或废止了27件。推动地方人大普遍建立听取备案审查工作报告制度。加强备案审查制度和能力建设，正式开通国家法律法规数据库，为立法活动、备案审查提供基础支撑。

二、围绕党和国家工作大局，顺应人民期盼，加强重点领域立法

中国特色社会主义进入新时代，适应国际形势深刻复杂变化、党和国家事业快速发展的需要，立法工作进入了一个加快发展的新阶段，呈现覆盖广、数量多、节奏快、要求高的新特点。

加强公共卫生立法修法。应对突如其来的新冠肺炎疫情，针对抗疫实践中暴露的法治短板，着眼于构建更加协调、相互衔接的法律体系，加快推进强化公共卫生法治保障立法修法工作。截至目前，已完成修订动物防疫法等6项任务，修改野生动物保护法、执业医师法、传染病防治法等11项任务将在今年年底前完成。通过完善法律制度，加强法律宣传和实施，推动依法做好公布疫情信息、调配应急物资、化解矛盾纠纷、维护市场秩序等工作，用法治的力量守护人民生命安全和身体健康。

加快国家安全立法。当今世界正处于百年未有之大变局，维护国家安全比任何时候都更为紧要。常委会贯彻总体国家安全观，加快重点领域维护国家安全的立法，制定生物安全法、出口管制法，修改档案法，审议海上交通安全法修订草案、数据安全法草案、个人信息保护法草案。这些法律，涵盖了经济安全、资源安全、核安全、生态安全、信息安全、海外利益保护等领域，既是国家应对风险挑战的重要法律，也是人民群众关心关注的重大问题。贯彻落实习近平强军思想，适应新时代国防和军队建设需要，修改国防法、人民武装警察法，制定海警法、退役军人保障法，审议军人地位和权益保障法草案、兵役法修订草案、军事设施保护法修订草案，为国家领土安全、军事安全、国民安全提供法律保障。

围绕推进高质量发展和高水平对外开放立法。制定城市维护建设税法、契税法，修改专利法、著作权法，审议乡村振兴促进法草案、印花税法草案、海南自由贸易港法草案，作出关于设立海南自由贸易港知识产权法院的决定和关于设立北京金融法院的决定。这些立法，涉及财税、金融、知识产权保护、农业农村发展、对外开放等领域，就是要为推动经济发展质量变革、效率变革、动力变革提供法律保障。建设海南自由贸易试验区和自由贸易港，是以习近平同志为核心的党在新时代推进高水平对外开放的战略举措。制定一部体现中国特色、符合国际惯例、反映时代要求的自由贸易港法，就是要在法治轨道上打造开放层次更高、营商环境更优、辐射作用更强的开放新高地。

抓紧社会建设和社会治理领域立法。通过[刑法修正案（十一）](#)，修改未成年人保护法、预防未成年人犯罪法、行政处罚法，审议反食品浪费法草案、反有组织犯罪法草案、法律援助法草案、家庭教育法草案、教育法修正草案，适应国际国内形势变化，顺应人民对美好生活的向往，为推动形成既生机勃勃又井然有序的良好社会局面提供了法律支撑。[刑法修正案（十一）](#)是近年来社会关注度最高的一次修改，补充修改47个条文，涉及安全生产、食品药品、金融秩序、营商环境、公共卫生、生物安全、生态环保等方面，对社会关注的冒名顶替上学就业、抢控公交车方向盘、高空抛物、非法集资、刑事责任年龄等新情况新问题作出直接回应。反食品浪费法草案弘扬中华民族传统美德，倡导文明、健康、理性、绿色消费理念。聚焦特定领域、特殊问题，积极开展“小切口”立法，拓展了立法工作方法和路径，标志着立法工作进一步向专业化、具体化方向发展。

继续完善生态环保法律。贯彻习近平生态文明思想，持续推动生态环保法律制度集成创新，本届以来制定和修改长江保护法、土壤污染防治法、固体废物污染环境防治法等12部相关法律，作出1项决议，正在审议湿地保护法草案，用最严格的制度、最严密的法治划定生态红线，守护绿水青山。去年12月通过的长江保护法，全面贯彻“共抓大保护、不搞大开发”理念，是我国第一部全流域的专门法。这部法律用一年时间完成了起草，又用一年时间进行了3次审议，常委会还及时召开长江保护法实施座谈会，用法治力量推动实现长江母亲河一江清水绵

延后世、惠泽人民，促进和保障长江经济带成为我国生态优先绿色发展主战场、畅通国内国际双循环主动脉、引领经济高质量发展主力军。

做好民法典实施相关工作。民法典是新中国成立以来第一部以“法典”命名的法律，是中国特色社会主义法律体系中固根本、稳预期、利长远的基础性法律。常委会认真做好民法典实施准备工作，推动相关配套法规和司法解释的修改完善，阐释好民法典一系列新规定新概念新精神，带头做好宣传、推进、保障实施工作，让民法典走到群众身边、走进人民心里。

三、坚持寓支持于监督之中，依法开展法律监督和工作监督

始终把握依照法定职责、限于法定范围、遵守法定程序的原则，坚持正确监督、有效监督，推动宪法法律全面有效实施，确保行政权、监察权、审判权、检察权依法行使。

强化计划和预算、决算审查监督。紧扣十三届全国人大三次会议批准的社会发展目标任务，突出做好“六稳”工作、落实“六保”任务，听取审议国民经济和社会发展规划执行情况报告，定期召开经济形势分析会，跟踪监督经济运行情况，确保党中央重大决策部署落实落地、大会批准的计划全面贯彻执行。贯彻积极财政政策更加积极有为的要求，听取审议中央决算报告、预算执行情况报告、审计工作报告，审查和批准2019年中央决算。听取审议关于审计查出问题整改情况的报告并进行专题询问，开展整改情况跟踪监督，推动有关问题切实整改。认真开展疫情防控税费优惠政策、减税降费专题调研，为加大资金投入、保障好各地疫情防控资金需要提供法律支撑。

深入推进人大预算审查监督重点拓展改革。制定关于加强地方人大对政府债务审查监督的若干意见，推动预算审查监督重点拓展改革落细落实。开展全口径预算审查、全过程预算监管，强化“事前”监督，聚焦“事中”监督，做实“事后”监督。加强政策实施效果和资金使用绩效情况监督，建立听取政府预算绩效评价情况及相关重要政策和重点资金绩效情况通报机制，推动建立绩效评价结果与完善政策和安排预算的挂钩机制。坚持“线上”监测与“线下”调研分析

相结合，推进预算联网监督系统二期建设，为全国人大代表履行预算审查监督职责提供便利。

认真履行对国有资产管理的监督职责。作出关于加强国有资产管理情况监督的决定，准确把握职责定位，增强监督工作的针对性、规范性和可操作性，为更好监督国有资产管理提供法律保障。听取审议2019年度国有资产管理情况综合报告和关于企业国有资产管理情况专项报告。开展企业国有资产（不含金融企业）管理情况监督调研，推动国务院深化以管资本为主的监管体制改革、国有企业混合所有制改革以及优化调整国有资本布局。开展健全国有资产治理体系专题调研，推进国资联网监督工作，用3年时间基本实现省级、设区的市级、县级地方建立国有资产管理情况报告制度全覆盖的目标。

听取审议专项工作报告。围绕全面建成小康社会目标任务，紧盯经济运行重点难点问题，听取审议国务院关于科技创新、股票发行注册制改革、脱贫攻坚、财政农业农村资金分配使用情况的报告。首次听取审议国家监察委员会关于开展反腐败国际追逃追赃工作情况的报告，展现了国家监察体制改革的成果和国家治理能力的提升，标志着人大对“一府一委两院”监督工作迈出新步伐。

加强执法司法工作监督。听取审议国务院关于公安机关执法规范化建设工作情况的报告，推动公安机关进一步提升严格规范文明公正执法水平。适应民事案件新特点、刑事犯罪新变化，听取审议最高人民法院关于加强民事审判工作依法服务保障经济社会持续健康发展情况的报告、关于民事诉讼程序繁简分流改革试点情况的中期报告，听取审议最高人民检察院关于适用认罪认罚从宽制度情况的报告，推动提高民事审判质效和刑事案件办理质量，实现司法公正与效率有机统一，办案政治效果、法律效果和社会效果有机统一。

持续加大执法检查力度。围绕统筹推进疫情防控和经济社会发展，回应人大代表和人民群众要求和期盼，常委会检查了关于全面禁止野生动物非法交易和食用的决定、野生动物保护法、土壤污染防治法、农业机械化促进法、慈善法、公共文化服务保障法、反不正当竞争法的实施情况，听取审议国务院关于研究处理“一决定一法”执法检查报告及审议意见情况的报告，宣传普及法律，紧扣法律规定推动法律责任落到实处。聚焦蓝天、碧水、净土保卫战，连续3年先后检查

大气污染防治法、水污染防治法、土壤污染防治法实施情况，实地检查22个省份的78个地市，召开74场座谈会，暗访170个单位和项目，梳理20类82个问题，点名曝光143个单位存在的问题。持续推进生态环保领域的执法检查，运用法治方式助力打好污染防治攻坚战，有力推动了生态文明理念、生态环保法律深入人心，凝聚起建设青山常在、绿水长流、空气常新美丽中国的法治力量。

扎实做好专题调研。把专题调研作为常委会开展工作监督的重要方式，委员长会议组成人员、常委会、专门委员会和工作委员会开展232次调研，形成了307个调研报告。其中，常委会组织开展“十四五”规划纲要编制工作若干重要问题、生态环保决议落实情况、珍惜粮食反对浪费情况、社会保险制度改革和社会保险法实施、民族团结进步创建工作、政府投资基金管理与改革等6项专题调研。“十四五”规划纲要相关专题调研历时4个多月，有关专门委员会和工作委员会精心组织，深入了解民族、国家安全、财政经济、教科文卫、侨务、环保、“三农”、社会保障等方面情况，形成22份专题调研报告。通过多种渠道、多种途径推动调研成果转化运用，使调研报告有效服务人大监督和立法修法工作，也为中央和国家机关提供决策参考和工作参考。

四、坚持代表主体地位，支持和服务代表依法履职

牢固树立服务代表的理念，围绕密切常委会同代表的联系、密切代表同人民群众的联系，认真落实关于加强和改进全国人大代表工作“35条具体措施”，不断提高代表工作水平。

认真办好代表议案和建议。十三届全国人大三次会议主席团交付的506件代表议案全部审议完毕，其中118件议案涉及的22个立法项目已审议通过或正在审议，168件议案涉及的58个立法项目已列入立法规划或计划。代表提出的9180件建议，交由194家承办单位办理并全部答复代表，代表建议所提问题得到解决或计划逐步解决的占71.28%。将181件代表建议涉及的9个方面问题确定为重点督办建议，全国人大有关专门委员会负责督办，有力推动了一批群众关心、社会关注重点难点问题的解决。代表在闭会期间提交的400多件建议，交由98家承办单位研究处理，做到即收即办、逐件反馈。完善代表议案建议交办协调工作机制，协

调解决意见最集中、反映最突出的问题，推动议案建议转化为促发展、惠民生、暖民心的政策举措。

密切常委会同代表的联系。常委会组成人员直接联系439位代表，通过座谈、走访、电话、邮件、微信、参加调研等方式，认真听取代表意见建议。推动代表深度参与常委会工作，邀请175人次代表列席常委会会议，召开2次列席代表座谈会。各专门委员会探索建立对口联系代表机制，500多人次代表参加执法检查、工作调研、计划和预算审查监督、国有资产管理监督等工作。落实重要法律草案征求代表意见机制，修订未成年人保护法时，采纳214位代表提出的完善青少年控烟长效机制等建议。增设6个立法联系点，新设5个基层预算审查监督联系点，搭建听取代表、群众意见的“直通车”。

密切代表同人民群众的联系。代表联系群众形式多样、内容丰富，这是近年代表工作的一个亮点。代表通过走访、座谈、回原选举单位述职、参加代表小组活动等方式直接听取和反映群众意见建议，发挥了党和政府联系群众的桥梁纽带作用。按照常委会统一安排，约1800人次代表参加集中视察、专题调研活动，形成一批重要调研成果。全国人大代表就近参加代表联络站、代表之家活动，积极推动解决就业、教育、医疗、住房、养老、食品安全、生态环保等方面人民群众反映突出的问题，有效发挥代表在反映群众诉求、解决民生难题中的积极作用。

加强代表履职能力建设。创建全国人大网络学院，为代表和各级人大提供了学习培训的新途径。开设人大历史、代表履职知识、代表风采等具有人大特色的专栏，增强培训课程针对性和实效性，截至目前课程总点播量达到83万次。举办3期网络视频学习班和2期线上线下相结合的代表学习班，1.1万人次代表和地方人大负责同志参加学习。基层代表积极参加学习培训，思想政治水平、法律政策水平、专业知识水平进一步提高，联系人民、代表人民、服务人民自觉性主动性进一步增强，在联系群众、接触实际中积极发现并反映带有普遍性、共性、典型性的问题，推动从法律上、制度上、政策上予以解决。

改进人大信访工作。制定全国人大代表信访事项办理工作规程，交办转办代表来信141件次。开通网上信访平台，一年多来处理网上信访2.4万件次。拓展民

主立法的渠道，认真研究分析群众来信来访反映集中的问题，在相关立法修法工作中予以回应。

五、服务国家外交大局，发挥人大外事工作的职能作用

疫情改变了外事活动形式，但没有阻隔人大的对外交往。以落实国家元首共识为主要任务，创新外事活动形式，举行各层级双边视频活动46场，出席视频会议26场，进行通话交流15次，开展线下外事活动27场，外交信函往来近600件。

加强双边友好交往。人大外事工作的一个优势是覆盖面广、方式灵活，与有关国家建立了130个友好小组，与22个国家议会和欧洲议会建立了定期交流机制，与近190个国家和地区议会保持交往与联系。举行中俄议会合作委员会第六次会议、中法议会合作委员会第十一次会议，同蒙古国家大呼拉尔开展定期机制交流；与日本、韩国、老挝、柬埔寨、印尼、新加坡、乌兹别克斯坦、德国、肯尼亚等国议会领导人视频会晤，深化立法经验交流互鉴，为国家间务实合作提供法律保障，从立法机构角度助力国家关系深入发展。香港特别行政区维护国家安全法通过，全国人大以双边友好小组组长名义给93个国家议会和欧洲议会发了106封信函，介绍有关情况、阐释中方立场，获得广泛理解和支持。

推动多边交流合作。围绕共建“一带一路”倡议，加强与沿线国家议会的政策沟通和立法交流。出席第五次世界议长大会、第六届金砖国家议会论坛等视频会议，参加各国议会联盟、议会世贸大会指导委员会、亚洲议会大会、东盟各国议会间大会等多边活动，推动将“人类命运共同体”、“以人民为中心”、“团结合作、共同抗疫”等主张写入多边会议文件，坚定维护多边主义，坚定维护以联合国为核心的国际体系，坚定维护以国际法为基础的国际秩序。

对外宣介中国道路和中国制度。积极宣介习近平新时代中国特色社会主义思想，主动介绍中国发展成就和对世界的贡献。主动宣介习近平法治思想，介绍人大制度和立法工作。主动宣介中国坚持人民至上、生命至上的抗疫理念，分享中国抗疫经验做法。加强人大英文网站建设，办好中国人大杂志英文版，展示中国特色社会主义民主政治制度的优势和功效。

坚定维护国家利益。发挥常委会发言人、外事委发言人、法工委发言人机制作用，在涉藏、涉疆、涉港、涉台和抗疫问题上阐明中方立场。人大是人民的人大。任何时候、任何情况下，只要党、国家和人民需要，人大就将毫不犹豫站到一线进行法律的、政治的、外交的斗争，伸出肩膀扛起应尽的政治责任。

六、加强履职能力建设，不断提升常委会自身建设水平

围绕做到政治可靠、尊崇法治、发扬民主、服务人民、运行高效，成为全面担负起宪法法律赋予各项职责的工作机关、同人民群众保持密切联系的代表机关的目标，全面加强常委会自身建设。

加强思想政治建设。巩固深化“不忘初心、牢记使命”主题教育成果，深入学习《习近平谈治国理政》第三卷，开展7次常委会党组集体学习，举办6次常委会专题讲座，及时传达学习习近平总书记重要讲话和中央会议、文件精神。召开习近平总书记关于坚持和完善人民代表大会制度的重要思想学习交流会、第26次全国地方立法工作座谈会，深入学习习近平法治思想，带头学习宣传宪法法律和相关履职知识，常委会组成人员的政治素质和运用法治思维、法治方式做好人大工作的能力水平进一步提高。

完善常委会运行机制。总结十三届全国人大三次会议成功经验和做法，适应疫情防控常态化需要，制定全国人大例会和其他重要会议改进会风的具体措施。合理安排委员长会议、常委会会议，确保每一次会议、每一件议案、每一个事项都符合法律规定。按照紧凑高效的原则，合理安排会议日程，适当压缩会期，优化会议流程，提高审议质量。常委会召开了8次会议，平均出席率超过97%，列席人员到会率超过95%。坚持民主集中制原则，保障常委会组成人员充分行使民主权利，保证人大通过的法律、作出的决议更好体现党的主张和人民意志。

充分发挥专门委员会作用。修订专门委员会分党组工作规则，推进分党组工作规范化、制度化。各专门委员会共召开152次会议，高质量、高效率完成立法、监督、代表议案建议办理等工作。牵头起草13件法律草案并依法提请审议。对其他国家机关负责起草的法律草案，提前介入并加强督促和指导。协助常委会做好

备案审查工作。组织开展执法检查 and 专题调研，持续跟踪监督常委会审议意见研究处理情况。

加强人大机关建设。坚持办好党风廉政宣传教育周活动，继续开展机关内部巡视，梳理完善137项机关制度，用制度巩固党建成果、提升机关效能。严格执行中央八项规定及其实施细则精神，深入推进“灯下黑”问题专项整治，坚决纠治形式主义、官僚主义。以新一轮中央巡视和巡视整改为契机，提高参谋服务保障工作水平，努力建设让党中央放心、让人民群众满意的模范机关。

统筹做好人大舆论宣传工作。积极研究、阐释、宣传人民代表大会制度，全面准确报道人大会议和立法、监督工作，认真办好“代表通道”、“部长通道”集中采访活动。大力宣传代表在抗疫斗争、脱贫攻坚、民族团结中的履职担当，讲好中国故事、中国人大故事、人大代表故事。

各位代表!

常委会工作取得的成绩，根本在于以习近平同志为核心的党中央坚强领导，根本在于习近平新时代中国特色社会主义思想科学指引，是全国人大代表、常委会组成人员、各专门委员会组成人员和全国人大机关工作人员担当尽责、扎实工作的结果，是国务院、国家监察委员会、最高人民法院、最高人民检察院和地方各级人大密切配合、大力支持的结果，是全国各族人民积极参与、充分信任的结果。在此，我代表全国人大常委会表示崇高的敬意和衷心的感谢!

常委会工作还有一些差距和不足，主要是：立法质量需要进一步提升，立法形式不够丰富，一些领域法律跟不上新时代提出的新要求；监督工作的实效性需要进一步提升，监督的形式和工作机制有待探索创新和不断完善；服务代表的意识和能力需要进一步提升，需要为代表履职创造更好的条件。常委会将虚心听取代表和各方面意见建议，不断加强和改进工作，更好履行宪法法律赋予的职责。

各位代表!

中央全面依法治国工作会议确立了习近平法治思想的指导地位，习近平总书记多次就人大工作发表重要讲话、作出重要指示，为坚持和完善人民代表大会制度指明了方向、提供了遵循。党和国家事业的快速发展，丰富了人民代表大会制

度的实践内涵。人大工作的生动实践，进一步展示了中国特色社会主义民主政治、人民代表大会制度的显著优势和生机活力。在新的奋斗征程上，必须充分发挥人民代表大会制度的根本政治制度作用，坚持党的领导、人民当家作主、依法治国有机统一，通过人民代表大会制度牢牢把国家和民族前途命运掌握在人民手中。

今后一年的主要任务

2021年是实施“十四五”规划、开启全面建设社会主义现代化国家新征程的第一年，也是中国共产党成立100周年，中华民族伟大复兴迎来更加光明的前景。当前和今后一个时期，我国发展环境面临深刻复杂变化，国际形势不稳定性不确定性明显增加，我们在前进道路上面临着许多难关和挑战。我们有习近平新时代中国特色社会主义思想的指导，有以习近平同志为核心的党中央坚强领导，有中国特色社会主义制度的显著优势，有14亿中国人民众志成城、团结奋斗的磅礴力量，就一定能夺取改革开放和社会主义现代化建设新的胜利。进入新发展阶段，必须增强使命感、责任感、紧迫感，勇于担当、敢于负责、善于作为，自觉承担起新时代新征程对人大工作提出的新任务新要求。

常委会工作的总体要求是：在以习近平同志为核心的党中央坚强领导下，以习近平新时代中国特色社会主义思想为指导，深入学习贯彻习近平法治思想和习近平总书记关于坚持和完善人民代表大会制度的重要思想，全面贯彻落实党的十九大和十九届二中、三中、四中、五中全会精神，坚持党的领导、人民当家作主、依法治国有机统一，立足新发展阶段，贯彻新发展理念，构建新发展格局，紧紧围绕“十四五”规划和2035年远景目标谋划人大工作，依法行使立法权、监督权、决定权、任免权，发挥好在全面建设社会主义现代化国家中的职能作用。

一、切实加强宪法实施和监督，维护宪法尊严和权威。认真抓好宪法实施工作，落实宪法解释程序机制，积极回应涉及宪法有关问题的关切。加快推进宪法相关法立法修法工作，制定监察官法，修改全国人大常委会议事规则、国务院组织法、地方各级人民代表大会和地方各级人民政府组织法等。切实加强宪法监督工作，认真做好合宪性审查、备案审查工作，维护国家法治统一。持续推动宪法宣传教育，组织好宪法宣誓、国家宪法日活动。坚持和完善“一国两制”制度体系，维护宪法和基本法确定的特别行政区宪制秩序，确保“一国两制”实践行稳

致远。运用法律手段捍卫一个中国原则、反对“台独”，增进维护一个中国框架的共同认知，依法规范和保障两岸人民关系、推进两岸交流合作，推进祖国和平统一。

二、切实加强重点领域、新兴领域、涉外领域立法，不断提高立法质量和效率。坚持系统观念，坚持急用先行，统筹立改废释纂，发挥人大在立法工作中的主导作用，加快完善中国特色社会主义法律体系。积极推进国家安全、科技创新、公共卫生、生物安全、生态文明、防范风险、涉外法治等重要领域立法，健全国家治理急需的法律制度、满足人民日益增长的美好生活需要必备的法律制度。

根据立法工作计划，初步安排审议45件法律案，还提出了近20件预备项目。继续实施强化公共卫生法治保障立法修法工作计划，制定突发公共卫生事件应对法，修改野生动物保护法、传染病防治法、国境卫生检疫法、执业医师法等。坚持统筹发展和安全，健全国家安全法治体系，制定粮食安全保障法、反有组织犯罪法、陆地国界法、数据安全法、军人地位和权益保障法，修改突发事件应对法、海上交通安全法、安全生产法、兵役法、军事设施保护法等。围绕建设现代化经济体系、促进科技创新，制定乡村振兴促进法、海南自由贸易港法、期货法、印花税法，修改反垄断法、科学技术进步法、公司法、企业破产法、审计法、农产品质量安全法、畜牧法等。完善民生保障、教育文化、社会治理、生态环保、绿色低碳急需的法律制度，制定反食品浪费法、文化产业促进法、家庭教育法、学前教育法、个人信息保护法、社会救助法、法律援助法、湿地保护法、南极活动与环境保护法，修改体育法、教育法、职业教育法、妇女权益保障法、治安管理处罚法、行政复议法、环境噪声污染防治法等，加快推进黄河保护立法。抓紧研究数字经济、互联网金融、人工智能、大数据、云计算等新技术新应用领域的相关法律制度，以法治促进和保障新业态、新模式健康发展。加快推进涉外领域立法，围绕反制裁、反干涉、反制长臂管辖等，充实应对挑战、防范风险的法律“工具箱”，推动形成系统完备的涉外法律法规体系。

适应立法新形势新要求，必须丰富立法形式，坚持既要搞“大块头”，又要搞“小快灵”，适时启动条件成熟领域法典编纂工作，针对实际需要以“小切口”形式推进立法，增强立法的针对性、适用性、可操作性。

三、切实加强监督工作，确保国家机关依法履行职责。监督工作要围绕党和国家中心工作来开展，以高质量发展为主题，以供给侧结构性改革为主线，以改革创新为根本动力，以满足人民日益增长的美好生活需要为根本目的，推动做好“六稳”工作、落实“六保”任务，为顺利完成改革发展稳定各项目标任务发挥职能作用。

根据监督工作计划，预安排了29个监督项目。切实承担好推进人大预算审查监督重点拓展改革、监督国有资产管理情况两项职责，听取审议计划执行、预算执行、决算、审计工作、审计查出问题整改、国有资产管理、环保目标完成情况等7个工作报告，修改关于加强中央预算审查监督的决定、关于加强经济工作监督的决定。坚持围绕中心、服务大局，做好专项工作监督，听取审议关于加快构建新型农业经营体系、长江流域生态环保、雄安新区和白洋淀生态保护、建设现代综合交通运输体系、财政交通运输资金分配和使用、教师队伍建设、文物保护、“七五”普法决议实施、知识产权审判、控告申诉检察等10个专项报告，作出“八五”普法决议。坚持做好立法与推进法律实施并重，检查企业破产法、畜牧法、中医药法、消防法、固体废物污染环境防治法、公证法等6部法律的实施情况，推动法定职责、法律责任得到严格落实。结合听取审议关于建设现代综合交通运输体系、检查固体废物污染环境防治法实施情况的报告，开展2次专题询问。围绕财政补贴管理与改革、发挥海外侨胞在共建“一带一路”中的重要作用、人口较少民族经济社会发展、自然保护地体系建设、设区的市地方立法、推进监察监督全覆盖等，开展6项专题调研。进一步完善监督工作机制，改进方式方法，增强监督工作实效性。

四、切实加强代表工作，更好发挥人大代表作用。深入落实常委会组成人员联系代表制度，健全专门委员会、工作委员会联系代表机制，拓展联系深度、增强联系实效。强化代表对常委会和专门委员会、工作委员会立法、监督、对外交往工作的参与，紧紧依靠代表做好人大工作。提高代表议案和建议工作水平。支持代表密切联系群众，丰富代表小组活动形式，鼓励代表就近参加代表联络站、代表之家、基层联系点的活动。加强代表服务保障工作，继续建好代表履职信息化平台。加强全国人大网络学院建设，完善代表系统培训机制。支持原选举单位

依法监督代表履职，推动代表履职档案规范化建设。实施新修改的选举法，做好全国县乡两级人大换届选举工作。

五、切实加强人大外事工作，深化和拓展各层级各领域交流合作。围绕国家外交总体布局，发挥职能作用，统筹安排疫情防控常态化背景下的对外交往。认真组织委员长会议组成人员外事活动，开展多层次、多渠道对外交往，深化机制交流和专门委员会、友好小组、工作机构交流，积极参与议会多边机制活动。围绕国家核心利益和重大问题主动发声，宣介中国道路、制度和政策、理念、主张。

六、切实加强自身建设，夯实履职的思想政治组织基础。发挥常委会党组集体学习的带动作用，办好常委会专题讲座，深入学习贯彻习近平新时代中国特色社会主义思想，深入学习贯彻习近平法治思想和习近平总书记关于坚持和完善人民代表大会制度的重要思想，认真开展党史学习教育。切实加强人民代表大会制度理论、中国特色社会主义法学理论研究。深入研究常委会运行机制，认真贯彻执行全国人大及其常委会议事规则，认真贯彻执行常委会会议、委员长会议、专门委员会会议有关制度规定。更好发挥专门委员会作用，切实做好研究、审议和拟订有关议案工作，支持专门委员会组成人员全面参与立法、监督、代表、外事等工作。更好发挥常委会工作机构作用，提高全国人大机关参谋服务保障水平。全面贯彻中央八项规定及其实施细则精神，驰而不息改进作风。健全网上受理信访制度。加强新闻舆论工作，全面深入宣传报道人民代表大会制度建设和人大工作新进展新成效。加强与地方人大的工作交流，密切工作协同，提升工作合力。

各位代表!

在全面建设社会主义现代化国家新征程上，我们要更加紧密地团结在以习近平同志为核心的党中央周围，增强“四个意识”、坚定“四个自信”、做到“两个维护”，把宪法法律赋予的职责履行好，把党和人民交给的任务完成好，以优异成绩庆祝中国共产党成立100周年，为实现中华民族伟大复兴中国梦不懈奋斗!

(七) 全国人民代表大会常务委员会关于加强网络信息保护的決定

(2012年12月28日第十一届全国人民代表大会常务委员会第三十次会议通过)

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，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，采取删除等处置措施，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。

(八) 中华人民共和国国民经济和社会发展第十四个五年规划纲要和 2035年远景目标纲要

(2021年3月11日第十三届全国人民代表大会第四次会议批准)

目录

第一篇 开启全面建设社会主义现代化国家新征程

第一章 发展环境

第二章 指导方针

第三章 主要目标

第二篇 坚持创新驱动发展 全面塑造发展新优势

第四章 强化国家战略科技力量

第五章 提升企业技术创新能力

第六章 激发人才创新活力

第七章 完善科技创新体制机制

第三篇 加快发展现代产业体系 巩固壮大实体经济根基

第八章 深入实施制造强国战略

第九章 发展壮大战略性新兴产业

第十章 促进服务业繁荣发展

第十一章 建设现代化基础设施体系

第四篇 形成强大国内市场 构建新发展格局

第十二章 畅通国内大循环

第十三章 促进国内国际双循环

第十四章 加快培育完整内需体系

第五篇 加快数字化发展 建设数字中国

第十五章 打造数字经济新优势

第十六章 加快数字社会建设步伐

第十七章 提高数字政府建设水平

第十八章 营造良好数字生态

第六篇 全面深化改革 构建高水平社会主义市场经济体制

第十九章 激发各类市场主体活力

第二十章 建设高标准市场体系

第二十一章 建立现代财税金融体制

第二十二章 提升政府经济治理能力

第七篇 坚持农业农村优先发展 全面推进乡村振兴

第二十三章 提高农业质量效益和竞争力

第二十四章 实施乡村建设行动

第二十五章 健全城乡融合发展体制机制

第二十六章 实现巩固拓展脱贫攻坚成果同乡村振兴有效衔接

第八篇 完善新型城镇化战略 提升城镇化发展质量

第二十七章 加快农业转移人口市民化

第二十八章 完善城镇化空间布局

第二十九章 全面提升城市品质

第九篇 优化区域经济布局 促进区域协调发展

第三十章 优化国土空间开发保护格局

第三十一章 深入实施区域重大战略

- 第三十二章 深入实施区域协调发展战略
- 第三十三章 积极拓展海洋经济发展空间
- 第十篇 发展社会主义先进文化 提升国家文化软实力
- 第三十四章 提高社会文明程度
- 第三十五章 提升公共文化服务水平
- 第三十六章 健全现代文化产业体系
- 第十一篇 推动绿色发展 促进人与自然和谐共生
- 第三十七章 提升生态系统质量和稳定性
- 第三十八章 持续改善环境质量
- 第三十九章 加快发展方式绿色转型
- 第十二篇 实行高水平对外开放 开拓合作共赢新局面
- 第四十章 建设更高水平开放型经济新体制
- 第四十一章 推动共建“一带一路”高质量发展
- 第四十二章 积极参与全球治理体系改革和建设
- 第十三篇 提升国民素质 促进人的全面发展
- 第四十三章 建设高质量教育体系
- 第四十四章 全面推进健康中国建设
- 第四十五章 实施积极应对人口老龄化国家战略
- 第十四篇 增进民生福祉 提升共建共治共享水平
- 第四十六章 健全国家公共服务制度体系
- 第四十七章 实施就业优先战略
- 第四十八章 优化收入分配结构
- 第四十九章 健全多层次社会保障体系

第五十章 保障妇女未成年人和残疾人基本权益

第五十一章 构建基层社会治理新格局

第十五篇 统筹发展和安全 建设更高水平的平安中国

第五十二章 加强国家安全体系和能力建设

第五十三章 强化国家经济安全保障

第五十四章 全面提高公共安全保障能力

第五十五章 维护社会稳定和安全

第十六篇 加快国防和军队现代化 实现富国和强军相统一

第五十六章 提高国防和军队现代化质量效益

第五十七章 促进国防实力和经济实力同步提升

第十七篇 加强社会主义民主法治建设 健全党和国家监督制度

第五十八章 发展社会主义民主

第五十九章 全面推进依法治国

第六十章 完善党和国家监督体系

第十八篇 坚持“一国两制” 推进祖国统一

第六十一章 保持香港、澳门长期繁荣稳定

第六十二章 推进两岸关系和平发展和祖国统一

第十九篇 加强规划实施保障

第六十三章 加强党中央集中统一领导

第六十四章 健全统一规划体系

第六十五章 完善规划实施机制

中华人民共和国国民经济和社会发展第十四个五年（2021－2025年）规划和2035年远景目标纲要，根据《中共中央关于制定国民经济和社会发展第十四个五年规划和二〇三五年远景目标的建议》编制，主要阐明国家战略意图，明确政府工作重点，引导规范市场主体行为，是我国开启全面建设社会主义现代化国家新征程的宏伟蓝图，是全国各族人民共同的行动纲领。

第一篇 开启全面建设社会主义现代化国家新征程

“十四五”时期是我国全面建成小康社会、实现第一个百年奋斗目标之后，乘势而上开启全面建设社会主义现代化国家新征程、向第二个百年奋斗目标进军的第一个五年。

第一章 发展环境

我国进入新发展阶段，发展基础更加坚实，发展条件深刻变化，进一步发展面临新的机遇和挑战。

第一节 决胜全面建成小康社会取得决定性成就

“十三五”时期是全面建成小康社会决胜阶段。面对错综复杂的国际形势、艰巨繁重的国内改革发展稳定任务特别是新冠肺炎疫情严重冲击，以习近平同志为核心的党中央不忘初心、牢记使命，团结带领全党全国各族人民砥砺前行、开拓创新，奋发有为推进党和国家各项事业。全面深化改革取得重大突破，全面依法治国取得重大进展，全面从严治党取得重大成果，国家治理体系和治理能力现代化加快推进，中国共产党领导和我国社会主义制度优势进一步彰显。

经济运行总体平稳，经济结构持续优化，国内生产总值突破100万亿元。创新型国家建设成果丰硕，在载人航天、探月工程、深海工程、超级计算、量子信息、“复兴号”高速列车、大飞机制造等领域取得一批重大科技成果。决战脱贫攻坚取得全面胜利，5575万农村贫困人口实现脱贫，困扰中华民族几千年的绝对贫困问题得到历史性解决，创造了人类减贫史上的奇迹。农业现代化稳步推进，粮食年产量连续稳定在1.3万亿斤以上。1亿农业转移人口和其他常住人口在城镇落户目标顺利实现，区域重大战略扎实推进。污染防治力度加大，主要污染物排放总量减少目标超额完成，资源利用效率显著提升，生态环境明显改善。金融风

险处置取得重要阶段性成果。对外开放持续扩大，共建“一带一路”成果丰硕。人民生活水平显著提高，教育公平和质量较大提升，高等教育进入普及化阶段，城镇新增就业超过6000万人，建成世界上规模最大的社会保障体系，基本医疗保险覆盖超过13亿人，基本养老保险覆盖近10亿人，城镇棚户区住房改造开工超过2300万套。新冠肺炎疫情防控取得重大战略成果，应对突发事件能力和水平大幅提高。公共文化服务水平不断提高，文化事业和文化产业繁荣发展。国防和军队建设水平大幅提升，军队组织形态实现重大变革。国家安全全面加强，社会保持和谐稳定。

“十三五”规划目标任务胜利完成，我国经济实力、科技实力、综合国力和人民生活水平跃上新的大台阶，全面建成小康社会取得伟大历史性成就，中华民族伟大复兴向前迈出了新的一大步，社会主义中国以更加雄伟的身姿屹立于世界东方。

第二节 我国发展环境面临深刻复杂变化

当前和今后一个时期，我国发展仍然处于重要战略机遇期，但机遇和挑战都有新的发展变化。当今世界正经历百年未有之大变局，新一轮科技革命和产业变革深入发展，国际力量对比深刻调整，和平与发展仍然是时代主题，人类命运共同体理念深入人心。同时，国际环境日趋复杂，不稳定性不确定性明显增加，新冠肺炎疫情影响广泛深远，世界经济陷入低迷期，经济全球化遭遇逆流，全球能源供需版图深刻变革，国际经济政治格局复杂多变，世界进入动荡变革期，单边主义、保护主义、霸权主义对世界和平与发展构成威胁。

我国已转向高质量发展阶段，制度优势显著，治理效能提升，经济长期向好，物质基础雄厚，人力资源丰富，市场空间广阔，发展韧性强劲，社会大局稳定，继续发展具有多方面优势和条件。同时，我国发展不平衡不充分问题仍然突出，重点领域关键环节改革任务仍然艰巨，创新能力不适应高质量发展要求，农业基础还不稳固，城乡区域发展和收入分配差距较大，生态环保任重道远，民生保障存在短板，社会治理还有弱项。

必须统筹中华民族伟大复兴战略全局和世界百年未有之大变局，深刻认识我国社会主要矛盾变化带来的新特征新要求，深刻认识错综复杂的国际环境带来的

新矛盾新挑战，增强机遇意识和风险意识，立足社会主义初级阶段基本国情，保持战略定力，办好自己的事，认识和把握发展规律，发扬斗争精神，增强斗争本领，树立底线思维，准确识变、科学应变、主动求变，善于在危机中育先机、于变局中开新局，抓住机遇，应对挑战，趋利避害，奋勇前进。

第二章 指导方针

“十四五”时期经济社会发展，必须牢牢把握以下指导思想、原则和战略导向。

第一节 指导思想

高举中国特色社会主义伟大旗帜，深入贯彻党的十九大和十九届二中、三中、四中全会精神，坚持以马克思列宁主义、毛泽东思想、邓小平理论、“三个代表”重要思想、科学发展观、习近平新时代中国特色社会主义思想为指导，全面贯彻党的基本理论、基本路线、基本方略，统筹推进经济建设、政治建设、文化建设、社会建设、生态文明建设的总体布局，协调推进全面建设社会主义现代化国家、全面深化改革、全面依法治国、全面从严治党的战略布局，坚定不移贯彻创新、协调、绿色、开放、共享的新发展理念，坚持稳中求进工作总基调，以推动高质量发展为主题，以深化供给侧结构性改革为主线，以改革创新为根本动力，以满足人民日益增长的美好生活需要为根本目的，统筹发展和安全，加快建设现代化经济体系，加快构建以国内大循环为主体、国内国际双循环相互促进的新发展格局，推进国家治理体系和治理能力现代化，实现经济行稳致远、社会安定和谐，为全面建设社会主义现代化国家开好局、起好步。

第二节 必须遵循的原则

--坚持党的全面领导。坚持和完善党领导经济社会发展的体制机制，坚持和完善中国特色社会主义制度，不断提高贯彻新发展理念、构建新发展格局能力和水平，为实现高质量发展提供根本保证。

--坚持以人民为中心。坚持人民主体地位，坚持共同富裕方向，始终做到发展为了人民、发展依靠人民、发展成果由人民共享，维护人民根本利益，激发全体人民积极性、主动性、创造性，促进社会公平，增进民生福祉，不断实现人民

对美好生活的向往。

--坚持新发展理念。把新发展理念完整、准确、全面贯穿发展全过程和各领域，构建新发展格局，切实转变发展方式，推动质量变革、效率变革、动力变革，实现更高质量、更有效率、更加公平、更可持续、更为安全的发展。

--坚持深化改革开放。坚定不移推进改革，坚定不移扩大开放，加强国家治理体系和治理能力现代化建设，破除制约高质量发展、高品质生活的体制机制障碍，强化有利于提高资源配置效率、有利于调动全社会积极性的重大改革开放举措，持续增强发展动力和活力。

--坚持系统观念。加强前瞻性思考、全局性谋划、战略性布局、整体性推进，统筹国内国际两个大局，办好发展安全两件大事，坚持全国一盘棋，更好发挥中央、地方和各方面积极性，着力固根基、扬优势、补短板、强弱项，注重防范化解重大风险挑战，实现发展质量、结构、规模、速度、效益、安全相统一。

第三节 战略导向

“十四五”时期推动高质量发展，必须立足新发展阶段、贯彻新发展理念、构建新发展格局。把握新发展阶段是贯彻新发展理念、构建新发展格局的现实依据，贯彻新发展理念为把握新发展阶段、构建新发展格局提供了行动指南，构建新发展格局则是应对新发展阶段机遇和挑战、贯彻新发展理念的战略选择。必须坚持深化供给侧结构性改革，以创新驱动、高质量供给引领和创造新需求，提升供给体系的韧性和对国内需求的适配性。必须建立扩大内需的有效制度，加快培育完整内需体系，加强需求侧管理，建设强大国内市场。必须坚定不移推进改革，破除制约经济循环的制度障碍，推动生产要素循环流转和生产、分配、流通、消费各环节有机衔接。必须坚定不移扩大开放，持续深化要素流动型开放，稳步拓展制度型开放，依托国内经济循环体系形成对全球要素资源的强大引力场。必须强化国内大循环的主导作用，以国际循环提升国内大循环效率和水平，实现国内国际双循环互促共进。

第三章 主要目标

按照全面建设社会主义现代化国家的战略安排，2035年远景目标和“十四五”时期经济社会发展主要目标如下。

第一节 2035年远景目标

展望2035年，我国将基本实现社会主义现代化。经济实力、科技实力、综合国力将大幅跃升，经济总量和城乡居民人均收入将再迈上新的大台阶，关键核心技术实现重大突破，进入创新型国家前列。基本实现新型工业化、信息化、城镇化、农业现代化，建成现代化经济体系。基本实现国家治理体系和治理能力现代化，人民平等参与、平等发展权利得到充分保障，基本建成法治国家、法治政府、法治社会。建成文化强国、教育强国、人才强国、体育强国、健康中国，国民素质和社会文明程度达到新高度，国家文化软实力显著增强。广泛形成绿色生产生活方式，碳排放达峰后稳中有降，生态环境根本好转，美丽中国建设目标基本实现。形成对外开放新格局，参与国际经济合作和竞争新优势明显增强。人均国内生产总值达到中等发达国家水平，中等收入群体显著扩大，基本公共服务实现均等化，城乡区域发展差距和居民生活水平差距显著缩小。平安中国建设达到更高水平，基本实现国防和军队现代化。人民生活更加美好，人的全面发展、全体人民共同富裕取得更为明显的实质性进展。

第二节 “十四五”时期经济社会发展主要目标

--经济发展取得新成效。发展是解决我国一切问题的基础和关键，发展必须坚持新发展理念，在质量效益明显提升的基础上实现经济持续健康发展，增长潜力充分发挥，国内生产总值年均增长保持在合理区间、各年度视情提出，全员劳动生产率增长高于国内生产总值增长，国内市场更加强大，经济结构更加优化，创新能力显著提升，全社会研发经费投入年均增长7%以上、力争投入强度高于“十三五”时期实际，产业基础高级化、产业链现代化水平明显提高，农业基础更加稳固，城乡区域发展协调性明显增强，常住人口城镇化率提高到65%，现代化经济体系建设取得重大进展。

--改革开放迈出新步伐。社会主义市场经济体制更加完善，高标准市场体系基本建成，市场主体更加充满活力，产权制度改革和要素市场化配置改革取得重大进展，公平竞争制度更加健全，更高水平开放型经济新体制基本形成。

--社会文明程度得到新提高。社会主义核心价值观深入人心，人民思想道德素质、科学文化素质和身心健康素质明显提高，公共文化服务体系和文化产业体

系更加健全，人民精神文化生活日益丰富，中华文化影响力进一步提升，中华民族凝聚力进一步增强。

--生态文明建设实现新进步。国土空间开发保护格局得到优化，生产生活方式绿色转型成效显著，能源资源配置更加合理、利用效率大幅提高，单位国内生产总值能源消耗和二氧化碳排放分别降低13.5%、18%，主要污染物排放总量持续减少，森林覆盖率提高到24.1%，生态环境持续改善，生态安全屏障更加牢固，城乡人居环境明显改善。

--民生福祉达到新水平。实现更加充分更高质量就业，城镇调查失业率控制在5.5%以内，居民人均可支配收入增长与国内生产总值增长基本同步，分配结构明显改善，基本公共服务均等化水平明显提高，全民受教育程度不断提升，劳动年龄人口平均受教育年限提高到11.3年，多层次社会保障体系更加健全，基本养老保险参保率提高到95%，卫生健康体系更加完善，人均预期寿命提高1岁，脱贫攻坚成果巩固拓展，乡村振兴战略全面推进，全体人民共同富裕迈出坚实步伐。

--国家治理效能得到新提升。社会主义民主法治更加健全，社会公平正义进一步彰显，国家行政体系更加完善，政府作用更好发挥，行政效率和公信力显著提升，社会治理特别是基层治理水平明显提高，防范化解重大风险体制机制不断健全，突发公共事件应急处置能力显著增强，自然灾害防御水平明显提升，发展安全保障更加有力，国防和军队现代化迈出重大步伐。

专栏1 “十四五”时期经济社会发展主要指标					
类别	指标	2020 年	2025 年	年均/累计	属性
经济发展	1.国内生产总值（GDP）增长（%）	2.3	—	保持在合理区间、各年度视情提出	预期性
	2.全员劳动生产率增长（%）	2.5	—	高于GDP增长	预期性
	3.常住人口城镇化率（%）	60.6 ^②	65	—	预期性
创新驱动	4.全社会研发经费投入增长（%）	—	—	>7，力争投入强度高于“十三五”时期实际	预期性
	5.每万人口高价值发明专利拥有量（件）	6.3	12	—	预期性
	6.数字经济核心产业增加值占GDP比重（%）	7.8	10	—	预期性
民生福祉	7.居民人均可支配收入增长（%）	2.1	—	与GDP增长基本同步	预期性
	8.城镇调查失业率（%）	5.2	—	<5.5	预期性
	9.劳动年龄人口平均受教育年限（年）	10.8	11.3	—	约束性
	10.每千人口拥有执业（助理）医师数（人）	2.9	3.2	—	预期性
	11.基本养老保险参保率（%）	91	95	—	预期性
	12.每千人口拥有3岁以下婴幼儿托位数（个）	1.8	4.5	—	预期性
	13.人均预期寿命（岁）	77.3 ^③	—	（1）	预期性
绿色生态	14.单位GDP能源消耗降低（%）	—	—	（13.5）	约束性
	15.单位GDP二氧化碳排放降低（%）	—	—	（18）	约束性
	16.地级及以上城市空气质量优良天数比率（%）	87	87.5	—	约束性
	17.地表水达到或好于Ⅲ类水体比例（%）	83.4	85	—	约束性
安全保障	18.森林覆盖率（%）	23.2 ^④	24.1	—	约束性
	19.粮食综合生产能力（亿吨）	—	>6.5	—	约束性
	20.能源综合生产能力（亿吨标准煤）	—	>46	—	约束性

注：①（1）内为5年累计数。②带*的为2019年数据。③能源综合生产能力指煤炭、石油、天然气、非化石能源生产能力之和。④2020年地级及以上城市空气质量优良天数比率和地表水达到或好于Ⅲ类水体比例指标值受新冠肺炎疫情等因素影响，明显高于正常年份。⑤2020年全员劳动生产率增长2.5%为预计数。

第二篇 坚持创新驱动发展 全面塑造发展新优势

坚持创新在我国现代化建设全局中的核心地位，把科技自立自强作为国家发展的战略支撑，面向世界科技前沿、面向经济主战场、面向国家重大需求、面向人民生命健康，深入实施科教兴国战略、人才强国战略、创新驱动发展战略，完善国家创新体系，加快建设科技强国。

第四章 强化国家战略科技力量

制定科技强国行动纲要，健全社会主义市场经济条件下新型举国体制，打好关键核心技术攻坚战，提高创新链整体效能。

第一节 整合优化科技资源配置

以国家战略性需求为导向推进创新体系优化组合，加快构建以国家实验室为引领的战略科技力量。聚焦量子信息、光子与微纳电子、网络通信、人工智能、生物医药、现代能源系统等重大创新领域组建一批国家实验室，重组国家重点实验室，形成结构合理、运行高效的实验室体系。优化提升国家工程研究中心、国家技术创新中心等创新基地。推进科研院所、高等院校和企业科研力量优化配置和资源共享。支持发展新型研究型大学、新型研发机构等新型创新主体，推动投入主体多元化、管理制度现代化、运行机制市场化、用人机制灵活化。

第二节 加强原创性引领性科技攻关

在事关国家安全和发展的基础核心领域，制定实施战略性科学计划和科学工程。瞄准人工智能、量子信息、集成电路、生命健康、脑科学、生物育种、空天科技、深地深海等前沿领域，实施一批具有前瞻性、战略性的国家重大科技项目。从国家急迫需要和长远需求出发，集中优势资源攻关新发突发传染病和生物安全风险防控、医药和医疗设备、关键元器件零部件和基础材料、油气勘探开发等领域关键核心技术。

专栏2 科技前沿领域攻关	
01 新一代人工智能	前沿基础理论突破，专用芯片研发，深度学习框架等开源算法平台构建，学习推理与决策、图像图形、语音视频、自然语言识别处理等领域创新。
02 量子信息	域域、域际、自由空间量子通信技术研发，通用量子计算原型机和实用化量子模拟机研制，量子精密测量技术突破。
03 集成电路	集成电路设计工具，重点装备和高纯靶材等关键材料研发，集成电路先进工艺和绝缘栅双极型晶体管（IGBT）、微机电系统（MEMS）等特色工艺突破，先进存储技术升级，碳化硅、氮化镓等宽禁带半导体发展。
04 脑科学与类脑研究	脑认知原理解析，脑介观神经联接图谱绘制，脑重大疾病机理与干预研究，儿童青少年脑智发育，类脑计算与脑机融合技术研发。
05 基因与生物技术	基因组学研究应用，遗传细胞和遗传育种、合成生物、生物药等技术创新，创新疫苗、体外诊断、抗体药物等研发，农作物、畜禽水产、农业微生物等重大新品种创制，生物安全关键技术研创。
06 临床医学与健康	癌症和心脑血管、呼吸、代谢性疾病等发病机制基础研究，主动健康干预技术研发，再生医学、微生物组、新型治疗等前沿技术研发，重大传染病，重大慢性非传染性疾病预防关键技术研究。
07 深空深地深海和极地探测	宇宙起源与演化、透视地球等基础科学研究，火星环绕、小行星巡视等星际探测，新一代重型运载火箭和重复使用航天运输系统、地球深部探测装备，深海运维保障和装备试验型，极地立体观测监测平台和重型破冰船等研制，探月工程四期、蛟龙探海二期、雪龙探极二期建设。

第三节 持之以恒加强基础研究

强化应用研究带动，鼓励自由探索，制定实施基础研究十年行动方案，重点布局一批基础学科研究中心。加大基础研究财政投入力度、优化支出结构，对企业投入基础研究实行税收优惠，鼓励社会以捐赠和建立基金等方式多渠道投入，形成持续稳定投入机制，基础研究经费投入占研发经费投入比重提高到8%以上。建立健全符合科学规律的评价体系和激励机制，对基础研究探索实行长周期评价，创造有利于基础研究的良好科研生态。

第四节 建设重大科技创新平台

支持北京、上海、粤港澳大湾区形成国际科技创新中心，建设北京怀柔、上海张江、大湾区、安徽合肥综合性国家科学中心，支持有条件的地方建设区域科技创新中心。强化国家自主创新示范区、高新技术产业开发区、经济技术开发区等创新功能。适度超前布局国家重大科技基础设施，提高共享水平和使用效率。集约化建设自然科技资源库、国家野外科学观测研究站（网）和科学大数据中心。加强高端科研仪器设备研发制造。构建国家科研论文和科技信息高端交流平台。

专栏3 国家重大科技基础设施	
01 战略导向型	建设空间环境地基监测网、高精度地基授时系统、大型低速风洞、海底科学观测网、空间环境地面模拟装置、聚变堆主机关键系统综合研究设施等。
02 应用支撑型	建设高能同步辐射光源、高效低碳燃气轮机试验装置、超重力离心模拟与试验装置、加速器驱动嬗变研究装置、未来网络试验设施等。
03 前瞻引领型	建设硬X射线自由电子激光装置、高海拔宇宙线观测站、综合极端条件实验装置、散裂中子源、地下核反应堆本底前沿物理实验设施、精密重力测量研究设施、强流重离子加速器装置等。
04 民生改善型	建设转化医学研究设施、多模态跨尺度生物医学成像设施、模式动物表型与遗传研究设施、地震科学实验场、地球系统数值模拟器等。

第五章 提升企业技术创新能力

完善技术创新市场导向机制，强化企业创新主体地位，促进各类创新要素向企业集聚，形成以企业为主体、市场为导向、产学研用深度融合的技术创新体系。

第一节 激励企业加大研发投入

实施更大力度的研发费用加计扣除、高新技术企业税收优惠等普惠性政策。拓展优化首台（套）重大技术装备保险补偿和激励政策，发挥重大工程牵引示范作用，运用政府采购政策支持创新产品和服务。通过完善标准、质量和竞争规制等措施，增强企业创新动力。健全鼓励国有企业研发的考核制度，设立独立核算、免于增值保值考核、容错纠错的研发准备金制度，确保中央国有工业企业研发支出年增长率明显超过全国平均水平。完善激励科技型中小企业创新的税收优惠政

策。

第二节 支持产业共性基础技术研发

集中力量整合提升一批关键共性技术平台，支持行业龙头企业联合高等院校、科研院所和行业上下游企业共建国家产业创新中心，承担国家重大科技项目。支持有条件企业联合转制科研院所组建行业研究院，提供公益性共性技术服务。打造新型共性技术平台，解决跨行业跨领域关键共性技术问题。发挥大企业引领支撑作用，支持创新型中小微企业成长为创新重要发源地，推动产业链上中下游、大中小企业融通创新。鼓励有条件地方依托产业集群创办混合所有制产业技术研究院，服务区域关键共性技术研发。

第三节 完善企业创新服务体系

推动国家科研平台、科技报告、科研数据进一步向企业开放，创新科技成果转化机制，鼓励将符合条件的由财政资金支持形成的科技成果许可给中小企业使用。推进创新创业机构改革，建设专业化市场化技术转移机构和技术经理人队伍。完善金融支持创新体系，鼓励金融机构发展知识产权质押融资、科技保险等科技金融产品，开展科技成果转化贷款风险补偿试点。畅通科技型企业国内上市融资渠道，增强科创板“硬科技”特色，提升创业板服务成长型创新创业企业功能，鼓励发展天使投资、创业投资，更好发挥创业投资引导基金和私募股权基金作用。

第六章 激发人才创新活力

贯彻尊重劳动、尊重知识、尊重人才、尊重创造方针，深化人才发展体制机制改革，全方位培养、引进、用好人才，充分发挥人才第一资源的作用。

第一节 培养造就高水平人才队伍

遵循人才成长规律和科研活动规律，培养造就更多国际一流的战略科技人才、科技领军人才和创新团队，培养具有国际竞争力的青年科技人才后备军，注重依托重大科技任务和重大创新基地培养发现人才，支持设立博士后创新岗位。加强创新型、应用型、技能型人才培养，实施知识更新工程、技能提升行动，壮大高水平工程师和高技能人才队伍。加强基础学科拔尖学生培养，建设数理化生

等基础学科基地和前沿科学中心。实行更加开放的人才政策，构筑集聚国内外优秀人才的科研创新高地。完善外籍高端人才和专业人才来华工作、科研、交流的停居留政策，完善外国人在华永久居留制度，探索建立技术移民制度。健全薪酬福利、子女教育、社会保障、税收优惠等制度，为海外科学家在华工作提供具有国际竞争力和吸引力的环境。

第二节 激励人才更好发挥作用

完善人才评价和激励机制，健全以创新能力、质量、实效、贡献为导向的科技人才评价体系，构建充分体现知识、技术等创新要素价值的收益分配机制。选好用好领军人才和拔尖人才，赋予更大技术路线决定权和经费使用权。全方位为科研人员松绑，拓展科研管理“绿色通道”。实行以增加知识价值为导向的分配政策，完善科研人员职务发明成果权益分享机制，探索赋予科研人员职务科技成果所有权或长期使用权，提高科研人员收益分享比例。深化院士制度改革。

第三节 优化创新创业创造生态

大力弘扬新时代科学家精神，强化科研诚信建设，健全科技伦理体系。依法保护企业家的财产权和创新收益，发挥企业家在把握创新方向、凝聚人才、筹措资金等方面重要作用。推进创新创业创造向纵深发展，优化双创示范基地建设布局。倡导敬业、精益、专注、宽容失败的创新创业文化，完善试错容错纠错机制。弘扬科学精神和工匠精神，广泛开展科学普及活动，加强青少年科学兴趣引导和培养，形成热爱科学、崇尚创新的社会氛围，提高全民科学素质。

第七章 完善科技创新体制机制

深入推进科技体制改革，完善国家科技治理体系，优化国家科技计划体系和运行机制，推动重点领域项目、基地、人才、资金一体化配置。

第一节 深化科技管理体制改革

加快科技管理职能转变，强化规划政策引导和创新环境营造，减少分钱分物定项目等直接干预。整合财政科研投入体制，重点投向战略性关键性领域，改变部门分割、小而散的状态。改革重大科技项目立项和组织管理方式，给予科研单

位和科研人员更多自主权，推行技术总师负责制，实行“揭榜挂帅”、“赛马”等制度，健全奖补结合的资金支持机制。健全科技评价机制，完善自由探索型和任务导向型科技项目分类评价制度，建立非共识科技项目的评价机制，优化科技奖励项目。建立健全科研机构现代院所制度，支持科研事业单位试行更灵活的编制、岗位、薪酬等管理制度。建立健全高等院校、科研机构、企业间创新资源自由有序流动机制。深入推进全面创新改革试验。

第二节 健全知识产权保护运用体制

实施知识产权强国战略，实行严格的知识产权保护制度，完善知识产权相关法律法规，加快新领域新业态知识产权立法。加强知识产权司法保护和行政执法，健全仲裁、调解、公证和维权援助体系，健全知识产权侵权惩罚性赔偿制度，加大损害赔偿力度。优化专利资助奖励政策和考核评价机制，更好保护和激励高价值专利，培育专利密集型产业。改革国有知识产权归属和权益分配机制，扩大科研机构和高等院校知识产权处置自主权。完善无形资产评估制度，形成激励与监管相协调的管理机制。构建知识产权保护运用公共服务平台。

第三节 积极促进科技开放合作

实施更加开放包容、互惠共享的国际科技合作战略，更加主动融入全球创新网络。务实推进全球疫情防控和公共卫生等领域国际科技合作，聚焦气候变化、人类健康等问题加强同各国科研人员联合研发。主动设计和牵头发起国际大科学计划和大科学工程，发挥科学基金独特作用。加大国家科技计划对外开放力度，启动一批重大科技合作项目，研究设立面向全球的科学研究基金，实施科学家交流计划。支持在我国境内设立国际科技组织、外籍科学家在我国科技学术组织任职。

第三篇 加快发展现代产业体系 巩固壮大实体经济根基

坚持把发展经济着力点放在实体经济上，加快推进制造强国、质量强国建设，促进先进制造业和现代服务业深度融合，强化基础设施支撑引领作用，构建实体经济、科技创新、现代金融、人力资源协同发展的现代产业体系。

第八章 深入实施制造强国战略

坚持自主可控、安全高效，推进产业基础高级化、产业链现代化，保持制造业比重基本稳定，增强制造业竞争优势，推动制造业高质量发展。

第一节 加强产业基础能力建设

实施产业基础再造工程，加快补齐基础零部件及元器件、基础软件、基础材料、基础工艺和产业技术基础等瓶颈短板。依托行业龙头企业，加大重要产品和关键核心技术攻关力度，加快工程化产业化突破。实施重大技术装备攻关工程，完善激励和风险补偿机制，推动首台（套）装备、首批次材料、首版次软件示范应用。健全产业基础支撑体系，在重点领域布局一批国家制造业创新中心，完善国家质量基础设施，建设生产应用示范平台和标准计量、认证认可、检验检测、试验验证等产业技术基础公共服务平台，完善技术、工艺等工业基础数据库。

第二节 提升产业链供应链现代化水平

坚持经济性和安全性相结合，补齐短板、锻造长板，分行业做好供应链战略设计和精准施策，形成具有更强创新力、更高附加值、更安全可靠的产业链供应链。推进制造业补链强链，强化资源、技术、装备支撑，加强国际产业安全合作，推动产业链供应链多元化。立足产业规模优势、配套优势和部分领域先发优势，巩固提升高铁、电力装备、新能源、船舶等领域全产业链竞争力，从符合未来产业变革方向的整机产品入手打造战略性全局性产业链。优化区域产业链布局，引导产业链关键环节留在国内，强化中西部和东北地区承接产业转移能力建设。实施应急产品生产能力储备工程，建设区域性应急物资生产保障基地。实施领航企业培育工程，培育一批具有生态主导力和核心竞争力的龙头企业。推动中小企业提升专业化优势，培育专精特新“小巨人”企业和制造业单项冠军企业。加强技术经济安全评估，实施产业竞争力调查和评价工程。

第三节 推动制造业优化升级

深入实施智能制造和绿色制造工程，发展服务型制造新模式，推动制造业高端化智能化绿色化。培育先进制造业集群，推动集成电路、航空航天、船舶与海洋工程装备、机器人、先进轨道交通装备、先进电力装备、工程机械、高端数控机床、医药及医疗设备等产业创新发展。改造提升传统产业，推动石化、钢铁、

有色、建材等原材料产业布局优化和结构调整，扩大轻工、纺织等优质产品供给，加快化工、造纸等重点行业企业改造升级，完善绿色制造体系。深入实施增强制造业核心竞争力和技术改造专项，鼓励企业应用先进适用技术、加强设备更新和新产品规模化应用。建设智能制造示范工厂，完善智能制造标准体系。深入实施质量提升行动，推动制造业产品“增品种、提品质、创品牌”。

第四节 实施制造业降本减负行动

强化要素保障和高效服务，巩固拓展减税降费成果，降低企业生产经营成本，提升制造业根植性和竞争力。推动工业用地提容增效，推广新型产业用地模式。扩大制造业中长期贷款、信用贷款规模，增加技改贷款，推动股权投资、债券融资等向制造业倾斜。允许制造业企业全部参与电力市场化交易，规范和降低港口航运、公路铁路运输等物流收费，全面清理规范涉企收费。建立制造业重大项目全周期服务机制和企业家参与涉企政策制定制度，支持建设中小企业信息、技术、进出口和数字化转型综合性服务平台。

专栏4 制造业核心竞争力提升	
01	高端新材料 推动高端稀土功能材料，高品质特殊钢材，高性能合金、高温合金、高纯稀有金属材料、高性能陶瓷、电子玻璃等先进金属和无机非金属材料取得突破，加强碳纤维、芳纶等高性能纤维及其复合材料，生物基和生物医用材料研发应用，加快茂金属聚乙烯等高性能树脂和集成电路用光刻胶等电子高纯材料关键技术突破。
02	重大技术装备 推进CR450高速度等级中国标准动车组，谱系化中国标准地铁列车、高端机床装备、先进工程机械、核电机组关键部件、邮轮、大型LNG船舶和深海油气生产平台等研发应用，推动C919大型客机示范运营和ARJ21支线客机系列化发展。
03	智能制造与机器人技术 重点研制分散式控制系统、可编程逻辑控制器、数据采集和传输监控系统等工业控制装备，突破先进控制器、高精度伺服驱动系统、高性能减速器等智能机器人关键技术，发展增材制造。
04	航空发动机及燃气轮机 加快先进航空发动机关键材料研发验证，推进民用大涵道比涡扇发动机CJ1000产品研制，突破宽体客机发动机关键技术，实现先进民用涡轴发动机产业化，建设上海重型燃气轮机试验电站。
05	北斗产业化应用 突破通信导航一体化融合等技术，建设北斗应用产业创新平台，在通信、金融、能源、民航等行业开展典型示范，推动北斗在车载导航、智能手机、穿戴设备等领域市场化规模化应用。
06	新能源汽车和智能（网联）汽车 突破新能源汽车高安全动力电池、高效驱动电机、高性能动力系统等关键技术，加快研发智能（网联）汽车基础技术平台及软硬件系统、线控底盘和智能终端等关键部件。
07	高端医疗装备和创新药 突破腔镜手术机器人、体外膜肺氧合机等核心技术，研制高端影像、放射治疗等大型医疗设备及其关键零部件，发展起搏器、全降解血管支架等植入介入产品，推动康复辅助器具提质升级，研发重大传染性疾病所需疫苗，开发治疗恶性肿瘤、心脑血管等疾病特效药，加强中药药关键技术装备研发。
08	农业机械装备 开发智能大功率拖拉机、精量（免耕）播种机、喷杆喷雾机、深松施肥机、高效联合收割机、果蔬采收机、甘蔗收获机、采棉机等先进适用农业机械，发展丘陵山区农业生产高效专用农机，推动先进粮油加工装备研发和产业化，研发绿色智能养殖饲喂、环控、粪集、粪污利用等设施，研发造林种菜等机械装备。

第九章 发展壮大战略性新兴产业

着眼于抢占未来产业发展先机，培育先导性和支柱性产业，推动战略性新兴产业融合化、集群化、生态化发展，战略性新兴产业增加值占GDP比重超过17%。

第一节 构筑产业体系新支柱

聚焦新一代信息技术、生物技术、新能源、新材料、高端装备、新能源汽车、绿色环保以及航空航天、海洋装备等战略性新兴产业，加快关键核心技术创新应用，增强要素保障能力，培育壮大产业发展新动能。推动生物技术和信息技术融合创新，加快发展生物医药、生物育种、生物材料、生物能源等产业，做大做强生物经济。深化北斗系统推广应用，推动北斗产业高质量发展。深入推进国家战略性新兴产业集群发展工程，健全产业集群组织管理和专业化推进机制，建设创新和公共服务综合体，构建一批各具特色、优势互补、结构合理的战略性新兴产业增长引擎。鼓励技术创新和企业兼并重组，防止低水平重复建设。发挥产业投资基金引导作用，加大融资担保和风险补偿力度。

第二节 前瞻谋划未来产业

在类脑智能、量子信息、基因技术、未来网络、深海空天开发、氢能与储能等前沿科技和产业变革领域，组织实施未来产业孵化与加速计划，谋划布局一批未来产业。在科教资源优势突出、产业基础雄厚的地区，布局一批国家未来产业技术研究院，加强前沿技术多路径探索、交叉融合和颠覆性技术供给。实施产业跨界融合示范工程，打造未来技术应用场景，加速形成若干未来产业。

第十章 促进服务业繁荣发展

聚焦产业转型升级和居民消费升级需要，扩大服务业有效供给，提高服务效率和服务品质，构建优质高效、结构优化、竞争力强的服务产业新体系。

第一节 推动生产性服务业融合化发展

以服务制造业高质量发展为导向，推动生产性服务业向专业化和价值链高端延伸。聚焦提高产业创新力，加快发展研发设计、工业设计、商务咨询、检验检测认证等服务。聚焦提高要素配置效率，推动供应链金融、信息数据、人力资源

等服务创新发展。聚焦增强全产业链优势，提高现代物流、采购分销、生产控制、运营管理、售后服务等发展水平。推动现代服务业与先进制造业、现代农业深度融合，深化业务关联、链条延伸、技术渗透，支持智能制造系统解决方案、流程再造等新型专业化服务机构发展。培育具有国际竞争力的服务企业。

第二节 加快生活性服务业品质化发展

以提升便利度和改善服务体验为导向，推动生活性服务业向高品质和多样化升级。加快发展健康、养老、托育、文化、旅游、体育、物业等服务业，加强公益性、基础性服务业供给，扩大覆盖全生命期的各类服务供给。持续推动家政服务业提质扩容，与智慧社区、养老托育等融合发展。鼓励商贸流通业态与模式创新，推进数字化智能化改造和跨界融合，线上线下全渠道满足消费需求。加快完善养老、家政等服务标准，健全生活性服务业认证认可制度，推动生活性服务业诚信化职业化发展。

第三节 深化服务领域改革开放

扩大服务业对内对外开放，进一步放宽市场准入，全面清理不合理的限制条件，鼓励社会力量扩大多元化多层次服务供给。完善支持服务业发展的政策体系，创新适应服务新业态新模式和产业融合发展需要的土地、财税、金融、价格等政策。健全服务质量标准体系，强化标准贯彻执行和推广。加快制定重点服务领域监管目录、流程和标准，构建高效协同的服务业监管体系。完善服务领域人才职称评定制度，鼓励从业人员参加职业技能培训和鉴定。深入推进服务业综合改革试点和扩大开放。

第十一章 建设现代化基础设施体系

统筹推进传统基础设施和新型基础设施建设，打造系统完备、高效实用、智能绿色、安全可靠的现代化基础设施体系。

第一节 加快建设新型基础设施

围绕强化数字转型、智能升级、融合创新支撑，布局建设信息基础设施、融合基础设施、创新基础设施等新型基础设施。建设高速泛在、天地一体、集成互

联、安全高效的信息基础设施，增强数据感知、传输、存储和运算能力。加快5G网络规模化部署，用户普及率提高到56%，推广升级千兆光纤网络。前瞻布局6G网络技术储备。扩容骨干网互联节点，新设一批国际通信出入口，全面推进互联网协议第六版（IPv6）商用部署。实施中西部地区中小城市基础网络完善工程。推动物联网全面发展，打造支持固移融合、宽窄结合的物联接入能力。加快构建全国一体化大数据中心体系，强化算力统筹智能调度，建设若干国家枢纽节点和大数据中心集群，建设E级和10E级超级计算中心。积极稳妥发展工业互联网和车联网。打造全球覆盖、高效运行的通信、导航、遥感空间基础设施体系，建设商业航天发射场。加快交通、能源、市政等传统基础设施数字化改造，加强泛在感知、终端联网、智能调度体系建设。发挥市场主导作用，打通多元化投资渠道，构建新型基础设施标准体系。

第二节 加快建设交通强国

建设现代化综合交通运输体系，推进各种运输方式一体化融合发展，提高网络效应和运营效率。完善综合运输大通道，加强出疆入藏、中西部地区、沿江沿海沿边战略骨干通道建设，有序推进能力紧张通道升级扩容，加强与周边国家互联互通。构建快速网，基本贯通“八纵八横”高速铁路，提升国家高速公路网络质量，加快建设世界级港口群和机场群。完善干线网，加快普速铁路建设和既有铁路电气化改造，优化铁路客货布局，推进普通国省道瓶颈路段贯通升级，推动内河高等级航道扩能升级，稳步建设支线机场、通用机场和货运机场，积极发展通用航空。加强邮政设施建设，实施快递“进村进厂出海”工程。推进城市群都市圈交通一体化，加快城际铁路、市域（郊）铁路建设，构建高速公路环线系统，有序推进城市轨道交通发展。提高交通通达深度，推动区域性铁路建设，加快沿边抵边公路建设，继续推进“四好农村路”建设，完善道路安全设施。构建多层次、一体化综合交通枢纽体系，优化枢纽场站布局、促进集约综合开发，完善集疏运系统，发展旅客联程运输和货物多式联运，推广全程“一站式”、“一单制”服务。推进中欧班列集结中心建设。深入推进铁路企业改革，全面深化空管体制改革，推动公路收费制度和养护体制改革。

专栏5 交通基础设施建设	
01 战略骨干通道	建设川藏铁路雅安至林定段和伊宁至阿克苏、酒泉至格尔木、若羌至罗布泊等铁路，推进日喀则至吉隆、和田至日喀则铁路前期工作，打通沿边公路G219和G331线，提质改造川藏公路G318线。
02 新建铁路	建设成都重庆至上海沿江高铁、上海经宁波至台州沿海高铁、京沪高铁辅助通道天津至新沂段和北京经雄安新区至商丘、西安至重庆、长沙至赣州、包头至银川等高铁。
03 普速铁路	建设西部陆海新通道黄桶至百色、黔桂增建二线铁路和瑞金至梅州、中卫经平凉至庆阳、柳州至广州铁路，推进玉溪至墨江、大理至瑞丽等与周边互联互通铁路建设，提升铁路集装箱运输能力，推进中欧班列运输通道和口岸扩能改造，建设大型工矿企业、物流园区和重点港口铁路专用线，全面实现长江干线主要港口铁路进港。
04 城市群和都市圈轨道交通	新增城际铁路和市域（郊）铁路运营里程3000公里，基本建成京津冀、长三角、粤港澳大湾区轨道交通网。新增城市轨道交通运营里程3000公里。
05 高速公路	实施京沪、京港澳、长深、沪昆、连霍等国家高速公路主线扩容改造，加快建设国家高速公路主线并行线、联络线，推进京雄等雄安新区高速公路建设。规划布局建设充换电设施。新改建高速公路里程2.5万公里。
06 港航设施	建设京津冀、长三角、粤港澳大湾区世界级港口群，建设洋山港区小洋山北侧、天津北疆港区C段、广州南沙港五期、深圳盐田港区等集装箱码头，推进曹妃甸港煤炭运能扩容，青山江海联运服务中心和北部湾国际门户港、洋浦枢纽港建设。深化三峡水运新通道前期论证，研究平陆运河等碍水航运河连通工程。
07 现代化机场	建设京津冀、长三角、粤港澳大湾区、成渝世界级机场群，实施广州、深圳、昆明、西安、重庆、乌鲁木齐、哈尔滨等国际枢纽机场和杭州、合肥、济南、长沙、南宁等区域枢纽机场改扩建工程，建设厦门、大连、三亚新机场。建成鄂州专业性货运机场，建设杭州、嘉兴、瑞金、黔北、阿拉尔等支线机场，新增民用运输机场30个以上。
08 综合交通和物流枢纽	推进既有客运枢纽一体化智能化升级改造和站城融合，实施枢纽机场引入轨道交通工程。推进120个左右国家物流枢纽建设。加快邮政国际寄递中心建设。

第三节 构建现代能源体系

推进能源革命，建设清洁低碳、安全高效的能源体系，提高能源供给保障能力。加快发展非化石能源，坚持集中式和分布式并举，大力提升风电、光伏发电规模，加快发展东中部分布式能源，有序发展海上风电，加快西南水电基地建设，安全稳妥推动沿海核电建设，建设一批多能互补的清洁能源基地，非化石能源占能源消费总量比重提高到20%左右。推动煤炭生产向资源富集地区集中，合理控制煤电建设规模和发展节奏，推进以电代煤。有序放开油气勘探开发市场准入，加快深海、深层和非常规油气资源利用，推动油气增储上产。因地制宜开发利用地热能。提高特高压输电通道利用率。加快电网基础设施智能化改造和智能微电网建设，提高电力系统互补互济和智能调节能力，加强源网荷储衔接，提升清洁能源消纳和存储能力，提升向边远地区输配电能力，推进煤电灵活性改造，加快抽水蓄能电站建设和新型储能技术规模化应用。完善煤炭跨区域运输通道和集疏运体系，加快建设天然气主干管道，完善油气互联互通网络。

专栏6 现代能源体系建设工程	
01	大型清洁能源基地 建设雅鲁藏布江下游水电基地。建设金沙江上下游、雅鲁江流域、黄河上游和几字湾、河西走廊、新疆、冀北、松辽等清洁能源基地。建设广东、福建、浙江、江苏、山东等海上风电基地。
02	沿海核电 建成华龙一号、国和一号、高温气冷堆示范工程，积极有序推进沿海三代核电建设。推动模块化小型堆、60万千瓦级商用高温气冷堆、海上浮动式核动力平台等先进堆型示范。建设核电站中低放废物处置场，建设乏燃料后处理厂。开展山东海阳等核能综合利用示范。核电运行装机容量达到7000万千瓦。
03	电力外送通道 建设白鹤滩至华东、金沙江上游外送等特高压输电通道，实施闽粤联网、川渝特高压交流工程。研究论证陇东至山东、哈密至重庆等特高压输电通道。
04	电力系统调节 建设桐城、磐安、泰安二期、浑源、庄河、安化、贵阳、南宁等抽水蓄能电站。实施电化学、压缩空气、飞轮等储能示范项目。开展黄河梯级电站大型储能项目研究。
05	油气储运能力 新建中俄东线境内段，川气东送二线等油气管道。建设石油储备重大工程。加快中原文23、辽河储气库群等地下储气库建设。

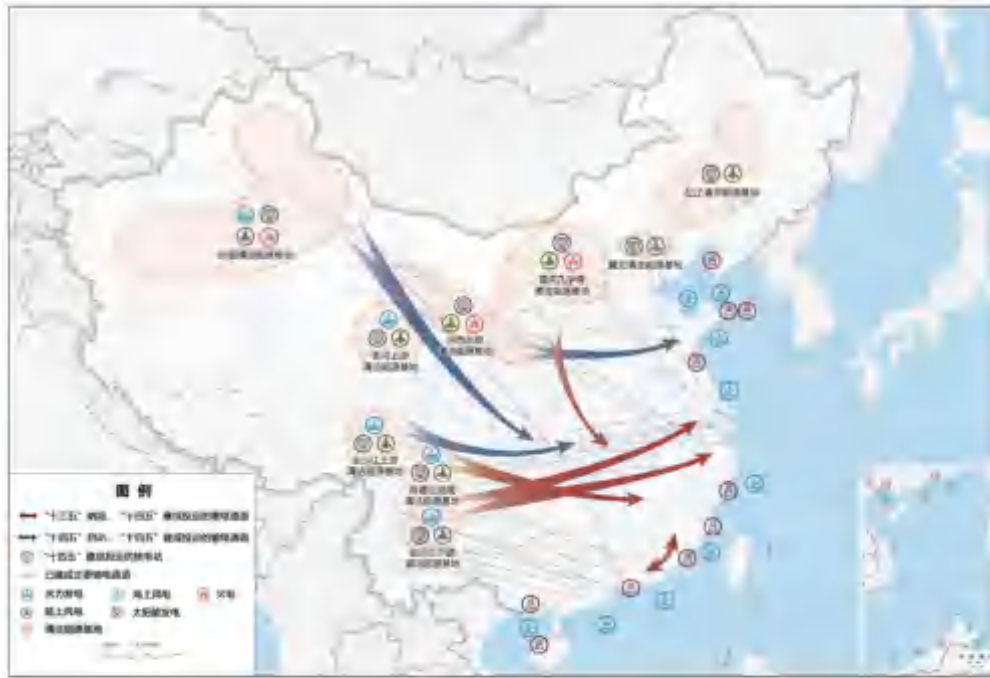


图1 “十四五”大型清洁能源基地布局示意图

第四节 加强水利基础设施建设

立足流域整体和水资源空间均衡配置，加强跨行政区河流水系治理保护和骨干工程建设，强化大中小微水利设施协调配套，提升水资源优化配置和水旱灾害防御能力。坚持节水优先，完善水资源配置体系，建设水资源配置骨干项目，加强重点水源和城市应急备用水源工程建设。实施防洪提升工程，解决防汛薄弱环节，加快防洪控制性枢纽工程建设和中小河流治理、病险水库除险加固，全面推进堤防和蓄滞洪区建设。加强水源涵养区保护修复，加大重点河湖保护和综合治理力度，恢复水清岸绿的水生态体系。

专栏 7 国家水网骨干工程	
01 重大引调水	推动南水北调东中线后续工程建设，深化南水北调西线工程方案比选论证。建设珠三鲁水资源配置、渝西水资源配置、引江济淮、滇中引水、引汉济渭、新疆奎屯河引水、河北雄安千渠供水、海南琼西北水资源配置等工程。加快引黄济宁、黑龙江三江连通、环北鄱湖水资源配置工程前期论证。
02 供水灌溉	推进新疆库东干、黑龙江关门嘴子、贵州观音、湖南大木塘、浙江开化、广西长塘等大型水库建设。实施黄河河套、四川郫江堰、安徽淝河等大中型灌区续建配套和现代化改造。推进四川向家坝、云南耿马、安徽怀洪新河、海南牛路岭、江西大塘等大中型灌区建设。
03 防洪减灾	建设雄安新区防洪工程、长江中下游崩岸治理和重要蓄滞洪区、黄河干流河道和滩区综合治理、淮河入海水道二期、海河河道治理、西江干流堤防、太湖吴淞江、海南琼海水利枢纽等工程。加强黄河古贤水利枢纽、福建上白石水库等工程前期论证。

第四篇 形成强大国内市场 构建新发展格局

坚持扩大内需这个战略基点，加快培育完整内需体系，把实施扩大内需战略同深化供给侧结构性改革有机结合起来，以创新驱动、高质量供给引领和创造新需求，加快构建以国内大循环为主体、国内国际双循环相互促进的新发展格局。

第十二章 畅通国内大循环

依托强大国内市场，贯通生产、分配、流通、消费各环节，形成需求牵引供给、供给创造需求的更高水平动态平衡，促进国民经济良性循环。

第一节 提升供给体系适配性

深化供给侧结构性改革，提高供给适应引领创造新需求能力。适应个性化、差异化、品质化消费需求，推动生产模式和产业组织方式创新，持续扩大优质消费品、中高端产品供给和教育、医疗、养老等服务供给，提升产品和服务质量和客户满意度，推动供需协调匹配。优化提升供给结构，促进农业、制造业、服务业、能源资源等产业协调发展。完善产业配套体系，加快自然垄断行业竞争性环节市场化，实现上下游、产供销有效衔接。健全市场化法治化化解过剩产能长效机制，完善企业兼并重组法律法规和配套政策。建立健全质量分级制度，加快标准升级

迭代和国际标准转化应用。开展中国品牌创建行动，保护发展中华老字号，提升自主品牌影响力和竞争力，率先在化妆品、服装、家纺、电子产品等消费品领域培育一批高端品牌。

第二节 促进资源要素顺畅流动

破除制约要素合理流动的堵点，矫正资源要素失衡错配，从源头上畅通国民经济循环。提高金融服务实体经济能力，健全实体经济中长期资金供给制度安排，创新直达实体经济的金融产品和服务，增强多层次资本市场融资功能。实施房地产市场平稳健康发展长效机制，促进房地产与实体经济均衡发展。有效提升劳动者技能，提高就业质量和收入水平，形成人力资本提升和产业转型升级良性循环。健全城乡要素自由流动机制，构建区域产业梯度转移格局，促进城乡区域良性互动。

第三节 强化流通体系支撑作用

深化流通体制改革，畅通商品服务流通渠道，提升流通效率，降低全社会交易成本。加快构建国内统一大市场，对标国际先进规则和最佳实践优化市场环境，促进不同地区和行业标准、规则、政策协调统一，有效破除地方保护、行业垄断和市场分割。建设现代物流体系，加快发展冷链物流，统筹物流枢纽设施、骨干线路、区域分拨中心和末端配送节点建设，完善国家物流枢纽、骨干冷链物流基地设施条件，健全县乡村三级物流配送体系，发展高铁快运等铁路快捷货运产品，加强国际航空货运能力建设，提升国际海运竞争力。优化国际物流通道，加快形成内外联通、安全高效的物流网络。完善现代商贸流通体系，培育一批具有全球竞争力的现代流通企业，支持便利店、农贸市场等商贸流通设施改造升级，发展无接触交易服务，加强商贸流通标准化建设和绿色发展。加快建立储备充足、反应迅速、抗冲击能力强的应急物流体系。

第四节 完善促进国内大循环的政策体系

保持合理的财政支出力度和赤字率水平，完善减税降费政策，构建有利于企业扩大投资、增加研发投入、调节收入分配、减轻消费者负担的税收制度。保持流动性合理充裕，保持货币供应量和社会融资规模增速同名义经济增速基本匹

配，创新结构性政策工具，引导金融机构加大对重点领域和薄弱环节支持力度，规范发展消费信贷。推动产业政策向普惠化和功能性转型，强化竞争政策基础性地位，支持技术创新和结构升级。健全与经济发展水平相适应的收入分配、社会保障和公共服务制度。

第十三章 促进国内国际双循环

立足国内大循环，协同推进强大国内市场和贸易强国建设，形成全球资源要素强大引力场，促进内需和外需、进口和出口、引进外资和对外投资协调发展，加快培育参与国际合作和竞争新优势。

第一节 推动进出口协同发展

完善内外贸一体化调控体系，促进内外贸法律法规、监管体制、经营资质、质量标准、检验检疫、认证认可等相衔接，推进同线同标同质。降低进口关税和制度性成本，扩大优质消费品、先进技术、重要设备、能源资源等进口，促进进口来源多元化。完善出口政策，优化出口商品质量和结构，稳步提高出口附加值。优化国际市场布局，引导企业深耕传统出口市场、拓展新兴市场，扩大与周边国家贸易规模，稳定国际市场份额。推动加工贸易转型升级，深化外贸转型升级基地、海关特殊监管区域、贸易促进平台、国际营销服务网络建设，加快发展跨境电商、市场采购贸易等新模式，鼓励建设海外仓，保障外贸产业链供应链畅通运转。创新发展服务贸易，推进服务贸易创新发展试点开放平台建设，提升贸易数字化水平。实施贸易投资融合工程。办好中国国际进口博览会、中国进出口商品交易会、中国国际服务贸易交易会等展会。

第二节 提高国际双向投资水平

坚持引进来和走出去并重，以高水平双向投资高效利用全球资源要素和市场空间，完善产业链供应链保障机制，推动产业竞争力提升。更大力度吸引和利用外资，有序推进电信、互联网、教育、文化、医疗等领域相关业务开放。全面优化外商投资服务，加强外商投资促进和保护，发挥重大外资项目示范效应，支持外资加大中高端制造、高新技术、传统制造转型升级、现代服务等领域和中西部地区投资，支持外资企业设立研发中心和参与承担国家科技计划项目。鼓励外资

企业利润再投资。坚持企业主体，创新境外投资方式，优化境外投资结构和布局，提升风险防范能力和收益水平。完善境外生产服务网络和流通体系，加快金融、咨询、会计、法律等生产性服务业国际化发展，推动中国产品、服务、技术、品牌、标准走出去。支持企业融入全球产业链供应链，提高跨国经营能力和水平。引导企业加强合规管理，防范化解境外政治、经济、安全等各类风险。推进多双边投资合作机制建设，健全促进和保障境外投资政策和服务体系，推动境外投资立法。

第十四章 加快培育完整内需体系

深入实施扩大内需战略，增强消费对经济发展的基础性作用和投资对优化供给结构的关键性作用，建设消费和投资需求旺盛的强大国内市场。

第一节 全面促进消费

顺应居民消费升级趋势，把扩大消费同改善人民生活品质结合起来，促进消费向绿色、健康、安全发展，稳步提高居民消费水平。提升传统消费，加快推动汽车等消费品由购买管理向使用管理转变，健全强制报废制度和废旧家电、消费电子等耐用消费品回收处理体系，促进住房消费健康发展。培育新型消费，发展信息消费、数字消费、绿色消费，鼓励定制、体验、智能、时尚消费等新模式新业态发展。发展服务消费，放宽服务消费领域市场准入，推动教育培训、医疗健康、养老托育、文旅体育等消费提质扩容，加快线上线下融合发展。适当增加公共消费，提高公共服务支出效率。扩大节假日消费，完善节假日制度，全面落实带薪休假制度。培育建设国际消费中心城市，打造一批区域消费中心。完善城乡融合消费网络，扩大电子商务进农村覆盖面，改善县域消费环境，推动农村消费梯次升级。完善市内免税店政策，规划建设一批中国特色市内免税店。采取增加居民收入与减负并举等措施，不断扩大中等收入群体，持续释放消费潜力。强化消费者权益保护，完善质量标准和后评价体系，健全缺陷产品召回、产品伤害监测、产品质量担保等制度，完善多元化消费维权机制和纠纷解决机制。

第二节 拓展投资空间

优化投资结构，提高投资效率，保持投资合理增长。加快补齐基础设施、市

政工程、农业农村、公共安全、生态环保、公共卫生、物资储备、防灾减灾、民生保障等领域短板，推动企业设备更新和技术改造，扩大战略性新兴产业投资。推进既促消费惠民生又调结构增后劲的新型基础设施、新型城镇化、交通水利等重大工程建设。面向服务国家重大战略，实施川藏铁路、西部陆海新通道、国家水网、雅鲁藏布江下游水电开发、星际探测、北斗产业化等重大工程，推进重大科研设施、重大生态系统保护修复、公共卫生应急保障、重大引调水、防洪减灾、送电输气、沿边沿江沿海交通等一批强基础、增功能、利长远的重大项目建设。深化投融资体制改革，发挥政府投资撬动作用，激发民间投资活力，形成市场主导的投资内生增长机制。健全项目谋划、储备、推进机制，加大资金、用地等要素保障力度，加快投资项目落地见效。规范有序推进政府和社会资本合作（PPP），推动基础设施领域不动产投资信托基金（REITs）健康发展，有效盘活存量资产，形成存量资产和新增投资的良性循环。

第五篇 加快数字化发展 建设数字中国

迎接数字时代，激活数据要素潜能，推进网络强国建设，加快建设数字经济、数字社会、数字政府，以数字化转型整体驱动生产方式、生活方式和治理方式变革。

第十五章 打造数字经济新优势

充分发挥海量数据和丰富应用场景优势，促进数字技术与实体经济深度融合，赋能传统产业转型升级，催生新产业新业态新模式，壮大经济发展新引擎。

第一节 加强关键数字技术创新应用

聚焦高端芯片、操作系统、人工智能关键算法、传感器等关键领域，加快推进基础理论、基础算法、装备材料等研发突破与迭代应用。加强通用处理器、云计算系统和软件核心技术一体化研发。加快布局量子计算、量子通信、神经芯片、DNA存储等前沿技术，加强信息科学与生命科学、材料等基础学科的交叉创新，支持数字技术开源社区等创新联合体发展，完善开源知识产权和法律体系，鼓励企业开放软件源代码、硬件设计和应用服务。

第二节 加快推动数字产业化

培育壮大人工智能、大数据、区块链、云计算、网络安全等新兴数字产业，提升通信设备、核心电子元器件、关键软件等产业水平。构建基于5G的应用场景和产业生态，在智能交通、智慧物流、智慧能源、智慧医疗等重点领域开展试点示范。鼓励企业开放搜索、电商、社交等数据，发展第三方大数据服务产业。促进共享经济、平台经济健康发展。

第三节 推进产业数字化转型

实施“上云用数赋智”行动，推动数据赋能全产业链协同转型。在重点行业和区域建设若干国际水准的工业互联网平台和数字化转型促进中心，深化研发设计、生产制造、经营管理、市场服务等环节的数字化应用，培育发展个性定制、柔性制造等新模式，加快产业园区数字化改造。深入推进服务业数字化转型，培育众包设计、智慧物流、新零售等新增长点。加快发展智慧农业，推进农业生产经营和管理服务数字化改造。

专栏8 数字经济重点产业	
01 云计算	加快云操作系统迭代升级,推动超大规模分布式存储、弹性计算、数据虚拟隔离等技术创新,提高云安全水平。以混合云为重点培育行业解决方案、系统集成、运维管理等云服务产业。
02 大数据	推动大数据采集、清洗、存储、挖掘、分析、可视化解法等技术创新,培育数据采集、标注、存储、传输、管理、应用等全生命周期产业体系,完善大数据标准体系。
03 物联网	推动传感器、网络切片、高精度定位等技术创新,协同发展云服务与边缘计算服务,培育车联网、医疗物联网、家居物联网产业。
04 工业互联网	打造自主可控的标识解析体系、标准体系、安全管理体系,加强工业软件研发应用,培育形成具有国际影响力的工业互联网平台,推进“工业互联网+智能制造”产业生态建设。
05 区块链	推动智能合约、共识算法、加密算法、分布式系统等区块链技术创新,以联盟链为重点发展区块链服务平台和金融科技、供应链管理、政务服务等领域应用方案,完善监管机制。
06 人工智能	建设重点行业人工智能数据集,发展算法推理训练场景,推进智能医疗装备、智能运载工具、智能识别系统等智能产品设计与制造,推动通用化和行业性人工智能开放平台建设。
07 虚拟现实和增强现实	推动三维图形生成、动态环境建模、实时动作捕捉、快速渲染处理等技术创新,发展虚拟现实整机、感知交互、内容采集制作等设备和开发工具软件,行业解决方案。

第十六章 加快数字社会建设步伐

适应数字技术全面融入社会交往和日常生活新趋势,促进公共服务和社会运行方式创新,构筑全民畅享的数字生活。

第一节 提供智慧便捷的公共服务

聚焦教育、医疗、养老、抚幼、就业、文体、助残等重点领域,推动数字化服务普惠应用,持续提升群众获得感。推进学校、医院、养老院等公共服务机构资源数字化,加大开放共享和应用力度。推进线上线下公共服务共同发展、深度

融合，积极发展在线课堂、互联网医院、智慧图书馆等，支持高水平公共服务机构对接基层、边远和欠发达地区，扩大优质公共服务资源辐射覆盖范围。加强智慧法院建设。鼓励社会力量参与“互联网+公共服务”，创新提供服务模式和产品。

第二节 建设智慧城市和数字乡村

以数字化助推城乡发展和治理模式创新，全面提高运行效率和宜居度。分级分类推进新型智慧城市建设，将物联网感知设施、通信系统等纳入公共基础设施统一规划建设，推进市政公用设施、建筑等物联网应用和智能化改造。完善城市信息模型平台和运行管理服务平台，构建城市数据资源体系，推进城市数据大脑建设。探索建设数字孪生城市。加快推进数字乡村建设，构建面向农业农村的综合信息服务体系，建立涉农信息普惠服务机制，推动乡村管理服务数字化。

第三节 构筑美好数字生活新图景

推动购物消费、居家生活、旅游休闲、交通出行等各类场景数字化，打造智慧共享、和睦共治的新型数字生活。推进智慧社区建设，依托社区数字化平台和线下社区服务机构，建设便民惠民智慧服务圈，提供线上线下融合的社区生活服务、社区治理及公共服务、智能小区等服务。丰富数字生活体验，发展数字家庭。加强全民数字技能教育和培训，普及提升公民数字素养。加快信息无障碍建设，帮助老年人、残疾人等共享数字生活。

第十七章 提高数字政府建设水平

将数字技术广泛应用于政府管理服务，推动政府治理流程再造和模式优化，不断提高决策科学性和服务效率。

第一节 加强公共数据开放共享

建立健全国家公共数据资源体系，确保公共数据安全，推进数据跨部门、跨层级、跨地区汇聚融合和深度利用。健全数据资源目录和责任清单制度，提升国家数据共享交换平台功能，深化国家人口、法人、空间地理等基础信息资源共享利用。扩大基础公共信息数据安全有序开放，探索将公共数据服务纳入公共服务

体系，构建统一的国家公共数据开放平台和开发利用端口，优先推动企业登记监管、卫生、交通、气象等高价值数据集向社会开放。开展政府数据授权运营试点，鼓励第三方深化对公共数据的挖掘利用。

第二节 推动政务信息化共建共用

加大政务信息化建设统筹力度，健全政务信息化项目清单，持续深化政务信息系统整合，布局建设执政能力、依法治国、经济治理、市场监管、公共安全、生态环境等重大信息系统，提升跨部门协同治理能力。完善国家电子政务网络，集约建设政务云平台和数据中心体系，推进政务信息系统云迁移。加强政务信息化建设快速迭代，增强政务信息系统快速部署能力和弹性扩展能力。

第三节 提高数字化政务服务效能

全面推进政府运行方式、业务流程和服务模式数字化智能化。深化“互联网+政务服务”，提升全流程一体化在线服务平台功能。加快构建数字技术辅助政府决策机制，提高基于高频大数据精准动态监测预测预警水平。强化数字技术在公共卫生、自然灾害、事故灾难、社会安全等突发公共事件应对中的运用，全面提升预警和应急处置能力。

第十八章 营造良好数字生态

坚持放管并重，促进发展与规范管理相统一，构建数字规则体系，营造开放、健康、安全的数字生态。

第一节 建立健全数据要素市场规则

统筹数据开发利用、隐私保护和公共安全，加快建立数据资源产权、交易流通、跨境传输和安全保护等基础制度和标准规范。建立健全数据产权交易和行业自律机制，培育规范的数据交易平台和市场主体，发展数据资产评估、登记结算、交易撮合、争议仲裁等市场运营体系。加强涉及国家利益、商业秘密、个人隐私的数据保护，加快推进数据安全、个人信息保护等领域基础性立法，强化数据资源全生命周期安全保护。完善适用于大数据环境下的数据分类分级保护制度。加强数据安全评估，推动数据跨境安全有序流动。

第二节 营造规范有序的政策环境

构建与数字经济发展相适应的政策法规体系。健全共享经济、平台经济和新个体经济管理规范，清理不合理的行政许可、资质资格事项，支持平台企业创新发展、增强国际竞争力。依法依规加强互联网平台经济监管，明确平台企业定位和监管规则，完善垄断认定法律规范，打击垄断和不正当竞争行为。探索建立无人驾驶、在线医疗、金融科技、智能配送等监管框架，完善相关法律法规和伦理审查规则。健全数字经济统计监测体系。

第三节 加强网络安全保护

健全国家网络安全法律法规和制度标准，加强重要领域数据资源、重要网络和信息系统安全保障。建立健全关键信息基础设施保护体系，提升安全防护和维护政治安全能力。加强网络安全风险评估和审查。加强网络安全基础设施建设，强化跨领域网络安全信息共享和工作协同，提升网络安全威胁发现、监测预警、应急指挥、攻击溯源能力。加强网络安全关键技术研发，加快人工智能安全技术创新，提升网络安全产业综合竞争力。加强网络安全宣传教育和人才培养。

第四节 推动构建网络空间命运共同体

推进网络空间国际交流与合作，推动以联合国为主渠道、以联合国宪章为基本原则制定数字和网络空间国际规则。推动建立多边、民主、透明的全球互联网治理体系，建立更加公平合理的网络基础设施和资源治理机制。积极参与数据安全、数字货币、数字税等国际规则和数字技术标准制定。推动全球网络安全保障合作机制建设，构建保护数据要素、处置网络安全事件、打击网络犯罪的国际协调合作机制。向欠发达国家提供技术、设备、服务等数字援助，使各国共享数字时代红利。积极推进网络文化交流互鉴。

专栏9 数字化应用场景	
01 智能交通	发展自动驾驶和车路协同的出行服务。推广公路智能管理、交通信号联动、公交优先通行控制。建设智能铁路、智慧民航、智慧港口、数字航道、智慧停车场。
02 智慧能源	推动煤矿、油气田、电厂等智能化升级，开展用能信息广泛采集，能效在线分析，实现源网荷储互动、多能协同互补，用能需求智能调控。
03 智能制造	促进设备联网、生产环节数字化连接和供应链协同响应，推进生产数据贯通化、制造柔性化、产品个性化、管理智能化。
04 智慧农业及水利	推广大田作物精准播种、精准施肥施药、精准收获，推动设施园艺、畜禽水产养殖智能化应用。构建智慧水利体系，以流域为单元提升水情监测和智能调度能力。
05 智慧教育	推动社会化高质量在线课程资源纳入公共教学体系，推进优质教育资源在线辐射农村和边远地区薄弱学校，发展场景式、体验式学习和智能化教育管理评价。
06 智慧医疗	完善电子健康档案和病历、电子处方等数据库，加快医疗卫生机构数据共享。推广远程医疗，推进医学影像辅助诊断、临床辅助诊断等应用。运用大数据提升对医疗机构和医疗行为的监管能力。
07 智慧文旅	推动景区、博物馆等发展线上数字化体验产品，建设景区监测设施和大数据平台，发展沉浸式体验、虚拟展厅、高清直播等新型文旅服务。
08 智慧社区	推动政务服务平台、社区感知设施和家庭终端联通，发展智能预警、应急救援救助和智慧养老等社区惠民服务，建立无人物流配送体系。
09 智慧家居	应用感应控制、语音控制、远程控制等技术手段，发展智能家电、智能照明、智能安防监控、智能音箱、新型穿戴设备、服务机器人等。
10 智慧政务	推进政务服务一网通办，推广应用电子证照、电子合同、电子签章、电子发票、电子档案，健全政务服务“好差评”评价体系。

第六篇 全面深化改革 构建高水平社会主义市场经济体制

坚持和完善社会主义基本经济制度，充分发挥市场在资源配置中的决定性作

用，更好发挥政府作用，推动有效市场和有为政府更好结合。

第十九章 激发各类市场主体活力

毫不动摇巩固和发展公有制经济，毫不动摇鼓励、支持、引导非公有制经济发展，培育更有活力、创造力和竞争力的市场主体。

第一节 加快国有经济布局优化和结构调整

围绕服务国家战略，坚持有进有退、有所为有所不为，加快国有经济布局优化、结构调整和战略性重组，增强国有经济竞争力、创新力、控制力、影响力、抗风险能力，做强做优做大国有资本和国有企业。发挥国有经济战略支撑作用，推动国有经济进一步聚焦战略安全、产业引领、国计民生、公共服务等功能，调整盘活存量资产，优化增量资本配置，向关系国家安全、国民经济命脉的重要行业集中，向提供公共服务、应急能力建设和公益性等关系国计民生的重要行业集中，向前瞻性战略性新兴产业集中。对充分竞争领域的国有经济，强化资本收益目标和财务硬约束，增强流动性，完善国有资本优化配置机制。建立布局结构调整长效机制，动态发布国有经济布局优化和结构调整指引。

第二节 推动国有企业完善中国特色现代企业制度

坚持党对国有企业的全面领导，促进加强党的领导和完善公司治理相统一，加快建立权责法定、权责透明、协调运转、有效制衡的公司治理机制。加强董事会建设，落实董事会职权，使董事会成为企业经营决策主体。按照完善治理、强化激励、突出主业、提高效率的要求，深化国有企业混合所有制改革，深度转换经营机制，对混合所有制企业探索实行有别于国有独资、全资公司的治理机制和监管制度。推行经理层成员任期制和契约化管理，完善市场化薪酬分配机制，灵活开展多种形式的中长期激励。

第三节 健全管资本为主的国有资产监管体制

坚持授权与监管相结合、放活与管好相统一，大力推进国资监管理念、重点、方式等多方位转变。优化管资本方式，全面实行清单管理，深入开展分类授权放权，注重通过法人治理结构履职，加强事中事后监管。深化国有资本投资、运营

公司改革，科学合理界定政府及国资监管机构，国有资本投资、运营公司和所持企业的权利边界。健全协同高效的监督机制，严格责任追究，切实防止国有资产流失。加快推进经营性国有资产集中统一监管。

第四节 优化民营企业发展环境

健全支持民营企业发展的法治环境、政策环境和市场环境，依法平等保护民营企业产权和企业家权益。保障民营企业依法平等使用资源要素、公开公平公正参与竞争、同等受到法律保护。进一步放宽民营企业市场准入，破除招投标等领域各种壁垒。创新金融支持民营企业政策工具，健全融资增信支持体系，对民营企业信用评级、发债一视同仁，降低综合融资成本。完善促进中小微企业和个体工商户发展的政策体系，加大税费优惠和信贷支持力度。构建亲清政商关系，建立规范化政企沟通渠道。健全防范和化解拖欠中小企业账款长效机制。

第五节 促进民营企业高质量发展

鼓励民营企业改革创新，提升经营能力和管理水平。引导有条件的民营企业建立现代企业制度。支持民营企业开展基础研究和科技创新、参与关键核心技术研发和国家重大科技项目攻关。完善民营企业参与国家重大战略实施机制。推动民营企业守法合规经营，鼓励民营企业积极履行社会责任、参与社会公益和慈善事业。弘扬企业家精神，实施年轻一代民营企业健康成长促进计划。

第二十章 建设高标准市场体系

实施高标准市场体系建设行动，健全市场体系基础制度，坚持平等准入、公正监管、开放有序、诚信守法，形成高效规范、公平竞争的统一大市场。

第一节 全面完善产权制度

健全归属清晰、权责明确、保护严格、流转顺畅的现代产权制度。实施民法典，制修订物权、债权、股权等产权法律法规，明晰产权归属、完善产权权能。健全以公平为原则的产权保护制度，依法平等保护国有、民营、外资等各种所有制企业产权。健全产权执法司法保护制度，完善涉企产权案件申诉、复核、重审等保护机制，推动涉企冤错案件依法甄别纠正常态化机制化，畅通涉政府产权纠

纷反映和处理渠道。加强数据、知识、环境等领域产权制度建设，健全自然资源资产产权制度和法律法规。

第二节 推进要素市场化配置改革

建立健全城乡统一的建设用地市场，统筹推进农村土地征收、集体经营性建设用地入市、宅基地制度改革。改革土地计划管理方式，赋予省级政府更大用地自主权，探索建立全国性的建设用地、补充耕地指标跨区域交易机制。建立不同产业用地类型合理转换机制，增加混合产业用地供给。健全统一规范的人力资源市场体系，破除劳动力和人才在城乡、区域和不同所有制单位间的流动障碍，减少人事档案管理中的不合理限制。发展技术和数据要素市场。健全要素市场运行机制，完善交易规则和服务体系。深化公共资源交易平台整合共享。

第三节 强化竞争政策基础地位

坚持鼓励竞争、反对垄断，完善竞争政策框架，构建覆盖事前、事中、事后全环节的竞争政策实施机制。统筹做好增量审查与存量清理，强化公平竞争审查制度的刚性约束，完善公平竞争审查细则，持续清理废除妨碍全国统一市场和公平竞争的规定及做法。完善市场竞争状况评估制度，建立投诉举报和处理回应机制。加大反垄断和反不正当竞争执法司法力度，防止资本无序扩张。推进能源、铁路、电信、公用事业等行业竞争性环节市场化改革，放开竞争性业务准入，进一步引入市场竞争机制，加强对自然垄断业务的监管。

第四节 健全社会信用体系

建立健全信用法律法规和标准体系，制定公共信用信息目录和失信惩戒措施清单，完善失信主体信用修复机制。推广信用承诺制度。加强信用信息归集、共享、公开和应用，推广惠民便企信用产品与服务。建立公共信用信息和金融信息的共享整合机制。培育具有国际竞争力的企业征信机构和信用评级机构，加强征信监管，推动信用服务市场健康发展。加强信用信息安全管理，保障信用主体合法权益。建立健全政府失信责任追究制度。

第二十一章 建立现代财税金融体制

更好发挥财政在国家治理中的基础和重要支柱作用，增强金融服务实体经济能力，健全符合高质量发展要求的财税金融制度。

第一节 加快建立现代财政制度

深化预算管理制度改革，强化对预算编制的宏观指导和审查监督。加强财政资源统筹，推进财政支出标准化，强化预算约束和绩效管理。完善跨年度预算平衡机制，加强中期财政规划管理，增强国家重大战略任务财力保障。建立权责清晰、财力协调、区域均衡的中央和地方财政关系，适当加强中央在知识产权保护、养老保险、跨区域生态环境保护等方面事权，减少并规范中央和地方共同事权。健全省以下财政体制，增强基层公共服务保障能力。完善财政转移支付制度，优化转移支付结构，规范转移支付项目。完善权责发生制政府综合财务报告制度。建立健全规范的政府举债融资机制。

第二节 完善现代税收制度

优化税制结构，健全直接税体系，适当提高直接税比重。完善个人所得税制度，推进扩大综合征收范围，优化税率结构。聚焦支持稳定制造业、巩固产业链供应链，进一步优化增值税制度。调整优化消费税征收范围和税率，推进征收环节后移并稳步下划地方。规范完善税收优惠。推进房地产税立法，健全地方税体系，逐步扩大地方税政管理权。深化税收征管制度改革，建设智慧税务，推动税收征管现代化。

第三节 深化金融供给侧结构性改革

健全具有高度适应性、竞争力、普惠性的现代金融体系，构建金融有效支持实体经济的体制机制。建设现代中央银行制度，完善货币供应调控机制。稳妥推进数字货币研发。健全市场化利率形成和传导机制，完善央行政策利率体系，更好发挥贷款市场报价利率基准作用。优化金融体系结构，深化国有商业银行改革，加快完善中小银行和农村信用社治理结构，规范发展非银行金融机构，增强金融普惠性。改革优化政策性金融，强化服务国家战略和规划能力。深化保险公司改革，提高商业保险保障能力。健全金融机构公司治理，强化股东股权和关联交易监管。完善资本市场基础制度，健全多层次资本市场体系，大力发展机构投资者，

提高直接融资特别是股权融资比重。全面实行股票发行注册制，建立常态化退市机制，提高上市公司质量。深化新三板改革。完善市场化债券发行机制，稳步扩大债券市场规模，丰富债券品种，发行长期国债和基础设施长期债券。完善投资者保护制度和存款保险制度。完善现代金融监管体系，补齐监管制度短板，在审慎监管前提下有序推进金融创新，健全风险全覆盖监管框架，提高金融监管透明度和法治化水平。稳妥发展金融科技，加快金融机构数字化转型。强化监管科技运用和金融创新风险评估，探索建立创新产品纠偏和暂停机制。

第二十二章 提升政府经济治理能力

加快转变政府职能，建设职责明确、依法行政的政府治理体系，创新和完善宏观调控，提高政府治理效能。

第一节 完善宏观经济治理

健全以国家发展规划为战略导向，以财政政策和货币政策为主要手段，就业、产业、投资、消费、环保、区域等政策紧密配合，目标优化、分工合理、高效协同的宏观经济治理体系。增强国家发展规划对公共预算、国土开发、资源配置等政策的宏观引导、统筹协调功能，健全宏观政策制定和执行机制，重视预期管理和引导，合理把握经济增长、就业、价格、国际收支等调控目标，在区间调控基础上加强定向调控、相机调控和精准调控。完善宏观调控政策体系，搞好跨周期政策设计，提高逆周期调节能力，促进经济总量平衡、结构优化、内外均衡。加强宏观经济治理数据库等建设，提升大数据等现代技术手段辅助治理能力，推进统计现代化改革。健全宏观经济政策评估评价制度和重大风险识别预警机制，畅通政策制定参与渠道，提高决策科学化、民主化、法治化水平。

第二节 构建一流营商环境

深化简政放权、放管结合、优化服务改革，全面实行政府权责清单制度，持续优化市场化法治化国际化营商环境。实施全国统一的[市场准入负面清单](#)制度，破除清单之外隐性准入壁垒，以服务业为重点进一步放宽准入限制。精简行政许可事项，减少归并资质资格许可，取消不必要的备案登记和年检认定，规范涉企检查。全面推行“证照分离”、“照后减证”改革，全面开展工程建设项目审批

制度改革。改革生产许可制度，简化工业产品审批程序，实施涉企经营许可事项清单管理。建立便利、高效、有序的市场主体退出制度，简化普通注销程序，建立健全企业破产和自然人破产制度。创新政务服务方式，推进审批服务便民化。深化国际贸易“单一窗口”建设。完善营商环境评价体系。

第三节 推进监管能力现代化

健全以“双随机、一公开”监管和“互联网+监管”为基本手段、以重点监管为补充、以信用监管为基础的新型监管机制，推进线上线下一体化监管。严格市场监管、质量监管、安全监管，加强对食品药品、特种设备和网络交易、旅游、广告、中介、物业等的监管，强化要素市场交易监管，对新产业新业态实施包容审慎监管。深化市场监管综合行政执法改革，完善跨领域跨部门联动执法、协同监管机制。深化行业协会、商会和中介机构改革。加强社会公众、新闻媒体监督。

第七篇 坚持农业农村优先发展 全面推进乡村振兴

走中国特色社会主义乡村振兴道路，全面实施乡村振兴战略，强化以工补农、以城带乡，推动形成工农互促、城乡互补、协调发展、共同繁荣的新型工农城乡关系，加快农业农村现代化。

第二十三章 提高农业质量效益和竞争力

持续强化农业基础地位，深化农业供给侧结构性改革，强化质量导向，推动乡村产业振兴。

第一节 增强农业综合生产能力

夯实粮食生产能力基础，保障粮、棉、油、糖、肉、奶等重要农产品供给安全。坚持最严格的耕地保护制度，强化耕地数量保护和质量提升，严守18亿亩耕地红线，遏制耕地“非农化”、防止“非粮化”，规范耕地占补平衡，严禁占优补劣、占水田补旱地。以粮食生产功能区和重要农产品生产保护区为重点，建设国家粮食安全产业带，实施高标准农田建设工程，建成10.75亿亩集中连片高标准农田。实施黑土地保护工程，加强东北黑土地保护和地力恢复。推进大中型灌区节水改造和精细化管理，建设节水灌溉骨干工程，同步推进水价综合改革。加强

大中型、智能化、复合型农业机械研发应用，农作物耕种收综合机械化率提高到75%。加强种质资源保护利用和种子库建设，确保种源安全。加强农业良种技术攻关，有序推进生物育种产业化应用，培育具有国际竞争力的种业龙头企业。完善农业科技创新体系，创新农技推广服务方式，建设智慧农业。加强动物防疫和农作物病虫害防治，强化农业气象服务。



图2 粮食生产功能区和重要农产品生产保护区布局示意图

第二节 深化农业结构调整

优化农业生产布局，建设优势农产品产业带和特色农产品优势区。推进粮经饲统筹、农林牧渔协调，优化种植业结构，大力发展现代畜牧业，促进水产生态健康养殖。积极发展设施农业，因地制宜发展林果业。深入推进优质粮食工程。推进农业绿色转型，加强产地环境保护治理，发展节水农业和旱作农业，深入实施农药化肥减量行动，治理农膜污染，提升农膜回收利用率，推进秸秆综合利用和畜禽粪污资源化利用。完善绿色农业标准体系，加强绿色食品、有机农产品和地理标志农产品认证管理。强化全过程农产品质量安全监管，健全追溯体系。建设现代农业产业园区和农业现代化示范区。

第三节 丰富乡村经济业态

发展县域经济，推进农村一二三产业融合发展，延长农业产业链条，发展各

具特色的现代乡村富民产业。推动种养加结合和产业链再造，提高农产品加工业和农业生产性服务业发展水平，壮大休闲农业、乡村旅游、民宿经济等特色产业。加强农产品仓储保鲜和冷链物流设施建设，健全农村产权交易、商贸流通、检验检测认证等平台 and 智能标准厂房等设施，引导农村二三产业集聚发展。完善利益联结机制，通过“资源变资产、资金变股金、农民变股东”，让农民更多分享产业增值收益。

第二十四章 实施乡村建设行动

把乡村建设摆在社会主义现代化建设的重要位置，优化生产生活生态空间，持续改善村容村貌和人居环境，建设美丽宜居乡村。

第一节 强化乡村建设的规划引领

统筹县域城镇和村庄规划建设，通盘考虑土地利用、产业发展、居民点建设、人居环境整治、生态保护、防灾减灾和历史文化传承。科学编制县域村庄布局规划，因地制宜、分类推进村庄建设，规范开展全域土地综合整治，保护传统村落、民族村寨和乡村风貌，严禁随意撤并村庄搞大社区、违背农民意愿大拆大建。优化布局乡村生活空间，严格保护农业生产空间和乡村生态空间，科学划定养殖业适养、限养、禁养区域。鼓励有条件地区编制实用性村庄规划。

第二节 提升乡村基础设施和公共服务水平

以县域为基本单元推进城乡融合发展，强化县城综合服务能力和乡镇服务农民功能。健全城乡基础设施统一规划、统一建设、统一管护机制，推动市政公用设施向郊区乡村和规模较大中心镇延伸，完善乡村水、电、路、气、邮政通信、广播电视、物流等基础设施，提升农房建设质量。推进城乡基本公共服务标准统一、制度并轨，增加农村教育、医疗、养老、文化等服务供给，推进县域内教师医生交流轮岗，鼓励社会力量兴办农村公益事业。提高农民科技文化素质，推动乡村人才振兴。

第三节 改善农村人居环境

开展农村人居环境整治提升行动，稳步解决“垃圾围村”和乡村黑臭水体等

突出环境问题。推进农村生活垃圾就地分类和资源化利用，以乡镇政府驻地和中心村为重点梯次推进农村生活污水治理。支持因地制宜推进农村厕所革命。推进农村水系综合整治。深入开展村庄清洁和绿化行动，实现村庄公共空间及庭院房屋、村庄周边干净整洁。

专栏 10 现代农业农村建设工程	
01 高标准农田	新建高标准农田 2.75 亿亩，其中新增高效节水灌溉面积 0.6 亿亩。实施东北地区 1.4 亿亩黑土地保护性耕作。
02 现代种业	建设国家农作物种质资源长期库、种质资源中期库，提升海南、甘肃、四川等国家繁育制种基地水平，建设黑龙江大豆等区域性育种基地。新建、改扩建国家畜禽和水产品种质资源库、保种场（区）、基因库，推进国家级畜禽核心育种场建设。
03 农业机械化	创建 300 个农作物生产全程机械化示范县，建设 300 个设施农业和规模养殖全程机械化示范县，推进农机深松整地和丘陵山区农田宜机化改造。
04 动物防疫和农作物病虫害防治	提升动物疫病国家参考实验室和病原学监测区域中心设施条件，改善牧区动物防疫专用设施和基层动物疫苗冷藏设施，建设动物防疫指定通道和病死动物无害化处理场，分省建设农作物病虫害监测中心和病虫害应急防治中心、农药风险防控中心，建设林草病虫害防治中心。
05 农业面源污染治理	在长江、黄河等重点流域环境敏感区建设 200 个农业面源污染综合治理示范县，继续推进畜禽养殖粪污资源化利用，在水产养殖主产区推进养殖尾水治理。
06 农产品冷链物流设施	建设 30 个全国性和 70 个区域性农产品骨干冷链物流基地，提升田头市场仓储保鲜设施，改造畜禽定点屠宰加工厂冷链储藏和运输设施。
07 乡村基础设施	因地制宜推动自然村通硬化路，加强村组道路和村内道路建设，推进农村水源保护和供水保障工程建设，升级改造农村电网，提升农村宽带网络水平，强化运行管护。
08 农村人居环境整治提升	有序推进经济欠发达地区以及高海拔、寒冷、缺水地区的农村改厕。支持 600 个县整县推进人居环境整治，建设农村生活垃圾和污水处理设施。

第二十五章 健全城乡融合发展体制机制

建立健全城乡要素平等交换、双向流动政策体系，促进要素更多向乡村流动，增强农业农村发展活力。

第一节 深化农业农村改革

巩固完善农村基本经营制度，落实第二轮土地承包到期后再延长30年政策，完善农村承包地所有权、承包权、经营权分置制度，进一步放活经营权。发展多种形式适度规模经营，加快培育家庭农场、农民合作社等新型农业经营主体，健全农业专业化社会化服务体系，实现小农户和现代农业有机衔接。深化农村宅基地制度改革试点，加快房地一体的宅基地确权颁证，探索宅基地所有权、资格权、使用权分置实现形式。积极探索实施农村集体经营性建设用地入市制度。允许农村集体在农民自愿前提下，依法把有偿收回的闲置宅基地、废弃的集体公益性建设用地转变为集体经营性建设用地入市。建立土地征收公共利益认定机制，缩小土地征收范围。深化农村集体产权制度改革，完善产权权能，将经营性资产量化到集体经济组织成员，发展壮大新型农村集体经济。切实减轻村级组织负担。发挥国家城乡融合发展试验区、农村改革试验区示范带动作用。

第二节 加强农业农村发展要素保障

健全农业农村投入保障制度，加大中央财政转移支付、土地出让收入、地方政府债券支持农业农村力度。健全农业支持保护制度，完善粮食主产区利益补偿机制，构建新型农业补贴政策体系，完善粮食最低收购价政策。深化供销合作社改革。完善农村用地保障机制，保障设施农业和乡村产业发展合理用地需求。健全农村金融服务体系，完善金融支农激励机制，扩大农村资产抵押担保融资范围，发展农业保险。允许入乡就业创业人员在原籍地或就业创业地落户并享受相关权益，建立科研人员入乡兼职兼薪和离岗创业制度。

第二十六章 实现巩固拓展脱贫攻坚成果同乡村振兴有效衔接

建立完善农村低收入人口和欠发达地区帮扶机制，保持主要帮扶政策和财政投入力度总体稳定，接续推进脱贫地区发展。

第一节 巩固提升脱贫攻坚成果

严格落实“摘帽不摘责任、摘帽不摘政策、摘帽不摘帮扶、摘帽不摘监管”要求，建立健全巩固拓展脱贫攻坚成果长效机制。健全防止返贫动态监测和精准帮扶机制，对易返贫致贫人口实施常态化监测，建立健全快速发现和响应机制，分层分类及时纳入帮扶政策范围。完善农村社会保障和救助制度，健全农村低收入人口常态化帮扶机制。对脱贫地区继续实施城乡建设用地增减挂钩节余指标省内交易政策、调整完善跨省域交易政策。加强扶贫项目资金资产管理和监督，推动特色产业可持续发展。推广以工代赈方式，带动低收入人口就地就近就业。做好易地扶贫搬迁后续帮扶，加强大型搬迁安置区新型城镇化建设。

第二节 提升脱贫地区整体发展水平

实施脱贫地区特色种养业提升行动，广泛开展农产品产销对接活动，深化拓展消费帮扶。在西部地区脱贫县中集中支持一批乡村振兴重点帮扶县，从财政、金融、土地、人才、基础设施、公共服务等方面给予集中支持，增强其巩固脱贫成果及内生发展能力。坚持和完善东西部协作和对口支援、中央单位定点帮扶、社会力量参与帮扶等机制，调整优化东西部协作结对帮扶关系和帮扶方式，强化产业合作和劳务协作。

第八篇 完善新型城镇化战略 提升城镇化发展质量

坚持走中国特色新型城镇化道路，深入推进以人为核心的新型城镇化战略，以城市群、都市圈为依托促进大中小城市和小城镇协调联动、特色化发展，使更多人民群众享有更高品质的城市生活。

第二十七章 加快农业转移人口市民化

坚持存量优先、带动增量，统筹推进户籍制度改革和城镇基本公共服务常住人口全覆盖，健全农业转移人口市民化配套政策体系，加快推动农业转移人口全面融入城市。

第一节 深化户籍制度改革

放开放宽除个别超大城市外的落户限制，试行以经常居住地登记户口制度。全面取消城区常住人口300万以下的城市落户限制，确保外地与本地农业转移人

口进城落户标准一视同仁。全面放宽城区常住人口300万至500万的I型大城市落户条件。完善城区常住人口500万以上的超大特大城市积分落户政策，精简积分项目，确保社会保险缴纳年限和居住年限分数占主要比例，鼓励取消年度落户名额限制。健全以居住证为载体、与居住年限等条件相挂钩的基本公共服务提供机制，鼓励地方政府提供更多基本公共服务和办事便利，提高居住证持有人城镇义务教育、住房保障等服务的实际享有水平。

第二节 健全农业转移人口市民化机制

完善财政转移支付与农业转移人口市民化挂钩相关政策，提高均衡性转移支付分配中常住人口折算比例，中央财政市民化奖励资金分配主要依据跨省落户人口数量确定。建立财政性建设资金对吸纳落户较多城市的基础设施投资补助机制，加大中央预算内投资支持力度。调整城镇建设用地年度指标分配依据，建立同吸纳农业转移人口落户数量和提供保障性住房规模挂钩机制。根据人口流动实际调整人口流入流出地区教师、医生等编制定额和基本公共服务设施布局。依法保障进城落户农民农村土地承包权、宅基地使用权、集体收益分配权，建立农村产权流转市场体系，健全农户“三权”市场化退出机制和配套政策。

第二十八章 完善城镇化空间布局

发展壮大城市群和都市圈，分类引导大中小城市发展方向和建设重点，形成疏密有致、分工协作、功能完善的城镇化空间格局。

第一节 推动城市群一体化发展

以促进城市群发展为抓手，全面形成“两横三纵”城镇化战略格局。优化提升京津冀、长三角、珠三角、成渝、长江中游等城市群，发展壮大山东半岛、粤闽浙沿海、中原、关中平原、北部湾等城市群，培育发展哈长、辽中南、山西中部、黔中、滇中、呼包鄂榆、兰州—西宁、宁夏沿黄、天山北坡等城市群。建立健全城市群一体化协调发展机制和成本共担、利益共享机制，统筹推进基础设施协调布局、产业分工协作、公共服务共享、生态共建环境共治。优化城市群内部空间结构，构筑生态和安全屏障，形成多中心、多层次、多节点的网络型城市群。

第二节 建设现代化都市圈

依托辐射带动能力较强的中心城市，提高1小时通勤圈协同发展水平，培育发展一批同城化程度高的现代化都市圈。以城际铁路和市域（郊）铁路等轨道交通为骨干，打通各类“断头路”、“瓶颈路”，推动市内市外交通有效衔接和轨道交通“四网融合”，提高都市圈基础设施连接性贯通性。鼓励都市圈社保和落户积分互认、教育和医疗资源共享，推动科技创新券通兑通用、产业园区和科研平台合作共建。鼓励有条件的都市圈建立统一的规划委员会，实现规划统一编制、统一实施，探索推进土地、人口等统一管理。

第三节 优化提升超大特大城市中心城区功能

统筹兼顾经济、生活、生态、安全等多元需要，转变超大特大城市开发建设方式，加强超大特大城市治理中的风险防控，促进高质量、可持续发展。有序疏解中心城区一般性制造业、区域性物流基地、专业市场等功能和设施，以及过度集中的医疗和高等教育等公共服务资源，合理降低开发强度和人口密度。增强全球资源配置、科技创新策源、高端产业引领功能，率先形成以现代服务业为主体、先进制造业为支撑的产业结构，提升综合能级与国际竞争力。坚持产城融合，完善郊区新城功能，实现多中心、组团式发展。

第四节 完善大中城市宜居宜业功能

充分利用综合成本相对较低的优势，主动承接超大特大城市产业转移和功能疏解，夯实实体经济发展基础。立足特色资源和产业基础，确立制造业差异化定位，推动制造业规模化集群化发展，因地制宜建设先进制造业基地、商贸物流中心和区域专业服务中心。优化市政公用设施布局和功能，支持三级医院和高等院校在大中城市布局，增加文化体育资源供给，营造现代时尚的消费场景，提升城市生活品质。

第五节 推进以县城为重要载体的城镇化建设

加快县城补短板强弱项，推进公共服务、环境卫生、市政公用、产业配套等设施提级扩能，增强综合承载能力和治理能力。支持东部地区基础较好的县城建设，重点支持中西部和东北城镇化地区县城建设，合理支持农产品主产区、重点生态功能区县城建设。健全县城建设投融资机制，更好发挥财政性资金作用，引

图例

- 沿海经济带
- 中部崛起经济带
- 西部开发经济带
- 长江经济带
- 黄河经济带
- 珠江经济带
- 京沪经济带
- 京广经济带
- 京哈经济带
- 京昆经济带
- 京兰经济带
- 京藏经济带
- 京新经济带
- 京滇经济带
- 京黔经济带
- 京桂经济带
- 京琼经济带
- 京台经济带
- 京澳经济带
- 京港经济带
- 京马经济带
- 京蒙经济带
- 京藏经济带
- 京新经济带
- 京滇经济带
- 京黔经济带
- 京桂经济带
- 京琼经济带
- 京台经济带
- 京澳经济带
- 京港经济带
- 京马经济带
- 京蒙经济带

图3 城镇化空间格局示意图

加快转变城市发展方式，统筹城市规划建设管理，实施城市更新行动，推动城市空间结构优化和品质提升。

按照资源环境承载力合理确定城市规模和空间结构，统筹安排城市建设、产业发展、生态涵养、基础设施和公共服务。推行功能复合、立体开发、公交导向的集约紧凑型发展模式，统筹地上地下空间利用，增加绿化节点和公共开敞空间，新建住宅推广街区制。推行城市设计和风貌管控，落实适用、经济、绿色、美观的新时期建筑方针，加强新建高层建筑管控。加快推进城市更新，改造提升老旧小区、老旧厂区、老旧街区和城中村等存量片区功能，推进老旧楼宇改造，积极扩建新建停车场、充电桩。

147

顺应城市发展新理念新趋势，开展城市现代化试点示范，建设宜居、创新、智慧、绿色、人文、韧性城市。提升城市智慧化水平，推行城市楼宇、公共空间、地下管网等“一张图”数字化管理和城市运行一网统管。科学规划布局城市绿环绿廊绿楔绿道，推进生态修复和功能完善工程，优先发展城市公共交通，建设自行车道、步行道等慢行网络，发展智能建造，推广绿色建材、装配式建筑和钢结构住宅，建设低碳城市。保护和延续城市文脉，杜绝大拆大建，让城市留下记忆、让居民记住乡愁。建设源头减排、蓄排结合、排涝除险、超标应急的城市防洪排涝体系，推动城市内涝治理取得明显成效。增强公共设施应对风暴、干旱和地质灾害的能力，完善公共设施和建筑应急避难功能。加强无障碍环境建设。拓展城市建设资金来源渠道，建立期限匹配、渠道多元、财务可持续的融资机制。

第三节 提高城市治理水平

坚持党建引领、重心下移、科技赋能，不断提升城市治理科学化精细化智能化水平，推进市域社会治理现代化。改革完善城市管理体制。推广“街乡吹哨、部门报到、接诉即办”等基层管理机制经验，推动资源、管理、服务向街道社区下沉，加快建设现代社区。运用数字技术推动城市管理手段、管理模式、管理理念创新，精准高效满足群众需求。加强物业服务监管，提高物业服务覆盖率、服务质量和标准化水平。

第四节 完善住房市场体系和住房保障体系

坚持房子是用来住的、不是用来炒的定位，加快建立多主体供给、多渠道保障、租购并举的住房制度，让全体人民住有所居、职住平衡。坚持因地制宜、多策并举，夯实城市政府主体责任，稳定地价、房价和预期。建立住房和土地联动机制，加强房地产金融调控，发挥住房税收调节作用，支持合理自住需求，遏制投资投机性需求。加快培育和发展住房租赁市场，有效盘活存量住房资源，有力有序扩大城市租赁住房供给，完善长租房政策，逐步使租购住房在享受公共服务上具有同等权利。加快住房租赁法规建设，加强租赁市场监管，保障承租人和出租人合法权益。有效增加保障性住房供给，完善住房保障基础性制度和支持政策。以人口流入多、房价高的城市为重点，扩大保障性租赁住房供给，着力解决困难群体和新市民住房问题。单列租赁住房用地计划，探索利用集体建设用地和企事

业单位自有闲置土地建设租赁住房，支持将非住宅房屋改建为保障性租赁住房。完善土地出让收入分配机制，加大财税、金融支持力度。因地制宜发展共有产权住房。处理好基本保障和非基本保障的关系，完善住房保障方式，健全保障对象、准入门槛、退出管理等政策。改革完善住房公积金制度，健全缴存、使用、管理和运行机制。

专栏 11 新型城镇化建设工程	
01 都市圈建设	在中心城市辐射带动作用强、与周边城市同城化程度高的地区，培育发展一批现代化都市圈，推进基础设施互联互通、公共服务互认共享。
02 城市更新	完成 2000 年底前建成的 21.9 万个城镇老旧小区改造，基本完成大城市老旧厂区改造，改造一批大型老旧街区，因地制宜改造一批城中村。
03 城市防洪排涝	以 31 个重点防洪城市和大江大河沿岸沿线城市为重点，提升改造城市蓄滞洪空间、堤防、护岸、河道、防冲工程，排水管网等防潮排涝设施，因地制宜建设海绵城市，全部消除城市严重易涝积水区段。
04 县城补短板	推进县城、县级市城区及特大型补短板，完善综合医院、疾控中心、养老中心、幼儿园、市政管网、市政交通、停车场、充电桩、污水处理设施和处理设施和产业平台配套设施。高质量完成 120 个县城补短板示范任务。
05 现代社区培育	完善社区养老托育、医疗卫生、文化体育、物流配送、便民商超、家政物业等服务网络和线上平台，城市社区综合服务设施实现全覆盖。实施大学生社工计划，每万城镇常住人口拥有社区工作者 18 人。
06 城乡融合发展	建设嘉兴湖州、福州东部、广州清远、南京无锡常州、济南青岛、成都西部、重庆西部、西安咸阳、长春吉林、许昌、鹰潭等国家城乡融合发展试验区，加强改革整权和政策集成。

第九篇 优化区域经济布局 促进区域协调发展

深入实施区域重大战略、区域协调发展战略、主体功能区战略，健全区域协调发展体制机制，构建高质量发展的区域经济布局和国土空间支撑体系。

第三十章 优化国土空间开发保护格局

立足资源环境承载能力，发挥各地区比较优势，促进各类要素合理流动和高

效集聚，推动形成主体功能明显、优势互补、高质量发展的国土空间开发保护新格局。

第一节 完善和落实主体功能区制度

顺应空间结构变化趋势，优化重大基础设施、重大生产力和公共资源布局，分类提高城市化地区发展水平，推动农业生产向粮食生产功能区、重要农产品生产保护区和特色农产品优势区集聚，优化生态安全屏障体系，逐步形成城市化地区、农产品主产区、生态功能区三大空间格局。细化主体功能区划分，按照主体功能定位划分政策单元，对重点开发地区、生态脆弱地区、能源资源富集地区等制定差异化政策，分类精准施策。加强空间发展统筹协调，保障国家重大发展战略落地实施。

第二节 开拓高质量发展的重要动力源

以中心城市和城市群等经济发展优势区域为重点，增强经济和人口承载能力，带动全国经济效率整体提升。以京津冀、长三角、粤港澳大湾区为重点，提升创新策源能力和全球资源配置能力，加快打造引领高质量发展的第一梯队。在中西部有条件的地区，以中心城市为引领，提升城市群功能，加快工业化城镇化进程，形成高质量发展的重要区域。破除资源流动障碍，优化行政区划设置，提高中心城市综合承载能力和资源优化配置能力，强化对区域发展的辐射带动作用。

第三节 提升重要功能性区域的保障能力

以农产品主产区、重点生态功能区、能源资源富集地区和边境地区等承担战略功能的区域为支撑，切实维护国家粮食安全、生态安全、能源安全和边疆安全，与动力源地区共同打造高质量发展的动力系统。支持农产品主产区增强农业生产能力，支持生态功能区把发展重点放到保护生态环境、提供生态产品上，支持生态功能区人口逐步有序向城市化地区转移并定居落户。优化能源开发布局和运输格局，加强能源资源综合开发利用基地建设，提升国内能源供给保障水平。增强边疆地区发展能力，强化人口和经济支撑，促进民族团结和边疆稳定。健全公共资源配置机制，对重点生态功能区、农产品主产区、边境地区等提供有效转移支

付。

第三十一章 深入实施区域重大战略

聚焦实现战略目标和提升引领带动能力，推动区域重大战略取得新的突破性进展，促进区域间融合互动、融通补充。

第一节 加快推动京津冀协同发展

紧抓疏解北京非首都功能“牛鼻子”，构建功能疏解政策体系，实施一批标志性疏解项目。高标准高质量建设雄安新区，加快启动区和起步区建设，推动管理体制创新。高质量建设北京城市副中心，促进与河北省三河、香河、大厂三县市一体化发展。推动天津滨海新区高质量发展，支持张家口首都水源涵养功能区 and 生态环境支撑区建设。提高北京科技创新中心基础研究和原始创新能力，发挥中关村国家自主创新示范区先行先试作用，推动京津冀产业链与创新链深度融合。基本建成轨道上的京津冀，提高机场群港口群协同水平。深化大气污染联防联控联治，强化华北地下水超采及地面沉降综合治理。



图4 京津冀地区轨道交通规划图

第二节 全面推动长江经济带发展

坚持生态优先、绿色发展和共抓大保护、不搞大开发，协同推动生态环境保

护和经济发展，打造人与自然和谐共生的美丽中国样板。持续推进生态环境突出问题整改，推动长江全流域按单元精细化分区管控，实施城镇污水垃圾处理、工业污染治理、农业面源污染治理、船舶污染治理、尾矿库污染治理等工程。深入开展绿色发展示范，推进赤水河流域生态环境保护。实施长江十年禁渔。围绕建设长江大动脉，整体设计综合交通运输体系，疏解三峡枢纽瓶颈制约，加快沿江高铁和货运铁路建设。发挥产业协同联动整体优势，构建绿色产业体系。保护好长江文物和文化遗产。

第三节 积极稳妥推进粤港澳大湾区建设

加强粤港澳产学研协同发展，完善广深港、广珠澳科技创新走廊和深港河套、粤澳横琴科技创新极点“两廊两点”架构体系，推进综合性国家科学中心建设，便利创新要素跨境流动。加快城际铁路建设，统筹港口和机场功能布局，优化航运和航空资源配置。深化通关模式改革，促进人员、货物、车辆便捷高效流动。扩大内地与港澳专业资格互认范围，深入推进重点领域规则衔接、机制对接。便利港澳青年到大湾区内地城市就学就业创业，打造粤港澳青少年交流精品品牌。



图5 粤港澳大湾区轨道交通规划图

第四节 提升长三角一体化发展水平

瞄准国际先进科创能力和产业体系，加快建设长三角G60科创走廊和沿沪宁

产业创新带，提高长三角地区配置全球资源能力和辐射带动全国发展能力。加快基础设施互联互通，实现长三角地级及以上城市高铁全覆盖，推进港口群一体化治理。打造虹桥国际开放枢纽，强化上海自贸试验区临港新片区开放型经济集聚功能，深化沪苏浙皖自贸试验区联动发展。加快公共服务便利共享，优化优质教育和医疗卫生资源布局。推进生态环境共保联治，高水平建设长三角生态绿色一体化发展示范区。



图 6 长三角地区轨道交通规划图

第五节 扎实推进黄河流域生态保护和高质量发展

加大上游重点生态系统保护和修复力度，筑牢三江源“中华水塔”，提升甘南、若尔盖等区域水源涵养能力。创新中游黄土高原水土流失治理模式，积极开展小流域综合治理、旱作梯田和淤地坝建设。推动下游二级悬河治理和滩区综合治理，加强黄河三角洲湿地保护和修复。开展汾渭平原、河套灌区等农业面源污染治理，清理整顿黄河岸线内工业企业，加强沿黄河城镇污水处理设施及配套管网建设。实施深度节水控水行动，降低水资源开发利用强度。合理控制煤炭开发强度，推进能源资源一体化开发利用，加强矿山生态修复。优化中心城市和城市群发展格局，统筹沿黄河县城和乡村建设。实施黄河文化遗产系统保护工程，打造具有国际影响力的黄河文化旅游带。建设黄河流域生态保护和高质量发展先行

区。

第三十二章 深入实施区域协调发展战略

深入推进西部大开发、东北全面振兴、中部地区崛起、东部率先发展，支持特殊类型地区加快发展，在发展中促进相对平衡。

第一节 推进西部大开发形成新格局

强化举措推进西部大开发，切实提高政策精准性和有效性。深入实施一批重大生态工程，开展重点区域综合治理。积极融入“一带一路”建设，强化开放大通道建设，构建内陆多层次开放平台。加大西部地区基础设施投入，支持发展特色优势产业，集中力量巩固脱贫攻坚成果，补齐教育、医疗卫生等民生领域短板。推进成渝地区双城经济圈建设，打造具有全国影响力的重要经济中心、科技创新中心、改革开放新高地、高品质生活宜居地，提升关中平原城市群建设水平，促进西北地区与西南地区合作互动。支持新疆建设国家“三基地一通道”，支持西藏打造面向南亚开放的重要通道。促进400毫米降水线西侧区域保护发展。

第二节 推动东北振兴取得新突破

从维护国家国防、粮食、生态、能源、产业安全的战略高度，加强政策统筹，实现重点突破。加快转变政府职能，深化国有企业改革攻坚，着力优化营商环境，大力发展民营经济。打造辽宁沿海经济带，建设长吉图开发开放先导区，提升哈尔滨对俄合作开放能级。加快发展现代农业，打造保障国家粮食安全的“压舱石”。加大生态资源保护力度，筑牢祖国北疆生态安全屏障。改造提升装备制造等传统优势产业，培育发展新兴产业，大力发展寒地冰雪、生态旅游等特色产业，打造具有国际影响力的冰雪旅游带，形成新的均衡发展产业结构和竞争优势。实施更具吸引力的人才集聚措施。深化与东部地区对口合作。

第三节 开创中部地区崛起新局面

着力打造重要先进制造业基地、提高关键领域自主创新能力、建设内陆地区开放高地、巩固生态绿色发展格局，推动中部地区加快崛起。做大做强先进制造业，在长江、京广、陇海、京九等沿线建设一批中高端产业集群，积极承接新兴

产业布局和转移。推动长江中游城市群协同发展，加快武汉、长株潭都市圈建设，打造全国重要增长极。夯实粮食生产基础，不断提高农业综合效益和竞争力，加快发展现代农业。加强生态环境共保联治，着力构筑生态安全屏障。支持淮河、汉江生态经济带上下游合作联动发展。加快对外开放通道建设，高标准高水平建设内陆地区开放平台。提升公共服务保障特别是应对公共卫生等重大突发事件能力。

第四节 鼓励东部地区加快推进现代化

发挥创新要素集聚优势，加快在创新引领上实现突破，推动东部地区率先实现高质量发展。加快培育世界级先进制造业集群，引领新兴产业和现代服务业发展，提升要素产出效率，率先实现产业升级。更高层次参与国际经济合作和竞争，打造对外开放新优势，率先建立全方位开放型经济体系。支持深圳建设中国特色社会主义先行示范区、浦东打造社会主义现代化建设引领区、浙江高质量发展建设共同富裕示范区。深入推进山东新旧动能转换综合试验区建设。

第五节 支持特殊类型地区发展

统筹推进革命老区振兴，因地制宜发展特色产业，传承弘扬红色文化，支持赣闽粤原中央苏区高质量发展示范，推进陕甘宁、大别山、左右江、川陕、沂蒙等革命老区绿色创新发展。推进生态退化地区综合治理和生态脆弱地区保护修复，支持毕节试验区建设。推动资源型地区可持续发展示范区和转型创新试验区建设，实施采煤沉陷区综合治理和独立工矿区改造提升工程。推进老工业基地制造业竞争优势重构，建设产业转型升级示范区。改善国有林场林区基础设施。多措并举解决高海拔地区群众生产生活困难。推进兴边富民、稳边固边，大力改善边境地区生产生活条件，完善沿边城镇体系，支持边境口岸建设，加快抵边村镇和抵边通道建设。推动边境贸易创新发展。加大对重点边境地区发展精准支持力度。

专栏 12 促进边境地区发展工程	
01 边境城镇	完善边境城镇功能，重点支持满洲里、二连、瑞春、绥芬河、东兴、腾冲、米林、塔城、可克达拉等边境城镇提升承载能力。
02 抵边村庄	完善边境村庄基础设施和公共服务设施，新建抵边新村 200 个左右，实现抵边自然村道路、电力、通信、邮政、广电普遍覆盖。
03 沿边抵边公路	建设集安至桓仁、珲春至圈河、沪水至腾冲、墨脱经察隅至滇藏界、青河经富蕴至阿勒泰、布伦口至红其拉甫、巴里坤至老多庙、二连浩特至赛罕塔拉等沿边抵边公路。
04 边境机场	建设塔什库尔干、墨子、绥芬河等机场，迁建延吉机场，建设 20 个左右边境通用机场。
05 边境口岸	建设里孜、黑河、同江、黑瞎子岛口岸，改造提升吉隆、樟木、吉隆、霍尔果斯、阿拉山口、满洲里、二连浩特、瑞丽、友谊关、红其拉甫、甘其毛都、策克、吐尔滚特、伊尔克什坦口岸。

第六节 健全区域协调发展体制机制

建立健全区域战略统筹、市场一体化发展、区域合作互助、区际利益补偿等机制，更好促进发达地区和欠发达地区、东中西部和东北地区共同发展。提升区域合作层次和水平，支持省际交界地区探索建立统一规划、统一管理、合作共建、利益共享的合作新机制。完善财政转移支付支持欠发达地区的机制，逐步实现基本公共服务均等化，引导人才向西部和艰苦边远地区流动。完善区域合作与利益调节机制，支持流域上下游、粮食主产区主销区、资源输出地输入地之间开展多种形式的利益补偿，鼓励探索共建园区、飞地经济等利益共享模式。聚焦铸牢中华民族共同体意识，加大对民族地区发展支持力度，全面深入持久开展民族团结进步宣传教育和创建，促进各民族交往交流交融。

第三十三章 积极拓展海洋经济发展空间

坚持陆海统筹、人海和谐、合作共赢，协同推进海洋生态保护、海洋经济发展和海洋权益维护，加快建设海洋强国。

第一节 建设现代海洋产业体系

围绕海洋工程、海洋资源、海洋环境等领域突破一批关键核心技术。培育壮大海洋工程装备、海洋生物医药产业，推进海水淡化和海洋能规模化利用，提高海洋文化旅游开发水平。优化近海绿色养殖布局，建设海洋牧场，发展可持续远洋渔业。建设一批高质量海洋经济发展示范区和特色化海洋产业集群，全面提高北部、东部、南部三大海洋经济圈发展水平。以沿海经济带为支撑，深化与周边国家涉海合作。

第二节 打造可持续海洋生态环境

探索建立沿海、流域、海域协同一体的综合治理体系。严格围填海管控，加强海岸带综合管理与滨海湿地保护。拓展入海污染物排放总量控制范围，保障入海河流断面水质。加快推进重点海域综合治理，构建流域－河口－近岸海域污染防治联动机制，推进美丽海湾保护与建设。防范海上溢油、危险化学品泄露等重大环境风险，提升应对海洋自然灾害和突发环境事件能力。完善海岸线保护、海域和无居民海岛有偿使用制度，探索海岸建筑退缩线制度和海洋生态环境损害赔偿制度，自然岸线保有率不低于35%。

第三节 深度参与全球海洋治理

积极发展蓝色伙伴关系，深度参与国际海洋治理机制和相关规则制定与实施，推动建设公正合理的国际海洋秩序，推动构建海洋命运共同体。深化与沿海国家在海洋环境监测和保护、科学研究和海上搜救等领域务实合作，加强深海战略性资源和生物多样性调查评价。参与北极务实合作，建设“冰上丝绸之路”。提高参与南极保护和利用能力。加强形势研判、风险防范和法理斗争，加强海事司法建设，坚决维护国家海洋权益。有序推进海洋基本法立法。

第十篇 发展社会主义先进文化 提升国家文化软实力

坚持马克思主义在意识形态领域的指导地位，坚定文化自信，坚持以社会主义核心价值观引领文化建设，围绕举旗帜、聚民心、育新人、兴文化、展形象的使命任务，促进满足人民文化需求和增强人民精神力量相统一，推进社会主义文化强国建设。

第三十四章 提高社会文明程度

加强社会主义精神文明建设，培育和践行社会主义核心价值观，推动形成适应新时代要求的思想观念、精神面貌、文明风尚、行为规范。

第一节 推动理想信念教育常态化制度化

深入开展习近平新时代中国特色社会主义思想学习教育，健全用党的创新理论武装全党、教育人民的工作体系。建立健全“不忘初心、牢记使命”的制度和长效机制，加强和改进思想政治工作，持续开展中国特色社会主义和中国梦宣传教育，加强党史、新中国史、改革开放史、社会主义发展史教育，加强爱国主义、集体主义、社会主义教育，加强革命文化研究阐释和宣传教育，弘扬党和人民在各个历史时期奋斗中形成的伟大精神。完善弘扬社会主义核心价值观的法律政策体系，把社会主义核心价值观要求融入法治建设和社会治理，体现到国民教育、精神文明创建、文化产品创作生产全过程。完善青少年理想信念教育齐抓共管机制。

第二节 发展中国特色哲学社会科学

加强对习近平新时代中国特色社会主义思想的整体性系统性研究、出版传播、宣传阐释，推进马克思主义中国化、时代化、大众化。深入实施马克思主义理论研究和建设工程，推进习近平新时代中国特色社会主义思想研究中心（院）、中国特色社会主义理论体系研究中心等建设，建好用好“学习强国”等学习平台。构建中国特色哲学社会科学学科体系、学术体系和话语体系，深入实施哲学社会科学创新工程，加强中国特色新型智库建设。

第三节 传承弘扬中华优秀传统文化

深入实施中华优秀传统文化传承发展工程，强化重要文化和自然遗产、非物质文化遗产系统性保护，推动中华优秀传统文化创造性转化、创新性发展。加强文物科技创新，实施中华文明探源和考古中国工程，开展中华文化资源普查，加强文物和古籍保护研究利用，推进革命文物和红色遗址保护，完善流失文物追索返还制度。建设长城、大运河、长征、黄河等国家文化公园，加强世界文化遗产、文物保护单位、考古遗址公园、历史文化名城名镇名村保护。健全非物质文化遗

产保护传承体系，加强各民族优秀传统文化保护和传承。

第四节 持续提升公民文明素养

推进公民道德建设，大力开展社会公德、职业道德、家庭美德、个人品德建设。开展国家勋章、国家荣誉称号获得者和时代楷模、道德模范、最美人物、身边好人的宣传学习。实施文明创建工程，拓展新时代文明实践中心建设，科学规范做好文明城市、文明村镇、文明单位、文明校园、文明家庭评选表彰，深化未成年人思想道德建设。完善市民公约、乡规民约、学生守则、团体章程等社会规范，建立惩戒失德行为机制。弘扬诚信文化，建设诚信社会。广泛开展志愿服务关爱行动。提倡艰苦奋斗、勤俭节约，开展以劳动创造幸福为主题的宣传教育。加强网络文明建设，发展积极健康的网络文化。

第三十五章 提升公共文化服务水平

坚持为人民服务、为社会主义服务的方向，坚持百花齐放、百家争鸣的方针，加强公共文化服务体系和体制机制创新，强化中华文化传播推广和文明交流互鉴，更好保障人民文化权益。

第一节 加强优秀文化作品创作生产传播

把提高质量作为文艺作品的生命线，提高文艺原创能力。实施文艺作品质量提升工程，健全重大现实、重大革命、重大历史题材创作规划组织机制，加强农村、少儿等题材创作，不断推出反映时代新气象、讴歌人民新创造的文艺精品。建立健全文化产品创作生产、传播引导、宣传推广的激励机制和评价体系，推动形成健康清朗的文艺生态。加强文化队伍建设，培养造就高水平创作人才和德艺双馨的名家大师。

第二节 完善公共文化服务体系

优化城乡文化资源配置，推进城乡公共文化服务体系一体建设。创新实施文化惠民工程，提升基层综合性文化服务中心功能，广泛开展群众性文化活动。推进公共图书馆、文化馆、美术馆、博物馆等公共文化场馆免费开放和数字化发展。推进媒体深度融合，做强新型主流媒体。完善应急广播体系，实施智慧广电固边

工程和乡村工程。发展档案事业。深入推进全民阅读，建设“书香中国”，推动农村电影放映优化升级。创新公共文化服务运行机制，鼓励社会力量参与公共文化服务供给和设施建设运营。

第三节 提升中华文化影响力

加强对外文化交流和多层次文明对话，创新推进国际传播，利用网上网下，讲好中国故事，传播好中国声音，促进民心相通。开展“感知中国”、“走读中国”、“视听中国”活动，办好中国文化年（节）、旅游年（节）。建设中文传播平台，构建中国语言文化全球传播体系和国际中文教育标准体系。

第三十六章 健全现代文化产业体系

坚持把社会效益放在首位、社会效益和经济效益相统一，健全现代文化产业体系和市场体系。

第一节 扩大优质文化产品供给

实施文化产业数字化战略，加快发展新型文化企业、文化业态、文化消费模式，壮大数字创意、网络视听、数字出版、数字娱乐、线上演播等产业。加快提升超高清电视节目制播能力，推进电视频道高清化改造，推进沉浸式视频、云转播等应用。实施文化品牌战略，打造一批有影响力、代表性的文化品牌。培育骨干文化企业，规范发展文化产业园区，推动区域文化产业带建设。积极发展对外文化贸易，开拓海外文化市场，鼓励优秀传统文化产品和影视剧、游戏等数字文化产品“走出去”，加强国家文化出口基地建设。

第二节 推动文化和旅游融合发展

坚持以文塑旅、以旅彰文，打造独具魅力的中华文化旅游体验。深入发展大众旅游、智慧旅游，创新旅游产品体系，改善旅游消费体验。加强区域旅游品牌和服务整合，建设一批富有文化底蕴的世界级旅游景区和度假区，打造一批文化特色鲜明的国家级旅游休闲城市和街区。推进红色旅游、文化遗产旅游、旅游演艺等创新发展，提升度假休闲、乡村旅游等服务品质，完善邮轮游艇、低空旅游等发展政策。健全旅游基础设施和集散体系，推进旅游厕所革命，强化智慧景区

建设。建立旅游服务质量评价体系，规范在线旅游经营服务。

第三节 深化文化体制改革

完善文化管理体制和生产经营机制，提升文化治理效能。完善国有文化资产管理体制机制，深化公益性文化事业单位改革，推进公共文化机构法人治理结构改革。深化国有文化企业分类改革，推进国有文艺院团改革和院线制改革。完善文化市场综合执法体制，制定未成年人网络保护、信息网络传播视听等领域法律法规。

专栏 13 社会主义文化繁荣发展工程	
01	中国特色社会主义理论出版传播 编辑出版习近平谈治国理政、习近平新时代中国特色社会主义思想学习问答、分领域学习纲要等系列理论读物，编辑出版党史、新中国史、改革开放史、社会主义发展史经典教材，加强海外翻译出版和宣介推广。
02	文艺精品创作 开展精神文明建设“五个一”、舞台艺术、影视精品、优秀剧本、美术创作收藏、重大出版等工程，实施当代文学艺术创作、中华文化新媒体传播、纪录片创作传播、地方戏曲传承发展、网络文艺创作传播等重大项目。
03	全媒体传播和数字文化 推进国家、省、市、县四级融媒体中心（平台）建设，推进国家有线电视网络整合和 5G 一体化发展，分类采集梳理文化遗产数据，建设国家文化大数据体系，实施出版融合发展工程。
04	文化遗产保护传承 加强安阳殷墟、汉长安城、隋唐洛阳城和重要石窟寺等遗址保护，开展江西汉代海昏侯国、河南仰韶村、良渚古城、古邕、陶寺、三星堆、曲阜鲁国故城等国家考古遗址公园建设，建设 20 个国家重点区域考古标本库房，30 个国家级文化生态保护区和 20 个国家级非物质文化遗产馆。
05	中华典籍整理出版 整理出版 300 种中华典籍，组织《永乐大典》、敦煌文献等重点古籍系统性保护整理出版，实施国家古籍数字化工程。推进点校本“二十四史”及清史稿修订等重大出版工程，推进复兴文库建设，启动新编中国通史纂修工程，中华民族交往交流交融史编纂工程。
06	重大文化设施建设 建设中国共产党历史展览馆、中央档案馆新馆，国家版本馆，国家文献储备库，故宫博物院北院区，国家美术馆，国家文化遗产科技创新中心。
07	旅游目的地质量提升 打造海南国际旅游消费中心，粤港澳大湾区世界级旅游目的地，长江国际黄金旅游带、黄河文化旅游带、杭州自然生态和文化旅游廊道、巴蜀文化旅游走廊，桂林国际旅游胜地，健全游客服务、停车及充电、交通、流量监测管理等设施。

第十一篇 推动绿色发展 促进人与自然和谐共生

坚持绿水青山就是金山银山理念，坚持尊重自然、顺应自然、保护自然，坚持节约优先、保护优先、自然恢复为主，实施可持续发展战略，完善生态文明领域统筹协调机制，构建生态文明体系，推动经济社会发展全面绿色转型，建设美丽中国。

第三十七章 提升生态系统质量和稳定性

坚持山水林田湖草系统治理，着力提高生态系统自我修复能力和稳定性，守住自然生态安全边界，促进自然生态系统质量整体改善。

第一节 完善生态安全屏障体系

强化国土空间规划和用途管控，划定落实生态保护红线、永久基本农田、城镇开发边界以及各类海域保护线。以国家重点生态功能区、生态保护红线、国家级自然保护区等为重点，实施重要生态系统保护和修复重大工程，加快推进青藏高原生态屏障区、黄河重点生态区、长江重点生态区和东北森林带、北方防沙带、南方丘陵山地带、海岸带等生态屏障建设。加强长江、黄河等大江大河和重要湖泊湿地生态保护治理，加强重要生态廊道建设和保护。全面加强天然林和湿地保护，湿地保护率提高到55%。科学推进水土流失和荒漠化、石漠化综合治理，开展大规模国土绿化行动，推行林长制。科学开展人工影响天气活动。推行草原森林河流湖泊休养生息，健全耕地休耕轮作制度，巩固退耕还林还草、退田还湖还湿、退围还滩还海成果。

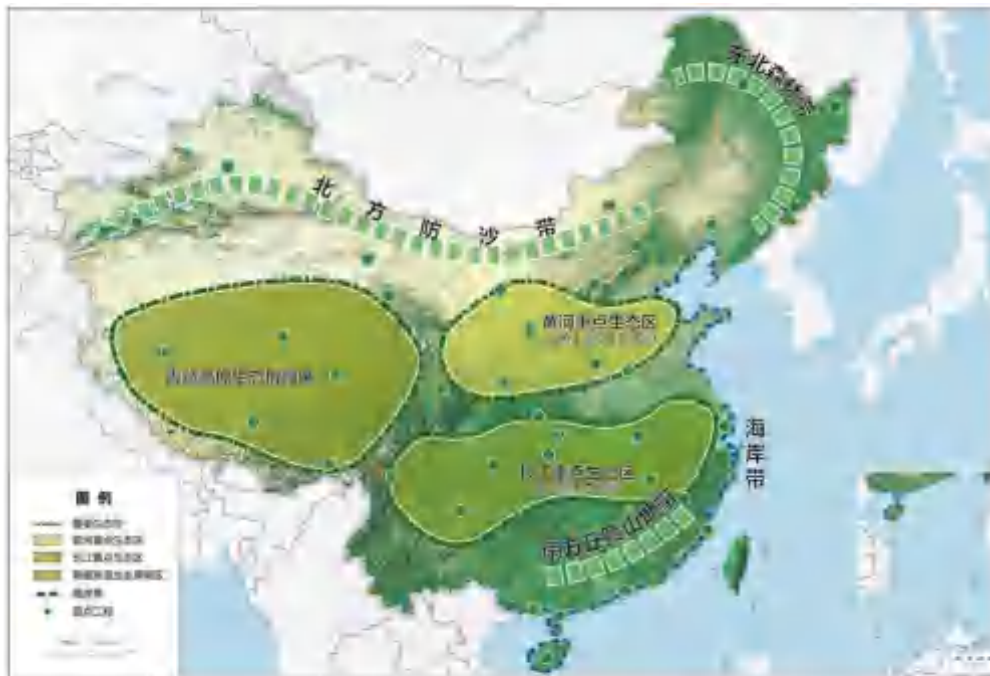


图7 重要生态系统保护和修复重大工程布局示意图

第二节 构建自然保护地体系

科学划定自然保护地保护范围及功能分区，加快整合归并优化各类保护地，构建以国家公园为主体、自然保护区为基础、各类自然公园为补充的自然保护地体系。严格管控自然保护地范围内非生态活动，稳妥推进核心区内居民、耕地、矿权有序退出。完善国家公园管理体制和运营机制，整合设立一批国家公园。实施生物多样性保护重大工程，构筑生物多样性保护网络，加强国家重点保护和珍稀濒危野生动植物及其栖息地的保护修复，加强外来物种管控。完善生态保护和修复用地用海等政策。完善自然保护地、生态保护红线监管制度，开展生态系统保护成效监测评估。

第三节 健全生态保护补偿机制

加大重点生态功能区、重要水系源头地区、自然保护地转移支付力度，鼓励受益地区和保护地区、流域上下游通过资金补偿、产业扶持等多种形式开展横向生态补偿。完善市场化多元化生态补偿，鼓励各类社会资本参与生态保护修复。完善森林、草原和湿地生态补偿制度。推动长江、黄河等重要流域建立全流域生态补偿机制。建立生态产品价值实现机制，在长江流域和三江源国家公园等开展试点。制定实施生态保护补偿条例。

专栏 14 重要生态系统保护和修复工程	
01 青藏高原生态屏障区	以三江源、祁连山、若尔盖、甘南黄河重要水源补给区等为重点，加强原生地帶性植被、珍稀物种及其栖息地保护，新增沙化土地治理 100 万公顷、退化草原治理 320 万公顷，沙化土地封禁保护 20 万公顷。
02 黄河重点生态区（含黄土高原生态屏障）	以黄土高原、秦岭、贺兰山等为重点，加强“三化”草场治理和水土流失综合治理，保护修复黄河三角洲等湿地，保护修复林草植被 80 万公顷，新增水土流失治理 200 万公顷，沙化土地治理 80 万公顷。
03 长江重点生态区（含川滇生态屏障）	以横断山区、岷山石漠化区、三峡库区、洞庭湖、鄱阳湖等为重点，开展森林质量精准提升、河湖湿地修复、石漠化综合治理等，加强珍稀濒危野生动植物保护恢复，完成营造林 110 万公顷，新增水土流失治理 500 万公顷，石漠化治理 100 万公顷。
04 东北森林带	以大小兴安岭、长白山及三江平原、松嫩平原重要湿地等为重点，实施天然林保护修复，保护重点沼泽湿地和珍稀候鸟迁徙地，修复天然林后备资源 70 万公顷，新增退化草原治理 30 万公顷。
05 北方防沙带	以内蒙古高原、河西走廊、塔里木河流域、京津冀地区等为重点，推进防护林体系建设及退化林修复、退化草原修复、京津风沙源治理等，完成营造林 220 万公顷，新增沙化土地治理 750 万公顷、退化草原治理 270 万公顷。
06 南方丘陵山地带	以南岭山地、武夷山区、湘桂岩溶石漠化区等为重点，实施森林质量精准提升行动，推进水土流失和石漠化综合治理，加强河湖生态保护修复，保护两栖物种及其栖息地，营造防护林 9 万公顷，新增石漠化治理 30 万公顷。
07 海岸带	以黄渤海、长三角、粤闽浙沿海、粤港澳大湾区、海南岛、北部湾等为重点，全面保护自然岸线，整治修复岸线长度 400 公里，滨海湿地 2 万公顷，营造防护林 11 万公顷。
08 自然保护地及野生动植物保护	推进三江源、东北虎豹、大熊猫和海南热带雨林等国家公园建设，新整合设立秦岭、黄河口等国家公园。建设珍稀濒危野生动植物基因保存库，救护繁育场所。专项监测 48 种极度濒危野生动物和 50 种极小种群植物。

第三十八章 持续改善环境质量

深入打好污染防治攻坚战，建立健全环境治理体系，推进精准、科学、依法、系统治污，协同推进减污降碳，不断改善空气、水环境质量，有效管控土壤污染风险。

第一节 深入开展污染防治行动

坚持源头防治、综合施策，强化多污染物协同控制和区域协同治理。加强城市大气质量达标管理，推进细颗粒物（PM_{2.5}）和臭氧（O₃）协同控制，地级及以上城市PM_{2.5}浓度下降10%，有效遏制O₃浓度增长趋势，基本消除重污染天气。持续改善京津冀及周边地区、汾渭平原、长三角地区空气质量，因地制宜推动北方地区清洁取暖、工业窑炉治理、非电行业超低排放改造，加快挥发性有机物排放综合整治，氮氧化物和挥发性有机物排放总量分别下降10%以上。完善水污染防治流域协同机制，加强重点流域、重点湖泊、城市水体和近岸海域综合治理，推进美丽河湖保护与建设，化学需氧量和氨氮排放总量分别下降8%，基本消除劣Ⅴ类国控断面和城市黑臭水体。开展城市饮用水水源地规范化建设，推进重点流域重污染企业搬迁改造。推进受污染耕地和建设用地管控修复，实施水土环境风险协同防控。加强塑料污染全链条防治。加强环境噪声污染治理。重视新污染物治理。

第二节 全面提升环境基础设施水平

构建集污水、垃圾、固废、危废、医废处理处置设施和监测监管能力于一体的环境基础设施体系，形成由城市向建制镇和乡村延伸覆盖的环境基础设施网络。推进城镇污水管网全覆盖，开展污水处理差别化精准提标，推广污泥集中焚烧无害化处理，城市污泥无害化处置率达到90%，地级及以上缺水城市污水资源化利用率超过25%。建设分类投放、分类收集、分类运输、分类处理的生活垃圾处理系统。以主要产业基地为重点布局危险废弃物集中利用处置设施。加快建设地级及以上城市医疗废弃物集中处理设施，健全县域医疗废弃物收集转运处置体系。

第三节 严密防控环境风险

建立健全重点风险源评估预警和应急处置机制。全面整治固体废物非法堆存，提升危险废弃物监管和风险防范能力。强化重点区域、重点行业重金属污染监控预警。健全有毒有害化学物质环境风险管理体系，完成重点地区危险化学品生产企业搬迁改造。严格核与辐射安全监管，推进放射性污染防治。建立生态环

境突发事件后评估机制和公众健康影响评估制度。在高风险领域推行环境污染强制责任保险。

第四节 积极应对气候变化

落实2030年应对气候变化国家自主贡献目标，制定2030年前碳排放达峰行动方案。完善能源消费总量和强度双控制度，重点控制化石能源消费。实施以碳强度控制为主、碳排放总量控制为辅的制度，支持有条件的地方和重点行业、重点企业率先达到碳排放峰值。推动能源清洁低碳安全高效利用，深入推进工业、建筑、交通等领域低碳转型。加大甲烷、氢氟碳化物、全氟化碳等其他温室气体控制力度。提升生态系统碳汇能力。锚定努力争取2060年前实现碳中和，采取更加有力的政策和措施。加强全球气候变暖对我国承受力脆弱地区影响的观测和评估，提升城乡建设、农业生产、基础设施适应气候变化能力。加强青藏高原综合科学考察研究。坚持公平、共同但有区别的责任及各自能力原则，建设性参与和引领应对气候变化国际合作，推动落实[联合国气候变化框架公约](#)及其巴黎协定，积极开展气候变化南南合作。

第五节 健全现代环境治理体系

建立地上地下、陆海统筹的生态环境治理制度。全面实行排污许可制，实现所有固定污染源排污许可证核发，推动工业污染源限期达标排放，推进排污权、用能权、用水权、碳排放权市场化交易。完善环境保护、节能减排约束性指标管理。完善河湖管理保护机制，强化河长制、湖长制。加强领导干部自然资源资产离任审计。完善中央生态环境保护督察制度。完善省以下生态环境机构监测监察执法垂直管理制度，推进生态环境保护综合执法改革，完善生态环境公益诉讼制度。加大环保信息公开力度，加强企业环境治理责任制度建设，完善公众监督和举报反馈机制，引导社会组织和公众共同参与环境治理。

(注：PM2.5为PM右下角加2.5，O3为O右下角加3)

第三十九章 加快发展方式绿色转型

坚持生态优先、绿色发展，推进资源总量管理、科学配置、全面节约、循环利用，协同推进经济高质量发展和生态环境高水平保护。

第一节 全面提高资源利用效率

坚持节能优先方针，深化工业、建筑、交通等领域和公共机构节能，推动5G、大数据中心等新兴领域能效提升，强化重点用能单位节能管理，实施能量系统优化、节能技术改造等重点工程，加快能耗限额、产品设备能效强制性国家标准制修订。实施国家节水行动，建立水资源刚性约束制度，强化农业节水增效、工业节水减排和城镇节水降损，鼓励再生水利用，单位GDP用水量下降16%左右。加强土地节约集约利用，加大批而未供和闲置土地处置力度，盘活城镇低效用地，支持工矿废弃土地恢复利用，完善土地复合利用、立体开发支持政策，新增建设用地规模控制在2950万亩以内，推动单位GDP建设用地使用面积稳步下降。提高矿产资源开发保护水平，发展绿色矿业，建设绿色矿山。

第二节 构建资源循环利用体系

全面推行循环经济理念，构建多层次资源高效循环利用体系。深入推进园区循环化改造，补齐和延伸产业链，推进能源资源梯级利用、废物循环利用和污染物集中处置。加强大宗固体废弃物综合利用，规范发展再制造产业。加快发展种养有机结合的循环农业。加强废旧物品回收设施规划建设，完善城市废旧物品回收分拣体系。推行生产企业“逆向回收”等模式，建立健全线上线下融合、流向可控的资源回收体系。拓展生产者责任延伸制度覆盖范围。推进快递包装减量化、标准化、循环化。

第三节 大力发展绿色经济

坚决遏制高耗能、高排放项目盲目发展，推动绿色转型实现积极发展。壮大节能环保、清洁生产、清洁能源、生态环境、基础设施绿色升级、绿色服务等产业，推广合同能源管理、合同节水管理、环境污染第三方治理等服务模式。推动煤炭等化石能源清洁高效利用，推进钢铁、石化、建材等行业绿色化改造，加快大宗货物和中长途货物运输“公转铁”、“公转水”。推动城市公交和物流配送车辆电动化。构建市场导向的绿色技术创新体系，实施绿色技术创新攻关行动，开展重点行业 and 重点产品资源效率对标提升行动。建立统一的绿色产品标准、认证、标识体系，完善节能家电、高效照明产品、节水器具推广机制。深入开展绿

色生活创建行动。

第四节 构建绿色发展政策体系

强化绿色发展的法律和政策保障。实施有利于节能环保和资源综合利用的税收政策。大力发展绿色金融。健全自然资源有偿使用制度，创新完善自然资源、污水垃圾处理、用水用能等领域价格形成机制。推进固定资产投资项目节能审查、节能监察、重点用能单位管理制度改革。完善能效、水效“领跑者”制度。强化高耗水行业用水定额管理。深化生态文明试验区建设。深入推进山西国家资源型经济转型综合配套改革试验区建设和能源革命综合改革试点。

专栏 15 环境保护和资源节约工程	
01 大气污染物减排	实施 8.5 亿吨水泥熟料、4.6 亿吨焦化产能和 4000 台左右有色行业炉窑清洁生产改造，完成 5.3 亿吨钢铁产能超低排放改造，开展石化、化工、涂装、医药、包装印刷等重点行业挥发性有机物治理改造，推进大气污染防治重点区域散煤清零。
02 水污染防治和水生态修复	巩固地级及以上城市黑臭水体治理成效，推进 363 个县级城市建成区 1500 段黑臭水体综合治理。加强太湖、巢湖、滇池、丹江口水库、洱海、白洋淀、鄱阳湖、洞庭湖、查干湖、乌梁素海等重点湖库污染防治和生态修复，实施永定河、木兰溪等综合治理，加快华北地区及其他重点区域地下水超采综合治理和黄河河口综合治理。
03 土壤污染防治与安全利用	在土壤污染面积较大的 100 个县推进农用地安全利用示范。以化工、有色金属行业为重点，实施 100 个土壤污染源头管控项目。
04 城镇污水垃圾处理设施	新增和改造污水收集管网 8 万公里，新增污水处理能力 2000 万立方米/日。加快垃圾焚烧设施建设，城市生活垃圾日清运量超过 300 吨地区实现原生垃圾零填埋，开展小型生活垃圾焚烧设施建设试点。
05 医废危废处置和固废综合利用	补齐医疗废弃物处置设施短板，建设国家和 6 个区域性危废风险防控技术中心、20 个区域性特殊危废集中处置中心。以尾矿和共伴生矿、煤矸石、粉煤灰、建筑垃圾等为重点，开展 100 个大宗固体废物综合利用示范。
06 资源节约利用	实施重大节能低碳技术产业化示范工程，开展近零能耗建筑、近零碳排放、碳捕集利用与封存（CCUS）等重大项目示范。开展 60 个大中城市废旧物资循环利用体系建设。

第十二篇 实行高水平对外开放 开拓合作共赢新局面

坚持实施更大范围、更宽领域、更深层次对外开放，依托我国超大市场规模优势，促进国际合作，实现互利共赢，推动共建“一带一路”行稳致远，推动构建人类命运共同体。

第四十章 建设更高水平开放型经济新体制

全面提高对外开放水平，推进贸易和投资自由化便利化，持续深化商品和要素流动型开放，稳步拓展规则、规制、管理、标准等制度型开放。

第一节 加快推进制度型开放

构建与国际通行规则相衔接的制度体系和监管模式。健全外商投资准入前国民待遇加负面清单管理制度，进一步缩减外资准入负面清单，落实准入后国民待遇，促进内外资企业公平竞争。建立健全跨境服务贸易负面清单管理制度，健全技术贸易促进体系。稳妥推进银行、证券、保险、基金、期货等金融领域开放，深化境内外资本市场互联互通，健全合格境外投资者制度。稳慎推进人民币国际化，坚持市场驱动和企业自主选择，营造以人民币自由使用为基础的新型互利合作关系。完善出入境、海关、外汇、税收等环节管理服务。

第二节 提升对外开放平台功能

统筹推进各类开放平台建设，打造开放层次更高、营商环境更优、辐射作用更强的开放新高地。完善自由贸易试验区布局，赋予其更大改革自主权，深化首创性、集成化、差别化改革探索，积极复制推广制度创新成果。稳步推进海南自由贸易港建设，以货物贸易“零关税”、服务贸易“既准入又准营”为方向推进贸易自由化便利化，大幅放宽市场准入，全面推行“极简审批”投资制度，开展跨境证券投融资改革试点和数据跨境传输安全管理试点，实施更加开放的人才、出入境、运输等政策，制定出台海南自由贸易港法，初步建立中国特色自由贸易港政策和制度体系。创新提升国家级新区和开发区，促进综合保税区高水平开放，完善沿边重点开发开放试验区、边境经济合作区、跨境经济合作区功能，支持宁夏、贵州、江西建设内陆开放型经济试验区。

第三节 优化区域开放布局

鼓励各地立足比较优势扩大开放，强化区域间开放联动，构建陆海内外联动、东西双向互济的开放格局。巩固东部沿海地区和超大特大城市开放先导地位，率先推动全方位高水平开放。加快中西部和东北地区开放步伐，支持承接国内外产业转移，培育全球重要加工制造基地和新增长极，研究在内陆地区增设国家一类口岸，助推内陆地区成为开放前沿。推动沿边开发开放高质量发展，加快边境贸易创新发展，更好发挥重点口岸和边境城市内外联通作用。支持广西建设面向东盟的开放合作高地、云南建设面向南亚东南亚和环印度洋地区开放的辐射中心。

第四节 健全开放安全保障体系

构筑与更高水平开放相匹配的监管和风险防控体系。健全产业损害预警体系，丰富贸易调整援助、贸易救济等政策工具，妥善应对经贸摩擦。健全外商投资国家安全审查、反垄断审查和国家技术安全清单管理、不可靠实体清单等制度。建立重要资源和产品全球供应链风险预警系统，加强国际供应链保障合作。加强国际收支监测，保持国际收支基本平衡和外汇储备基本稳定。加强对外资产负债监测，建立健全全口径外债监管体系。完善境外投资分类分级监管体系。构建海外利益保护和风险预警防范体系。优化提升驻外外交机构基础设施保障能力，完善领事保护工作体制机制，维护海外中国公民、机构安全和正当权益。

第四十一章 推动共建“一带一路”高质量发展

坚持共商共建共享原则，秉持绿色、开放、廉洁理念，深化务实合作，加强安全保障，促进共同发展。

第一节 加强发展战略和政策对接

推进战略、规划、机制对接，加强政策、规则、标准联通。创新对接方式，推进已签文件落实见效，推动与更多国家商签投资保护协定、避免双重征税协定等，加强海关、税收、监管等合作，推动实施更高水平的通关一体化。拓展规则对接领域，加强融资、贸易、能源、数字信息、农业等领域规则对接合作。促进共建“一带一路”倡议同区域和国际发展议程有效对接、协同增效。

第二节 推进基础设施互联互通

推动陆海天网四位一体联通，以“六廊六路多国多港”为基本框架，构建以新亚欧大陆桥等经济走廊为引领，以中欧班列、陆海新通道等大通道和信息高速路为骨架，以铁路、港口、管网等为依托的互联互通网络，打造国际陆海贸易新通道。聚焦关键通道和关键城市，有序推动重大合作项目建设，将高质量、可持续、抗风险、价格合理、包容可及目标融入项目建设全过程。提高中欧班列开行质量，推动国际陆运贸易规则制定。扩大“丝路海运”品牌影响。推进福建、新疆建设“一带一路”核心区。推进“一带一路”空间信息走廊建设。建设“空中丝绸之路”。

第三节 深化经贸投资务实合作

推动与共建“一带一路”国家贸易投资合作优化升级，积极发展丝路电商。深化国际产能合作，拓展第三方市场合作，构筑互利共赢的产业链供应链合作体系，扩大双向贸易和投资。坚持以企业为主体、市场为导向，遵循国际惯例和债务可持续原则，健全多元化投融资体系。创新融资合作框架，发挥共建“一带一路”专项贷款、丝路基金等作用。建立健全“一带一路”金融合作网络，推动金融基础设施互联互通，支持多边和各国金融机构共同参与投融资。完善“一带一路”风险防控和安全保障体系，强化法律服务保障，有效防范化解各类风险。

第四节 架设文明互学互鉴桥梁

深化公共卫生、数字经济、绿色发展、科技教育、文化艺术等领域人文合作，加强议会、政党、民间组织往来，密切妇女、青年、残疾人等群体交流，形成多元互动的人文交流格局。推进实施共建“一带一路”科技创新行动计划，建设数字丝绸之路、创新丝绸之路。加强应对气候变化、海洋合作、野生动物保护、荒漠化防治等交流合作，推动建设绿色丝绸之路。积极与共建“一带一路”国家开展医疗卫生和传染病防控合作，建设健康丝绸之路。

第四十二章 积极参与全球治理体系改革和建设

高举和平、发展、合作、共赢旗帜，坚持独立自主的和平外交政策，推动构建新型国际关系，推动全球治理体系朝着更加公正合理的方向发展。

第一节 维护和完善多边经济治理机制

维护多边贸易体制，积极参与世界贸易组织改革，坚决维护发展中成员地位。推动二十国集团等发挥国际经济合作功能，建设性参与亚太经合组织、金砖国家等机制经济治理合作，提出更多中国倡议、中国方案。推动主要多边金融机构深化治理改革，支持亚洲基础设施投资银行和新开发银行更好发挥作用，提高参与国际金融治理能力。推动国际宏观经济政策沟通协调，搭建国际合作平台，共同维护全球产业链供应链稳定畅通、全球金融市场稳定，合力促进世界经济增长。推动新兴领域经济治理规则制定。

第二节 构建高标准自由贸易区网络

实施自由贸易区提升战略，构建面向全球的高标准自由贸易区网络。优化自由贸易区布局，推动区域全面经济伙伴关系协定实施，加快中日韩自由贸易协定谈判进程，稳步推进亚太自贸区建设。提升自由贸易区建设水平，积极考虑加入全面与进步跨太平洋伙伴关系协定，推动商签更多高标准自由贸易协定和区域贸易协定。

第三节 积极营造良好外部环境

积极发展全球伙伴关系，推进大国协调和合作，深化同周边国家关系，加强同发展中国家团结合作。坚持多边主义和共商共建共享原则，维护以联合国为核心的国际体系和以国际法为基础的国际秩序，共同应对全球性挑战。积极参与重大传染病防控国际合作，推动构建人类卫生健康共同体。深化对外援助体制机制改革，优化对外援助布局，向发展中国家特别是最不发达国家提供力所能及的帮助，加强医疗卫生、科技教育、绿色发展、减贫、人力资源开发、紧急人道主义等领域对外合作和援助。积极落实联合国2030年可持续发展议程。

第十三篇 提升国民素质 促进人的全面发展

把提升国民素质放在突出重要位置，构建高质量的教育体系和全方位全周期的健康体系，优化人口结构，拓展人口质量红利，提升人力资本水平和人的全面发展能力。

第四十三章 建设高质量教育体系

全面贯彻党的教育方针，坚持优先发展教育事业，坚持立德树人，增强学生文明素养、社会责任意识、实践本领，培养德智体美劳全面发展的社会主义建设者和接班人。

第一节 推进基本公共教育均等化

巩固义务教育基本均衡成果，完善办学标准，推动义务教育优质均衡发展和城乡一体化。加快城镇学校扩容增位，保障农业转移人口随迁子女平等享有基本公共教育服务。改善乡村小规模学校和乡镇寄宿制学校条件，加强乡村教师队伍建设，提高乡村教师素质能力，完善留守儿童关爱体系，巩固义务教育控辍保学成果。巩固提升高中阶段教育普及水平，鼓励高中阶段学校多样化发展，高中阶段教育毛入学率提高到92%以上。规范校外培训。完善普惠性学前教育和特殊教育、专门教育保障机制，学前教育毛入园率提高到90%以上。提高民族地区教育质量和水平，加大国家通用语言文字推广力度。

第二节 增强职业技术教育适应性

突出职业技术（技工）教育类型特色，深入推进改革创新，优化结构与布局，大力培养技术技能人才。完善职业技术教育国家标准，推行“学历证书+职业技能等级证书”制度。创新办学模式，深化产教融合、校企合作，鼓励企业举办高质量职业技术教育，探索中国特色学徒制。实施现代职业技术教育质量提升计划，建设一批高水平职业技术学院和专业，稳步发展职业本科教育。深化职普融通，实现职业技术教育与普通教育双向互认、纵向流动。

第三节 提高高等教育质量

推进高等教育分类管理和高等学校综合改革，构建更加多元的高等教育体系，高等教育毛入学率提高到60%。分类建设一流大学和一流学科，支持发展高水平研究型大学。建设高质量本科教育，推进部分普通本科高校向应用型转变。建立学科专业动态调整机制和特色发展引导机制，增强高校学科设置针对性，推进基础学科高层次人才培养模式改革，加快培养理工农医类专业紧缺人才。加强研究生培养管理，提升研究生教育质量，稳步扩大专业学位研究生规模。优化区

域高等教育资源布局，推进中西部地区高等教育振兴。

第四节 建设高素质专业化教师队伍

建立高水平现代教师教育体系，加强师德师风建设，完善教师管理和发政策体系，提升教师教书育人能力素质。重点建设一批师范教育基地，支持高水平综合大学开展教师教育，健全师范生公费教育制度，推进教育类研究生和公费师范生免试认定教师资格改革。支持高水平工科大学举办职业技术师范专业，建立高等学校、职业学校与行业企业联合培养“双师型”教师机制。深化中小学、幼儿园教师管理综合改革，统筹教师编制配置和跨区调整，推进义务教育教师“县管校聘”管理改革，适当提高中高级教师岗位比例。

第五节 深化教育改革

深化新时代教育评价改革，建立健全教育评价制度和机制，发展素质教育，更加注重学生爱国情怀、创新精神和健康人格培养。坚持教育公益性原则，加大教育经费投入，改革完善经费使用管理制度，提高经费使用效益。落实和扩大学校办学自主权，完善学校内部治理结构，有序引导社会参与学校治理。深化考试招生综合改革。支持和规范民办教育发展，开展高水平中外合作办学。发挥在线教育优势，完善终身学习体系，建设学习型社会。推进高水平大学开放教育资源，完善注册学习和弹性学习制度，畅通不同类型学习成果的互认和转换渠道。

专栏 16 教育提质扩容工程	
01 普惠性幼儿园	以人口集中流入地、农村地区和“三区三州”为重点，新建、改扩建2万所幼儿园，增加普惠学位400万个以上。
02 基础教育	以教育基础薄弱县和人口流入地为重点，新建、改扩建中小学校4000所以上。在边境县（团场）建设100所“国门学校”。
03 职业技术教育	支持建设200所以上高水平高职院校和600个以上高水平专业，支持建设一批优秀中职学校和优质专业。
04 高等教育	加强“双一流”建设高校基础研究和协同创新能力建设，提升100所中西部本科高校办学条件，布局建设一批高水平公共卫生学院和高水平师范院校。
05 产教融合平台	围绕集成电路、人工智能、工业互联网、储能等重点领域，布局建设一批国家产教融合创新平台和研究生联合培养基地。建设100个高水平、专业化、开放型产教融合实训基地。

第四十四章 全面推进健康中国建设

把保障人民健康放在优先发展的战略位置，坚持预防为主的方针，深入实施健康中国行动，完善国民健康促进政策，织牢国家公共卫生防护网，为人民提供全方位全生命期健康服务。

第一节 构建强大公共卫生体系

改革疾病预防控制体系，强化监测预警、风险评估、流行病学调查、检验检测、应急处置等职能。建立稳定的公共卫生事业投入机制，改善疾控基础条件，强化基层公共卫生体系。落实医疗机构公共卫生责任，创新医防协同机制。完善突发公共卫生事件监测预警处置机制，加强实验室检测网络建设，健全医疗救治、科技支撑、物资保障体系，提高应对突发公共卫生事件能力。建立分级分层分流的传染病救治网络，建立健全统一的国家公共卫生应急物资储备体系，大型公共建筑预设平疫结合改造接口。筑牢口岸防疫防线。加强公共卫生学院和人才队伍建设。完善公共卫生服务项目，扩大国家免疫规划，强化慢性病预防、早期筛查和综合干预。完善心理健康和精神卫生服务体系。

第二节 深化医药卫生体制改革

坚持基本医疗卫生事业公益属性，以提高医疗质量和效率为导向，以公立医疗机构为主体、非公立医疗机构为补充，扩大医疗服务资源供给。加强公立医院建设，加快建立现代医院管理制度，深入推进治理结构、人事薪酬、编制管理和绩效考核改革。加快优质医疗资源扩容和区域均衡布局，建设国家医学中心和区域医疗中心。加强基层医疗卫生队伍建设，以城市社区和农村基层、边境口岸城市、县级医院为重点，完善城乡医疗服务网络。加快建设分级诊疗体系，积极发展医疗联合体。加强预防、治疗、护理、康复有机衔接。推进国家组织药品和耗材集中带量采购使用改革，发展高端医疗设备。完善创新药物、疫苗、医疗器械等快速审评审批机制，加快临床急需和罕见病治疗药品、医疗器械审评审批，促进临床急需境外已上市新药和医疗器械尽快在境内上市。提升医护人员培养质量与规模，扩大儿科、全科等短缺医师规模，每千人口拥有注册护士数提高到3.8人。实施医师区域注册，推动医师多机构执业。稳步扩大城乡家庭医生签约服务覆盖范围，提高签约服务质量。支持社会办医，鼓励有经验的执业医师开办诊所。

第三节 健全全民医保制度

健全基本医疗保险稳定可持续筹资和待遇调整机制，完善医保缴费参保政策，实行医疗保障待遇清单制度。做实基本医疗保险市级统筹，推动省级统筹。完善基本医疗保险门诊共济保障机制，健全重大疾病医疗保险和救助制度。完善医保目录动态调整机制。推行以按病种付费为主的多元复合式医保支付方式。将符合条件的互联网医疗服务纳入医保支付范围，落实异地就医结算。扎实推进医保标准化、信息化建设，提升经办服务水平。健全医保基金监管机制。稳步建立长期护理保险制度。积极发展商业医疗保险。

第四节 推动中医药传承创新

坚持中西医并重和优势互补，大力发展中医药事业。健全中医药服务体系，发挥中医药在疾病预防、治疗、康复中的独特优势。加强中西医结合，促进少数民族医药发展。加强古典医籍精华的梳理和挖掘，建设中医药科技支撑平台，改革完善中药审评审批机制，促进中药新药研发保护和产业发展。强化中药质量监管，促进中药质量提升。强化中医药特色人才培养，加强中医药文化传承与创新，推动中医药走向世界。

第五节 建设体育强国

广泛开展全民健身运动，增强人民体质。推动健康关口前移，深化体教融合、体卫融合、体旅融合。完善全民健身公共服务体系，推进社会体育场地设施建设和学校场馆开放共享，提高健身步道等便民健身场所覆盖面，因地制宜发展体育公园，支持在不妨碍防洪安全前提下利用河滩地等建设公共体育设施。保障学校体育课和课外锻炼时间，以青少年为重点开展国民体质监测和干预。坚持文化教育和专业训练并重，加强竞技体育后备人才培养，提升重点项目竞技水平，巩固传统项目优势，探索中国特色足球篮球排球发展路径，持续推进冰雪运动发展，发展具有世界影响力的职业体育赛事。扩大体育消费，发展健身休闲、户外运动等体育产业。办好北京冬奥会、冬残奥会及杭州亚运会等。

第六节 深入开展爱国卫生运动

丰富爱国卫生工作内涵，促进全民养成文明健康生活方式。加强公共卫生环境基础设施建设，推进城乡环境卫生整治，强化病媒生物防制。深入推进卫生城镇创建。加强健康教育和健康知识普及，树立良好饮食风尚，制止餐饮浪费行为，开展控烟限酒行动，坚决革除滥食野生动物等陋习，推广分餐公筷、垃圾分类投放等生活习惯。

专栏 17 全民健康保障工程	
01 疾病预防控制	启动中国疾病预防控制中心二期项目，依托现有疾控机构建设 15 个左右区域公共卫生中心，升级改造 20 个左右国家重大传染病防控救治基地，20 个左右国家紧急医学救援基地。
02 国家医学中心	加强国家心血管、呼吸、肿瘤、创伤、儿科等医学中心建设。聚焦重大病种，打造若干引领国内、具有全球影响力的高水平医学中心和医学创新转化中心。
03 区域医疗中心	支持高水平医疗机构在外设医多。医疗资源薄弱的省份建设一批区域医疗中心。建成河北、河南、山西、辽宁、安徽、福建、云南、新疆等区域医疗中心。
04 县级医院	推动省市优质医疗资源支持县级医院发展，力争新增 500 个县级医院（含中医院）达到三级医院设施条件和服务能力。
05 中医药发展	打造 20 个左右国家中医药传承创新中心，20 个左右中西医协同旗舰医院，20 个左右中医疫病防治基地，100 个左右中医特色重点医院，形成一批中医优势专科。
06 全民健身场地设施	新建、改扩建 1000 个左右体育公园，建设户外运动、健身休闲等配套公共基础设施。推进社会足球场地和体育健身步道建设。

第四十五章 实施积极应对人口老龄化国家战略

制定人口长期发展战略，优化生育政策，以“一老一小”为重点完善人口服务体系，促进人口长期均衡发展。

第一节 推动实现适度生育水平

增强生育政策包容性，推动生育政策与经济社会政策配套衔接，减轻家庭生育、养育、教育负担，释放生育政策潜力。完善幼儿养育、青少年发展、老人赡养、病残照料等政策和产假制度，探索实施父母育儿假。改善优生优育全程服务，加强孕前孕产期健康服务，提高出生人口质量。建立健全计划生育特殊困难家庭全方位帮扶保障制度。改革完善人口统计和监测体系，密切监测生育形势。深化人口发展战略研究，健全人口与发展综合决策机制。

第二节 健全婴幼儿发展政策

发展普惠托育服务体系，健全支持婴幼儿照护服务和早期发展的政策体系。加强对家庭照护和社区服务的支持指导，增强家庭科学育儿能力。严格落实城镇小区配套园政策，积极发展多种形式的婴幼儿照护服务机构，鼓励有条件的用人单位提供婴幼儿照护服务，支持企事业单位和社会组织等社会力量提供普惠托育服务，鼓励幼儿园发展托幼一体化服务。推进婴幼儿照护服务专业化、规范化发展，提高保育保教质量和水平。

第三节 完善养老服务体系

推动养老事业和养老产业协同发展，健全基本养老服务体系，大力发展普惠型养老服务，支持家庭承担养老功能，构建居家社区机构相协调、医养康养相结合的养老服务体系。完善社区居家养老服务网络，推进公共设施适老化改造，推动专业机构服务向社区延伸，整合利用存量资源发展社区嵌入式养老。强化对失能、部分失能特困老年人的兜底保障，积极发展农村互助幸福院等互助性养老。深化公办养老机构改革，提升服务能力和水平，完善公建民营管理机制，支持培训疗养资源转型发展养老，加强对护理型民办养老机构的政策扶持，开展普惠养老城企联动专项行动。加强老年健康服务，深入推进医养康养结合。加大养老护理型人才培养力度，扩大养老机构护理型床位供给，养老机构护理型床位占比提高到55%，更好满足高龄失能失智老年人护理服务需求。逐步提升老年人福利水平，完善经济困难高龄失能老年人补贴制度和特殊困难失能留守老年人探访关爱制度。健全养老服务综合监管制度。构建养老、孝老、敬老的社会环境，强化老年人权益保障。综合考虑人均预期寿命提高、人口老龄化趋势加快、受教育年限增加、劳动力结构变化等因素，按照小步调整、弹性实施、分类推进、统筹兼顾等原则，逐步延迟法定退休年龄，促进人力资源充分利用。发展银发经济，开发适老化技术和产品，培育智慧养老等新业态。

专栏 18 “一老一小”服务项目	
01	特殊困难家庭适老化改造 支持 200 万户特殊困难高龄、失能、残疾老年人家庭实施适老化改造，配备辅助器具和防走失装置等设施。
02	社区居家养老服务网络建设 支持 500 个区县建设连锁化运营、标准化管理的示范性社区居家养老服务网络，提供失能护理、日间照料以及助餐助浴助洁助医助行等服务。
03	养老机构服务提升 支持 300 个左右护理型养老机构转型为普惠养老机构，1000 个左右公办养老机构增加护理型床位，支持城市依托基层医疗卫生资源建设医养结合设施。
04	普惠托育服务扩容 支持 150 个城市利用社会力量发展综合托育服务机构和社区托育服务设施，新增示范性普惠托位 50 万个以上。
05	儿童友好城市建设 开展 100 个儿童友好城市示范，加强校外活动场所、社区儿童之家建设和公共空间适儿化改造，完善儿童公共服务设施。

第十四篇 增进民生福祉 提升共建共治共享水平

坚持尽力而为、量力而行，健全基本公共服务体系，加强普惠性、基础性、兜底性民生建设，完善共建共治共享的社会治理制度，制定促进共同富裕行动纲要，自觉主动缩小地区、城乡和收入差距，让发展成果更多更公平惠及全体人民，不断增强人民群众获得感、幸福感、安全感。

第四十六章 健全国家公共服务制度体系

加快补齐基本公共服务短板，着力增强非基本公共服务弱项，努力提升公共服务质量和水平。

第一节 提高基本公共服务均等化水平

推动城乡区域基本公共服务制度统一、质量水平有效衔接。围绕公共教育、就业创业、社会保险、医疗卫生、社会服务、住房保障、公共文化体育、优抚安置、残疾人服务等领域，建立健全基本公共服务标准体系，明确国家标准并建立动态调整机制，推动标准水平城乡区域间衔接平衡。按照常住人口规模和服务半径统筹基本公共服务设施布局 and 共建共享，促进基本公共服务资源向基层延伸、向农村覆盖、向边远地区和生活困难群众倾斜。

第二节 创新公共服务提供方式

区分基本与非基本，突出政府在基本公共服务供给保障中的主体地位，推动非基本公共服务提供主体多元化、提供方式多样化。在育幼、养老等供需矛盾突出的服务领域，支持社会力量扩大普惠性规范性服务供给，保障提供普惠性规范性服务的各类机构平等享受优惠政策。鼓励社会力量通过公建民营、政府购买服务、政府和社会资本合作等方式参与公共服务供给。深化公共服务领域事业单位改革，营造事业单位与社会力量公平竞争的市场环境。

第三节 完善公共服务政策保障体系

优化财政支出结构，优先保障基本公共服务补短板。明确中央和地方在公共服务领域事权和支出责任，加大中央和省级财政对基层政府提供基本公共服务的财力支持。将更多公共服务项目纳入政府购买服务指导性目录，加大政府购买力度，完善财政、融资和土地等优惠政策。在资格准入、职称评定、土地供给、财政支持、政府采购、监督管理等方面公平对待民办与公办机构。

第四十七章 实施就业优先战略

健全有利于更充分更高质量就业的促进机制，扩大就业容量，提升就业质量，缓解结构性就业矛盾。

第一节 强化就业优先政策

坚持经济发展就业导向，健全就业目标责任考核机制和就业影响评估机制。完善高校毕业生、退役军人、农民工等重点群体就业支持体系。完善与就业容量挂钩的产业政策，支持吸纳就业能力强的服务业、中小微企业和劳动密集型企业发展，稳定拓展社区超市、便利店和社区服务岗位。促进平等就业，增加高质量就业，注重发展技能密集型产业，支持和规范发展新就业形态，扩大政府购买基层教育、医疗和专业化社会服务规模。建立促进创业带动就业、多渠道灵活就业机制，全面清理各类限制性政策，增强劳动力市场包容性。统筹城乡就业政策，积极引导农村劳动力就业。扩大公益性岗位安置，着力帮扶残疾人、零就业家庭成员等困难人员就业。

第二节 健全就业公共服务体系

健全覆盖城乡的就业公共服务体系，加强基层公共就业创业服务平台建设，为劳动者和企业免费提供政策咨询、职业介绍、用工指导等服务。构建常态化援企稳岗帮扶机制，统筹用好就业补助资金和失业保险基金。健全劳务输入集中区域与劳务输出省份对接协调机制，加强劳动力跨区域精准对接。加强劳动者权益保障，健全劳动合同制度和劳动关系协调机制，完善欠薪治理长效机制和劳动争议调解仲裁制度，探索建立新业态从业人员劳动权益保障机制。健全就业需求调查和失业监测预警机制。

第三节 全面提升劳动者就业创业能力

健全终身技能培训制度，持续大规模开展职业技能培训。深入实施职业技能提升行动和重点群体专项培训计划，广泛开展新业态新模式从业人员技能培训，有效提高培训质量。统筹各级各类职业技能培训资金，创新使用方式，畅通培训补贴直达企业和培训者渠道。健全培训经费税前扣除政策，鼓励企业开展岗位技能提升培训。支持开展订单式、套餐制培训。建设一批公共实训基地和产教融合基地，推动培训资源共建共享。办好全国职业技能大赛。

第四十八章 优化收入分配结构

坚持居民收入增长和经济增长基本同步、劳动报酬提高和劳动生产率提高基本同步，持续提高低收入群体收入，扩大中等收入群体，更加积极有为地促进共同富裕。

第一节 拓展居民收入增长渠道

坚持按劳分配为主体、多种分配方式并存，提高劳动报酬在初次分配中的比重。健全工资决定、合理增长和支付保障机制，完善最低工资标准和工资指导线形成机制，积极推行工资集体协商制度。完善按要素分配政策制度，健全各类生产要素由市场决定报酬的机制，探索通过土地、资本等要素使用权、收益权增加中低收入群体要素收入。完善国有企业市场化薪酬分配机制，普遍实行全员绩效管理。改革完善体现岗位绩效和分级分类管理的事业单位薪酬制度。规范劳务派遣用工行为，保障劳动者同工同酬。多渠道增加城乡居民财产性收入，提高农民

土地增值收益分享比例，完善上市公司分红制度，创新更多适应家庭财富管理需求的金融产品。完善国有资本收益上缴公共财政制度，加大公共财政支出用于民生保障力度。

第二节 扩大中等收入群体

实施扩大中等收入群体行动计划，以高校和职业院校毕业生、技能型劳动者、农民工等为重点，不断提高中等收入群体比重。提高高校、职业院校毕业生就业匹配度和劳动参与率。拓宽技术工人上升通道，畅通非公有制经济组织、社会组织、自由职业专业技术人员职称申报和技能等级认定渠道，提高技能型人才待遇水平和社会地位。实施高素质农民培育计划，运用农业农村资源和现代经营方式增加收入。完善小微创业者扶持政策，支持个体工商户、灵活就业人员等群体勤劳致富。

第三节 完善再分配机制

加大税收、社会保障、转移支付等调节力度和精准性，发挥慈善等第三次分配作用，改善收入和财富分配格局。健全直接税体系，完善综合与分类相结合的个人所得税制度，加强对高收入者的税收调节和监管。增强社会保障待遇和服务的公平性可及性，完善兜底保障标准动态调整机制。规范收入分配秩序，保护合法收入，合理调节过高收入，取缔非法收入，遏制以垄断和不正当竞争行为获取收入。建立完善个人收入和财产信息系统。健全现代支付和收入监测体系。

第四十九章 健全多层次社会保障体系

坚持应保尽保原则，按照兜底线、织密网、建机制的要求，加快健全覆盖全民、统筹城乡、公平统一、可持续的多层次社会保障体系。

第一节 改革完善社会保险制度

健全养老保险制度体系，促进基本养老保险基金长期平衡。实现基本养老保险全国统筹，放宽灵活就业人员参保条件，实现社会保险法定人群全覆盖。完善划转国有资本充实社保基金制度，优化做强社会保障战略储备基金。完善城镇职工基本养老金合理调整机制，逐步提高城乡居民基础养老金标准。发展多层次、

多支柱养老保险体系，提高企业年金覆盖率，规范发展第三支柱养老保险。推进失业保险、工伤保险向职业劳动者广覆盖，实现省级统筹。推进社保转移接续，完善全国统一的社会保险公共服务平台。

第二节 优化社会救助和慈善制度

以城乡低保对象、特殊困难人员、低收入家庭为重点，健全分层分类的社会救助体系，构建综合救助格局。健全基本生活救助制度和医疗、教育、住房、就业、受灾人员等专项救助制度，完善救助标准和救助对象动态调整机制。健全临时救助政策措施，强化急难社会救助功能。加强城乡救助体系统筹，逐步实现常住地救助申领。积极发展服务类社会救助，推进政府购买社会救助服务。促进慈善事业发展，完善财税等激励政策。规范发展网络慈善平台，加强彩票和公益金管理。

第三节 健全退役军人工作体系和保障制度

完善退役军人事务组织管理体系、工作运行体系和政策制度体系，提升退役军人服务保障水平。深化退役军人安置制度改革，加大教育培训和就业扶持力度，拓展就业领域，提升安置质量。建立健全新型待遇保障体系，完善和落实优抚政策，合理提高退役军人和其他优抚对象待遇标准，做好随调配偶子女工作安排、落户和教育等工作。完善离退休军人和伤病残退役军人移交安置、收治休养制度，加强退役军人服务中心（站）建设，提升优抚医院、光荣院、军供站等建设服务水平。加强退役军人保险制度衔接。大力弘扬英烈精神，加强烈士纪念设施建设和管护，建设军人公墓。深入推动双拥模范城（县）创建。

第五十章 保障妇女未成年人和残疾人基本权益

坚持男女平等基本国策，坚持儿童优先发展，提升残疾人关爱服务水平，切实保障妇女、未成年人、残疾人等群体发展权利和机会。

第一节 促进男女平等和妇女全面发展

深入实施妇女发展纲要，持续改善妇女发展环境，促进妇女平等依法行使权利、参与经济社会发展、共享发展成果。保障妇女享有卫生健康服务，完善宫颈

癌、乳腺癌综合防治体系和救助政策。保障妇女平等享有受教育权利，持续提高受教育年限和综合能力素质。保障妇女平等享有经济权益，消除就业性别歧视，依法享有产假和生育津贴，保障农村妇女土地权益。保障妇女平等享有政治权利，推动妇女广泛参与社会事务和民主管理。落实法规政策性别平等评估机制，完善分性别统计制度。提高留守妇女关爱服务水平。严厉打击侵害妇女和女童人身权利的违法犯罪行为。

第二节 提升未成年人关爱服务水平

深入实施儿童发展纲要，优化儿童发展环境，切实保障儿童生存权、发展权、受保护权和参与权。完善儿童健康服务体系，预防和控制儿童疾病，减少儿童死亡和严重出生缺陷发生，有效控制儿童肥胖和近视，实施学龄前儿童营养改善计划。保障儿童公平受教育权利，加强儿童心理健康教育和服务。加强困境儿童分类保障，完善农村留守儿童关爱服务体系，健全孤儿和事实无人抚养儿童保障机制。完善落实未成年人监护制度，严厉打击侵害未成年人权益的违法犯罪行为，完善未成年人综合保护体系。深入实施青年发展规划，促进青年全面发展，搭建青年成长成才和建功立业的平台，激发青年创新创业活力。

第三节 加强家庭建设

以建设文明家庭、实施科学家教、传承优良家风为重点，深入实施家家幸福安康工程。构建支持家庭发展的法律政策体系，推进家庭教育立法进程，加大[反家庭暴力法](#)实施力度，加强婚姻家庭辅导服务，预防和化解婚姻家庭矛盾纠纷。构建覆盖城乡的家庭教育指导服务体系，健全学校家庭社会协同育人机制。促进家庭服务多元化发展。充分发挥家庭家教家风在基层社会治理中的作用。

第四节 提升残疾人保障和发展能力

健全残疾人帮扶制度，帮助残疾人普遍参加基本医疗和基本养老保险，动态调整困难残疾人生活补贴和重度残疾人护理补贴标准。完善残疾人就业支持体系，加强残疾人劳动权益保障，优先为残疾人提供职业技能培训，扶持残疾人自主创业。推进适龄残疾儿童和少年教育全覆盖，提升特殊教育质量。建成康复大学，促进康复服务市场化发展，提高康复辅助器具适配率，提升康复服务质量。

开展重度残疾人托养照护服务。加强残疾人服务设施和综合服务能力建设，完善无障碍环境建设和维护政策体系，支持困难残疾人家庭无障碍设施改造。

专栏 19 社会关爱服务行动	
01 残疾人服务	加强专业化残疾人康复、托养和综合服务设施建设，补贴 110 万户困难重度残疾人家庭无障碍设施改造，提升社区无障碍建设水平。
02 困难儿童关爱	支持儿童福利机构建设，提升孤弃儿童集中养育服务水平。加强留守儿童数量较多的欠发达地区未成年人保护设施建设。建设残疾儿童康复救助定点机构，推动残疾儿童普遍享有基本康复服务。
03 流浪乞讨人员救助	充分利用现有社会福利设施建设流浪乞讨人员救助设施或救助站，实现救助服务网络覆盖全部县市。
04 精神卫生福利设施	在精神卫生服务能力不足的地区建设 100 个左右精神卫生福利设施，为困难精神障碍患者提供集中养护、康复服务。
05 公益性殡葬服务	加强殡仪馆、公益性骨灰安葬（放）设施建设，推动老旧殡仪馆改造，推动基本殡葬服务设施覆盖全部县市。推进农村公墓建设，加大生态殡葬奖补力度。

第五十一章 构建基层社会治理新格局

健全党组织领导的自治、法治、德治相结合的城乡基层社会治理体系，完善基层民主协商制度，建设人人有责、人人尽责、人人享有的社会治理共同体。

第一节 夯实基层社会治理基础

健全党组织领导、村（居）委会主导、人民群众为主体的基层社会治理框架。依法厘清基层政府与基层群众性自治组织的权责边界，制定县（区）职能部门、乡镇（街道）在城乡社区治理方面的权责清单制度，实行工作事项准入制度，减轻基层特别是村级组织负担。加强基层群众性自治组织规范化建设，合理确定其功能、规模和事务范围。加强基层群众自治机制建设，完善村（居）民议事会、理事会、监督委员会等自治载体，健全村（居）民参与社会治理的组织形式和制度化渠道。

第二节 健全社区管理和服务机制

推动社会治理和服务重心下移、资源下沉，提高城乡社区精准化精细化服务管理能力。推进审批权限和公共服务事项向基层延伸，构建网格化管理、精细化服务、信息化支撑、开放共享的基层管理服务平台，推动就业社保、养老托育、扶残助残、医疗卫生、家政服务、物流商超、治安执法、纠纷调处、心理援助等便民服务场景有机集成和精准对接。完善城市社区居委会职能，督促业委会和物业服务企业履行职责，改进社区物业服务管理。构建专职化、专业化的城乡社区工作者队伍。

第三节 积极引导社会力量参与基层治理

发挥群团组织和社会组织在社会治理中的作用，畅通和规范市场主体、新社会阶层、社会工作者和志愿者等参与社会治理的途径，全面激发基层社会治理活力。培育规范化行业协会商会、公益慈善组织、城乡社区社会组织，加强财政补助、购买服务、税收优惠、人才保障等政策支持和事中事后监管。支持和发展社会工作服务机构和志愿服务组织，壮大志愿者队伍，搭建更多志愿服务平台，健全志愿服务体系。

第十五篇 统筹发展和安全 建设更高水平的平安中国

坚持总体国家安全观，实施国家安全战略，维护和塑造国家安全，统筹传统安全和非传统安全，把安全发展贯穿国家发展各领域和全过程，防范和化解影响我国现代化进程的各种风险，筑牢国家安全屏障。

第五十二章 加强国家安全体系和能力建设

坚持政治安全、人民安全、国家利益至上有机统一，以人民安全为宗旨，以政治安全为根本，以经济安全为基础，以军事、科技、文化、社会安全为保障，不断增强国家安全能力。完善集中统一、高效权威的国家安全领导体制，健全国家安全法治体系、战略体系、政策体系、人才体系和运行机制，完善重要领域国家安全立法、制度、政策。巩固国家安全人民防线，加强国家安全宣传教育，增强全民国家安全意识，建立健全国家安全风险研判、防控协同、防范化解机制。健全国家安全审查和监管制度，加强国家安全执法。坚定维护国家政权安全、制度安全、意识形态安全，全面加强网络安全保障体系和能力建设，切实维护新型

领域安全，严密防范和严厉打击敌对势力渗透、破坏、颠覆、分裂活动。

第五十三章 强化国家经济安全保障

强化经济安全风险预警、防控机制和能力建设，实现重要产业、基础设施、战略资源、重大科技等关键领域安全可控，着力提升粮食、能源、金融等领域安全发展能力。

第一节 实施粮食安全战略

实施分品种保障策略，完善重要农产品供给保障体系和粮食产购储加销体系，确保口粮绝对安全、谷物基本自给、重要农副产品供应充足。毫不放松抓好粮食生产，深入实施藏粮于地、藏粮于技战略，开展种源“卡脖子”技术攻关，提高良种自主可控能力。严守耕地红线和永久基本农田控制线，稳定并增加粮食播种面积和产量，合理布局区域性农产品应急保供基地。深化农产品收储制度改革，加快培育多元市场购销主体，改革完善中央储备粮管理体制，提高粮食储备调控能力。强化粮食安全省长责任制和“菜篮子”市长负责制，实行党政同责。有效降低粮食生产、储存、运输、加工环节损耗，开展粮食节约行动。积极开展重要农产品国际合作，健全农产品进口管理机制，推动进口来源多元化，培育国际大粮商和农业企业集团。制定粮食安全保障法。

第二节 实施能源资源安全战略

坚持立足国内、补齐短板、多元保障、强化储备，完善产供储销体系，增强能源持续稳定供应和风险管控能力，实现煤炭供应安全兜底、油气核心需求依靠自保、电力供应稳定可靠。夯实国内产量基础，保持原油和天然气稳产增产，做好煤制油气战略基地规划布局和管控。扩大油气储备规模，健全政府储备和企业社会责任储备有机结合、互为补充的油气储备体系。加强煤炭储备能力建设。完善能源风险应急管控体系，加强重点城市和用户电力供应保障，强化重要能源设施、能源网络安全防护。多元拓展油气进口来源，维护战略通道和关键节点安全。培育以我为主的交易中心和定价机制，积极推进本币结算。加强战略性矿产资源规划管控，提升储备安全保障能力，实施新一轮找矿突破战略行动。

第三节 实施金融安全战略

健全金融风险预防、预警、处置、问责制度体系，落实监管责任和属地责任，对违法违规行为零容忍，守住不发生系统性风险的底线。完善宏观审慎管理体系，保持宏观杠杆率以稳为主、稳中有降。加强系统重要性金融机构和金融控股公司监管，强化不良资产认定和处置，防范化解影子银行风险，有序处置高风险金融机构，严厉打击非法金融活动，健全互联网金融监管长效机制。完善债务风险识别、评估预警和有效防控机制，健全债券市场违约处置机制，推动债券市场统一执法，稳妥化解地方政府隐性债务，严惩逃废债行为。完善跨境资本流动管理框架，加强监管合作，提高开放条件下风险防控和应对能力。加强人民币跨境支付系统建设，推进金融业信息化核心技术安全可控，维护金融基础设施安全。

专栏 20 经济安全保障工程	
01	粮食储备设施 建设高标准粮仓，实施粮食绿色仓储提升工程，整合布局一批大型粮食物流枢纽和园区，提高应急分拨集散和通道衔接能力。
02	油气勘探开发 加强四川、鄂尔多斯、塔里木、准噶尔等重点盆地油气勘探开发，稳定渤海湾、松辽盆地老油区产量，建设川渝天然气生产基地。推进山西沁水盆地、鄂尔多斯市缘煤层气和川南、鄂西、云贵地区页岩气勘探开发，推进页岩油勘探开发，开展南海等地区天然气水合物试采。
03	煤制油气基地 稳妥推进内蒙古鄂尔多斯、陕西榆林、山西晋北、新疆准东、新疆哈密等煤制油气战略基地建设，建立产能和技术储备。
04	电力安全保障 布局一批坚强局部电网，建设本地支撑电源和重要用户应急保安电源。建设电力应急指挥系统，大型水电站安全和应急管理平台。构建电力行业网络安全仿真验证环境和网络安全态势感知平台。
05	新一轮找矿突破战略行动 开展基础性地质调查，优选油气、铀、铜、铝等 100~200 个找矿远景区，提交可供商业勘查的靶区 200~300 处。
06	应急处置能力提升 建设 6 个区域应急救援中心和综合应急实训基地。推动救援装备现代化，升级完善中央和地方综合应急物资储备库，建设一批应急物资物流基地。建设 3 个区域抗与辐射应急监测物资储备库。

第五十四章 全面提高公共安全保障能力

坚持人民至上、生命至上，健全公共安全体制机制，严格落实公共安全责任

和管理制度，保障人民生命安全。

第一节 提高安全生产水平

完善和落实安全生产责任制，建立公共安全隐患排查和安全预防控制体系。建立企业全员安全生产责任制度，压实企业安全生产主体责任。加强安全生产监测预警和监管监察执法，深入推进危险化学品、矿山、建筑施工、交通、消防、民爆、特种设备等重点领域安全整治，实行重大隐患治理逐级挂牌督办和整改效果评价。推进企业安全生产标准化建设，加强工业园区等重点区域安全管理。加强矿山深部开采与重大灾害防治等领域先进技术装备创新应用，推进危险岗位机器人替代。在重点领域推进安全生产责任保险全覆盖。

第二节 严格食品药品安全监管

加强和改进食品药品安全监管制度，完善食品药品安全法律法规和标准体系，探索建立食品安全民事公益诉讼惩罚性赔偿制度。深入实施食品安全战略，加强食品全链条质量安全监管，推进食品安全放心工程建设攻坚行动，加大重点领域食品安全问题联合整治力度。严防严控药品安全风险，构建药品和疫苗全生命周期管理机制，完善药品电子追溯体系，实现重点类别药品全过程来源可溯、去向可追。稳步推进医疗器械唯一标识制度。加强食品药品安全风险监测、抽检和监管执法，强化快速通报和快速反应。

第三节 加强生物安全风险防控

建立健全生物安全风险防控和治理体系，全面提高国家生物安全治理能力。完善国家生物安全风险监测预警体系和防控应急预案制度，健全重大生物安全事件信息统一发布机制。加强动植物疫情和外来入侵物种口岸防控。统筹布局生物安全基础设施，构建国家生物数据中心体系，加强高级别生物安全实验室体系建设和运行管理。强化生物安全资源监管，制定完善人类遗传资源和生物资源目录，建立健全生物技术研究开发风险评估机制。推进生物安全法实施。加强生物安全领域国际合作，积极参与生物安全国际规则制定。

第四节 完善国家应急管理体系

构建统一指挥、专常兼备、反应灵敏、上下联动的应急管理体制，优化国家应急管理能力体系建设，提高防灾减灾救灾能力。坚持分级负责、属地为主，健全中央与地方分级响应机制，强化跨区域、跨流域灾害事故应急协同联动。开展灾害事故风险隐患排查治理，实施公共基础设施安全加固和自然灾害防治能力提升工程，提升洪涝干旱、森林草原火灾、地质灾害、气象灾害、地震等自然灾害防御工程标准。加强国家综合性消防救援队伍建设，增强全灾种救援能力。加强和完善航空应急救援体系与能力。科学调整应急物资储备品类、规模和结构，提高快速调配和紧急运输能力。构建应急指挥信息和综合监测预警网络体系，加强极端条件应急救援通信保障能力建设。发展巨灾保险。

第五十五章 维护社会稳定和安全

正确处理新形势下人民内部矛盾，加强社会治安防控，编织全方位、立体化、智能化社会安全网。

第一节 健全社会矛盾综合治理机制

坚持和发展新时代“枫桥经验”，构建源头防控、排查梳理、纠纷化解、应急处置的社会矛盾综合治理机制。畅通和规范群众诉求表达、利益协调、权益保障通道，完善人民调解、行政调解、司法调解联动工作体系。健全矛盾纠纷多元化解机制，充分发挥调解、仲裁、行政裁决、行政复议、诉讼等防范化解社会矛盾的作用。完善和落实信访制度，依法及时就地解决群众合理诉求。健全社会矛盾风险防控协同机制。健全社会心理服务体系和危机干预机制。

第二节 推进社会治安防控体系现代化

坚持专群结合、群防群治，提高社会治安立体化、法治化、专业化、智能化水平，形成问题联治、工作联动、平安联创的工作机制，健全社会治安防控体系。继续开展好禁毒人民战争和反恐怖斗争，推动扫黑除恶常态化，严厉打击各类违法犯罪活动，提升打击新型网络犯罪和跨国跨区域犯罪能力。坚持打防结合、整体防控，强化社会治安重点地区排查整治，健全社会治安协调联动机制。推进公安大数据智能化平台建设。完善执法司法权力运行监督和制约机制，健全执法司法人员权益保障机制。建设国门安全防控体系。深化国际执法安全务实合作。

第十六篇 加快国防和军队现代化 实现富国和强军相统一

贯彻习近平强军思想，贯彻新时代军事战略方针，坚持党对人民军队的绝对领导，坚持政治建军、改革强军、科技强军、人才强军、依法治军，加快机械化信息化智能化融合发展，全面加强练兵备战，提高捍卫国家主权、安全、发展利益的战略能力，确保2027年实现建军百年奋斗目标。

第五十六章 提高国防和军队现代化质量效益

加快军事理论现代化，与时俱进创新战争和战略指导，健全新时代军事战略体系，发展先进作战理论。加快军队组织形态现代化，深化国防和军队改革，推进军事管理革命，加快军兵种和武警部队转型建设，壮大战略力量和新域新质作战力量，打造高水平战略威慑和联合作战体系，加强军事力量联合训练、联合保障、联合运用。加快军事人员现代化，贯彻新时代军事教育方针，完善三位一体新型军事人才培养体系，锻造高素质专业化新型军事人才方阵。加快武器装备现代化，聚力国防科技自主创新、原始创新，加速战略性前沿性颠覆性技术发展，加速武器装备升级换代和智能化武器装备发展。

第五十七章 促进国防实力和经济实力同步提升

同国家现代化发展相协调，搞好战略层面筹划，深化资源要素共享，强化政策制度协调，完善组织管理、工作运行、政策制度、人才队伍、风险防控体系，构建一体化国家战略体系和能力。推动重点区域、重点领域、新兴领域协调发展，集中力量实施国防领域重大工程。促进军事建设布局与区域经济发展布局有机结合，更好服务国家安全发展战略需要。深化军民科技协同创新，加强海洋、空天、网络空间、生物、新能源、人工智能、量子科技等领域军民统筹发展，推动军地科研设施资源共享，推进军地科研成果双向转化应用和重点产业发展。强化基础设施共建共用，加强新型基础设施统筹建设，加大经济建设项目贯彻国防要求力度。加快建设现代军事物流体系和资产管理体系。加强军地人才联合培养，健全军地人才交流使用、资格认证等制度。优化国防科技工业布局，加快标准化通用化进程。推进武器装备市场准入、空中交通管理等改革。完善国防动员体系，加强应急应战协同，健全强边固防机制，强化全民国防教育，巩固军政军民团结。

维护军人军属合法权益，让军人成为全社会尊崇的职业。

第十七篇 加强社会主义民主法治建设 健全党和国家监督制度

坚持中国共产党领导、人民当家作主、依法治国有机统一，推进中国特色社会主义政治制度自我完善和发展。

第五十八章 发展社会主义民主

坚持和完善党总揽全局、协调各方的领导制度体系，把党的领导落实到国家发展各领域各方面各环节。坚持和完善人民代表大会制度，加强人大对“一府一委两院”的监督，保障人民依法通过各种途径和形式管理国家事务、管理经济文化事业、管理社会事务。坚持和完善中国共产党领导的多党合作和政治协商制度，提高中国特色社会主义参政党建设水平，加强人民政协专门协商机构建设，发挥社会主义协商民主独特优势，提高建言资政和凝聚共识水平。全面贯彻党的民族政策，坚持和完善民族区域自治制度，铸牢中华民族共同体意识，促进各民族共同团结奋斗、共同繁荣发展。全面贯彻党的宗教工作基本方针，坚持我国宗教中国化方向，积极引导宗教与社会主义社会相适应。健全基层群众自治制度，增强群众自我管理、自我服务、自我教育、自我监督实效。发挥工会、共青团、妇联等人民团体作用，把各自联系的群众紧紧凝聚在党的周围。完善大统战工作格局，促进政党关系、民族关系、宗教关系、阶层关系、海内外同胞关系和谐，巩固和发展大团结大联合局面。全面贯彻党的侨务政策，凝聚侨心、服务大局。

第五十九章 全面推进依法治国

坚定不移走中国特色社会主义法治道路，坚持依法治国、依法执政、依法行政共同推进，一体建设法治国家、法治政府、法治社会，实施法治中国建设规划。健全保障宪法全面实施的体制机制，加强宪法实施和监督，落实宪法解释程序机制，推进合宪性审查。完善立法体制机制，加强重点领域、新兴领域、涉外领域立法，立改废释纂并举，完善以宪法为核心的中国特色社会主义法律体系。实施法治政府建设实施纲要，坚持和完善重大行政决策程序制度，深化行政执法体制改革，严格规范公正文明执法，规范执法自由裁量权，推进行政复议体制改革。深化司法体制综合配套改革，完善审判制度、检察制度、刑罚执行制度、律师制

度，全面落实司法责任制，加强对司法活动监督，深化执行体制改革，促进司法公正。实施法治社会建设实施纲要，加强社会主义法治文化建设，深入开展法治宣传教育，实施“八五”普法规划，完善公共法律服务体系、法律援助和国家司法救助制度。全面加强人权司法保护，促进人权事业全面发展。加强涉外法治体系建设，加强涉外法律人才培养。

第六十章 完善党和国家监督体系

健全党统一领导、全面覆盖、权威高效的监督体系，形成决策科学、执行坚决、监督有力的权力运行机制。落实全面从严治党主体责任、监督责任，强化政治监督，深化政治巡视并强化整改落实。推进纪律监督、监察监督、派驻监督、巡视监督统筹衔接，以党内监督为主导、推动各类监督贯通协调，形成常态长效的监督合力，使监督体系更好融入国家治理体系。深化纪检监察体制改革，加强上级纪委监委对下级纪委监委的领导，推进纪检监察工作规范化、法治化，发挥监督保障执行、促进完善发展作用。完善权力配置和运行制约机制，健全分事行权、分岗设权、分级授权、定期轮岗制度，完善党务、政务、司法和各领域办事公开制度，健全发现问题、纠正偏差、精准问责有效机制，构建全覆盖的责任制度和监督制度。坚持无禁区、全覆盖、零容忍，一体推进不敢腐、不能腐、不想腐，营造风清气正的良好政治生态和发展环境。深化反腐败国际合作。锲而不舍落实中央八项规定精神，完善作风建设长效机制，持续纠治形式主义、官僚主义，切实防止享乐主义、奢靡之风反弹回潮，坚决整治群众身边的腐败和不正之风。

第十八篇 坚持“一国两制” 推进祖国统一

保持香港、澳门长期繁荣稳定，推进两岸关系和平发展和祖国统一，共创中华民族伟大复兴的美好未来。

第六十一章 保持香港、澳门长期繁荣稳定

全面准确贯彻“一国两制”、“港人治港”、“澳人治澳”、高度自治的方针，坚持依法治港治澳，维护宪法和基本法确定的特别行政区宪制秩序，落实中央对特别行政区全面管治权，落实特别行政区维护国家安全的法律制度和执行机制，维护国家主权、安全、发展利益和特别行政区社会大局稳定，坚决防范和遏

制外部势力干预港澳事务，支持港澳巩固提升竞争优势，更好融入国家发展大局。

第一节 支持港澳巩固提升竞争优势

支持香港提升国际金融、航运、贸易中心和国际航空枢纽地位，强化全球离岸人民币业务枢纽、国际资产管理中心及风险管理中心功能。支持香港建设国际创新科技中心、亚太区国际法律及解决争议服务中心、区域知识产权贸易中心，支持香港服务业向高端高增值方向发展，支持香港发展中外文化艺术交流中心。支持澳门丰富世界旅游休闲中心内涵，支持粤澳合作共建横琴，扩展中国与葡语国家商贸合作服务平台功能，打造以中华文化为主流、多元文化共存的交流合作基地，支持澳门发展中医药研发制造、特色金融、高新技术和会展商贸等产业，促进经济适度多元发展。

第二节 支持港澳更好融入国家发展大局

完善港澳融入国家发展大局、同内地优势互补、协同发展机制。支持港澳参与、助力国家全面开放和现代化经济体系建设，打造共建“一带一路”功能平台。深化内地与港澳经贸、科创合作关系，深化并扩大内地与港澳金融市场互联互通。高质量建设粤港澳大湾区，深化粤港澳合作、泛珠三角区域合作，推进深圳前海、珠海横琴、广州南沙、深港河套等粤港澳重大合作平台建设。加强内地与港澳各领域交流合作，完善便利港澳居民在内地发展和生活居住的政策措施，加强宪法和基本法教育、国情教育，增强港澳同胞国家意识和爱国精神。支持港澳同各国各地区开展交流合作。

第六十二章 推进两岸关系和平发展和祖国统一

坚持一个中国原则和“九二共识”，以两岸同胞福祉为依归，推动两岸关系和平发展、融合发展，高度警惕和坚决遏制“台独”分裂活动。

第一节 深化两岸融合发展

完善保障台湾同胞福祉和在大陆享受同等待遇的制度和政策，持续出台实施惠台利民政策措施，让台湾同胞分享发展机遇，参与大陆经济社会发展进程。支持台商台企参与“一带一路”建设和国家区域协调发展战略。推进两岸金融合作，

支持符合条件的台资企业在大陆上市。推进海峡两岸产业合作区、平潭综合实验区、昆山深化两岸产业合作试验区等两岸合作平台建设。支持福建探索海峡两岸融合发展新路，加快两岸融合发展示范区建设。加强两岸产业合作，打造两岸共同市场，壮大中华民族经济。

第二节 加强两岸人文交流

积极促进两岸交流合作和人员往来，加深相互理解，增进互信认同。推动两岸文化教育、医疗卫生等领域交流合作，促进社会保障和公共资源共享，支持两岸邻近或条件相当地区基本公共服务均等化、普惠化、便捷化，促进两岸同胞共同传承和创新发展中华优秀传统文化。加强两岸基层和青少年交流，鼓励台湾青年来大陆追梦、筑梦、圆梦。团结广大台湾同胞共同反对“台独”分裂活动，维护和推动两岸关系和平发展，致力中华民族伟大复兴。

第十九篇 加强规划实施保障

坚持党的全面领导，健全规划实施保障机制，更好履行政府职责，最大程度激发各类主体的活力和创造力，形成全面建设社会主义现代化国家的强大合力。

第六十三章 加强党中央集中统一领导

贯彻党把方向、谋大局、定政策、促改革的要求，深入学习贯彻习近平新时代中国特色社会主义思想，增强“四个意识”、坚定“四个自信”、做到“两个维护”，不断提高政治判断力、政治领悟力、政治执行力，把党的领导贯穿到规划实施的各领域和全过程，确保党中央重大决策部署贯彻落实。充分发挥全面从严治党引领保障作用，把完善党和国家监督体系融入规划实施之中。完善上下贯通、执行有力的组织体系，提高各级领导班子和干部适应新时代新要求抓改革、促发展、保稳定的政治能力和专业化水平。

激发全社会参与规划实施的积极性，注重发挥工会、共青团、妇联等作用，充分发挥民主党派、工商联和无党派人士作用，最大限度凝聚全社会共识和力量。构建适应高质量发展要求的内生激励机制，健全激励导向的绩效评价考核机制和尽职免责机制，调动广大干部特别是基层干部的积极性、主动性、创造性。

第六十四章 健全统一规划体系

加快建立健全以国家发展规划为统领，以空间规划为基础，以专项规划、区域规划为支撑，由国家、省、市县级规划共同组成，定位准确、边界清晰、功能互补、统一衔接的国家规划体系。

第一节 强化国家发展规划的统领作用

更好发挥国家发展规划战略导向作用，强化空间规划、专项规划、区域规划对本规划实施的支撑。按照本规划确定的国土空间开发保护要求和重点任务，制定实施国家级空间规划，为重大战略任务落地提供空间保障。聚焦本规划确定的战略重点和主要任务，在科技创新、数字经济、绿色生态、民生保障等领域，制定实施一批国家级重点专项规划，明确细化落实发展任务的时间表和路线图。根据本规划确定的区域发展战略任务，制定实施一批国家级区域规划实施方案。加强地方规划对本规划提出的发展战略、主要目标、重点任务、重大工程项目的贯彻落实。

第二节 加强规划衔接协调

健全目录清单、编制备案、衔接协调等规划管理制度，制定“十四五”国家级专项规划等目录清单，依托国家规划综合管理信息平台推进规划备案，将各类规划纳入统一管理。建立健全规划衔接协调机制，报请党中央、国务院批准的规划及省级发展规划报批前须与本规划进行衔接，确保国家级空间规划、专项规划、区域规划等各级各类规划与本规划在主要目标、发展方向、总体布局、重大政策、重大工程、风险防控等方面协调一致。

第六十五章 完善规划实施机制

加强对本规划实施的组织、协调和督导，建立健全规划实施监测评估、政策保障、考核监督机制。

第一节 落实规划实施责任

各地区、各部门要根据职责分工，制定本规划涉及本地区、本部门的主要目标任务实施方案。本规划确定的约束性指标、重大工程项目和公共服务、生态环保、安全保障等领域任务，要明确责任主体和进度要求，合理配置公共资源，引

导调控社会资源，确保如期完成。本规划提出的预期性指标和产业发展、结构调整等领域任务，主要依靠发挥市场主体作用实现，各级政府要创造良好的政策环境、体制环境和法治环境。年度计划要贯彻本规划提出的发展目标和重点任务，将本规划确定的主要指标分解纳入年度计划指标体系，设置年度目标并做好年度间综合平衡，合理确定年度工作重点。

第二节 加强规划实施监测评估

开展规划实施情况动态监测、中期评估和总结评估，中期评估和总结评估情况按程序提请中央政治局常委会审议，并依法向全国人民代表大会常务委员会报告规划实施情况，自觉接受人大监督。发挥国家监察机关和审计机关对推进规划实施的监督作用。规划实施情况纳入各有关部门、地方领导班子和干部评价体系，作为改进政府工作的重要依据。需要对本规划进行调整时，由国务院提出调整方案，报全国人民代表大会常务委员会批准。

第三节 强化政策协同保障

坚持规划定方向、财政作保障、金融为支撑、其他政策相协调，着力构建规划与宏观政策协调联动机制。按照本规划目标任务、结合经济发展形势，合理确定宏观政策取向。坚持公共财政服从和服务于公共政策，增强国家重大战略任务财力保障，加强中期财政规划和年度预算、政府投资计划与本规划实施的衔接协调，中央财政性资金优先投向本规划确定的重大任务和重大工程项目。坚持项目跟着规划走、资金和要素跟着项目走，依据本规划制定重大工程项目清单，对清单内工程项目简化审批核准程序，优先保障规划选址、土地供应和资金需求，单体重大工程项目用地需求由国家统一保障。

第四节 加快发展规划立法

坚持依法制定规划、依法实施规划的原则，将党中央、国务院关于统一规划体系建设和国家发展规划的规定、要求和行之有效的经验做法以法律形式固定下来，加快出台发展规划法，强化规划编制实施的法治保障。

二、行政法规

(一) 中华人民共和国政府信息公开条例

(2007年4月5日中华人民共和国国务院令第492号公布，2019年4月3日中华人民共和国国务院令第711号修订)

第一章 总 则

第一条 为了保障公民、法人和其他组织依法获取政府信息，提高政府工作的透明度，建设法治政府，充分发挥政府信息对人民群众生产、生活和经济社会活动的服务作用，制定本条例。

第二条 本条例所称政府信息，是指行政机关在履行行政管理职能过程中制作或者获取的，以一定形式记录、保存的信息。

第三条 各级人民政府应当加强对政府信息公开工作的组织领导。

国务院办公厅是全国政府信息公开工作的主管部门，负责推进、指导、协调、监督全国的政府信息公开工作。

县级以上地方人民政府办公厅（室）是本行政区域的政府信息公开工作主管部门，负责推进、指导、协调、监督本行政区域的政府信息公开工作。

实行垂直领导的部门的办公厅（室）主管本系统的政府信息公开工作。

第四条 各级人民政府及县级以上人民政府部门应当建立健全本行政机关的政府信息公开工作制度，并指定机构（以下统称政府信息公开工作机构）负责本行政机关政府信息公开的日常工作。

政府信息公开工作机构的具体职能是：

- 1、办理本行政机关的政府信息公开事宜；
- 2、维护和更新本行政机关公开的政府信息；
- 3、组织编制本行政机关的政府信息公开指南、政府信息公开目录和政府信息公开工作年度报告；
- 4、组织开展对拟公开政府信息的审查；
- 5、本行政机关规定的与政府信息公开有关的其他职能。

第五条 行政机关公开政府信息，应当坚持以公开为常态、不公开为例外，

遵循公正、公平、合法、便民的原则。

第六条 行政机关应当及时、准确地公开政府信息。

行政机关发现影响或者可能影响社会稳定、扰乱社会和经济管理秩序的虚假或者不完整信息的，应当发布准确的政府信息予以澄清。

第七条 各级人民政府应当积极推进政府信息公开工作，逐步增加政府信息公开的内容。

第八条 各级人民政府应当加强政府信息资源的规范化、标准化、信息化管理，加强互联网政府信息公开平台建设，推进政府信息公开平台与政务服务平台融合，提高政府信息公开在线办理水平。

第九条 公民、法人和其他组织有权对行政机关的政府信息公开工作进行监督，并提出批评和建议。

第二章 公开的主体和范围

第十条 行政机关制作的政府信息，由制作该政府信息的行政机关负责公开。行政机关从公民、法人和其他组织获取的政府信息，由保存该政府信息的行政机关负责公开；行政机关获取的其他行政机关的政府信息，由制作或者最初获取该政府信息的行政机关负责公开。法律、法规对政府信息公开的权限另有规定的，从其规定。

行政机关设立的派出机构、内设机构依照法律、法规对外以自己名义履行行政管理职能的，可以由该派出机构、内设机构负责与所履行行政管理职能有关的政府信息公开工作。

两个以上行政机关共同制作的政府信息，由牵头制作的行政机关负责公开。

第十一条 行政机关应当建立健全政府信息公开协调机制。行政机关公开政府信息涉及其他机关的，应当与有关机关协商、确认，保证行政机关公开的政府信息准确一致。

行政机关公开政府信息依照法律、行政法规和国家有关规定需要批准的，经批准予以公开。

第十二条 行政机关编制、公布的政府信息公开指南和政府信息公开目录应当及时更新。

政府信息公开指南包括政府信息的分类、编排体系、获取方式和政府信息公

开工作机构的名称、办公地址、办公时间、联系电话、传真号码、互联网联系方式等内容。

政府信息公开目录包括政府信息的索引、名称、内容概述、生成日期等内容。

第十三条 除本条例第十四条、第十五条、第十六条规定的政府信息外，政府信息应当公开。

行政机关公开政府信息，采取主动公开和依申请公开的方式。

第十四条 依法确定为国家秘密的政府信息，法律、行政法规禁止公开的政府信息，以及公开后可能危及国家安全、公共安全、经济安全、社会稳定的政府信息，不予公开。

第十五条 涉及商业秘密、个人隐私等公开会对第三方合法权益造成损害的政府信息，行政机关不得公开。但是，第三方同意公开或者行政机关认为不公开会对公共利益造成重大影响的，予以公开。

第十六条 行政机关的内部事务信息，包括人事管理、后勤管理、内部工作流程等方面的信息，可以不予公开。

行政机关在履行行政管理职能过程中形成的讨论记录、过程稿、磋商信函、请示报告等过程性信息以及行政执法案卷信息，可以不予公开。法律、法规、规章规定上述信息应当公开的，从其规定。

第十七条 行政机关应当建立健全政府信息公开审查机制，明确审查的程序和责任。

行政机关应当依照《中华人民共和国保守国家秘密法》以及其他法律、法规和国家有关规定对拟公开的政府信息进行审查。

行政机关不能确定政府信息是否可以公开的，应当依照法律、法规和国家有关规定报有关主管部门或者保密行政管理部门确定。

第十八条 行政机关应当建立健全政府信息管理动态调整机制，对本行政机关不予公开的政府信息进行定期评估审查，对因情势变化可以公开的政府信息应当公开。

第三章 主动公开

第十九条 对涉及公众利益调整、需要公众广泛知晓或者需要公众参与决策的政府信息，行政机关应当主动公开。

第二十条 行政机关应当依照本条例第十九条的规定，主动公开本行政机关的下列政府信息：

- 1、行政法规、规章和规范性文件；
- 2、机关职能、机构设置、办公地址、办公时间、联系方式、负责人姓名；
- 3、国民经济和社会发展规划、专项规划、区域规划及相关政策；
- 4、国民经济和社会发展统计信息；
- 5、办理行政许可和其他对外管理服务事项的依据、条件、程序以及办理结果；
- 6、实施行政处罚、行政强制的依据、条件、程序以及本行政机关认为具有一定社会影响的行政处罚决定；
- 7、财政预算、决算信息；
- 8、行政事业性收费项目及其依据、标准；
- 9、政府集中采购项目的目录、标准及实施情况；
- 10、重大建设项目的批准和实施情况；
- 11、扶贫、教育、医疗、社会保障、促进就业等方面的政策、措施及其实施情况；
- 12、突发公共事件的应急预案、预警信息及应对情况；
- 13、环境保护、公共卫生、安全生产、食品药品、产品质量的监督检查情况；
- 14、公务员招考的职位、名额、报考条件等事项以及录用结果；
- 15、法律、法规、规章和国家有关规定规定应当主动公开的其他政府信息。

第二十一条 除本条例第二十条规定的政府信息外，设区的市级、县级人民政府及其部门还应当根据本地方的具体情况，主动公开涉及市政建设、公共服务、公益事业、土地征收、房屋征收、治安管理、社会救助等方面的政府信息；乡（镇）人民政府还应当根据本地方的具体情况，主动公开贯彻落实农业农村政策、农田水利工程建设运营、农村土地承包经营权流转、宅基地使用情况审核、土地征收、房屋征收、筹资筹劳、社会救助等方面的政府信息。

第二十二条 行政机关应当依照本条例第二十条、第二十一条的规定，确定主动公开政府信息的具体内容，并按照上级行政机关的部署，不断增加主动公开的内容。

第二十三条 行政机关应当建立健全政府信息发布机制，将主动公开的政府信息通过政府公报、政府网站或者其他互联网政务媒体、新闻发布会以及报刊、广播、电视等途径予以公开。

第二十四条 各级人民政府应当加强依托政府门户网站公开政府信息的工作，利用统一的政府信息公开平台集中发布主动公开的政府信息。政府信息公开平台应当具备信息检索、查阅、下载等功能。

第二十五条 各级人民政府应当在国家档案馆、公共图书馆、政务服务场所设置政府信息查阅场所，并配备相应的设施、设备，为公民、法人和其他组织获取政府信息提供便利。

行政机关可以根据需要设立公共查阅室、资料索取点、信息公告栏、电子信息屏等场所、设施，公开政府信息。

行政机关应当及时向国家档案馆、公共图书馆提供主动公开的政府信息。

第二十六条 属于主动公开范围的政府信息，应当自该政府信息形成或者变更之日起20个工作日内及时公开。法律、法规对政府信息公开的期限另有规定的，从其规定。

第四章 依申请公开

第二十七条 除行政机关主动公开的政府信息外，公民、法人或者其他组织可以向地方各级人民政府、对外以自己名义履行行政管理职能的县级以上人民政府部门（含本条例第十条第二款规定的派出机构、内设机构）申请获取相关政府信息。

第二十八条 本条例第二十七条规定的行政机关应当建立完善政府信息公开申请渠道，为申请人依法申请获取政府信息提供便利。

第二十九条 公民、法人或者其他组织申请获取政府信息的，应当向行政机关的政府信息公开工作机构提出，并采用包括信件、数据电文在内的书面形式；采用书面形式确有困难的，申请人可以口头提出，由受理该申请的政府信息公开工作机构代为填写政府信息公开申请。

政府信息公开申请应当包括下列内容：

- 1、申请人的姓名或者名称、身份证明、联系方式；
- 2、申请公开的政府信息的名称、文号或者便于行政机关查询的其他特征性

描述；

3、申请公开的政府信息的形式要求，包括获取信息的方式、途径。

第三十条 政府信息公开申请内容不明确的，行政机关应当给予指导和释明，并自收到申请之日起7个工作日内一次性告知申请人作出补正，说明需要补正的事项和合理的补正期限。答复期限自行政机关收到补正的申请之日起计算。申请人无正当理由逾期不补正的，视为放弃申请，行政机关不再处理该政府信息公开申请。

第三十一条 行政机关收到政府信息公开申请的时间，按照下列规定确定：

1、申请人当面提交政府信息公开申请的，以提交之日为收到申请之日；

2、申请人以邮寄方式提交政府信息公开申请的，以行政机关签收之日为收到申请之日；以平常信函等无需签收的邮寄方式提交政府信息公开申请的，政府信息公开工作机构应当于收到申请的当日与申请人确认，确认之日为收到申请之日；

3、申请人通过互联网渠道或者政府信息公开工作机构的传真提交政府信息公开申请的，以双方确认之日为收到申请之日。

第三十二条 依申请公开的政府信息公开会损害第三方合法权益的，行政机关应当书面征求第三方的意见。第三方应当自收到征求意见书之日起15个工作日内提出意见。第三方逾期未提出意见的，由行政机关依照本条例的规定决定是否公开。第三方不同意公开且有合理理由的，行政机关不予公开。行政机关认为不公开可能对公共利益造成重大影响的，可以决定予以公开，并将决定公开的政府信息内容和理由书面告知第三方。

第三十三条 行政机关收到政府信息公开申请，能够当场答复的，应当当场予以答复。

行政机关不能当场答复的，应当自收到申请之日起20个工作日内予以答复；需要延长答复期限的，应当经政府信息公开工作机构负责人同意并告知申请人，延长的期限最长不得超过20个工作日。

行政机关征求第三方和其他机关意见所需时间不计算在前款规定的期限内。

第三十四条 申请公开的政府信息由两个以上行政机关共同制作的，牵头制作的行政机关收到政府信息公开申请后可以征求相关行政机关的意见，被征求意见

见机关应当自收到征求意见书之日起15个工作日内提出意见，逾期未提出意见的视为同意公开。

第三十五条 申请人申请公开政府信息的数量、频次明显超过合理范围，行政机关可以要求申请人说明理由。行政机关认为申请理由不合理的，告知申请人不予处理；行政机关认为申请理由合理，但是无法在本条例第三十三条规定的期限内答复申请人的，可以确定延迟答复的合理期限并告知申请人。

第三十六条 对政府信息公开申请，行政机关根据下列情况分别作出答复：

- 1、所申请公开信息已经主动公开的，告知申请人获取该政府信息的方式、途径；
- 2、所申请公开信息可以公开的，向申请人提供该政府信息，或者告知申请人获取该政府信息的方式、途径和时间；
- 3、行政机关依据本条例的规定决定不予公开的，告知申请人不予公开并说明理由；
- 4、经检索没有所申请公开信息的，告知申请人该政府信息不存在；
- 5、所申请公开信息不属于本行政机关负责公开的，告知申请人并说明理由；能够确定负责公开该政府信息的行政机关的，告知申请人该行政机关的名称、联系方式；
- 6、行政机关已就申请人提出的政府信息公开申请作出答复、申请人重复申请公开相同政府信息的，告知申请人不予重复处理；
- 7、所申请公开信息属于工商、不动产登记资料等信息，有关法律、行政法规对信息的获取有特别规定的，告知申请人依照有关法律、行政法规的规定办理。

第三十七条 申请公开的信息中含有不应当公开或者不属于政府信息的内容，但是能够作区分处理的，行政机关应当向申请人提供可以公开的政府信息内容，并对不予公开的内容说明理由。

第三十八条 行政机关向申请人提供的信息，应当是已制作或者获取的政府信息。除依照本条例第三十七条的规定能够作区分处理的外，需要行政机关对现有政府信息进行加工、分析的，行政机关可以不予提供。

第三十九条 申请人以政府信息公开申请的形式进行信访、投诉、举报等活动，行政机关应当告知申请人不作为政府信息公开申请处理并可以告知通过相应

渠道提出。

申请人提出的申请内容为要求行政机关提供政府公报、报刊、书籍等公开出版物的，行政机关可以告知获取的途径。

第四十条 行政机关依申请公开政府信息，应当根据申请人的要求及行政机关保存政府信息的实际情况，确定提供政府信息的具体形式；按照申请人要求的形式提供政府信息，可能危及政府信息载体安全或者公开成本过高的，可以通过电子数据以及其他适当形式提供，或者安排申请人查阅、抄录相关政府信息。

第四十一条 公民、法人或者其他组织有证据证明行政机关提供的与其自身相关的政府信息记录不准确的，可以要求行政机关更正。有权更正的行政机关审核属实的，应当予以更正并告知申请人；不属于本行政机关职能范围的，行政机关可以转送有权更正的行政机关处理并告知申请人，或者告知申请人向有权更正的行政机关提出。

第四十二条 行政机关依申请提供政府信息，不收取费用。但是，申请人申请公开政府信息的数量、频次明显超过合理范围的，行政机关可以收取信息处理费。

行政机关收取信息处理费的具体办法由国务院价格主管部门会同国务院财政部门、全国政府信息公开工作主管部门制定。

第四十三条 申请公开政府信息的公民存在阅读困难或者视听障碍的，行政机关应当为其提供必要的帮助。

第四十四条 多个申请人就相同政府信息向同一行政机关提出公开申请，且该政府信息属于可以公开的，行政机关可以纳入主动公开的范围。

对行政机关依申请公开的政府信息，申请人认为涉及公共利益调整、需要公众广泛知晓或者需要公众参与决策的，可以建议行政机关将该信息纳入主动公开的范围。行政机关经审核认为属于主动公开范围的，应当及时主动公开。

第四十五条 行政机关应当建立健全政府信息公开申请登记、审核、办理、答复、归档的工作制度，加强工作规范。

第五章 监督和保障

第四十六条 各级人民政府应当建立健全政府信息公开工作考核制度、社会评议制度和责任追究制度，定期对政府信息公开工作进行考核、评议。

第四十七条 政府信息公开工作主管部门应当加强对政府信息公开工作的日常指导和监督检查，对行政机关未按照要求开展政府信息公开工作的，予以督促整改或者通报批评；需要对负有责任的领导人员和直接责任人员追究责任的，依法向有权机关提出处理建议。

公民、法人或者其他组织认为行政机关未按照要求主动公开政府信息或者对政府信息公开申请不依法答复处理的，可以向政府信息公开工作主管部门提出。政府信息公开工作主管部门查证属实的，应当予以督促整改或者通报批评。

第四十八条 政府信息公开工作主管部门应当对行政机关的政府信息公开工作人员定期进行培训。

第四十九条 县级以上人民政府部门应当在每年1月31日前向本级政府信息公开工作主管部门提交本行政机关上一年度政府信息公开工作年度报告并向社会公布。

县级以上地方人民政府的政府信息公开工作主管部门应当在每年3月31日前向社会公布本级政府上一年度政府信息公开工作年度报告。

第五十条 政府信息公开工作年度报告应当包括下列内容：

- 1、行政机关主动公开政府信息的情况；
- 2、行政机关收到和处理政府信息公开申请的情况；
- 3、因政府信息公开工作被申请行政复议、提起行政诉讼的情况；
- 4、政府信息公开工作存在的主要问题及改进情况，各级人民政府的政府信息公开工作年度报告还应当包括工作考核、社会评议和责任追究结果情况；
- 5、其他需要报告的事项。

全国政府信息公开工作主管部门应当公布政府信息公开工作年度报告统一格式，并适时更新。

第五十一条 公民、法人或者其他组织认为行政机关在政府信息公开工作中侵犯其合法权益的，可以向上一级行政机关或者政府信息公开工作主管部门投诉、举报，也可以依法申请行政复议或者提起行政诉讼。

第五十二条 行政机关违反本条例的规定，未建立健全政府信息公开有关制度、机制的，由上一级行政机关责令改正；情节严重的，对负有责任的领导人员和直接责任人员依法给予处分。

第五十三条 行政机关违反本条例的规定，有下列情形之一的，由上一级行政机关责令改正；情节严重的，对负有责任的领导人员和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：

- 1、不依法履行政府信息公开职能；
- 2、不及时更新公开的政府信息内容、政府信息公开指南和政府信息公开目录；
- 3、违反本条例规定的其他情形。

第六章 附 则

第五十四条 法律、法规授权的具有管理公共事务职能的组织公开政府信息的活动，适用本条例。

第五十五条 教育、卫生健康、供水、供电、供气、供热、环境保护、公共交通等与人民群众利益密切相关的公共企事业单位，公开在提供社会公共服务过程中制作、获取的信息，依照相关法律、法规和国务院有关主管部门或者机构的规定执行。全国政府信息公开工作主管部门根据实际需要可以制定专门的规定。

前款规定的公共企事业单位未依照相关法律、法规和国务院有关主管部门或者机构的规定公开在提供社会公共服务过程中制作、获取的信息，公民、法人或者其他组织可以向有关主管部门或者机构申诉，接受申诉的部门或者机构应当及时调查处理并将处理结果告知申诉人。

第五十六条 本条例自2019年5月15日起施行。

(二) 国务院关于加快推进全国一体化在线政务服务平台建设的指导意见

(国发〔2018〕27号)

各省、自治区、直辖市人民政府，国务院各部委、各直属机构：

党的十八大以来，各地区各部门认真贯彻党中央、国务院决策部署，围绕转变政府职能、深化简政放权、创新监管方式、优化政务服务，深入推进“互联网+政务服务”，加快建设地方和部门政务服务平台，一些地方和部门依托平台创新政务服务模式，“只进一扇门”、“最多跑一次”、“不见面审批”等改革措施不断涌现，政务服务平台已成为提升政务服务水平的重要支撑，对深化“放管服”改革、优化营商环境、便利企业和群众办事创业发挥了重要作用。但同时，政务服务平台建设管理分散、办事系统繁杂、事项标准不一、数据共享不畅、业务协同不足等问题较为普遍，政务服务整体效能不强，办事难、办事慢、办事繁的问题还不同程度存在，需要进一步强化顶层设计、强化整体联动、强化规范管理，加快建设全国一体化在线政务服务平台。为深入推进“放管服”改革，全面提升政务服务规范化、便利化水平，更好为企业和群众提供全流程一体化在线服务，推动政府治理现代化，现就加快推进全国一体化在线政务服务平台建设提出以下意见。

一、总体要求

(一) 指导思想。

全面贯彻党的十九大和十九届二中、三中全会精神，以习近平新时代中国特色社会主义思想为指导，统筹推进“五位一体”总体布局和协调推进“四个全面”战略布局，坚持以人民为中心的发展思想，牢固树立新发展理念，充分发挥市场在资源配置中的决定性作用，更好发挥政府作用，推动“放管服”改革向纵深发展，深入推进“互联网+政务服务”，加快建设全国一体化在线政务服务平台，整合资源，优化流程，强化协同，着力解决企业和群众关心的热点难点问题，推动政务服务从政府供给导向向群众需求导向转变，从“线下跑”向“网上办”、

“分头办”向“协同办”转变，全面推进“一网通办”，为优化营商环境、便利企业和群众办事、激发市场活力和社会创造力、建设人民满意的服务型政府提供有力支撑。

（二）工作原则。

坚持全国统筹。加强顶层设计，做好政策衔接，注重统分结合，完善统筹协调工作机制。强化标准规范，推进服务事项、办事流程、数据交换等方面标准化建设。充分利用各地区各部门已建政务服务平台，整合各类政务服务资源，协同共建，整体联动，不断提升建设集约化、管理规范化的服务便利化水平。

坚持协同共享。坚持政务服务上网是原则、不上网是例外，联网是原则、孤网是例外，推动线上线下深度融合，充分发挥国家政务服务平台的公共入口、公共通道、公共支撑作用，以数据共享为核心，不断提升跨地区、跨部门、跨层级业务协同能力，推动面向市场主体和群众的政务服务事项公开、政务服务数据开放共享，深入推进“网络通”、“数据通”、“业务通”。

坚持优化流程。坚持问题导向和需求导向，梳理企业和群众办事的“难点”、“堵点”、“痛点”，聚焦需要反复跑、窗口排队长的事项和“进多站、跑多网”等问题，充分运用互联网和信息化发展成果，优化政务服务流程，创新服务方式，强化全国一体化在线政务服务平台功能，不断提升用户体验，推动政务服务更加便利高效，切实提升企业和群众获得感、满意度。

坚持试点先行。选择有基础、有条件的部分省（自治区、直辖市）和国务院部门先行试点，推动在全国一体化在线政务服务平台建设管理、服务模式、流程优化等方面积极探索、不断创新，以试点示范破解难题、总结做法，分步推进、逐步完善，为加快建设全国一体化在线政务服务平台、推动实现政务服务“一网通办”积累经验。

坚持安全可控。全面落实总体国家安全观，树立网络安全底线思维，健全管理制度，落实主体责任，强化网络安全规划、安全建设、安全监测和安全态势感知分析，健全安全通报机制，加强综合防范，积极运用安全可靠技术产品，推动安全与应用协调发展，筑牢平台建设和网络安全防线，确保政务网络和数据信息

安全。

(三) 工作目标。

加快建设全国一体化在线政务服务平台，推进各地区各部门政务服务平台规范化、标准化、集约化建设和互联互通，形成全国政务服务“一张网”。政务服务平台不断优化，全过程留痕、全流程监管，政务服务数据资源有效汇聚、充分共享，大数据服务能力显著增强。政务服务线上线下融合互通，跨地区、跨部门、跨层级协同办理，全城通办、就近能办、异地可办，服务效能大幅提升，全面实现全国“一网通办”，为持续推进“放管服”改革、推动政府治理现代化提供强有力支撑。

2018年底前，国家政务服务平台主体功能建设基本完成，通过试点示范实现部分省（自治区、直辖市）和国务院部门政务服务平台与国家政务服务平台对接。制定国家政务服务平台政务服务事项编码、统一身份认证、统一电子印章、统一电子证照等标准规范，各省（自治区、直辖市）和国务院有关部门按照全国一体化在线政务服务平台要求对本地区本部门政务服务平台进行优化完善，为全面构建全国一体化在线政务服务平台奠定基础。

2019年底前，国家政务服务平台上线运行，各省（自治区、直辖市）和国务院有关部门政务服务平台与国家政务服务平台对接，全国一体化在线政务服务平台标准规范体系、安全保障体系和运营管理体系基本建立，国务院部门垂直业务办理系统为地方政务服务需求提供数据共享服务的水平显著提升，全国一体化在线政务服务平台框架初步形成。

2020年底前，国家政务服务平台功能进一步强化，各省（自治区、直辖市）和国务院部门政务服务平台与国家政务服务平台应接尽接、政务服务事项应上尽上，全国一体化在线政务服务平台标准规范体系、安全保障体系和运营管理体系不断完善，国务院部门数据实现共享，满足地方普遍性政务需求，“一网通办”能力显著增强，全国一体化在线政务服务平台基本建成。

2022年底前，以国家政务服务平台为总枢纽的全国一体化在线政务服务平台更加完善，全国范围内政务服务事项基本做到标准统一、整体联动、业务协同，

除法律法规另有规定或涉及国家秘密等外，政务服务事项全部纳入平台办理，全面实现“一网通办”。

二、总体架构和任务要求

全国一体化在线政务服务平台由国家政务服务平台、国务院有关部门政务服务平台（业务办理系统）和各地区政务服务平台组成。国家政务服务平台是全国一体化在线政务服务平台的总枢纽，各地区和国务院有关部门政务服务平台是全国一体化在线政务服务平台的具体办事服务平台。

（一）国家政务服务平台。

国家政务服务平台建设统一政务服务门户、统一政务服务事项管理、统一身份认证、统一电子印章、统一电子证照等公共支撑系统，建设电子监察、服务评估、咨询投诉、用户体验监测等应用系统，建立政务服务平台建设管理的标准规范体系、安全保障体系和运营管理体系，为各地区和国务院有关部门政务服务平台提供公共入口、公共通道和公共支撑。

国家政务服务平台作为全国一体化在线政务服务平台的总枢纽，联通各省（自治区、直辖市）和国务院有关部门政务服务平台，实现政务服务数据汇聚共享和业务协同，支撑各地区各部门政务服务平台为企业和群众提供高效、便捷的政务服务。

国家政务服务平台以中国政府网为总门户，具有独立的服务界面和访问入口，两者用户访问互通，对外提供一体化服务。

（二）国务院有关部门政务服务平台（业务办理系统）和各地区政务服务平台。

国务院有关部门政务服务平台统筹整合本部门业务办理系统，依托国家政务服务平台的公共支撑系统，统筹利用政务服务资源，办理本部门政务服务业务，通过国家政务服务平台与各地区和国务院有关部门政务服务平台互联互通、数据共享、业务协同，依托国家政务服务平台办理跨地区、跨部门、跨层级的政务服务业务。全国投资项目在线审批监管平台、公共资源交易平台、相关信用信息系

统等专项领域国家重点信息系统要与国家政务服务平台做好对接。

各地区政务服务平台按照省级统筹原则建设。通过整合本地区各类办事服务平台，建成本地区各级互联、协同联动的政务服务平台，办理本地区政务服务业务，实现网上政务服务省、市、县、乡镇（街道）、村（社区）全覆盖。各省（自治区、直辖市）政务服务平台与国家政务服务平台互联互通，依托国家政务服务平台办理跨地区、跨部门、跨层级的政务服务业务。

各级政府要依托全国一体化在线政务服务平台整合各类网上政务服务系统，向企业和群众提供统一便捷的服务。国务院有关部门和各省（自治区、直辖市）政务服务平台按照全国一体化在线政务服务平台统一标准规范及相关要求，全面对接国家政务服务平台，其政务服务门户与国家政务服务平台的政务服务门户形式统一规范、内容深度融合，实现事项集中发布、服务集中提供。鼓励各地区各部门依托全国一体化在线政务服务平台，开展个性化、有特色的服务创新。

三、推进政务服务一体化，推动实现政务服务事项国家标准统一、全流程网上办理

（一）规范政务服务事项。

政务服务事项包括行政权力事项和公共服务事项。编制全国统一的标准统一的行政权力事项目录清单，按照统一规划、试点先行、突出重点、逐步完善的实施路径，以依申请办理的行政权力事项为重点，推动实现同一事项名称、编码、依据、类型等基本要素在国家、省、市、县四级统一。全面梳理教育、医疗、住房、社保、民政、扶贫、公共法律服务等与群众日常生活密切相关的公共服务事项，编制公共服务事项清单及办事指南，逐步推进公共服务事项规范化。完善政务服务事项受理条件、申请材料、中介服务、办理流程等信息要素，实现办事要件和办事指南标准化、规范化。建设国家政务服务平台事项库，与各地区和国务院有关部门政务服务事项库联通，推动实现一库汇聚、应上尽上。建立全国联动的政务服务事项动态管理机制，逐步实现各区域、各层级、各渠道发布的政务服务事项数据同源、同步更新，推动实现同一事项无差别受理、办理流程和评价标准统一。

（二）优化政务服务流程。

按照“一网通办”要求进一步优化政务服务流程，依托国家政务服务平台身份认证、电子印章、电子证照等基础支撑，推动证照、办事材料、数据资源共享互认，压缩办理环节、精简办事材料、缩短办理时限，实现更多政务服务事项的申请、受理、审查、决定、证照制作、决定公开、收费、咨询等环节全流程在线办理。整合优化企业开办、投资项目审批、工程建设项目审批、不动产登记等涉及多个部门、地区的事项办理流程，逐步做到一张清单告知、一张表单申报、一个标准受理、一个平台流转。积极推进多证合一、多图联审、多规合一、告知承诺、容缺受理、联审联办。通过流程优化、系统整合、数据共享、业务协同，实现审批更简、监管更强、服务更优，更多政务服务事项实现“一窗受理、一次办成”，为推动尽快实现企业开办时间再减一半、项目审批时间再砍一半、凡是没有法律法规依据的证明一律取消等改革目标提供有力支撑。

（三）融合线上线下服务。

依托全国一体化在线政务服务平台，推进线上线下深度融合，推动政务服务整体联动、全流程在线，做到线上线下一套服务标准、一个办理平台。推动政务服务事项清单、办事指南、办理状态等相关信息在政务服务平台、移动终端、实体大厅、政府网站和第三方互联网入口等服务渠道同源发布。推动政务服务平台和便民服务站向乡镇（街道）、村（社区）延伸。归集、关联与企业 and 群众相关的电子证照、申请材料、事项办理等政务服务信息并形成相应目录清单，持续提高办事材料线上线下共享复用水平。

（四）推广移动政务服务。

以公安、人力资源社会保障、教育、卫生健康、民政、住房城乡建设等领域为重点，积极推进覆盖范围广、应用频率高的政务服务事项向移动端延伸，推动实现更多政务服务事项“掌上办”、“指尖办”。加快建设国家政务服务平台移动端，接入各省（自治区、直辖市）和国务院有关部门移动端服务资源，提供分级运营、协同联动的全国一体化在线政务服务平台移动端服务。制定全国一体化在线政务服务平台移动端建设指引，明确功能定位、设计展现、应用接入、安全防护、运营保障等内容和要求，指导各地区和国务院有关部门集约建设、规范管理。加强对各级政务服务平台移动端的日常监管，强化注册认证、安全检测、安

全加固、应用下载和使用推广等规范管理。充分发挥“两微一端”等政务新媒体优势，同时积极利用第三方平台不断拓展政务服务渠道，提升政务服务便利化水平。

四、推进公共支撑一体化，促进政务服务跨地区、跨部门、跨层级数据共享和业务协同

（一）统一网络支撑。

各级政务服务平台原则上统一依托国家电子政务外网构建，通过部署在互联网上的政务服务门户提供服务。拓展国家电子政务外网覆盖范围，加强网络安全保障，满足业务量大、实时性高的政务服务应用需求。推动各地区和国务院有关部门非涉密业务专网与电子政务外网对接整合。

（二）统一身份认证。

国家政务服务平台基于自然人身份信息、法人单位信息等国家认证资源，建设全国统一身份认证系统，积极稳妥与第三方机构开展网上认证合作，为各地区和国务院有关部门政务服务平台及移动端提供统一身份认证服务。各地区和国务院有关部门统一利用国家政务服务平台认证能力，按照标准建设完善可信凭证和单点登录系统，解决企业和群众办事在不同地区和部门平台重复注册验证等问题，实现“一次认证、全网通办”。各地区各部门已建身份认证系统按照相关规范对接国家政务服务平台统一身份认证系统。

（三）统一电子印章。

制定政务服务领域电子印章管理办法，规范电子印章全流程管理，明确加盖电子印章的电子材料合法有效。应用基于商用密码的数字签名等技术，依托国家政务服务平台建设权威、规范、可信的国家统一电子印章系统。各地区和国务院有关部门使用国家统一电子印章制章系统制发电子印章。未建立电子印章用章系统的按照国家电子印章技术规范建立，已建电子印章用章系统的按照相关规范对接。

（四）统一电子证照。

依托国家政务服务平台电子证照共享服务系统，实现电子证照跨地区、跨部门共享。各地区和国务院有关部门按照国家电子证照业务技术规范制作和管理电子证照，上报电子证照目录数据。电子证照采用标准版式文档格式，通过电子印章用章系统加盖电子印章或加签数字签名，实现全国互信互认，切实解决企业和群众办事提交材料、证明多等问题。

（五）统一数据共享。

国家政务服务平台充分利用国家人口、法人、信用、地理信息等基础资源库，对接国务院部门垂直业务办理系统，满足政务服务数据共享需求。发挥国家数据共享交换平台作为国家政务服务平台基础设施和数据交换通道的作用，对于各省（自治区、直辖市）和国务院有关部门提出的政务服务数据共享需求，由国家政务服务平台统一受理和提供服务，并通过国家数据共享交换平台交换数据。进一步加强政务信息系统整合共享，简化共享数据申请使用流程，满足各地区和国务院有关部门政务服务数据需求。落实数据提供方责任，国务院有关部门按照“谁主管，谁提供，谁负责”的原则，保障数据供给，提高数据质量。除特殊情况外，国务院部门政务信息系统不按要求与一体化平台共享数据的，中央财政不予经费保障。强化数据使用方责任，加强共享数据使用全过程管理，确保数据安全。整合市场监管相关数据资源，推动事中事后监管信息与政务服务深度融合、“一网通享”。建设国家政务服务平台数据资源中心，汇聚各地区和国务院有关部门政务服务数据，积极运用大数据、人工智能等新技术，开展全国政务服务态势分析，为提升政务服务质量提供大数据支撑。

五、推进综合保障一体化，确保平台运行安全平稳规范

（一）健全标准规范。

按照“急用先行、分类推进，成熟一批、发布一批”的原则，抓紧制定并不断完善全国一体化在线政务服务平台总体框架、数据、应用、运营、安全、管理等标准规范，指导各地区和国务院有关部门政务服务平台规范建设，推进政务服务事项、数据、流程等标准化，实现政务服务平台标准统一、互联互通、数据共享、业务协同。加强政务服务平台标准规范宣传培训、应用推广和贯彻实施，总

结推广平台建设经验做法和应用案例，定期对标准规范进行应用评估和修订完善，以标准化促进平台建设一体化、政务服务规范化。

（二）加强安全保障。

强化各级政务服务平台安全保障系统的风险防控能力，构建全方位、多层次、一致性的防护体系，切实保障全国一体化在线政务服务平台平稳高效安全运行。落实《中华人民共和国网络安全法》和信息安全等级保护制度等信息网络安全相关法律法规和政策性文件，加强国家关键基础设施安全防护，明确各级政务服务平台网络安全管理机构，落实安全管理主体责任，建立健全安全管理和保密审查制度，加强安全规划、安全建设、安全测评、容灾备份等保障。强化日常监管，加强安全态势感知分析，准确把握安全风险趋势，定期开展风险评估和压力测试，及时通报、整改问题，化解安全风险。加强政务大数据安全管理，制定平台数据安全管理办法，加强对涉及国家利益、公共安全、商业秘密、个人隐私等重要信息的保护和管理。应用符合国家要求的密码技术产品加强身份认证和数据保护，优先采用安全可靠软硬件产品、系统和服务，以应用促进技术创新，带动产业发展，确保安全可控。加强网络安全保障队伍建设，建立多部门协调联动工作机制，制定完善应急预案，强化日常预防、监测、预警和应急处置能力。

（三）完善运营管理。

按照统一运营管理要求，各级政务服务平台分别建立运营管理系统，形成分级管理、责任明确、保障有力的全国一体化在线政务服务平台运营管理体系。加强国家政务服务平台运营管理力量，建立健全相关规章制度，优化运营工作流程，提升国家政务服务平台作为总枢纽的服务支撑能力。各地区和国务院有关部门要整合运营资源，加强平台运营管理队伍建设，统一负责政务服务平台和实体大厅运行管理的组织协调、督促检查、评估考核等工作，推进“一套制度管理、一支队伍保障”。创新平台运营服务模式，充分发挥社会机构运营优势，建立健全运营服务社会化机制，形成配备合理、稳定可持续的运营服务力量。

（四）强化咨询投诉。

按照“统一规划、分级建设、分级办理”原则，形成上下覆盖、部门联动、

标准统一的政务服务咨询投诉体系，畅通网上咨询投诉渠道，及时回应和推动解决政务服务中的热点难点问题。国家政务服务平台咨询投诉系统提供在线受理、转办、督办、反馈等全流程咨询投诉服务，与各地区和国务院有关部门协同处理，通过受理咨询投诉不断完善平台功能、提升平台服务水平。各地区和国务院有关部门建设完善政务服务平台专业咨询投诉系统，与各类政务热线做好对接，对事项上线、政务办件、证照共享、结果送达等事项服务，开展全程监督、评价、投诉并及时反馈，实现群众诉求件件有落实、事事有回应。国家政务服务平台咨询投诉系统做好与中国政府网咨询投诉功能的衔接。

（五）加强评估评价。

依托国家政务服务平台网上评估系统，建立政务服务评估指标体系，加强对各地区和国务院有关部门政务服务平台的在线评估。同时，将各级政务服务平台网络安全工作情况纳入评估指标体系，督促做好网络安全防护工作。建立完善各级政务服务平台网上评估评价系统，实时监测事项、办件、业务、用户等信息数据，接受申请办事的企业和群众对政务服务事项办理情况的评价，实现评估评价数据可视化展示与多维度对比分析，以评估评价强化常态化监督，实现全流程动态精准监督，促进各地区和国务院有关部门政务服务水平不断提升。

六、组织实施

（一）加强组织领导。

国务院办公厅牵头成立全国一体化在线政务服务平台建设和管理协调工作小组，负责全国一体化在线政务服务平台顶层设计、规划建设、组织推进、统筹协调和监督指导等工作。各地区和国务院有关部门要建立健全推进本地区本部门政务服务平台建设和管理协调机制，负责统筹建设和完善本地区本部门政务服务平台，同时做好对接国家政务服务平台等工作。要充分发挥各省（自治区、直辖市）政府和国务院有关部门办公厅的优势，统筹协调各方面力量，抓好各项工作任务落实。

（二）强化分工协作。

国务院办公厅负责牵头推进国家政务服务平台建设，会同各地区和国务院有

关部门推动建设全国一体化在线政务服务平台标准规范体系、安全保障体系和运营管理体系。全国一体化在线政务服务平台建设和管理工作要与转变政府职能、深化“放管服”改革紧密结合。各地区和国务院有关部门分级负责本地区本部门政务服务平台建设、安全保障和运营管理，做好与国家政务服务平台对接。国务院有关部门依托全国一体化在线政务服务平台，对属于本部门职责范围内的政务服务业务由该部门负责办理，跨部门的政务服务业务由牵头部门负责，相关部门积极配合、协同办理，国务院办公厅负责总体协调。政务服务平台建设和运行所需经费纳入各地区各部门财政预算，做好经费统筹管理使用。通过政府购买服务，鼓励社会力量参与政务服务平台建设。

（三）完善法规制度。

抓紧制修订全国一体化在线政务服务平台建设运营急需的电子印章、电子证照、电子档案等方面的法规、规章。同步推进现有法规、规章和规范性文件立改废释工作。加快完善配套政策，制定政务服务平台建设运营、数据共享、事项管理、业务协同、网络安全保障等方面管理制度，为平台建设管理提供法规制度支撑。

（四）加强培训交流。

建立常态化培训机制，围绕业务应用、技术体系、运营管理、安全保障、标准规范等定期组织开展培训，加强专业队伍建设。建立日常沟通交流机制，以简报、培训、研讨等多种形式开展交流，总结成熟经验，加强推广应用。加强对各地区和国务院有关部门政务服务平台建设管理经验的宣传推广。针对全国一体化在线政务服务平台建设管理中的重点难点问题开展专项试点、区域试点，总结成熟经验，做好试点成果转化推广。

（五）加强督查考核。

建立全国一体化在线政务服务平台建设管理督查考核机制，明确督查考核范围、周期和内容，实现督查考核工作制度化、规范化、标准化、常态化。各地区和国务院有关部门要把政务服务平台建设管理纳入工作绩效考核范围，列入重点督查事项。围绕全国一体化在线政务服务平台建设管理等组织开展第三方评估。

充分发挥督查考核的导向作用，形成推进工作的良性机制。

各地区各部门要把加快全国一体化在线政务服务平台建设作为深化“放管服”改革、推进政府治理现代化的重要举措，制定具体实施方案，明确时间表、路线图，加大政策支持力度，强化工作责任，确保各项任务措施落实到位。有关实施方案和工作进展要及时报送国务院办公厅。

附件：全国一体化在线政务服务平台建设组织推进和任务分工方案

国务院

2018年7月25日

为做好全国一体化在线政务服务平台建设组织实施工作，制定本方案。

一、工作目标

通过建立强有力的工作推进和协调机制，精心组织，周密安排，上下协同，集中攻关，加快建设全国一体化在线政务服务平台，形成全国政务服务“一张网”，确保到2018年底前，国家政务服务平台主体功能建设基本完成，通过试点示范实现部分省（自治区、直辖市）和国务院部门政务服务平台与国家政务服务平台对接；到2019年底前，国家政务服务平台上线运行，全国一体化在线政务服务平台框架初步形成；到2020年底前，各省（自治区、直辖市）和国务院部门政务服务平台与国家政务服务平台应接尽接、政务服务事项应上尽上，国务院部门数据实现共享，满足地方普遍性政务需求，全国一体化在线政务服务平台基本建成；到2022年底前，全国范围内政务服务事项基本做到标准统一、整体联动、业务协同，除法律法规另有规定或涉及国家秘密等外，政务服务事项全部纳入平台办理，全面实现“一网通办”。

二、组织推进

紧密结合深入推进“放管服”改革各项要求，统筹规划、标准先行，试点带动、迭代创新，统分结合、上下联动，以国家政务服务平台建设为重点，充分利用各地区和国务院有关部门已建政务服务平台，整合各类政务服务资源，推进数据共享和流程优化再造，坚持安全与应用同步规划、同步建设、同步运行，扎实

做好平台建设组织实施工作，确保如期完成各项任务。

（一）成立平台建设和管理协调工作小组。国务院办公厅牵头成立全国一体化在线政务服务平台建设和管理协调工作小组，负责全国一体化在线政务服务平台顶层设计、规划建设、组织推进、统筹协调和监督指导等工作。平台建设和管理协调工作小组办公室设在国务院办公厅电子政务办公室，承担协调工作小组日常工作，组织督促各地区和国务院有关部门任务落实。各地区和国务院有关部门要建立健全相应的建设和管理协调机制，负责统筹建设和完善本地区本部门政务服务平台，同时做好对接国家政务服务平台等工作。

（二）建立协同推进工作机制。国务院办公厅与各地区各部门形成紧密协作机制，牵头推进国家政务服务平台建设，会同各地区和国务院有关部门推动建设全国一体化在线政务服务平台标准规范体系、安全保障体系和运营管理体系，推动跨地区、跨部门、跨层级数据共享和政务服务流程不断优化；牵头对全国一体化在线政务服务平台建设和管理工作进行督查评估。全国一体化在线政务服务平台建设和管理工作要与转变政府职能、深化“放管服”改革紧密结合。各地区和国务院有关部门分级负责本地区本部门政务服务平台建设、安全保障和运营管理，做好与国家政务服务平台对接。

（三）加强日常运营管理。按照统一运营管理要求，建立形成分级管理、责任明确、保障有力的全国一体化在线政务服务平台运营管理体系。国务院办公厅要加强对全国一体化在线政务服务平台运营管理的统筹协调，充实国家政务服务平台运营管理力量，建立健全相关规章制度，优化运营工作流程，提升国家政务服务平台作为总枢纽的服务支撑能力。各地区和国务院有关部门要整合运营资源，加强平台运营管理队伍建设，统一负责政务服务平台和实体大厅运行管理的组织协调、督促检查、评估考核等工作，推进“一套制度管理、一支队伍保障”。

三、重点任务分工及进度安排

（一）做好试点推进工作。

1.选择部分条件成熟的省（自治区、直辖市）和国务院部门开展与国家政务服务平台对接试点，积累经验，逐步推广。第一批试点省份为上海市、江苏省、

浙江省、安徽省、山东省、广东省、重庆市、四川省、贵州省；试点国务院部门为国家发展改革委、教育部、公安部、人力资源社会保障部、商务部、市场监管总局。其他地方和国务院有关部门，根据本地区本部门政务服务平台建设成熟程度分批接入，2019年底前完成接入任务。（国务院办公厅牵头，各地区和国务院有关部门负责，2019年底前完成；试点地区、部门2018年底前完成）

（二）规范政务服务事项。

2.编制全国统一行政权力事项目录清单，以依申请办理的行政权力事项为重点，推动实现同一事项名称、编码、依据、类型等基本要素在国家、省、市、县四级统一。（国务院办公厅牵头协调各有关方面推进，各地区和国务院有关部门分工负责，2020年底前印发全国统一行政权力事项目录清单，2022年底前全国范围内政务服务事项基本做到标准统一、整体联动、业务协同）

3.编制公共服务事项清单及办事指南，全面梳理教育、医疗、住房、社保、民政、扶贫、公共法律服务等与群众日常生活密切相关的公共服务事项，逐步推进公共服务事项规范化。（各地区和国务院有关部门负责，2020年底前完成；试点地区、部门2019年底前完成）

4.推进办事要件和办事指南标准化、规范化，在编制行政权力事项目录清单和公共服务事项清单基础上，完善政务服务事项受理条件、申请材料、中介服务、办理流程等信息要素。（各地区和国务院有关部门负责，2020年底前完成；试点地区、部门2019年底前完成）

5.建设国家政务服务平台事项库，与各地区和国务院有关部门政务服务事项库联通，推动实现一库汇聚、应上尽上。建立全国联动的政务服务事项动态管理机制，逐步实现各区域、各层级、各渠道发布的政务服务事项数据同源、同步更新。（国务院办公厅牵头，各地区和国务院有关部门负责，2020年底前实现各省（自治区、直辖市）和国务院部门政务服务平台与国家政务服务平台应接尽接、政务服务事项应上尽上；试点地区、部门2018年底前完成与国家政务服务平台事项库对接）

（三）优化政务服务流程。

6.依托国家政务服务平台身份认证、电子印章、电子证照等基础支撑，推动证照、办事材料、数据资源共享互认。（各地区和国务院有关部门负责，2020年底前完成）

7.整合优化涉及跨地区、跨部门、跨层级的事项办理流程，实现一张清单告知、一张表单申报、一个标准受理、一个平台流转。（各地区和国务院有关部门负责，2020年底前完成）

（四）融合线上线下服务。

8.推动政务服务事项清单、办事指南、办理状态等相关信息在政务服务平台、移动终端、实体大厅、政府网站和第三方互联网入口等服务渠道同源发布。（各地区和国务院有关部门负责，2020年底前完成；试点地区、部门2019年底前完成）

9.依托全国一体化在线政务服务平台，推进线上线下深度融合，逐步实现线上线下一套服务标准、一个办理平台。推动政务服务平台和便民服务站向乡镇（街道）、村（社区）延伸。（各地区和国务院有关部门负责，2022年底前完成；试点地区、部门2020年底前完成）

（五）推广移动政务服务。

10.以公安、人力资源社会保障、教育、卫生健康、民政、住房城乡建设等领域为重点，积极推进覆盖范围广、应用频率高的政务服务事项向移动端延伸，推动实现更多政务服务事项“掌上办”、“指尖办”。（各地区和国务院有关部门负责，2020年底前完成）

11.加快建设国家政务服务平台移动端，接入各省（自治区、直辖市）和国务院有关部门移动端服务资源，提供分级运营、协同联动的全国一体化在线政务服务平台移动端服务。（国务院办公厅牵头，各地区和国务院有关部门负责，2019年底前完成）

12.制定全国一体化在线政务服务平台移动端建设指引，明确功能定位、设计展现、应用接入、安全防护、运营保障等内容和要求，指导各地区和国务院有关部门集约建设、规范管理。（国务院办公厅牵头，2019年底前完成）

(六) 统一网络支撑。

13.各级政务服务平台原则上统一依托国家电子政务外网构建，通过部署在互联网上的政务服务门户提供服务。（各地区和国务院有关部门负责，2019年底前完成）

14.拓展国家电子政务外网覆盖范围，推动各地区和国务院有关部门非涉密业务专网与电子政务外网对接整合。（国务院办公厅、国家发展改革委牵头，各地区和国务院有关部门负责，2020年底前完成）

(七) 统一身份认证。

15.国家政务服务平台基于自然人身份信息、法人单位信息等国家认证资源，建设全国统一身份认证系统。（国务院办公厅、公安部、市场监管总局等部门负责，2019年底前完成）

16.各地区和国务院有关部门统一利用国家政务服务平台认证能力，按照标准建设完善可信凭证和单点登录系统，解决企业和群众办事在不同地区和部门平台重复注册验证等问题，实现“一次认证、全网通办”。各地区各部门已建身份认证系统按照相关规范对接国家政务服务平台统一身份认证系统。（各地区和国务院有关部门负责，2020年底前完成；试点地区、部门2019年底前完成）

(八) 统一电子印章。

17.应用基于商用密码的数字签名等技术，借鉴二代身份证等制发和管理经验，依托国家政务服务平台建设权威、规范、可信的国家统一电子印章系统。（国务院办公厅负责，2019年底前完成）

18.制定政务服务领域电子印章管理办法，规范电子印章全流程管理。（国务院办公厅、公安部牵头，2019年底前完成）

19.各地区和国务院有关部门使用国家统一电子印章制章系统制发电子印章。未建立电子印章用章系统的按照国家电子印章技术规范建立，已建电子印章用章系统的按照相关规范对接。（各地区和国务院有关部门负责，2020年底前完成；试点地区、部门2019年底前完成）

(九) 统一电子证照。

20.借鉴二代身份证等制发和管理经验，建成国家政务服务平台电子证照共享服务系统，支撑电子证照跨地区、跨部门共享。（国务院办公厅牵头，各地区和国务院有关部门负责，2019年底前完成）

21.各地区和国务院有关部门按照国家电子证照业务技术规范制作和管理电子证照，通过电子印章用章系统加盖电子印章或加签数字签名，实现全国互信互认。（各地区和国务院有关部门负责，2020年底前完成；试点地区、部门2019年底前完成）

(十) 统一数据共享。

22.国家人口、法人、信用、地理信息等基础资源库和全国投资项目在线审批监管平台、公共资源交易平台等专项领域国家重点信息系统与国家政务服务平台实现对接。（国务院办公厅牵头，国家发展改革委、公安部、自然资源部、市场监管总局等国务院有关部门按职责分工负责，2018年底前完成）

23.实现国务院部门垂直业务办理系统依托国家政务服务平台向各级政务服务平台共享数据。（国务院有关部门负责，2020年底前完成）

24.国家政务服务平台统一受理各省（自治区、直辖市）和国务院有关部门提出的政务服务数据共享需求，提供服务。发挥国家数据共享交换平台作为国家政务服务平台的基础设施和数据交换通道作用，满足全国一体化在线政务服务平台数据共享需求。（国务院办公厅、国家发展改革委牵头，各地区和国务院有关部门负责，2020年底前完成）

25.建设国家政务服务平台数据资源中心，汇聚各地区和国务院有关部门政务服务数据，开展全国政务服务态势分析，提供政务大数据服务。（国务院办公厅牵头，各地区和国务院有关部门负责，2019年底前完成）

(十一) 健全标准规范。

26.制定完善全国一体化在线政务服务平台总体框架、数据、应用、运营、安全、管理等标准规范。加强政务服务平台标准规范宣传培训、应用推广和贯彻实

施，总结推广平台建设经验做法和应用案例。（国务院办公厅、工业和信息化部、国家标准委牵头，2018年9月底前印发国家政务服务平台统一政务服务门户、政务服务事项编码、统一身份认证、统一电子印章、统一电子证照、统一数据共享等第一批工程建设标准规范，2018年底前印发国家政务服务平台安全保障、运营管理、数据分析等第二批工程建设标准规范；国家标准委牵头会同有关方面制定全国一体化在线政务服务平台建设管理急需的基础性国家标准，2019年底前基本建立全国一体化在线政务服务平台标准规范体系）

（十二）加强安全保障。

27.建立全国一体化在线政务服务平台安全保障协调联动工作机制，制定完善应急预案，构建全方位、多层次、一致性的防护体系。（国务院办公厅牵头，各地区和国务院有关部门负责，2019年底前基本完成）

28.制定全国一体化在线政务服务平台数据安全管理办法，加强对涉及国家利益、公共安全、商业秘密、个人隐私等重要信息的保护和管理，加强政务大数据安全管理。（国务院办公厅、国家网信办、公安部负责，2019年底前完成）

（十三）强化咨询投诉。

29.各地区和国务院有关部门建设完善政务服务平台专业咨询投诉系统，与各类政务热线做好对接，开展全程监督、评价、投诉并及时反馈。（各地区和国务院有关部门负责，2019年底前完成）

30.建设国家政务服务平台咨询投诉系统，与各地区和国务院有关部门协同处理，形成上下覆盖、部门联动、标准统一的政务服务咨询投诉体系。（国务院办公厅牵头，各地区和国务院有关部门负责，2020年底前完成）

（十四）加强评估评价。

31.建设国家政务服务平台网上评估系统，建立政务服务评估指标体系，对各地区和国务院有关部门政务服务平台进行在线评估。建立完善各级政务服务平台网上评估评价系统，以评估评价强化常态化监督。（国务院办公厅牵头，各地区和国务院有关部门负责，2019年底前完成）

(十五) 完善法规制度。

32.制修订全国一体化在线政务服务平台建设运营急需的电子印章、电子证照、电子档案等方面的法规、规章。（司法部会同国家发展改革委、公安部、国家档案局等相关部门负责，2020年底前完成）

(十六) 加强培训交流。

33.围绕业务应用、技术体系、运营管理、安全保障、标准规范等定期组织开展培训。加强对各地区和国务院有关部门政务服务平台建设管理经验的宣传推广。持续深入开展全国一体化在线政务服务平台建设管理专项试点、区域试点，做好试点成果转化推广。（国务院办公厅牵头，各地区和国务院有关部门负责，2019年底前完成并持续推进）

(三) 国务院办公厅关于促进和规范健康医疗大数据应用发展的指导意见

(国办发〔2016〕47号)

各省、自治区、直辖市人民政府，国务院各部委、各直属机构：

健康医疗大数据是国家重要的基础性战略资源。健康医疗大数据应用发展将带来健康医疗模式的深刻变化，有利于激发深化医药卫生体制改革的动力和活力，提升健康医疗服务效率和质量，扩大资源供给，不断满足人民群众多层次、多样化的健康需求，有利于培育新的业态和经济增长点。为贯彻落实《国务院关于印发促进大数据发展行动纲要的通知》（国发〔2015〕50号）要求，顺应新兴信息技术发展趋势，规范和推动健康医疗大数据融合共享、开放应用，经国务院同意，现提出如下意见。

一、指导思想、基本原则和发展目标

（一）指导思想。深入贯彻落实党的十八大和十八届三中、四中、五中全会精神，牢固树立并切实贯彻创新、协调、绿色、开放、共享的发展理念，按照党中央、国务院决策部署，发挥市场在资源配置中的决定性作用，更好发挥政府作用，以保障全体人民健康为出发点，强化顶层设计，夯实基层基础，完善政策制度，创新工作机制，大力推动政府健康医疗信息系统和公众健康医疗数据互联融合、开放共享，消除信息孤岛，积极营造促进健康医疗大数据安全规范、创新应用的发展环境，通过“互联网+健康医疗”探索服务新模式、培育发展新业态，努力建设人民满意的医疗卫生事业，为打造健康中国、全面建成小康社会和实现中华民族伟大复兴的中国梦提供有力支撑。

（二）基本原则。

坚持以人为本、创新驱动。将健康医疗大数据应用发展纳入国家大数据战略布局，推进政产学研用联合协同创新，强化基础研究和核心技术攻关，突出健康医疗重点领域和关键环节，利用大数据拓展服务渠道，延伸和丰富服务内容，更好满足人民健康医疗需求。

坚持规范有序、安全可控。建立健全健康医疗大数据开放、保护等法规制度，强化标准和安全体系建设，强化安全管理责任，妥善处理应用发展与保障安全的关系，增强安全技术支撑能力，有效保护个人隐私和信息安全。

坚持开放融合、共建共享。鼓励政府和社会力量合作，坚持统筹规划、远近结合、示范引领，注重盘活、整合现有资源，推动形成各方支持、依法开放、便民利民、蓬勃发展的良好局面，充分释放数据红利，激发大众创业、万众创新活力。

(三) 发展目标。到2017年底，实现国家和省级人口健康信息平台以及全国药品招标采购业务应用平台互联互通，基本形成跨部门健康医疗数据资源共享共用格局。到2020年，建成国家医疗卫生信息分级开放应用平台，实现与人口、法人、空间地理等基础数据资源跨部门、跨区域共享，医疗、医药、医保和健康各相关领域数据融合应用取得明显成效；统筹区域布局，依托现有资源建成100个区域临床医学数据示范中心，基本实现城乡居民拥有规范化的电子健康档案和功能完备的健康卡，健康医疗大数据相关政策法规、安全防护、应用标准体系不断完善，适应国情的健康医疗大数据应用发展模式基本建立，健康医疗大数据产业体系初步形成、新业态蓬勃发展，人民群众得到更多实惠。

二、重点任务和重大工程

(一) 夯实健康医疗大数据应用基础。

1. 加快建设统一权威、互联互通的人口健康信息平台。实施全民健康保障信息化工程，按照安全为先、保护隐私的原则，充分依托国家电子政务外网和统一数据共享交换平台，拓展完善现有设施资源，全面建成互通共享的国家、省、市、县四级人口健康信息平台，强化公共卫生、计划生育、医疗服务、医疗保障、药品供应、综合管理等应用信息系统数据采集、集成共享和业务协同。创新管理模式，推动生育登记网上办理。消除数据壁垒，畅通部门、区域、行业之间的数据共享通道，探索社会化健康医疗数据信息互通机制，推动实现健康医疗数据在平台集聚、业务事项在平台办理、政府决策依托平台支撑。

2. 推动健康医疗大数据资源共享开放。鼓励各类医疗卫生机构推进健康医疗

大数据采集、存储，加强应用支撑和运维技术保障，打通数据资源共享通道。加快建设和完善以居民电子健康档案、电子病历、电子处方等为核心的基础数据库。建立卫生计生、中医药与教育、科技、工业和信息化、公安、民政、人力资源社会保障、环保、农业、商务、安全监管、检验检疫、食品药品监管、体育、统计、旅游、气象、保险监管、残联等跨部门密切配合、统一归口的健康医疗数据共享机制。探索推进可穿戴设备、智能健康电子产品、健康医疗移动应用等产生的数据资源规范接入人口健康信息平台。建立全国健康医疗数据资源目录体系，制定分类、分级、分域健康医疗大数据开放应用政策规范，稳步推动健康医疗大数据开放。

（二）全面深化健康医疗大数据应用。

3.推进健康医疗行业治理大数据应用。加强深化医药卫生体制改革评估监测，加强居民健康状况等重要数据精准统计和预测评价，有力支撑健康中国建设规划和决策。综合运用健康医疗大数据资源和信息技术手段，健全医院评价体系，推动深化公立医院改革，完善现代医院管理制度，优化医疗卫生资源布局。加强医疗机构监管，健全对医疗、药品、耗材等收入构成及变化趋势的监测机制，协同医疗服务价格、医保支付、药品招标采购、药品使用等业务信息，助推医疗、医保、医药联动改革。

4.推进健康医疗临床和科研大数据应用。依托现有资源建设一批心脑血管、肿瘤、老年病和儿科等临床医学数据示范中心，集成基因组学、蛋白质组学等国家医学大数据资源，构建临床决策支持系统。推进基因芯片与测序技术在遗传性疾病诊断、癌症早期诊断和疾病预防检测方面的应用，加强人口基因信息安全管理，推动精准医疗技术发展。围绕重大疾病临床用药研制、药物产业化共性关键技术等需求，建立药物副作用预测、创新药物研发数据融合共享机制。充分利用优势资源，优化生物医学大数据布局，依托国家临床医学研究中心和协同研究网络，系统加强临床和科研数据资源整合共享，提升医学科研及应用效能，推动智慧医疗发展。

5.推进公共卫生大数据应用。加强公共卫生业务信息系统建设，完善国家免疫规划、网络直报、网络化急救、职业病防控、口岸公共卫生风险预警决策等信

息系统以及移动应急业务平台应用功能，推进医疗机构、公共卫生机构和口岸检验检疫机构的信息共享和业务协同，全面提升公共卫生监测评估和决策管理能力。整合社会网络公共信息资源，完善疾病敏感信息预警机制，及时掌握和动态分析全人群疾病发生趋势及全球传染病疫情信息等国际公共卫生风险，提高突发公共卫生事件预警与应急响应能力。整合环境卫生、饮用水、健康危害因素、口岸医学媒介生物和核生化等多方监测数据，有效评价影响健康的社会因素。开展重点传染病、职业病、口岸输入性传染病和医学媒介生物监测，整合传染病、职业病多源监测数据，建立实验室病原检测结果快速识别网络体系，有效预防控制重大疾病。推动疾病危险因素监测评估和妇幼保健、老年保健、国际旅行卫生健康保健等智能应用，普及健康生活方式。

6.培育健康医疗大数据应用新业态。加强健康医疗海量数据存储清洗、分析挖掘、安全隐私保护等关键技术攻关。积极鼓励社会力量创新发展健康医疗业务，促进健康医疗业务与大数据技术深度融合，加快构建健康医疗大数据产业链，不断推进健康医疗与养生、养老、家政等服务业协同发展。发展居家健康信息服务，规范网上药店和医药物流第三方配送等服务，推动中医药养生、健康养老、健康管理、健康咨询、健康文化、体育健身、健康医疗旅游、健康环境、健康饮食等产业发展。

7.研制推广数字化健康医疗智能设备。支持研发健康医疗相关的人工智能技术、生物三维（3D）打印技术、医用机器人、大型医疗设备、健康和康复辅助器械、可穿戴设备以及相关微型传感器件。加快研发成果转化，提高数字医疗设备、物联网设备、智能健康产品、中医功能状态检测与养生保健仪器设备的生产制造水平，促进健康医疗智能装备产业升级。

（三）规范和推动“互联网+健康医疗”服务。

8.发展智慧健康医疗便民惠民服务。发挥优质医疗资源的引领作用，鼓励社会力量参与，整合线上线下资源，规范医疗物联网和健康医疗应用程序（APP）管理，大力推进互联网健康咨询、网上预约分诊、移动支付和检查检验结果查询、随访跟踪等应用，优化形成规范、共享、互信的诊疗流程。探索互联网健康医疗服务模式。以家庭医生签约服务为基础，推进居民健康卡、社会保障卡等应用集

成，激活居民电子健康档案应用，推动覆盖全生命周期的预防、治疗、康复和健康管理的一体化电子健康服务。

9.全面建立远程医疗应用体系。实施健康中国云服务计划，建设健康医疗服务集成平台，提供远程会诊、远程影像、远程病理、远程心电诊断服务，健全检查检验结果互认共享机制。推进大医院与基层医疗卫生机构、全科医生与专科医生的数据资源共享和业务协同，健全基于互联网、大数据技术的分级诊疗信息系统，延伸放大医疗卫生机构服务能力，有针对性地促进“重心下移、资源下沉”。

10.推动健康医疗教育培训应用。支持建立以国家健康医疗开放大学为基础、中国健康医疗教育慕课联盟为支撑的健康医疗教育培训云平台，鼓励开发慕课健康医疗培训教材，探索新型互联网教学模式和方法，组织优质师资推进网络医学教育资源开放共享和在线互动、远程培训、远程手术示教、学习成效评估等应用，便捷医务人员终身教育，提升基层医疗卫生服务能力。

（四）加强健康医疗大数据保障体系建设。

11.加强法规和标准体系建设。制定完善健康医疗大数据应用发展的法律法规，强化居民健康信息服务规范管理，明确信息使用权限，切实保护相关各方合法权益。完善数据开放共享支撑服务体系，建立“分级授权、分类应用、权责一致”的管理制度。规范健康医疗大数据应用领域的准入标准，建立大数据应用诚信机制和退出机制，严格规范大数据开发、挖掘、应用行为。建立统一的疾病诊断编码、临床医学术语、检查检验规范、药品应用编码、信息数据接口和传输协议等相关标准，促进健康医疗大数据产品、服务流程标准化。

12.推进网络可信体系建设。强化健康医疗数字身份管理，建设全国统一标识的医疗卫生人员和医疗卫生机构可信医学数字身份、电子实名认证、数据访问控制信息系统，积极推进电子签名应用，逐步建立服务管理留痕可溯、诊疗数据安全运行、多方协作参与的健康医疗管理新模式。

13.加强健康医疗数据安全保障。加快健康医疗数据安全体系建设，建立数据安全管理制度，制定标识赋码、科学分类、风险分级、安全审查规则。制定人口健康信息安全规划，强化国家、区域人口健康信息工程技术能力，注重内容

安全和技术安全，确保国家关键信息基础设施和核心系统自主可控稳定安全。开展大数据平台及服务商的可靠性、可控性和安全性评测以及应用的安全性评测和风险评估，建立安全防护、系统互联共享、公民隐私保护等软件评价和安全审查制度。加强大数据安全监测和预警，建立安全信息通报和应急处置联动机制，建立健全“互联网+健康医疗”服务安全工作机制，完善风险隐患化解和应对工作措施，加强对涉及国家利益、公共安全、患者隐私、商业秘密等重要信息的保护，加强医学院、科研机构等方面的安全防范。

14.加强健康医疗信息化复合型人才队伍建设。实施国家健康医疗信息化人才发展计划，强化医学信息学学科建设和“数字化医生”培育，着力培育高层次、复合型的研发人才和科研团队，培养一批有国际影响力的专门人才、学科带头人和行业领军人物。创新专业人才继续教育形式，完善多层次、多类型人才培养培训体系，推动政府、高等院校、科研院所、医疗机构、企业共同培养人才，促进健康医疗大数据人才队伍建设。

三、加强组织实施

（一）强化统筹规划。建立党委政府领导、多方参与、资源共享、协同推进的工作格局。国家卫生计生委要综合统筹、强化实施，各有关部门要密切配合、形成合力，推动重点任务落实。各地区要重视健康医疗大数据应用发展，切实搞好总体规划、基础建设、安全监管，确保各项任务措施落到实处。推进健康医疗大数据军民融合发展，促进军地健康医疗数据规范衔接、互通共享、协同应用。加强对健康医疗大数据应用发展的指导，强化对技术研发、新业态构建、应用推广的统筹协调，研究建立专家委员会，组织研究制定发展战略及相关政策、法规、标准。

（二）抓住重点着力突破。从人民群众迫切需求的领域入手，重点推进网上预约分诊、远程医疗和检查检验结果共享互认等便民惠民应用。加快推进基本医保全国联网和异地就医结算。支持发展医疗智能设备、智能可穿戴设备，加强疑难疾病等重点方面的研究。选择一批基础条件好、工作积极性高、隐私安全防范有保障的地区和领域开展健康医疗大数据应用试点，总结经验，扎实有序推进。

(三) 加大政策扶持力度。研究制定政府支持政策，从财税、投资、创新等方面对健康医疗大数据应用发展给予必要支持。推广运用政府和社会资本合作

(PPP) 模式，鼓励和引导社会资本参与健康医疗大数据的基础工程、应用开发和运营服务。鼓励政府与企事业单位、社会机构开展合作，探索通过政府采购、社会众包等方式，实现健康医疗大数据领域政府应用与社会应用相融合。充分发挥已设立的有关投资基金作用，充分激发社会资本和民间资本参与热情，鼓励创新多元投资机制，健全风险防范和监管制度，支持健康医疗大数据应用发展。

(四) 加强政策宣传普及。加强健康医疗大数据应用发展政策解读，大力宣传应用发展的重要意义和应用前景，积极回应社会关切，形成良好社会氛围。积极引导医疗卫生机构和社会力量参与开展形式多样的科普活动，宣传普及健康医疗大数据应用知识，鼓励开发简便易行的数字医学工具，不断提升人民群众掌握相关应用的能力和社会公众健康素养。

(五) 推进国际交流合作。有序推进健康医疗大数据应用发展的人才技术交流与合作。鼓励相关企业和科研单位开展对国际先进技术的引进、消化吸收和再创新，推动我国自主技术与全球同步发展。加大对国际健康医疗大数据应用标准的跟踪、评估和转化力度，积极参与国际标准制定，增强相关规则制定的话语权。坚持以我为主、加强监管、确保安全原则，稳步探索国际健康医疗大数据应用发展合作新模式，不断提升我国健康医疗大数据应用水平、产业核心竞争力和国际化水平。

国务院办公厅

2016年6月21日

(四) 国务院关于印发促进大数据发展行动纲要的通知

(国发〔2015〕50号)

各省、自治区、直辖市人民政府，国务院各部委、各直属机构：

现将《促进大数据发展行动纲要》印发给你们，请认真贯彻落实。

国务院

2015年8月31日

促进大数据发展行动纲要

大数据是以容量大、类型多、存取速度快、应用价值高为主要特征的数据集合，正快速发展为对数量巨大、来源分散、格式多样的数据进行采集、存储和关联分析，从中发现新知识、创造新价值、提升新能力的新一代信息技术和服务业态。

信息技术与经济社会的交汇融合引发了数据迅猛增长，数据已成为国家基础性战略资源，大数据正日益对全球生产、流通、分配、消费活动以及经济运行机制、社会生活方式和国家治理能力产生重要影响。目前，我国在大数据发展和应用方面已具备一定基础，拥有市场优势和发展潜力，但也存在政府数据开放共享不足、产业基础薄弱、缺乏顶层设计和统筹规划、法律法规建设滞后、创新应用领域不广等问题，亟待解决。为贯彻落实党中央、国务院决策部署，全面推进我国大数据发展和应用，加快建设数据强国，特制定本行动纲要。

一、发展形势和重要意义

全球范围内，运用大数据推动经济发展、完善社会治理、提升政府服务和监管能力正成为趋势，有关发达国家相继制定实施大数据战略性文件，大力推动大数据发展和应用。目前，我国互联网、移动互联网用户规模居全球第一，拥有丰富的数据资源和应用市场优势，大数据部分关键技术研发取得突破，涌现出一批互联网创新企业和创新应用，一些地方政府已启动大数据相关工作。坚持创新驱动发展，加快大数据部署，深化大数据应用，已成为稳增长、促改革、调结构、

惠民生和推动政府治理能力现代化的内在需要和必然选择。

（一）大数据成为推动经济转型发展的新动力。以数据流引领技术流、物质流、资金流、人才流，将深刻影响社会分工协作的组织模式，促进生产组织方式的集约和创新。大数据推动社会生产要素的网络化共享、集约化整合、协作化开发和高效化利用，改变了传统的生产方式和经济运行机制，可显著提升经济运行水平和效率。大数据持续激发商业模式创新，不断催生新业态，已成为互联网等新兴领域促进业务创新增值、提升企业核心价值的重要驱动力。大数据产业正在成为新的经济增长点，将对未来信息产业格局产生重要影响。

（二）大数据成为重塑国家竞争优势的新机遇。在全球信息化快速发展的大背景下，大数据已成为国家重要的基础性战略资源，正引领新一轮科技创新。充分利用我国的数据规模优势，实现数据规模、质量和应用水平同步提升，发掘和释放数据资源的潜在价值，有利于更好发挥数据资源的战略作用，增强网络空间数据主权保护能力，维护国家安全，有效提升国家竞争力。

（三）大数据成为提升政府治理能力的新途径。大数据应用能够揭示传统技术方式难以展现的关联关系，推动政府数据开放共享，促进社会事业数据融合和资源整合，将极大提升政府整体数据分析能力，为有效处理复杂社会问题提供新的手段。建立“用数据说话、用数据决策、用数据管理、用数据创新”的管理机制，实现基于数据的科学决策，将推动政府管理理念和社会治理模式进步，加快建设与社会主义市场经济体制和中国特色社会主义事业发展相适应的法治政府、创新政府、廉洁政府和服务型政府，逐步实现政府治理能力现代化。

二、指导思想和总体目标

（一）指导思想。深入贯彻党的十八大和十八届二中、三中、四中全会精神，按照党中央、国务院决策部署，发挥市场在资源配置中的决定性作用，加强顶层设计和统筹协调，大力推动政府信息系统和公共数据互联开放共享，加快政府信息平台整合，消除信息孤岛，推进数据资源向社会开放，增强政府公信力，引导社会发展，服务公众企业；以企业为主体，营造宽松公平环境，加大大数据关键技术研发、产业发展和人才培养力度，着力推进数据汇集和发掘，深化大数据在

各行业创新应用，促进大数据产业健康发展；完善法规制度和标准体系，科学规范利用大数据，切实保障数据安全。通过促进大数据发展，加快建设数据强国，释放技术红利、制度红利和创新红利，提升政府治理能力，推动经济转型升级。

（二）总体目标。立足我国国情和现实需要，推动大数据发展和应用在未来5-10年逐步实现以下目标：

打造精准治理、多方协作的社会治理新模式。将大数据作为提升政府治理能力的重要手段，通过高效采集、有效整合、深化应用政府数据和社会数据，提升政府决策和风险防范水平，提高社会治理的精准性和有效性，增强乡村社会治理能力；助力简政放权，支持从事前审批向事中事后监管转变，推动商事制度改革；促进政府监管和社会监督有机结合，有效调动社会力量参与社会治理的积极性。2017年底前形成跨部门数据资源共享共用格局。

建立运行平稳、安全高效的经济运行新机制。充分运用大数据，不断提升信用、财政、金融、税收、农业、统计、进出口、资源环境、产品质量、企业登记监管等领域数据资源的获取和利用能力，丰富经济统计数据来源，实现对经济运行更为准确的监测、分析、预测、预警，提高决策的针对性、科学性和时效性，提升宏观调控以及产业发展、信用体系、市场监管等方面管理效能，保障供需平衡，促进经济平稳运行。

构建以人为本、惠及全民的民生服务新体系。围绕服务型政府建设，在公用事业、市政管理、城乡环境、农村生活、健康医疗、减灾救灾、社会救助、养老服务、劳动就业、社会保障、文化教育、交通旅游、质量安全、消费维权、社区服务等领域全面推广大数据应用，利用大数据洞察民生需求，优化资源配置，丰富服务内容，拓展服务渠道，扩大服务范围，提高服务质量，提升城市辐射能力，推动公共服务向基层延伸，缩小城乡、区域差距，促进形成公平普惠、便捷高效的民生服务体系，不断满足人民群众日益增长的个性化、多样化需求。

开启大众创业、万众创新创新驱动新格局。形成公共数据资源合理适度开放共享的法规制度和政策体系，2018年底前建成国家政府数据统一开放平台，率先在信用、交通、医疗、卫生、就业、社保、地理、文化、教育、科技、资源、

农业、环境、安监、金融、质量、统计、气象、海洋、企业登记监管等重要领域实现公共数据资源合理适度向社会开放，带动社会公众开展大数据增值性、公益性开发和创新应用，充分释放数据红利，激发大众创业、万众创新活力。

培育高端智能、新兴繁荣的产业发展新生态。推动大数据与云计算、物联网、移动互联网等新一代信息技术融合发展，探索大数据与传统产业协同发展的新业态、新模式，促进传统产业转型升级和新兴产业发展，培育新的经济增长点。形成一批满足大数据重大应用需求的产品、系统和解决方案，建立安全可信的大数据技术体系，大数据产品和服务达到国际先进水平，国内市场占有率显著提高。培育一批面向全球的骨干企业和特色鲜明的创新型中小企业。构建形成政产学研用多方联动、协调发展的大数据产业生态体系。

三、主要任务

（一）加快政府数据开放共享，推动资源整合，提升治理能力。

1.大力推动政府部门数据共享。加强顶层设计和统筹规划，明确各部门数据共享的范围边界和使用方式，厘清各部门数据管理及共享的义务和权利，依托政府数据统一共享交换平台，大力推进国家人口基础信息库、法人单位信息资源库、自然资源和空间地理基础信息库等国家基础数据资源，以及金税、金关、金财、金审、金盾、金宏、金保、金土、金农、金水、金质等信息系统跨部门、跨区域共享。加快各地区、各部门、各有关企事业单位及社会组织信用信息系统的互联互通和信息共享，丰富面向公众的信用信息服务，提高政府服务和监管水平。结合信息惠民工程实施和智慧城市建设，推动中央部门与地方政府条块结合、联合试点，实现公共服务的多方数据共享、制度对接和协同配合。

2.稳步推动公共数据资源开放。在依法加强安全保障和隐私保护的前提下，稳步推动公共数据资源开放。推动建立政府部门和事业单位等公共机构数据资源清单，按照“增量先行”的方式，加强对政府部门数据的国家统筹管理，加快建设国家政府数据统一开放平台。制定公共机构数据开放计划，落实数据开放和维护责任，推进公共机构数据资源统一汇聚和集中向社会开放，提升政府数据开放共享标准化程度，优先推动信用、交通、医疗、卫生、就业、社保、地理、文化、

教育、科技、资源、农业、环境、安监、金融、质量、统计、气象、海洋、企业登记监管等民生保障服务相关领域的政府数据集向社会开放。建立政府和社会互动的大数据采集形成机制，制定政府数据共享开放目录。通过政务数据公开共享，引导企业、行业协会、科研机构、社会组织等主动采集并开放数据。

专栏1 政府数据资源共享开放工程

推动政府数据资源共享。制定政府数据资源共享管理办法，整合政府部门公共数据资源，促进互联互通，提高共享能力，提升政府数据的一致性和准确性。2017年底前，明确各部门数据共享的范围边界和使用方式，跨部门数据资源共享共用格局基本形成。

形成政府数据统一共享交换平台。充分利用统一的国家电子政务网络，构建跨部门的政府数据统一共享交换平台，到2018年，中央政府层面实现数据统一共享交换平台的全覆盖，实现金税、金关、金财、金审、金盾、金宏、金保、金土、金农、金水、金质等信息系统通过统一平台进行数据共享和交换。

形成国家政府数据统一开放平台。建立政府部门和事业单位等公共机构数据资源清单，制定实施政府数据开放共享标准，制定数据开放计划。2018年底前，建成国家政府数据统一开放平台。2020年底前，逐步实现信用、交通、医疗、卫生、就业、社保、地理、文化、教育、科技、资源、农业、环境、安监、金融、质量、统计、气象、海洋、企业登记监管等民生保障服务相关领域的政府数据集向社会开放。

专栏2 国家大数据资源统筹发展工程

整合各类政府信息平台和信息系统。严格控制新建平台，依托现有平台资源，在地市级以上（含地市级）政府集中构建统一的互联网政务数据服务平台和信息惠民服务平台，在基层街道、社区统一应用，并逐步向农村特别是农村社区延伸。除国务院另有规定外，原则上不再审批有关部门、地市级以下（不含地市级）政府新建孤立的信息平台和信息系统。到2018年，中央层面构建形成统一的互联网政务数据服务平台；国家信息惠民试点城市实现基础信息集中采集、多方利用，实现公共服务和社会信息服务的全人群覆盖、全天候受理和“一站式”办理。

整合分散的数据中心资源。充分利用现有政府和社会数据中心资源，运用云计算技术，整合规模小、效率低、能耗高的分散数据中心，构建形成布局合理、规模适度、保障有力、绿色集约的政务数据中心体系。统筹发挥各部门已建数据中心的作用，严格控制部门新建数据中心。开展区域试点，推进贵州等大数据综合试验区建设，促进区域性大数据基础设施的整合和数据资源的汇聚应用。

加快完善国家基础信息资源体系。加快建设完善国家人口基础信息库、法人单位信息资源库、自然资源和空间地理基础信息库等基础信息资源。依托现有相关信息系统，逐步完善健康、社保、就业、能源、信用、统计、质量、国土、农业、城乡建设、企业登记监管等重要领域信息资源。到2018年，跨部门共享校核的国家人口基础信息库、法人单位信息资源库、自然资源和空间地理基础信息库等国家基础信息资源体系基本建成，实现与各领域信息资源的汇聚整合和关联应用。

加强互联网信息采集利用。加强顶层设计，树立国际视野，充分利用已有资源，加强互联网信息采集、保存和分析能力建设，制定完善互联网信息保存相关法律法规，构建互联网信息保存和信息服务体系。

3.统筹规划大数据基础设施建设。结合国家政务信息化工程建设规划，统筹政务数据资源和社会数据资源，布局国家大数据平台、数据中心等基础设施。加快完善国家人口基础信息库、法人单位信息资源库、自然资源和空间地理基础信息库等基础信息资源和健康、就业、社保、能源、信用、统计、质量、国土、农业、城乡建设、企业登记监管等重要领域信息资源，加强与社会大数据的汇聚整合和关联分析。推动国民经济动员大数据应用。加强军民信息资源共享。充分利用现有企业、政府等数据资源和平台设施，注重对现有数据中心及服务器资源的改造和利用，建设绿色环保、低成本、高效率、基于云计算的大数据基础设施和区域性、行业性数据汇聚平台，避免盲目建设和重复投资。加强对互联网重要数据资源的备份及保护。

4.支持宏观调控科学化。建立国家宏观调控数据体系，及时发布有关统计指标和数据，强化互联网数据资源利用和信息服务，加强与政务数据资源的关联分析和融合利用，为政府开展金融、税收、审计、统计、农业、规划、消费、投资、

进出口、城乡建设、劳动就业、收入分配、电力及产业运行、质量安全、节能减排等领域运行动态监测、产业安全预测预警以及转变发展方式分析决策提供信息支持，提高宏观调控的科学性、预见性和有效性。

5.推动政府治理精准化。在企业监管、质量安全、节能降耗、环境保护、食品安全、安全生产、信用体系建设、旅游服务等领域，推动有关政府部门和企业单位将市场监管、检验检测、违法失信、企业生产经营、销售物流、投诉举报、消费维权等数据进行汇聚整合和关联分析，统一公示企业信用信息，预警企业不正当行为，提升政府决策和风险防范能力，支持加强事中事后监管和服务，提高监管和服务的针对性、有效性。推动改进政府管理和公共治理方式，借助大数据实现政府负面清单、权力清单和责任清单的透明化管理，完善大数据监督和技术反腐体系，促进政府简政放权、依法行政。

6.推进商事服务便捷化。加快建立公民、法人和其他组织统一社会信用代码制度，依托全国统一的信用信息共享交换平台，建设企业信用信息公示系统和“信用中国”网站，共享整合各地区、各领域信用信息，为社会公众提供查询注册登记、行政许可、行政处罚等各类信用信息的一站式服务。在全面实行工商营业执照、组织机构代码证和税务登记证“三证合一”、“一照一码”登记制度改革中，积极运用大数据手段，简化办理程序。建立项目并联审批平台，形成网上审批大数据资源库，实现跨部门、跨层级项目审批、核准、备案的统一受理、同步审查、信息共享、透明公开。鼓励政府部门高效采集、有效整合并充分运用政府数据和社会数据，掌握企业需求，推动行政管理流程优化再造，在注册登记、市场准入等商事服务中提供更加便捷有效、更有针对性的服务。利用大数据等手段，密切跟踪中小微企业特别是新设小微企业运行情况，为完善相关政策提供支持。

7.促进安全保障高效化。加强有关执法部门间的数据流通，在法律许可和确保安全的前提下，加强对社会治理相关领域数据的归集、发掘及关联分析，强化对妥善应对和处理重大突发公共事件的数据支持，提高公共安全保障能力，推动构建智能防控、综合治理的公共安全体系，维护国家安全和社会安定。

专栏3 政府治理大数据工程

推动宏观调控决策支持、风险预警和执行监督大数据应用。统筹利用政府和社会数据资源，探索建立国家宏观调控决策支持、风险预警和执行监督大数据应用体系。到2018年，开展政府和社会合作开发利用大数据试点，完善金融、税收、审计、统计、农业、规划、消费、投资、进出口、城乡建设、劳动就业、收入分配、电力及产业运行、质量安全、节能减排等领域国民经济相关数据的采集和利用机制，推进各级政府按照统一体系开展数据采集和综合利用，加强对宏观调控决策的支撑。

推动信用信息共享机制和信用信息系统建设。加快建立统一社会信用代码制度，建立信用信息共享交换机制。充分利用社会各方面信息资源，推动公共信用数据与互联网、移动互联网、电子商务等数据的汇聚整合，鼓励互联网企业运用大数据技术建立市场化的第三方信用信息共享平台，使政府主导征信体系的权威性和互联网大数据征信平台的规模效应得到充分发挥，依托全国统一的信用信息共享交换平台，建设企业信用信息公示系统，实现覆盖各级政府、各类别信用主体的基础信用信息共享，初步建成社会信用体系，为经济高效运行提供全面准确的基础信用信息服务。

建设社会治理大数据应用体系。到2018年，围绕实施区域协调发展、新型城镇化等重大战略和主体功能区规划，在企业监管、质量安全、质量诚信、节能降耗、环境保护、食品安全、安全生产、信用体系建设、旅游服务等领域探索开展一批应用试点，打通政府部门、企事业单位之间的数据壁垒，实现合作开发和综合利用。实时采集并汇总分析政府部门和企事业单位的市场监管、检验检测、违法失信、企业生产经营、销售物流、投诉举报、消费维权等数据，有效促进各级政府社会治理能力提升。

8.加快民生服务普惠化。结合新型城镇化发展、信息惠民工程实施和智慧城市建设，以优化提升民生服务、激发社会活力、促进大数据应用市场化服务为重点，引导鼓励企业和社会机构开展创新应用研究，深入发掘公共服务数据，在城乡建设、人居环境、健康医疗、社会救助、养老服务、劳动就业、社会保障、质量安全、文化教育、文化旅游、消费维权、城乡服务等领域开展大数据应用示范，推动传统公共服务数据与互联网、移动互联网、可穿戴设备等数据的汇聚整合，

开发各类便民应用，优化公共资源配置，提升公共服务水平。

专栏4 公共服务大数据工程

医疗健康服务大数据。构建电子健康档案、电子病历数据库，建设覆盖公共卫生、医疗服务、医疗保障、药品供应、计划生育和综合管理业务的医疗健康管理和数据应用体系。探索预约挂号、分级诊疗、远程医疗、检查检验结果共享、防治结合、医养结合、健康咨询等服务，优化形成规范、共享、互信的诊疗流程。鼓励和规范有关企事业单位开展医疗健康大数据创新应用研究，构建综合健康服务应用。

社会保障服务大数据。建设由城市延伸到农村的统一社会救助、社会福利、社会保障大数据平台，加强与相关部门的数据对接和信息共享，支撑大数据在劳动用工和社保基金监管、医疗保险对医疗服务行为监控、劳动保障监察、内控稽核以及人力资源社会保障相关政策制定和执行效果跟踪评价等方面的应用。利用大数据创新服务模式，为社会公众提供更为个性化、更具针对性的服务。

教育文化大数据。完善教育管理公共服务平台，推动教育基础数据的伴随式收集和全国互通共享。建立各阶段适龄入学人口基础数据库、学生基础数据库和终身电子学籍档案，实现学生学籍档案在不同教育阶段的纵向贯通。推动形成覆盖全国、协同服务、全网互通的教育资源云服务体系。探索发挥大数据对变革教育方式、促进教育公平、提升教育质量的支撑作用。加强数字图书馆、档案馆、博物馆、美术馆和文化馆等公益设施建设，构建文化传播大数据综合服务平台，传播中国文化，为社会提供文化服务。

交通旅游服务大数据。探索开展交通、公安、气象、安监、地震、测绘等跨部门、跨地域数据融合和协同创新。建立综合交通服务大数据平台，共同利用大数据提升协同管理和公共服务能力，积极吸引社会优质资源，利用交通大数据开展出行信息服务、交通诱导等增值服务。建立旅游投诉及评价全媒体交互中心，实现对旅游城市、重点景区游客流量的监控、预警和及时分流疏导，为规范市场秩序、方便游客出行、提升旅游服务水平、促进旅游消费和旅游产业转型升级提供有力支撑。

（二）推动产业创新发展，培育新兴业态，助力经济转型。

1.发展工业大数据。推动大数据在工业研发设计、生产制造、经营管理、市场营销、售后服务等产品全生命周期、产业链全流程各环节的应用，分析感知用户需求，提升产品附加价值，打造智能工厂。建立面向不同行业、不同环节的工业大数据资源聚合和分析应用平台。抓住互联网跨界融合机遇，促进大数据、物联网、云计算和三维（3D）打印技术、个性化定制等在制造业全产业链集成运用，推动制造模式变革和工业转型升级。

2.发展新兴产业大数据。大力培育互联网金融、数据服务、数据探矿、数据化学、数据材料、数据制药等新业态，提升相关产业大数据资源的采集获取和分析利用能力，充分发掘数据资源支撑创新的潜力，带动技术研发体系创新、管理方式变革、商业模式创新和产业价值链体系重构，推动跨领域、跨行业的数据融合和协同创新，促进战略性新兴产业发展、服务业创新发展和信息消费扩大，探索形成协同发展的新业态、新模式，培育新的经济增长点。

专栏5 工业和新兴产业大数据工程

工业大数据应用。利用大数据推动信息化和工业化深度融合，研究推动大数据在研发设计、生产制造、经营管理、市场营销、售后服务等产业链各环节的应用，研发面向不同行业、不同环节的大数据分析应用平台，选择典型企业、重点行业、重点地区开展工业企业大数据应用项目试点，积极推动制造业网络化和智能化。

服务业大数据应用。利用大数据支持品牌建立、产品定位、精准营销、认证认可、质量诚信提升和定制服务等，研发面向服务业的大数据解决方案，扩大服务范围，增强服务能力，提升服务质量，鼓励创新商业模式、服务内容和服务形式。

培育数据应用新业态。积极推动不同行业大数据的聚合、大数据与其他行业的融合，大力培育互联网金融、数据服务、数据处理分析、数据影视、数据探矿、数据化学、数据材料、数据制药等新业态。

电子商务大数据应用。推动大数据在电子商务中的应用，充分利用电子商务

中形成的大数据资源为政府实施市场监管和调控服务，电子商务企业应依法向政府部门报送数据。

3.发展农业农村大数据。构建面向农业农村的综合信息服务体系，为农民生产生活提供综合、高效、便捷的信息服 务，缩小城乡数字鸿沟，促进城乡发展一体化。加强农业农村经济大数据建设，完善村、县相关数据采集、传输、共享基础设施，建立农业农村数据采集、运算、应用、服务体系，强化农村生态环境治理，增强乡村社会治理能力。统筹国内国际农业数据资源，强化农业资源要素数据的集聚利用，提升预测预警能力。整合构建国家涉农大数据中心，推进各地区、各行业、各领域涉农数据资源的共享开放，加强数据资源发掘运用。加快农业大数据关键技术研发，加大示范力度，提升生产智能化、经营网络化、管理高效化、服务便捷化能力和水平。

专栏6 现代农业大数据工程

农业农村信息综合服务。充分利用现有数据资源，完善相关数据采集共享功能，完善信息进村入户村级站的数据采集和信息发布功能，建设农产品全球生产、消费、库存、进出口、价格、成本等数据调查分析系统工程，构建面向农业农村的综合信息服务平台，涵盖农业生产、经营、管理、服务和农村环境整治等环节，集合公益服务、便民服务、电子商务和网络服务，为农业农村农民生产生活提供综合、高效、便捷的信息服 务，加强全球农业调查分析，引导国内农产品生产和消费，完善农产品价格形成机制，缩小城乡数字鸿沟，促进城乡发展一体化。

农业资源要素数据共享。利用物联网、云计算、卫星遥感等技术，建立我国农业耕地、草原、林地、水利设施、水资源、农业设施设备、新型经营主体、农业劳动力、金融资本等资源要素数据监测体系，促进农业环境、气象、生态等信息共享，构建农业资源要素数据共享平台，为各级政府、企业、农户提供农业资源数据查询服务，鼓励各类市场主体充分发掘平台数据，开发测土配方施肥、统防统治、农业保险等服务。

农产品质量安全信息服务。建立农产品生产的生态环境、生产资料、生产过程、市场流通、加工储藏、检验检测等数据共享机制，推进数据实现自动化采集、

网络化传输、标准化处理和可视化运用，提高数据的真实性、准确性、及时性和关联性，与农产品电子商务等交易平台互联共享，实现各环节信息可查询、来源可追溯、去向可跟踪、责任可追究，推进实现种子、农药、化肥等重要生产资料信息可追溯，为生产者、消费者、监管者提供农产品质量安全信息服务，促进农产品消费安全。

4.发展万众创新大数据。适应国家创新驱动发展战略，实施大数据创新行动计划，鼓励企业和公众发掘利用开放数据资源，激发创新创业活力，促进创新链和产业链深度融合，推动大数据发展与科研创新有机结合，形成大数据驱动型的科研创新模式，打通科技创新和经济社会发展之间的通道，推动万众创新、开放创新和联动创新。

专栏7 万众创新大数据工程

大数据创新应用。通过应用创新开发竞赛、服务外包、社会众包、助推计划、补助奖励、应用培训等方式，鼓励企业和公众发掘利用开放数据资源，激发创新创业活力。

大数据创新服务。面向经济社会发展需求，研发一批大数据公共服务产品，实现不同行业、领域大数据的融合，扩大服务范围、提高服务能力。

发展科学大数据。积极推动由国家公共财政支持的公益性科研活动获取和产生的科学数据逐步开放共享，构建科学大数据国家重大基础设施，实现对国家重要科技数据的权威汇集、长期保存、集成管理和全面共享。面向经济社会发展需求，发展科学大数据应用服务中心，支持解决经济社会发展和国家安全重大问题。

知识服务大数据应用。利用大数据、云计算等技术，对各领域知识进行大规模整合，搭建层次清晰、覆盖全面、内容准确的知识资源库群，建立国家知识服务平台与知识资源服务中心，形成以国家平台为枢纽、行业平台为支撑，覆盖国民经济主要领域，分布合理、互联互通的国家知识服务体系，为生产生活提供精准、高水平的知识服务。提高我国知识资源的生产与供给能力。

5.推进基础研究和核心技术攻关。围绕数据科学理论体系、大数据计算系统与分析理论、大数据驱动的颠覆性应用模型探索等重大基础研究进行前瞻布局，

开展数据科学研究，引导和鼓励在大数据理论、方法及关键应用技术等方面展开探索。采取政产学研用相结合的协同创新模式和基于开源社区的开放创新模式，加强海量数据存储、数据清洗、数据分析发掘、数据可视化、信息安全与隐私保护等领域关键技术攻关，形成安全可靠的大数据技术体系。支持自然语言理解、机器学习、深度学习等人工智能技术创新，提升数据分析处理能力、知识发现能力和辅助决策能力。

6.形成大数据产品体系。围绕数据采集、整理、分析、发掘、展现、应用等环节，支持大型通用海量数据存储与管理软件、大数据分析发掘软件、数据可视化软件等软件产品和海量数据存储设备、大数据一体机等硬件产品发展，带动芯片、操作系统等信息技术核心基础产品发展，打造较为健全的大数据产品体系。大力发展与重点行业领域业务流程及数据应用需求深度融合的大数据解决方案。

专栏8 大数据关键技术及产品研发与产业化工程

通过优化整合后的国家科技计划（专项、基金等），支持符合条件的大数据关键技术研发。

加强大数据基础研究。融合数理科学、计算机科学、社会科学及其他应用学科，以研究相关性和复杂网络为主，探讨建立数据科学的学科体系；研究面向大数据计算的新体系和大数据分析理论，突破大数据认知与处理的技术瓶颈；面向网络、安全、金融、生物组学、健康医疗等重点需求，探索建立数据科学驱动行业应用的模型。

大数据技术产品研发。加大投入力度，加强数据存储、整理、分析处理、可视化、信息安全与隐私保护等领域技术产品的研发，突破关键环节技术瓶颈。到2020年，形成一批具有国际竞争力的大数据处理、分析、可视化软件和硬件支撑平台等产品。

提升大数据技术服务能力。促进大数据与各行业应用的深度融合，形成一批代表性应用案例，以应用带动大数据技术和产品研发，形成面向各行业的成熟的大数据解决方案。

7.完善大数据产业链。支持企业开展基于大数据的第三方数据分析发掘服务、

技术外包服务和知识流程外包服务。鼓励企业根据数据资源基础和业务特色，积极发展互联网金融和移动金融等新业态。推动大数据与移动互联网、物联网、云计算的深度融合，深化大数据在各行业的创新应用，积极探索创新协作共赢的应用模式和商业模式。加强大数据应用创新能力建设，建立政产学研用联动、大中小企业协调发展的大数据产业体系。建立和完善大数据产业公共服务支撑体系，组建大数据开源社区和产业联盟，促进协同创新，加快计量、标准化、检验检测和认证认可等大数据产业质量技术基础建设，加速大数据应用普及。

专栏9 大数据产业支撑能力提升工程

培育骨干企业。完善政策体系，着力营造服务环境优、要素成本低的良好氛围，加速培育大数据龙头骨干企业。充分发挥骨干企业的带动作用，形成大中小企业相互支撑、协同合作的大数据产业生态体系。到2020年，培育10家国际领先的大数据核心龙头企业，500家大数据应用、服务和产品制造企业。

大数据产业公共服务。整合优质公共服务资源，汇聚海量数据资源，形成面向大数据相关领域的公共服务平台，为企业和用户提供研发设计、技术产业化、人力资源、市场推广、评估评价、认证认可、检验检测、宣传展示、应用推广、行业咨询、投融资、教育培训等公共服务。

中小微企业公共服务大数据。整合现有中小微企业公共服务系统与数据资源，链接各省（区、市）建成的中小微企业公共服务线上管理系统，形成全国统一的中小微企业公共服务大数据平台，为中小微企业提供科技服务、综合服务、商贸服务等各类公共服务。

（三）强化安全保障，提高管理水平，促进健康发展。

1.健全大数据安全保障体系。加强大数据环境下的网络安全问题研究和基于大数据的网络安全技术研究，落实信息安全等级保护、风险评估等网络安全制度，建立健全大数据安全保障体系。建立大数据安全评估体系。切实加强关键信息基础设施安全防护，做好大数据平台及服务商的可靠性及安全性评测、应用安全评测、监测预警和风险评估。明确数据采集、传输、存储、使用、开放等各环节保障网络安全的范围边界、责任主体和具体要求，切实加强对涉及国家利益、公共

安全、商业秘密、个人隐私、军工科研生产等信息的保护。妥善处理发展创新与保障安全的关系，审慎监管，保护创新，探索完善安全保密管理规范措施，切实保障数据安全。

2.强化安全支撑。采用安全可信产品和服务，提升基础设施关键设备安全可靠水平。建设国家网络安全信息汇聚共享和关联分析平台，促进网络安全相关数据融合和资源合理分配，提升重大网络安全事件应急处理能力；深化网络安全防护体系和态势感知能力建设，增强网络空间安全防护和安全事件识别能力。开展安全监测和预警通报工作，加强大数据环境下防攻击、防泄露、防窃取的监测、预警、控制和应急处置能力建设。

专栏10 网络和大数据安全保障工程

网络和大数据安全支撑体系建设。在涉及国家安全稳定的领域采用安全可靠的产品和服务，到2020年，实现关键部门的关键设备安全可靠。完善网络安全保密防护体系。

大数据安全保障体系建设。明确数据采集、传输、存储、使用、开放等各环节保障网络安全的范围边界、责任主体和具体要求，建设完善金融、能源、交通、电信、统计、广电、公共安全、公共事业等重要数据资源和信息系统的安全保密防护体系。

网络安全信息共享和重大风险识别大数据支撑体系建设。通过对网络安全威胁特征、方法、模式的追踪、分析，实现对网络安全威胁新技术、新方法的及时识别与有效防护。强化资源整合与信息共享，建立网络安全信息共享机制，推动政府、行业、企业间的网络风险信息共享，通过大数据分析，对网络安全重大事件进行预警、研判和应对指挥。

四、政策机制

(一)完善组织实施机制。建立国家大数据发展和应用统筹协调机制，推动形成职责明晰、协同推进的工作格局。加强大数据重大问题研究，加快制定出台配套政策，强化国家数据资源统筹管理。加强大数据与物联网、智慧城市、云计算等相关政策、规划的协同。加强中央与地方协调，引导地方各级政府结合自身

条件合理定位、科学谋划，将大数据发展纳入本地区经济社会和城镇化发展规划，制定出台促进大数据产业发展的政策措施，突出区域特色和分工，抓好措施落实，实现科学有序发展。设立大数据专家咨询委员会，为大数据发展应用及相关工程实施提供决策咨询。各有关部门要进一步统一思想，认真落实本行动纲要提出的各项任务，共同推动形成公共信息资源共享共用和大数据产业健康安全发展的良好格局。

（二）加快法规制度建设。修订政府信息公开条例。积极研究数据开放、保护等方面制度，实现对数据资源采集、传输、存储、利用、开放的规范管理，促进政府数据在风险可控原则下最大程度开放，明确政府统筹利用市场主体大数据的权限及范围。制定政府信息资源管理办法，建立政府部门数据资源统筹管理和共享复用制度。研究推动网上个人信息保护立法工作，界定个人信息采集应用的范围和方式，明确相关主体的权利、责任和义务，加强对数据滥用、侵犯个人隐私等行为的管理和惩戒。推动出台相关法律法规，加强对基础信息网络和关键行业领域重要信息系统的安全保护，保障网络数据安全。研究推动数据资源权益相关立法工作。

（三）健全市场发展机制。建立市场化的数据应用机制，在保障公平竞争的前提下，支持社会资本参与公共服务建设。鼓励政府与企业、社会机构开展合作，通过政府采购、服务外包、社会众包等多种方式，依托专业企业开展政府大数据应用，降低社会管理成本。引导培育大数据交易市场，开展面向应用的数据交易市场试点，探索开展大数据衍生产品交易，鼓励产业链各环节市场主体进行数据交换和交易，促进数据资源流通，建立健全数据资源交易机制和定价机制，规范交易行为。

（四）建立标准规范体系。推进大数据产业标准体系建设，加快建立政府部门、事业单位等公共机构的数据标准和统计标准体系，推进数据采集、政府数据开放、指标口径、分类目录、交换接口、访问接口、数据质量、数据交易、技术产品、安全保密等关键共性标准的制定和实施。加快建立大数据市场交易标准体系。开展标准验证和应用试点示范，建立标准符合性评估体系，充分发挥标准在培育服务市场、提升服务能力、支撑行业管理等方面的作用。积极参与相关国际

标准制定工作。

(五) 加大财政金融支持。强化中央财政资金引导，集中力量支持大数据核心技术攻关、产业链构建、重大应用示范和公共服务平台建设等。利用现有资金渠道，推动建设一批国际领先的重大示范工程。完善政府采购大数据服务的配套政策，加大对政府部门和企业合作开发大数据的支持力度。鼓励金融机构加强和改进金融服务，加大对大数据企业的支持力度。鼓励大数据企业进入资本市场融资，努力为企业重组并购创造更加宽松的金融政策环境。引导创业投资基金投向大数据产业，鼓励设立一批投资于大数据产业领域的创业投资基金。

(六) 加强专业人才培养。创新人才培养模式，建立健全多层次、多类型的大数据人才培养体系。鼓励高校设立数据科学和数据工程相关专业，重点培养专业化数据工程师等大数据专业人才。鼓励采取跨校联合培养等方式开展跨学科大数据综合型人才培养，大力培养具有统计分析、计算机技术、经济管理等多学科知识的跨界复合型人才。鼓励高等院校、职业院校和企业合作，加强职业技能人才实践培养，积极培育大数据技术和应用创新型人才。依托社会化教育资源，开展大数据知识普及和教育培训，提高社会整体认知和应用水平。

(七) 促进国际交流合作。坚持平等合作、互利共赢的原则，建立完善国际合作机制，积极推进大数据技术交流与合作，充分利用国际创新资源，促进大数据相关技术发展。结合大数据应用创新需要，积极引进大数据高层次人才和领军人才，完善配套措施，鼓励海外高端人才回国就业创业。引导国内企业与国际优势企业加强大数据关键技术、产品的研发合作，支持国内企业参与全球市场竞争，积极开拓国际市场，形成若干具有国际竞争力的大数据企业和产品。

(五) 国务院关于印发政务信息资源共享管理暂行办法的通知

(国发〔2016〕51号)

各省、自治区、直辖市人民政府，国务院各部委、各直属机构：

现将《政务信息资源共享管理暂行办法》印发给你们，请认真贯彻执行。

国务院

2016年9月5日

政务信息资源共享管理暂行办法

第一章 总 则

第一条 为加快推动政务信息系统互联和公共数据共享，增强政府公信力，提高行政效率，提升服务水平，充分发挥政务信息资源共享在深化改革、转变职能、创新管理中的重要作用，依据相关法律法规和《国务院关于印发促进大数据发展行动纲要的通知》（国发〔2015〕50号）等规定，制定本办法。

第二条 本办法所称政务信息资源，是指政务部门在履行职责过程中制作或获取的，以一定形式记录、保存的文件、资料、图表和数据等各类信息资源，包括政务部门直接或通过第三方依法采集的、依法授权管理的和因履行职责需要依托政务信息系统形成的信息资源等。

本办法所称政务部门，是指政府部门及法律法规授权具有行政职能的事业单位和社会组织。

第三条 本办法用于规范政务部门间政务信息资源共享工作，包括因履行职责需要使用其他政务部门政务信息资源和为其他政务部门提供政务信息资源的行为。

第四条 促进大数据发展部际联席会议（以下简称联席会议）负责组织、指导、协调和监督政务信息资源共享工作，指导和组织国务院各部门、各地方政府编制政务信息资源目录，组织编制国家政务信息资源目录，并指导国家数据共享

交换平台建设、运行、管理单位开展国家政务信息资源目录的日常维护工作。

各政务部门按本办法规定负责本部门与数据共享交换平台（以下简称共享平台）的联通，并按照政务信息资源目录向共享平台提供共享的政务信息资源（以下简称共享信息），从共享平台获取并使用共享信息。

第五条 政务信息资源共享应遵循以下原则：

（一）以共享为原则，不共享为例外。各政务部门形成的政务信息资源原则上应予共享，涉及国家秘密和安全的，按相关法律法规执行。

（二）需求导向，无偿使用。因履行职责需要使用共享信息的部门（以下简称使用部门）提出明确的共享需求和信息使用用途，共享信息的产生和提供部门（以下统称提供部门）应及时响应并无偿提供共享服务。

（三）统一标准，统筹建设。按照国家政务信息资源相关标准进行政务信息资源的采集、存储、交换和共享工作，坚持“一数一源”、多元校核，统筹建设政务信息资源目录体系和共享交换体系。

（四）建立机制，保障安全。联席会议统筹建立政务信息资源共享管理机制和信息共享工作评价机制，各政务部门和共享平台管理单位应加强对共享信息采集、共享、使用全过程的身份鉴别、授权管理和安全保障，确保共享信息安全。

第六条 各政务部门应加强基于信息共享的业务流程再造和优化，创新社会管理和服务模式，提高信息化条件下社会治理能力和公共服务水平。

第二章 政务信息资源目录

第七条 国家发展改革委负责制定《政务信息资源目录编制指南》，明确政务信息资源的分类、责任方、格式、属性、更新时限、共享类型、共享方式、使用要求等内容。

第八条 各政务部门按照《政务信息资源目录编制指南》要求编制、维护部门政务信息资源目录，并在有关法律法规作出修订或行政管理职能发生变化之日起15个工作日内更新本部门政务信息资源目录。各地方政府按照《政务信息资源目录编制指南》要求编制、维护地方政务信息资源目录，并负责对本级各政务部

门政务信息资源目录更新工作的监督考核。

国家发展改革委汇总形成国家政务信息资源目录，并建立目录更新机制。国家政务信息资源目录是实现国家政务信息资源共享和业务协同的基础，是政务部门间信息资源共享的依据。

第三章 政务信息资源分类与共享要求

第九条 政务信息资源按共享类型分为无条件共享、有条件共享、不予共享等三种类型。

可提供给所有政务部门共享使用的政务信息资源属于无条件共享类。

可提供给相关政务部门共享使用或仅能够部分提供给所有政务部门共享使用的政务信息资源属于有条件共享类。

不宜提供给其他政务部门共享使用的政务信息资源属于不予共享类。

第十条 政务信息资源共享及目录编制应遵循以下要求：

（一）凡列入不予共享类的政务信息资源，必须有法律、行政法规或党中央、国务院政策依据。

（二）人口信息、法人单位信息、自然资源和空间地理信息、电子证照信息等基础信息资源的基础信息项是政务部门履行职责的共同需要，必须依据整合共建原则，通过在各级共享平台上集中建设或通过接入共享平台实现基础数据统筹管理、及时更新，在部门间实现无条件共享。基础信息资源的业务信息项可按照分散和集中相结合的方式建设，通过各级共享平台予以共享。基础信息资源目录由基础信息资源库的牵头建设部门负责编制并维护。

（三）围绕经济社会发展的同一主题领域，由多部门共建项目形成的主题信息资源，如健康保障、社会保障、食品药品安全、安全生产、价格监管、能源安全、信用体系、城乡建设、社区治理、生态环保、应急维稳等，应通过各级共享平台予以共享。主题信息资源目录由主题信息资源牵头部门负责编制并维护。

第四章 共享信息的提供与使用

第十一条 国家发展改革委负责组织推动国家共享平台及全国共享平台体系建设。各地市级以上地方人民政府要明确政务信息资源共享主管部门，负责组织本级共享平台建设。共享平台是管理国家政务信息资源目录、支撑各政务部门开展政务信息资源共享交换的国家关键信息基础设施，包括共享平台（内网）和共享平台（外网）两部分。

共享平台（内网）应按照涉密信息系统分级保护要求，依托国家电子政务内网建设和管理；共享平台（外网）应按照国家网络安全相关制度和要求，依托国家电子政务外网建设和管理。

各政务部门业务信息系统原则上通过国家电子政务内网或国家电子政务外网承载，通过共享平台与其他政务部门共享交换数据。各政务部门应抓紧推进本部门业务信息系统向国家电子政务内网或国家电子政务外网迁移，并接入本地区共享平台。凡新建的需要跨部门共享信息的业务信息系统，必须通过各级共享平台实施信息共享，原有跨部门信息共享交换系统应逐步迁移到共享平台。

第十二条 使用部门应根据履行职责需要使用共享信息。属于无条件共享类的信息资源，使用部门在共享平台上直接获取；属于有条件共享类的信息资源，使用部门通过共享平台向提供部门提出申请，提供部门应在10个工作日内予以答复，使用部门按答复意见使用共享信息，对不予共享的，提供部门应说明理由；属于不予共享类的信息资源，以及有条件共享类中提供部门不予共享的信息资源，使用部门因履行职责确需使用的，由使用部门与提供部门协商解决，协商未果的由本级政务信息资源共享主管部门协调解决，涉及中央有关部门的由联席会议协调解决。

提供部门在向使用部门提供共享信息时，应明确信息的共享范围和使用用途（如，作为行政依据、工作参考，用于数据校核、业务协同等），原则上通过共享平台提供，鼓励采用系统对接、前置机共享、联机查询、部门批量下载等方式。

各政务部门应充分利用共享信息。凡属于共享平台可以获取的信息，各政务部门原则上不得要求自然人、法人或其他组织重复提交。

第十三条 按照“谁主管，谁提供，谁负责”的原则，提供部门应及时维护

和更新信息，保障数据的完整性、准确性、时效性和可用性，确保所提供的共享信息与本部门所掌握信息的一致性。

第十四条 按照“谁经手，谁使用，谁管理，谁负责”的原则，使用部门应根据履行职责需要依法依规使用共享信息，并加强共享信息使用全过程管理。

使用部门对从共享平台获取的信息，只能按照明确的使用用途用于本部门履行职责需要，不得直接或以改变数据形式等方式提供给第三方，也不得用于或变相用于其他目的。

第十五条 建立疑义、错误信息快速校核机制，使用部门对获取的共享信息有疑义或发现有明显错误的，应及时反馈提供部门予以校核。校核期间，办理业务涉及自然人、法人或其他组织的，如已提供合法有效证明材料，受理单位应照常办理，不得拒绝、推诿或要求办事人办理信息更正手续。

第五章 信息共享工作的监督和保障

第十六条 联席会议负责政务信息资源共享的统筹协调，建立信息共享工作评价机制，督促检查政务信息资源共享工作落实情况。

第十七条 国家发展改革委、国家网信办组织编制信息共享工作评价办法，每年会同中央编办、财政部等部门，对各政务部门提供和使用共享信息情况进行评估，并公布评估报告和改进意见。

第十八条 国务院各部门、各省级人民政府和国家共享平台管理单位应于每年2月底前向联席会议报告上一年度政务信息资源共享情况，联席会议向国务院提交政务信息资源共享情况年度报告。

第十九条 国家标准委会同共享平台管理单位，在已有政务信息资源相关标准基础上，建立完善政务信息资源的目录分类、采集、共享交换、平台对接、网络安全保障等方面的标准，形成完善的政务信息资源共享标准体系。

第二十条 国家网信办负责组织建立政务信息资源共享网络安全管理制度，指导督促政务信息资源采集、共享、使用全过程的网络安全保障工作，指导推进政务信息资源共享风险评估和安全审查。

共享平台管理单位要加强共享平台安全防护，切实保障政务信息资源共享交换时的数据安全；提供部门和使用部门要加强政务信息资源采集、共享、使用时的安全保障工作，落实本部门对接系统的网络安全防护措施。

共享信息涉及国家秘密的，提供部门和使用部门应当遵守有关保密法律法规的规定，在信息共享工作中分别承担相关保障责任。

第二十一条 国家发展改革委、财政部、国家网信办建立国家政务信息化项目建设投资和运维经费协商机制，对政务部门落实政务信息资源共享要求和网络安全要求的情况进行联合考核，凡不符合政务信息资源共享要求的，不予审批建设项目，不予安排运维经费。

国家发展改革委负责在国家政务信息化建设规划制定、项目审批、投资计划安排、项目验收等环节进行考核。财政部负责在国家政务信息化建设项目预算下达、运维经费安排等环节进行考核。国家网信办负责在网络安全保障方面进行考核。

政务信息化项目立项申请前应预编形成项目信息资源目录，作为项目审批要件。项目建成后应将项目信息资源目录纳入共享平台目录管理系统，作为项目验收要求。

政务信息资源共享相关项目建设资金纳入政府固定资产投资，政务信息资源共享相关工作经费纳入部门财政预算，并给予优先安排。

第二十二条 审计机关应依法履行职责，在国家大数据政策的贯彻落实、政务信息资源共享中发挥监督作用，保障专项资金使用的真实性、合法性和效益性，推动完善相关政策制度。

第二十三条 各政务部门应建立健全政务信息资源共享工作管理制度，明确目标、责任和实施机构。各政务部门主要负责人是本部门政务信息资源共享工作的第一责任人。

第二十四条 国务院各部门、各省级人民政府有下列情形之一的，由国家发展改革委通知整改；未在规定时间内完成整改的，国家发展改革委要及时将有关

情况上报国务院:

- (一) 未按要求编制或更新政务信息资源目录;
- (二) 未向共享平台及时提供共享信息;
- (三) 向共享平台提供的数据和本部门所掌握信息不一致, 未及时更新数据或提供的数据不符合有关规范、无法使用;
- (四) 将共享信息用于履行本单位职责需要以外的目的;
- (五) 违反本办法规定的其他行为。

第六章 附 则

第二十五条 本办法由国家发展改革委负责解释。

第二十六条 本办法自印发之日起施行。

(六) 国务院办公厅关于印发进一步深化“互联网+政务服务”推进政务服务“一网、一门、一次”改革实施方案的通知

(国办发〔2018〕45号)

各省、自治区、直辖市人民政府，国务院各部委、各直属机构：

《进一步深化“互联网+政务服务”推进政务服务“一网、一门、一次”改革实施方案》已经国务院同意，现印发给你们，请认真贯彻执行。

国务院办公厅

2018年6月10日

进一步深化“互联网+政务服务”，充分运用信息化手段解决企业和群众反映强烈的办事难、办事慢、办事繁的问题，是党中央、国务院作出的重大决策部署。为加快推进政务服务“一网通办”和企业群众办事“只进一扇门”、“最多跑一次”，根据党中央、国务院关于推进审批服务便民化、“互联网+政务服务”、政务信息系统整合共享等重要工作部署，制定本实施方案。

一、发展现状和总体要求

党的十八大以来，以习近平同志为核心的党中央高度重视以信息化推进国家治理体系和治理能力现代化，强调要加快推动电子政务，打通信息壁垒，构建全流程一体化在线服务平台，助力建设人民满意的服务型政府。国务院将“互联网+政务服务”作为深化“放管服”改革的关键环节，专门印发文件，作出全面部署。一些部门和地方积极探索，深入推进“互联网+政务服务”，加强信息共享，优化政务流程，一批堵点难点问题得到初步解决，服务创新典型不断涌现，引领政务服务改革创新不断取得新成效。同时也应看到，目前政务服务“一网通办”、“只进一扇门”、“最多跑一次”等改革仍是局部区域和部分领域的探索实践，不少地区、部门、领域仍大量存在困扰企业群众的“办证多、办事难”等现象，与构建方便快捷、公平普惠、优质高效的网上政务服务体系目标相比仍有较大差距。

民之所望，改革所向。党的十九大对决胜全面建成小康社会、开启全面建设社会主义现代化国家新征程作出了全面部署。要深入贯彻党的十九大和十九届二中、三中全会精神，以习近平新时代中国特色社会主义思想为指导，牢固树立和贯彻落实新发展理念，深化“放管服”改革，进一步推进“互联网+政务服务”，加快构建全国一体化网上政务服务体系，推进跨层级、跨地域、跨系统、跨部门、跨业务的协同管理和服务，推动企业和群众办事线上“一网通办”（一网），线下“只进一扇门”（一门），现场办理“最多跑一次”（一次），让企业和群众到政府办事像“网购”一样方便。

二、基本原则和工作目标

（一）基本原则。

需求导向、聚焦问题、分类施策。坚持以人民为中心的发展思想，聚焦企业和群众办事的难点、政务服务的堵点和痛点，因事制宜，对各类办事事项分别提出有针对性的推进方案，不断满足人民群众的需求。

重点先行、总结经验、加快推广。选择与企业和群众生产生活关系最密切的重点领域和办理量大的高频事项，分阶段、分步骤推进，总结各地政务服务工作成功经验和创新做法，加强成果复制和宣传推广，形成高效有序推进局面。

整合共享、优化流程、创新服务。坚持联网通办是原则、孤网是例外，政务服务上网是原则、不上网是例外，加强政务信息资源跨层级、跨地域、跨系统、跨部门、跨业务互联互通和协同共享。运用互联网、大数据、人工智能等信息技术，通过技术创新和流程再造，增强综合服务能力，进一步提升政务服务效能。

统筹推进、条块结合、上下联动。注重政府管理和服务的系统性、整体性，加强行业主管部门业务指导和政策支持，充分调动地方政府的积极性和主动性，加强制度衔接，有效整合各方资源，促进纵横协同、上下联动，构建一体化联合推进机制，提升协同服务能力和综合管理水平。

（二）工作目标。

到2018年底，“一网、一门、一次”改革初见成效，先进地区成功经验在全

国范围内得到有效推广。在“一网通办”方面，省级政务服务事项网上可办率不低于80%，市县级政务服务事项网上可办率不低于50%；在“只进一扇门”方面，市县级政务服务事项进驻综合性实体政务大厅比例不低于70%，50%以上政务服务事项实现“一窗”分类受理；在“最多跑一次”方面，企业和群众到政府办事提供的材料减少30%以上，省市县各级30个高频事项实现“最多跑一次”。

到2019年底，重点领域和高频事项基本实现“一网、一门、一次”。在“一网通办”方面，省级政务服务事项网上可办率不低于90%，市县级政务服务事项网上可办率不低于70%；在“只进一扇门”方面，除对场地有特殊要求的事项外，政务服务事项进驻综合性实体政务大厅基本实现“应进必进”，70%以上政务服务事项实现“一窗”分类受理；在“最多跑一次”方面，企业和群众到政府办事提供的材料减少60%以上，省市县各级100个高频事项实现“最多跑一次”。

三、以整合促便捷，推进线上“一网通办”

按照政务服务“一网通办”的要求，加快建设国家、省、市三级互联的网上政务服务平台体系，推动政务服务“一次登录、全网通办”，大幅提高政务服务便捷性。

（一）整合构建全国一体化网上政务服务平台。

按照党中央、国务院关于推进审批服务便民化有关要求，加强顶层设计，加快构建以国家政务服务平台为枢纽、以各地区各部门网上政务服务平台为基础的全流程一体化在线服务平台。加强各省（自治区、直辖市）平台一体化、规范化建设。整合各级政府部门分散的政务服务资源和网上服务入口，加快推动各级政府部门业务信息系统接入本级或上级政务服务平台。依托国家政务服务平台为全国各地区各部门网上政务服务提供公共入口、公共通道和公共支撑，实现全国网上政务服务统一实名身份认证，让企业和群众网上办事“一次认证、全国漫游”。发挥好中国政府网总门户作用。

（二）推动更多政务服务事项网上办理。

切实提高政务服务事项网上办理比例，除法律法规另有规定或涉密等外，原则上各级政务服务事项均应纳入网上政务服务平台办理，并按照国家政务服务平

台相关标准规范组织实施。根据推进审批服务标准化有关要求，推动各地区各部门网上政务服务平台标准化建设和互联互通，实现政务服务同一事项、同一标准、同一编码。拓展网上办事广度和深度，延长网上办事链条，实现从网上咨询、网上申报到网上预审、网上办理、网上反馈“应上尽上、全程在线”。

（三）拓展政务服务移动应用。

推动政务服务向“两微一端”等延伸拓展，为群众提供多样性、多渠道、便利化服务。结合国家政务服务平台建设，加强和规范政务服务移动应用建设管理，推动更多政务服务事项提供移动端服务。调动社会资源力量，鼓励开展第三方便民服务应用。加强政务新媒体监管，提升服务水平。

四、以集成提效能，推进线下“只进一扇门”

以企业和群众办事“只进一扇门”为目标，大力推行政务服务集中办理，实现“多门”变“一门”，促进政务服务线上线下集成融合，不断提升政府服务效能。

（一）推动实体大厅“多门”变“一门”。

优化提升政务服务大厅“一站式”功能，完善省、市、县、乡镇综合性政务大厅集中服务模式，推动将垂直管理部门在本行政区域办理的政务服务事项纳入综合性政务大厅集中办理，加快实现“前台综合受理、后台分类审批、综合窗口出件”，实现企业和群众必须到现场办理的事项“只进一扇门”。除因安全等特殊原因外，原则上不再保留各地政府部门单独设立的服务大厅。

（二）推动线上线下集成融合。

依托网上政务服务平台，实时汇入网上申报、排队预约、现场排队叫号、服务评价、事项受理、审批（审查）结果和审批证照等信息，实现线上线下功能互补、无缝衔接、全过程留痕，为企业和群众办事线下“只进一扇门”提供有力支撑。

五、以创新促精简，让企业和群众“最多跑一次”

以企业和群众办事“少跑腿”为目标，梳理必须到现场办理事项的“最多跑

一次”目录，精简办事环节和材料，推动政务服务入口全面向基层延伸，力争实现企业和群众办事“最多跑一次”。

（一）大力推进减材料、减环节。

整合涉及多部门事项的共性材料，推广多业务申请表信息复用，通过“一表申请”将企业和个人基本信息材料一次收齐、后续反复使用，减少重复填写和重复提交。充分依托网上政务服务平台，以与企业生产经营、群众生产生活密切相关的重点领域和办理量大的高频事项为重点，通过优化办事系统、简化办事材料、精简办事环节，让更多政务服务事项“最多跑一次”。

（二）推进“最多跑一次”向基层延伸。

按照推进审批服务便民化“马上办、网上办、就近办、一次办”的要求，加强乡镇（街道）便民服务中心、村庄（社区）服务站点建设，推动基于互联网、自助终端、移动终端的政务服务入口全面向基层延伸，打造基层“一站式”综合便民服务平台，进一步提高基层响应群众诉求和为民服务的能力，推动实现“最多跑一次”省市县乡村全覆盖。

六、以共享筑根基，让“数据多跑路”

（一）建立完善全国数据共享交换体系。

构建全国统一、多级互联的数据共享交换平台体系，强化平台功能、完善管理规范，使其具备跨层级、跨地域、跨系统、跨部门、跨业务的数据调度能力。按照“统一受理、平台授权”的原则，建立数据共享授权机制。对于无条件共享且服务接口不需要管控参数的数据，由平台直接提供；对于有条件共享，或者无条件共享但服务接口需要管控参数的数据，由平台推送给部门受理。建立限期反馈机制，对于数据需求申请，平台管理部门应于3个工作日内完成申请规范性审查，并通过平台回复受理意见，不予受理的应回复原因；由平台直接提供的数据，应于受理后3个工作日内提供；由部门受理的数据，数据提供部门应在受理后10个工作日内完成审批。

（二）加快完善政务数据资源体系。

遵循“一数一源、多源校核、动态更新”原则，各级政府要构建并完善政务数据资源体系，持续完善数据资源目录，动态更新政务数据资源，不断提升数据质量，扩大共享覆盖面，提高服务可用性。完善数据共享责任清单机制，进一步明确各部门共享责任，在落实国务院部门第一批数据共享责任清单的基础上，制定发布第二批数据共享责任清单，新增拓展1000项数据共享服务，加强数据共享服务运行监测，全面清理并制止仅向特定企业、社会组织开放公共数据的行为。

（三）做好政务信息系统改造对接。

按照谁建设系统、谁负责对接的原则，各级政务部门要加快改造自有的跨层级垂直业务信息系统，并与各级政务服务平台对接，实现跨层级、跨地域、跨系统、跨部门、跨业务数据互联互通，避免数据和业务“两张皮”，减少在不同系统中重复录入，提高基层窗口工作效率。各级政务信息化建设项目审批部门和运维经费审批部门要联合建立政务信息系统清单制度，加强清单式管理，对于未按要求进行改造对接的，不审批新项目，不拨付运维经费。原则上不再批准单个部门建设孤立信息系统。

（四）推进事中事后监管信息“一网通享”。

积极推进跨部门“双随机、一公开”监管信息共享，依托“信用中国”网站和国家企业信用信息公示系统，提供登记备案、行政许可、行政处罚、经营异常名录、严重违法失信企业名单、监督检查、质量抽检等信用信息查询和共享服务。推进事中事后监管信息与政务服务深度融合，整合市场监管相关数据资源，加强对市场环境的大数据监测分析和预测预警，推进线上线下一体化监管。

（五）加强数据共享安全保障。

依法加强隐私等信息保护。研究政务信息资源分类分级制度，制定数据安全管理办法，明确数据采集、传输、存储、使用、共享、开放等环节安全保障的措施、责任主体和具体要求。提高国家电子政务外网、国家数据共享交换平台和国家政务服务平台的安全防护能力。推进政务信息资源共享风险评估和安全审查，强化应急预案管理，切实做好数据安全事件的应急处置。

七、保障措施

（一）建立健全“一网通办”的标准规范。

研究制定人口、法人、电子证照等基础数据共享的国家标准。加快完成电子证照库、人口综合库、法人综合库、公共信用库等规范编制工作，加快电子证照应用推广和跨部门、跨区域互认共享。建立健全政务信息资源数据采集、数据质量、目录分类管理、共享交换接口、共享交换服务、平台运行管理等方面的标准。

（二）加快完善相关法规制度。

各部门要抓紧梳理“互联网+政务服务”急需的以及开展“一网通办”不相适应的法律法规和规章制度，加快推动立改废。推动制定完善信息保护的法律制度，切实保护政务信息资源使用过程中的个人隐私和商业秘密。研究制订政务服务事项电子文件归档规范，推动开展相关试点，逐步消除电子化归档的法规制度障碍。

（三）建立监督举报投诉机制。

依托中国政府网及各级政府网站、各级政务服务平台、政务服务热线等，畅通互动渠道，方便群众咨询办事和投诉举报，接受群众监督。建立政务服务举报投诉平台，统一受理企业和群众对未实现政务服务“一网通办”、办事不便利等突出问题的举报投诉，并及时开展核查处理。

（四）开展百项问题疏解和百佳案例推广行动。

开展百项问题疏解行动，聚焦企业和群众关注的身份和教育证明、商事服务、社保低保、就业创业、居住户籍等方面的堵点难点问题，形成分级覆盖、热点聚焦的百项问题清单，逐项研究解决。开展百佳案例推广行动，深入分析总结先进经验，统筹组织对口帮扶工作，推动百佳案例先进经验复制落地。

各地区、各部门要认真贯彻落实党中央、国务院决策部署和推进审批服务便民化的要求，层层压实责任，加强统筹协调，结合实际精心组织落实本实施方案，推动“互联网+政务服务”取得更大实效。

(七) 国务院办公厅关于印发科学数据管理办法的通知

(国办发〔2018〕17号)

各省、自治区、直辖市人民政府，国务院各部委、各直属机构：

《科学数据管理办法》已经国务院同意，现印发给你们，请认真贯彻执行。

国务院办公厅

2018年3月17日

第一章 总 则

第一条 为进一步加强和规范科学数据管理，保障科学数据安全，提高开放共享水平，更好支撑国家科技创新、经济社会发展和国家安全，根据《中华人民共和国科学技术进步法》、《中华人民共和国促进科技成果转化法》和《政务信息资源共享管理暂行办法》等规定，制定本办法。

第二条 本办法所称科学数据主要包括在自然科学、工程技术科学等领域，通过基础研究、应用研究、试验开发等产生的数据，以及通过观测监测、考察调查、检验检测等方式取得并用于科学研究活动的原始数据及其衍生数据。

第三条 政府预算资金支持开展的科学数据采集生产、加工整理、开放共享和管理使用等活动适用本办法。

任何单位和个人在中华人民共和国境内从事科学数据相关活动，符合本办法规定情形的，按照本办法执行。

第四条 科学数据管理遵循分级管理、安全可控、充分利用的原则，明确责任主体，加强能力建设，促进开放共享。

第五条 任何单位和个人从事科学数据采集生产、使用、管理活动应当遵守国家有关法律法规及部门规章，不得利用科学数据从事危害国家安全、社会公共利益和他人合法权益的活动。

第二章 职 责

第六条 科学数据管理工作实行国家统筹、各部门与各地区分工负责的体制。

第七条 国务院科学技术行政部门牵头负责全国科学数据的宏观管理与综合协调，主要职责是：

- 1、组织研究制定国家科学数据管理政策和标准规范；
- 2、协调推动科学数据规范管理、开放共享及评价考核工作；
- 3、统筹推进国家科学数据中心建设和发展；
- 4、负责国家科学数据网络管理平台建设和数据维护。

第八条 国务院相关部门、省级人民政府相关部门（以下统称主管部门）在科学数据管理方面的主要职责是：

- 1、负责建立健全本部门（本地区）科学数据管理政策和规章制度，宣传贯彻落实国家科学数据管理政策；
- 2、指导所属法人单位加强和规范科学数据管理；
- 3、按照国家有关规定做好或者授权有关单位做好科学数据定密工作；
- 4、统筹规划和建设本部门（本地区）科学数据中心，推动科学数据开放共享；
- 5、建立完善有效的激励机制，组织开展本部门（本地区）所属法人单位科学数据工作的评价考核。

第九条 有关科研院所、高等院校和企业等法人单位（以下统称法人单位）是科学数据管理的责任主体，主要职责是：

- 1、贯彻落实国家和部门（地方）科学数据管理政策，建立健全本单位科学数据相关管理制度；
- 2、按照有关标准规范进行科学数据采集生产、加工整理和长期保存，确保数据质量；

3、按照有关规定做好科学数据保密和安全管理工

4、建立科学数据管理系统，公布科学数据开放目录并及时更新，积极开展科学数据共享服务；

5、负责科学数据管理运行所需软硬件设施等条件、资金和人员保障。

第十条 科学数据中心是促进科学数据开放共享的重要载体，由主管部门委托有条件的法人单位建立，主要职责是：

1、承担相关领域科学数据的整合汇交工作；

2、负责科学数据的分级分类、加工整理和分析挖掘；

3、保障科学数据安全，依法依规推动科学数据开放共享；

（四）加强国内外科学数据方面交流与合作。

第三章 采集、汇交与保存

第十一条 法人单位及科学数据生产者要按照相关标准规范组织开展科学数据采集生产和加工整理，形成便于使用的数据库或数据集。

法人单位应建立科学数据质量控制体系，保证数据的准确性和可用性。

第十二条 主管部门应建立科学数据汇交制度，在国家统一政务网络和数据共享交换平台的基础上开展本部门（本地区）的科学数据汇交工作。

第十三条 政府预算资金资助的各级科技计划（专项、基金等）项目所形成的科学数据，应由项目牵头单位汇交到相关科学数据中心。接收数据的科学数据中心应出具汇交凭证。

各级科技计划（专项、基金等）管理部门应建立先汇交科学数据、再验收科技计划（专项、基金等）项目的机制；项目/课题验收后产生的科学数据也应进行汇交。

第十四条 主管部门和法人单位应建立健全国内外学术论文数据汇交的管理制度。

利用政府预算资金资助形成的科学数据撰写并在国外学术期刊发表论文时需对外提交相应科学数据的，论文作者应在论文发表前将科学数据上交至所在单位统一管理。

第十五条 社会资金资助形成的涉及国家秘密、国家安全和公共利益的科学数据必须按照有关规定予以汇交。

鼓励社会资金资助形成的其他科学数据向相关科学数据中心汇交。

第十六条 法人单位应建立科学数据保存制度，配备数据存储、管理、服务和安全等必要设施，保障科学数据完整性和安全性。

第十七条 法人单位应加强科学数据人才队伍建设，在岗位设置、绩效收入、职称评定等方面建立激励机制。

第十八条 国务院科学技术行政部门应加强统筹布局，在条件好、资源优势明显的科学数据中心基础上，优化整合形成国家科学数据中心。

第四章 共享与利用

第十九条 政府预算资金资助形成的科学数据应当按照开放为常态、不开放为例外的原则，由主管部门组织编制科学数据资源目录，有关目录和数据应及时接入国家数据共享交换平台，面向社会和相关部门开放共享，畅通科学数据军民共享渠道。国家法律法规有特殊规定的除外。

第二十条 法人单位要对科学数据进行分级分类，明确科学数据的密级和保密期限、开放条件、开放对象和审核程序等，按要求公布科学数据开放目录，通过在线下载、离线共享或定制服务等方式向社会开放共享。

第二十一条 法人单位应根据需求，对科学数据进行分析挖掘，形成有价值的科学数据产品，开展增值服务。鼓励社会组织和企业开展市场化增值服务。

第二十二条 主管部门和法人单位应积极推动科学数据出版和传播工作，支持科研人员整理发表产权清晰、准确完整、共享价值高的科学数据。

第二十三条 科学数据使用者应遵守知识产权相关规定，在论文发表、专利

申请、专著出版等工作中注明所使用和参考引用的科学数据。

第二十四条 对于政府决策、公共安全、国防建设、环境保护、防灾减灾、公益性科学研究等需要使用科学数据的，法人单位应当无偿提供；确需收费的，应按照规定程序和非营利原则制定合理的收费标准，向社会公布并接受监督。

对于因经营性活动需要使用科学数据的，当事人双方应当签订有偿服务合同，明确双方的权利和义务。

国家法律法规有特殊规定的，遵从其规定。

第五章 保密与安全

第二十五条 涉及国家秘密、国家安全、社会公共利益、商业秘密和个人隐私的科学数据，不得对外开放共享；确需对外开放的，要对利用目的、用户资质、保密条件等进行审查，并严格控制知悉范围。

第二十六条 涉及国家秘密的科学数据的采集生产、加工整理、管理和使用，按照国家有关保密规定执行。主管部门和法人单位应建立健全涉及国家秘密的科学数据管理与使用制度，对制作、审核、登记、拷贝、传输、销毁等环节进行严格管理。

对外交往与合作中需要提供涉及国家秘密的科学数据的，法人单位应明确提出利用数据的类别、范围及用途，按照保密管理规定程序报主管部门批准。经主管部门批准后，法人单位按规定办理相关手续并与用户签订保密协议。

第二十七条 主管部门和法人单位应加强科学数据全生命周期安全管理，制定科学数据安全保护措施；加强数据下载的认知、授权等防护管理，防止数据被恶意使用。

对于需对外公布的科学数据开放目录或需对外提供的科学数据，主管部门和法人单位应建立相应的安全保密审查制度。

第二十八条 法人单位和科学数据中心应按照国家网络安全管理规定，建立网络安全保障体系，采用安全可靠的产品和服务，完善数据管控、属性管理、身份识别、行为追溯、黑名单等管理措施，健全防篡改、防泄露、防攻击、防病毒

等安全防护体系。

第二十九条 科学数据中心应建立应急管理和容灾备份机制，按照要求建立应急管理系统，对重要的科学数据进行异地备份。

第六章 附 则

第三十条 主管部门和法人单位应建立完善科学数据管理和开放共享工作评价考核制度。

第三十一条 对于伪造数据、侵犯知识产权、不按规定汇交数据等行为，主管部门可视情节轻重对相关单位和责任人给予责令整改、通报批评、处分等处理或依法给予行政处罚。

对违反国家有关法律法规的单位和个人，依法追究相应责任。

第三十二条 主管部门可参照本办法，制定具体实施细则。涉及国防领域的科学数据管理制度，由有关部门另行规定。

第三十三条 本办法自印发之日起施行。

(八) 国务院办公厅关于印发国家政务信息化项目建设管理办法的通知

(国办发〔2019〕57号)

各省、自治区、直辖市人民政府，国务院各部委、各直属机构：

《国家政务信息化项目建设管理办法》已经国务院同意，现印发给你们，请认真贯彻执行。

国务院办公厅

2019年12月30日

国家政务信息化项目建设管理办法

第一章 总 则

第一条 为规范国家政务信息化建设管理，推动政务信息系统跨部门跨层级互联互通、信息共享和业务协同，强化政务信息系统应用绩效考核，根据《国务院关于印发政务信息资源共享管理暂行办法的通知》（国发〔2016〕51号）等有关规定，制定本办法。

第二条 本办法适用的国家政务信息系统主要包括：国务院有关部门和单位负责实施的国家统一电子政务网络平台、国家重点业务信息系统、国家信息资源库、国家信息安全基础设施、国家电子政务基础设施（数据中心、机房等）、国家电子政务标准化体系以及相关支撑体系等符合《政务信息系统定义和范围》规定的系统。

第三条 国家政务信息化建设管理应当坚持统筹规划、共建共享、业务协同、安全可靠的原则。

第四条 国家发展改革委负责牵头编制国家政务信息化建设规划，对各部门审批的国家政务信息化项目进行备案管理。财政部负责国家政务信息化项目预算管理和政府采购管理。各有关部门按照职责分工，负责国家政务信息化项目审批、

建设、运行和安全监管等相关工作，并按照“以统为主、统分结合、注重实效”的要求，加强对政务信息化项目的并联管理。

第五条 国家发展改革委会同中央网信办、国务院办公厅、财政部建立国家政务信息化建设管理的协商机制，做好统筹协调，开展督促检查和评估评价，推广经验成果，形成工作合力。

第二章 规划和审批管理

第六条 国家发展改革委会同有关部门根据信息化发展规律和政务信息化建设特点，统筹考虑并充分论证各部门建设需求，编制国家政务信息化建设规划并报国务院批准后实施；如内外部发展环境发生重大变化，适时组织评估论证，提出调整意见报国务院批准。各有关部门编制规划涉及政务信息化建设的，应当与国家政务信息化建设规划进行衔接。

第七条 国家发展改革委审批或者核报国务院审批的政务信息化项目，以及其他有关部门按照项目审批管理的政务信息化项目，原则上包括编报项目建议书、可行性研究报告、初步设计方案等环节。

对于已经纳入国家政务信息化建设规划的项目，可以直接编报可行性研究报告。

对于党中央、国务院有明确要求，或者涉及国家重大战略、国家安全等特殊原因，情况紧急，且前期工作深度达到规定要求的项目，可以直接编报项目可行性研究报告、初步设计方案和投资概算。

第八条 国家政务信息化项目原则上不再进行节能评估、规划选址、用地预审、环境影响评价等审批，涉及新建土建工程、高耗能项目的除外。

第九条 除国家发展改革委审批或者核报国务院审批的外，其他有关部门自行审批新建、改建、扩建，以及通过政府购买服务方式产生的国家政务信息化项目，应当按规定履行审批程序并向国家发展改革委备案。

备案文件应当包括项目名称、建设单位、审批部门、绩效目标及绩效指标、投资额度、运行维护经费、经费渠道、信息资源目录、信息共享开放、应用系统、

等级保护或者分级保护备案情况、密码应用方案和密码应用安全性评估报告等内容，其中改建、扩建项目还需提交前期项目第三方后评价报告。

第十条 跨部门共建共享的政务信息化项目，由牵头部门会同参建部门共同开展跨部门工程框架设计，形成统一框架方案后联合报国家发展改革委。框架方案要确定工程的参建部门、建设目标、主体内容，明确各部门项目与总体工程的业务流、数据流及系统接口，初步形成数据目录，确保各部门建设内容无重复交叉，实现共建共享要求。框架方案确定后，各部门按照项目管理要求申请建设本部门参建内容。

各有关部门对于需要地方共享协同的政务信息化项目，应当按照统筹规划、分级审批、分级建设、共享协同的原则建设，并加强与地方已有项目的衔接。项目建设单位应当加强对地方的指导，统筹制定信息共享、业务协同的总体要求和标准规范。地方项目建设单位应当根据项目的总体目标、整体框架、建设任务、绩效目标及指标等，按照本地有关规定开展项目审批建设工作，并做好与国家有关项目建设单位的衔接配合。

第十一条 可行性研究报告、初步设计方案应当包括信息资源共享分析篇（章）。咨询评估单位的评估报告应当包括对信息资源共享分析篇（章）的评估意见。审批部门的批复文件或者上报国务院的请示文件应当包括对信息资源共享分析篇（章）的意见。

项目建设单位应当编制信息资源目录，建立信息共享长效机制和共享信息使用情况反馈机制，确保信息资源共享，不得将应当普遍共享的数据仅向特定企业、社会组织开放。

信息资源目录是审批政务信息化项目的必备条件。信息共享的范围、程度以及网络安全情况是确定项目建设投资、运行维护经费和验收的重要依据。

第十二条 各部门所有新建政务信息化项目，均应当在全国投资项目在线审批监管平台政务信息化项目管理子平台（以下简称管理平台）报批或者备案。

所有中央本级政务信息系统应当全口径纳入管理平台进行统一管理。各部门应当在管理平台及时更新本部门政务信息系统目录。管理平台汇总形成国家政务

信息系统总目录。

第三章 建设和资金管理

第十三条 项目建设单位应当确定项目实施机构和项目责任人，建立健全项目管理制度，加强对项目全过程的统筹协调，强化信息共享和业务协同，并严格执行招标投标、政府采购、工程监理、合同管理等制度。招标采购涉密信息系统的，还应当执行保密有关法律法规规定。

第十四条 项目建设单位应当按照《中华人民共和国网络安全法》等法律法规以及党政机关安全管理等有关规定，建立网络安全管理制度，采取技术措施，加强政务信息系统与信息资源的安全保密设施建设，定期开展网络安全检测与风险评估，保障信息系统安全稳定运行。

第十五条 项目建设单位应当落实国家密码管理有关法律法规和标准规范的要求，同步规划、同步建设、同步运行密码保障系统并定期进行评估。

第十六条 项目应当采用安全可靠的软硬件产品。在项目报批阶段，要对产品的安全可靠情况进行说明。项目软硬件产品的安全可靠情况，项目密码应用和安全审查情况，以及硬件设备和新建数据中心能源利用效率情况是项目验收的重要内容。

第十七条 项目建设单位应当充分依托云服务资源开展集约化建设。

第十八条 对于人均投资规模过大、项目建设单位不具备建设运行维护能力的项目，应当充分发挥职能部门作用或者外包，减少自建自管自用自维。

第十九条 国家政务信息化项目实行工程监理制，项目建设单位应当按照信息系统工程监理有关规定，委托工程监理单位对项目建设进行工程监理。

第二十条 项目建设单位应当对项目绩效目标执行情况进行评价，并征求有关项目使用单位和监理单位的意见，形成项目绩效评价报告，在建设期内每年年底前向项目审批部门提交。

项目绩效评价报告主要包括建设进度和投资计划执行情况。对于已投入试运行的系统，还应当说明试运行效果及遇到的问题等。

第二十一条 项目建设过程中出现工程严重逾期、投资重大损失等问题的，项目建设单位应当及时向项目审批部门报告，项目审批部门按照有关规定要求项目建设单位进行整改或者暂停项目建设。

第二十二条 项目建设单位应当严格按照项目审批部门批复的初步设计方案和投资概算实施项目建设。项目建设目标和内容不变，项目总投资有结余的，应当按照相关规定将结余资金退回。

项目建设的资金支出按照国库集中支付有关制度规定执行。

第二十三条 项目投资规模未超出概算批复、建设目标不变，项目主要内容确需调整且资金调整数额不超过概算总投资15%，并符合下列情形之一的，可以由项目建设单位调整，同时向项目审批部门备案：

- 1、根据党中央、国务院部署，确需改变建设内容的；
- 2、确需对原项目技术方案进行完善优化的；
- 3、根据所建政务信息化项目业务发展需要，在已批复项目建设规划的框架下调整相关建设内容及进度的。

不符合上述情形的，应当按照国家有关规定履行相应手续。

第二十四条 初步设计方案和投资概算未获批复前，原则上不予下达项目投资。对于因开展需求分析、编制可行性研究报告和初步设计、购地、拆迁等确需提前安排投资的政务信息化项目，项目建设单位可以在项目可行性研究报告获批复后，向项目审批部门提出申请。

第二十五条 国家政务信息化项目建成后半年内，项目建设单位应当按照国家有关规定申请审批部门组织验收，提交验收申请报告时应当一并附上项目建设总结、财务报告、审计报告、安全风险评估报告（包括涉密信息系统安全保密测评报告或者非涉密信息系统网络安全等级保护测评报告等）、密码应用安全性评估报告等材料。

项目建设单位不能按期申请验收的，应当向项目审批部门提出延期验收申请。

项目审批部门应当及时组织验收。验收完成后，项目建设单位应当将验收报告等材料报项目审批部门备案。

第二十六条 项目建设单位应当按照国家有关档案管理的规定，做好项目档案管理，并探索应用电子档案。

未进行档案验收或者档案验收不合格的，不得通过项目验收。

第二十七条 项目建设单位应当在项目通过验收并投入运行后12至24个月内，依据国家政务信息化建设管理绩效评价有关要求，开展自评价，并将自评价报告报送项目审批部门和财政部门。项目审批部门结合项目建设单位自评价情况，可以委托相应的第三方咨询机构开展后评价。

第二十八条 加强国家政务信息化项目建设投资和运行维护经费协同联动，坚持“联网通办是原则，孤网是例外”。部门已建的政务信息化项目需升级改造，或者拟新建政务信息化项目，能够按要求进行信息共享的，由国家发展改革委同有关部门进行审核；如果部门认为根据有关法律法规和党中央、国务院要求不能进行信息共享，但是确有必要建设或者保留的，由国家发展改革委报国务院，由国务院办公厅会同有关部门进行审核，经国务院批准后方可建设或者保留。

（一）对于未按要求共享数据资源或者重复采集数据的政务信息系统，不安排运行维护经费，项目建设单位不得新建、改建、扩建政务信息系统。

（二）对于未纳入国家政务信息系统总目录的系统，不安排运行维护经费。

（三）对于不符合密码应用和网络安全要求，或者存在重大安全隐患的政务信息系统，不安排运行维护经费，项目建设单位不得新建、改建、扩建政务信息系统。

第四章 监督管理

第二十九条 项目建设单位应当接受项目审批部门及有关部门的监督管理，配合做好绩效评价、审计等监督管理工作，如实提供建设项目有关资料 and 情况，不得拒绝、隐匿、瞒报。

第三十条 国务院办公厅、国家发展改革委、财政部、中央网信办会同有关

部门按照职责分工，对国家政务信息化项目是否符合国家有关政务信息共享的要求，以及项目建设中招标采购、资金使用、密码应用、网络安全等情况实施监督管理。发现违反国家有关规定或者批复要求的，应当要求项目建设单位限期整改。逾期不整改或者整改后仍不符合要求的，项目审批部门可以对其进行通报批评、暂缓安排投资计划、暂停项目建设直至终止项目。

网络安全监管部门应当依法加强对国家政务信息系统的安全监管，并指导监督项目建设单位落实网络安全审查制度要求。

各部门应当严格遵守有关保密等法律法规规定，构建全方位、多层次、一致性的防护体系，按要求采用密码技术，并定期开展密码应用安全性评估，确保政务信息系统运行安全和政务信息资源共享交换的数据安全。

第三十一条 审计机关应当依法加强对国家政务信息系统的审计，促进专项资金使用真实、合法和高效，推动完善并监督落实相关制度政策。

第三十二条 项目审批部门、主管部门应当加强对绩效评价和项目后评价结果的应用，根据评价结果对国家政务信息化项目存在的问题提出整改意见，指导完善相关管理制度，并按照项目审批管理要求将评价结果作为下一年度安排政府投资和运行维护经费的重要依据。

第三十三条 单位或者个人违反本办法规定未履行审批、备案程序，或者因管理不善、弄虚作假造成严重超概算、质量低劣、损失浪费、安全事故或者其他责任事故的，相关部门应当予以通报批评，并对负有直接责任的主管人员和其他责任人员依法给予处分。

相关部门、单位或者个人违反国家有关规定，截留、挪用政务信息化项目资金，或者违规安排运行维护经费的，由有关部门按照《财政违法行为处罚处分条例》等相关规定予以查处。

第五章 附 则

第三十四条 国务院有关部门可以根据本办法的规定及职责分工，制定本部门的具体管理办法。

各省、自治区、直辖市人民政府可以参照本办法制定本地区的管理办法。

第三十五条 本办法由国家发展改革委同财政部负责解释。

第三十六条 本办法自2020年2月1日起施行。2007年8月13日国家发展改革委公布的《国家电子政务工程建设项目管理暂行办法》同时废止。

(九) 关键信息基础设施安全保护条例

中华人民共和国国务院令（第745号）

《关键信息基础设施安全保护条例》已经2021年4月27日国务院第133次常务会议通过，现予公布，自2021年9月1日起施行。

总理 李克强

2021年7月30日

第一章 总 则

第一条 为了保障关键信息基础设施安全，维护网络安全，根据《中华人民共和国网络安全法》，制定本条例。

第二条 本条例所称关键信息基础设施，是指公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域的，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统等。

第三条 在国家网信部门统筹协调下，国务院公安部门负责指导监督关键信息基础设施安全保护工作。国务院电信主管部门和其他有关部门依照本条例和有关法律、行政法规的规定，在各自职责范围内负责关键信息基础设施安全保护和监督管理工作。

省级人民政府有关部门依据各自职责对关键信息基础设施实施安全保护和监督管理。

第四条 关键信息基础设施安全保护坚持综合协调、分工负责、依法保护，强化和落实关键信息基础设施运营者（以下简称运营者）主体责任，充分发挥政府及社会各方面的作用，共同保护关键信息基础设施安全。

第五条 国家对关键信息基础设施实行重点保护，采取措施，监测、防御、处置来源于中华人民共和国境内外的网络安全风险和威胁，保护关键信息基础设施免受攻击、侵入、干扰和破坏，依法惩治危害关键信息基础设施安全的违法犯

罪活动。

任何个人和组织不得实施非法侵入、干扰、破坏关键信息基础设施的活动，不得危害关键信息基础设施安全。

第六条 运营者依照本条例和有关法律、行政法规的规定以及国家标准的强制性要求，在网络安全等级保护的基础上，采取技术保护措施和其他必要措施，应对网络安全事件，防范网络攻击和违法犯罪活动，保障关键信息基础设施安全稳定运行，维护数据的完整性、保密性和可用性。

第七条 对在关键信息基础设施安全保护工作中取得显著成绩或者作出突出贡献的单位和个人，按照国家有关规定给予表彰。

第二章 关键信息基础设施认定

第八条 本条例第二条涉及的重要行业和领域的主管部门、监督管理部门是负责关键信息基础设施安全保护工作的部门（以下简称保护工作部门）。

第九条 保护工作部门结合本行业、本领域实际，制定关键信息基础设施认定规则，并报国务院公安部门备案。

制定认定规则应当主要考虑下列因素：

- 1、网络设施、信息系统等对于本行业、本领域关键核心业务的重要程度；
- 2、网络设施、信息系统等一旦遭到破坏、丧失功能或者数据泄露可能带来的危害程度；
- 3、对其他行业和领域的关联性影响。

第十条 保护工作部门根据认定规则负责组织认定本行业、本领域的关键信息基础设施，及时将认定结果通知运营者，并通报国务院公安部门。

第十一条 关键信息基础设施发生较大变化，可能影响其认定结果的，运营者应当及时将相关情况报告保护工作部门。保护工作部门自收到报告之日起3个月内完成重新认定，将认定结果通知运营者，并通报国务院公安部门。

第三章 运营者责任义务

第十二条 安全保护措施应当与关键信息基础设施同步规划、同步建设、同步使用。

第十三条 运营者应当建立健全网络安全保护制度和责任制，保障人力、财力、物力投入。运营者的主要负责人对关键信息基础设施安全保护负总责，领导关键信息基础设施安全保护和重大网络安全事件处置工作，组织研究解决重大网络安全问题。

第十四条 运营者应当设置专门安全管理机构，并对专门安全管理机构负责人和关键岗位人员进行安全背景审查。审查时，公安机关、国家安全机关应当予以协助。

第十五条 专门安全管理机构具体负责本单位的关键信息基础设施安全保护工作，履行下列职责：

- 1、建立健全网络安全管理、评价考核制度，拟订关键信息基础设施安全保护计划；
- 2、组织推动网络安全防护能力建设，开展网络安全监测、检测和风险评估；
- 3、按照国家及行业网络安全事件应急预案，制定本单位应急预案，定期开展应急演练，处置网络安全事件；
- 4、认定网络安全关键岗位，组织开展网络安全工作考核，提出奖励和惩处建议；
- 5、组织网络安全教育、培训；
- 6、履行个人信息和数据安全保护责任，建立健全个人信息和数据安全保护制度；
- 7、对关键信息基础设施设计、建设、运行、维护等服务实施安全管理；
- 8、按照规定报告网络安全事件和重要事项。

第十六条 运营者应当保障专门安全管理机构的运行经费、配备相应的人员，开展与网络安全和信息化有关的决策应当有专门安全管理机构人员参与。

第十七条 运营者应当自行或者委托网络安全服务机构对关键信息基础设施每年至少进行一次网络安全检测和风险评估，对发现的安全问题及时整改，并按照保护工作部门要求报送情况。

第十八条 关键信息基础设施发生重大网络安全事件或者发现重大网络安全威胁时，运营者应当按照有关规定向保护工作部门、公安机关报告。

发生关键信息基础设施整体中断运行或者主要功能故障、国家基础信息以及其他重要数据泄露、较大规模个人信息泄露、造成较大经济损失、违法信息较大范围传播等特别重大网络安全事件或者发现特别重大网络安全威胁时，保护工作部门应当在收到报告后，及时向国家网信部门、国务院公安部门报告。

第十九条 运营者应当优先采购安全可信的网络产品和服务；采购网络产品和服务可能影响国家安全的，应当按照国家网络安全规定通过安全审查。

第二十条 运营者采购网络产品和服务，应当按照国家有关规定与网络产品和服务提供者签订安全保密协议，明确提供者的技术支持和安全保密义务与责任，并对义务与责任履行情况进行监督。

第二十一条 运营者发生合并、分立、解散等情况，应当及时报告保护工作部门，并按照保护工作部门的要求对关键信息基础设施进行处置，确保安全。

第四章 保障和促进

第二十二条 保护工作部门应当制定本行业、本领域关键信息基础设施安全规划，明确保护目标、基本要求、工作任务、具体措施。

第二十三条 国家网信部门统筹协调有关部门建立网络安全信息共享机制，及时汇总、研判、共享、发布网络安全威胁、漏洞、事件等信息，促进有关部门、保护工作部门、运营者以及网络安全服务机构等之间的网络安全信息共享。

第二十四条 保护工作部门应当建立健全本行业、本领域的关键信息基础设施网络安全监测预警制度，及时掌握本行业、本领域关键信息基础设施运行状况、安全态势，预警通报网络安全威胁和隐患，指导做好安全防范工作。

第二十五条 保护工作部门应当按照国家网络安全事件应急预案的要求，建

立健全本行业、本领域的网络安全事件应急预案，定期组织应急演练；指导运营者做好网络安全事件应对处置，并根据需要组织提供技术支持与协助。

第二十六条 保护工作部门应当定期组织开展本行业、本领域关键信息基础设施网络安全检查检测，指导监督运营者及时整改安全隐患、完善安全措施。

第二十七条 国家网信部门统筹协调国务院公安部门、保护工作部门对关键信息基础设施进行网络安全检查检测，提出改进措施。

有关部门在开展关键信息基础设施网络安全检查时，应当加强协同配合、信息沟通，避免不必要的检查和交叉重复检查。检查工作不得收取费用，不得要求被检查单位购买指定品牌或者指定生产、销售单位的产品和服务。

第二十八条 运营者对保护工作部门开展的关键信息基础设施网络安全检查检测工作，以及公安、国家安全、保密行政管理、密码管理等有关部门依法开展的关键信息基础设施网络安全检查工作应当予以配合。

第二十九条 在关键信息基础设施安全保护工作中，国家网信部门和国务院电信主管部门、国务院公安部门等应当根据保护工作部门的需要，及时提供技术支持和协助。

第三十条 网信部门、公安机关、保护工作部门等有关部门，网络安全服务机构及其工作人员对于在关键信息基础设施安全保护工作中获取的信息，只能用于维护网络安全，并严格按照有关法律、行政法规的要求确保信息安全，不得泄露、出售或者非法向他人提供。

第三十一条 未经国家网信部门、国务院公安部门批准或者保护工作部门、运营者授权，任何个人和组织不得对关键信息基础设施实施漏洞探测、渗透性测试等可能影响或者危害关键信息基础设施安全的活动。对基础电信网络实施漏洞探测、渗透性测试等活动，应当事先向国务院电信主管部门报告。

第三十二条 国家采取措施，优先保障能源、电信等关键信息基础设施安全运行。

能源、电信行业应当采取措施，为其他行业和领域的关键信息基础设施安全

运行提供重点保障。

第三十三条 公安机关、国家安全机关依据各自职责依法加强关键信息基础设施安全保卫，防范打击针对和利用关键信息基础设施实施的违法犯罪活动。

第三十四条 国家制定和完善关键信息基础设施安全标准，指导、规范关键信息基础设施安全保护工作。

第三十五条 国家采取措施，鼓励网络安全专门人才从事关键信息基础设施安全保护工作；将运营者安全管理人员、安全技术人员培训纳入国家继续教育体系。

第三十六条 国家支持关键信息基础设施安全防护技术创新和产业发展，组织力量实施关键信息基础设施安全技术攻关。

第三十七条 国家加强网络安全服务机构建设和管理，制定管理要求并加强监督指导，不断提升服务机构能力水平，充分发挥其在关键信息基础设施安全保护中的作用。

第三十八条 国家加强网络安全军民融合，军地协同保护关键信息基础设施安全。

第五章 法律责任

第三十九条 运营者有下列情形之一的，由有关主管部门依据职责责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处10万元以上100万元以下罚款，对直接负责的主管人员处1万元以上10万元以下罚款：

- 1、在关键信息基础设施发生较大变化，可能影响其认定结果时未及时将相关情况报告保护工作部门的；
- 2、安全保护措施未与关键信息基础设施同步规划、同步建设、同步使用的；
- 3、未建立健全网络安全保护制度和责任制的；
- 4、未设置专门安全管理机构的；
- 5、未对专门安全管理机构负责人和关键岗位人员进行安全背景审查的；

6、开展与网络安全和信息化有关的决策没有专门安全管理机构人员参与的；

7、专门安全管理机构未履行本条例第十五条规定的职责的；

8、未对关键信息基础设施每年至少进行一次网络安全检测和风险评估，未对发现的安全问题及时整改，或者未按照保护工作部门要求报送情况的；

9、采购网络产品和服务，未按照国家有关规定与网络产品和服务提供者签订安全保密协议的；

10、发生合并、分立、解散等情况，未及时报告保护工作部门，或者未按照保护工作部门的要求对关键信息基础设施进行处置的。

第四十条 运营者在关键信息基础设施发生重大网络安全事件或者发现重大网络安全威胁时，未按照有关规定向保护工作部门、公安机关报告的，由保护工作部门、公安机关依据职责责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处10万元以上100万元以下罚款，对直接负责的主管人员处1万元以上10万元以下罚款。

第四十一条 运营者采购可能影响国家安全的网络产品和服务，未按照国家网络安全规定进行安全审查的，由国家网信部门等有关主管部门依据职责责令改正，处采购金额1倍以上10倍以下罚款，对直接负责的主管人员和其他直接责任人员处1万元以上10万元以下罚款。

第四十二条 运营者对保护工作部门开展的关键信息基础设施网络安全检查检测工作，以及公安、国家安全、保密行政管理、密码管理等有关部门依法开展的关键信息基础设施网络安全检查工作不予配合的，由有关主管部门责令改正；拒不改正的，处5万元以上50万元以下罚款，对直接负责的主管人员和其他直接责任人员处1万元以上10万元以下罚款；情节严重的，依法追究相应法律责任。

第四十三条 实施非法侵入、干扰、破坏关键信息基础设施，危害其安全的活动尚不构成犯罪的，依照《中华人民共和国网络安全法》有关规定，由公安机关没收违法所得，处5日以下拘留，可以并处5万元以上50万元以下罚款；情节较

重的，处5日以上15日以下拘留，可以并处10万元以上100万元以下罚款。

单位有前款行为的，由公安机关没收违法所得，处10万元以上100万元以下罚款，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。

违反本条例第五条第二款和第三十一条规定，受到治安管理处罚的人员，5年内不得从事网络安全管理和网络运营关键岗位的工作；受到刑事处罚的人员，终身不得从事网络安全管理和网络运营关键岗位的工作。

第四十四条 网信部门、公安机关、保护工作部门和其他有关部门及其工作人员未履行关键信息基础设施安全保护和监督管理职责或者玩忽职守、滥用职权、徇私舞弊的，依法对直接负责的主管人员和其他直接责任人员给予处分。

第四十五条 公安机关、保护工作部门和其他有关部门在开展关键信息基础设施网络安全检查工作中收取费用，或者要求被检查单位购买指定品牌或者指定生产、销售单位的产品和服务的，由其上级机关责令改正，退还收取的费用；情节严重的，依法对直接负责的主管人员和其他直接责任人员给予处分。

第四十六条 网信部门、公安机关、保护工作部门等有关部门、网络安全服务机构及其工作人员将在关键信息基础设施安全保护工作中获取的信息用于其他用途，或者泄露、出售、非法向他人提供的，依法对直接负责的主管人员和其他直接责任人员给予处分。

第四十七条 关键信息基础设施发生重大和特别重大网络安全事件，经调查确定为责任事故的，除应当查明运营者责任并依法予以追究外，还应查明相关网络安全服务机构及有关部门的责任，对有失职、渎职及其他违法行为的，依法追究责任。

第四十八条 电子政务关键信息基础设施的运营者不履行本条例规定的网络安全保护义务的，依照《中华人民共和国网络安全法》有关规定予以处理。

第四十九条 违反本条例规定，给他人造成损害的，依法承担民事责任。

违反本条例规定，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。

第六章 附 则

第五十条 存储、处理涉及国家秘密信息的关键信息基础设施的安全保护，还应当遵守保密法律、行政法规的规定。

关键信息基础设施中的密码使用和管理，还应当遵守相关法律、行政法规的规定。

第五十一条 本条例自2021年9月1日起施行。

三、司法解释

（一）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 法释〔2017〕10号）

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”：

- 1、出售或者提供行踪轨迹信息，被他人用于犯罪的；
- 2、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；
- 3、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；
- 4、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；
- 5、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；
- 6、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；
- 7、违法所得五千元以上的；
- 8、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；
- 9、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；
- 10、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”：

- 1、造成被害人死亡、重伤、精神失常或者被绑架等严重后果的；
- 2、造成重大经济损失或者恶劣社会影响的；
- 3、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；

4、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”：

1、利用非法购买、收受的公民个人信息获利五万元以上的；

2、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；

3、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，不起诉或者免于刑事处罚；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。

（二）最高人民法院关于审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的规定

（2014年6月23日最高人民法院审判委员会第1621次会议通过，根据2020年12月23日最高人民法院审判委员会第1823次会议通过的《最高人民法院关于修改〈最高人民法院关于在民事审判工作中适用《中华人民共和国工会法》若干问题的解释〉等二十七件民事类司法解释的决定》修正）

为正确审理利用信息网络侵害人身权益民事纠纷案件，根据《中华人民共和国民法典》《全国人民代表大会常务委员会关于加强网络信息保护的決定》《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 本规定所称的利用信息网络侵害人身权益民事纠纷案件，是指利用信息网络侵害他人姓名权、名称权、名誉权、荣誉权、肖像权、隐私权等人身权益引起的纠纷案件。

第二条 原告依据民法典第一千一百九十五条、第一千一百九十七条的规定起诉网络用户或者网络服务提供者的，人民法院应予受理。

原告仅起诉网络用户，网络用户请求追加涉嫌侵权的网络服务提供者作为共同被告或者第三人的，人民法院应予准许。

原告仅起诉网络服务提供者，网络服务提供者请求追加可以确定的网络用户为共同被告或者第三人的，人民法院应予准许。

第三条 原告起诉网络服务提供者，网络服务提供者以涉嫌侵权的信息系网络用户发布为由抗辩的，人民法院可以根据原告的请求及案件的具体情况，责令网络服务提供者向人民法院提供能够确定涉嫌侵权的网络用户的姓名（名称）、联系方式、网络地址等信息。

网络服务提供者无正当理由拒不提供的，人民法院可以依据民事诉讼法第一百一十四条的规定对网络服务提供者采取处罚等措施。

原告根据网络服务提供者提供的信息请求追加网络用户为被告的，人民法院

应予准许。

第四条 人民法院适用民法典第一千一百九十五条第二款的规定，认定网络服务提供者采取的删除、屏蔽、断开链接等必要措施是否及时，应当根据网络服务的类型和性质、有效通知的形式和准确程度、网络信息侵害权益的类型和程度等因素综合判断。

第五条 其发布的信息被采取删除、屏蔽、断开链接等措施的网络用户，主张网络服务提供者承担违约责任或者侵权责任，网络服务提供者以收到民法典第一千一百九十五条第一款规定的有效通知为由抗辩的，人民法院应予支持。

第六条 人民法院依据民法典第一千一百九十七条认定网络服务提供者是否“知道或者应当知道”，应当综合考虑下列因素：

- 1、网络服务提供者是否以人工或者自动方式对侵权网络信息以推荐、排名、选择、编辑、整理、修改等方式作出处理；
- 2、网络服务提供者应当具备的管理信息的能力，以及所提供服务的性质、方式及其引发侵权的可能性大小；
- 3、该网络信息侵害人身权益的类型及明显程度；
- 4、该网络信息的社会影响程度或者一定时间内的浏览量；
- 5、（五）网络服务提供者采取预防侵权措施的技术可能性及其是否采取了相应的合理措施；
- 6、网络服务提供者是否针对同一网络用户的重复侵权行为或者同一侵权信息采取了相应的合理措施；
- 7、与本案相关的其他因素。

第七条 人民法院认定网络用户或者网络服务提供者转载网络信息行为的过错及其程度，应当综合以下因素：

- 1、转载主体所承担的与其性质、影响范围相适应的注意义务；
- 2、所转载信息侵害他人人身权益的明显程度；

3、对所转载信息是否作出实质性修改，是否添加或者修改文章标题，导致其与内容严重不符以及误导公众的可能性。

第八条 网络用户或者网络服务提供者采取诽谤、诋毁等手段，损害公众对经营主体的信赖，降低其产品或者服务的社会评价，经营主体请求网络用户或者网络服务提供者承担侵权责任的，人民法院应依法予以支持。

第九条 网络用户或者网络服务提供者，根据国家机关依职权制作的文书和公开实施的职权行为等信息来源所发布的信息，有下列情形之一的，侵害他人人身权益，被侵权人请求侵权人承担侵权责任的，人民法院应予支持：

1、网络用户或者网络服务提供者发布的信息与前述信息来源内容不符；

2、网络用户或者网络服务提供者以添加侮辱性内容、诽谤性信息、不当标题或者通过增删信息、调整结构、改变顺序等方式致人误解；

3、前述信息来源已被公开更正，但网络用户拒绝更正或者网络服务提供者不予更正；

4、前述信息来源已被公开更正，网络用户或者网络服务提供者仍然发布更正之前的信息。

第十条 被侵权人与构成侵权的网络用户或者网络服务提供者达成一方支付报酬，另一方提供删除、屏蔽、断开链接等服务的协议，人民法院应认定为无效。

擅自篡改、删除、屏蔽特定网络信息或者以断开链接的方式阻止他人获取网络信息，发布该信息的网络用户或者网络服务提供者请求侵权人承担侵权责任的，人民法院应予支持。接受他人委托实施该行为的，委托人与受托人承担连带责任。

第十一条 网络用户或者网络服务提供者侵害他人人身权益，造成财产损失或者严重精神损害，被侵权人依据民法典第一千一百八十二条和第一千一百八十三条的规定，请求其承担赔偿责任的，人民法院应予支持。

第十二条 被侵权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。合理开支包括被侵权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，可以将符合国家有关部门规定的律师费用计算在赔偿范围内。

被侵权人因人身权益受侵害造成的财产损失以及侵权人因此获得的利益难以确定的，人民法院可以根据具体案情在50万元以下的范围内确定赔偿数额。

第十三条 本规定施行后人民法院正在审理的一审、二审案件适用本规定。

本规定施行前已经终审，本规定施行后当事人申请再审或者按照审判监督程序决定再审的案件，不适用本规定。

(三) 最高人民法院关于人民法院在线办理案件若干问题的规定 (征求意见稿)

为推进和规范人民法院在线办理案件，完善在线诉讼程序规则，依法保障当事人及其他诉讼参与人诉讼权利，确保公正高效审理案件，根据《中华人民共和国民事诉讼法》《中华人民共和国行政诉讼法》《中华人民共和国刑事诉讼法》等有关法律规定，结合审判实践，制定本规定。

第一条【在线诉讼涵义及效力】在线诉讼是指人民法院、当事人及其他诉讼参与人依托电子诉讼平台，通过互联网在线完成案件的起诉、受理、送达、调解、证据交换、询问、听证、庭审、宣判、执行等全部或者部分诉讼环节的诉讼形式。诉讼主体的在线诉讼活动，与线下诉讼活动具有同等效力。

人民法院应当建设电子诉讼平台（以下简称“诉讼平台”），作为开展在线诉讼的专用平台。

第二条【在线诉讼适用范围】人民法院可以综合考虑案件情况、当事人意愿和技术条件，决定在线办理以下案件：

- 1、民事、行政诉讼案件；
- 2、民事特别程序、督促程序案件；
- 3、民事执行、行政执行、刑事附带民事执行案件。

上述案件在线下办理的，当事人可以主动申请适用在线诉讼。

第三条【在线诉讼适用条件】人民法院开展在线诉讼，应当向当事人告知案件在线办理的具体环节、主要形式、权利义务和法律后果，并在立案和审理前准备阶段征得当事人同意。当事人在第一审程序中已同意适用在线诉讼，人民法院决定在第二审程序、审判监督程序或者执行程序中继续适用在线诉讼的，应当另行征得当事人同意。

对老年人群体适用在线诉讼，人民法院应当充分尊重老年人意愿，细化说明告知事项，优化设置平台功能，降低在线诉讼难度，引导帮助老年人熟悉、掌握在线诉讼操作流程，为老年人群体参与在线诉讼提供全方位司法便利。

第四条【同意适用在线诉讼的效力和范围】当事人已同意适用在线诉讼，但无正当理由不参与在线诉讼活动的，视为放弃相应诉讼权利或者不履行相应诉讼义务。

当事人已同意适用在线诉讼，但因存在个人意愿变化、欠缺在线诉讼能力、不具备在线诉讼条件或者认为不宜全程在线诉讼等情形，提出相应诉讼环节转为线下进行的，应当在人民法院在线开展相应诉讼环节5日前提出申请，经人民法院审查同意的，相应诉讼环节转为线下进行。已经完成的在线诉讼活动具有法律效力。

当事人明确表示不同意对自身参与的全部或者部分诉讼环节适用在线诉讼的，人民法院针对该方当事人的全部或者部分诉讼活动应当在线下完成。

一方当事人不同意对调解、证据交换、询问、听证、庭审、宣判等需要各方当事人共同参与的诉讼环节适用在线诉讼，要求各方当事人均在线下完成的，应当提出具体理由。人民法院经审查，认为理由正当的，相应诉讼环节可以在线下完成；理由不成立的，相应诉讼环节可以采取同意方当事人线上、不同意方当事人线下的方式完成。

第五条【身份认证】参与在线诉讼的诉讼主体应当先行在诉讼平台完成实名注册，通过证件证照比对、生物特征识别、实名手机号码关联、国家统一身份认证平台认证等方式在线完成身份认证，取得登录诉讼平台的专用账号。

参与在线诉讼的诉讼主体应当妥善保管诉讼平台专用账号和密码，除有相反证据外，使用专用账号登录诉讼平台所作出的行为，视为被认证人本人行为。

人民法院根据案件审理需要，可以对在线调解、证据交换、庭审等多方参与的诉讼环节，采用短信验证、二维码扫描、人脸识别等方式再次验证身份。人民法院认为有必要的，可以要求在线下进一步核实相关诉讼主体身份。

第六条【在线调解】人民法院、特邀调解组织、特邀调解员可以通过诉讼平台、人民法院调解平台等开展在线调解活动。在线调解应当遵循调解保密原则，当事人及其他诉讼参与人、特邀调解主体以及平台建设主体不得录制调解音视频，不得披露、传播调解过程和内容。

第七条【在线立案】当事人采取在线方式提交起诉材料的，人民法院应当自收到材料后七日内，在线作出以下处理：

1、符合起诉条件的，登记立案并送达案件受理通知书、交纳诉讼费用通知书、举证通知书等诉讼文书。

2、提交材料不符合要求的，人民法院应当通过诉讼平台及时要求补正，并一次性告知补正内容和补正期限，案件受理时间自收到补正材料后次日重新起算；原告未在指定期限内按要求补正的，起诉材料作退回处理。

3、不符合起诉条件的，经人民法院释明后，原告坚持继续起诉的，裁定或者决定不予受理、不予立案。

第八条【在线应诉】人民法院受理案件后，决定案件适用在线诉讼的，应当通知被告、被上诉人或者其他诉讼参与人，并征求其是否同意以在线方式参与诉讼。被通知人同意适用在线诉讼的，应当通过诉讼平台验证身份、关联案件、了解案件信息、接收和提交诉讼材料，以及实施其他诉讼行为。

被通知人未在人民法院指定的时间内关联诉讼平台的，视为不同意对其适用在线诉讼，相应诉讼环节应当在线下完成。

第九条【电子材料提交】案件适用在线诉讼的，当事人应当将起诉状、答辩状、反诉状、代理意见、身份证明、营业执照副本、授权委托书等线下诉讼材料，以及书证、物证、鉴定意见等实体证据材料，通过扫描、翻拍、转录等方式作电子化处理后上传至诉讼平台，或者在诉讼平台直接填写录入起诉状、答辩状、反诉状、代理意见等诉讼材料。

当事人的诉讼材料或者证据材料为电子数据，且人民法院诉讼平台与相关平台系统已实现数据对接的，可以将电子数据直接提交至诉讼平台。

当事人同意适用在线诉讼，但提交电子化材料确有困难的，人民法院可以对当事人提交的线下材料作电子化处理后导入诉讼平台。

第十条【电子化材料效力】当事人提交的电子化材料，经人民法院审核通过后，可以直接在诉讼中使用，不再提交原件、原物，但存在下列情形之一的，人民法院应当要求当事人提供原件、原物：

- 1、对方当事人认为电子化材料与原件、原物不一致，并提出合理理由和依据的；
- 2、电子化材料呈现不完整、内容不清晰、格式不规范的；
- 3、人民法院卷宗、档案管理相关规定要求提供原件、原物的；
- 4、根据案件审理需要，人民法院认为有必要提交原件、原物的。

第十一条【电子化材料形式真实性审核】当事人提交的电子化材料，符合下列情形之一的，人民法院可以认定符合原件形式要求：

- 1、对方当事人对电子化材料真实性未提出异议的；
- 2、电子化材料形成过程经过公证机关公证的；
- 3、该电子化材料已在之前诉讼中提交过并经人民法院确认的；
- 4、电子化材料已通过在线或者线下方式与原件、原物比对一致的；
- 5、有其他证据证明电子化材料与原件、原物一致的。

第十二条【在线证据交换方式与效力】人民法院根据案件情况，可以向各方当事人发送在线证据交换通知，通过同步或者非同步的方式在线交换证据。

双方当事人选择同步在线交换证据的，应当在人民法院指定的时间登陆诉讼平台，通过在线视频或者其他方式，对已经导入诉讼平台的电子化证据材料或者线下送达的证据材料副本，集中发表质证意见。

双方当事人选择非同步在线交换证据的，应当在人民法院确定的合理期限内，分别登陆诉讼平台，查看已经导入诉讼平台的电子化证据材料并发表质证意见。

双方当事人对在线证据交换方式无法达成一致意见的，人民法院可以根据案件情况和当事人申请，决定在线证据交换的具体方式。

第十三条【电子证据材料的认定】当事人作为证据提交的电子化材料和电子数据，人民法院应当按照《中华人民共和国民事诉讼法》《中华人民共和国民事诉讼法》《中华人民共和国民事诉讼法》及其司法解释，以及关于诉讼证据的司法解释等相关规定，经当事人举证质证后，依法认定其内容的真实性、关联性和合法性。

第十四条【区块链证据的效力】当事人提交的证据系通过区块链技术存证，并经技术核验后一致的，推定该证据材料上链后未经篡改，人民法院可以确认该证据的真实性，但有相反证据足以推翻的除外。

第十五条【区块链证据审核规则】当事人对区块链存证证据提出异议并有合理理由的，人民法院应当主要审查以下内容：

- 1、存证平台是否符合国家有关部门关于提供区块链存证服务的相关规定；
- 2、当事人与存证平台是否存在利害关系，并利用技术手段不当干预取证、存证过程；
- 3、存证平台的信息系统是否符合清洁性、安全性、可用性的国家标准或者行业标准；
- 4、存证技术和过程是否符合《电子数据存证技术规范》关于系统环境、技术安全、加密方式、数据传输、信息验证等方面的要求。

第十六条【上链前数据的真实性审查】当事人提出数据上链存证时已不具备真实性，并提供证据予以证明或者说明理由的，人民法院应当予以审查。

人民法院根据案件情况，可以要求提供区块链存证证据的一方当事人提供证据证明上链存证数据的真实性，或者说明上链存证数据的具体来源、生成机制、

存储过程、第三方公证见证、关联印证数据等情况。当事人不能提供证据证明或者作出合理说明，该区块链存证证据也无法与其他证据相互印证的，人民法院对该证据的真实性不予确认。

第十七条【区块链证据补强认定】当事人可以申请具有专门知识的人就区块链平台存证相关技术问题提出意见。人民法院可以根据当事人申请或者依职权，委托鉴定区块链存证证据的真实性或者调取其他相关证据进行核对。

第十八条【异步审理的涵义、范围和效力】经双方当事人同意，人民法院可以指定当事人在一定期限内，分别登录诉讼平台，以非同步的方式开展调解、证据交换、谈话询问、庭审等诉讼活动。

当事人未在人民法院指定的期限内，以非同步方式完成在线诉讼活动的，视为放弃相应诉讼权利。

第十九条【异步庭审适用条件】案件同时符合下列情形的，人民法院和当事人可以录制视频并上传至诉讼平台，在人民法院指定的期限内，按照庭审程序环节非同步完成庭审活动：

- 1、各方当事人同时在线参与庭审确有困难；
- 2、一方当事人提出书面申请，各方当事人均表示同意；
- 3、案件适用小额诉讼程序或者民事、行政简易程序审理。

第二十条【在线庭审适用范围、方式和条件】人民法院开庭审理的民事、行政案件，可以根据案件复杂程度、技术条件、当事人意愿等因素，决定采取在线视频方式庭审，但具有下列情形之一的，不得适用在线庭审：

- 1、双方当事人均明确表示不同意，或者一方当事人表示不同意且有正当理由的；
- 2、双方当事人明显不具备参与在线庭审的技术条件和能力的；
- 3、需要通过庭审现场查明身份、核对原件、查验实物的；
- 4、案件疑难复杂、证据繁多，适用在线庭审不便于查明事实和适用法律的；

5、人民法院认为存在其他不宜适用在线庭审情形的。

采用在线庭审方式审理的案件，审理过程中出现上述情形之一的，应当将案件转为线下开庭方式审理。已完成的在线庭审活动具有法律效力。

第二十一条【公告案件适用在线庭审】需要公告送达开庭传票的案件，人民法院可以在公告中告知当事人选择在线庭审的权利。被公告方当事人未在开庭前向人民法院表示同意在线庭审的，适用线下庭审。其他同意适用在线庭审的当事人，可以在线参与庭审。

第二十二条【在线庭审环境】在线庭审一般应当在法庭内进行。在线法庭应保持国徽、审判人员及席位名称等在视频画面合理区域。有条件的人民法院，可以通过信息技术设置环境要素齐全的虚拟法庭。因存在特殊情形，确需在法庭或者虚拟法庭之外的其他场所组织在线庭审的，应当报请本院院长同意。

出庭人员参加在线庭审，应当选择安静、无干扰、光线适宜、网络信号良好、相对封闭的场所，不得在可能影响庭审音视频效果或者有损庭审严肃性的场所参加庭审。

出庭人员在线庭审环境不符合要求的，人民法院可以要求其改正，出庭人员拒不改正或者调整后仍不符合要求的，人民法院视情节轻重，可以采取训诫、责令退出在线庭审、罚款等措施。

第二十三条【在线庭审纪律】出庭人员参加在线庭审过程中，应当保持通讯设备静音或关闭，服从审判人员指挥，尊重司法礼仪，遵守法庭纪律，不得作出《中华人民共和国民事诉讼法法庭规则》[第十七条](#)所禁止的行为。

出庭人员出现不按时到庭、脱离庭审画面、庭审音视频静止等情形时，人民法院应当作出提示、警告，并要求出庭人员说明理由。

除确属网络故障、设备损坏、电力中断或者不可抗力等原因外，当事人无正当理由不按时参加在线庭审，视为“拒不到庭”；在庭审中擅自脱离庭审画面，视为“中途退庭”，分别按照相关法律及司法解释规定处理。

出庭人员不听从法庭诉讼指挥，实施妨害在线庭审秩序的行为，经提醒、警告、训诫后，仍拒不改正的，人民法院可以依法采取强制关闭音视频功能、责令退出在线庭审、罚款、拘留等措施。

第二十四条【证人在线出庭】证人等通过在线方式出庭的，不得旁听法庭审理。人民法院应当通过指定在线出庭场所、设置在线候审室、隔断音视频信号等方式，保证其不旁听案件审理和受他人干扰。

当事人对证人在线出庭提出异议且有合理理由的，或者人民法院认为确有必要的，可以要求证人线下出庭作证。

鉴定人、勘验人、具有专门知识的人在线出庭参照证人在线出庭规则执行。

第二十五条【在线庭审公开】适用在线庭审的案件，应当按照法律和司法解释的有关规定公开庭审活动。

对于《中华人民共和国民事诉讼法》第一百三十四条规定的依法不公开审理的案件，经双方当事人同意，可以适用在线庭审，但庭审参与人不得违规录制、截取、传播涉及庭审过程的音视频、图文资料。庭审参与人实施上述行为的，人民法院视情节轻重，可以采取训诫、责令退出在线庭审、罚款、拘留等措施。

第二十六条【电子送达方式、范围和条件】经受送达人同意，人民法院可以通过中国审判流程信息公开网、人民法院送达平台、在线诉讼平台、电子邮件等方式送达诉讼文书、裁判文书和当事人提交的证据材料。

具备下列情形之一的，人民法院可以确定受送达人同意电子送达：

- 1、受送达人明确表示同意的；
- 2、受送达人在诉讼前对适用电子送达已作出过约定或者承诺的；
- 3、受送达人在提交的起诉状、答辩状中主动提供用于接收送达的电子地址的；
- 4、受送达人通过回复收悉、参加诉讼等方式接受已经完成的电子送达，并且未明确表示不同意电子送达的。

人民法院电子送达判决书、裁定书、调解书等裁判文书的，应当告知当事人权利义务，并征得其同意。当事人提出需要纸质版裁判文书的，人民法院应当提供。

第二十七条【电子送达确认】 人民法院可以通过电话确认、诉讼平台在线确认、线下发送电子送达确认书等方式，确认受送达人是否同意电子送达，以及受送达人接收电子送达的具体方式和地址，并告知电子送达的适用范围、效力、送达地址变更方式以及其他需告知的送达事项。

第二十八条【电子送达生效标准】 人民法院向受送达人主动提供或者确认的电子地址送达的，送达信息到达电子地址所在系统时，即为送达。

受送达人未提供或者确认有效电子送达地址，人民法院向能够确认为受送达人本人的电子地址送达的，根据下列情形确定是否完成送达：

- 1、送达人回复已收到送达材料，或者根据送达内容作出相应诉讼行为的，视为完成有效送达；
- 2、受送达人的电子地址所在系统反馈受送达人已阅知，或者有其他证据可以证明受送达人已经收悉的，推定完成有效送达，但受送达人能够证明存在系统错误、送达地址非本人使用或者非本人阅知等未收悉送达内容的情形除外。

人民法院开展电子送达，应当在审判系统中全程留痕。完成有效送达的，人民法院应当制作电子送达凭证。电子送达凭证具有送达回证效力。

对同一送达材料采取多种电子送达方式的，以最先完成的有效送达时间作为送达生效时间。

第二十九条【电子送达的附随职责】 人民法院适用电子送达，应当同步通过短信、电话、即时通讯工具等方式，通知受送达人查阅、接收、下载相关送达材料。

第三十条【在线签名和确认】 案件适用在线诉讼的，各方诉讼主体可以通过在线确认、电子签章等方式对调解协议、笔录、电子送达凭证及其他诉讼材料予以确认。

第三十一条【电子笔录】案件适用在线诉讼的，人民法院可以在调解、证据交换、庭审、合议等诉讼环节运用语音识别技术同步生成等方式形成电子笔录。电子笔录以在线方式核对确认后，与书面笔录具有同等法律效力。

第三十二条【电子卷宗档案】人民法院采取在线方式办理的案件，应当利用诉讼平台随案同步生成电子卷宗，形成电子档案。电子档案的立卷、归档、存储、利用等，按照档案管理相关法律法规的规定执行。

案件无纸质材料或者纸质材料已经全部转化为电子材料的，经第二审人民法院同意，第一审人民法院可以采用电子卷宗代替纸质卷宗进行上诉移送。

第三十三条【在线执行程序】执行案件的在线立案、电子化材料提交、在线执行和解、在线询问当事人、电子送达等环节，参照诉讼案件相关规则办理。

人民法院可以通过财产查控系统、网络拍卖平台、信用惩戒系统等，在线完成财产查明、查封、扣押、冻结、变价和惩戒等执行实施环节。

第三十四条【刑事案件在线审理】人民法院审理的刑事自诉、速裁程序案件和减刑、假释案件，可以在告知当事人在线诉讼权利义务，并征得其同意的基础上，通过互联网或者专用网络，采取在线方式召开庭前会议、提讯被告人、开庭审理、宣告判决等。

适用在线诉讼的刑事案件的身份认证、电子材料提交、在线庭审条件和方式、在线庭审环境、在线庭审纪律、在线签名或者确认、电子笔录等规则，适用本规定相关条款。

第三十五条【在线诉讼数据保护】在线诉讼过程中形成的数据信息，除人民法院依法公开的以外，当事人及其他诉讼参与人、第三人不得违法违规披露、传播和使用。出现上述情形的，人民法院可以根据具体情节，依照法律和司法解释关于妨害诉讼的相关规定追究相关人员法律责任，构成犯罪的，依法追究刑事责任。

第三十六条【附则】本规定自2021年月日起施行。最高人民法院之前发布的司法解释、司法文件与本规定不一致的，以本规定为准。

(四) 最高人民法院、最高人民检察院关于办理非法利用信息网络、帮助信息网络犯罪活动等刑事案件适用法律若干问题的解释

中华人民共和国最高人民法院、中华人民共和国最高人民检察院公告

《最高人民法院、最高人民检察院关于办理非法利用信息网络、帮助信息网络犯罪活动等刑事案件适用法律若干问题的解释》已于2019年6月3日由最高人民法院审判委员会第1771次会议、2019年9月4日由最高人民检察院第十三届检察委员会第二十三次会议通过，现予公布，自2019年11月1日起施行。

最高人民法院

2019年10月21日

(2019年6月3日最高人民法院审判委员会第1771次会议、2019年9月4日最高人民检察院

第十三届检察委员会第二十三次会议通过，自2019年11月1日起施行 法释〔2019〕15号)

为依法惩治拒不履行信息网络安全管理义务、非法利用信息网络、帮助信息网络犯罪活动等犯罪，维护正常网络秩序，根据《中华人民共和国刑法》《中华人民共和国刑事诉讼法》的规定，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 提供下列服务的单位和个人，应当认定为刑法第二百八十六条之一第一款规定的“网络服务提供者”：

(一) 网络接入、域名注册解析等信息网络接入、计算、存储、传输服务；

(二) 信息发布、搜索引擎、即时通讯、网络支付、网络预约、网络购物、网络游戏、网络直播、网站建设、安全防护、广告推广、应用商店等信息网络应用服务；

(三) 利用信息网络提供的电子政务、通信、能源、交通、水利、金融、教育、医疗等公共服务。

第二条 刑法第二百八十六条之一第一款规定的“监管部门责令采取改正措施”，是指网信、电信、公安等依照法律、行政法规的规定承担信息网络安全监管职责的部门，以责令整改通知书或者其他文书形式，责令网络服务提供者采取改正措施。

认定“经监管部门责令采取改正措施而拒不改正”，应当综合考虑监管部门责令改正是否具有法律、行政法规依据，改正措施及期限要求是否明确、合理，网络服务提供者是否具有按照要求采取改正措施的能力等因素进行判断。

第三条 拒不履行信息网络安全管理义务，具有下列情形之一的，应当认定为刑法第二百八十六条之一第一款第一项规定的“致使违法信息大量传播”：

(一) 致使传播违法视频文件二百个以上的；

(二) 致使传播违法视频文件以外的其他违法信息二千个以上的；

(三) 致使传播违法信息，数量虽未达到第一项、第二项规定标准，但是按相应比例折算合计达到有关数量标准的；

(四) 致使向二千个以上用户账号传播违法信息的；

(五) 致使利用群组成员账号数累计三千以上的通讯群组或者关注人员账号数累计三万以上的社交网络传播违法信息的；

(六) 致使违法信息实际被点击数达到五万以上的；

(七) 其他致使违法信息大量传播的情形。

第四条 拒不履行信息网络安全管理义务，致使用户信息泄露，具有下列情形之一的，应当认定为刑法第二百八十六条之一第一款第二项规定的“造成严重后果”：

(一) 致使泄露行踪轨迹信息、通信内容、征信信息、财产信息五百条以上的；

(二) 致使泄露住宿信息、通信记录、健康生理信息、交易信息等其他可能影响人身、财产安全的用户信息五千条以上的；

(三) 致使泄露第一项、第二项规定以外的用户信息五万条以上的；

(四) 数量虽未达到第一项至第三项规定标准，但是按相应比例折算合计达到有关数量标准的；

(五) 造成他人死亡、重伤、精神失常或者被绑架等严重后果的；

(六) 造成重大经济损失的；

(七) 严重扰乱社会秩序的；

(八) 造成其他严重后果的。

第五条 拒不履行信息网络安全管理义务，致使影响定罪量刑的刑事案件证据灭失，具有下列情形之一的，应当认定为刑法第二百八十六条之一第一款第三项规定的“情节严重”：

(一) 造成危害国家安全犯罪、恐怖活动犯罪、黑社会性质组织犯罪、贪污贿赂犯罪案件的证据灭失的；

(二) 造成可能判处五年有期徒刑以上刑罚犯罪案件的证据灭失的；

(三) 多次造成刑事案件证据灭失的；

(四) 致使刑事诉讼程序受到严重影响的；

(五) 其他情节严重的情形。

第六条 拒不履行信息网络安全管理义务，具有下列情形之一的，应当认定为刑法第二百八十六条之一第一款第四项规定的“有其他严重情节”：

(一) 对绝大多数用户日志未留存或者未落实真实身份信息认证义务的；

(二) 二年内经多次责令改正拒不改正的；

(三) 致使信息网络服务被主要用于违法犯罪的；

(四) 致使信息网络服务、网络设施被用于实施网络攻击，严重影响生产、生活的；

(五) 致使信息网络服务被用于实施危害国家安全犯罪、恐怖活动犯罪、黑社会性质组织犯罪、贪污贿赂犯罪或者其他重大犯罪的；

(六) 致使国家机关或者通信、能源、交通、水利、金融、教育、医疗等领域提供公共服务的信息网络受到破坏，严重影响生产、生活的；

(七) 其他严重违反信息网络安全管理义务的情形。

第七条 刑法第二百八十七条之一规定的“违法犯罪”，包括犯罪行为和属于刑法分则规定的行为类型但尚未构成犯罪的违法行为。

第八条 以实施违法犯罪活动为目的而设立或者设立后主要用于实施违法犯罪活动的网站、通讯群组，应当认定为刑法第二百八十七条之一第一款第一项规定的“用于实施诈骗、传授犯罪方法、制作或者销售违禁物品、管制物品等违法犯罪活动的网站、通讯群组”。

第九条 利用信息网络提供信息的链接、截屏、二维码、访问账号密码及其他指引访问服务的，应当认定为刑法第二百八十七条之一第一款第二项、第三项规定的“发布信息”。

第十条 非法利用信息网络，具有下列情形之一的，应当认定为刑法第二百八十七条之一第一款规定的“情节严重”：

(一) 假冒国家机关、金融机构名义，设立用于实施违法犯罪活动的网站的；

(二) 设立用于实施违法犯罪活动的网站，数量达到三个以上或者注册账号数累计达到二千以上的；

(三) 设立用于实施违法犯罪活动的通讯群组，数量达到五个以上或者群组成员账号数累计达到一千以上的；

(四) 发布有关违法犯罪的信息或者为实施违法犯罪活动发布信息，具有下列情形之一的：

- 1.在网站上发布有关信息一百条以上的;
- 2.向二千个以上用户账号发送有关信息的;
- 3.向群组成员数累计达到三千以上的通讯群组发送有关信息的;
- 4.利用关注人员账号数累计达到三万以上的社交网络传播有关信息的;

(五) 违法所得一万元以上的;

(六) 二年内曾因非法利用信息网络、帮助信息网络犯罪活动、危害计算机信息系统安全受过行政处罚, 又非法利用信息网络的;

(七) 其他情节严重的情形。

第十一条 为他人实施犯罪提供技术支持或者帮助, 具有下列情形之一的, 可以认定行为人明知他人利用信息网络实施犯罪, 但是有相反证据的除外:

(一) 经监管部门告知后仍然实施有关行为的;

(二) 接到举报后不履行法定管理职责的;

(三) 交易价格或者方式明显异常的;

(四) 提供专门用于违法犯罪的程序、工具或者其他技术支持、帮助的;

(五) 频繁采用隐蔽上网、加密通信、销毁数据等措施或者使用虚假身份, 逃避监管或者规避调查的;

(六) 为他人逃避监管或者规避调查提供技术支持、帮助的;

(七) 其他足以认定行为人明知的情形。

第十二条 明知他人利用信息网络实施犯罪, 为其犯罪提供帮助, 具有下列情形之一的, 应当认定为刑法第二百八十七条之二第一款规定的“情节严重”:

(一) 为三个以上对象提供帮助的;

(二) 支付结算金额二十万元以上的;

(三) 以投放广告等方式提供资金五万元以上的;

(四) 违法所得一万元以上的;

(五) 二年内曾因非法利用信息网络、帮助信息网络犯罪活动、危害计算机信息系统安全受过行政处罚, 又帮助信息网络犯罪活动的;

(六) 被帮助对象实施的犯罪造成严重后果的;

(七) 其他情节严重的情形。

实施前款规定的行为, 确因客观条件限制无法查证被帮助对象是否达到犯罪的程度, 但相关数额总计达到前款第二项至第四项规定标准五倍以上, 或者造成特别严重后果的, 应当以帮助信息网络犯罪活动罪追究行为人的刑事责任。

第十三条 被帮助对象实施的犯罪行为可以确认, 但尚未到案、尚未依法裁判或者因未达到刑事责任年龄等原因依法未予追究刑事责任的, 不影响帮助信息网络犯罪活动罪的认定。

第十四条 单位实施本解释规定的犯罪的, 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, 并对单位处罚金。

第十五条 综合考虑社会危害程度、认罪悔罪态度等情节, 认为犯罪情节轻微的, 可以不起诉或者免于刑事处罚; 情节显著轻微危害不大的, 不以犯罪论处。

第十六条 多次拒不履行信息网络安全管理义务、非法利用信息网络、帮助信息网络犯罪活动构成犯罪, 依法应当追诉的, 或者二年内多次实施前述行为未经处理的, 数量或者数额累计计算。

第十七条 对于实施本解释规定的犯罪被判处刑罚的, 可以根据犯罪情况和预防再犯罪的需要, 依法宣告职业禁止; 被判处管制、宣告缓刑的, 可以根据犯罪情况, 依法宣告禁止令。

第十八条 对于实施本解释规定的犯罪的, 应当综合考虑犯罪的危害程度、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。

第十九条 本解释自2019年11月1日起施行。

（五）最高人民检察院关于印发《检察机关办理侵犯公民个人信息案件指引》的通知

（高检发侦监字〔2018〕13号）

各省、自治区、直辖市人民检察院，新疆生产建设兵团人民检察院：

《检察机关办理侵犯公民个人信息案件指引》已经2018年8月24日最高人民检察院第十三届检察委员会第五次会议通过，现印发你们，供参考。

最高人民检察院

2018年11月9日

检察机关办理侵犯公民个人信息案件指引

根据《中华人民共和国刑法》第二百五十三条之一的规定，侵犯公民个人信息罪是指违反国家有关规定，向他人出售、提供公民个人信息，或者通过窃取等方法非法获取公民个人信息，情节严重的行为。结合《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》（法释〔2017〕10号）（以下简称《解释》），办理侵犯公民个人信息案件，应当特别注意以下问题：一是对“公民个人信息”的审查认定；二是对“违反国家有关规定”的审查认定；三是对“非法获取”的审查认定；四是对“情节严重”和“情节特别严重”的审查认定；五是对关联犯罪的审查认定。

一、审查证据的基本要求

（一）审查逮捕

1. 有证据证明发生了侵犯公民个人信息犯罪事实

（1）证明侵犯公民个人信息案件发生

主要证据包括：报案登记、受案登记、立案决定书、破案经过、证人证言、被害人陈述、犯罪嫌疑人供述和辩解以及证人、被害人提供的短信、微信或QQ截图等电子数据。

(2) 证明被侵犯对象系公民个人信息

主要证据包括：扣押物品清单、勘验检查笔录、电子数据、司法鉴定意见及公民信息查询结果说明、被害人陈述、被害人提供的原始信息资料 and 对比资料等。

2. 有证据证明侵犯公民个人信息行为是犯罪嫌疑人实施的

(1) 证明违反国家有关规定的证据：犯罪嫌疑人关于所从事的职业的供述、其所在公司的工商注册资料、公司出具的犯罪嫌疑人职责范围说明、劳动合同、保密协议及公司领导、同事关于犯罪嫌疑人职责范围的证言等。

(2) 证明出售、提供行为的证据：远程勘验笔录及QQ、微信等即时通讯工具聊天记录、论坛、贴吧、电子邮件、手机短信记录等电子数据，证明犯罪嫌疑人通过上述途径向他人出售、提供、交换公民个人信息的情况。公民个人信息贩卖者、提供者、担保交易人及购买者、收受者的证言或供述，相关银行账户明细、第三方支付平台账户明细，证明出售公民个人信息违法所得情况。此外，如果犯罪嫌疑人系通过信息网络发布方式提供公民个人信息，证明该行为的证据还包括远程勘验笔录、扣押笔录、扣押物品清单、对手机、电脑存储介质、云盘、FTP等的司法鉴定意见等。

(3) 证明犯罪嫌疑人或公民个人信息购买者、收受者控制涉案信息的证据：搜查笔录、扣押笔录、扣押物品清单，对手机、电脑存储介质等的司法鉴定意见等，证实储存有公民个人信息的电脑、手机、U盘或者移动硬盘、云盘、FTP等介质与犯罪嫌疑人或公民个人信息购买者、收受者的关系。犯罪嫌疑人供述、辨认笔录及证人证言等，证实犯罪嫌疑人或公民个人信息购买者、收受者所有或实际控制、使用涉案存储介质。

(4) 证明涉案公民个人信息真实性的证据：被害人陈述、被害人提供的原始信息资料、公安机关或相关单位出具的涉案公民个人信息与权威数据库内信息同一性的比对说明。针对批量的涉案公民个人信息的真实性问题，根据《解释》精神，可以根据查获的数量直接认定，但有证据证明信息不真实或重复的除外。

(5) 证明违反国家规定，通过窃取、购买、收受、交换等方式非法获取公民个人信息的证据：主要证据与上述以出售、提供方式侵犯公民个人信息行为的

证据基本相同。针对窃取的方式如通过技术手段非法获取公民个人信息的行为，需证明犯罪嫌疑人实施上述行为，除被害人陈述、犯罪嫌疑人供述和辩解外，还包括侦查机关从被害公司数据库中发现入侵电脑IP地址情况、从犯罪嫌疑人电脑中提取的侵入被害公司数据的痕迹等现场勘验检查笔录，以及涉案程序（木马）的司法鉴定意见等。

3. 有证据证明犯罪嫌疑人具有侵犯公民个人信息的主观故意

(1) 证明犯罪嫌疑人明知没有获取、提供公民个人信息的法律依据或资格，主要证据包括：犯罪嫌疑人的身份证明、犯罪嫌疑人关于所从事职业的供述、其所在公司的工商资料和营业范围、公司关于犯罪嫌疑人的职责范围说明、公司主要负责人的证人证言等。

(2) 证明犯罪嫌疑人积极实施窃取、出售、提供、购买、交换、收受公民个人信息的行为，主要证据除了证人证言、犯罪嫌疑人供述和辩解外，还包括远程勘验笔录、手机短信记录、即时通讯工具聊天记录、电子数据司法鉴定意见、银行账户明细、第三方支付平台账户明细等。

4. 有证据证明“情节严重”或“情节特别严重”

(1) 公民个人信息购买者或收受者的证言或供述。

(2) 公民个人信息购买、收受公司工作人员利用公民个人信息进行电话或短信推销、商务调查等经营性活动后出具的证言或供述。

(3) 公民个人信息购买者或者收受者利用所获信息从事违法犯罪活动后出具的证言或供述。

(4) 远程勘验笔录、电子数据司法鉴定意见书、最高人民检察院或公安部指定的机构对电子数据涉及的专门性问题出具的报告、公民个人信息资料等。证明犯罪嫌疑人通过即时通讯工具、电子邮箱、论坛、贴吧、手机等向他人出售、提供、购买、交换、收受公民个人信息的情况。

(5) 银行账户明细、第三方支付平台账户明细。

(6) 死亡证明、伤情鉴定意见、医院诊断记录、经济损失鉴定意见、相关

案件起诉书、判决书等。

（二）审查起诉

除审查逮捕阶段证据审查基本要求之外，对侵犯公民个人信息案件的审查起诉工作还应坚持“犯罪事实清楚，证据确实、充分”的标准，保证定罪量刑的事实都有证据证明；据以定案的证据均经法定程序查证属实；综合全案证据，对所认定的事实已排除合理怀疑。

1. 有确实充分的证据证明发生了侵犯公民个人信息犯罪事实。该证据与审查逮捕的证据类型相同。

2. 有确实充分的证据证明侵犯公民个人信息行为是犯罪嫌疑人实施的

（1）对于证明犯罪行为是犯罪嫌疑人实施的证据审查，需要结合《解释》精神，准确把握对“违反国家有关规定”“出售、提供行为”“窃取或以其他方法”的认定。

（2）对证明违反国家有关规定的证据审查，需要明确国家有关规定的具体内容，违反法律、行政法规、部门规章有关公民个人信息保护规定的，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”。

（3）对证明出售、提供行为的证据审查，应当明确“出售、提供”包括在履职或提供服务的过程中将合法持有的公民个人信息出售或者提供给他人的行为：向特定人提供、通过信息网络或者其他途径发布公民个人信息、未经被收集者同意，将合法收集的公民个人信息（经过处理无法识别特定个人且不能复原的除外）向他人提供的，均属于刑法第二百五十三条之一规定的“提供公民个人信息”。应当全面审查犯罪嫌疑人所出售提供公民个人信息的来源、途经与去向，对相关供述、物证、书证、证人证言、被害人陈述、电子数据等证据种类进行综合审查，针对使用信息网络进行犯罪活动的，需要结合专业知识，根据证明该行为的远程勘验笔录、扣押笔录、扣押物品清单、电子存储介质、网络存储介质等的司法鉴定意见进行审查。

（4）对证明通过窃取或以其他非法方法获取公民个人信息等方式非法获取

公民个人信息的证据审查，应当明确“以其他方法获取公民个人信息”包括购买、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行为。

针对窃取行为，如通过信息网络窃取公民个人信息，则应当结合犯罪嫌疑人供述、证人证言、被害人陈述，着重审查证明犯罪嫌疑人侵入信息网络、数据库时的IP地址、MAC地址、侵入工具、侵入痕迹等内容的现场勘验检查笔录以及涉案程序（木马）的司法鉴定意见等。

针对购买、收受、交换行为，应当全面审查购买、收受、交换公民个人信息的来源、途经、去向，结合犯罪嫌疑人供述和辩解、辨认笔录、证人证言等证据，对搜查笔录、扣押笔录、扣押物品清单、涉案电子存储介质等司法鉴定意见进行审查，明确上述证据同犯罪嫌疑人或公民个人信息购买、收受、交换者之间的关系。

针对履行职责、提供服务过程中收集公民个人信息的行为，应当审查证明犯罪嫌疑人所从事职业及其所负职责的证据，结合法律、行政法规、部门规章等国家有关公民个人信息保护的规定，明确犯罪嫌疑人的行为属于违反国家有关规定，以其他方法非法获取公民个人信息的行为。

(5) 对证明涉案公民个人信息真实性证据的审查，应当着重审查被害人陈述、被害人提供的原始信息资料、公安机关或其他相关单位出具的涉案公民个人信息与权威数据库内信息同一性的对比说明。对批量的涉案公民个人信息的真实性问题，根据《解释》精神，可以根据查获的数量直接认定，但有证据证明信息不真实或重复的除外。

3. 有确实充分的证据证明犯罪嫌疑人具有侵犯公民个人信息的主观故意

(1) 对证明犯罪嫌疑人主观故意的证据审查，应当综合审查犯罪嫌疑人的身份证明、犯罪嫌疑人关于所从事职业的供述、其所在公司的工商资料和营业范围、公司关于犯罪嫌疑人的职责范围说明、公司主要负责人的证人证言等，结合国家公民个人信息保护的相关规定，夯实犯罪嫌疑人在实施犯罪时的主观明知。

(2) 对证明犯罪嫌疑人积极实施窃取或者以其他方法非法获取公民个人信

息行为的证据审查，应当结合犯罪嫌疑人供述、证人证言，着重审查远程勘验笔录、手机短信记录、即时通讯工具聊天记录、电子数据司法鉴定意见、银行账户明细、第三方支付平台账户明细等，明确犯罪嫌疑人在实施犯罪时的积极作为。

4. 有确实充分的证据证明“情节严重”或“情节特别严重”。该证据与审查逮捕的证据类型相同。

二、需要特别注意的问题

在侵犯公民个人信息案件审查逮捕、审查起诉中，要根据相关法律、司法解释等规定，结合在案证据，重点关注以下问题：

（一）对“公民个人信息”的审查认定

根据《解释》的规定，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。经过处理无法识别特定自然人且不能复原的信息，虽然也可能反映自然人活动情况，但与特定自然人无直接关联，不属于公民个人信息的范畴。

对于企业工商登记等信息中所包含的手机、电话号码等信息，应当明确该号码的用途。对由公司购买、使用的手机、电话号码等信息，不属于个人信息的范畴，从而严格区分“手机、电话号码等由公司购买，归公司使用”与“公司经办人在工商登记等活动中登记个人电话、手机号码”两种不同情形。

（二）对“违反国家有关规定”的审查认定

《中华人民共和国刑法修正案（九）》将原第二百五十三条之一的“违反国家规定”修改为“违反国家有关规定”，后者的范围明显更广。根据刑法第九十六条的规定，“国家规定”仅限于全国人大及其常委会制定的法律和决定，国务院制定的行政法规、规定的行政措施、发布的决定和命令。而“国家有关规定”还包括部门规章，这些规定散见于金融、电信、交通、教育、医疗、统计、邮政等领域的法律、行政法规或部门规章中。

(三) 对“非法获取”的审查认定

在窃取或者以其他方法非法获取公民个人信息的行为中，需要着重把握“其他方法”的范围问题。“其他方法”，是指“窃取”以外，与窃取行为具有同等危害性的方法，其中，购买是最常见的非法获取手段。侵犯公民个人信息犯罪作为电信网络诈骗的上游犯罪，诈骗分子往往先通过网络向他人购买公民个人信息，然后自己直接用于诈骗或转发给其他同伙用于诈骗，诈骗分子购买公民个人信息的行为属于非法获取行为，其同伙接收公民个人信息的行为明显也属于非法获取行为。同时，一些房产中介、物业管理公司、保险公司、担保公司的业务员往往与同行通过QQ、微信群互相交换各自掌握的客户信息，这种交换行为也属于非法获取行为。此外，行为人在履行职责、提供服务过程中，违反国家有关规定，未经他人同意收集公民个人信息，或者收集与提供的服务无关的公民个人信息的，也属于非法获取公民个人信息的行为。

(四) 对“情节严重”和“情节特别严重”的审查认定

1. 关于“情节严重”的具体认定标准，根据《解释》第五条第一款的规定，主要涉及五个方面：

(1) 信息类型和数量。①行踪轨迹信息、通信内容、征信信息、财产信息，此类信息与公民人身、财产安全直接相关，数量标准为五十条以上，且仅限于上述四类信息，不允许扩大范围。对于财产信息，既包括银行、第三方支付平台、证券期货等金融服务账户的身份认证信息（一组确认用户操作权限的数据，包括账号、口令、密码、数字证书等），也包括存款、房产、车辆等财产状况信息。②住宿信息、通信记录、健康生理信息、交易信息等可能影响公民人身、财产安全的信息，数量标准为五百条以上，此类信息也与人身、财产安全直接相关，但重要程度要弱于行踪轨迹信息、通信内容、征信信息、财产信息。对“其他可能影响人身、财产安全的公民个人信息”的把握，应当确保所适用的公民个人信息涉及人身、财产安全，且与“住宿信息、通信记录、健康生理信息、交易信息”在重要程度上具有相当性。③除上述两类信息以外的其他公民个人信息，数量标准为五千条以上。

(2) 违法所得数额。对于违法所得，可直接以犯罪嫌疑人出售公民个人信息的收入予以认定，不必扣减其购买信息的犯罪成本。同时，在审查认定违法所得数额过程中，应当以查获的银行交易记录、第三方支付平台交易记录、聊天记录、犯罪嫌疑人供述、证人证言综合予以认定，对于犯罪嫌疑人无法说明合法来源的用于专门实施侵犯公民个人信息犯罪的银行账户或第三方支付平台账户内资金收入，可综合全案证据认定为违法所得。

(3) 信息用途。公民个人信息被他人用于违法犯罪活动的，不要求他人的行为必须构成犯罪，只要行为人明知他人非法获取公民个人信息用于违法犯罪活动即可。

(4) 主体身份。如果行为人系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，涉案信息数量、违法所得数额只要达到一般主体的一半，即可认为“情节严重”。

(5) 主观恶性。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，即可认为“情节严重”。

2. 关于“情节特别严重”的认定标准，根据《解释》，主要分为两类：一是信息数量、违法所得数额标准。二是信息用途引发的严重后果，其中造成人身伤亡、经济损失、恶劣社会影响等后果，需要审查认定侵犯公民个人信息的行为与严重后果间存在因果关系。

对于涉案公民个人信息数量的认定，根据《解释》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；对批量出售、提供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。在实践中，如犯罪嫌疑人多次获取同一条公民个人信息，一般认定为一条，不重复累计；但获取的该公民个人信息内容发生了变化的除外。

对于涉案公民个人信息的数量、社会危害性等因素的审查，应当结合刑法第二百五十三条和《解释》的规定进行综合审查。涉案公民个人信息数量极少，但

造成被害人死亡等严重后果的，应审查犯罪嫌疑人行为与该后果之间的因果关系，符合条件的，可以认定为实施《解释》第五条第一款第十项“其他情节严重的情形”的行为，造成被害人死亡等严重后果，从而认定为“情节特别严重”。如涉案公民个人信息数量较多，但犯罪嫌疑人仅仅获取而未向他人出售或提供，则可以在认定相关犯罪事实的基础上，审查该行为是否符合《解释》第五条第一款第三、四、五、六、九项及第二款第三项的情形，符合条件的，可以分别认定为“情节严重”“情节特别严重”。

此外，针对为合法经营活动而购买、收受公民个人信息的行为，在适用《解释》第六条的定罪量刑标准时须满足三个条件：一是为了合法经营活动，对此可以综合全案证据认定，但主要应当由犯罪嫌疑人一方提供相关证据；二是限于普通公民个人信息，即不包括可能影响人身、财产安全的敏感信息；三是信息没有再流出扩散，即行为方式限于购买、收受。如果将购买、收受的公民个人信息非法出售或者提供的，定罪量刑标准应当适用《解释》第五条的规定。

（五）对关联犯罪的审查认定

对于侵犯公民个人信息犯罪与电信网络诈骗犯罪相交织的案件，应严格按照《最高人民法院、最高人民检察院、公安部关于办理电信网络诈骗等刑事案件适用法律若干问题的意见》（法发〔2016〕32号）的规定进行审查认定，即通过认真审查非法获取、出售、提供公民个人信息的犯罪嫌疑人对电信网络诈骗犯罪的参与程度，结合能够证实其认知能力的学历文化、聊天记录、通话频率、获取固定报酬还是参与电信网络诈骗犯罪分成等证据，分析判断其是否属于诈骗共同犯罪、是否应该数罪并罚。

根据《解释》第八条的规定，设立用于实施出售、提供或者非法获取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；同时构成侵犯公民个人信息罪的，应当认定为侵犯公民个人信息罪。

对于违反国家有关规定，采用技术手段非法侵入合法存储公民个人信息的单位数据库窃取公民个人信息的行为，也符合刑法第二百八十五条第二款非法获取

计算机信息系统数据罪的客观特征，同时触犯侵犯公民个人信息罪和非法获取计算机信息系统数据罪的，应择一重罪论处。

此外，针对公安民警在履行职责过程中，违反国家有关规定，查询、提供公民个人信息的情形，应当认定为“违反国家有关规定，将在履行职责或者提供服务过程中以其他方法非法获取或提供公民个人信息”。但同时，应当审查犯罪嫌疑人除该行为之外有无其他行为侵害其他法益，从而对可能存在的其他犯罪予以准确认定。

三、社会危险性及羁押必要性审查

（一）审查逮捕

1. 犯罪动机：一是出售牟利；二是用于经营活动；三是用于违法犯罪活动。犯罪动机表明犯罪嫌疑人主观恶性，也能证明犯罪嫌疑人是否可能实施新的犯罪。

2. 犯罪情节。犯罪嫌疑人的行为直接反映其人身危险性。具有下列情节的侵犯公民个人信息犯罪，能够证实犯罪嫌疑人主观恶性和人身危险性较大，实施新的犯罪的可能性也较大，可以认为具有较大的社会危险性：一是犯罪持续时间较长、多次实施侵犯公民个人信息犯罪的；二是被侵犯的公民个人信息数量或违法所得巨大的；三是利用公民个人信息进行违法犯罪活动的；四是犯罪手段行为本身具有违法性或者破坏性，即犯罪手段恶劣的，如骗取、窃取公民个人信息，采取胁迫、植入木马程序侵入他人计算机系统等方式非法获取信息。

犯罪嫌疑人实施侵犯公民个人信息犯罪，不属于“情节特别严重”，系初犯，全部退赃，并确有悔罪表现的，可以认定社会危险性较小，没有逮捕必要。

（二）审查起诉

在审查起诉阶段，要结合侦查阶段取得的事实证据，进一步引导侦查机关加大捕后侦查力度，及时审查新证据。在羁押期限届满前对全案进行综合审查，对于未达到逮捕证明标准的，撤销原逮捕决定。

经羁押必要性审查，发现犯罪嫌疑人具有下列情形之一的，应当向办案机关

提出释放或者变更强制措施的建议：

1. 案件证据发生重大变化，没有证据证明有犯罪事实或者犯罪行为系犯罪嫌疑人、被告人所为的。
2. 案件事实或者情节发生变化，犯罪嫌疑人、被告人可能被判处拘役、管制、独立适用附加刑、免于刑事处罚或者判决无罪的。
3. 继续羁押犯罪嫌疑人、被告人，羁押期限将超过依法可能判处的刑期的。
4. 案件事实基本查清，证据已经收集固定，符合取保候审或者监视居住条件的。

经羁押必要性审查，发现犯罪嫌疑人、被告人具有下列情形之一，且具有悔罪表现，不予羁押不致发生社会危险性的，可以向办案机关提出释放或者变更强制措施的建议：

1. 预备犯或者中止犯；共同犯罪中的从犯或者胁从犯。
2. 主观恶性较小的初犯。
3. 系未成年人或者年满七十五周岁的人。
4. 与被害方依法自愿达成和解协议，且已经履行或者提供担保的。
5. 患有严重疾病、生活不能自理的。
6. 系怀孕或者正在哺乳自己婴儿的妇女。
7. 系生活不能自理的人的唯一扶养人。
8. 可能被判处一年以下有期徒刑或者宣告缓刑的。
9. 其他不需要继续羁押犯罪嫌疑人、被告人的情形。

(六) 最高人民法院、最高人民检察院、公安部关于依法惩处侵害公民个人信息犯罪活动的通知

(公通字〔2013〕12号)

各省、自治区、直辖市高级人民法院，人民检察院，公安厅、局，新疆维吾尔自治区高级人民法院生产建设兵团分院，新疆生产建设兵团人民检察院、公安局：

近年来，随着我国经济快速发展和信息网络的广泛普及，侵害公民个人信息的违法犯罪日益突出，互联网上非法买卖公民个人信息泛滥，由此滋生的电信诈骗、网络诈骗、敲诈勒索、绑架和非法讨债等犯罪屡打不绝，社会危害严重，群众反响强烈。为有效遏制、惩治侵害公民个人信息犯罪，切实保障广大人民群众的个人信息和合法权益，促进社会协调发展，维护社会稳定，现就有关事项通知如下：

一、切实提高认识，坚决打击侵害公民个人信息犯罪活动。当前，一些犯罪分子为追求不法利益，利用互联网大肆倒卖公民个人信息，已逐渐形成庞大“地下产业”和黑色利益链。买卖的公民个人信息包括户籍、银行、电信开户资料等，涉及公民个人生活的方方面面。部分国家机关和金融、电信、交通、教育、医疗以及物业公司、房产中介、保险、快递等企事业单位的一些工作人员，将在履行职责或者提供服务过程中获取的公民个人信息出售、非法提供给他人。获取信息的中间商在互联网上建立数据平台，大肆出售信息谋取暴利。非法调查公司根据这些信息从事非法讨债、诈骗和敲诈勒索等违法犯罪活动。此类犯罪不仅危害公民的信息安全，而且极易引发多种犯罪，成为电信诈骗、网络诈骗以及滋扰型“软暴力”等信息犯罪的根源，甚至与绑架、敲诈勒索、暴力追债等犯罪活动相结合，影响人民群众的安全感，威胁社会和谐稳定。各级公安机关、人民检察院、人民法院务必清醒认识此类犯罪的严重危害，以对党和人民高度负责的精神，统一思想，提高认识，精心组织，周密部署，依法惩处侵害公民个人信息犯罪活动。

二、正确适用法律，实现法律效果与社会效果的有机统一。侵害公民个人信息犯罪是新型犯罪，各级公安机关、人民检察院、人民法院要从切实保护公民个

人信息安全和维护社会和谐稳定的高度，借鉴以往的成功判例，综合考虑出售、非法提供或非法获取个人信息的次数、数量、手段和牟利数额、造成的损害后果等因素，依法加大打击力度，确保取得良好的法律效果和社会效果。出售、非法提供公民个人信息罪的犯罪主体，除国家机关或金融、电信、交通、医疗单位的工作人员之外，还包括在履行职责或者提供服务过程中获得公民个人信息的商业、房地产业等服务业中其他企事业单位的工作人员。公民个人信息包括公民的姓名、年龄、有效证件号码、婚姻状况、工作单位、学历、履历、家庭住址、电话号码等能够识别公民个人身份或者涉及公民个人隐私的信息、数据资料。对于在履行职责或者提供服务过程中，将获得的公民个人信息出售或者非法提供给他人的，被他人用以实施犯罪，造成受害人人身伤害或者死亡，或者造成重大经济损失、恶劣社会影响的，或者出售、非法提供公民个人信息数量较大，或者违法所得数额较大的，均应当依法以非法出售、非法提供公民个人信息罪追究刑事责任。对于窃取或者以购买等方法非法获取公民个人信息数量较大，或者违法所得数额较大，或者造成其他严重后果的，应当依法以非法获取公民个人信息罪追究刑事责任。对使用非法获取的个人信息，实施其他犯罪行为，构成数罪的，应当依法予以并罚。单位实施侵害公民个人信息罪的，应当追究直接负责的主管人员和其他直接责任人员的刑事责任。要依法加大对财产刑的适用力度，剥夺犯罪分子非法获利和再次犯罪的资本。

三、加强协作配合，确保执法司法及时高效。侵害公民个人信息犯罪网络覆盖面大，关系错综复杂。犯罪行为发生地、犯罪结果发生地、犯罪分子所在地等往往不在一地。同时，由于犯罪行为大多依托互联网、移动电子设备，通过即时通讯工具、电子邮件等多种方式实施，调查取证难度很大、各级公安机关、人民检察院、人民法院要在分工负责、依法高效履行职责的基础上，进一步加强沟通协调，通力配合，密切协作，保证立案、侦查、批捕、审查起诉、审判等各个环节顺利进行。对查获的及时立案侦查，及时移送审查起诉。对于几个公安机关都有管辖的案件，由最初受理的公安机关管辖。必要时，可以由主要犯罪地的公安机关管辖。对管辖不明确或者有争议的刑事案件，可以由公安机关协商。协商不成的，由共同上级公安机关指定管辖。对于指定管辖的案件，需要逮捕犯罪嫌疑人的，由被指定管辖的公安机关提请同级人民检察院审查批准；需要提起公诉

的，由该公安机关移送同级人民检察院审查决定；认为应当由上级人民检察院或者同级其他人民检察院起诉的，应当将案件移交有管辖权的人民检察院；人民检察院认为需要依照刑事诉讼法的规定指定审判管辖的，应当协商同级人民法院办理指定管辖有关事宜。在办理侵害公民个人信息犯罪案件的过程中，对于疑难、复杂案件，人民检察院可以适时派员会同公安机关共同就证据收集等方面进行研究和沟通协调。人民检察院对于公安机关提请批准逮捕、移送审查起诉的相关案件，符合批捕、起诉条件的，要依法尽快予以批捕、起诉；对于确需补充侦查的，要制作具体、详细的补充侦查提纲。人民法院要加强审判力量，准确定性，依法快审快结。

四、推进综合治理，建立防范、打击长效工作机制。预防和打击侵害公民个人信息犯罪是一项艰巨任务，必须标本兼治，积极探索和构建防范、打击的长效工作机制。各地公安机关、人民检察院、人民法院在依法惩处此类犯罪的同时，要积极参与综合治理，注意发现保护公民个人信息工作中的疏漏和隐患，及时通报相关部门，提醒和督促有关部门和单位加强监管、完善制度。要充分利用报纸、广播、电视、网络等多种媒体平台，大力宣传党和国家打击此类犯罪的决心和力度，宣传相关的政策和法律法规，提醒和教育广大群众运用法律保障和维护自身合法权益，提高自我防范的意识和能力。

给地接此通知后，请迅速传达至各级人民法院、人民检察院、公安机关。执行中遇到的问题，请及时报最高人民法院、最高人民检察院、公安部。

最高人民法院

最高人民检察院

公安部

2013年4月23日

(七) 最高人民法院关于审理网络消费纠纷案件适用法律若干问题的规定（一）（征求意见稿）

为妥善审理网络消费纠纷案件，依法保护消费者合法权益，促进网络经济健康发展，我院起草了《关于审理网络消费纠纷案件适用法律若干问题的规定（一）》（征求意见稿）。为进一步完善该司法解释，现通过最高人民法院政务网、中国法院网、人民法院报、民一庭公众号等向社会公开征求意见，欢迎社会各界人士踊跃提出宝贵意见。具体的修改意见反馈可采取书面寄送或者电子邮件的方式，并请在提出建议时说明具体理由。书面意见可寄往北京市东城区东交民巷 27 号，最高人民法院民事审判第一庭李雪薇，邮编 100745；电子邮件请发送至邮箱 zgf_minyingting@163.com。本次征求意见截止日期为 2022 年 1 月 7 日。

特此公告！

中华人民共和国最高人民法院

二〇二一年十二月二十七日

为妥善审理网络消费纠纷案件，依法保护消费者合法权益，促进网络经济健康发展，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》等法律规定，结合民事审判实践，制定本规定。

一、合同权利义务

第一条【格式条款】 电子商务经营者提供的格式条款约定以下内容，消费者主张该格式条款无效的，人民法院应予支持：

- （一）收货人签收商品即视为认可商品质量符合约定；
- （二）电子商务平台经营者依法应承担的责任一概由平台内经营者承担；
- （三）电子商务经营者享有单方解释权或者最终解释权；

(四) 排除或者限制消费者依法投诉、举报、请求调解、申请仲裁、提起诉讼的权利;

(五) 其他排除或者限制消费者权利、减轻或者免除电子商务经营者责任、加重消费者责任等对消费者不公平、不合理的约定。

第二条【管辖权异议】 消费者以电子商务平台经营者和平台内经营者为共同被告提起诉讼, 电子商务平台经营者仅以其与平台内经营者或者消费者分别签订的用户协议约定的诉讼管辖条款为由提出管辖权异议的, 人民法院不予支持。

第三条【七日内无理由退货】 电子商务经营者依据消费者权益保护法第二十五条第二款规定, 根据商品性质以格式条款方式约定所售商品不适用七日无理由退货制度, 但未依法履行提示说明义务且经消费者确认, 消费者主张该条款不成为合同的内容的, 人民法院应予支持。

第四条【七日内无理由退货】 电子商务经营者就消费者权益保护法第二十五条第一款规定的四项除外商品做出无理由退货承诺, 消费者主张电子商务经营者应当遵守其承诺的, 人民法院应予支持。

第五条【七日内无理由退货】 消费者因检查商品的必要对商品进行拆封查验且不影响商品完好, 电子商务经营者以商品已拆封为由主张不适用消费者权益保护法第二十五条规定的无理由退货制度的, 人民法院不予支持, 但法律另有规定的除外。

第六条【平台自营业务民事责任】 电子商务平台经营者以标记自营业务方式或者虽未标记自营但实际开展自营业务所销售的商品或者提供的服务给消费者造成损害, 消费者主张电子商务平台经营者承担作为商品销售者或者服务提供者的赔偿责任的, 人民法院应予支持。

电子商务平台经营者虽非实际开展自营业务, 但其所作标识等足以误导消费者使消费者相信系电子商务平台经营者自营, 消费者主张电子商务平台经营者承担作为商品销售者或者服务提供者的赔偿责任的, 人民法院应予支持。

第七条【诱导平台外支付】平台内经营者的工作人员在出售商品或者提供服务过程中，引导消费者通过交易平台提供的支付方式以外的方式进行支付，经营行为侵害消费者合法权益，消费者主张平台内经营者承担商品销售者或者服务提供者责任，平台内经营者以未经过交易平台支付为由抗辩的，人民法院不予支持。

第八条【网络店铺转让】平台内经营者注册网络经营账号开设网络店铺后，通过协议等方式将网络账号及店铺转让给其他经营者，但未依法进行相关经营主体信息变更公示，实际经营者的经营活动给消费者造成损害，消费者主张注册经营者、实际经营者承担赔偿责任的，人民法院应予支持。

第九条【二手商品责任】消费者在二手商品网络交易平台购买二手商品受到损害，人民法院综合销售者出售商品的性质、来源、数量、价格、频率、是否有其他销售渠道、收入等情况，能够认定销售者系通过买卖二手商品从事商业经营活动，消费者主张商品销售者依据消费者权益保护法承担经营者责任的，人民法院应予支持。

第十条【促销奖品、赠品、换购商品】电子商务经营者在促销活动中提供的奖品、赠品或者消费者换购的商品不符合相关安全标准，给消费者造成损害，消费者主张电子商务经营者承担赔偿责任，电子商务经营者以奖品、赠品属于免费提供或者商品属于换购为由主张免责的，人民法院不予支持。

二、网络消费欺诈

第十一条【虚假宣传】电子商务经营者与他人签订的以虚构交易、虚构点击量、编造用户评价等方式进行虚假宣传的合同，人民法院应当依法认定无效。

第十二条【虚假原价优惠价】平台内经营者在提供商品或者服务过程中以虚构原价、虚假优惠折价等方式实施欺诈消费者行为，消费者依据消费者权益保护法第五十五条第一款规定主张平台内经营者承担赔偿责任的，人民法院应予支持。

第十三条【更有利于消费者的承诺】平台内经营者经营假冒伪劣商品侵害消费者合法权益，平台内经营者向消费者承诺的赔偿标准高于法律规定的赔偿标准，消费者主张平台内经营者按照承诺赔偿的，人民法院应依法予以支持。

三、网络直播带货

第十四条【品牌自播】平台内经营者通过网络直播方式销售商品，其员工在网络直播中因虚假宣传等给消费者造成损害，消费者主张平台内经营者承担赔偿责任的，人民法院应予支持。

第十五条【直播间运营者责任】

方案一：消费者因在网络直播间点击购买商品合法权益受到损害，直播间运营者不能证明已经以足以使消费者辨别的方式标明其并非销售者并标明实际销售者的，消费者主张直播间运营者承担商品销售者责任的，人民法院应予支持。

直播间运营者能够证明已经以足以使消费者辨别的方式标明其并非销售者且标明实际销售者并以此为由抗辩的，人民法院应当综合交易外观、直播间运营者与经营者的约定、与经营者的合作模式、交易过程以及消费者主观认知等事实予以认定。

方案二：消费者因在网络直播间点击购买商品合法权益受到损害，消费者主张直播间运营者承担商品销售者责任的，人民法院应予支持。

接受经营者委托的网络直播间未在直播间提供点击购买链接，仅以网络直播形式向消费者推荐商品，构成商业广告的，因虚假宣传等侵害消费者合法权益，消费者主张直播间运营者依据广告法承担相应民事责任的，人民法院应予支持。

消费者与网络直播间之间构成委托合同等法律关系的，人民法院依据相关法律关系予以认定。

第十六条【直播营销平台自营责任】网络直播营销平台经营者通过网络直播方式开展自营业务销售商品，消费者主张其承担商品销售者责任的，人民法院应予支持。

第十七条【直播营销平台责任】网络直播营销平台经营者不能提供直播间运营者的真实姓名、名称、地址和有效联系方式的，消费者可以参照消费者权益保护法第四十四条向网络直播营销平台经营者请求赔偿。网络直播营销平台经营者承担责任后，有权向直播间运营者追偿。

第十八条【直播营销平台审核义务】网络直播营销平台经营者对销售食品的网络直播间的食品经营资质未依法尽到审核义务，给消费者造成损害，消费者主张网络直播营销平台经营者与直播间运营者承担连带责任的，人民法院应予支持。

第十九条【连带责任】网络直播营销平台经营者知道或者应当知道网络直播间销售的商品不符合保障人身、财产安全的要求，或者有其他侵害消费者合法权益行为，未采取必要措施，消费者依据电子商务法第三十八条主张网络直播营销平台经营者与直播间运营者承担连带责任的，人民法院应予支持。

直播间运营者、直播营销人员知道或者应当知道经营者提供的商品不符合保障人身、财产安全的要求，或者有其他侵害消费者合法权益行为，仍为其推广，给消费者造成损害，消费者主张直播间运营者、直播营销人员与提供该商品的经营者承担连带责任的，人民法院应予支持。

四、外卖餐饮

第二十条【外卖餐饮平台审查等义务】网络餐饮服务平台提供者违反食品安全法第六十二条和第一百三十一条规定，未对入网餐饮服务提供者进行实名登记、审查许可证，或者未履行报告、停止提供网络交易平台服务等义务，给消费者造成损害，消费者主张网络餐饮服务平台提供者与入网餐饮服务提供者承担连带责任的，人民法院应予支持。

第二十一条【餐具包装材料不符合安全标准】入网餐饮服务提供者在提供餐饮服务过程中使用明知是不符合强制性安全标准的食品容器、餐具和包装材料，消费者主张入网餐饮服务提供者依据食品安全法第一百四十八条第二款规定承担赔偿责任的，人民法院应予支持。

第二十二条【委托加工】入网餐饮服务提供者所经营食品给消费者造成损害，消费者主张入网餐饮服务提供者承担经营者责任，入网餐饮服务提供者以订单系委托他人加工制作为由抗辩的，人民法院不予支持。

五、其他

第二十三条【公益诉讼】电子商务经营者因经营行为侵害众多网络消费者合法权益，损害社会公共利益，民事诉讼法、消费者权益保护法、个人信息保护法等法律规定的机关和有关组织依法提起民事公益诉讼的，人民法院应予受理。

第二十四条【附则】本规定自 202X 年 XX 月 XX 日起施行。

本规定施行后人民法院正在审理的一审、二审案件适用本规定。

本规定施行前已经终审，本规定施行后当事人申请再审或者按照审判监督程序决定再审的案件，不适用本规定。

最高人民法院以前发布的司法解释与本规定不一致的，不再适用。

(八) 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

中华人民共和国最高人民法院公告

《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》已于2021年6月8日由最高人民法院审判委员会第1841次会议通过，现予公布，自2021年8月1日起施行。

最高人民法院

2021年7月27日

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。

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。

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”。

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：

（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；

（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；

（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；

（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；

（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；

（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；

（七）违背公序良俗处理人脸信息；

（八）违反合法、正当、必要原则处理人脸信息的其他情形。

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。

第四条 有下列情形之一的，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：

（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；

（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；

（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。

第五条 有下列情形之一的，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：

- （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；
- （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；
- （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；
- （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；
- （五）符合法律、行政法规规定的其他情形。

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。

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。

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。

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。

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。

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。

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。

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。

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。

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。

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。

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。

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。

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。

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。

第十六条 本规定自2021年8月1日起施行。

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。

四、部门及部委规章

(一) 数据安全管理办法（征求意见稿）

第一章 总则

第一条 为了维护国家安全、社会公共利益，保护公民、法人和其他组织在网络空间的合法权益，保障个人信息和重要数据安全，根据《[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 在中华人民共和国境内利用网络开展数据收集、存储、传输、处理、使用等活动（以下简称数据活动），以及数据安全的保护和监督管理，适用本办法。纯粹家庭和个人事务除外。

法律、行政法规另有规定的，从其规定。

第三条 国家坚持保障数据安全与发展并重，鼓励研发数据安全保护技术，积极推进数据资源开发利用，保障数据依法有序自由流动。

第四条 国家采取措施，监测、防御、处置来源于中华人民共和国境内外的数据安全风险和威胁，保护数据免受泄露、窃取、篡改、毁损、非法使用等，依法惩治危害数据安全的违法犯罪活动。

第五条 在中央网络安全和信息化委员会领导下，国家网信部门统筹协调、指导监督个人信息和重要数据安全保护工作。

地（市）及以上网信部门依据职责指导监督本行政区内个人信息和重要数据安全保护工作。

第六条 网络运营者应当按照有关法律、行政法规的规定，参照国家网络安全标准，履行数据安全保护义务，建立数据安全管理和评价考核制度，制定数据安全计划，实施数据安全技术防护，开展数据安全风险评估，制定网络安全事件应急预案，及时处置安全事件，组织数据安全教育、培训。

第二章 数据收集

第七条网络运营者通过网站、应用程序等产品收集使用个人信息，应当分别制定并公开收集使用规则。收集使用规则可以包含在网站、应用程序等产品的隐私政策中，也可以其他形式提供给用户。

第八条收集使用规则应当明确具体、简单通俗、易于访问，突出以下内容：

- (一) 网络运营者基本信息；
- (二) 网络运营者主要负责人、数据安全责任人的姓名及联系方式；
- (三) 收集使用个人信息的目的、种类、数量、频度、方式、范围等；
- (四) 个人信息保存地点、期限及到期后的处理方式；
- (五) 向他人提供个人信息的规则，如果向他人提供的；
- (六) 个人信息安全保护策略等相关信息；
- (七) 个人信息主体撤销同意，以及查询、更正、删除个人信息的途径和方法；
- (八) 投诉、举报渠道和方法等；
- (九) 法律、行政法规规定的其他内容。

第九条如果收集使用规则包含在隐私政策中，应相对集中，明显提示，以方便阅读。另仅当用户知悉收集使用规则并明确同意后，网络运营者方可收集个人信息。

第十条网络运营者应当严格遵守收集使用规则，网站、应用程序收集或使用个人信息的功能设计应同隐私政策保持一致，同步调整。

第十一条网络运营者不得以改善服务质量、提升用户体验、定向推送信息、研发新产品等为由，以默认授权、功能捆绑等形式强迫、误导个人信息主体同意其收集个人信息。

个人信息主体同意收集保证网络产品核心业务功能运行的个人信息后，网络运营者应当向个人信息主体提供核心业务功能服务，不得因个人信息主体拒绝或者撤销同意收集上述信息以外的其他信息，而拒绝提供核心业务功能服务。

第十二条收集14周岁以下未成年人个人信息的，应当征得其监护人同意。

第十三条网络运营者不得依据个人信息主体是否授权收集个人信息及授权范围，对个人信息主体采取歧视行为，包括服务质量、价格差异等。

第十四条网络运营者从其他途径获得个人信息，与直接收集个人信息负有同等的保护责任和义务。

第十五条网络运营者以经营为目的收集重要数据或个人敏感信息的，应向所在地网信部门备案。备案内容包括收集使用规则，收集使用的目的、规模、方式、范围、类型、期限等，不包括数据内容本身。

第十六条网络运营者采取自动化手段访问收集网站数据，不得妨碍网站正常运行；此类行为严重影响网站运行，如自动化访问收集流量超过网站日均流量三分之一，网站要求停止自动化访问收集时，应当停止。

第十七条网络运营者以经营为目的收集重要数据或个人敏感信息的，应当明确数据安全责任人。

数据安全责任人由具有相关管理工作经历和数据安全专业知识的人员担任，参与有关数据活动的重要决策，直接向网络运营者的主要负责人报告工作。

第十八条数据安全责任人履行下列职责：

- （一）组织制定数据保护计划并督促落实；
- （二）组织开展数据安全风险评估，督促整改安全隐患；
- （三）按要求向有关部门和网信部门报告数据安全保护和事件处置情况；
- （四）受理并处理用户投诉和举报。

网络运营者应为数据安全责任人提供必要的资源，保障其独立履行职责。

第三章 数据处理使用

第十九条网络运营者应当参照国家有关标准，采用数据分类、备份、加密等措施加强对个人信息和重要数据保护。

第二十条网络运营者保存个人信息不应超出收集使用规则中的保存期限，用户注销账号后应当及时删除其个人信息，经过处理无法关联到特定个人且不能复原（以下称匿名化处理）的除外。

第二十一条网络运营者收到有关个人信息查询、更正、删除以及用户注销账号请求时，应当在合理时间和代价范围内予以查询、更正、删除或注销账号。

第二十二条网络运营者不得违反收集使用规则使用个人信息。因业务需要，确需扩大个人信息使用范围的，应当征得个人信息主体同意。

第二十三条网络运营者利用用户数据和算法推送新闻信息、商业广告等（以下简称“定向推送”），应当以明显方式标明“定推”字样，为用户提供停止接收定向推送信息的功能；用户选择停止接收定向推送信息时，应当停止推送，并删除已经收集的设备识别码等用户数据和个人信息。

网络运营者开展定向推送活动应遵守法律、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。

第二十四条网络运营者利用大数据、人工智能等技术自动合成新闻、博文、帖子、评论等信息，应以明显方式标明“合成”字样；不得以谋取利益或损害他人利益为目的自动合成信息。

第二十五条网络运营者应采取措施督促提醒用户对自己的网络行为负责、加强自律，对于用户通过社交网络转发他人制作的信息，应自动标注信息制作者在该社交网络上的账户或不可更改的用户标识。

第二十六条网络运营者接到相关假冒、仿冒、盗用他人名义发布信息的举报投诉时，应当及时响应，一旦核实立即停止传播并作删除处理。

第二十七条网络运营者向他人提供个人信息前，应当评估可能带来的安全风险，并征得个人信息主体同意。下列情况除外：

- (一) 从合法公开渠道收集且不明显违背个人信息主体意愿;
- (二) 个人信息主体主动公开;
- (三) 经过匿名化处理;
- (四) 执法机关依法履行职责所必需;
- (五) 维护国家安全、社会公共利益、个人信息主体生命安全所必需。

第二十八条网络运营者发布、共享、交易或向境外提供重要数据前，应当评估可能带来的安全风险，并报经行业主管监管部门同意；行业主管监管部门不明确的，应经省级网信部门批准。

向境外提供个人信息按有关规定执行。

第二十九条境内用户访问境内互联网的，其流量不得被路由到境外。

第三十条网络运营者对接入其平台的第三方应用，应明确数据安全要求和责任，督促监督第三方应用运营者加强数据安全。第三方应用发生数据安全事件对用户造成损失的，网络运营者应当承担部分或全部责任，除非网络运营者能够证明无过错。

第三十一条网络运营者兼并、重组、破产的，数据承接方应承接数据安全责任和义务。没有数据承接方的，应当对数据作删除处理。法律、行政法规另有规定的，从其规定。

第三十二条网络运营者分析利用所掌握的数据资源，发布市场预测、统计信息、个人和企业信用等信息，不得影响国家安全、经济运行、社会稳定，不得损害他人合法权益。

第四章 数据安全监督管理

第三十三条网信部门在履行职责中，发现网络运营者数据安全责任落实不到位，应按照规定权限和程序约谈网络运营者的主要负责人，督促整改。

第三十四条国家鼓励网络运营者自愿通过数据安全认证和应用程序安全认证，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应用程序。

国家网信部门会同国务院市场监督管理部门，指导国家网络安全审查与认证机构，组织数据安全管理和应用程序安全认证工作。

第三十五条发生个人信息泄露、毁损、丢失等数据安全事件，或者发生数据安全事件风险明显加大时，网络运营者应当立即采取补救措施，及时以电话、短信、邮件或信函等方式告知个人信息主体，并按要求向行业主管监管部门和网信部门报告。

第三十六条国务院有关主管部门为履行维护国家安全、社会管理、经济调控等职责需要，依照法律、行政法规的规定，要求网络运营者提供掌握的相关数据的，网络运营者应当予以提供。

国务院有关主管部门对网络运营者提供的数据负有安全保护责任，不得用于与履行职责无关的用途。

第三十七条网络运营者违反本办法规定的，由有关部门依照相关法律、行政法规的规定，根据情节给予公开曝光、没收违法所得、暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或吊销营业执照等处罚；构成犯罪的，依法追究刑事责任。

第五章 附 则

第三十八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）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。

（三）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。

（四）个人信息主体，是指个人信息所标识或关联到的自然人。

(五) 重要数据，是指一旦泄露可能直接影响国家安全、经济安全、社会稳定、公共健康和安全的的数据，如未公开的政府信息，大面积人口、基因健康、地理、矿产资源等。重要数据一般不包括企业生产经营和内部管理信息、个人信息等。

第三十九条涉及国家秘密信息、密码使用的数据活动，按照国家有关规定执行。

第四十条本办法自 年 月 日起施行。

(二) 网络数据安全管理条例（征求意见稿）

国家互联网信息办公室关于《网络数据安全管理条例（征求意见稿）》公开征求意见的通知

为落实《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等法律关于数据安全管理的規定，规范网络数据处理活动，保护个人、组织在网络空间的合法权益，维护国家安全和公共利益，根据国务院2021年立法计划，我办会同相关部门研究起草《网络数据安全管理条例（征求意见稿）》，现向社会公开征求意见。公众可通过以下途径和方式反馈意见：

1.通过电子邮件将意见发送至：shujuju@cac.gov.cn。

2.通过信函将意见寄至：北京市西城区车公庄大街11号国家互联网信息办公室网络数据管理局，邮编：100044，并在信封上注明“网络数据安全管理条例征求意见”。

意见反馈截止时间为2021年12月13日。

附件：《网络数据安全管理条例（征求意见稿）》

国家互联网信息办公室

2021年11月14日

网络数据安全管理条例（征求意见稿）

第一章 总则

第一条 为了规范网络数据处理活动，保障数据安全，保护个人、组织在网络空间的合法权益，维护国家安全、公共利益，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》《中华人民共和国个人信息保护法》等法律，制定本条例。

第二条 在中华人民共和国境内利用网络开展数据处理活动，以及网络数据安全的监督管理，适用本条例。

在中华人民共和国境外处理中华人民共和国境内个人和组织数据的活动，有下列情形之一的，适用本条例：

- （一）以向境内提供产品或者服务为目的；
- （二）分析、评估境内个人、组织的行为；
- （三）涉及境内重要数据处理；
- （四）法律、行政法规规定的其他情形。

自然人因个人或者家庭事务开展数据处理活动，不适用本条例。

第三条 国家统筹发展和安全，坚持促进数据开发利用与保障数据安全并重，加强数据安全防护能力建设，保障数据依法有序自由流动，促进数据依法合理有效利用。

第四条 国家支持数据开发利用与安全保护相关的技术、产品、服务创新和人才培养。

国家鼓励国家机关、行业组织、企业、教育和科研机构、有关专业机构等开展数据开发利用和安全保护合作，开展数据安全宣传教育和培训。

第五条 国家建立数据分类分级保护制度。按照数据对国家安全、公共利益或者个人、组织合法权益的影响和重要程度，将数据分为一般数据、重要数据、核心数据，不同级别的数据采取不同的保护措施。

国家对个人信息和重要数据进行重点保护，对核心数据实行严格保护。

各地区、各部门应当按照国家数据分类分级要求，对本地区、本部门以及相关行业、领域的数据进行分类分级管理。

第六条 数据处理者对所处理数据的安全负责，履行数据安全保护义务，接受政府和社会监督，承担社会责任。

数据处理者应当按照有关法律、行政法规的规定和国家标准的强制性要求，建立完善数据安全管理制度和技术保护机制。

第七条 国家推动公共数据开放、共享，促进数据开发利用，并依法对公共数据实施监督管理。

国家建立健全数据交易管理制度，明确数据交易机构设立、运行标准，规范数据流通交易行为，确保数据依法有序流通。

第二章 一般规定

第八条 任何个人和组织开展数据处理活动应当遵守法律、行政法规，尊重社会公德和伦理，不得从事以下活动：

- （一）危害国家安全、荣誉和利益，泄露国家秘密和工作秘密；
- （二）侵害他人名誉权、隐私权、著作权和其他合法权益等；
- （三）通过窃取或者以其他非法方式获取数据；
- （四）非法出售或者非法向他人提供数据；
- （五）制作、发布、复制、传播违法信息；
- （六）法律、行政法规禁止的其他行为。

任何个人和组织知道或者应当知道他人从事前款活动的，不得为其提供技术支持、工具、程序和广告推广、支付结算等服务。

第九条 数据处理者应当采取备份、加密、访问控制等必要措施，保障数据免遭泄露、窃取、篡改、毁损、丢失、非法使用，应对数据安全事件，防范针对和利用数据的违法犯罪活动，维护数据的完整性、保密性、可用性。

数据处理者应当按照网络安全等级保护的要求，加强数据处理系统、数据传输网络、数据存储环境等安全防护，处理重要数据的系统原则上应当满足三级以上网络安全等级保护和关键信息基础设施安全保护要求，处理核心数据的系统依照有关规定从严保护。

数据处理者应当使用密码对重要数据和核心数据进行保护。

第十条 数据处理者发现其使用或者提供的网络产品和服务存在安全缺陷、漏洞，或者威胁国家安全、危害公共利益等风险时，应当立即采取补救措施。

第十一条 数据处理者应当建立数据安全应急处置机制，发生数据安全事件时及时启动应急响应机制，采取措施防止危害扩大，消除安全隐患。安全事件对个人、组织造成危害的，数据处理者应当在三个工作日内将安全事件和风险情况、危害后果、已经采取的补救措施等以电话、短信、即时通信工具、电子邮件等方式通知利害关系人，无法通知的可采取公告方式告知，法律、行政法规规定可以不通知的从其规定。安全事件涉嫌犯罪的，数据处理者应当按规定向公安机关报案。

发生重要数据或者十万人以上个人信息泄露、毁损、丢失等数据安全事件时，数据处理者还应当履行以下义务：

（一）在发生安全事件的八小时内向设区的市级网信部门和有关主管部门报告事件基本信息，包括涉及的数据数量、类型、可能的影响、已经或拟采取的处置措施等；

（二）在事件处置完毕后五个工作日内向设区的市级网信部门和有关主管部门报告包括事件原因、危害后果、责任处理、改进措施等情况的调查评估报告。

第十二条 数据处理者向第三方提供个人信息，或者共享、交易、委托处理重要数据的，应当遵守以下规定：

（一）向个人告知提供个人信息的目的、类型、方式、范围、存储期限、存储地点，并取得个人单独同意，符合法律、行政法规规定的不需要取得个人同意的情形或者经过匿名化处理的除外；

（二）与数据接收方约定处理数据的目的、范围、处理方式，数据安全保护措施等，通过合同等形式明确双方的数据安全责任义务，并对数据接收方的数据处理活动进行监督；

(三) 留存个人同意记录及提供个人信息的日志记录，共享、交易、委托处理重要数据的审批记录、日志记录至少五年。

数据接收方应当履行约定的义务，不得超出约定的目的、范围、处理方式处理个人信息和重要数据。

第十三条 数据处理者开展以下活动，应当按照国家有关规定，申报网络安全审查：

(一) 汇聚掌握大量关系国家安全、经济发展、公共利益的数据资源的互联网平台运营者实施合并、重组、分立，影响或者可能影响国家安全的；

(二) 处理一百万人以上个人信息的数据处理者赴国外上市的；

(三) 数据处理者赴香港上市，影响或者可能影响国家安全的；

(四) 其他影响或者可能影响国家安全的数据处理活动。

大型互联网平台运营者在境外设立总部或者运营中心、研发中心，应当向国家网信部门和主管部门报告。

第十四条 数据处理者发生合并、重组、分立等情况的，数据接收方应当继续履行数据安全保护义务，涉及重要数据和一百万人以上个人信息的，应当向设区的市级主管部门报告；数据处理者发生解散、被宣告破产等情况的，应当向设区的市级主管部门报告，按照相关要求移交或删除数据，主管部门不明确的，应当向设区的市级网信部门报告。

第十五条 数据处理者从其他途径获取的数据，应当按照本条例的规定履行数据安全保护义务。

第十六条 国家机关应当依照法律、行政法规的规定和国家标准的强制性要求，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。

第十七条 数据处理者在采用自动化工具访问、收集数据时，应当评估对网络服务的性能、功能带来的影响，不得干扰网络服务的正常功能。

自动化工具访问、收集数据违反法律、行政法规或者行业自律公约、影响网络服务正常功能，或者侵犯他人知识产权等合法权益的，数据处理者应当停止访问、收集数据行为并采取相应补救措施。

第十八条 数据处理者应当建立便捷的数据安全投诉举报渠道，及时受理、处置数据安全投诉举报。

数据处理者应当公布接受投诉、举报的联系方式、责任人信息，每年公开披露受理和收到的个人信息安全投诉数量、投诉处理情况、平均处理时间情况，接受社会监督。

第三章 个人信息保护

第十九条 数据处理者处理个人信息，应当具有明确、合理的目的，遵循合法、正当、必要的原则。基于个人同意处理个人信息的，应当满足以下要求：

（一）处理的个人信息是提供服务所必需的，或者是履行法律、行政法规规定的义务所必需的；

（二）限于实现处理目的最短周期、最低频次，采取对个人权益影响最小的方式；

（三）不得因个人拒绝提供服务必需的个人信息以外的信息，拒绝提供服务或者干扰个人正常使用服务。

第二十条 数据处理者处理个人信息，应当制定个人信息处理规则并严格遵守。个人信息处理规则应当集中公开展示、易于访问并置于醒目位置，内容明确具体、简明通俗，系统全面地向个人说明个人信息处理情况。

个人信息处理规则应当包括但不限于以下内容：

（一）依据产品或者服务的功能明确所需的个人信息，以清单形式列明每项功能处理个人信息的目的、用途、方式、种类、频次或者时机、保存地点等，以及拒绝处理个人信息对个人的影响；

(二) 个人信息存储期限或者个人信息存储期限的确定方法、到期后的处理方式;

(三) 个人查阅、复制、更正、删除、限制处理、转移个人信息, 以及注销账号、撤回处理个人信息同意的途径和方法;

(四) 以集中展示等便利用户访问的方式说明产品服务中嵌入的所有收集个人信息的第三方代码、插件的名称, 以及每个第三方代码、插件收集个人信息的目的、方式、种类、频次或者时机及其个人信息处理规则;

(五) 向第三方提供个人信息情形及其目的、方式、种类, 数据接收方相关信息等;

(六) 个人信息安全风险及保护措施;

(七) 个人信息安全问题的投诉、举报渠道及解决途径, 个人信息保护负责人联系方式。

第二十一条 处理个人信息应当取得个人同意的, 数据处理者应当遵守以下规定:

(一) 按照服务类型分别向个人申请处理个人信息的同意, 不得使用概括性条款取得同意;

(二) 处理个人生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等敏感个人信息应当取得个人单独同意;

(三) 处理不满十四周岁未成年人的个人信息, 应当取得其监护人同意;

(四) 不得以改善服务质量、提升用户体验、研发新产品等为由, 强迫个人同意处理其个人信息;

(五) 不得通过误导、欺诈、胁迫等方式获得个人的同意;

(六) 不得通过捆绑不同类型服务、批量申请同意等方式诱导、强迫个人进行批量个人信息同意;

(七) 不得超出个人授权同意的范围处理个人信息;

(八) 不得在个人明确表示不同意后，频繁征求同意、干扰正常使用服务。

个人信息处理目的、处理方式和处理的个人信息种类发生变更的，数据处理者应当重新取得个人同意，并同步修改个人信息处理规则。

对个人同意行为有效性存在争议的，数据处理者负有举证责任。

第二十二条 有下列情况之一的，数据处理者应当在十五个工作日内删除个人信息或者进行匿名化处理：

(一) 已实现个人信息处理目的或者实现处理目的不再必要；

(二) 达到与用户约定或者个人信息处理规则明确的存储期限；

(三) 终止服务或者个人注销账号；

(四) 因使用自动化采集技术等，无法避免采集到的非必要个人信息或者未经个人同意的个人信息。

删除个人信息从技术上难以实现，或者因业务复杂等原因，在十五个工作日内删除个人信息确有困难的，数据处理者不得开展除存储和采取必要的安全保护措施之外的处理，并应当向个人作出合理解释。

法律、行政法规另有规定的从其规定。

第二十三条 个人提出查阅、复制、更正、补充、限制处理、删除其个人信息的合理请求的，数据处理者应当履行以下义务：

(一) 提供便捷的支持个人结构化查询本人被收集的个人信息类型、数量等的方法和途径，不得以时间、位置等因素对个人的合理请求进行限制；

(二) 提供便捷的支持个人复制、更正、补充、限制处理、删除其个人信息、撤回授权同意以及注销账号的功能，且不得设置不合理条件；

(三) 收到个人复制、更正、补充、限制处理、删除本人个人信息、撤回授权同意或者注销账号申请的，应当在十五个工作日内处理并反馈。

法律、行政法规另有规定的从其规定。

第二十四条 符合下列条件的个人信息转移请求，数据处理者应当为个人指定的其他数据处理者访问、获取其个人信息提供转移服务：

- （一）请求转移的个人信息是基于同意或者订立、履行合同所必需而收集的个人信息；
- （二）请求转移的个人信息是本人信息或者请求人合法获得且不违背他人意愿的他人信息；
- （三）能够验证请求人的合法身份。

数据处理者发现接收个人信息的其他数据处理者有非法处理个人信息风险的，应当对个人信息转移请求做合理的风险提示。

请求转移个人信息次数明显超出合理范围的，数据处理者可以收取合理费用。

第二十五条 数据处理者利用生物特征进行个人身份认证的，应当对必要性、安全性进行风险评估，不得将人脸、步态、指纹、虹膜、声纹等生物特征作为唯一的个人身份认证方式，以强制个人同意收集其个人生物特征信息。

法律、行政法规另有规定的从其规定。

第二十六条 数据处理者处理一百万人以上个人信息的，还应当遵守本条例第四章对重要数据的处理者作出的规定。

第四章 重要数据安全

第二十七条 各地区、各部门按照国家有关要求和标准，组织本地区、本部门以及相关行业、领域的数据处理者识别重要数据和核心数据，组织制定本地区、本部门以及相关行业、领域重要数据和核心数据目录，并报国家网信部门。

第二十八条 重要数据的处理者，应当明确数据安全负责人，成立数据安全管理机构。数据安全管理机构在数据安全负责人的领导下，履行以下职责：

- （一）研究提出数据安全相关重大决策建议；
- （二）制定实施数据安全保护计划和数据安全事件应急预案；

- (三) 开展数据安全风险监测，及时处置数据安全风险和事件；
- (四) 定期组织开展数据安全宣传教育培训、风险评估、应急演练等活动；
- (五) 受理、处置数据安全投诉、举报；
- (六) 按照要求及时向网信部门和主管、监管部门报告数据安全情况。

数据安全负责人应当具备数据安全专业知识和相关管理工作经历，由数据处理器决策层成员承担，有权直接向网信部门和主管、监管部门反映数据安全情况。

第二十九条 重要数据的处理者，应当在识别其重要数据后的十五个工作日内向设区的市级网信部门备案，备案内容包括：

- (一) 数据处理者基本信息，数据安全管理机构信息、数据安全负责人姓名和联系方式等；
- (二) 处理数据的目的、规模、方式、范围、类型、存储期限、存储地点等，不包括数据内容本身；
- (三) 国家网信部门和主管、监管部门规定的其他备案内容。

处理数据的目的、范围、类型及数据安全防护措施等有重大变化的，应当重新备案。

依据部门职责分工，网信部门与有关部门共享备案信息。

第三十条 重要数据的处理者，应当制定数据安全培训计划，每年组织开展全员数据安全教育培训，数据安全相关的技术和管理人员每年教育培训时间不得少于二十小时。

第三十一条 重要数据的处理者，应当优先采购安全可信的网络产品和服务。

第三十二条 处理重要数据或者赴境外上市的数据处理者，应当自行或者委托数据安全服务机构每年开展一次数据安全评估，并在每年1月31日前将上一年度数据安全评估报告报设区的市级网信部门，年度数据安全评估报告的内容包括：

- (一) 处理重要数据的情况；
- (二) 发现的数据安全风险及处置措施；
- (三) 数据安全管理制度，数据备份、加密、访问控制等安全防护措施，以及管理制度实施情况和防护措施的有效性；
- (四) 落实国家数据安全法律、行政法规和标准情况；
- (五) 发生的数据安全事件及其处置情况；
- (六) 共享、交易、委托处理、向境外提供重要数据的安全评估情况；
- (七) 数据安全相关的投诉及处理情况；
- (八) 国家网信部门和主管、监管部门明确的其他数据安全情况。

数据处理者应当保留风险评估报告至少三年。

依据部门职责分工，网信部门与有关部门共享报告信息。

数据处理者开展共享、交易、委托处理、向境外提供重要数据的安全评估，应当重点评估以下内容：

- (一) 共享、交易、委托处理、向境外提供数据，以及数据接收方处理数据的目的、方式、范围等是否合法、正当、必要；
- (二) 共享、交易、委托处理、向境外提供数据被泄露、毁损、篡改、滥用的风险，以及对国家安全、经济发展、公共利益带来的风险；
- (三) 数据接收方的诚信状况、守法情况、境外政府机构合作关系、是否被中国政府制裁等背景情况，承诺承担的责任以及履行责任的能力等是否能够有效保障数据安全；
- (四) 与数据接收方订立的相关合同中关于数据安全的要求能否有效约束数据接收方履行数据安全保护义务；
- (五) 在数据处理过程中的管理和技术措施等是否能够防范数据泄露、毁损等风险。

评估认为可能危害国家安全、经济发展和公共利益，数据处理者不得共享、交易、委托处理、向境外提供数据。

第三十三条 数据处理者共享、交易、委托处理重要数据的，应当征得设区的市级以上主管部门同意，主管部门不明确的，应当征得设区的市级以上网信部门同意。

第三十四条 国家机关和关键信息基础设施运营者采购的云计算服务，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。

第五章 数据跨境安全管理

第三十五条 数据处理者因业务等需要，确需向中华人民共和国境外提供数据的，应当具备下列条件之一：

- (一) 通过国家网信部门组织的数据出境安全评估；
- (二) 数据处理者和数据接收方均通过国家网信部门认定的专业机构进行的个人信息保护认证；
- (三) 按照国家网信部门制定的关于标准合同的规定与境外数据接收方订立合同，约定双方权利和义务；
- (四) 法律、行政法规或者国家网信部门规定的其他条件。

数据处理者为订立、履行个人作为一方当事人的合同所必需向境外提供当事人个人信息的，或者为了保护个人生命健康和财产安全而必须向境外提供个人信息的除外。

第三十六条 数据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数据接收方的名称、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数据接收方行使个人信息权利的方式等事项，并取得个人的单独同意。

收集个人信息时已单独就个人信息出境取得个人同意，且按照取得同意的事项出境的，无需再次取得个人单独同意。

第三十七条 数据处理者向境外提供在中华人民共和国境内收集和产生的数据，属于以下情形的，应当通过国家网信部门组织的数据出境安全评估：

- （一）出境数据中包含重要数据；
- （二）关键信息基础设施运营者和处理一百万人以上个人信息的数据处理者向境外提供个人信息；
- （三）国家网信部门规定的其它情形。

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。

第三十八条 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件等有规定的，可以按照其规定执行。

第三十九条 数据处理者向境外提供数据应当履行以下义务：

- （一）不得超出报送网信部门的个人信息保护影响评估报告中明确的目的、范围、方式和数据类型、规模等向境外提供个人信息；
- （二）不得超出网信部门安全评估时明确的出境目的、范围、方式和数据类型、规模等向境外提供个人信息和重要数据；
- （三）采取合同等有效措施监督数据接收方按照双方约定的目的、范围、方式使用数据，履行数据安全保护义务，保证数据安全；
- （四）接受和处理数据出境所涉及的用户投诉；
- （五）数据出境对个人、组织合法权益或者公共利益造成损害的，数据处理者应当依法承担责任；
- （六）存留相关日志记录和数据出境审批记录三年以上；
- （七）国家网信部门会同国务院有关部门核验向境外提供个人信息和重要数据的类型、范围时，数据处理者应当以明文、可读方式予以展示；
- （八）国家网信部门认定不得出境的，数据处理者应当停止数据出境，并采取有效措施对已出境数据的安全予以补救；

(九) 个人信息出境后确需再转移的, 应当事先与个人约定再转移的条件, 并明确数据接收方履行的安全保护义务。

非经中华人民共和国主管机关批准, 境内的个人、组织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。

第四十条 向境外提供个人信息和重要数据的数据处理者, 应当在每年1月31日前编制数据出境安全报告, 向设区的市级网信部门报告上一年度以下数据出境情况:

- (一) 全部数据接收方名称、联系方式;
- (二) 出境数据的类型、数量及目的;
- (三) 数据在境外的存放地点、存储期限、使用范围和方式;
- (四) 涉及向境外提供数据的用户投诉及处理情况;
- (五) 发生的数据安全事件及其处置情况;
- (六) 数据出境后再转移的情况;
- (七) 国家网信部门明确向境外提供数据需要报告的其他事项。

第四十一条 国家建立数据跨境安全网关, 对来源于中华人民共和国境外、法律和行政法规禁止发布或者传输的信息予以阻断传播。

任何个人和组织不得提供用于穿透、绕过数据跨境安全网关的程序、工具、线路等, 不得为穿透、绕过数据跨境安全网关提供互联网接入、服务器托管、技术支持、传播推广、支付结算、应用下载等服务。

境内用户访问境内网络的, 其流量不得被路由至境外。

第四十二条 数据处理者从事跨境数据活动应当按照国家数据跨境安全监管要求, 建立健全相关技术和管理措施。

第六章 互联网平台运营者义务

第四十三条 互联网平台运营者应当建立与数据相关的平台规则、隐私政策和算法策略披露制度，及时披露制定程序、裁决程序，保障平台规则、隐私政策、算法公平公正。

平台规则、隐私政策制定或者对用户权益有重大影响的修订，互联网平台运营者应当在其官方网站、个人信息保护相关行业协会互联网平台面向社会公开征求意见，征求意见时长不得少于三十个工作日，确保用户能够便捷充分表达意见。互联网平台运营者应当充分采纳公众意见，修改完善平台规则、隐私政策，并以易于用户访问的方式公布意见采纳情况，说明未采纳的理由，接受社会监督。

日活用户超过一亿的大型互联网平台运营者平台规则、隐私政策制定或者对用户权益有重大影响的修订的，应当经国家网信部门认定的第三方机构评估，并报省级及以上网信部门和电信主管部门同意。

第四十四条 互联网平台运营者应当对接入其平台的第三方产品和服务承担数据安全责任，通过合同等形式明确第三方的数据安全责任义务，并督促第三方加强数据安全，采取必要的数据安全保护措施。

第三方产品和服务对用户造成损害的，用户可以要求互联网平台运营者先行赔偿。

移动通信终端预装第三方产品适用本条前两款规定。

第四十五条 国家鼓励提供即时通信服务的互联网平台运营者从功能设计上为用户提供个人通信和非个人通信选择。个人通信的信息按照个人信息保护要求严格保护，非个人通信的信息按照公共信息有关规定进行管理。

第四十六条 互联网平台运营者不得利用数据以及平台规则等从事以下活动：

（一）利用平台收集掌握的用户数据，无正当理由对交易条件相同的用户实施产品和服务差异化定价等损害用户合法利益的行为；

（二）利用平台收集掌握的经营者数据，在产品推广中实行最低价销售等损害公平竞争的行为；

(三) 利用数据误导、欺诈、胁迫用户，损害用户对其数据被处理的决定权，违背用户意愿处理用户数据；

(四) 在平台规则、算法、技术、流量分配等方面设置不合理的限制和障碍，限制平台上的中小企业公平获取平台产生的行业、市场数据等，阻碍市场创新。

第四十七条 提供应用程序分发服务的互联网平台运营者，应当按照有关法律、行政法规和国家网信部门的规定，建立、披露应用程序审核规则，并对应用程序进行安全审核。对不符合法律、行政法规的规定和国家标准的强制性要求的应用程序，应当采取拒绝上架、督促整改、下架处置等措施。

第四十八条 互联网平台运营者面向公众提供即时通信服务的，应当按照国务院电信主管部门的规定，为其他互联网平台运营者的即时通信服务提供数据接口，支持不同即时通信服务之间用户数据互通，无正当理由不得限制用户访问其他互联网平台以及向其他互联网平台传输文件。

第四十九条 互联网平台运营者利用个人信息和个性化推送算法向用户提供信息的，应当对推送信息的真实性、准确性以及来源合法性负责，并符合以下要求：

(一) 收集个人信息用于个性化推荐时，应当取得个人单独同意；

(二) 设置易于理解、便于访问和操作的一键关闭个性化推荐选项，允许用户拒绝接受定向推送信息，允许用户重置、修改、调整针对其个人特征的定向推送参数；

(三) 允许个人删除定向推送信息服务收集产生的个人信息，法律、行政法规另有规定或者与用户另有约定的除外。

第五十条 国家建设网络身份认证公共服务基础设施，按照政府引导、网民自愿原则，提供个人身份认证公共服务。

互联网平台运营者应当支持并优先使用国家网络身份认证公共服务基础设施提供的个人身份认证服务。

第五十一条 互联网平台运营者在为国家机关提供服务，参与公共基础设施、公共服务系统建设运维管理，利用公共资源提供服务过程中收集、产生的数据不得用于其他用途。

第五十二条 国务院有关部门履行法定职责需要调取或者访问互联网平台运营者掌握的公共数据、公共信息，应当明确调取或者访问的范围、类型、用途、依据，严格限定在履行法定职责范围内，不得将调取或者访问的公共数据、公共信息用于履行法定职责之外的目的。

互联网平台运营者应当对有关部门调取或者访问公共数据、公共信息予以配合。

第五十三条 大型互联网平台运营者应当通过委托第三方审计方式，每年对平台数据安全情况、平台规则和自身承诺的执行情况、个人信息保护情况、数据开发利用情况等进行年度审计，并披露审计结果。

第五十四条 互联网平台运营者利用人工智能、虚拟现实、深度合成等新技术开展数据处理活动的，应当按照国家有关规定进行安全评估。

第七章 监督管理

第五十五条 国家网信部门负责统筹协调数据安全和相关监督管理工作。

公安机关、国家安全机关等在各自职责范围内承担数据安全监管职责。

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。

主管部门应当明确本行业、本领域数据安全保护工作机构和人员，编制并组织实施本行业、本领域的数据安全规划和数据安全事件应急预案。

主管部门应当定期组织开展本行业、本领域的数据安全风险评估，对数据处理者履行数据安全保护义务情况进行监督检查，指导督促数据处理者及时对存在的风险隐患进行整改。

第五十六条 国家建立健全数据安全应急处置机制，完善网络安全事件应急预案和网络安全信息共享平台，将数据安全事件纳入国家网络安全事件应急响应机制，加强数据安全信息共享、数据安全风险和威胁监测预警以及数据安全事件应急处置工作。

第五十七条 有关主管、监管部门可以采取以下措施对数据安全进行监督检查：

- （一）要求数据处理者相关人员就监督检查事项作出说明；
- （二）查阅、调取与数据安全有关的文档、记录；
- （三）按照规定程序，利用检测工具或者委托专业机构对数据安全措施运行情况进行技术检测；
- （四）核验数据出境类型、范围等；
- （五）法律、行政法规、规章规定的其他必要方式。

有关主管、监管部门开展数据安全监督检查，应当客观公正，不得向被检查单位收取费用。在数据安全监督检查中获取的信息只能用于维护数据安全的需要，不得用于其他用途。

数据处理者应当对有关主管、监管部门的数据安全监督检查予以配合，包括对组织运作、技术系统、算法原理、数据处理程序等进行解释说明，开放安全相关数据访问、提供必要技术支持等。

第五十八条 国家建立数据安全审计制度。数据处理者应当委托数据安全审计专业机构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。

主管、监管部门组织开展对重要数据处理活动的审计，重点审计数据处理者履行法律、行政法规规定的义务等情况。

第五十九条 国家支持相关行业组织按照章程，制定数据安全行为规范，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。

国家支持成立个人信息保护行业组织，开展以下活动：

- （一）接受个人信息保护投诉举报并进行调查、调解；
- （二）向个人提供信息和咨询服务，支持个人依法对损害个人信息权益的行为提起诉讼；
- （三）曝光损害个人信息权益的行为，对个人信息保护开展社会监督；
- （四）向有关部门反映个人信息保护情况、提供咨询、建议；
- （五）违法处理个人信息、侵害众多个人的权益的行为，依法向人民法院提起诉讼。

第八章 法律责任

第六十条 数据处理者不履行第九条、第十条、第十一条、第十二条、第十三条、第十四条、第十五条、第十八条的规定，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；拒不改正或者导致危害数据安全等严重后果的，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。

第六十一条 数据处理者不履行第十九条、第二十条、第二十一条、第二十二条、第二十三条、第二十四条、第二十五条规定的数据安全保护义务的，由有关部门责令改正，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，由有关部门责令改正，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，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。

第六十二条 数据处理者不履行第二十八条、第二十九条、第三十条、第三十一条、第三十二条、第三十三条规定的数据安全保护义务的，由有关部门责令改正，给予警告，对违法处理重要数据的系统及应用，责令暂停或者终止提供服务；拒不改正的，并处二百万元以下罚款，对直接负责的主管人员和其他直接责任人员处五万元以上二十万元以下罚款。

有前款规定的违法行为，情节严重的，由有关部门责令改正，没收违法所得，并处二百万元以上五百万元以下罚款，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二十万元以上一百万元以下罚款。

第六十三条 关键信息基础设施运营者违反第三十四条的规定，由有关部门责令改正，依照有关法律、行政法规的规定予以处罚。

第六十四条 数据处理者违反第三十五条、第三十六条、第三十七条、第三十九条第一款、第四十条、第四十二条的规定，由有关部门责令改正，给予警告，暂停数据出境，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。

第六十五条 违反本条例第三十九条第二款的规定，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。

第六十六条 个人和组织违反第四十一条的规定，由有关主管部门责令改正，给予警告、没收违法所得；拒不改正的，处违法所得一倍以上十倍以下的罚款，没有违法所得的，对直接负责的主管人员和其他直接负责人员，处五万元以上五十万元以下罚款；情节严重的，由有关主管部门依照相关法律、行政法规的规定，责令其暂停相关业务、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，依照相关法律、行政法规的规定处罚。

第六十七条 互联网平台运营者违反第四十三条、第四十四条、第四十五条、第四十七条、第五十三条的规定，由有关部门责令改正，予以警告；拒不改正，处五十万元以上五百万元以下罚款，对直接负责的主管人员和其他直接负责人员，处五万元以上五十万元以下罚款；情节严重的，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。

第六十八条 互联网平台运营者违反第四十六条、第四十八条、第五十一条的规定，由有关主管部门责令改正，给予警告；拒不改正的，处上一年度销售额百分之一以上百分之五以下的罚款；情节严重的，由有关主管部门依照相关法律、行政法规的规定，责令其暂停相关业务、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，依照相关法律、行政法规的规定处罚。

第六十九条 互联网平台运营者违反第四十九条、第五十四条的规定，由有关主管部门责令改正，予以警告；拒不改正，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；情节严重的，可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。

第七十条 数据处理者违反本条例规定，给他人造成损害的，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。

第七十一条 国家机关不履行本法规定的数据安全保护义务的，由其上级机关或者履行数据安全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。

第七十二条 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。

第九章 附则

第七十三条 本条例下列用语的含义：

（一）网络数据（简称数据）是指任何以电子方式对信息的记录。

（二）数据处理活动是指数据收集、存储、使用、加工、传输、提供、公开、删除等活动。

（三）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、公共利益的数据。包括以下数据：

1.未公开的政务数据、工作秘密、情报数据和执法司法数据；

2.出口管制数据，出口管制物项涉及的核心技术、设计方案、生产工艺等相关的数据，密码、生物、电子信息、人工智能等领域对国家安全、经济竞争实力有直接影响的科学技术成果数据；

3.国家法律、行政法规、部门规章明确规定需要保护或者控制传播的国家经济运行数据、重要行业业务数据、统计数据等；

4.工业、电信、能源、交通、水利、金融、国防科技工业、海关、税务等重点行业和领域安全生产、运行的数据，关键系统组件、设备供应链数据；

5.达到国家有关部门规定的规模或者精度的基因、地理、矿产、气象等人口与健康、自然资源与环境国家基础数据；

6.国家基础设施、关键信息基础设施建设运行及其安全数据，国防设施、军事管理区、国防科研生产单位等重要敏感区域的地理位置、安保情况等数据；

7.其他可能影响国家政治、国土、军事、经济、文化、社会、科技、生态、资源、核设施、海外利益、生物、太空、极地、深海等安全的数据。

（四）核心数据是指关系国家安全、国民经济命脉、重要民生和重大公共利益等的的数据。

(五) 数据处理者是指在数据处理活动中自主决定处理目的和处理方式的个人和组织。

(六) 公共数据是指国家机关和法律、行政法规授权的具有管理公共事务职能的组织履行公共管理职责或者提供公共服务过程中收集、产生的各类数据，以及其他组织在提供公共服务中收集、产生的涉及公共利益的各类数据。

(七) 委托处理是指数据处理者委托第三方按照约定的目的和方式开展的数据处理活动。

(八) 单独同意是指数据处理者在开展具体数据处理活动时，对每项个人信息取得个人同意，不包括一次性针对多项个人信息、多种处理活动的同意。

(九) 互联网平台运营者是指为用户提供信息发布、社交、交易、支付、视听等互联网平台服务的数据处理者。

(十) 大型互联网平台运营者是指用户超过五千万、处理大量个人信息和重要数据、具有强大社会动员能力和市场支配地位的互联网平台运营者。

(十一) 数据跨境安全网关是指阻断访问境外反动网站和有害信息、防止来自境外的网络攻击、管控跨境网络数据传输、防范侦查打击跨境网络犯罪的重要安全基础设施。

(十二) 公共信息是指数据处理者在提供公共服务过程中收集、产生的具有公共传播特性的信息。包括公开发布信息、可转发信息、无明确接收人信息等。

第七十四条 涉及国家秘密信息、核心数据、密码使用的数据处理活动，按照国家有关规定执行。

第七十五条 本条例自 年 月 日起施行。

(三) 儿童个人信息网络保护规定

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

第一条 为了保护儿童个人信息安全，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；
- （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。

(四) 邮政业寄递安全监督管理办法

中华人民共和国交通运输部令（2020年第1号）

《邮政业寄递安全监督管理办法》已于2019年12月18日经第30次部务会议通过，现予公布，自2020年2月15日起施行。

部长 李小鹏

2020年1月2日

第一条 为加强邮政业寄递安全管理，维护邮政通信与信息安全，保障从业人员、用户人身和财产安全，促进邮政业持续健康发展，根据《中华人民共和国邮政法》、《快递暂行条例》等法律、行政法规，制定本办法。

第二条 在中华人民共和国境内经营邮政业务、快递业务，接受邮政服务、快递服务以及对邮政业寄递安全实施监督管理，适用本办法。

第三条 国务院邮政管理部门和省、自治区、直辖市邮政管理机构以及按照国务院规定设立的省级以下邮政管理机构（以下统称邮政管理部门）负责邮政业寄递安全监督管理工作。

第四条 邮政管理部门应当与有关部门相互配合，健全安全保障机制，加强对邮政业寄递安全的监督管理。

第五条 邮政企业、快递企业应当遵守国家有关安全管理的规定，不得危害国家安全、社会公共利益或者他人合法权益。

第六条 使用统一的商标、字号或者快递运单经营快递业务的，商标、字号或者快递运单所属企业应当对使用其商标、字号或者快递运单的企业的安全保障实行统一管理，监督使用其商标、字号或者快递运单的企业执行邮政业安全管理制度。

第七条 用户交寄邮件、快件应当遵守国家关于禁止寄递或者限制寄递物品的规定，不得利用邮件、快件危害国家安全、社会公共利益或者他人合法权益。

第八条 任何单位或者个人不得冒领、私自开拆、隐匿、毁弃、倒卖或者非法检查、非法扣留他人邮件、快件，不得损毁邮政设施、快递设施或者影响设施的正常使用。

第九条 交寄、收寄邮件、快件，应当遵守实名收寄管理制度。

第十条 邮政企业、快递企业应当依法验视用户交寄的物品是否属于禁止寄递或者限制寄递的物品，核对物品的名称、性质、数量等是否与寄递详情单显示或者关联的信息一致；予以收寄的，应当按照国务院邮政管理部门的规定作出验视标识。

按照国家规定需要用户提供有关书面凭证的，邮政企业、快递企业应当要求用户提供凭证原件，核对无误后，方可收寄。

第十一条 邮政企业、快递企业在收寄过程中发现禁止寄递物品的，应当拒绝收寄；发现已经收寄的邮件、快件中有疑似禁止寄递物品的，应当立即停止分拣、运输、投递。对邮件、快件中依法应当没收、销毁或者可能涉及违法犯罪的物品，应当立即向有关部门报告，并配合调查处理；对其他禁止寄递物品、限制寄递物品或者一同查处的禁止寄递物品之外的物品，邮政企业、快递企业应当通知寄件人或者收件人，并依法妥善处理。

第十二条 邮政企业、快递企业应当按照国务院邮政管理部门的规定对邮件、快件进行安全检查，并对经过安全检查的邮件、快件作出安全检查标识。委托第三方企业对邮件、快件进行安全检查的，不免除邮政企业、快递企业对邮件、快件安全承担的责任。

邮政企业、快递企业或者接受委托的第三方企业应当使用符合强制性国家标准的安全检查设备，并加强对安全检查人员的背景审查和技术培训，确保其具备安全检查所必须的知识和技能。

第十三条 邮政企业委托其他单位代办邮政服务的，或者经营快递业务的企业及其分支机构与其他单位、个人合作开办末端网点的，应当对收寄、投递邮件、快件的人员进行岗位安全操作规程和安全操作技能的教育和培训。

第十四条 邮政企业、快递企业应当依法向从业人员提供符合相关国家标准或者行业标准的劳动防护用品，为从业人员参加工伤保险。

第十五条 邮政企业、快递企业向寄件人长期、批量提供寄递服务的，应当与寄件人签订安全协议，明确自身与签订安全协议的寄件人（以下简称协议用户）的安全保障义务。

邮政企业、快递企业发现用户生产、销售的产品属于禁止寄递物品的，不得将其作为协议用户提供寄递服务。

第十六条 邮政企业、快递企业和用户应当依照法律、行政法规的规定，防止邮件、快件过度包装，减少包装废弃物。

鼓励邮政企业、快递企业采取措施回收邮件、快件包装材料，实现包装材料的减量化利用和再利用。

第十七条 邮政企业、快递企业应当使用环保材料对邮件、快件进行包装。

第十八条 邮件、快件塑料包装袋、普通胶带中的铅、汞、镉、铬总量以及邮件、快件塑料包装袋中的苯类溶剂残留应当符合国家规定。

第十九条 协议用户提供邮件、快件封装用品和胶带的，邮政企业、快递企业应当向其书面告知，所提供的封装用品和胶带应当符合国家规定。

第二十条 邮政企业、快递企业不得使用有毒物质作为邮件、快件填充材料。

第二十一条 邮政企业、快递企业应当对其提供寄递服务的营业场所、处理场所，包括其开办的快递末端网点、设置的智能快件箱进行全天候视频监控。其中，营业场所、快递末端网点、智能快件箱的视频监控设备应当全面覆盖，处理场所的视频监控设备应当覆盖各出入口、主要生产作业区域。

邮政企业、快递企业保存监控资料的时间不得少于30日。其中，营业场所交寄、接收、验视、安检、提取区域以及智能快件箱放置区域的监控资料保存时间不得少于90日。

邮政企业、快递企业应当按照邮政管理部门的要求报送监控资料。

第二十二條 郵政企業、快遞企業應當按照國家網絡安全等級保護制度的要求，履行下列安全保護義務，保障其網絡免受干擾、破壞或者未經授權的訪問，防止網絡數據泄露或者被竊取、篡改：

（一）制定內部安全管理制度和操作规程，確定網絡安全負責人，落實網絡安全保護責任；

（二）採取防范計算機病毒和網絡攻擊、網絡侵入等危害網絡安全行為的技術措施；

（三）採取監測、記錄網絡運行狀態、網絡安全事件的技术措施，並按照規定留存相關的網絡日志不少於6個月；

（四）採取數據分類、重要數據備份和加密等措施；

（五）法律、行政法規規定的其他義務。

第二十三條 郵政企業、快遞企業應當建立寄遞詳情單及電子數據管理制度，定期銷毀已經使用過的寄遞詳情單，妥善保管用戶信息等電子數據，採取有效手段保證用戶信息安全。

第二十四條 未經法律明確授權或者用戶書面同意，郵政企業、快遞企業及其從業人員不得將用戶身份信息以及用戶使用郵政服務、快遞服務的信息提供給任何單位或者個人。

發生或者可能發生用戶信息泄露、丟失等情況時，郵政企業、快遞企業應當立即採取補救措施，並向事件所在地郵政管理部門報告，配合有關部門進行調查處理。

第二十五條 郵政企業、快遞企業應當按照郵政管理部門的規定預留安全監管數據接口，收集、分析與寄遞安全有關的信息，確保數據真實、完整，並按時向郵政管理部門報送。

第二十六條 國務院郵政管理部門應當加強應急管理體系建設，制定國家郵政業突發事件應急預案，建立突發事件預防、監測、預警、信息報告、應急處置等工作機制。

省、自治区、直辖市邮政管理机构和省级以下邮政管理机构应当根据有关法律、法规、规章以及国家邮政业突发事件应急预案等，结合本地区的实际情况，制定突发事件应急预案。

邮政管理部门应当根据邮政业应急管理的实际需要和情势变化，适时评估、修订突发事件应急预案。

第二十七条 鼓励邮政企业、快递企业建立应急救援队伍，预防与处置突发事件。

第二十八条 发生自然灾害、事故灾难、公共卫生事件、社会安全事件等，邮政企业、快递企业应当根据法律、法规、规章以及国家邮政业突发事件应急预案，按照事件类型及分级，在规定时间内报告事件发生地省级以下邮政管理机构和负有相关职责的部门，同时对事件进行先行处置，控制事态发展。

第二十九条 事件发生地省级以下邮政管理机构接到突发事件报告后，依法启动应急预案，采取应急措施。

第三十条 邮政管理部门应当妥善处置邮政业突发事件，查明事件原因和责任，提出整改措施，并依法对有违法行为的责任人作出处理。涉及其他部门管理职权的，应当联合有关部门共同处理。

第三十一条 邮政管理部门应当加强邮政业安全运行的监测预警，建立安全信息管理体系，收集、分析与邮政业安全运行有关的信息，并依照法律、行政法规等规定，与有关部门共享与安全运行有关的信息。

第三十二条 邮政管理部门应当加强对邮政企业、快递企业建立健全和执行寄递安全制度、应急管理制度等情况以及安全生产行为的监督检查。建立和完善以随机抽查为重点的日常监督检查制度，建立随机抽查事项清单，公布抽查的安全事项目录，明确抽查的依据、频次、方式、内容和程序，随机抽取被检查企业，随机选派检查人员，建立检查对象名录库和执法检查人员名录库。抽查情况和查处结果依法向社会公布。

第三十三条 邮政管理部门可以依照《中华人民共和国行政处罚法》的规定，

委托依法成立并符合法定条件的管理公共事务的事业组织实施邮政行政处罚相关工作。

邮政管理部门可以委托符合法定条件的专业技术组织检验、检测邮件快件的处理设施、处理设备、封装用品、填充材料等邮政业用品用具。

第三十四条 邮政安全监督检查人员应当将检查的时间、地点、内容、发现的问题及其处理情况作出书面记录，并由监督检查人员和被检查单位的负责人签字；被检查单位负责人拒绝签字的，监督检查人员应当将情况记录在案，并向邮政管理部门报告。

第三十五条 邮政企业、快递企业应当配合邮政管理部门的安全监督检查，不得拒绝、阻碍。

第三十六条 邮政管理部门应当记录邮政企业、快递企业违法失信行为信息，并纳入邮政业信用管理，依法实施联合惩戒措施。

邮政管理部门依法通报邮政企业、快递企业违反安全监管有关规定、发生安全事件以及对有关责任人员进行处理的情况。对违法行为情节严重的单位，应当依法向社会公告，并通报有关部门和机构。

第三十七条 邮政企业、快递企业违反本办法第十条第一款、第十二条第一款规定，未按照国务院邮政管理部门的规定作出收寄验视标识、安全检查标识的，由邮政管理部门责令限期改正；逾期未改正的，处5000元以下的罚款。

第三十八条 邮政企业、快递企业违反本办法第十八条、第二十条规定，使用塑料包装袋、普通胶带不符合国家规定，或者使用有毒物质作为邮件、快件填充材料的，由邮政管理部门责令限期改正；逾期未改正的，处5000元以上1万元以下的罚款。

第三十九条 邮政企业、快递企业违反本办法第十九条规定，未向协议用户书面告知对封装用品和胶带的要求的，由邮政管理部门责令限期改正，可以处5000元以下的罚款。

第四十条 邮政企业、快递企业违反本办法第二十一条第一款、第二款规定，

未对其提供寄递服务的营业场所、处理场所、快递末端网点、设置的智能快件箱在规定的覆盖范围内进行全天候视频监控或者保存监控资料不符合规定期限的，由邮政管理部门责令限期改正；逾期未改正的，处1万元以下的罚款。

第四十一条 邮政企业、快递企业违反本办法第二十一条第三款、第二十五条规定，未按照要求报送资料、信息、数据的，由邮政管理部门责令限期改正；逾期未改正的，处3000元以下的罚款。

第四十二条 国家关于机要通信安全监督管理另有规定的，适用其规定。

第四十三条 本办法自2020年2月15日起施行。交通运输部于2011年1月4日以交通运输部令2011年第2号公布、2013年4月12日以交通运输部令2013年第6号修改的《邮政行业安全监督管理办法》同时废止。

(五) 网络安全标准实践指南——移动互联网应用程序(App)个人信息安全防范指引(征求意见稿)

1.1 范围

本文件规定了依据 GB/T 35273—2020《信息安全技术 个人信息安全规范》开展 App 个人信息安全测评的实施过程以及对各项具体安全要求进行测评的方法。

本文件适用于指导第三方测评机构对 App 个人信息安全进行测评，也适用于主管监管部门对 App 个人信息安全进行监督管理，还适用于 App 提供者开展个人信息安全自评时参考。

2.1 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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—2020 信息安全技术 个人信息安全规范

GB/T AAAA—BBBB 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

术语和定义

GB/T 25069—2010 和 GB/T 35273—2020 中界定的以及下列术语和定义适用于本文件。

3.1 移动互联网应用程序 mobile internet application

通过预装、下载等方式获取并运行在移动智能终端上，向用户提供服务的应用软件，简称 App。

3.2 移动互联网应用程序提供者 mobile internet application provider

移动互联网应用程序所有者或运营者，简称 App 提供者。

3.3 软件开发工具包 software development kit

辅助开发某一类软件的相关二进制文件、文档、范例和工具的集合，简称 SDK。

3.4 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，术语和定义 3.1]

注：个人信息的范围和类型参见 GB/T 35273—2020 附录 A。

3.5 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，术语和定义 3.2]

注：个人敏感信息的范围和类型参见 GB/T 35273—2020 附录 B。

3.6 个人信息保护政策 personal information protection policy

说明 App 收集、使用、传输、存储和删除个人信息的情况，以及用户享有的相关权利等收集使用个人信息规则的文本。

注 1：个人信息保护政策应包含的内容请参见 GB/T 35273—2020 5.5。

注 2：App 提供者习惯性将个人信息保护政策命名为『隐私政策』或其他名称。

3.7 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。

[GB/T 35273—2020，术语和定义 3.16]

3.8 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。

[GB/T 35273—2020, 术语和定义 3.17]

3.9 可收集个人信息权限 system permissions to access personal information

移动智能终端操作系统向 App 开放的，具有收集个人信息能力的系统权限，简称系统权限或权限。

[GB/T AAAA—BBBB, 术语和定义 3.10]

3.10 权限申请 system permission request

向移动智能终端操作系统声明，并向用户请求授权，以获得对移动智能终端数据或能力的访问许可的过程。

[GB/T AAAA—BBBB, 术语和定义 3.15]

3.11 测评对象 target of testing and evaluation

App 个人信息安全测评过程中不同测评方式作用的对象，主要涉及 App、App 服务端、相关文档资料等。

3.12 测评单元 testing and evaluation unit

对测评过程进行划分的最小独立单元，每个测评单元包括指标要求、测评对象、测评方式、测评步骤、单元判定等 5 项内容，可独立验证符合性。

缩略语

以下缩略语适用于本文件。

IMEI：国际移动设备识别码（International Mobile Equipment Identity）

MAC：媒体访问控制地址（Media Access Control Address）

IDFA: 广告标识符 (Identifier For Advertising)

IMSI: 国际移动用户识别码 (International Mobile Subscriber Identity)

API: 应用程序编程接口 (Application Programming Interface)

SDK: 软件开发工具包 (Software Development Kit)

测评过程

5.1 概述

App 个人信息安全测评主要针对 App、App 服务端和相关文档资料开展, 测评过程包含测评准备阶段、测评实施阶段、测评结果判定阶段和测评报告编写阶段, 如图 1 所示。



图 1 App 个人信息安全测评实施过程图

5.2 实施过程

5.2.1 测评准备

在测评准备阶段, 测评人员需完成的工作主要包括:

- a) App 提供者基本信息的收集与分析。测评人员应要求被测 App 提供者提供被测 App 样本、App 功能说明、App 收集使用个人信息情况说明等材料 (提交材料内容可参考附录 A)。为提高测评结果的准确性, 对于有特殊登录需求的 App, 测评人员宜要求被测 App 提供者提供对应登录账号;

- b) 测评工具和测评表单准备。测评人员应根据 App 提供者基本信息的收集与分析，初步确定测评工作中所使用的测评工具和测评记录表；
- c) 测评对象和测评内容确定。测评人员应根据 App 提供者基本信息的收集与分析，确定测评工作的具体测评对象，例如需验证的 App 功能范围、需查看的制度文档、需核查的服务端系统、需访谈的人员岗位等；
- d) 测评方案编制。测评人员应编制 App 个人信息安全测评方案，方案内容应涵盖测评对象、测评依据、测评内容、测评方法、测评工具、测评计划等。方案编制过程中，根据具体情况，测评人员可能还需要 App 提供者提供额外的信息材料或需要进行现场调研。

5.2.2 测评实施

在测评实施阶段，测评人员需完成的工作主要包括：

- a) 测评实施环境准备。开始实施测评时，测评人员应进行技术检测工具的部署和调试，保障技术检测工具输出结果的可靠性；
- b) 工具和人工测评及结果导出和记录。测评人员按照本文件第 6 章规定的测评方法实施测评，并将测评过程中获取的证据进行详细、准确的导出、记录；
- c) 结果确认及资料归还。测评实施阶段完成时，测评人员应与被测 App 提供者确认测评实施阶段全部完成且形成了对应的测评记录，并确认测评实施阶段记录的证据的准确性。确认测评实施动作完成后，测评人员应归还被测 App 的相关资料、移交相关权限。

5.2.3 测评结果判定

在测评结果判定阶段，测评人员对测评实施阶段所形成的证据进行分析，需完成的工作主要包括：

- a) 测评单元结果判定。测评人员首先应通过证据分析，给出每一个测评单元的判定结果；

- b) 测评项结果判定。测评人员根据测评单元的判定结果确定每一个测评项的判定结果；
- c) 整体测评结果判定。测评人员根据测评项的判定结果确定 App 个人信息安全测评的整体结果；
- d) 输出测评结论。测评人员根据整体测评结果给出 App 个人信息安全测评的结论。

5.2.4 测评报告编写

在测评报告编写阶段，测评人员根据App个人信息安全测评记录和结果判定，编制测评报告。测评报告应包括但不限于以下内容：

- a) 被测评对象信息，包括 App 名称、版本号、操作系统平台、运营机构信息等；
- b) 测评机构和测评人员信息，包括测评机构名称、测评人员名称等；
- c) 测评环境信息，包括测评地点、测评时间、测评工具等；
- d) 测评总体结论，包括测评范围、测评项总体符合情况、测评项符合率、测评是否通过等；
- e) 测评项符合情况，包括每个测评项的测评过程简述、符合情况判定等。

5.3 测评方式

测评人员宜综合采用文档审查、服务端核查、功能验证、技术检测、人员访谈等测评方式，以测评App个人信息安全性。

- a) 文档审查。为了分析 App 现有的或计划采取的个人信息安全保护措施，需要查看各类文档资料，包括策略文档（例如政策法规、指导性文档、组织管理制度等）、系统文档（例如用户手册、管理员手册、系统设计和需求文档、接口文档等）和个人信息安全相关文档（例如个人信息安全影响评估报告、审计报告、风险评估报告、安全测试报告、安全策略、应急预案、个人信息共享合同、个人信息处理记录等）等；

- b) 服务端核查。测评人员在 App 服务端核查个人信息安全相关配置情况和个人信息处理活动，寻找是否有违反个人信息安全策略的现象，比如个人敏感信息在显示时未进行脱敏、数据库访问未进行正确的权限设置和记录等；根据服务端核查，核实个人信息安全相关制度的落实情况；
- c) 功能验证。对 App 进行操作试用，以验证其在个人信息主体权利保障方面的行为情况；功能验证主要依据 App 在运行时通过功能界面显示的信息；
- d) 技术检测。技术检测是指测评人员通过 App 个人信息安全检测工具获得 App 未在功能界面显示的相关信息，并进行分析以帮助测评人员获取证据的过程；
- e) 人员访谈。测评人员与被测评 App 内有关的管理、技术人员进行逐个沟通。根据对测评人员所提问题的回答，测评人员为测评获得相应信息，并可验证之前收集到的证据，从而提高其准确度和完整性。通过访谈管理和技术人员，测评人员可以收集到 App 相关的个人信息安全管理组织结构、个人信息共享、交换行为等信息，也可以了解到被访谈者的个人信息安全意识和个人信息安全技能等自身素质。

测评方法

6.1 个人信息的收集的测评

6.1.1 收集个人信息的合法性的测评

6.1.1.1 测评项：详见 GB/T 35273—2020 中 5.1 的 a) 。

6.1.1.1.1 测评单元 (PIC-01)

- a) 指标要求：App 中不应存在以欺诈、诱骗、误导的方式收集个人信息的情况。
- b) 测评对象：App、文档资料
- c) 测评方式：功能验证、技术检测、文档审查

d) 测评步骤:

- 1) 查看 App 提供者的个人信息安全相关管理制度, 是否明确要求 App 不得以欺诈、诱骗、误导的方式收集个人信息;
- 2) 查看 App 隐私政策, 是否存在以欺诈、诱骗、误导的方式描述收集个人信息的行为;
- 3) 通过功能验证、技术检测查看 App 是否存在以欺诈、诱骗、误导的方式收集个人信息的行为。

注: 欺诈、诱骗、误导的行为参考附录 B 中描述。

- e) 单元判定: 如果 1) 为肯定, 2) 、3) 为否定, 则符合本测评单元指标要求, 否则不符合本测评单元指标要求。

6.1.1.2 测评项: 详见 GB/T 35273—2020 中 5.1 的 b) 。

6.1.1.2.1 测评单元 (PIC-02)

- a) 指标要求: App 不应隐瞒自身所具有的收集个人信息的业务功能;
- b) 测评对象: App、文档资料
- c) 测评方式: 功能验证、技术检测、文档审查
- d) 测评步骤:

1) 通过对 App 隐私政策等文件中描述收集个人信息的业务功能及其对应收集的个人信息, 和经功能验证、技术检测采集的 App 实际收集个人信息的业务功能和对应收集的个人信息比较, 判断 App 是否存在未说明的收集个人信息的业务功能。

- e) 单元判定: 如果 1) 为否定, 则符合本测评单元指标要求, 否则不符合本测评单元指标要求。

6.1.1.3 测评项: 详见 GB/T 35273—2020 中 5.1 的 c) 。

6.1.1.3.1 测评单元 (PIC-03)

- a) 指标要求: App 提供者不应从非法渠道获取个人信息;
- b) 测评对象: App、App 服务端、文档资料
- c) 测评方式: 功能验证、文档审查、服务端核查、人员访谈
- d) 测评步骤:
 - 1) 查看 App 提供者的个人信息安全相关管理制度, 是否明确要求不得从非法渠道获取个人信息;
 - 2) 访谈 App 运营相关人员, 询问获取个人信息的渠道是否合法;
 - 3) 是否存在被监管部门认定为存在违法违规收集个人信息行为且未进行整改。
- e) 单元判定: 如果 1)、2) 为肯定, 3) 为否定, 则符合本测评单元指标要求, 否则不符合本测评单元指标要求。

6.1.2 收集个人信息的最小必要的测评

6.1.2.1 测评项: 详见 GB/T 35273—2020 中 5.2 的 a) 。

6.1.2.1.1 测评单元 (PIC-04)

- a) 指标要求: App 强制收集的个人信息类型应是保障其基本服务类型正常运行最少够用的个人信息;
- b) 测评对象: App
- c) 测评方式: 功能验证、技术检测
- d) 测评步骤:
 - 1) 通过功能验证查看 App 提供的基本服务类型, 结合功能验证、技术检测查看 App 是否强制收集必要个人信息范围外的其他个人信息;

注: 服务类型正常运行最少够用的个人信息及相关要求见 GB/T AAAA—BBBB 附录 A。

2) 通过功能验证、技术检测查看 App 是否强制用户打开非必要权限。

e) 单元判定：如果 1) 、2) 均为否定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.1.2.1.2 测评单元 (PIC-05)

a) 指标要求：App 收集的个人信息类型应与实现其业务功能有直接关联；

b) 测评对象：App、文档资料

c) 测评方式：功能验证、技术检测、文档审查

d) 测评步骤：

1) 查看 App 隐私政策中描述的 App 收集的个人信息是否与业务功能有直接关联；

2) 通过功能验证、技术检测查看 App 申请的可收集个人信息的权限是否与业务功能有直接关联；

3) 通过功能验证、技术检测查看 App 实际收集的个人信息是否与业务功能有直接关联。

注：直接关联是指没有该个人信息的参与，与之相对应的服务功能无法实现。

e) 单元判定：如果 1) 、2) 、3) 均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.1.2.2 测评项：详见 GB/T 35273—2020 中 5.2 的 b) 。

6.1.2.2.1 测评单元 (PIC-06)

a) 指标要求：App 自动采集个人信息的频率应是实现 App 的业务功能所必需的最低频率；

b) 测评对象：App、文档资料

c) 测评方式：技术检测、文档审查

d) 测评步骤：

1) 通过技术检测查看 App 前台、后台和静默运行时自动收集个人信息的频率，结合 App 提供者提供的证明材料，判断 App 自动收集个人信息的频率是否是实现 App 的业务功能所必需的最低频率。

注 1：App 自动收集个人信息的频率可参考其调用可读取个人信息的 API 的频率或发送包含个人信息的网络数据包的频率；

注 2：不同场景下 App 采集个人信息的合理频率和相应的检测环境见附录 D。

e) 单元判定：如果 1) 为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.1.2.3 测评项：详见 GB/T 35273—2020 中 5.2 的 c) 。

6.1.2.3.1 测评单元 (PIC-07)

a) 指标要求：App 间接获取个人信息数量应是实现 App 业务功能所必需的最少数量；

b) 测评对象：App、App 服务端、文档资料

c) 测评方式：功能验证、技术检测、文档审查、服务端核查、人员访谈

d) 测评步骤：

1) 查看 App 提供者的个人信息安全相关管理制度，是否明确要求间接获取个人信息数量应是实现 App 业务功能所必需的最少数量；

2) 通过查看 App 的隐私政策和功能验证查看 App 是否存在间接获取个人信息的行为；

3) 通过功能验证、技术检测查看 App 间接获取的个人信息是否为实现 App 业务功能所必需的最少数量；

4) 询问 App 提供者是否存在间接获取个人信息的行为;

5) 查看在间接获取的场景下是否有获取个人信息的协议, 协议中是否规定了获取个人信息的类型、数据量以及与业务功能的关联关系, 据此判断 App 间接获取个人信息的数量是否是 App 业务功能所必需的最少数量。

注: App 间接获取个人信息的行为例如第三方账号登陆时获取昵称、头像, 内嵌第三方购物平台时聚合展示不同第三方购物平台的订单信息等。

e) 单元判定: 如果 2) 、4) 为否定, 则本测评单位为不适用; 如果 1) 、3) 、5) 为肯定, 则符合本测评单元指标要求, 否则不符合本测评单元指标要求。

6.1.3 多项业务功能的自主选择的测评

6.1.3.1 测评项: 详见 GB/T 35273—2020 中 5.3 的 a) 。

6.1.3.1.1 测评单元 (PIC-08)

a) 指标要求: App 不应在安装时一次性要求授权其申请的全部权限;

b) 测评对象: App

c) 测评方式: 功能验证, 技术检测

d) 测评步骤:

1) 针对 Android App, 通过技术检测查看其 targetSdkVersion 是否小于 23;

2) 通过功能验证查看 App 是否要求用户一次性授权其申请的全部权限才允许安装。

e) 单元判定: 如果 1) 、2) 为否定, 则符合本测评单元指标要求, 否则不符合本测评单元指标要求。

6.1.3.1.2 测评单元 (PIC-09)

- a) 指标要求: App 不应在打开时一次性连续弹窗要求用户授权当前还未使用的业务功能所需的权限或要求用户填写当前未使用的业务功能所需的个人信息;
- b) 测评对象: App
- c) 测评方式: 功能验证
- d) 测评步骤:
 - 1) 通过功能验证查看 App 是否在首次打开时一次性连续弹窗要求用户授权当前还未使用的业务功能所需的权限;
 - 2) 通过功能验证查看 App 是否在首次打开时要求用户填写当前未使用的业务功能所需的个人信息。
- e) 单元判定: 如果 1) 、2) 为否定, 则符合本测评单元指标要求, 否则不符合本测评单元指标要求。

6.1.3.1.3 测评单元 (PIC-10)

- a) 指标要求: 用户未使用 App 某项业务功能的某项特定功能时, 不应要求用户授权相应权限或要求用户填写相应的个人信息;
- b) 测评对象: App
- c) 测评方式: 功能验证
- d) 测评步骤:
 - 1) 通过功能验证查看 App 在进入某项业务功能时, 是否要求用户授权当前未使用的特定功能所需求的权限或要求用户填写当前未使用的特定功能需要的个人信息。

注: 用户未使用 App 特定功能时要求用户授权相应权限的行为例如进入客服功能时, 在未使用拍照和语音功能的情况下, 要求用户授权摄像头和麦克风权限。

- e) 单元判定：如果 1) 为否定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.1.3.2 测评项：详见 GB/T 35273—2020 中 5.3 的 b) 。

6.1.3.2.1 测评单元 (PIC-11)

- a) 指标要求：App 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；
- b) 测评对象：App
- c) 测评方式：功能验证
- d) 测评步骤：
 - 1) 通过功能验证查看 App 提供的业务功能类型，如地图导航、网络约车、网络支付等，查看用户打开 App 后是否能自主选择特定业务功能的开启，如通过主动点击、勾选、填写等方式。

- e) 单元判定：如果 1) 为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.1.3.2.2 测评单元 (PIC-12)

- a) 指标要求：App 应仅在用户开启业务功能后，才开始收集该业务功能需要的个人信息；
- b) 测评对象：App
- c) 测评方式：功能验证、技术检测
- d) 测评步骤：
 - 1) 通过功能验证、技术检测查看 App 是否在用户点击同意隐私政策后才开始收集个人信息或打开可收集个人信息的权限；
 - 2) 通过功能验证、技术检测查看 App 是否在用户开启特定业务功能后，App 才开始收集对应业务功能需要的个人信息或打开对应业务功

能需要的权限。

- e) 单元判定：如果 1) 、2) 均为肯定，则符合本测评单元指标要求；否则不符合本测评单元指标要求。

6.1.3.2.3 测评单元 (PIC-13)

- a) 指标要求：App 在未向用户告知且未经用户同意，或无合理的使用场景时，不应频繁自启动或关联启动第三方 App 并收集个人信息；

- b) 测评对象：App、文档资料

- c) 测评方式：功能验证、技术检测、文档审查

- d) 测评步骤：

1) 查看 App 的隐私政策中是否说明 App 具有自启动或关联启动第三方 App 并收集个人信息的行为；

2) 通过技术检测查看 App 是否存在自启动并在自启动后收集个人信息的行为；

3) 通过技术检测查看 App 在使用或静默状态是否存在关联启动第三方 App 并收集个人信息的行为；

4) 结合 App 提供者提供的证明材料，判断 App 自启动或关联启动第三方 App 并收集个人信息的行为是否合理。

- e) 单元判定：如果 2) 、3) 为否定，则本测评单位为不适用；如果 1) 、4) 为肯定，则符合本测评单元指标要求；否则不符合本测评单元指标要求。

6.1.3.3 测评项：详见 GB/T 35273—2020 中 5.3 的 c) 。

6.1.3.3.1 测评单元 (PIC-14)

- a) 指标要求：App 关闭或退出业务功能的途径或方式应与用户选择使用业务功能的途径或方式同样方便。

- b) 测评对象: App
- c) 测评方式: 功能验证
- d) 测评步骤:
 - 1) 通过 App 功能验证查看用户是否能自主选择关闭或退出特定业务功能, 关闭或退出的途径是否便捷。
- e) 单元判定: 如果 1) 为肯定, 则符合本测评单元指标要求, 否则不符合本测评单元指标要求。

6.1.3.3.2 测评单元 (PIC-15)

- a) 指标要求: 用户选择关闭或退出特定业务功能后, App 应停止该业务功能的个人信息收集活动;
- b) 测评对象: App
- c) 测评方式: 功能验证、技术检测
- d) 测评步骤:
 - 1) 进入 App 某项业务功能, 通过功能验证、技术检测查看 App 收集的个人信息。退出该业务功能, 通过功能验证、技术检测查看 App 收集的个人信息。对比该业务功能关闭或退出前后 App 收集的个人信息, 判断用户选择关闭或退出特定业务功能后, App 是否停止该业务功能的个人信息收集活动。
- e) 单元判定: 如果 1) 为肯定, 则符合本测评单元指标要求, 否则不符合本测评单元指标要求。

6.1.3.4 测评项: 详见 GB/T 35273—2020 中 5.3 的 d) 。

6.1.3.4.1 测评单元 (PIC-16)

- a) 指标要求: 用户不授权同意使用、关闭或退出特定业务功能的, App 不应频繁征求用户的授权同意;

b) 测评对象: App

c) 测评方式: 功能验证

d) 测评步骤:

1) 通过功能验证查看用户不同意某一业务功能收集非必要个人信息后, App 是否频繁询问用户同意收集该类个人信息;

2) 通过功能验证查看用户不同意打开某类可收集个人信息的非必要权限后, App 是否频繁询问用户是否同意打开该类可收集个人信息权限;

3) 通过功能验证查看用户退出特定业务功能后, App 是否频繁询问用户打开特定业务功能。

注: 48 小时内询问 1 次以上可认定为频繁打扰。

e) 单元判定: 如果 1)、2)、3) 均为否定, 则符合本测评单元指标要求, 否则不符合本测评单元指标要求。

6.1.3.5 测评项: 详见 GB/T 35273—2020 中 5.3 的 e) 。

6.1.3.5.1 测评单元 (PIC-17)

a) 指标要求: 用户不授权同意使用、关闭或退出特定业务功能, App 不应暂停用户自主选择使用其他的业务功能, 或降低其他业务功能的服务质量;

b) 测评对象: App

c) 测评方式: 功能验证

d) 测评步骤:

1) 通过功能验证查看用户关闭或退出特定业务功能, App 是否妨碍其他业务功能继续正常使用;

2) 通过功能验证查看用户关闭或退出特定业务功能, App 是否故意

设置障碍影响用户体验。

- e) 单元判定：如果 1)、2) 为否定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.1.3.5.2 测评单元 (PIC-18)

- a) 指标要求：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，不应拒绝提供原有业务功能；
- b) 测评对象：App、文档资料
- c) 测评方式：功能验证、文档审查
- d) 测评步骤：

1) 查看 App 的隐私政策，对比 App 新增业务功能申请收集的个人信息。进入 App 新增业务功能界面，不同意新增业务功能申请收集的个人信息或打开可收集个人信息权限，查看是否妨碍其他业务功能继续正常使用。

注：新增业务功能取代原有业务功能的除外。

- e) 单元判定：如果 1) 为否定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.1.3.6 测评项：详见 GB/T 35273—2020 中 5.3 的 f) 。

6.1.3.6.1 测评单元 (PIC-19)

- a) 指标要求：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，强制要求用户同意收集个人信息；
- b) 测评对象：App、文档资料
- c) 测评方式：功能验证、文档审查
- d) 测评步骤：

1) 查看 App 的隐私政策，或通过功能验证，记录仅以改善服务质量、

提升使用体验、研发新产品、增强安全性等为由，要求用户同意收集的个人信息。通过功能验证，不提供仅以改善服务质量、提升使用体验、研发新产品、增强安全性为由收集的信息，查看 App 是否拒绝提供所有服务。

注：为保障 App 基本的业务安全性，而非增强安全性而收集的个人信息，不在此项检测范围内。

e) 单元判定：如果 1) 为否定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.1.4 收集个人信息时的授权同意的测评

6.1.4.1 测评项：详见 GB/T 35273—2020 中 5.4 的 a) 。

6.1.4.1.1 测评单元 (PIC-20)

a) 指标要求：App 收集个人信息，应向用户告知收集、使用个人信息的目的、方式和范围等规则，并获得用户的授权同意；

b) 测评对象：App

c) 测评方式：技术检测、功能验证

d) 测评步骤：

1) 查看 App 的个人信息保护政策，核实个人信息保护政策是否逐一列出 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、范围等规则；

2) 查看 App 基本业务功能开启前（如个人信息主体初始安装、首次使用等），是否通过交互界面或设计（如弹窗、文字说明、填写框、提示条、提示音等形式），向个人信息主体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造成的影响，并通过个人信息主体对信息收集主动作出肯定性动作（如勾选、点击“同意”或“下一步”等）征得其明示同意；

3) 如 App 提供多项收集、使用个人信息业务功能时, 查看 App 除在个人信息保护政策外, 是否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, 能充分考虑对其具体影响, 并允许个人信息主体对扩展业务功能逐项选择同意;

4) 技术检测 App 是否在征得个人信息主体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;

5) 技术检测 App 是否在个人信息主体明确表示不同意后, 仍收集个人信息或打开可收集个人信息的权限, 或频繁征求个人信息主体同意、干扰个人信息主体正常使用;

6) 技术检测 App 实际收集的个人信息或打开的可收集个人信息权限是否超出个人信息主体授权范围;

7) 技术检测 App 是否未经个人信息主体同意更改其设置的可收集个人信息权限状态, 如 App 更新时自动将个人信息主体设置的权限恢复到默认状态。

e) 单元判定: 如果 1) 、2) 、3) 为肯定且 4) 至 7) 为否定, 则符合本测评单元指标要求, 否则不符合本测评单元指标要求。

6.1.4.2 测评项: 详见 GB/T 35273—2020 中 5.4 的 b) 。

6.1.4.2.1 测评单元 (PIC-21)

a) 指标要求: App 收集个人敏感信息前, 应征得用户的明示同意, 并确保用户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;

b) 测评对象: App

c) 测评方式: 功能验证

d) 测评步骤:

1) 查看 App 的个人信息保护政策, 了解收集个人敏感信息场景和类型, 确认个人信息保护政策中是否对需要收集的个人信息进行了明确标识或突出显示;

2) 进入 App 功能界面, 验证 App 在收集用户身份证号、银行账号、行踪轨迹等个人敏感信息前, 是否通过交互界面或设计 (如弹窗、文字说明、填写框、提示条、提示音等形式) 向个人信息主体明确告知收集、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, 能充分考虑对其具体影响, 并通过个人信息主体对信息收集主动作出肯定性动作 (如勾选、点击“同意”或“下一步”等) 征得其明示同意;

3) 查看 App 在申请打开可收集个人敏感信息的权限时, 是否同步告知用户其目的, 且目的说明清晰明确。

注: 收集用户实名信息时仅说明用于实名制认证, 收集地理位置信息时仅说明用于基于地理位置的相关服务, 申请存储权限时仅说明用于改进用户体验等可认为属于说明不清晰的情况。

e) 单元判定: 如果 1) 、2) 、3) 均为肯定, 则符合本测评单元指标要求, 否则不符合本测评单元指标要求。

6.1.4.3 测评项: 详见 GB/T 35273—2020 中 5.4 的 c) 。

6.1.4.3.1 测评单元 (PIC-22)

a) 指标要求: App 收集个人生物识别信息前, 应单独向用户告知收集、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, 并征得用户的明示同意;

b) 测评对象: App

c) 测评方式: 功能验证

d) 测评步骤:

1) 查看 App 的个人信息保护政策, 了解收集个人生物识别信息的场景和类型, 确认个人信息保护政策中是否对需要收集的个人信息进行了明确标识或突出显示;

2) 进入 App 功能界面, 验证 App 在收集个人生物识别信息前, 是否通过交互界面或设计 (如弹窗、文字说明、填写框、提示条、提示音等形式) 向个人信息主体明确告知收集、使用该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, 以便个人信息主体在作出具体的授权同意前, 能充分考虑对其具体影响, 并通过个人信息主体对生物识别信息收集主动作出肯定性动作 (如勾选、点击“同意”或“下一步”等) 征得其明示同意。

e) 单元判定: 如果 1) 、2) 为肯定, 则符合本测评单元指标要求, 否则不符合本测评单元指标要求。

6.1.4.4 测评项: 详见 GB/T 35273—2020 中 5.4 的 d) 。

6.1.4.4.1 测评单元 (PIC-23)

a) 指标要求: App 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;

b) 测评对象: App

c) 测评方式: 功能验证、人员访谈

d) 测评步骤:

1) 查看 App 的个人信息保护政策中是否告知了征得未成年人监护人同意的机制;

2) 如果 App 中存在设定生日、年龄等相关功能, 设置年龄为 14 周岁以下, 查看 App 是否有相应机制征得监护人的明示同意;

3) 询问 App 提供者在收集年满 14 周岁的未成年人的个人信息前,

是否具备相应措施去征得未成年人或其监护人的明示同意。

- e) 单元判定：如果 1) 、 2) 、 3) 为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.1.4.5 测评项：详见 GB/T 35273—2020 中 5.4 的 e) 。

6.1.4.5.1 测评单元 (PIC-24)

- a) 指标要求：App 提供者间接获取个人信息时，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；

- b) 测评对象：文档资料

- c) 测评方式：人员访谈、文档审查

- d) 测评步骤：

- 1) 访谈 App 提供者相关人员，确认 App 提供者是否通过间接渠道获取个人信息；

- 2) 查看 App 提供者在间接获取个人信息时，是否通过相关合同或协议保障个人信息来源的合法性；

- 3) 询问 App 提供者间接获取的个人信息类型以及来源，是否对其来源的合法性进行确认。

- e) 单元判定：如果 1) 为否定，则本测评单元为不适用；如果 1) 、 2) 、 3) 均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.1.4.5.2 测评单元 (PIC-25)

- a) 指标要求：App 提供者间接获取个人信息时，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，用户是否授权同意转让、共享、公开披露、删除等；

- b) 测评对象：文档资料

- c) 测评方式：人员访谈、文档审查
- d) 测评步骤：
 - 1) 访谈 App 提供者相关人员，确认 App 提供者是否通过间接渠道获取个人信息；
 - 2) 查看 App 提供者在间接获取个人信息时，是否通过相关合同或协议明确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，用户是否授权同意转让、共享、公开披露、删除等；
 - 3) 询问 App 提供者是否了解已获得的个人信息处理的授权同意范围，包括使用目的，用户是否授权同意转让、共享、公开披露等；
- e) 单元判定：如果 1) 为否定，则本测评单元为不适用；如果 1) 、2) 、3) 均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.1.4.5.3 测评单元 (PIC-26)

- a) 指标要求：App 间接获取个人信息时，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，征得用户的明示同意，或通过个人信息提供方征得用户的明示同意；
- b) 测评对象：App、App 服务端、文档资料
- c) 测评方式：功能验证、文档审查、服务端核查、人员访谈
- d) 测评步骤：
 - 1) 查看 App 提供者在间接获取个人信息时，是否通过相关合同或协议明确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，用户是否授权同意转让、共享、公开披露、删除等；
 - 2) 询问 App 提供者是否了解已获得的个人信息处理的授权同意范围，包括使用目的，用户是否授权同意转让、共享、公开披露等；

- 3) 通过询问 App 提供者或服务端核查, 查看 App 提供者开展业务需进行的个人信息处理活动是否超出该授权同意范围;
- 4) 通过功能验证查看 App 是否对超出范围部分征得用户的明示同意。
- e) 单元判定: 如果 3) 为否定, 则本测评单元不适用。如果 3) 为肯定, 且 4) 为肯定, 则符合本测评单元指标要求, 否则不符合本测评单元指标要求。

6.1.5 个人信息保护政策的测评

6.1.5.1 测评项: 详见 GB/T 35273—2020 中 5.5 的 a) 。

6.1.5.1.1 测评单元 (PIC-27)

- a) 指标要求: 应制定个人信息保护政策, 个人信息保护政策内容应满足 GB/T 35273—2020 中 5.5 的 a) 的要求;
- b) 测评对象: App
- c) 测评方式: 功能验证
- d) 测评步骤:
 - 1) 通过功能验证查看 App 的个人信息保护政策是否包括了相应内容并记录相应结果是否满足 GB/T 35273—2020 中 5.5 的 a) 的要求。
- e) 单元判定: 如果 1) 为肯定, 则符合本测评单元指标要求, 否则不符合本测评单元指标要求。

6.1.5.2 测评项: 详见 GB/T 35273—2020 中 5.5 的 b) 。

6.1.5.2.1 测评单元 (PIC-28)

- a) 指标要求: App 的个人信息保护政策所告知的信息应真实、准确、完整;
- b) 测评对象: App、App 服务端

c) 测评方式：功能验证、技术检测、服务端核查、人员访谈

d) 测评步骤：

1) 查看 App 的个人信息保护政策披露的个人信息控制者的基本情况，包括主体身份、联系方式，通过工商信息查询、拨打联系电话、向联系邮箱发送邮件等方式验证上述信息是否真实、准确、完整；

2) 技术检测 App 的业务功能及其收集个人信息的行为，验证 App 的业务功能以及各业务功能分别收集的个人信息类型是否与个人信息保护政策告知的信息相符；

3) 技术检测 App 的个人信息收集方式，验证 App 的个人信息收集方式是否与个人信息保护政策披露的个人信息收集方式相符；

4) 查看 App 的个人信息保护政策披露的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等，通过操作 App 相应功能、拨打联系电话、向联系邮箱发送邮件等方式验证上述信息是否真实、准确、完整；

5) 查看 App 的个人信息保护政策披露的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，通过操作 App 相应功能、拨打联系电话、向联系邮箱发送邮件等方式验证上述信息是否真实、准确、完整；

6) 通过人员访谈和服务端核查验证个人信息保护政策对个人信息存储期限的告知是否真实、准确、完整；

7) 通过人员访谈和服务端核查验证个人信息保护政策对个人信息的共享、转让、公开披露行为的告知是否真实、准确、完整；

8) 通过人员访谈和服务端核查验证个人信息保护政策对个人信息安全防护措施的告知是否真实、准确、完整。

e) 单元判定：如果 1) 至 8) 均为肯定，则符合本测评单元指标要求，

否则不符合本测评单元指标要求。

6.1.5.3 测评项：详见 GB/T 35273—2020 中 5.5 的 c) 。

6.1.5.3.1 测评单元 (PIC-29)

a) 指标要求：App 的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；

b) 测评对象：App

c) 测评方式：功能验证

d) 测评步骤：

1) 查看 App 是否提供简体中文版个人信息保护政策；

2) 查看 App 个人信息保护政策的字体大小、颜色、排版是否易于阅读；

3) 查看 App 个人信息保护政策语言是否通顺且易于理解，不存在概念混淆、逻辑混乱、冗长繁琐等；

4) 查看 App 个人信息保护政策是否存在错别字，错别字是否造成理解上的歧义。

e) 单元判定：如果 1) 、2) 、3) 为肯定且 4) 为否定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.1.5.4 测评项：详见 GB/T 35273—2020 中 5.5 的 d) 。

6.1.5.4.1 测评单元 (PIC-30)

a) 指标要求：App 个人信息保护政策应公开发布且易于访问；

b) 测评对象：App

c) 测评方式：功能验证

d) 测评步骤：

1) 查看 App 首次运行时是否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;

2) 进入注册及登录页面 (若有注册、登录功能), 查看是否具有个人信息保护政策或个人信息保护政策有效链接;

3) 查看 App 运行并进入主界面后, 是否通过 4 次及以下点击等操作能访问到个人信息保护政策。

e) 单元判定: 如果 1)、2)、3) 均为肯定, 则符合本测评单元指标要求, 否则不符合本测评单元指标要求。

6.1.5.5 测评项: 详见 GB/T 35273—2020 中 5.5 的 e) 。

6.1.5.5.1 测评单元 (PIC-31)

a) 指标要求: App 个人信息保护政策应逐一送达用户; 当成本过高或有显著困难时, 可以公告的形式发布;

b) 测评对象: App

c) 测评方式: 功能验证

d) 测评步骤:

1) 查看 App 中是否可以找到被测 App 提供的个人信息保护政策;

2) 若在 App 中未找到个人信息保护政策, 则判断是否存在逐一送达个人信息保护政策时成本过高或有显著困难的情况, 例如当 App 不存在用户交互界面时, 此种情况下, 查看 App 提供者是否在其官方网站公开发布个人信息保护政策。

e) 单元判定: 如果 1)、2) 为肯定, 则符合本测评单元指标要求, 否则不符合本测评单元指标要求。

6.1.5.6 测评项: 详见 GB/T 35273—2020 中 5.5 的 f) 。

6.1.5.6.1 测评单元 (PIC-32)

- a) 指标要求: App 提供者在个人信息保护政策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用户;
- b) 测评对象: App、App 服务端
- c) 测评方式: 功能验证、服务端核查、人员访谈
- d) 测评步骤:
 - 1) 查看个人信息保护政策是否标注了更新日期;
 - 2) 根据测评单元 PIC-28 的符合情况, 查看 App 是否存在个人信息保护政策所载事项发生变化时, 未及时更新个人信息保护政策的情况;
 - 3) 若个人信息保护政策更新过, 查看 App 是否向用户明示了更新后的个人信息保护政策并告知了个人信息保护政策的更新情况。
 - 4) 询问 App 提供者是否有在个人信息保护政策更新后, 重新告知用户的机制。
- e) 单元判定: 如果 2) 为否定且 1) 、3) 、4) 为肯定, 则符合本测评单元指标要求, 否则不符合本测评单元指标要求。

6.1.6 征得授权同意的例外的测评

6.1.6.1 测评项: 详见 GB/T 35273—2020 中的 5.6。

6.1.6.1.1 测评单元 (PIC-33)

- a) 指标要求: 个人信息控制者收集、使用个人信息不必征得用户的授权同意的情形, 应满足 GB/T 35273—2020 中 5.6 的要求;
- b) 测评对象: App
- c) 测评方式: 功能验证
- d) 测评步骤:
 - 1) 查看个人信息保护政策是否告知了“征得授权同意的例外”;

2) 查看“征得授权同意的例外”中是否包含不合理的例外情形。

e) 单元判定：如果 1) 为肯定且 2) 为否定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.2 个人信息的存储的测评

6.2.1 个人信息存储时间最小化的测评

6.2.1.1 测评项：详见 GB/T 35273—2020 中 6.1 的 a) 。

6.2.1.1.1 测评单元 (PIS-01)

a) 指标要求：App 提供者保存个人信息的期限应为实现用户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用户另行同意的除外。

b) 测评对象：App 服务端、文档资料

c) 测评方式：服务端核查、文档审查、人员访谈

d) 测评步骤：

1) 查看 App 提供者是否针对个人信息设立保存期限的相关制度，是否明确要求保存个人信息的期限为实现用户授权使用目的所需最短时间；

2) 询问 App 提供者针对各类个人信息的保存期限，包括制度中规定的、程序中设置的等，判断保存期限是否满足最短时间要求；

3) 查看 App 服务端是否有针对超期数据的甄别方式；

4) 对于超过最短保存时间的个人信息，查看 App 提供者是否能提供法律法规的另行规定或者用户另外同意的证明材料。

e) 单元判定：如果 1) 至 4) 为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.2.1.2 测评项：详见 GB/T 35273—2020 中 6.1 的 b) 。

6.2.1.2.1 测评单元 (PIS-02)

- a) 指标要求：超出个人信息保存期限后，应对个人信息进行删除或匿名化处理。
- b) 测评对象：App 服务端、文档资料
- c) 测评方式：服务端核查、文档审查、人员访谈
- d) 测评步骤：
 - 1) 查看 App 提供者是否有针对超期数据进行处理的相关制度；
 - 2) 询问并查看 App 提供者是否有针对已超期数据处理的技术手段；
 - 3) 查看 App 提供者针对超期数据进行处理日志信息，是否对超期数据进行了处理；
 - 4) 查看删除或匿名化处理数据的结果是否达到制度的要求。
- e) 单元判定：如果 1) 至 4) 为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.2.2 去标识化处理的测评

6.2.2.1 测评项：详见 GB/T 35273—2020 中的 6.2。

6.2.2.1.1 测评单元 (PIS-03)

- a) 指标要求：收集个人信息后，App 提供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，将去标识化后的信息与可用于恢复识别个人的信息分开存储并加强访问与使用权限管理。
- b) 测评对象：App 服务端
- c) 测评方式：服务端核查
- d) 测评步骤：
 - 1) 查看 App 服务端是否在收集个人信息后，立即进行去标识处理。
 - 2) 询问并查看 App 提供者是否有相关的管理制度，规定收集个人信

息后将去标识化后的信息与可用于恢复识别个人的信息分开存储，可用于恢复识别个人的信息在访问权限、审批流程、日志记录、安全审计等方面是否有更严格的规定；

3) 查看 App 服务端，验证去标识化后的信息与可用于恢复识别个人的信息是否分开存储；

4) 查看 App 服务端，验证可用于恢复识别个人的信息的访问和使用权限相关的审批流程、日志记录、安全审计方面是否有效。

e) 单元判定：如果 1) 至 4) 为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.2.3 个人敏感信息的传输和存储的测评

6.2.3.1 测评项：详见 GB/T 35273—2020 中 6.3 的 a) 。

6.2.3.1.1 测评单元 (PIS-04)

a) 指标要求：传输和存储个人敏感信息时，应采用加密等安全措施。

b) 测评对象：App、App 服务端、文档资料

c) 测评方式：技术检测、服务端核查、文档审查

d) 测评步骤：

1) 查看 App 的设计文档，在传输和存储个人敏感信息时是否采用加密等安全措施；

2) 采用技术手段检测 App，是否以明文形式通过网络传输用户个人敏感信息；

3) 采用技术手段检测 App，是否以明文形式将个人敏感信息存储在用户终端中；

4) 查看 App 服务端是否以明文形式存储个人敏感信息。

e) 单元判定：如果 2) 、3) 、4) 均为否定，则符合本测评单元指标要

求，否则不符合本测评单元指标要求。

6.2.3.2 测评项：详见 GB/T 35273—2020 中 6.3 的 b) 。

6.2.3.2.1 测评单元 (PIS-05)

a) 指标要求：App 收集个人生物识别信息的，应将其与收集的个人身份信息分开存储。

b) 测评对象：App、App 服务端、文档资料

c) 测评方式：服务端核查、人员访谈

d) 测评步骤：

1) 查看 App 提供者的个人信息安全相关管理制度或 App 设计文档是否明确将收集的 personal 生物识别信息与个人身份信息分开存储；

2) 采用技术手段检测 App 本地是否将收集的 personal 生物识别信息与个人身份信息分开存储；

3) 查看 App 服务端，是否将收集的 personal 生物识别信息与个人身份信息分开存储。

e) 单元判定：如果 1) 、2) 、3) 均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.2.3.3 测评项：详见 GB/T 35273—2020 中 6.3 的 c) 。

6.2.3.3.1 测评单元 (PIS-06)

a) 指标要求：App 应采取恰当措施以避免存储原始 personal 生物识别信息。

b) 测评对象：App、App 服务端、文档资料

c) 测评方式：技术检测、服务端核查、文档审查

d) 测评步骤：

1) 查看 App 提供者的个人信息安全相关管理制度或 App 设计文档是

否明确不存储个人生物识别信息的原始信息；

2) 通过技术手段检测 App 是否通过网络传输个人生物识别信息的原始信息；

3) 通过技术手段检测 App 是否将个人生物识别信息的原始信息存储在用户终端中；

4) 查看 App 服务端是否存储个人生物识别信息的原始信息。

注 1：可采取的措施包括但不限于：仅存储不可逆的个人生物识别信息的摘要信息；在用户终端中完成身份识别、认证等功能；身份识别、认证完成后删除可提取个人生物识别信息的原始图像。

注 2：App 提供者履行法律法规规定的义务相关的情形除外。

e) 单元判定：如果 1) 为肯定且 2) 、 3) 、 4) 为否定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.2.4 个人信息控制者停止运营的测评

6.2.4.1 测评项：详见 GB/T 35273—2020 中 6.4 的 a) 。

6.2.4.1.1 测评单元 (PIS-07)

a) 指标要求：App 提供者应确保停止运营后及时停止继续收集个人信息的活动，并有相应机制保障实施。

b) 测评对象：App 服务端、文档资料

c) 测评方式：服务端核查、文档审查、人员访谈

d) 测评步骤：

1) 查看 App 提供者的个人信息安全相关管理制度，是否明确要求停止运营产品或服务后及时停止继续收集个人信息的活动；

2) 询问 App 提供者是否存在停止运营产品或服务的情况；

3) 如果存在停止运营产品或服务的情况，询问是否及时停止继续收

集个人信息, 查看 App 服务端确保停止继续收集个人信息的机制和相关记录。

注: 例如停止某服务后, 是否移除仅供该服务使用的收集个人信息的代码。

e) 单元判定: 如果 1)、2)、3) 为肯定, 则符合本测评单元指标要求, 如果 1) 为肯定且 2) 为否定, 也符合本测评单元指标要求, 否则不符合本测评单元指标要求。

6.2.4.2 测评项: 详见 GB/T 35273—2020 中 6.4 的 b) 。

6.2.4.2.1 测评单元 (PIS-08)

a) 指标要求: App 提供者应明确要求在停止运营其产品或服务时, 将停止运营的通知以逐一送达或公告的形式通知用户, 并有相应机制保障实施。

b) 测评对象: App 服务端、文档资料

c) 测评方式: 服务端核查、文档审查、人员访谈

d) 测评步骤:

1) 查看相关管理制度, 是否明确要求在停止运营其产品或服务时, 将停止运营的通知以逐一送达或公告的形式通知用户;

2) 询问 App 提供者是否存在停止运营产品或服务的情况;

3) 如果存在停止运营产品或服务的情况, 询问是否将停止运营的通知以逐一送达或公告的形式通知用户, 查看 App 服务端发送通知的实现机制和相关记录。

e) 单元判定: 如果 1)、2)、3) 为肯定, 则符合本测评单元指标要求, 如果 1) 为肯定且 2) 为否定, 也符合本测评单元指标要求, 否则不符合本测评单元指标要求。

6.2.4.3 测评项: 详见 GB/T 35273—2020 中 6.4 的 c) 。

6.2.4.3.1 测评单元 (PIS-09)

- a) 指标要求: App 提供者应明确要求在停止运营其产品或服务时, 对其所持有的个人信息进行删除或匿名化处理, 并有相应机制保障实施。
- b) 测评对象: App 服务端、文档资料
- c) 测评方式: 服务端核查、文档审查、人员访谈
- d) 测评步骤:
 - 1) 查看相关管理制度, 是否明确要求在停止运营其产品或服务时, 对其所持有的个人信息进行删除或匿名化处理;
 - 2) 询问 App 提供者是否存在停止运营产品或服务的情况;
 - 3) 如果存在停止运营产品或服务的情况, 询问是否对其所持有的个人信息进行删除或匿名化处理, 查看 App 服务端相应的实现机制和相关记录;
 - 4) 查看删除或匿名化处理结果是否符合相关要求。
- e) 单元判定: 如果 1) 至 4) 为肯定, 则符合本测评单元指标要求, 如果 1) 为肯定且 2) 为否定, 也符合本测评单元指标要求, 否则不符合本测评单元指标要求。

6.3 个人信息的使用的测评

6.3.1 个人信息访问控制措施的测评

6.3.1.1 测评项: 详见 GB/T 35273—2020 中 7.1 的 a) 。

6.3.1.1.1 测评单元 (UPI-01)

- a) 指标要求: App 提供者应对被授权访问个人信息的人员, 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数据操作权限。
- b) 测评对象: 文档资料、App 服务端

c) 测评方式：文档审查、服务端核查

d) 测评步骤：

1) 查看 App 提供者的个人信息安全相关管理制度，是否建立访问控制策略，访问控制策略是否体现最少授权原则，如各类角色仅能访问职责所需的最少够用的个人信息；是否建立个人信息访问授权审批流程；

2) 服务端核查 App 服务端是否符合个人信息访问控制策略要求，例如不同权限的账号所能访问的个人信息类型、相关 API 接口等是否满足最小授权机制；App 服务端的角色账号访问和操作个人信息是否经过授权审批；

3) 核查是否存在相应的记录，如：针对个人信息访问权限和时效进行审批的记录、App 服务端的角色定义和账号分配进行审批的记录。

e) 单元判定：如果 1) 、2) 、3) 均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.3.1.2 测评项：详见 GB/T 35273—2020 中 7.1 的 b) 。

6.3.1.2.1 测评单元 (UIP-02)

a) 指标要求：App 提供者应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。

b) 测评对象：文档资料、App 服务端

c) 测评方式：文档审查、服务端核查

d) 测评步骤：

1) 查看 App 提供者的个人信息安全相关管理制度是否明确了各类个人信息的重要操作范围；是否针对个人信息重要操作定义了内部审批流程，审批流程是否覆盖所有定义的个人信息重要操作范围；

2) 核查 App 服务端的账号角色执行个人信息重要操作时是否符合审

批流程要求；

3) 核查是否存在相应的个人信息重要操作审批记录，App 服务端的重要操作是否有日志留存。

e) 单元判定：如果 1) 、2) 、3) 均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.3.1.3 测评项：详见 GB/T 35273—2020 中 7.1 的 c) 。

6.3.1.3.1 测评单元 (UPI-03)

a) 指标要求：App 提供者应对安全管理人员、数据操作人员、审计人员的角色进行分离设置。

b) 测评对象：文档资料、App 服务端

c) 测评方式：文档审查、服务端核查

d) 测评步骤：

1) 查看相关管理制度是否明确定义了安全管理人员、数据操作人员、审计人员各类角色的岗位职责，是否对各类角色的岗位分离有明确要求；

2) 核查实际岗位人员职责是否与管理制​​度一致，是否进行了岗位分离；

3) 核查 App 服务端账号角色是否覆盖安全管理人员、数据操作人员、审计人员，各类角色是否相互独立，是否不存在同一账号配置多个角色的情况。

e) 单元判定：如果 1) 、2) 、3) 均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.3.1.4 测评项：详见 GB/T 35273—2020 中 7.1 的 d) 。

6.3.1.4.1 测评单元 (UPI-04)

- a) 指标要求: App 提供者确因工作需要, 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。
- b) 测评对象: 文档资料
- c) 测评方式: 文档审查
- d) 测评步骤:
 - 1) 查看 App 提供者的个人信息安全相关管理制度是否明确超权限处理个人信息的规定或流程设置, 是否明确由个人信息保护责任人或个人信息保护工作机构对超权限处理个人信息进行审批;
 - 2) 核查 App 提供者是否由个人信息保护责任人或个人信息保护工作机构对超权限处理个人信息进行审批;
 - 3) 核查 App 提供者针对超权限处理个人信息是否存在相应的记录。
- e) 单元判定: 如果 1) 、2) 、3) 均为肯定, 则符合本测评单元指标要求, 否则不符合本测评单元指标要求。如果 App 提供者的相关管理制度规定不允许出现超权限处理个人信息的情形, 则本测评单元为不适用。

6.3.1.5 测评项: 详见 GB/T 35273—2020 中 7.1 的 e) 。

6.3.1.5.1 测评单元 (UPI-05)

- a) 指标要求: 对于访问、修改个人敏感信息等操作行为, App 提供者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。
- b) 测评对象: App 服务端
- c) 测评方式: 服务端核查
- d) 测评步骤:
 - 1) 核查 App 服务端是否具备相应机制实现按照业务流程的需求触发操作授权。

注：例如当收到客户投诉时，投诉处理人员才可访问该个人信息主体的相关信息。

e) 单元判定：如果 1) 为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.3.2 个人信息的展示限制的测评

6.3.2.1 测评项：详见 GB/T 35273—2020 中的 7.2。

6.3.2.1.1 测评单元 (UPI-06)

a) 指标要求：涉及通过界面展示个人信息的，App 提供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。

1) App 提供者应明确存在展示个人信息的系统范围（如 App 的个人设置功能界面、App 服务端的客服系统等）；

2) App 提供者应明确定义各类型和各级别个人信息的展示对象范围（如内部人员、个人信息主体）；

3) App 提供者应明确定义在各系统进行个人信息展示的安全管控要求，如去标识等。

b) 测评对象：文档资料、App、App 服务端

c) 测评方式：文档审查、功能验证、服务端核查

d) 测评步骤：

1) 查看 App 提供者的个人信息安全相关管理制度或设计文档中是否明确了各类各级个人信息在进行展示时的安全管理要求，如去标识化等；

2) 通过功能验证查看 App 中涉及个人信息展示的界面在展示个人信息时是否按管理要求对个人信息进行了去标识化处理等措施；

3) 通过服务端核查查看 App 服务端中涉及个人信息展示的界面在展示个人信息时是否按管理要求对个人信息进行了去标识化处理等措施。

e) 单元判定：如果 1) 、2) 、3) 均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.3.3 个人信息使用的目的限制的测评

6.3.3.1 测评项：详见 GB/T 35273—2020 中 7.3 的 a) 。

6.3.3.1.1 测评单元 (UPI-07)

a) 指标要求：App 提供者使用个人信息时，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。

b) 测评对象：App、App 服务端、文档资料

c) 测评方式：功能验证、服务端核查、文档审查

d) 测评步骤：

1) 查看 App 提供者的个人信息安全相关管理制度是否要求收集使用个人信息应征求个人信息主体的明示同意；是否要求超出征求同意范围收集使用个人信息的，应再次征得个人信息主体明示同意；

2) 通过功能验证查看 App 的个人信息保护政策说明的个人信息收集使用目的，服务端核查 App 提供者使用个人信息时，是否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；

3) 服务端核查 App 提供者因业务需要，确需超出征求同意范围使用个人信息时，是否存在再次征得个人信息主体明示同意的机制；

4) 核查 App 提供者是否存在超出征求同意范围使用个人信息的历史行为，是否为此再次征得个人信息主体的明示同意。

e) 单元判定：如果 1) 、3) 、4) 为肯定且 2) 为否定，则符合本测评

单元指标要求，否则不符合本测评单元指标要求。

6.3.3.2 测评项：详见 GB/T 35273—2020 中 7.3 的 b) 。

6.3.3.2.1 测评单元 (UPI-08)

a) 指标要求：App 提供者对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。

b) 测评对象：文档资料、App 服务端

c) 测评方式：文档审查、人员访谈、服务端核查

d) 测评步骤：

1) 查看 App 提供者处理个人信息活动环节中是否对加工处理产生的，能够单独或与其他信息结合识别特定自然人身份或反映特定自然人活动情况的个人信息，提供对应的管理制度、处理策略及相应技术措施；

2) 服务端核查个人信息加工处理的情况，产生的信息是否能够单独或与其他信息结合识别特定自然人身份或反映自然人活动情况；

3) 服务端核查针对加工处理后产生的个人信息的管理和使用等是否符合收集个人信息时获得的授权同意范围。

e) 单元判定：如果 1) 、2) 、3) 均为肯定，则符合本测评单元指标要求，如果 2) 不存在个人信息加工处理后产生的信息能够被认定为个人信息的情况，则判定为不适用；否则不符合本测评单元指标要求。

6.3.4 用户画像的使用限制的测评

6.3.4.1 测评项：详见 GB/T 35273—2020 中 7.4 的 a) 。

6.3.4.1.1 测评单元 (UPI-09)

- a) 指标要求: App 提供者不应对用户进行包含淫秽、色情、赌博、迷信、恐怖、暴力的内容以及对民族、种族、宗教、残疾、疾病歧视等内容的画像特征描述。
- b) 测评对象: App、App 服务端、文档资料
- c) 测评方式: 功能验证、服务端核查、文档审查、人员访谈
- d) 测评步骤:
 - 1) 查看 App 提供者的个人信息安全管理制度中是否禁止对用户进行包含淫秽、色情、赌博、迷信、恐怖、暴力的内容以及对民族、种族、宗教、残疾、疾病歧视等内容的画像特征描述;
 - 2) 询问相关管理人员、技术人员、产品经理, 了解用户画像的分析活动中, 是否禁止对用户进行包含淫秽、色情、赌博、迷信、恐怖、暴力的内容以及对民族、种族、宗教、残疾、疾病歧视等内容的画像特征描述;
 - 3) 检查 App 端的用户标签管理页面 (若有) 中对用户标签的类型、列表与配置规则, 是否包含淫秽、色情、赌博、迷信、恐怖、暴力的内容以及对民族、种族、宗教、残疾、疾病歧视等内容;
 - 4) 检查包含用户标签管理的 App 服务端 (若有) 中对用户标签的类型、列表与配置规则, 是否包含淫秽、色情、赌博、迷信、恐怖、暴力的内容以及对民族、种族、宗教、残疾、疾病歧视等内容。
- e) 单元判定: 如果 1) 、2) 为肯定且 3) 、4) 为否定, 则符合本测评单元指标要求, 否则不符合本测评单元指标要求。

6.3.4.2 测评项: 详见 GB/T 35273—2020 中 7.4 的 b) 。

6.3.4.2.1 测评单元 (UPI-10)

- a) 指标要求: App 提供者在业务运行或对外业务合作中使用用户画像时, 不应侵害公民、法人、和其他组织的合法权益, 不能危害国家安全,

宣扬恐怖主义，宣扬民族歧视，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。

b) 测评对象：App、App 服务端、文档资料

c) 测评方式：功能验证、服务端核查、文档审查、人员访谈

d) 测评步骤：

1) 查看 App 提供者的个人信息安全相关管理制度中是否包含对用户画像的相关管理规定；

2) 通过服务端核查、人员访谈查看用户画像的使用是否涉及侵害保护公民、法人和其他组织的合法权益；

3) 通过服务端核查、人员访谈查看用户画像的使用是否危害国家安全，宣扬恐怖主义，宣扬民族歧视，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等内容。

e) 单元判定：如果 1) 为肯定且 2)、3) 为否定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.3.4.3 测评项：详见 GB/T 35273—2020 中 7.4 的 c) 。

6.3.4.3.1 测评单元 (UPI-11)

a) 指标要求：App 提供者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。

b) 测评对象：文档资料、App 服务端

c) 测评方式：文档审查、服务端核查

d) 测评步骤：

1) 查看管理制度中是否包含对用户画像使用的相关管理规定，是否明确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；

2) 核查 App 服务端功能或日志，检查用户画像的使用情况，确认是否存在非必要场景中使用明确身份指向性信息进行精确画像的情况，例如生成用于推送广告的人物画像中不应使用可识别个人的信息；

e) 单元判定：如果 1) 为肯定且 2) 为否定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.3.5 个性化展示的使用的测评

6.3.5.1 测评项：详见 GB/T 35273—2020 中 7.5 的 a) 。

6.3.5.1.1 测评单元（UPI-12）

a) 指标要求：App 提供者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。

b) 测评对象：App

c) 测评方式：功能验证

d) 测评步骤：

1) 通过功能验证查看 App 是否向个人信息主体同时提供包含个性化展示和非个性化展示的业务功能；

2) 当 App 提供的业务功能使用个性化展示时，检查 App 是否通过标注“定推、推荐、关注、猜你喜欢”等字样显著区分个性化展示和非个性化展示的内容；

3) 当 App 提供的业务功能使用个性化展示时，查看 App 是否通过不同的栏目、板块、页面等显著区分个性化展示和非个性化展示内容；

4) 当 App 提供的业务功能使用个性化展示时，查看 App 是否通过其他显著方式区分个性化展示和非个性化展示内容；

5) 通过功能验证查看 App 利用用户个人信息和算法定向推送信息时，是否提供非定向推送信息的选项。

e) 单元判定：App 不涉及个性化展示服务时，本测评单元为不适用；如果 1) 、5) 为肯定，并且 2) 、3) 、4) 其中任一项为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.3.5.2 测评项：详见 GB/T 35273—2020 中 7.5 的 b) 。

6.3.5.2.1 测评单元 (UPI-13)

a) 指标要求：App 提供者向个人信息主体提供电子商务服务的过程中，根据用户的兴趣爱好，消费习惯等特征向用户提供商品或者服务搜索结果的个性化展示的，应当同时向该用户提供不针对其个人特征的选项。

b) 测评对象：App

c) 测评方式：功能验证

d) 测评步骤：

1) 通过功能验证查看 App 提供者是否向个人信息主体提供电子商务服务；

2) 当 App 提供者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时，检查是否同时对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。

e) 单元判定：如果 1) 为否定，则本测评单元为不适用；如果 1) 、2) 均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.3.5.3 测评项：详见 GB/T 35273—2020 中 7.5 的 c) 。

6.3.5.3.1 测评单元 (UPI-14)

a) 指标要求: App 提供者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; 当个人信息主体选择退出或关闭个性化展示模式时, 应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。

b) 测评对象: App、App 服务端

c) 测评方式: 功能验证、服务端核查、人员访谈

d) 测评步骤:

1) 通过功能验证查看 App 是否在向个人信息主体推送新闻信息服务过程中使用个性化展示;

2) 通过功能验证查看 App 向个人信息主体推送新闻信息服务过程中使用个性化展示时, 是否提供简单直观的退出或关闭个性化展示模式的选项;

3) 通过核查 App 服务端、访谈相关技术人员, 当个人信息主体选择退出或关闭个性化展示模式时, 在 App 服务端是否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。

e) 单元判定: 如果 1) 为否定, 则本测评单元为不适用; 如果 1) 、2) 、3) 均为肯定, 则符合本测评单元指标要求, 否则不符合本测评单元指标要求。

6.3.5.4 测评项: 详见 GB/T 35273—2020 中 7.5 的 d) 。

6.3.5.4.1 测评单元 (UPI-15)

a) 指标要求: App 提供者在使用个性化展示时, 宜建立个人信息主体对个性化展示所依赖的个人信息的自主控制机制, 保障个人信息主体调控个性化展示相关性程度的能力。

- b) 测评对象: App
- c) 测试方式: 功能验证
- d) 测评步骤:
 - 1) 通过功能验证查看 App 提供业务功能的过程中是否使用个性化展示;
 - 2) 通过功能验证查看 App 是否建立个性化展示所依赖的个人信息(如标签、画像维度等)的自主控制机制选项;
 - 3) 通过功能验证查看用户能否调控个性化展示模块的相关性程度。
- e) 单元判定: 如果 1) 为否定, 则本测评单元为不适用; 如果 1) 、2) 、3) 均为肯定, 则符合本测评单元指标要求, 否则不符合本测评单元指标要求。

6.3.6 基于不同业务目的所收集个人信息的汇聚融合的测评

6.3.6.1 测评项: 详见 GB/T 35273—2020 中 7.6 的 a) 。

测评规范参考 6.3.3 章节。

6.3.6.2 测评项: 详见 GB/T 35273—2020 中 7.6 的 b) 。

6.3.6.2.1 测评单元 (UPI-16)

- a) 指标要求: App 提供者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。
- b) 测评对象: App 服务端、文档资料
- c) 测评方式: 服务端核查、文档审查
- d) 测评步骤:
 - 1) 服务端核查 App 提供者是否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;

- 2) 服务端核查 App 提供者是否根据个人信息安全影响评估结果采取有效的个人信息保护措施;
 - 3) 核查 App 提供者开展个人信息安全影响评估及相关个人信息保护措施是否存在相应的记录。
- e) 单元判定: 如果 1) 、2) 、3) 均为肯定, 则符合本测评单元指标要求, 否则不符合本测评单元指标要求。

6.3.7 信息系统自动决策机制的使用的测评

6.3.7.1 测评项: 详见 GB/T 35273—2020 中 7.7 的 a) 。

6.3.7.1.1 测评单元 (UPI-17)

- a) 指标要求: App 提供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) 测评对象: App、App 服务端、文档资料
- c) 测评方式: 功能验证、服务端核查、文档审查
- d) 测评步骤:
 - 1) 通过功能验证查看 App 是否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;
 - 2) 通过服务端核查, 查看 App 服务端是否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;
 - 3) 核查 App 提供者是否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输出评估报告;
 - 4) 核查评估报告中说明会采取有效的保护个人信息主体的措施是否落地实施。

e) 单元判定：如果 1)、2) 均为否定，则该测评单元为不适用；如果 1) 或 2) 为肯定且 3)、4) 为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.3.7.2 测评项：详见 GB/T 35273—2020 中 7.7 的 b) 。

6.3.7.2.1 测评单元 (UPI-18)

a) 指标要求：App 提供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），在使用过程中应定期（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。

b) 测评对象：App、App 服务端、文档资料

c) 测评方式：功能验证、服务端核查、文档审查

d) 测评步骤：

1) 通过功能验证查看 App 是否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；

2) 通过服务端核查，查看 App 服务端是否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；

3) 核查 App 提供者是否在制度文件中明确对于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信息系统，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；

4) 服务端核查 App 提供者对于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系统是否每年至少有一份个人信息安全影响评估报告；

5) 服务端核查评估报告中说明会采取有效的保护个人信息主体的措施是否落地实施。

e) 单元判定：如果 1) 、2) 为否定，则该测评单元为不适用；如果 1) 或 2) 为肯定且 3) 、4) 、5) 均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.3.7.3 测评项：详见 GB/T 35273—2020 中 7.7 的 c) 。

6.3.7.3.1 测评单元 (UPI-19)

a) 指标要求：App 提供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。

b) 测评对象：App、App 服务端、过程文档

c) 测评方式：功能验证、服务端核查、文档审查、

d) 测评步骤：

1) 通过功能验证查看 App 是否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；

2) 通过服务端核查，查看 App 服务端是否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；

3) 通过功能验证查看 App 是否向个人信息主体提供针对自动决策结果的申诉渠道，并支持对自动决策结果的人工复核；

4) 核查 App 服务端是否向个人信息主体提供针对自动决策结果的申诉渠道，并对自动决策结果进行人工复核。

e) 单元判定：如果 1) 、2) 为否定，则该测评单元为不适用；如果 1) 或 2) 为肯定且 3) 、4) 均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.4 个人信息主体的权利的测评

6.4.1 个人信息查询的测评

6.4.1.1 测评项：详见 GB/T 35273—2020 中 8.1 的 a) 。

6.4.1.1.1 测评单元 (RPI-01)

- a) 指标要求：App 应对个人信息主体提供对其所持有的关于该主体的个人信息或个人信息类型的查询功能或方式。
- b) 测评对象：App
- c) 测评方式：功能验证
- d) 测评步骤：
 - 1) 通过功能验证查看 App 个人信息保护政策中是否向个人信息主体提供了查询其个人信息或个人信息类型的具体方式，例如客服电话、客服邮箱、个人信息保护机构或个人信息保护负责人的电话、邮箱等；
 - 2) 验证 App 个人信息保护政策中提供的查询个人信息的方式是否有效；
 - 3) 通过功能验证查看 App 功能界面中是否提供对于该主体的个人信息或个人信息类型的查询功能，例如个人信息展示页面、在线客服等；
 - 4) 验证 App 功能界面中提供的个人信息查询方式是否有效。
- e) 单元判定：如果 1) 、2) ，或 3) 、4) 为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.4.1.2 测评项：详见 GB/T 35273—2020 中 8.1 的 b) 。

6.4.1.2.1 测评单元 (RPI-02)

- a) 指标要求：App 应对个人信息主体提供对其所持有的关于该主体的个人信息的来源及所用于的目的的查询功能或方式。
- b) 测评对象：App
- c) 测评方式：功能验证。
- d) 测评步骤：

- 1) 查看 App 个人信息保护政策中是否向个人信息主体明示了个人信息的采集方式、对应的业务功能及使用目的;
 - 2) 查看 App 功能界面中是否提供关于该主体的个人信息的来源及所用于目的的查询功能;
 - 3) 验证 App 提供的客服电话、邮箱、在线客服, 个人信息保护机构或个人信息保护负责人的联系电话、邮箱等个人信息查询方式是否支持查询 App 提供者所持有的用户个人信息的来源及所用于的目的。
- e) 单元判定: 如果 1) 、2) 、3) 均为肯定, 则符合本测评单元指标要求, 否则不符合本测评单元指标要求。

6.4.1.3 测评项: 详见 GB/T 35273—2020 中 8.1 的 c) 。

6.4.1.3.1 测评单元 (RPI-03)

- a) 指标要求: App 应对个人信息主体提供已经获得该主体个人信息的第三方身份或类型的查询功能或方式。
- b) 测评对象: App
- c) 测评方式: 功能验证
- d) 测评步骤:
 - 1) 查看 App 个人信息保护政策中是否向个人信息主体明示了对外共享、转让和披露的规则, 其中是否包含可能获得该主体个人信息的第三方身份或类型;
 - 2) 查看 App 功能界面中是否提供了获取该主体个人信息的第三方身份或类型的查询功能;
 - 3) 验证 App 提供的客服电话、邮箱、在线客服, 个人信息保护机构或个人信息保护负责人的联系电话、邮箱等个人信息查询方式是否支持查询已获得用户个人信息的第三方身份或类型。
- e) 单元判定: 如果 1) 、2) 、3) 为肯定, 则符合本测评单元指标要求,

否则不符合本测评单元指标要求。

6.4.2 个人信息更正的测评

6.4.2.1 测评项：详见 GB/T 35273—2020 中的 8.2。

6.4.2.1.1 测评单元（RPI-04）

a) 指标要求：App 应为个人信息主体提供对其所持有的个人信息请求更正或补充信息的渠道或功能。

b) 测评对象：App

c) 测评方式：功能验证

d) 测评步骤：

1) 查看 App 个人信息保护政策或功能界面中是否向个人信息主体提供了更正或补充其个人信息的具体途径，包括 App 内个人信息修改界面、App 内客服渠道、联系电话、联系邮箱等；

2) 验证所提供的个人信息更正或补充途径是否有效。

e) 单元判定：如果 1)、2) 为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.4.3 个人信息删除的测评

6.4.3.1 测评项：详见 GB/T 35273—2020 中 8.3 的 a)。

6.4.3.1.1 测评单元（RPI-05）

a) 指标要求：App 违反法律法规规定，或违反与个人信息主体的约定，收集、使用个人信息的情形下，个人信息主体要求删除个人信息时，App 应提供删除功能或方式并及时删除。

b) 测评对象：App、App 服务端、文档资料

c) 测评方式：功能验证、服务端核查、文档审查、人员访谈

d) 测评步骤:

- 1) 查看 App 提供者的个人信息安全相关管理制度, 是否明确要求在 App 违反法律法规规定, 收集、使用个人信息, 或违反与个人信息主体的约定, 收集、使用个人信息的情形下, 个人信息主体要求删除个人信息时, App 应提供删除功能或方式并及时删除, 并明确删除个人信息的流程设计、响应时间等内容;
- 2) 查看 App 个人信息保护政策中是否向个人信息主体提供了删除其个人信息的具体途径, 并明确在 App 违反法律法规规定, 收集、使用个人信息的情形下, 及时响应个人信息主体要求删除个人信息;
- 3) 查看 App 的功能界面中是否向个人信息主体提供个人信息删除功能, 并能迅速处理;
- 4) 询问 App 提供者并查看 App 服务端是否具备按照要求删除个人信息的相应机制;
- 5) 核查 App 声明删除个人信息后, App 服务端是否存在个人信息残留。

e) 单元判定: 如果 1) 至 4) 为肯定, 5) 为否定, 则符合本测评单元指标要求, 否则不符合本测评单元指标要求。

6.4.3.2 测评项: 详见 GB/T 35273—2020 中 8.3 的 b) 。

6.4.3.2.1 测评单元 (RPI-06)

- a) 指标要求: App 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时, App 应立即停止共享、转让的行为, 并通知第三方及时删除。
- b) 测评对象: App、App 服务端、文档资料
- c) 测评方式: 功能验证、服务端核查、文档审查、人员访谈
- d) 测评步骤:

- 1) 查看 App 提供者的个人信息安全相关管理制度，是否明确要求在 App 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、转让个人信息的情形下，个人信息主体要求删除个人信息时，立即停止共享、转让的行为，并通知第三方及时删除；
 - 2) 查看 App 个人信息保护政策中是否向个人信息主体提供了删除其个人信息的具体途径，并明确在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、转让个人信息的情形下，及时响应个人信息主体要求立即停止共享、转让的行为，并通知第三方及时删除；
 - 3) 询问 App 提供者并查看 App 服务端是否具备停止共享、转让行为，并通知第三方及时删除的实现机制。
- e) 单元判定：如果 1) 、 2) 、 3) 为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.4.3.3 测评项：详见 GB/T 35273—2020 中 8.3 的 c) 。

6.4.3.3.1 测评单元 (RPI-07)

- a) 指标要求：App 提供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时，App 提供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信息。
- b) 测评对象：App、App 服务端、文档资料
- c) 测评方式：功能验证、服务端核查、文档审查
- d) 测评步骤：
 - 1) 查看 App 提供者的个人信息安全相关管理制度，是否明确要求在 App 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、转让个人信息的情形下，个人信息主体要求删除个人信息时，立即停止公开披露的行为，并发布通知要求相关接收方及时删除。

- 2) 查看 App 个人信息保护政策中是否向个人信息主体提供了删除其个人信息的具体途径, 并明确在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的情形下, 及时响应个人信息主体要求立即停止公开披露的行为, 并发布通知要求相关接收方及时删除;
 - 3) 询问 App 提供者并查看 App 服务端是否具备立即停止公开披露行为, 并发布通知要求相关接收方删除相应信息的机制。
- e) 单元判定: 如果 1) 、 2) 、 3) 为肯定, 则符合本测评单元指标要求, 否则不符合本测评单元指标要求。

6.4.4 个人信息主体撤回授权同意的测评

6.4.4.1 测评项: 详见 GB/T 35273—2020 中 8.4 的 a) 。

6.4.4.1.1 测评单元 (RPI-08)

- a) 指标要求: App 应在个人信息保护政策或功能界面中告知个人信息主体撤回收集、使用个人信息的授权同意的有效途径和方式, 且撤回授权同意后, 个人信息控制者后续不应再处理相应的个人信息。
- b) 测评对象: App、App 服务端
- c) 测评方式: 功能验证、技术检测、服务端核查
- d) 测评步骤:
 - 1) 查看 App 个人信息保护政策或功能界面中是否告知个人信息主体撤回收集、使用其个人信息的授权同意的的方法, 包括个人信息和权限;
 - 2) 验证 App 个人信息保护政策或功能界面中撤回收集、使用其个人信息的授权同意的的方法是否有效;
 - 3) 通过技术检测验证个人信息主体撤回同意后, App 是否继续收集和使用已撤回授权同意的个人信息;
 - 4) 核查 App 服务端, 在用户撤回同意后, App 服务端是否不再处理相应的个人信息。

e) 单元判定：如果 1)、2)、4) 为肯定，3) 为否定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.4.4.2 测评项：详见 GB/T 35273—2020 中 8.4 的 b)。

6.4.4.2.1 测评单元 (RPI-09)

a) 指标要求：App 应在个人信息保护政策或功能界面中提供基于个人信息推送广告的拒绝途径或关闭选项。

b) 测评对象：App

c) 测评方式：功能验证

d) 测评步骤：

1) 查看 App 是否具有基于个人信息的商业广告推送行为；

2) 若 App 存在基于个人信息的商业广告推送行为，则查看个人信息保护政策或功能界面中是否提供基于个人信息推送广告的拒绝途径或关闭选项；

3) 验证拒绝或关闭定向广告推送后，App 是否继续推送定向广告信息。

e) 单元判定：如果 1) 为否定，则该单元测评项判定为不适用；如果 1)、2) 为肯定，3) 为否定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.4.4.2.2 测评单元 (RPI-10)

a) 指标要求：App 应在个人信息保护政策或功能界面中向个人信息主体提供针对对外共享、转让、公开披露个人信息撤回授权同意的途径和方式。

b) 测评对象：App、App 服务端

c) 测评方式：功能验证、技术检测、服务端核查

d) 测评步骤:

- 1) 通过功能验证、技术检测查看 App 是否存在对外共享、转让、公开披露个人信息的行为;
- 2) 核查 App 服务端是否存在对外共享、转让、公开披露个人信息的行为;
- 3) 查看 App 的个人信息保护政策或功能界面中是否提供撤回授权同意的途径和方式;
- 4) 通过功能验证、技术检测查看用户撤回授权同意后, App 是否继续对外共享、转让、公开披露个人信息的行为;
- 5) 核查 App 服务端, 在用户撤回授权同意后, 是否停止对外共享、转让、公开披露其个人信息。

注: 常见的撤回对外共享授权的场景包括对第三方获取账号信息的授权、对小程序获取地理位置等权限的授权、对免密支付和自动支付等的授权等。

- e) 单元判定: 如果 1)、2) 为否定, 则本测评单元为不适用; 如果 1)、3)、4) 为肯定, 或 2)、3)、5) 为肯定, 则符合本测评单元指标要求, 否则不符合本测评单元指标要求。

6.4.5 个人信息主体注销账户的测评

6.4.5.1 测评项: 详见 GB/T 35273—2020 中 8.5 的 a) 。

6.4.5.1.1 测评单元 (RPI-11)

- a) 指标要求: 通过注册账户提供产品或服务的 App 提供者, 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) 测评对象: App、App 服务端
- c) 测评方式: 功能验证、服务端核查

d) 测评步骤:

- 1) 通过功能验证查看 App 个人信息保护政策或功能界面中是否向个人信息主体提供了注销账户的途径和方式;
- 2) 验证 App 提供的账户注销途径和方式是否可以正常执行, 且易于操作;
- 3) 服务端核查用户注销账户后, App 服务端是否对用户的个人信息作删除或匿名化处理。

e) 单元判定: 如果 1) 、2) 、3) 均为肯定, 则符合本测评单元指标要求, 否则不符合本测评单元指标要求。

6.4.5.2 测评项: 详见 GB/T 35273—2020 中 8.5 的 b) 。

6.4.5.2.1 测评单元 (RPI-12)

a) 指标要求: App 受理账户注销请求后, 需人工处理的, 应在 15 个工作日内完成核查和处理。

b) 测评对象: App、App 服务端、文档资料

c) 测评方式: 功能验证、服务端核查、文档审查

d) 测评步骤:

- 1) 查看 App 提供者的相关管理制度, 是否明确人工处理账户注销的核查和处理流程, 流程是否可在 15 个工作日内完成;
- 2) 通过功能验证查看 App 人工受理账户注销后, 是否可在 15 个工作日内完成核查和处理;
- 3) 核查 App 服务端对用户注销账号的处理机制, 是否能在 15 个工作日内完成核查和处理。

e) 单元判定: 如果 1) 、2) 、3) 为肯定, 则符合本测评单元指标要求, 否则不符合本测评单元指标要求。

6.4.5.3 测评项：详见 GB/T 35273—2020 中 8.5 的 c) 。

6.4.5.3.1 测评单元 (RPI-13)

- a) 指标要求：App 在账户注销时，如需进行身份核验，则所提供的个人信息不应多于注册、使用等服务环节收集的个人信息类型。
- b) 测评对象：App
- c) 测评方式：功能验证
- d) 测评步骤：
 - 1) 通过功能验证查看 App 在注册和使用等服务环节收集的个人信息类型；通过功能验证查看 App 在注销账户验证身份过程中，所提供的个人信息是否多于注册、使用等服务环节收集的个人信息类型。
- e) 单元判定：如果 1) 为否定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.4.5.4 测评项：详见 GB/T 35273—2020 中 8.5 的 d) 。

6.4.5.4.1 测评单元 (RPI-14)

- a) 指标要求：App 不应在注销账户功能中设置不合理或不必要的额外要求。
- b) 测评对象：App
- c) 测评方式：功能验证
- d) 测评步骤：
 - 1) 通过功能验证查看 App 在用户注销账户的流程中是否设置不合理的条件或提出额外要求增加用户义务。

注：注销账户时的不合理条件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。

- e) 单元判定：如果 1) 为否定，则符合本测评单元指标要求，否则不符

合本测评单元指标要求。

6.4.5.5 测评项：详见 GB/T 35273—2020 中 8.5 的 e) 。

6.4.5.5.1 测评单元 (RPI-15)

a) 指标要求：App 注销账户的过程中收集了个人敏感信息，应明确对收集个人敏感信息后的处理措施。

b) 测评对象：App、App 服务端

c) 测评方式：功能验证、服务端核查

d) 测评步骤：

1) 通过功能验证查看 App 注销账户的过程中是否需要收集个人敏感信息核验身份；

2) 通过功能验证查看 App 个人信息保护政策或功能界面中是否明确注销账户过程中对收集的个人信息使用后的处理措施，如达成目的后立即删除或匿名化处理等；

3) 核查 App 服务端是否在用户注销账户结束后，立即对所收集的个人信息进行了删除或匿名化处理。

e) 单元判定：如果 1) 为否定，则本测评单元为不适用；如果 1) 、2) 、3) 为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.4.5.6 测评项：详见 GB/T 35273—2020 中 8.5 的 f) 。

6.4.5.6.1 测评单元 (RPI-16)

a) 指标要求：App 应在个人信息主体注销操作完成后，及时删除或匿名化个人信息。因法律法规规定需要留存的个人信息，不能再次将其用于日常业务活动中。

b) 测评对象：App、App 服务端、文档资料

- c) 测评方式：功能验证、服务端核查、文档审查
- d) 测评步骤：
 - 1) 通过功能验证查看 App 个人信息保护政策中是否明确账户注销后如何处理个人信息；
 - 2) 核查 App 服务端在用户完成账户注销后，是否对用户个人信息进行删除或匿名化处理；
 - 3) 对于因法律法规规定需要留存的个人信息，核查 App 提供者提供的相关法律法规要求与实际留存的个人信息是否一致，核查是否有相应机制保障上述个人信息不再用于日常业务活动中。
- e) 单元判定：如果 1)、2)、3) 为肯定，则符合本单元测评指标要求，否则不符合本测评单元指标要求。

6.4.6 个人信息主体获取个人信息副本的测评

6.4.6.1 测评项：详见 GB/T 35273—2020 中的 8.6。

6.4.6.1.1 测评单元 (RPI-17)

- a) 指标要求：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本人的基本资料、身份信息、健康生理信息、教育工作信息副本的方法，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。
- b) 测评对象：App
- c) 测评方式：功能验证
- d) 测评步骤：
 - 1) 通过功能验证向 App 提供者提出获取本人基本资料、身份信息、健康生理信息、教育工作信息副本，核实其是否可按需求提供副本信息；

2) 通过功能验证向 App 提供者提出将本人基本资料、身份信息、健康生理信息、教育工作信息副本传输给第三方, 核实其是否可满足要求。

e) 单元判定: 如果 1) 或 2) 为肯定, 则符合本测评单元指标要求, 否则不符合本测评单元指标要求。

6.4.7 响应个人信息主体的请求的测评

6.4.7.1 测评项: 详见 GB/T 35273—2020 中 8.7 的 a) 。

6.4.7.1.1 测评单元 (RPI-18)

a) 指标要求: App 应在验证个人信息主体身份后, 及时响应个人信息主体基于 GB/T 35273—2020 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) 测评对象: App、文档资料

c) 测评方式: 功能验证、文档审查

d) 测评步骤:

1) 查看 App 提供者的个人信息安全相关管理制度, 是否明确及时响应个人信息主体基于 GB/T 35273—2020 8.1~8.6 提出的请求, 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, 并告知外部纠纷解决途径。

2) 基于 GB/T 35273—2020 8.1~8.6 向 App 提供者提出相关请求, 验证其是否可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。

e) 单元判定: 如果 1) 、2) 为肯定, 则符合本测评单元指标要求, 否则不符合本测评单元指标要求。

6.4.7.2 测评项: 详见 GB/T 35273—2020 中 8.7 的 b) 。

6.4.7.2.1 测评单元 (RPI-19)

- a) 指标要求: App 功能界面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;
- b) 测评对象: App
- c) 测评方式: 功能验证
- d) 测评步骤:
 - 1) 通过功能验证查看 App 功能界面是否提供有效的在线访问、更正、删除、撤回授权同意、注销账户等功能。
- e) 单元判定: 如果 1) 为肯定, 则符合本测评单元指标要求, 否则不符合本测评单元指标要求。

6.4.7.3 测评项: 详见 GB/T 35273—2020 中 8.7 的 c) 。

6.4.7.3.1 测评单元 (RPI-20)

- a) 指标要求: App 对合理的请求不应收取费用, 但对一定时期内多次重复的请求, 可视情况收取一定成本费用, 同时 App 的个人信息保护政策应特别针对请求收取费用事项进行说明。
- b) 测评对象: App、文档资料
- c) 测评方式: 功能验证、文档审查
- d) 测评步骤:
 - 1) 通过功能验证查看 App 响应用户请求是否涉及收费项目;
 - 2) 查看 App 提供者的个人信息安全相关管理制度中是否建立响应用户请求的收费机制, 并对收费事项及成本费用进行说明;
 - 3) 查看 App 个人信息保护政策中是否针对收取费用事项进行说明;

4) 验证 App 响应用户的请求收费功能是否合理以及收取的成本费用是否合理。

e) 单元判定：如果 1) 为否定，则本测评单元为不适用；如果 1) 至 4) 均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.4.7.4 测评项：详见 GB/T 35273—2020 中 8.8 的 d) 。

6.4.7.4.1 测评单元 (RPI-21)

a) 指标要求：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，App 提供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。

b) 测评对象：制度文件

c) 测评方式：文档审查

d) 测评步骤：

1) 查看 App 提供者的个人信息安全相关管理制度中是否梳理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情形，提出替代方法，并在个人信息保护政策中做出相应说明。

e) 单元判定：如果 1) 为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.4.7.5 测评项：详见 GB/T 35273—2020 中 8.7 的 e) 。

6.4.7.5.1 测评单元 (RPI-22)

a) 指标要求：App 提供者不响应个人信息主体基于 GB/T 35273—2020 8.1~8.6 提出的请求的情形应在 GB/T 35273—2020 中 8.7 节 e) 项规定范围内。

b) 测评对象：App、文档资料

c) 测评方式：功能验证、文档审查

d) 测评步骤：

1) 查看 App 提供者的个人信息安全相关管理制度中是否规定可不响应个人信息主体基于 GB/T 35273—2020 8.1~8.6 提出的请求的情形；

2) 查看规定的情形是否在 GB/T 35273—2020 中 8.7 节 e) 项规定范围内；

3) 询问并查看 App 提供者是否有不响应用户个人信息安全请求的记录；

4) 查看不响应的情形是否在 GB/T 35273—2020 中 8.7 节 e) 项规定范围内。

e) 单元判定：如果 1) 、3) 为否定，或者 1) 至 4) 均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.4.7.6 测评项：详见 GB/T 35273—2020 中 8.8 的 f) 。

6.4.7.6.1 测评单元 (RPI-23)

a) 指标要求：App 提供者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。

b) 测评对象：App、文档资料

c) 测评方式：功能验证、文档审查

d) 测评步骤：

1) 通过功能验证查看 App 是否存在不响应个人信息主体的请求的情况；

2) 查看 App 提供者的个人信息安全相关管理制度中是否梳理不响应个人信息主体的请求的情形及理由，是否明确决定不响应请求时应向个人信息主体告知理由，并提供投诉的途径；

- 3) 查看 App 个人信息保护政策中是否提供了投诉的途径;
- 4) 验证投诉途径是否有效。
- e) 单元判定: 如果 1) 为否定, 则本测评单元为不适用; 如果 1) 至 4) 为肯定, 则符合本测评单元指标要求, 否则不符合本测评单元指标要求。

6.4.8 投诉管理的测评

6.4.8.1 测评项: 详见 GB/T 35273—2020 中的 8.8。

6.4.8.1.1 测评单元 (RPI-24)

- a) 指标要求: App 提供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。
- b) 测评对象: App、App 服务端、文档资料
- c) 测评方式: 功能验证、服务端核查、文档审查
- d) 测评步骤:
 - 1) 查看 App 提供者的个人信息安全相关管理制度是否建立投诉管理机制和投诉跟踪流程, 并明确了投诉响应时限;
 - 2) 核查 App 服务端是否建立投诉管理机制和投诉跟踪流程;
 - 3) 查看 App 个人信息保护政策或功能界面中其是否向用户提供了投诉渠道或功能;
 - 4) 通过投诉渠道或功能就个人信息相关问题进行投诉, 验证其是否在十五个工作日内进行响应。
- e) 单元判定: 如果 1) 至 4) 为肯定, 则符合本测评单元指标要求, 否则不符合本测评单元指标要求。

6.5 个人信息的委托处理、共享、转让、公开披露的测评

6.5.1 委托处理的测评

6.5.1.1 测评项：详见 GB/T 35273—2020 中 9.1 的 a) 。

6.5.1.1.1 测评单元 (EPI-01)

- a) 指标要求：App 提供者作出委托行为，不应超出已征得个人信息主体授权同意的范围或应遵守 GB/T 35273—2020 5.6 所列情形；
- b) 测评对象：App、App 服务端、文档资料
- c) 测评方式：技术检测、服务端核查、文档审查、人员访谈
- d) 测评步骤：
 - 1) 通过技术检测 App、查看相关文档资料及询问 App 提供者等方式，查看 App 提供者是否存在委托处理行为；
 - 2) 查看 App 提供者的个人信息安全相关管理制度，是否明确规定委托行为不得超出已征得个人信息主体授权同意的范围或应遵守 GB/T35273—2020 5.6 所列情形；
 - 3) 查看委托行为的相关记录，是否超出已征得个人信息主体授权同意的范围或未遵守 GB/T 35273—2020 5.6 所列情形。
- e) 单元判定：如果 1) 为否定，则本测试单元为不适用。如果 1) 、2) 为肯定，3) 为否定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.5.1.2 测评项：详见 GB/T 35273—2020 中 9.1 的 b) 。

6.5.1.2.1 测评单元 (EPI-02)

- a) 指标要求：App 提供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 GB/T 35273—2020 11.5 节数据安全能力要求。
- b) 测评对象：文档资料
- c) 测评方式：人员访谈、文档审查
- d) 测评步骤：

- 1) 通过技术检测 App、查看相关文档资料及询问 App 提供者等方式, 查看 App 提供者是否存在委托处理行为;
 - 2) 查看 App 提供者的个人信息安全相关管理制度, 是否明确规定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 GB/T 35273—2020 11.5 节数据安全能力要求;
 - 3) 询问 App 提供者是否对委托行为进行个人信息安全影响评估, 并查看是否提供个人信息安全影响评估相关记录文档;
 - 4) 查看个人信息安全影响评估记录文档, 是否确保受委托者达到 GB/T 35273—2020 11.5 节数据安全能力要求。
- e) 单元判定: 如果 1) 为否定, 则本测评单元为不适用; 如果 1) 至 4) 均为肯定, 则符合本测评单元指标要求, 否则不符合本测评单元指标要求。

6.5.1.3 测评项: 详见 GB/T 35273—2020 中 9.1 的 c) 。

6.5.1.3.1 测评单元 (EPI-03)

- a) 指标要求: App 提供者应要求受委托者达到 GB/T 35273—2020 中 9.1 的 c) 中 1) 至 5) 项要求。
- b) 测评对象: 文档资料
- c) 测评方式: 文档审查、人员访谈
- d) 测评步骤:
 - 1) 通过技术检测 App、查看相关文档资料及询问 App 提供者等方式, 查看 App 提供者是否存在委托处理行为;
 - 2) 询问并查看 App 提供者是否具有对受委托者做出安全要求的管理制度, 且要求内容覆盖 GB/T 35273—2020 中 9.1 的 c) 中 1) 至 5) 项的要求;
 - 3) 询问并查看 App 提供者是否对委托行为签署合同等文件;

4) 查看委托合同等文件中是否规定 GB/T 35273—2020 9.1 c) 所列的 5 条安全要求。

e) 单元判定：如果 1) 为否定，则本测评单元为不适用；如果 1) 至 4) 均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.5.1.4 测评项：详见 GB/T 35273—2020 中 9.1 的 d) 。

6.5.1.4.1 测评单元 (EPI-04)

a) 指标要求：App 提供者应对受委托者进行监督，通过合同等方式规定受委托者的责任和义务，并对受委托者进行审计。

b) 测评对象：文档资料

c) 测评方式：文档审查、人员访谈

d) 测评步骤：

1) 通过技术检测 App、查看相关文档资料及询问 App 提供者等方式，查看 App 提供者是否存在委托处理行为；

2) 查看委托合同等相关文档，是否规定了受委托者的责任和义务；

3) 询问 App 提供者是否对受委托者进行审计；

4) 查看相关审计记录是否包含对受委托者处理个人信息行为的审计情况。

e) 单元判定：如果 1) 为否定，则本测评单元为不适用；如果 1) 至 4) 均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.5.1.5 测评项：详见 GB/T 35273—2020 中 9.1 的 e) 。

6.5.1.5.1 测评单元 (EPI-05)

a) 指标要求：App 提供者应准确记录和保存委托处理个人信息的情况。

- b) 测评对象：文档资料
- c) 测评方式：文档审查、人员访谈
- d) 测评步骤：
 - 1) 通过技术检测 App、查看相关文档资料及询问 App 提供者等方式，查看 App 提供者是否存在委托处理行为；
 - 2) 询问并查看 App 提供者是否制定相关制度，明确规定委托处理个人信息时准确记录和保存相关情况；
 - 3) 询问并查看 App 提供者是否记录委托处理行为以及保存委托处理行为的相关文档；
 - 4) 查看相关文档是否包括受委托方及其联系方式、委托处理个人信息类型、委托处理个人信息数量、委托处理个人信息目的等内容。
- e) 单元判定：如果 1) 为否定，则本测评单元为不适用；如果 1) 至 4) 均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.5.1.6 测评项：详见 GB/T 35273—2020 中 9.1 的 f) 。

6.5.1.6.1 测评单元 (EPI-06)

- a) 指标要求：App 提供者得知或者发现受委托者未按照委托要求处理个人信息时，或未能有效履行个人信息安全保护责任时，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的个人信息。
- b) 测评对象：文档资料、App 服务端
- c) 测评方式：文档审查、服务端核查、人员访谈
- d) 测评步骤：

- 1) 通过技术检测 App、查看相关文档资料及询问 App 提供者等方式，查看 App 提供者是否存在委托处理行为；
 - 2) 查看 App 提供者的个人信息安全相关管理制度，是否要求在得知或者发现受委托者未按照委托要求处理个人信息时，应采取行动控制或者消除个人信息面临的安全风险；
 - 3) 询问 App 提供者是否曾出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情况；若曾出现上述情况，查看当时的处理记录，判断 App 提供者是否立即要求受委托方停止相关行为，且采取或要求受委托方采取有效补救措施控制或消除个人信息面临的安全风险；
 - 4) 核查 App 服务端是否具备在上述情况下立即控制或消除个人信息安全风险的技术措施。
- e) 单元判定：如果 1) 为否定，则本测评单元为不适用；如果 1) 至 4) 为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.5.2 个人信息共享、转让的测评

6.5.2.1 测评项：详见 GB/T 35273—2020 中 9.2 的 a) 。

6.5.2.1.1 测评单元 (EPI-07)

- a) 指标要求：App 提供者共享、转让个人信息前，应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) 测评对象：App、App 服务端、文档资料
- c) 测评方式：文档审查、服务端核查、人员访谈
- d) 测评步骤：
 - 1) 通过 App 功能验证、查看文档资料及询问 App 提供者等方式，查看 App 提供者是否存在共享、转让个人信息的行为；

- 2) 查看 App 提供者的个人信息安全相关管理制度，是否明确个人信息共享、转让前应开展个人信息安全影响评估；
 - 3) 查看是否有个人信息安全影响评估报告以及依据评估结果实施的保护措施的相关文档；
 - 4) 核查 App 服务端、询问 App 提供者、查看相关的文档，判断保护措施是否有效实施。
- e) 单元判定：如果 1) 为否定，则本测评单元为不适用；如果 1) 至 4) 均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.5.2.2 测评项：详见 GB/T 35273—2020 中 9.2 的 b) 。

6.5.2.2.1 测评单元 (EPI-08)

- a) 指标要求：App 提供者应向用户告知共享、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。去标识化后且无法重新识别个人信息主体的信息除外。
- b) 测评对象：App、App 服务端、文档资料
- c) 测评方式：功能验证、技术检测、服务端核查、文档审查、人员访谈
- d) 测评步骤：
 - 1) 通过 App 功能验证、查看文档资料及询问 App 提供者等方式，查看 App 提供者是否存在共享、转让个人信息的行为；
 - 2) 查看 App 提供者的个人信息安全相关管理制度，是否明确规定告知用户共享、转让个人信息的目的、数据接收方的类型，并事先征得个人信息主体的授权同意；
 - 3) 查看 App 的个人信息保护政策，其中是否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，并征得用户授权同意；

- 4) 通过技术检测 App 中共享给第三方的个人信息和第三方类型，判断是否与 App 个人信息保护政策中说明的一致；
 - 5) 核查 App 服务端共享给第三方的个人信息和第三方类型，判断是否与 App 个人信息保护政策中说明的一致；
 - 6) 询问 App 提供者是否存在向接入的第三方应用提供个人信息的行为，若存在则判断是否与 App 个人信息保护政策中说明的一致；
 - 7) 询问并查看未告知的个人信息是否是经去标识化处理的个人信息。
- e) 单元判定：如果 1) 为否定，则本测评单元为不适用；如果 1) 至 7) 为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.5.2.3 测评项：详见 GB/T 35273—2020 中 9.2 的 c) 。

6.5.2.3.1 测评单元 (EPI-09)

- a) 指标要求：App 提供者共享、转让个人敏感信息前，除 GB/T 35273—2020 9.2 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。
- b) 测评对象：App、App 服务端、文档资料
- c) 测评方式：功能验证、技术检测、服务端核查、文档审查
- d) 测评步骤：
 - 1) 通过功能验证和技术检测 App, 查看 App 是否收集个人敏感信息；
 - 2) 技术检测 App 是否直接向第三方共享个人敏感信息；
 - 3) 询问并核查 App 服务端是否向第三方共享、转让个人敏感信息；
 - 4) 查看 App 的个人信息保护政策是否向个人信息主体告知除 GB/T 35273—2020 9.2 b) 中告知的内容外，涉及的个人敏感信息的类型、

数据接收方的身份和数据安全能力，并通过弹窗、界面文字说明、用户主动点击同意等明示方式征得个人信息主体同意；

5) 查看 App 提供者的个人信息安全相关管理制度，是否明确规定共享、转让个人敏感信息应额外告知涉及的个人敏感信息的类型、数据接收方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。

e) 单元判定：如果 1) 为否定，则本测评单元为不适用；如果 1) 至 5) 为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.5.2.4 测评项：详见 GB/T 35273—2020 中 9.2 的 d) 。

6.5.2.4.1 测评单元 (EPI-10)

a) 指标要求：App 提供者在共享、转让个人信息时，应通过合同等方式规定数据接收方的责任和义务。

b) 测评对象：文档资料

c) 测评方式：文档审查

d) 测评步骤：

1) 通过 App 功能验证、查看文档资料及询问 App 提供者等方式，查看 App 提供者是否存在共享、转让个人信息的行为；

2) 查看 App 提供者的数据共享、转让合同或协议，是否通过合同等方式规定数据接收方的责任和义务。

e) 单元判定：如果 1) 为否定，则本测评单元为不适用；如果 1) 、2) 为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.5.2.5 测评项：详见 GB/T 35273—2020 中 9.2 的 e) 。

6.5.2.5.1 测评单元 (EPI-11)

a) 指标要求：App 提供者应准确记录和保存个人信息的共享、转让的情况，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；

- b) 测评对象：文档资料、App 服务端
- c) 测评方式：文档审查、服务端核查、人员访谈
- d) 测评步骤：
 - 1) 通过 App 功能验证、查看文档资料及询问 App 提供者等方式，查看 App 提供者是否存在共享、转让个人信息的行为；
 - 2) 查看 App 提供者的个人信息安全相关管理制度，是否明确规定应准确记录和保存个人信息的共享、转让的情况；
 - 3) 询问并查看个人信息的共享、转让的记录，是否包括共享、转让的日期、规模、目的，以及数据接收方基本情况等；
 - 4) 对于实时进行的共享行为，查看系统中是否有相应记录。
- e) 单元判定：如果 1) 为否定，则本测评单元为不适用；如果 1) 至 4) 为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.5.2.6 测评项：详见 GB/T 35273—2020 中 9.2 的 f) 。

6.5.2.6.1 测评单元 (EPI-12)

- a) 指标要求：App 提供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。
- b) 测评对象：文档资料、App 服务端
- c) 测评方式：文档审查、服务端核查、人员访谈
- d) 测评步骤：
 - 1) 通过 App 功能验证、查看文档资料及询问 App 提供者等方式，查看 App 提供者是否存在共享、转让个人信息的行为；

- 2) 查看 App 提供者的个人信息安全相关管理制度, 是否明确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, 应立即采取行动控制或消除个人信息面临的安全风险;
 - 3) 询问是否曾出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情况; 若曾出现上述情况, 查阅当时的处理记录, 验证被评估对象是否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控制或消除个人信息面临的安全风险;
 - 4) 服务端核查 App 提供者是否具备在上述情况下立即控制或消除个人信息安全风险的技术措施。
- e) 单元判定: 如果 1) 为否定, 则本测评单元为不适用; 如果 1) 至 4) 为肯定, 则符合本测评单元指标要求, 否则不符合本测评单元指标要求。

6.5.2.7 测评项: 详见 GB/T 35273—2020 中 9.2 的 g) 。

6.5.2.7.1 测评单元 (EPI-13)

- a) 指标要求: App 提供者应承担因共享、转让个人信息对个人信息主体合法权益造成损害的相应责任。
- b) 测评对象: App
- c) 测评方式: 功能验证
- d) 测评步骤:
 - 1) 通过 App 功能验证、查看文档资料及询问 App 提供者等方式, 查看 App 提供者是否存在共享、转让个人信息的行为;
 - 2) 查阅 App 个人信息保护政策等相关文档是否有在对个人信息主体合法权益造成损害时承担相应责任的说明。
- e) 单元判定: 如果 1) 为否定, 则本测评单元为不适用; 如果 1) 、2) 为肯定, 则符合本测评单元指标要求, 否则不符合本测评单元指标要求。

6.5.2.8 测评项: 详见 GB/T 35273—2020 中 9.2 的 h) 。

6.5.2.8.1 测评单元 (EPI-14)

- a) 指标要求: App 提供者应帮助个人信息主体了解数据接收方对个人信息的保存、使用等情况, 以及个人信息主体的权利。
- b) 测评对象: App、App 服务端、文档资料
- c) 测评方式: 功能验证、服务端核查、文档审查
- d) 测评步骤:
 - 1) 通过 App 功能验证、查看文档资料及询问 App 提供者等方式, 查看 App 提供者是否存在共享、转让个人信息的行为;
 - 2) 查看 App 提供者的个人信息安全相关管理制度, 是否明确应帮助个人信息主体了解数据接收方对个人信息的保存、使用等情况, 以及个人信息主体的权利;
 - 3) 通过功能验证查看 App 是否提供了个人信息主体了解数据接收方对个人信息的保存、使用等情况以及个人信息主体权利的途径;
 - 4) 验证个人信息主体了解数据接收方对个人信息的保存、使用等情况以及个人信息主体权利的途径是否有效。
- e) 单元判定: 如果 1) 为否定, 则本测评单元为不适用; 如果 1) 至 4) 为肯定, 则符合本测评单元指标要求, 否则不符合本测评单元指标要求。

6.5.2.9 测评项: 详见 GB/T 35273—2020 中 9.2 的 i) 。

6.5.2.9.1 测评单元 (EPI-15)

- a) 指标要求: 因业务需要, App 提供者确需共享、转让个人生物识别信息的, 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。
- b) 测评对象: App、App 服务端、文档资料

- c) 测评方式：功能验证、服务端核查、文档审查
- d) 测评实施：
 - 1) 通过功能验证查看 App 是否存在共享个人生物识别信息的行为；
 - 2) 询问并核查 App 服务端是否存在将收集的 personal 生物识别信息进行共享、转让的行为；
 - 3) 若存在上述行为，验证 App 是否通过弹窗告知、显著标识等方式单独向个人信息主体告知目的、涉及的 personal 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。
- e) 单元判定：如果 1) 、2) 为否定，则本测评单元为不适用；如果 1) 或 2) 为肯定，且 3) 为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.5.3 收购、兼并、重组、破产时的个人信息转让的测评

6.5.3.1 测评项：详见 GB/T 35273—2020 中 9.3 的 a) 。

6.5.3.1.1 测评单元 (EPI-16)

- a) 指标要求：当 App 提供者发生收购、兼并、重组、破产等变更时，应向个人信息主体告知有关情况。
- b) 测评对象：文档资料
- c) 测评方式：文档审查、人员访谈
- d) 测评步骤：
 - 1) 查看 App 提供者是否有收购、兼并、重组、破产时的个人信息转让的管理制度，制度中应明确向个人信息主体告知有关情况；
 - 2) 如果存在收购、兼并、重组的情况，查阅是否有告知的相关记录。
- e) 单元判定：如果 1) 、2) 为肯定，则符合本测评单元指标要求，否

则不符合本测评单元指标要求。

6.5.3.2 测评项：详见 GB/T 35273—2020 中 9.3 的 b) 。

6.5.3.2.1 测评单元 (EPI-17)

a) 指标要求：当 App 提供者发生收购、兼并、重组、破产等变更时，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。

b) 测评对象：App、文档资料

c) 测评方式：功能验证、文档审查、人员访谈

d) 测评步骤：

1) 查看 App 提供者是否有收购、兼并、重组、破产时的个人信息转让的管理制度；

2) 如果 App 提供者是变更后的个人信息控制者，询问并查看其是否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，是否重新取得个人信息主体的明示同意。

e) 单元判定：如果 1) 、2) 为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.5.3.3 测评项：详见 GB/T 35273—2020 中 9.3 的 c) 。

6.5.3.3.1 测评单元 (EPI-18)

a) 指标要求：App 提供者如破产且无承接方，应对数据做删除处理。

b) 测评对象：文档资料

c) 测评方式：文档审查

d) 测评步骤：

1) 查看 App 提供者的相关管理文档，是否明确在破产且无承接方时，对数据做删除处理。

- e) 单元判定：如果 1) 为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.5.4 个人信息公开披露的测评

6.5.4.1 测评项：详见 GB/T 35273—2020 中 9.4 的 a) 。

6.5.4.1.1 测评单元 (EPI-19)

- a) 指标要求：App 提供者公开披露个人信息前，应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) 测评对象：文档资料、App 服务端、App
- c) 测评方式：文档审查、人员访谈、服务端核查、功能验证
- d) 测评步骤：
 - 1) 通过 App 功能验证，询问 App 提供者，判断是否存在个人信息公开披露的行为；
 - 2) 查看 App 提供者是否建立个人信息公开披露时的个人信息安全影响评估制度；
 - 3) 查看是否有个人信息安全影响评估报告以及依据评估结果应实施的保护措施内容；
 - 4) 通过 App 功能验证、核查 App 服务端，查看保护措施是否有效实施。
- e) 单元判定：如果 1) 为否定，则本测评单元为不适用；如果 1) 至 4) 均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.5.4.2 测评项：详见 GB/T 35273—2020 中 9.4 的 b) 。

6.5.4.2.1 测评单元 (EPI-20)

- a) 指标要求：App 提供者应向用户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的明示同意。

b) 测评对象: App、文档资料

c) 测评方式: 功能验证、文档审查

d) 测评步骤:

1) 通过 App 功能验证, 询问 App 提供者, 判断是否存在个人信息公开披露的行为;

2) 查看 App 提供者是否有个人信息公开披露的管理制度明确规定告知用户公开披露个人信息的目的、类型, 并事先征得个人信息主体的明示同意;

3) 通过 App 功能验证, 查看 App 个人信息保护政策或涉及公开披露个人信息的功能界面中是否向个人信息主体告知公开披露个人信息的目的、类型, 并征得用户明示同意。

e) 单元判定: 如果 1) 为否定, 则本测评单元为不适用; 如果 1) 、2) 、3) 均为肯定, 则符合本测评单元指标要求, 否则不符合本测评单元指标要求。

6.5.4.3 测评项: 详见 GB/T 35273—2020 中 9.4 的 c) 。

6.5.4.3.1 测评单元 (EPI-21)

a) 指标要求: App 提供者公开披露个人敏感信息前, 除 GB/T 35273—2020 9.4 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。

b) 测评对象: App、文档资料

c) 测评方式: 功能验证、文档审查

d) 测评步骤:

- 1) 通过 App 功能验证, 询问 App 提供者, 判断是否存在个人敏感信息公开披露的行为;
 - 2) 如果 App 存在公开披露个人敏感信息的行为, 查看是否在公开披露前, 除 GB/T 35273—2020 9.4 b) 中规定告知的内容外, 还向个人信息主体告知涉及的个人敏感信息的内容;
 - 3) 查看 App 提供者是否有相应的管理制度, 要求公开披露个人敏感信息前, 应向个人信息主体告知涉及的个人敏感信息的内容。
- e) 单元判定: 如果 1) 为否定, 则本测评单元为不适用; 如果 1) 、 2) 、 3) 均为肯定, 则符合本测评单元指标要求, 否则不符合本测评单元指标要求。

6.5.4.4 测评项: 详见 GB/T 35273—2020 中 9.4 的 d) 。

6.5.4.4.1 测评单元 (EPI-22)

- a) 指标要求: App 提供者应准确记录和保存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;
- b) 测评对象: App、文档资料、App 服务端
- c) 测评方式: 功能验证、人员访谈、文档审查、服务端核查
- d) 测评步骤:
 - 1) 通过 App 功能验证, 询问 App 提供者, 判断是否存在个人信息公开披露的行为;
 - 2) 查看 App 提供者是否有个人信息公开披露的管理制度明确规定应准确记录和保存个人信息的公开披露的情况;
 - 3) 通过 App 功能验证、核查 App 服务端、询问 App 提供者, 查看是否存在个人信息公开披露的情况, 如果存在则查看个人信息的公开披露的记录, 查看记录内容是否包括公开披露的日期、规模、目的、公开范围等;

4) 对于 App 中进行的公开披露行为, 查看系统中是否有相应记录。

e) 单元判定: 如果 1) 为否定, 则本测评单元为不适用; 如果 1) 至 4) 均为肯定, 则符合本测评单元指标要求, 否则不符合本测评单元指标要求。

6.5.4.5 测评项: 详见 GB/T 35273—2020 中 9.4 的 e) 。

6.5.4.5.1 测评单元 (EPI-23)

a) 指标要求: App 提供者应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。

b) 测评对象: App

c) 测评方式: 文档审查

d) 测评步骤:

1) 通过 App 功能验证, 询问 App 提供者, 判断是否存在个人信息公开披露的行为;

2) 查阅 App 个人信息保护政策等相关文档是否有因公开披露个人信息对个人信息主体合法权益造成损害时承担相应责任的说明。

e) 单元判定: 如果 1) 为否定, 则本测评单元为不适用; 如果 1) 、2) 为肯定, 则符合本测评单元指标要求, 否则不符合本测评单元指标要求。

6.5.4.6 测评项: 详见 GB/T 35273—2020 中 9.4 的 f) 。

6.5.4.6.1 测评单元 (EPI-24)

a) 指标要求: App 提供者不得公开披露个人生物识别信息。

b) 测评对象: App、App 服务端、文档资料

c) 测评方式: 功能验证、服务端核查、文档审查

d) 测评步骤:

- 1) 通过 App 功能验证, 询问 App 提供者, 判断是否存在个人信息公开披露的行为;
 - 2) 查看 App 提供者是否有不得公开披露个人生物识别信息的管理制度;
 - 3) 通过功能验证、服务端核查, 查看 App 提供者是否存在公开披露个人生物识别信息的情况。
- e) 单元判定: 如果 1) 为否定, 则本测评单元为不适用; 如果 1) 、2) 为肯定且 3) 为否定, 则符合本测评单元指标要求, 否则不符合本测评单元指标要求。

6.5.4.7 测评项: 详见 GB/T 35273—2020 中 9.4 的 g) 。

6.5.4.7.1 测评单元 (EPI-25)

- a) 指标要求: App 提供者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。
- b) 测评对象: App、App 服务端、文档资料
- c) 测评方式: 功能验证、服务端核查、文档审查
- d) 测评步骤:
 - 1) 通过 App 功能验证, 询问 App 提供者, 判断是否存在个人信息公开披露的行为;
 - 2) 查看 App 提供者是否有不得公开披露种族、民族、政治观点、宗教信仰等个人敏感数据的分析结果的管理制度;
 - 3) 通过功能验证、服务端核查, 查看 App 是否存在公开披露种族、民族、政治观点、宗教信仰等个人敏感数据的分析结果的情况。
- e) 单元判定: 如果 1) 为否定, 则本测评单元为不适用; 如果 1) 、2) 为肯定且 3) 为否定, 则符合本测评单元指标要求, 否则不符合本测评单元指标要求。

6.5.5 共享、转让、公开披露个人信息时事先征得授权同意的例外的测评

6.5.5.1 测评项：详见 GB/T 35273—2020 中的 9.5。

6.5.5.1.1 测评单元 (EPI-26)

- a) 指标要求：App 提供者共享、转让、公开披露个人信息时事先征得授权同意的例外的情形应在 GB/T 35273—2020 9.5 列举范围内。
- b) 测评对象：App、App 服务端、文档资料
- c) 测评方式：功能验证、服务端核查、文档审查
- d) 测评步骤：
 - 1) 查看 App 的个人信息保护政策，是否声明了不合理的共享、转让、公开披露个人信息时事先征得授权同意的例外；
 - 2) 通过 App 功能验证、核查 App 服务端、询问 App 提供者等方式，判断是否存在未征得用户授权同意共享、转让、公开披露个人信息，且不在事先征得授权同意的例外范围的行为。
- e) 单元判定：如果 1)、2) 为否定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.5.6 共同个人信息控制者的测评

6.5.6.1 测评项：详见 GB/T 35273—2020 中 9.6 的 a)。

6.5.6.1.1 测评单元 (EPI-27)

- a) 指标要求：当 App 提供者与第三方为共同个人信息控制者时，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) 测评对象：App、文档资料
- c) 测评方式：功能验证、技术检测、文档审查、人员访谈

d) 测评步骤:

- 1) 通过 App 功能验证、技术检测, 询问 App 提供者, 判断是否存在与第三方为共同个人信息控制者的情况;
- 2) 查看 App 提供者是否建立相关管理制度, 要求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;
- 3) 查看合同等与第三方签订的文件是否包含应满足个人信息安全方面的要求, 以及在个人信息安全方面双方分别承担的责任和义务;
- 4) 查看是否通过个人信息保护政策等方式向用户明确告知关于共同个人信息者应满足的个人信息安全要求以及双方分别承担的责任和义务等内容。

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。

- e) 单元判定: 如果 1) 为否定, 则本测试单元为不适用。如果 1) 至 4) 均为肯定, 则符合本测评单元指标要求, 否则不符合本测评单元指标要求。

6.5.6.2 测评项: 详见 GB/T 35273—2020 中 9.6 的 b) 。

6.5.6.2.1 测评单元 (EPI-28)

- a) 指标要求: App 提供者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, 应承担因第三方引起的个人信息安全责任。

- b) 测评对象: App、文档资料

- c) 测评方式：功能验证、技术检测、文档审查、人员访谈
- d) 测评步骤：
 - 1) 通过 App 功能验证、技术检测，询问 App 提供者，判断是否存在与第三方为共同个人信息控制者的情况；
 - 2) 查看是否在个人信息保护政策或其他文档中向用户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；
 - 3) 如果未告知，检查是否有对第三方引起的个人信息安全责任的免责声明。。
- e) 单元判定：如果 1) 为否定，则本测评单元为不适用。如果 1) 、2) 为肯定，或 1) 为肯定且 2) 、3) 为否定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.5.7 第三方接入管理的测评

6.5.7.1 测评项：详见 GB/T 35273—2020 中 9.7 的 a) 。

6.5.7.1.1 测评单元 (EPI-29)

- a) 指标要求：App 提供者应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) 测评对象：App 服务端、文档资料
- c) 测评方式：服务端核查、文档审查、人员访谈
- d) 测评步骤：
 - 1) 查看 App 提供者的相关管理制度，是否明确第三方产品或服务接入管理机制、工作流程、安全评估制度等；
 - 2) 核查 App 服务端、询问 App 提供者的第三方产品或服务业务相关责任人，记录是否按照相关管理制度的要求进行了第三方接入管理，

是否形成了相关的第三方接入管理记录, 第三方接入安全评估记录等文档。

- e) 单元判定: 如果 1) 、2) 均为肯定, 则符合本测评单元指标要求, 其他情况不符合本测评单元指标要求。

6.5.7.2 测评项: 详见 GB/T 35273—2020 中 9.7 的 b) 。

6.5.7.2.1 测评单元 (EPI-30)

- a) 指标要求: App 提供者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。

b) 测评对象: 文档资料

c) 测评方式: 文档审查

d) 测评步骤:

1) 查看 App 提供者是否具备与第三方产品或服务提供者签订的接入有关合同等文件, 明确双方应承担的责任、义务、个人信息保护方面采取的措施;

2) 查看合同等相关文件是否明确第三方产品或服务收集的个人信息类型、申请的系统权限、个人信息收集目的、所收集的个人信息保存期限和个人信息处理方式。

- e) 单元判定: 如果以上 1) 、2) 为肯定, 则符合本测评单元指标要求, 否则不符合本测评单元指标要求。

6.5.7.3 测评项: 详见 GB/T 35273—2020 中 9.7 的 c) 。

6.5.7.3.1 测评单元 (EPI-31)

- a) 指标要求: App 提供者应向个人信息主体明确标识产品或服务由第三方提供。

b) 测评对象: App、App 服务端

c) 测评方式：功能验证、技术检测、人员访谈、服务端核查

d) 测评步骤：

- 1) 通过 App 功能验证、技术检测，核查 App 服务端，以及询问 App 提供者等方式，判断 App 是否存在由第三方提供的功能；
- 2) 如果存在第三方接入，通过功能验证查看 App 功能界面中是否明确标识产品或服务由第三方提供。

e) 单元判定：如果 1) 为否定，则本测评单元为不适用；如果 1) 、2) 为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.5.7.4 测评项：详见 GB/T 35273—2020 中 9.7 的 d) 。

6.5.7.4.1 测评单元 (EPI-32)

a) 指标要求：App 提供者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。

b) 测评对象：文档资料

c) 测评方式：文档审查、人员访谈

d) 测评步骤：

- 1) 询问 App 提供者是否有第三方接入有关合同和管理记录；
- 2) 查看第三方接入有关合同和管理记录的文件资料是否完整；
- 3) 查看管理记录，是否涵盖了第三方产品或服务接入、评估、更改、停止、责任落实情况等记录。

e) 单元判定：如果 1) 、2) 、3) 为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.5.7.5 测评项：详见 GB/T 35273—2020 中 9.7 的 e) 。

6.5.7.5.1 测评单元 (EPI-33)

- a) 指标要求: App 提供者应要求第三方根据 GB/T 35273—2020 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。
- b) 测评对象: App、App 服务端、文档资料
- c) 测评方式: 功能验证、服务端核查、文档审查
- d) 测评步骤:
 - 1) 通过功能验证查看 App 中的第三方收集个人信息时是否征得用户同意;
 - 2) 查看 App 提供者与第三方签订的合同或合作协议, 是否明确要求第三方根据 GB/T 35273—2020 相关要求向个人信息主体征得收集个人信息的授权同意;
 - 3) 核查 App 服务端是否具备必要时核验第三方向个人信息主体征得收集个人信息的授权同意的实现方式的机制。
- e) 单元判定: 如果 1)、2)、3) 为肯定, 则符合本测评单元指标要求, 否则不符合本测评单元指标要求。

6.5.7.6 测评项: 详见 GB/T 35273—2020 中 9.7 的 f) 。

6.5.7.6.1 测评单元 (EPI-34)

- a) 指标要求: App 提供者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的机制, 以供个人信息主体查询、使用。
- b) 测评对象: App、文档资料
- c) 测试方式: 功能验证、文档审查
- d) 测评步骤:
 - 1) 查看 App 提供者与第三方签订的合同或合作协议, 是否明确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的机制;

- 2) 通过 App 功能验证查看第三方产品或服务的个人信息保护政策或功能页面, 查看第三方产品或服务的投诉链接或联系方式; 验证第三方产品或服务的投诉链接或联系方式是否有效;
 - 3) 查看是否可以通过 App 提供者的反馈渠道向第三方进行请求和投诉。
- e) 单元判定: 如果 1) 、 2) 、 3) 为肯定, 则符合本测评单元指标要求, 否则不符合本测评单元指标要求。

6.5.7.7 测评项: 详见 GB/T 35273—2020 中 9.7 的 g) 。

6.5.7.7.1 测评单元 (EPI-35)

- a) 指标要求: App 提供者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。
- b) 测评对象: 文档资料、App 服务端
- c) 测评方式: 文档审查、人员访谈、服务端核查
- d) 测评步骤:
 - 1) 查看 App 提供者有关接入第三方产品或服务的管理机制、评估机制和 workflow 资料, 是否有对第三方产品或服务动态监测或定期进行个人信息安全审计的方式说明; 查看管理机制中是否规定停止接入的情形;
 - 2) 查看接入第三方产品或服务管理记录, 是否有第三方产品或服务未落实安全管理要求和责任的记录。对于未落实安全管理要求和责任的第三方产品或服务, 是否有整改或停止接入记录;
 - 3) 核查 App 服务端是否具备停止接入第三方产品或服务的技术机制。
- e) 单元判定: 如果 1) 、 2) 、 3) 为肯定, 则符合本测评单元指标要求,

否则不符合本测评单元指标要求。

6.5.7.8 测评项：详见 GB/T 35273—2020 中 9.7 的 h) 。

6.5.7.8.1 测评单元（EPI-36）

a) 指标要求：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。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。

b) 测评对象：文档资料、App 服务端

c) 测评方式：人员访谈、服务端核查、技术检测

d) 测评步骤：

1) 查看 App 提供者的第三方产品或服务相关管理制度，是否规定对第三方自动化工具进行个人信息收集、使用行为进行技术检测，从而使其符合管理要求；是否规定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，以及发现超出约定的行为的处理方式；

2) 服务端核查并询问 App 提供者是否对接入的第三方自动化工具进行技术检测，查看检测报告内容是否覆盖个人信息收集、使用行为等方面；

3) 询问并查看 App 提供者是否对接入的第三方自动化工具收集个人信息的行为进行审计，是否具备发现超出约定行为时及时切断接入的机制；查看第三方工具对收集个人信息行为的审计记录及超出约定行为的切断接入记录。

e) 单元判定：如果 1)、2)、3) 为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.5.8 个人信息跨境传输的测评

6.5.8.1 测评项：详见 GB/T 35273—2020 中的 9.8。

6.5.8.1.1 测评单元 (EPI-37)

- a) 指标要求：App 提供者向境外提供在中华人民共和国境内运营中收集和产生的个人信息时，应遵循国家相关规定和标准要求对向境外传输个人信息的业务进行安全评估。
- b) 测评对象：App、App 服务端、文档资料
- c) 测评方式：技术检测、服务端核查、文档审查、人员访谈
- d) 测评步骤：
 - 1) 通过 App 技术检测、核查 App 服务端、询问 App 提供者等方式，查看 App 是否存在向境外传输个人信息的业务场景；
 - 2) 查看涉及个人信息出境的业务功能、个人信息类型、境外传输的目的、传输的境外区域等信息；核查 App 提供者是否依据相关要求进行了申报和安全评估。
- e) 单元判定：如果 1) 为否定，则本测评单元为不适用；如果 1) 、2) 为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.5.8.1.2 测评单元 (EPI-38)

- a) 指标要求：App 不应存在私自向境外传输个人信息的行为。
- b) 测评对象：App、App 服务端
- c) 测评方式：技术检测、服务端核查
- d) 测评步骤：
 - 1) 通过 App 技术检测，查看与境外 IP 或域名有通信连接的 IP 地址、域名、传输的数据包；

- 2) 对向境外传输的数据进行分析, 判断通信数据中是否存在个人信息。如传输数据采用加密技术或无法直接分析传输数据类型, 则要求 App 提供者提供相关澄清材料;
 - 3) 根据 1)、2) 的检测结果判断 App 是否存在私自向境外传输个人信息的情况。
- e) 单元判定: 如果 3) 为否定, 则符合本测评单元指标要求, 否则不符合本测评单元指标要求。

6.6 个人信息安全事件处置的测评

6.6.1 个人信息安全事件应急处置和报告的测评

6.6.1.1 测评项: 详见 GB/T 35273—2020 中 10.1 的 a)。

6.6.1.1.1 测评单元 (HPI-01)

- a) 指标要求: App 提供者应制定个人信息安全事件应急预案。
- b) 测评对象: 文档资料
- c) 测评方式: 文档审查
- d) 测评实施:
 - 1) 查看 App 提供者是否制定个人信息安全事件应急预案的相关制度文件, 应急预案应内容完整, 能够满足相关法律法规要求, 并满足公司实际情况。
- e) 单元判定: 如果 1) 为肯定, 则符合本测评单元指标要求, 否则不符合本测评单元指标要求。

6.6.1.2 测评项: 详见 GB/T 35273—2020 中 10.1 的 b)。

6.6.1.2.1 测评单元 (HPI-02)

- a) 指标要求: App 提供者应定期 (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、应急处置策略和规程。

- b) 测评对象：文档资料
- c) 测评方式：文档审查、人员访谈
- d) 测评实施：
 - 1) 检查 App 提供者是否具有应急演练相关记录，应急预案演练记录是否记录演练时间、操作内容、演练结果等；
 - 2) 检查 App 提供者是否具有应急响应培训记录，如：培训时间、培训计划、培训方案、培训效果等；
 - 3) 访谈 App 提供者是否要求相关人员定期（至少每年一次）参加应急响应培训和应急演练；
 - 4) 访谈事件处置人员是否掌握岗位职责以及应急处置策略和规程。
- e) 单元判定：如果 1) 至 4) 为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.6.1.3 测评项：详见 GB/T 35273—2020 中 10.1 的 c) 。

6.6.1.3.1 测评单元 (HPI-03)

- a) 指标要求：发生个人信息安全事件后，App 提供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) 按照有关规定及时报告，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 GB/T 35273—2020 10.2 的要求实施安全事件的告知。

b) 测评对象：文档资料

c) 测评方式：文档审查、人员访谈

d) 测评实施：

1) 访谈 App 提供者，是否发生过个人信息安全事件；如发生个人信息安全事件，访谈个人信息安全事件的处置情况；

2) 核查 App 提供者在发生个人信息安全事件后是否对事件内容进行记录，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；

3) 核查个人信息安全事件评估报告，内容是否包括安全事件可能造成的影响、处置过程、补救措施等；

4) 检查个人信息安全事件报告及相关记录，是否按照有关规定及时报告，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；

5) 访谈 App 提供者，是否评估个人信息泄露事件对个人信息主体的合法权益造成的危害，如涉及个人敏感信息泄露的，是否按照 GB/T 35273—2020 10.2 中安全事件告知要求进行告知。

e) 单元判定：如果 1) 为否定，则本测评单元为不适用；如果 1) 至 5) 为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.6.1.4 测评项：详见 GB/T 35273—2020 中 10.1 的 d) 。

6.6.1.4.1 测评单元 (HPI-04)

- a) 指标要求: App 提供者应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。
- b) 测评对象: 文档资料
- c) 测评方式: 文档审查
- d) 测评实施:
 - 1) 查看 App 提供者的管理制度或应急预案相关更新条款, 是否包含应急预案更新要求;
 - 2) 查看应急预案修订记录是否根据相关法律法规变化情况, 以及事件处置情况, 修订完善应急预案。
- e) 单元判定: 如果 1) 、2) 为肯定, 则符合本测评单元指标要求, 否则不符合本测评单元指标要求。

6.6.2 安全事件告知的测评

6.6.2.1 测评项: 详见 GB/T 35273—2020 中 10.2 的 a) 。

6.6.2.1.1 测评单元 (HPI-05)

- a) 指标要求: App 提供者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) 测评对象: 文档资料
- c) 测评方式: 文档审查、人员访谈
- d) 测评实施:
 - 1) 查看 App 提供者的个人信息安全事件处置相关的管理制度, 是否包含个人信息安全事件告知要求;
 - 2) 访谈 App 提供者的个人信息安全事件处置相关人员, 是否曾发生个人信息安全事件, 如发生个人信息安全事件, 查阅是否具备相关告

知记录，检查是否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，是否采取合理、有效的方式发布与公众有关的警示信息。

e) 单元判定：如果 1)、2) 为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.6.2.2 测评项：详见 GB/T 35273—2020 中 10.2 的 b)。

6.6.2.2.1 测评单元 (HPI-06)

a) 指标要求：个人信息安全事件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。

b) 测评对象：文档资料

c) 测评方式：文档审查

d) 测评实施：

- 1) 查看 App 提供者的个人信息安全事件处置相关的管理制度，是否包含个人信息安全事件告知内容，内容是否完备；
- 2) 访谈个人信息安全事件处置相关人员，是否曾发生个人信息安全事件，如发生个人信息安全事件，查阅相关告知记录，检查安全事件告知是否包括安全事件的内容和影响、已采取或将要采取的处置措施、个人信息主体自主防范和降低风险的建议、针对个人信息主体提供的补救措施、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等方面内容。

e) 单元判定：如果 1)、2) 为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.7 组织的个人信息安全管理要求的测评

6.7.1 明确责任部门与人员的测评

6.7.1.1 测评项：详见 GB/T 35273—2020 中 11.1 的 a) 。

6.7.1.1.1 测评单元 (PIO-01)

a) 指标要求：App 提供者应明确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) 测评对象：文档资料

c) 测评方式：文档审查、人员访谈

d) 测评步骤：

1) 查看 App 提供者的个人信息安全相关管理制度，是否明确了法定代表人或主要负责人在个人信息安全方面的领导责任；

2) 对信息安全负责人进行访谈，确认其是否了解相关的个人信息安全管理制度并按照管理制度的要求履行其个人信息安全领导义务；

3) 对相关的管理记录进行查验并结合访谈，以确认是否有充分的人力、物力、财力保障个人信息安全管理制度得到有效运行。

e) 单元判定：如果 1)、2)、3) 均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.7.1.2 测评项：详见 GB/T 35273—2020 中 11.1 的 b) 。

6.7.1.2.1 测评单元 (PIO-02)

a) 指标要求：App 提供者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向组织主要负责人报告工作。

b) 测评对象：文档资料

c) 测评方式：文档审查、人员访谈

d) 测评步骤：

1) 查看 App 提供者的个人信息安全相关管理制度，是否明确了个人信息保护负责人和个人信息保护机构；

2) 对个人信息保护负责人的个人资料进行查验并对其进行访谈，确认其是否具有相关管理工作经历和个人信息保护专业知识；

3) 对相关的活动记录进行查验并结合访谈，以确认个人信息保护负责人是否能参与有关个人信息处理活动的重要决策并直接向组织主要负责人报告工作。

e) 单元判定：如果 1) 、2) 、3) 均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.7.1.3 测评项：详见 GB/T 35273—2020 中 11.1 的 c) 。

6.7.1.3.1 测评单元 (PIO-03)

a) 指标要求：App 提供者应在满足 GB/T 35273—2020 中 11.1 的 c) 中的 1) 2) 3) 项条件之一时，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。

b) 测评对象：App 服务端、文档资料

c) 测评方式：服务端核查、文档审查、人员访谈

d) 测评步骤：

1) 通过审查相关文档并结合访谈确认：该组织内的该 App 从业人员规模是否大于 200 人；

2) 核查 App 服务端, 并结合文档审查及访谈确认: 该组织处理的个人信息规模是否超过 100 万人, 或未来 12 个月内预计处理的个人信息规模超过 100 万人;

3) 核查 App 服务端, 并结合文档审查及访谈确认: 该组织处理的个人信息敏感信息规模是否超过 10 万人;

4) 如果以上 1) 、 2) 、 3) 其中一项为肯定, 则需通过文档审查及人员访谈确认: 组织是否设立了专职的个人信息保护负责人和个人信息保护工作机构以负责个人信息安全工作。

e) 单元判定: 如果 1) 、 2) 、 3) 均为否定, 则本测评单元为不适用; 如果 4) 为肯定, 则符合本测评单元指标要求, 否则不符合本测评单元指标要求。

6.7.1.4 测评项: 详见 GB/T 35273—2020 中 11.1 的 d) 。

6.7.1.4.1 测评单元 (PIO-04)

a) 指标要求: 个人信息保护负责人和个人信息保护工作机构的职责应覆盖 GB/T 35273—2020 中 11.1 的 d) 中 1) ~10) 的内容。

b) 测评对象: 文档资料

c) 测评方式: 文档审查、人员访谈

d) 测评步骤:

1) 查看 App 提供者的个人信息安全相关管理制度, 其个人信息保护负责人和个人信息保护机构的职责是否覆盖了 GB/T 35273—2020 中 11.1 的 d) 中 1) ~10) 的所有内容;

2) 对个人信息保护负责人及个人信息保护机构中的人员进行访谈, 确认其是否了解 GB/T 35273—2020 中 11.1 的 d) 中 1) ~10) 的内容, 并按照管理制度的要求履行其个人信息安全保护义务;

3) 对相关的过程记录进行查验并结合访谈, 以确认个人信息保护负

责人及个人信息保护机构的职责得到有效贯彻和运行;

e) 单元判定: 如果 1)、2)、3) 均为肯定, 则符合本测评单元指标要求, 否则不符合本测评单元指标要求。

6.7.1.5 测评项: 详见 GB/T 35273—2020 中 11.1 的 e) 。

6.7.1.5.1 测评单元 (PIO-05)

a) 指标要求: App 提供者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。

b) 测评对象: 文档资料

c) 测评方式: 文档审查、人员访谈

d) 测评步骤:

1) 查看 App 提供者的个人信息安全相关管理制度, 是否明确了个人信息保护负责人和个人信息保护工作机构的资源配置 (人力、物力、财力等);

2) 通过人员访谈及查验过程记录等方式, 确认管理制度所规定的个人信息保护负责人和个人信息保护工作机构的资源配置得到有效落实;

3) 通过人员访谈及查验过程记录等方式, 确认个人信息保护负责人和个人信息保护工作机构是否能独立履行职责。

e) 单元判定: 如果 1)、2)、3) 均为肯定, 则符合本测评单元指标要求, 否则不符合本测评单元指标要求。

6.7.2 个人信息安全工程的测评

6.7.2.1 测评项: 详见 GB/T 35273—2020 中的 11.2。

6.7.2.1.1 测评单元 (PIO-06)

a) 指标要求: 在开发 App 时, App 提供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。

b) 测评对象：文档资料、App 服务端

c) 测评方式：文档审查、服务端核查、人员访谈

d) 测评步骤：

1) 查看 App 提供者的个人信息安全相关管理制度，是否明确了 App 开发过程在需求、设计、开发、测试、发布等阶段的个人信息保护要求；

2) 通过人员访谈、服务端核查、文档审查等手段进行核实，记录 App 提供者是否按照管理制度的要求在开发过程中将个人信息保护措施同步规划、同步建设和同步使用。

e) 单元判定：如果 1) 、2) 均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.7.3 个人信息处理活动记录的测评

6.7.3.1 测评项：详见 GB/T 35273—2020 中 11.3 的 a) 。

6.7.3.1.1 测评单元 (PIO-07)

a) 指标要求：App 提供者宜建立、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：所涉及个人信息的类型、数量、来源（例如从个人信息主体直接收集或通过间接获取方式获得）。

b) 测评对象：App 服务端、文档资料

c) 测评方式：文档审查、服务端核查、人员访谈

d) 测评步骤：

1) 查看 App 提供者的个人信息安全相关管理制度，是否明确要求需建立、维护和更新所收集、使用的个人信息处理活动记录；

2) 通过人员访谈、服务端核查、文档审查等手段进行核实, 记录 App 提供者是否保存了个人信息处理活动记录, 并按制度的规定进行维护和更新;

3) 查看个人信息处理活动记录, 是否包含所涉及个人信息类别、数量、来源。

e) 单元判定: 如果 1) 、2) 、3) 均为肯定, 则符合本测评单元指标要求, 否则不符合本测评单元指标要求。

6.7.3.2 测评项: 详见 GB/T 35273—2020 中 11.3 的 b) 。

6.7.3.2.1 测评单元 (PIO-08)

a) 指标要求: App 提供者宜建立、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: 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。

b) 测评对象: App 服务端、文档资料

c) 测评方式: 文档审查、服务端核查、人员访谈

d) 测评步骤:

1) 查看 App 提供者的个人信息安全相关管理制度, 是否明确了对以下内容记录: 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, 委托处理、共享、转让、公开披露、是否涉及出境等情况;

2) 通过人员访谈、服务端核查、文档审查等手段进行核实, App 提供者是否保存了: 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, 委托处理、共享、转让、公开披露、是否涉及出境等情况的记录。

e) 单元判定: 如果 1) 、2) 均为肯定, 则符合本测评单元指标要求, 否则不符合本测评单元指标要求。

6.7.3.3 测评项：详见 GB/T 35273—2020 中 11.3 的 c) 。

6.7.3.3.1 测评单元 (PIO-09)

- a) 指标要求：App 提供者宜建立、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：与个人信息处理活动各环节相关的信息系统、组织或人员。
- b) 测评对象：App 服务端、文档资料
- c) 测评方式：文档审查、服务端核查、人员访谈
- d) 测评步骤：
 - 1) 查看 App 提供者的个人信息安全相关管理制度，其中是否需明确记录：与个人信息处理活动各环节相关的信息系统、组织或人员；
 - 2) 通过人员访谈、服务端核查、文档审查等手段进行核实，App 提供者是否保存了：个人信息处理活动各环节相关的信息系统、组织或人员的记录。
- e) 单元判定：如果 1) 、2) 均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.7.4 开展个人信息安全影响评估的测评

6.7.4.1 测评项：详见 GB/T 35273—2020 中 11.4 的 a) 。

6.7.4.1.1 测评单元 (PIO-10)

- a) 指标要求：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) 测评对象：文档资料
- c) 测评方式：文档审查、人员访谈
- d) 测评步骤：
 - 1) 查看 App 的个人信息安全影响评估相关制度，是否包含评估并处

置个人信息处理活动存在的安全风险的内容；

2) 通过访谈 App 提供者的相关人员，是否了解制度中评估并处置个人信息处理活动存在的安全风险等相关内容；

3) 通过人员访谈、服务端核查、文档审查等手段进行核实，App 提供者是否有评估并处置个人信息处理活动存在的安全风险的相关记录。

e) 单元判定：如果 1) 、2) 、3) 均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.7.4.2 测评项：详见 GB/T 35273—2020 中 11.4 的 b) 。

6.7.4.2.1 测评单元 (PIO-11)

a) 指标要求：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 GB/T 35273—2020 中 11.4 的 b) 中的 1) 至 6) 的要求。

b) 测评对象：App 服务端、文档资料

c) 测评方式：服务端核查、文档审查、人员访谈

d) 测评步骤：

1) 查看 App 提供者的个人信息安全影响评估相关管理制度，是否明确个人信息安全影响评估的内容应包括 GB/T 35273—2020 中 11.4 的 b) 中的 1) 至 6) 的要求；

2) 查看 App 提供者的个人信息安全影响评估记录，核查个人信息安全影响评估内容是否覆盖 GB/T 35273—2020 中 11.4 的 b) 中的 1) 至 6) 的要求。

注：App 提供者可能针对不同的场景产生不同的个人信息安全影响评估报告，因此，个人信息安全影响评估报告可以是多个，总体上涵盖 GB/T

35273—2020 中 11.4 的 b) 中的 1) 至 6) 的要求即可。

e) 单元判定：如果 1) 、 2) 为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.7.4.3 测评项：详见 GB/T 35273—2020 中 11.4 的 c) 。

6.7.4.3.1 测评单元 (PIO-12)

a) 指标要求：App 提供者应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。

b) 测评对象：文档资料

c) 测评方式：文档审查、人员访谈

d) 测评步骤：

1) 查看 App 提供者的个人信息安全影响评估相关制度，是否包含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的相关内容；

2) 通过访谈 App 提供者的相关人员，是否了解制度中产品或服务发布前，或业务功能发生重大变化时，进行个人信息安全影响评估的相关内容；

3) 通过服务端核查、文档审查等方式，核查 App 提供者是否有产品或服务发布前，或业务功能发生重大变化时，进行个人信息安全影响评估的相关记录。

e) 单元判定：如果 1) 、 2) 、 3) 均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.7.4.4 测评项：详见 GB/T 35273—2020 中 11.4 的 d) 。

6.7.4.4.1 测评单元 (PIO-13)

a) 指标要求：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，App 提供者应进行个人信息安全影响评估。

b) 测评对象：文档资料

c) 测评方式：文档审查、人员访谈

d) 测评步骤：

1) 查看 App 提供者的个人信息安全影响评估相关制度，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，是否有个人信息安全影响评估的相关要求，是否详细界定了法律法规新要求、是否定义了业务模式、信息系统、运行环境发生重大变更的情形，是否定义了重大个人信息安全事件；

2) 通过访谈 App 提供者的相关人员，核查其是否了解制度中的相关规定；

3) 通过文档审查等方式，核查 App 提供者是否有相关的评估记录。

e) 单元判定：如果 1) 、2) 、3) 均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.7.4.5 测评项：详见 GB/T 35273—2020 中 11.4 的 e) 。

6.7.4.5.1 测评单元 (PIO-14)

a) 指标要求：App 提供者应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。

b) 测评对象：App、App 服务端、文档材料

c) 测评方式：功能验证、技术检测、服务端核查、文档审查

d) 测评步骤：

1) 查看 App 提供者的个人信息安全影响评估报告，其中是否明确了

保护个人信息主体的措施;

2) 通过 App 功能验证、技术检测, 核查 App 服务端, 核查个人信息安全影响评估报告中明确的个人信息主体保护措施是否有效实施。

e) 单元判定: 如果 1) 、2) 均为肯定, 则符合本测评单元指标要求, 否则不符合本测评单元指标要求。

6.7.4.6 测评项: 详见 GB/T 35273—2020 中 11.4 的 f) 。

6.7.4.6.1 测评单元 (PIO-15)

a) 指标要求: App 提供者应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。

b) 测评对象: 文档资料

c) 测评方式: 文档审查、人员访谈

d) 测评步骤:

1) 查看 App 的个人信息安全影响评估相关制度, 是否明确妥善留存个人信息安全影响评估报告的具体方式, 从而确保可供相关方查阅, 并明确了对外公开的具体途径;

2) 查看 App 提供者是否按照制度的规定留存了个人信息安全影响评估报告, 制度所规定的对外公开个人信息安全影响评估报告的途径是否真实有效。

e) 单元判定: 如果 1) 、2) 均为肯定, 则符合本测评单元指标要求, 否则不符合本测评单元指标要求。

6.7.5 数据安全能力的测评

6.7.5.1 测评项: 详见 GB/T 35273—2020 中的 11.5。

6.7.5.1.1 测评单元 (PIO-16)

a) 指标要求: App 提供者应根据有关国家标准的要求, 建立适当的数据

安全能力，并落实必要的管理和技术措施，防止个人信息的泄露、损毁、丢失、篡改。

b) 测评对象：文档资料、App 服务端

c) 测评方式：文档审查、服务端核查、人员访谈

d) 测评步骤：

1) 查看 App 提供者的个人信息安全相关管理制度，是否明确了数据安全组织架构图、数据安全管理人员及角色、数据安全策略、数据分类分级管理策略等制度；

2) 查看相关管理制度是否明确数据安全生命周期各阶段的数据安全管理要求，是否设置数据安全管理相关岗位或角色，并规范数据安全管理人员的操作；

3) 查看 App 提供者建立的数据安全能力是否符合 App 所属类型有关国家标准要求，是否存在缺失或遗漏；

4) 通过文档审查、服务端核查、人员访谈等方式，核查 App 提供者是否按制度要求建立数据安全能力，落实在数据采集、传输、存储、处理、共享、销毁等过程的安全管理和安全技术保障措施。

e) 单元判定：如果 1) 至 4) 均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.7.6 人员管理与培训

6.7.6.1 测评项：详见 GB/T 35273—2020 中 11.6 的 a) 。

6.7.6.1.1 测评单元 (PIO-17)

a) 指标要求：App 提供者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) 测评对象：文档资料

c) 测评方式：文档审查、人员访谈

d) 测评步骤：

1) 查看 App 提供者的个人信息安全相关管理制度，是否明确要求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；

2) 通过访谈，以确认是否明确个人信息处理岗位，以及大量接触个人敏感信息的岗位，并形成相应岗位人员名单；

3) 通过文档审查，查看是否与所有从事个人信息处理岗位上的相关人员签署保密协议；

4) 通过文档审查，查看是否对接触个人敏感信息的人员进行背景审查、评审等形成相关记录，查看现有大量接触个人敏感信息的人员是否均通过背景审查。

e) 单元判定：如果 1) 至 4) 均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.7.6.2 测评项：详见 GB/T 35273—2020 中 11.6 的 b) 。

6.7.6.2.1 测评单元 (PIO-18)

a) 指标要求：App 提供者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。

b) 测评对象：文档资料

c) 测评方式：文档审查、人员访谈

d) 测评步骤：

1) 查看 App 提供者的个人信息安全相关管理制度，是否明确内部涉及个人信息处理不同岗位的安全职责，是否建立发生安全事件的处罚机制；

2) 通过访谈, 验证岗位人员是否明确且满足岗位要求;

3) 查看如果发生安全事件是否按相关处罚机制进行处理。

e) 单元判定: 如果 1) 、2) 、3) 均为肯定, 则符合本测评单元指标要求, 否则不符合本测评单元指标要求。

6.7.6.3 测评项: 详见 GB/T 35273—2020 中 11.6 的 c) 。

6.7.6.3.1 测评单元 (PIO-19)

a) 指标要求: App 提供者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。

b) 测评对象: 文档资料

c) 测评方式: 文档审查、人员访谈

d) 测评步骤:

1) 查看 App 提供者的个人信息安全相关管理制度, 是否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;

2) 通过访谈和文档审查, 验证相关管理制度要求是否有效落实, 是否在劳动合同、入职协议、保密协议、离职保密协议等文件中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;

3) 通过访谈相关人员及互联网信息搜集, 查看 App 是否存在终止劳动合同的人员发生泄密事件。

e) 单元判定: 如果 1) 、2) 、3) 均为肯定, 则符合本测评单元指标要求, 否则不符合本测评单元指标要求。

6.7.6.4 测评项: 详见 GB/T 35273—2020 中 11.6 的 d) 。

6.7.6.4.1 测评单元 (PIO-20)

- a) 指标要求: App 提供者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, 并进行监督。
- b) 测评对象: 文档资料
- c) 测评方式: 文档审查、人员访谈
- d) 测评步骤:
 - 1) 查看 App 提供者的个人信息安全相关管理制度, 是否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, 并要求与其签署保密协议, 并进行监督的要求;
 - 2) 通过访谈和文档审查, 核查 App 提供者是否形成可能访问个人信息的外部服务人员名单, 是否与其签订保密协议, 并进行有效监督。
- e) 单元判定: 如果 1) 、2) 均为肯定, 则符合本测评单元指标要求, 否则不符合本测评单元指标要求。

6.7.6.5 测评项: 详见 GB/T 35273—2020 中 11.6 的 e) 。

6.7.6.5.1 测评单元 (PIO-21)

- a) 指标要求: App 提供者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。
- b) 测评对象: 文档资料
- c) 测评方式: 人员访谈、文档审查
- d) 测评步骤:
 - 1) 查看 App 提供者的个人信息安全相关管理制度, 是否明确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;
 - 2) 通过访谈方式, 以确认相关指引和要求是否有效传达, 是否对员工的个人信息保护的指引和要求执行情况进行评估。
- e) 单元判定: 如果 1) 、2) 均为肯定, 则符合本测评单元指标要求,

否则不符合本测评单元指标要求。

6.7.6.6 测评项：详见 GB/T 35273—2020 中 11.6 的 f) 。

6.7.6.6.1 测评单元 (PIO-22)

a) 指标要求：App 提供者应定期（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。

b) 测评对象：文档资料

c) 测评方式：文档审查、人员访谈

d) 测评步骤：

1) 查看 App 提供者的个人信息安全相关管理制度，是否明确定期（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的要求；

2) 通过查验培训、考核等相关记录资料，是否按照规定定期（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；

3) 访谈个人信息处理岗位相关人员，以确认是否掌握个人信息保护政策和相关规程。

e) 单元判定：如果 1) 、2) 、3) 均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.7.7 安全审计

6.7.7.1 测评项：详见 GB/T 35273—2020 中 11.7 的 a) 。

6.7.7.1.1 测评单元 (PIO-23)

a) 指标要求：App 提供者应对个人信息保护政策、相关规程和安全措施

的有效性进行定期审计。

b) 测评对象：文档资料

c) 测评方式：文档审查、人员访谈

d) 测评步骤：

1) 查看 App 提供者的个人信息安全相关管理制度，是否明确了对个人信息保护政策、相关规程和安全措施的有效性进行定期审计的要求，是否明确审计管理岗位职责及人员、审计流程、审计策略、审计范围、审计频率、审计报告、审计问题的预防措施等具体内容；

2) 通过访谈审计相关人员、查验审计过程资料、服务端核查等方式，验证对个人信息保护政策、相关规程和安全措施的审计是否有效。

e) 单元判定：如果 1) 、2) 均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.7.7.2 测评项：详见 GB/T 35273—2020 中 11.7 的 b) 。

6.7.7.2.1 测评单元 (PIO-24)

a) 指标要求：App 提供者应建立自动化审计系统，监测记录个人信息处理活动。

b) 测评对象：App 服务端、文档资料

c) 测评方式：文档审查、服务端核查、人员访谈

d) 测评步骤：

1) 核查 App 服务端是否建立自动化审计系统，监测记录个人信息处理活动；

2) 通过人员访谈、文档审查，查看 App 提供者是否对自动化审计系统监测情况有效性进行核查分析处理。

e) 单元判定：如果 1) 、2) 均为肯定，则符合本测评单元指标要求，

否则不符合本测评单元指标要求。

6.7.7.3 测评项：详见 GB/T 35273—2020 中 11.7 的 c) 。

6.7.7.3.1 测评单元 (PIO-25)

a) 指标要求：App 提供者对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。

b) 测评对象：文档资料

c) 测评方式：文档审查、人员访谈

d) 测评步骤：

1) 查看 App 提供者的个人信息安全相关管理制度，是否明确要求针对审计过程形成记录能对安全事件的处置、应急响应和事后调查提供支撑；

2) 通过人员访谈、文档审查等方式，查验审计过程形成的记录是否包含审计问题、计划整改措施、计划整改结果、计划整改时间、计划整改责任人等内容以对安全事件的处置、应急响应和事后调查提供支撑。

e) 单元判定：如果 1) 、2) 均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.7.7.4 测评项：详见 GB/T 35273—2020 中 11.7 的 d) 。

6.7.7.4.1 测评单元 (PIO-26)

a) 指标要求：App 提供者应防止非授权访问、篡改或删除审计记录。

b) 测评对象：文档资料、App 服务端

c) 测评方式：文档审查、服务端核查、人员访谈

d) 测评步骤：

1) 查看 App 提供者的个人信息安全相关管理制度，是否明确应防止

非授权访问、篡改或删除审计记录的要求；

2) 通过核查 App 服务端审计系统访问控制情况、人员访谈及文档审查等方式，查看是否有防止非授权访问、篡改或删除审计记录的安全策略或预防措施，如设置访问审计记录权限、对删除修改操作审批等，以确认安全策略或预防措施得到有效落实。

e) 单元判定：如果 1) 、2) 均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.7.7.5 测评项：详见 GB/T 35273—2020 中 11.7 的 e) 。

6.7.7.5.1 测评单元 (PIO-27)

a) 指标要求：App 提供者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。

b) 测评对象：文档资料

c) 测评方式：文档审查、人员访谈

d) 测评步骤：

1) 查看 App 提供者相关管理制度，是否明确针对审计过程中发现的个人信息违规使用、滥用等情况建立及时处理的机制和流程的要求；

2) 通过人员访谈及文档审查等方式，查看 App 提供者是否按照相关机制和流程处理个人信息违规使用、滥用等情况。

e) 单元判定：如果 1) 、2) 均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.7.7.6 测评项：详见 GB/T 35273—2020 中 11.7 的 f) 。

6.7.7.6.1 测评单元 (PIO-28)

a) 指标要求：App 提供者审计产生的审计记录和留存时间应符合法律法规的要求。

- b) 测评对象：文档资料
- c) 测评方式：文档审查、人员访谈
- d) 测评步骤：
 - 1) 查看 App 提供者相关管理制度，是否明确审计记录和留存时间要求；
 - 2) 通过文档审查和人员访谈，以确认审计记录和留存时间是否符合法律法规或内部管理制度的要求。
- e) 单元判定：如果 1) 、2) 均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

结果判定

测评人员进行 App 个人信息安全整体测评结果判定时，应首先给出每一个测评单元的判定结果。在进行测评单元结果判定时，不同测评方式的采信顺序按照：技术检测、功能验证、服务端核查、文档审查、人员访谈的顺序排列。根据测评单元的判定结果确定每一个测评项的判定结果时，仅当每一个测评项下的测评单元全部符合时，判定该测评项为符合。当所有测评项的结果均为符合时，App 个人信息安全测评的结论为符合。GB/T 35273—2020 中宜达到的要求，不作为必须符合的测评项要求。

附录 A
(资料性)
App提供者基本信息采集表

开始测评前, App提供者可参考下列表格提供App收集使用个人信息的基本情况。

表 A.1 App 基本信息表

App 名称		操作系统类型	
版本号		运营者名称	
样本获取时间		App 提供者联系人和联系方式	
基本业务功能		App 个人信息保护负责人/机构和联系方式	
业务功能描述			

表 A.2 App 收集个人信息基本情况表

服务类型	功能模块	功能	收集个人信息	收集方式	对应权限	收集目的	收集时机或频率	必要性	用户授权方式	保存方式	保存期限	超期处理方式
				自动采集、主动提供、间接获取								

表 A.3 第三方服务基本情况表

服务名称	收集个人信息	用户授权方式	服务提供者名称	第三方收集的个人信息	App 共享给第三方的个人信息	第三方提供给 App 的个人信息	第三方服务访问方式	是否签署合同或数据保护协议

表 A.4 第三方 SDK 基本情况表

SDK 名称	SDK 版本	SDK 提供者名称	SDK 获取方式	SDK 使用目的	是否签署合同或数据保护协议	SDK 收集的个人信息	SDK 收集个人信息频率	对应权限	收集个人信息目的	向第三方提供个人信息的方式 (委托处理/共享/转让)

附录 B
 (资料性)

App 欺诈、诱骗、误导方式收集个人信息行为举例

表B.1给出了App通过欺诈、诱骗、误导方式收集个人信息的典型行为。

表B.1 App通过欺诈、诱骗、误导方式收集个人信息行为举例

序号	举例
1	以红包、积分、福利、抽奖等奖励为由收集与奖励内容不相关的个人信息。
2	以红包、积分、福利、抽奖等奖励为由要求用户额外提供个人信息，用户提供个人信息后未给予说明的奖励，或将以此为由收集的个人信息用于说明以外的目的。
3	申请权限时的说明与获得权限后的实际行为不符，如以添加联系人为由申请通讯录权限，用户打开权限后上传整个通讯录。
4	应用市场描述与 App 实际业务功能存在较大的不一致。例如，应用市场中描述 App 为阅读类应用，用户下载后，App 在服务端修改内嵌 H5 页面的内容，向用户提供网络借贷服务。
5	App 本身是欺诈、诱骗、误导的 App。例如，App 是其他 App 的仿冒版。
6	App 隐私政策或界面描述中误导用户多提供信息，例如将某项业务功能的非必要个人信息描述为该业务功能的必要个人信息。
7	App 内欺诈、诱骗、误导用户下载其他 App，特别是具有分发功能的 App 欺骗、误导用户下载非用户所自愿下载 App 的行为。
8	采用伪造、欺骗下载或其他不正当方式操纵用户评论、误导用户行为，影响在应用商店中的排名，如刷量行为。
9	在应用中展现钓鱼网站，欺骗用户访问，盗取用户重要的认证凭据或其他敏感信息。
10	伪装成系统或其他应用发送的通知，欺骗用户执行操作。
11	直接展示虚假的系统或应用界面，滥用悬浮窗权限，在其他应用或系统界面之上展示虚假的界面，欺骗用户执行操作。
12	通过图标或内容等方式，伪装成系统应用，在用户不知情的情况下实施恶意行为。

附 录 C
(资料性)
测试单元编号说明

测评单元编号为 2 组数据，格式为 xxx-xx，各组含义和编码规则如下：

第 1 组由字母组成，字母代表对个人信息安全要求的类别：个人信息的收集为 PIC (PI collection)，个人信息的存储为 PIS (PI storage)，个人信息的使用为 UPI (Use of PI)，个人信息主体的权利为 RPI (Rights of PI Subjects)，个人信息的委托处理、共享、转让、公开披露为 EPI (Entrusted processing, sharing, transfer and public disclosure of PI)，个人信息安全事件处置为 HPI (Handling of PI security incidents)，组织的个人信息安全管理要求为 PIO (PI security management requirements for organizations)。

第 2 组由 2 位数字组成，按类对测试单元进行顺序编号

附录 D

(资料性)

不同场景下 App 收集个人信息的频率参考

表 D.1 给出了 App 在不同场景下收集个人信息的频率参考。

表 D.1 不同场景下 App 收集个人信息的频率参考

个人信息	场景	合理频率	备注
地理位置	地图导航、位置追踪等实时定位场景	持续读取（每秒 1 次）	户外开阔地带，设备 GPS 定位成功后。
	展示周边可用服务等场景	周期性读取（每 30 秒 1 次）	
	识别当前地址等场景	一次性读取（进入功能界面时读取 1 次或者用户主动刷新时读取 1 次）	
通讯录	添加特定通讯录好友、分享特定通讯录联系人、设置特定通讯录联系人为紧急联系人等场景	用户主动触发时读取特定条目 1 次	
	通讯录备份、未知联系人骚扰拦截等场景	用户主动触发时读取或经用户明确授权后在通讯录出现变更时自动读取	
人脸信息	各类人脸识别应用场景	用户主动触发时读取	
应用程序列表	应用管理等场景	用户主动触发时读取	
短信	短信备份、短信骚扰拦截等场景	用户主动触发时读取或经用户明确授权后在接收到新短信时自动读取	
通话记录	通话记录备份	用户主动触发时读取或经用户明确授权后在通话记录变更时自动读取	

参 考 文 献

- [1] 《App 违法违规收集使用个人信息行为认定方法》（国信办秘字〔2019〕191号）
- [2] 《网络安全标准实践指南—移动互联网应用程序（App）收集使用个人信息自评估指南》
- [3] 《网络安全标准实践指南—移动互联网应用程序（App）系统权限申请使用指南》
- [4] 《网络安全标准实践指南—移动互联网应用程序（App）个人信息保护常见问题及处置指南》
- [5] GB/T 34975—2017《信息安全技术 移动智能终端应用软件安全技术要求和测试评价方法》

(六) 网络安全标准实践指南——移动互联网应用程序 (App) 收集使用个人信息自评估指南

前 言

《网络安全标准实践指南》(以下简称《实践指南》) 是全国信息安全标准化技术委员会(以下简称“信安标委”) 秘书处组织制定和发布的标准相关技术文件, 旨在围绕网络安全法律法规政策、标准、网络安全热点和事件等主题, 宣传网络安全相关标准及知识, 提供标准化实践指引。

声 明

本《实践指南》版权属于信安标委秘书处，未经秘书处书面授权，不得以任何方式抄袭、翻译《实践指南》的任何部分。凡转载或引用本《实践指南》的观点、数据，请注明“来源：全国信息安全标准化技术委员会秘书处”。

技术支持单位

本《实践指南》得到中国电子技术标准化研究院、中国网络安全审查技术与认证中心、中国信息通信研究院、公安部第一研究所、中国网络空间安全协会、中国电子科技集团公司第三十研究所、国家计算机病毒应急处理中心等单位的 技术支持。

摘 要

2016年《网络安全法》颁布，明确我国网络安全保护的基本要求和制度，并将个人信息保护问题作为网络信息安全的重要内容予以规定。App运营者作为典型的网络运营者，在其收集、使用个人信息时，应当遵守《网络安全法》等法律法规有关个人信息保护的要求。2019年1月，中央网信办、工业和信息化部、公安部、市场监管总局发布《关于开展App违法违规收集使用个人信息专项治理的公告》，公告中指出，由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。2019年3月1日，App专项治理工作组结合2017年和2018年“隐私条款专项评审”等工作经验，对外发布第一版《App违法违规收集使用个人信息自评估指南》技术文件，提出评估点，以便于指导App运营者自查自纠。2019年12月30日，中央网信办、工信部、公安部、市场监管总局联合制定的《App违法违规收集使用个人信息行为认定方法》正式发布，认定方法的内容结合了一年来关于App违法违规收集使用个人信息检测评估工作的经验和规律，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。

本实践指南在2019年3月1日版《App违法违规收集使用个人信息自评估指南》的基础上，依据《网络安全法》等法律法规要求，参照《App违法违规收集使用个人信息行为认定方法》和相关国家标准，结合检测评估工作经验，归纳总结出App收集使用个人信息评估点，供App运营者自评估参考，帮助其持续提升个人信息保护水平。

评估点一：是否公开收集使用个人信息的规则

《网络安全法》第 41 条规定，网络运营者收集、使用个人信息，应当公开收集、使用规则。

《消费者权益保护法》第 29 条规定，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”。

1.1 是否有隐私政策等收集使用规则

- a. 在App界面中能够找到隐私政策，包括通过弹窗、文本链接、附件、常见问题（FAQs）等形式，且隐私政策可正常显示。
- b. 隐私政策中需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，且文本可正常显示。

1.2 是否提示用户阅读隐私政策等收集使用规则

- a. App需在首次运行或用户注册时通过弹窗等明显方式，提示用户阅读隐私政策。
- b. 避免使用灰色字体、缩小字号、键盘遮挡、置于边缘等方式未突出显示隐私政策链接。

1.3 隐私政策等收集使用规则是否易于访问

- a. 用户进入App主功能界面后，通过 4 次（含）以内的点击，能够访问到隐私政策。
- b. 在App常规交互界面展示隐私政策链接，避免仅在注册/登录界面展示隐私政策链接，或只能以咨询客服等方式查看隐私政策的情形。
- c. 隐私政策以单独成文的形式发布，而不是作为用户协议、用户说明等文件中的一部分存在。

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（字号、颜色、行间距、清晰度等）

不会造成阅读困难。

b. 需提供简体中文版隐私政策。

c. 隐私政策的内容需符合通用的语言习惯，使用标准化的数字、图示，避免出现错别字或有歧义的语句。

1.5是否公开App运营者的基本情况

a. 隐私政策应对App运营者基本情况描述, 至少包括组织或公司名称、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。

1.6是否公开收集使用个人信息的其他规则

a. 隐私政策应说明发布、生效或更新日期。

b. 隐私政策应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）、超期处理方式进行明确说明。

c. 如果App运营者将个人信息用于用户画像、个性化展示等，隐私政策中应说明其应用场景和可能对用户产生的影响。

d. 如果存在个人信息出境情形，隐私政策中应将出境个人信息类型逐项列出并显著标识（如字体加粗、标星号、下划线、斜体、不同颜色等）；如果不存在个人信息出境情形，则明确说明。

e. 隐私政策中应对App运营者在个人信息保护方面采取的措施和具备的能力进行说明，如身份鉴别、数据加密、访问控制、恶意代码防范、安全审计等。

f. 如果存在个人信息对外共享、转让、公开披露等情况，隐私政策中应明确以下内容：①对外共享、转让、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。

g. 隐私政策中应对以下用户权利和相关操作方法进行明确说

明：①个人信息查询；②个人信息更正；③个人信息删除；④用户账户注销；⑤撤回已同意的授权。

h. 隐私政策中至少提供以下一种申诉渠道：①电子邮件；②电话；③在线客服；④在线表单。

注：相关定义和内容可参考GB/T 35273《个人信息安全规范》。

评估点二：是否明示收集使用个人信息的目的、方式和范围

《网络安全法》第 41 条规定，网络运营者收集、使用个人信息，应当公开收集、使用规则。

《消费者权益保护法》第 29 条规定，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”。

2.1是否逐一列出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

a. 完整、清晰、区分说明各业务功能所收集的个人信息。隐私政策中所述内容应与App实际业务相符，并逐项说明各业务功能收集个人信息的目的、类型、方式，不应使用“等、例如”等方式不完整列举。

b. 注 业务功能是指App面向个人用户所提供的一类完整的服务，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、短视频、快递配送、餐饮外卖、交通票务、婚恋相亲、房屋租售、求职招聘、二手车交易、金融借贷等。

c. 如App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，应向用户说明使用该类技术收集个人信息的目的、类型、方式。

d. 如App嵌入了第三方代码、插件（如SDK）收集个人信息，应说明第三方类型，及收集个人信息的目的、类型、方式，说明方式包括隐私政策、弹窗提示、文字备注、文本链接等。

e. 如委托的第三方或嵌入的第三方代码、插件直接将个人信息传输至境外的，应明确说明跨境传输个人信息的目的、类型和接收方等。

2.2是否以适当的方式通知用户收集使用个人信息的目的、方式、范围发生的变化

a. 收集使用个人信息的目的、方式和范围发生变化时，应以适当方式通知用户，适当方式包括更新隐私政策并以信息、邮件、弹窗等方式提醒用户阅读发生变化的条款等。

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的权限时，App应通过显著方式（如弹窗提示等）同步告知用户其目的，对目的的描述应明确、易懂。

注：常见可收集个人信息的系统权限有：

iOS系统：定位、通讯录、日历、提醒事项、照片、麦克风、相机、健康；

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。

b. 在要求用户提供个人敏感信息（用户身份证号、银行账号、行踪轨迹等）时，App应通过显著方式（如弹窗提示、文字备注、文本链接等）同步告知用户其目的，对目的的描述应明确、易懂。

注：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）未成年人的个人信息等。（该定义见GB/T 35273《个人信息安全规范》3.2 节）

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应简练、结构清晰、重点突出，避免使用晦涩难懂的词语（如使用大量专业术语）和冗长繁琐的篇幅。

评估点三：收集使用个人信息是否征得用户同意

《网络安全法》第 41 条规定网络运营者收集、使用个人信息，应“经被收集者同意”且“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”。

《消费者权益保护法》第 29 条规定经营者收集、使用消费者个人信息，应“经消费者同意”且“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。”

3.1 收集个人信息或打开可收集个人信息的权限前是否征得用户同意

App 收集个人信息前应提供由用户主动选择同意或不同意（包括退出、上一步、关闭、取消等）的选项。

a. 未征得用户同意时，不应收集个人信息或打开可收集个人信息权限。如 App 首次打开时，在用户未得知收集个人信息的目的前，App 就开始收集个人信息。

注：征得同意，指个人信息主体通过书面声明或主动做出肯定性动作，对其个人信息进行特定处理做出明确授权的行为。肯定性动作包括个人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。

b. 不应在征得用户同意前，利用 Cookie 等同类技术、或私自调用可收集用户个人信息的权限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或打开可收集个人信息的权限

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，明确拒绝 App 收集某类个人信息后，不应以任何形式收集该类个人信息或打开可收集个人信息的权限。

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，不应在每次重新打开App、或使用某一业务功能时，向用户频繁（如 48 小时内）询问是否同意收集个人信息。

用户明确表示不同意收集后，不应在每次重新打开App、或使用某一业务功能时，向用户频繁（如 48 小时内）询问是否同意打开可收集个人信息的权限。

注：用户选择使用App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。如用户自行选择使用拍摄、扫码等功能，App需获取“相机”权限。

3.4实际收集的个人信息或打开的可收集个人信息权限是否超出用户授权范围

a. App收集使用个人信息的过程应与其所声明的隐私政策等收集使用规则保持一致。如实际收集的个人信息类型、申请打开的可收集使用个人信息的系统权限、调用系统权限函数的行为应与隐私政策所描述内容一致，不应超出隐私政策所述范围。

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App或用户注册时，不应采用默认勾选隐私政策等非明示方式征求用户同意；

b. 注册（包括登录即代表注册）的选项与同意隐私政策等的因果逻辑关系应清楚，且主动提示用户阅读以显著方式展示的隐私政策等收集使用规则后，执行下一步注册/登录等动作。

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，不应私自更改用户设置的收集个人信息权限。

b. App更新升级后，不应自动将用户设置的权限恢复到默认状态。

3.7 App利用用户个人信息和算法定向推送信息时，是否提供非定向推送信息的选项

a. App存在利用用户个人信息和算法定向推送信息情形（包括利用个人信息和算法推送新闻和信息、展示商品、推送广告等）应提供拒绝接受定向推送信息，或者停止、退出、关闭相应功能的机制，或者不基于个人信息、用户画像等推送的模式、选项。

注：相关定义和内容可参考GB/T 35273《个人信息安全规范》。

3.8是否以欺诈、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

a. App所明示收集使用个人信息的目的应真实、准确，不应故意欺瞒、掩饰收集使用个人信息的真实目的。如以红包、金币、抽奖等方式诱骗用户打开可收集个人信息的通讯录权限后，立即上传所有通讯录信息。

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. App应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确。

b. 如用户拒绝或撤回特定业务功能收集个人信息的授权时，App不应暂停提供其他业务功能，或降低其他业务功能的服务质量。

c. 如用户拒绝或撤回可收集个人信息的权限时，不得影响用户正常使用与该权限无关的功能，除非该权限是保证App正常运行所必需。

4.0是否违反其所声明的收集使用规则，收集使用个人信息

a. App应严格遵循其披露的隐私政策等收集使用规则，开展个人信息处理活动，如个人信息使用目的发生变化的，应再次征得用户同意。

评估点四：是否遵循必要原则，仅收集与其提供的服务直接相关的个人信息

4.1是否收集与业务功能无关的个人信息

a. 不应收集与业务功能无关的个人信息。

b. App不应申请打开与业务功能无关的可收集个人信息的权限。

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. App收集业务功能非必要的个人信息或申请打开非必要权限时，应征得用户同意，用户不同意不得拒绝提供相应业务功能。

b. App不应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可收集个人信息权限，作为业务功能打开的前提条件。

c. 如App提供无需注册即可使用（如浏览、游客模式）的业务模式，当用户拒绝支撑浏览、游客等模式以外的个人信息收集行为，App不应拒绝提供服务。

注：必要信息指与基本业务功能直接相关的个人信息，缺少该个人信息则

基本业务功能无法实现。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》（征求意见稿），如果业务类型不在该标准内，则应根据其业务特点，参考该规范相关定义和理念自行判定。

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App的各个业务功能打开或开始收集使用个人信息的条件。

b. 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时，不应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. 不应仅以改善服务质量、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其个人信息并以此作为提供服务的条

件。

d. App不得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。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。

4.4收集个人信息的频度是否超出业务功能实际需要

a. App收集个人信息的频度不应超出业务功能实际需要, 在使用App某业务功能过程中, 应仅收集与当前业务功能相关的个人信息。

b. 在未打开App或后台运行App时App不应收集用户个人信息, 除非App业务功能需要后台运行时继续提供服务, 如导航功能。

c. App接入第三方应用时, 应提醒用户关注第三方应用收集使用个人信息的规则, 不得私自截留第三方应用收集的个人信息。

评估点五: 是否未经同意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App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App客户端嵌入第三方代码、插件(如SDK)等方式, 应事先征得用户同意, 经匿名化处理的除外。

b. 如个人信息传输至App服务器后, App运营者向第三方提供其收集的个人信息, 应事先征得用户同意, 经匿名化处理的除外。

c. 如App接入第三方应用, 当用户使用第三方应用时, 应事先征得用户同意后, 再向第三方应用提供个人信息, 用户获知应用为第三方且在知悉收集使用个人信息规则后, 自行同意提供给第三方的除外。

评估点六: 是否按法律规定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. App应提供有效的注销账号的途径（如在线操作、客服电话、电子邮件等），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，法律法规另有规定的除外。

b. 受理注销账号请求后，App运营者应在承诺时限内（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. 注销账号的过程应简单易操作，不应设置不必要或不合理的注销条件，如提供额外的个人敏感信息用于身份验证，或未明确注销所需个人敏感信息在注销成功后是否会删除等。

注：相关内容可参考GB/T 35273《个人信息安全规范》。

6.2是否提供有效的更正或删除个人信息

a. App应提供有效的查询、更正、删除个人信息的途径。

b. 用户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，App运营者应在承诺时限内（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. 查询、更正和删除个人信息的过程应简单易操作，不应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，App后台应同步执行完成相关操作。

6.3是否建立并公布个人信息安全投诉、举报渠道

a. App运营者应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，受理可采取在线操作、客服电话、电子邮件等方式。

b. App运营者应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。

(七) 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

(GB/Z 28828-2012 国家质量监督检验检疫总局、国家标准化管理委员会2012年11月5日批准发布 2013年2月1日起实施)

随着信息技术的广泛应用和互联网的不断普及, 个人信息在社会、经济活动中的地位日益凸显, 滥用个人信息的现象随之出现, 给社会秩序和个人切身利益带来了危害。为促进个人信息的合理利用, 指导和规范利用信息系统处理个人信息的活动, 制定本指导性技术文件。

1 范围 本指导性技术文件规范了全部或部分通过信息系统进行个人信息处理的过程, 为信息系统中个人信息处理不同阶段的个人信息保护提供指导。

本指导性技术文件适用于指导除政府机关等行使公共管理职责的机构以外的各类组织和机构, 如电信、金融、医疗等领域的服务机构, 开展信息系统中的个人信息保护工作。

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/T20269-2006信息安全技术信息系统安全管理要求

GB/Z20986-2007信息安全技术信息安全事件分类分级指南

3 术语和定义

GB/T20269-2006和GB/Z20986-2007中界定的以及下列术语和定义适用于本技术性指导文件。

3.1 信息系统 informationsystem

即计算机信息系统, 由计算机(含移动通信终端)及其相关的和配套的设备、

设施（含网络）构成，能够按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理。

3.2 个人信息 personalinformation

可为信息系统所处理、与特定自然人相关、能够单独或通过与其他信息结合识别该特定自然人的计算机数据。个人信息可以分为个人敏感信息和个人一般信息。

3.3 个人信息主体 subjectofpersonalinformation

个人信息指向的自然人。

3.4 个人信息管理者 administratorofpersonalinformation

决定个人信息处理的目的和方式，实际控制个人信息并利用信息系统处理个人信息的组织和机构。

3.5 个人信息获得者 receiverofpersonalinformation

从信息系统获取个人信息的个人、组织和机构，依据个人信息主体的意愿对获得的个人信息进行处理。

3.6 第三方测评机构 thirdpartytestingandevaluationagency

独立于个人信息管理者的专业测评机构。

3.7 个人敏感信息 personalsensitiveinformation

一旦遭到泄露或修改，会对标识的个人信息主体造成不良影响的个人信息。各行业个人敏感信息的具体内容根据接受服务的个人信息主体意愿和各自业务特点确定。例如个人敏感信息可以包括身份证号码、手机号码、种族、政治观点、宗教信仰、基因、指纹等。

3.8 个人一般信息 personalgeneralinformation

除个人敏感信息以外的个人信息。

3.9 个人信息处理 personalinformationhandling

处置个人信息的行为，包括收集、加工、转移、删除。

3.10 默许同意 tacitconsent

在个人信息主体无明确反对的情况下，认为个人信息主体同意。

3.11 明示同意 expressedconsent

个人信息主体明确授权同意，并保留证据。

4 个人信息保护概述

4.1 角色和职责

4.1.1 综述

信息系统个人信息保护实施过程中涉及的角色主要有个人信息主体、个人信息管理者、个人信息获得者和独立测评机构，其职责见4.1.2至4.1.5。

4.1.2 个人信息主体

在提供个人信息前，要主动了解个人信息管理者收集的目的、用途等信息，按照个人意愿提供个人信息；发现个人信息出现泄漏、丢失、篡改后，向个人信息管理者投诉或提出质询，或向个人信息保护管理部门发起申诉。

4.1.3 个人信息管理者

负责依照国家法律、法规和本指导性技术文件，规划、设计和建立信息系统个人信息处理流程；制定个人信息管理制度、落实个人信息管理责任；指定专门机构或人员负责机构内部的个人信息保护工作，接受个人信息主体的投诉与质询；制定个人信息保护的教育培训计划并组织落实；建立个人信息保护的内部控制，并定期对信息系统个人信息的安全状况、保护制度及措施的落实情况进行自查或委托独立测评机构进行测评。

管控信息系统个人信息处理过程中的风险，对个人信息处理过程中可能出现的泄露、丢失、损坏、篡改、不当使用等事件制定预案；发现个人信息遭到泄漏、

丢失、篡改后，及时采取应对措施，防止事件影响进一步扩大，并及时告知受影响的个人信息主体；发生重大事件的，及时向个人信息保护管理部门通报。

接受个人信息保护管理部门对个人信息保护状况的检查、监督和指导，积极参与和配合第三方测评机构对信息系统个人信息保护状况的测评。

4.1.4 个人信息获得者

当个人信息的获取是出于对方委托加工等目的，个人信息获得者要依照本指导性技术文件和委托合同，对个人信息进行加工，并在完成加工任务后，立即删除相关个人信息。

4.1.5 第三方测评机构

从维护公众利益角度出发、根据个人信息保护管理部门和行业协会的授权、或受个人信息管理者的委托，依据相关国家法律、法规和本指导性技术文件，对信息系统进行测试和评估，获取个人信息保护状况，作为个人信息管理者评价、监督和指导个人信息保护的依据。

4.2 基本原则

个人信息管理者在使用信息系统对个人信息进行处理时，宜遵循以下基本原则：

- a) 目的明确原则--处理个人信息具有特定、明确、合理的目的，不扩大使用范围，不在个人信息主体不知情的情况下改变处理个人信息的目的。
- b) 最少够用原则--只处理与处理目的有关的最少信息，达到处理目的后，在最短时间内删除个人信息。
- c) 公开告知原则--对个人信息主体要尽到告知、说明和警示的义务。以明确、易懂和适宜的方式如实向个人信息主体告知处理个人信息的目的、个人信息的收集和使用范围、个人信息保护措施等信息。
- d) 个人同意原则--处理个人信息前要征得个人信息主体的同意。

e) 质量保证原则--保证处理过程中的个人信息保密、完整、可用，并处于最新状态。

f) 安全保障原则--采取适当的、与个人信息遭受损害的可能性和严重性相适应的管理措施和技术手段，保护个人信息安全，防止未经个人信息管理者授权的检索、披露及丢失、泄露、损毁和篡改个人信息。

g) 诚信履行原则--按照收集时的承诺，或基于法定事由处理个人信息，在达到既定目的后不再继续处理个人信息。

h) 责任明确原则--明确个人信息处理过程中的责任，采取相应的措施落实相关责任，并对个人信息处理过程进行记录以便于追溯。

5 个人信息保护

5.1 概述

信息系统中个人信息的处理过程可分为收集、加工、转移、删除4个主要环节。对个人信息的保护贯穿于4个环节中：

a) 收集指对个人信息进行获取并记录。

b) 加工指对个人信息进行的操作，如录入、存储、修改、标注、比对、挖掘、屏蔽等。

c) 转移指将个人信息提供给个人信息获得者的行为，如向公众公开、向特定群体披露、由于委托他人加工而将个人信息复制到其他信息系统等。

d) 删除指使个人信息在信息系统中不再可用。

5.2 收集阶段

5.2.1 要具有特定、明确、合法的目的。

5.2.2 收集前要采用个人信息主体易知悉的方式，向个人信息主体明确告知和警示如下事项：

a) 处理个人信息的目的；

- b) 个人信息的收集方式和手段、收集的具体内容和留存时限;
- c) 个人信息的使用范围, 包括披露或向其他组织和机构提供其个人信息的范围;
- d) 个人信息的保护措施;
- e) 个人信息管理者的名称、地址、联系方式等相关信息;
- f) 个人信息主体提供个人信息后可能存在的风险;
- g) 个人信息主体不提供个人信息可能出现的后果;
- h) 个人信息主体的投诉渠道;
- i) 如需将个人信息转移或委托于其他组织和机构, 要向个人信息主体明确告知包括但不限于以下信息: 转移或委托的目的、转移或委托个人信息的具体内容和使用范围、接受委托的个人信息获得者的名称、地址、联系方式等。

5.2.3 处理个人信息前要征得个人信息主体的同意, 包括默许同意或明示同意。收集个人一般信息时, 可认为个人信息主体默许同意, 如果个人信息主体明确反对, 要停止收集或删除个人信息; 收集个人敏感信息时, 要得到个人信息主体的明示同意。

5.2.4 只收集能够达到已告知目的的最少信息。

5.2.5 要采用已告知的手段和方式直接向个人信息主体收集, 不采取隐蔽手段或以间接方式收集个人信息。

5.2.6 持续收集个人信息时提供相关功能, 允许个人信息主体配置、调整、关闭个人信息收集功能。

5.2.7 不直接向未满16周岁的未成年人等限制民事行为能力或无行为能力人收集个人敏感信息, 确需收集其个人敏感信息的, 要征得其法定监护人的明示同意。

5.3 加工阶段

5.3.1 不违背收集阶段已告知的使用目的，或超出告知范围对个人信息进行加工。

5.3.2 采用已告知的方法和手段。

5.3.3 保证加工过程中个人信息不被任何与处理目的无关的个人、组织和机构获知。

5.3.4 未经个人信息主体明示同意，不向其他个人、组织和机构披露其处理的个人信息。

5.3.5 保证加工过程中信息系统持续稳定运行，个人信息处于完整、可用状态，且保持最新。

5.3.6 个人信息主体发现其个人信息存在缺陷并要求修改时，个人信息管理者要根据个人信息主体的要求进行查验核对，在保证个人信息完整性的前提下，修改或补充相关信息。

5.3.7 详细记录对个人信息的状态，个人信息主体要求对其个人信息进行查询时，个人信息管理者要如实并免费告知是否拥有其个人信息、拥有其个人信息的内容、个人信息的加工状态等内容，除非告知成本或者请求频率超出合理的范围。

5.4 转移阶段

5.4.1 不违背收集阶段告知的转移目的，或超出告知的转移范围转移个人信息。

5.4.2 向其他组织和机构转移个人信息前，评估其是否能够按照本指导性技术文件的要求处理个人信息，并通过合同明确该组织和机构的个人信息保护责任。

5.4.3 保证转移过程中，个人信息不被个人信息获得者之外的任何个人、组织和机构所获知。

5.4.4 保证转移前后，个人信息的完整性和可用性，且保持最新。

5.4.5 未经个人信息主体的明示同意，或法律法规明确规定，或未经主管部门同意，个人信息管理者不得将个人信息转移给境外个人信息获得者，包括位于境外的个人或境外注册的组织和机构。

5.5 删除阶段

5.5.1 个人信息主体有正当理由要求删除其个人信息时，及时删除个人信息。删除个人信息可能会影响执法机构调查取证时，采取适当的存储和屏蔽措施。

5.5.2 收集阶段告知的个人信息使用目的达到后，立即删除个人信息；如需继续处理，要消除其中能够识别具体个人的内容；如需继续处理个人敏感信息，要获得个人信息主体的明示同意。

5.5.3 超出收集阶段告知的个人信息留存期限，要立即删除相关信息；对留存期限有明确规定的，按相关规定执行。

5.5.4 个人信息管理者破产或解散时，若无法继续完成承诺的个人信息处理目的，要删除个人信息。删除个人信息可能会影响执法机构调查取证时，采取适当的存储和屏蔽措施。

(八) 电信和互联网用户个人信息保护规定

中华人民共和国工业和信息化部令（第24号）

《电信和互联网用户个人信息保护规定》已经2013年6月28日中华人民共和国工业和信息化部第2次部务会议审议通过，现予公布，自2013年9月1日起施行。

部长 苗圩

2013年7月16日

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 and 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。

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。

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。

(九) 信息安全技术 个人信息告知同意指南（征求意见稿）

前 言

本标准按照GB/T 1.1—2009《标准化工作导则 第1部分：标准的结构和编写》给出的规则起草。

请注意本文件的其他内容可能涉及专利，本文件的发布机构不承担识别这些专利的责任。

本标准由全国信息安全标准化技术委员会（SAC/TC260）提出并归口。

本标准起草单位：中国电子技术标准化研究院、深圳腾讯计算机系统有限公司、中国信息通信研究院、北京小米移动软件有限公司、华为技术有限公司、阿里巴巴（北京）软件服务有限公司、北京字节跳动科技有限公司、北京三快科技有限公司等。

本标准主要起草人：何延哲、赵冉冉、洪延青、葛鑫、胡影、陈湑、朱玲凤、衣强、田申、刘笑岑、娜迪娅、陈松、周晨炜、张有科、付伟、李腾、张灵子、张娜、彭骏涛、姚一楠、王磊、刘熙君、杨立春、王昕、孟靖卓、封莎、罗妍等。

信息安全技术个人信息告知同意指南

1 适用范围

本标准在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。

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。

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；
- 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人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；
- 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收者转让个人信息，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：

- 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；
- 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。

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;
- 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，以使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。

应用程序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：

下载安装前：应用程序在下载安装前，宜通过应用程序主页或下载页面等方式告知用户应用程序在运行使用过程中需收集处理的个人信息。

首次使用前：应用程序在首次运行时，应告知用户需收集处理的个人信息。

信息收集前：应用程序收集个人信息前，应告知用户需收集处理的个人信息。

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。

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。

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。

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。

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危险情况。

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。

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

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；

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；

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；
- 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

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，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。

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。

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。

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。

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

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、餐饮娱乐场所、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；
- 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

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。

- 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。

(十) 国家互联网信息办公室关于《网络安全审查办法》（修订草案征求意见稿）公开征求意见的通知

依据《中华人民共和国国家安全法》《中华人民共和国网络安全法》《中华人民共和国数据安全法》等法律法规，我办会同有关部门修订了《网络安全审查办法》，现向社会公开征求意见。公众可通过以下途径和方式提出反馈意见：

- 1.登录中华人民共和国司法部 中国政府法制信息网（www.moj.gov.cn、www.chinalaw.gov.cn），进入首页主菜单的“立法意见征集”栏目提出意见。
- 2.通过电子邮件方式发送至：shencha@cac.gov.cn。
- 3.通过信函方式将意见寄至：北京市西城区车公庄大街11号国家互联网信息办公室网络安全协调局，邮编100044，并在信封上注明“网络安全审查办法征求意见”。

意见反馈截止日期为2021年7月25日。

附件：网络安全审查办法（修订草案征求意见稿）

国家互联网信息办公室

2021年7月10日

附件

网络安全审查办法（修订草案征求意见稿）

第一条 为了确保关键信息基础设施供应链安全，维护国家安全，依据《中华人民共和国国家安全法》《中华人民共和国网络安全法》《中华人民共和国数据安全法》，制定本办法。

第二条 关键信息基础设施运营者（以下简称运营者）采购网络产品和服务，数据处理者（以下称运营者）开展数据处理活动，影响或可能影响国家安全的，应当按照本办法进行网络安全审查。

第三条 网络安全审查坚持防范网络安全风险与促进先进技术应用相结合、过程公正透明与知识产权保护相结合、事前审查与持续监管相结合、企业承诺与社会监督相结合，从产品和服务安全性、可能带来的国家安全风险等方面进行审查。

第四条 在中央网络安全和信息化委员会领导下，国家互联网信息办公室会同中华人民共和国国家发展和改革委员会、中华人民共和国工业和信息化部、中华人民共和国公安部、中华人民共和国国家安全部、中华人民共和国财政部、中华人民共和国商务部、中国人民银行、国家市场监督管理总局、国家广播电视总局、中国证券监督管理委员会、国家保密局、国家密码管理局建立国家网络安全审查工作机制。

网络安全审查办公室设在国家互联网信息办公室，负责制定网络安全审查相关制度规范，组织网络安全审查。

第五条 运营者采购网络产品和服务的，应当预判该产品和服务投入使用后可能带来的国家安全风险。影响或者可能影响国家安全的，应当向网络安全审查办公室申报网络安全审查。

关键信息基础设施保护工作部门可以制定本行业、本领域预判指南。

第六条 掌握超过100万用户个人信息的运营者赴国外上市，必须向网络安全审查办公室申报网络安全审查。

第七条 对于申报网络安全审查的采购活动，运营者应通过采购文件、协议等要求产品和服务提供者配合网络安全审查，包括承诺不利用提供产品和服务的便利条件非法获取用户数据、非法控制和操纵用户设备，无正当理由不中断产品供应或必要的技术支持服务等。

第八条 运营者申报网络安全审查，应当提交以下材料：

- (一) 申报书；
- (二) 关于影响或可能影响国家安全的分析报告；

(三) 采购文件、协议、拟签订的合同或拟提交的IPO材料等；

(四) 网络安全审查工作需要的其他材料。

第九条 网络安全审查办公室应当自收到审查申报材料起，10个工作日内确定是否需要审查并书面通知运营者。

第十条 网络安全审查重点评估采购活动、数据处理活动以及国外上市可能带来的国家安全风险，主要考虑以下因素：

(一) 产品和服务使用后带来的关键信息基础设施被非法控制、遭受干扰或破坏的风险；

(二) 产品和服务供应中断对关键信息基础设施业务连续性的危害；

(三) 产品和服务的安全性、开放性、透明性、来源的多样性，供应渠道的可靠性以及因为政治、外交、贸易等因素导致供应中断的风险；

(四) 产品和服务提供者遵守中国法律、行政法规、部门规章情况；

(五) 核心数据、重要数据或大量个人信息被窃取、泄露、毁损以及非法利用或出境的风险；

(六) 国外上市后关键信息基础设施，核心数据、重要数据或大量个人信息被国外政府影响、控制、恶意利用的风险；

(七) 其他可能危害关键信息基础设施安全和国家数据安全的因素。

第十一条 网络安全审查办公室认为需要开展网络安全审查的，应当自向运营者发出书面通知之日起30个工作日内完成初步审查，包括形成审查结论建议并将审查结论建议发送网络安全审查工作机制成员单位、相关关键信息基础设施保护工作部门征求意见；情况复杂的，可以延长15个工作日。

第十二条 网络安全审查工作机制成员单位和相关关键信息基础设施保护工作部门应当自收到审查结论建议之日起15个工作日内书面回复意见。

网络安全审查工作机制成员单位、相关关键信息基础设施保护工作部门意见

一致的，网络安全审查办公室以书面形式将审查结论通知运营者；意见不一致的，按照特别审查程序处理，并通知运营者。

第十三条 按照特别审查程序处理的，网络安全审查办公室应当听取相关部门和单位意见，进行深入分析评估，再次形成审查结论建议，并征求网络安全审查工作机制成员单位和相关单位意见，按程序报中央网络安全和信息化委员会批准后，形成审查结论并书面通知运营者。

第十四条 特别审查程序一般应当在3个月内完成，情况复杂的可以延长。

第十五条 网络安全审查办公室要求提供补充材料的，运营者、产品和服务提供者应当予以配合。提交补充材料的时间不计入审查时间。

第十六条 网络安全审查工作机制成员单位认为影响或可能影响国家安全的网络产品和服务、数据处理活动以及国外上市行为，由网络安全审查办公室按程序报中央网络安全和信息化委员会批准后，依照本办法的规定进行审查。

第十七条 参与网络安全审查的相关机构和人员应严格保护企业商业秘密和知识产权，对运营者、产品和服务提供者提交的未公开材料，以及审查工作中获悉的其他未公开信息承担保密义务；未经信息提供方同意，不得向无关方披露或用于审查以外的目的。

第十八条 运营者或网络产品和服务提供者认为审查人员有失客观公正，或未能对审查工作中获悉的信息承担保密义务的，可以向网络安全审查办公室或者有关部门举报。

第十九条 运营者应当督促产品和服务提供者履行网络安全审查中作出的承诺。

网络安全审查办公室通过接受举报等形式加强事前事中事后监督。

第二十条 运营者违反本办法规定的，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》的规定处理。

第二十一条 本办法中关键信息基础设施运营者是指经关键信息基础设施

保护工作部门认定的运营者。

本办法所称网络产品和服务主要指核心网络设备、重要通信产品、高性能计算机和服务器、大容量存储设备、大型数据库和应用软件、网络安全设备、云计算服务，以及其他对关键信息基础设施安全有重要影响的网络产品和服务。

第二十二条 涉及国家秘密信息的，依照国家有关保密规定执行。

第二十三条 本办法自2021年 月 日起实施，《网络产品和服务安全审查办法（试行）》同时废止。

(十一) 汽车数据安全若干规定

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;

(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,应当进行匿名化处理,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。

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。

(十二) 工业和信息化领域数据安全管理办法（试行）（征求意见稿）

第一章 总则

第一条【目的依据】为了规范工业和信息化领域数据处理活动，加强数据安全的管理，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，维护国家安全和利益，根据《中华人民共和国民法典》《中华人民共和国数据安全法》《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【适用范围】在中华人民共和国境内开展的工业和电信数据处理活动及其安全监管，应当遵守相关法律、行政法规和本办法的要求。

第三条【数据定义】工业数据是指原材料工业、装备工业、消费品工业、电子信息制造业、软件和信息技术服务业、民爆等行业领域，在研发设计、生产制造、经营管理、运维服务、平台运营、应用服务等过程中收集和产生的数据。

电信数据是指在电信业务经营活动中收集和产生的数据。

工业和电信数据处理者是指对工业、电信数据进行收集、存储、使用、加工、传输、提供、公开等数据处理活动的工业企业、软件和信息技术服务企业和取得电信业务经营许可证的电信业务经营者等工业和信息化领域各类主体。

第四条【监管机构】工业和信息化部负责对工业和电信数据处理者的数据处理活动和安全保护进行监督管理。各省、自治区、直辖市及计划单列市、新疆生产建设兵团工业和信息化主管部门（以下统称地方工业和信息化主管部门）负责对本地区工业数据处理者的数据处理活动和安全保护进行监督管理。各省、自治区、直辖市通信管理局（以下统称地方通信管理局）负责对本地区电信数据处理者的数据处理活动和安全保护进行监督管理。

工业和信息化部及地方工业和信息化主管部门、通信管理局统称为行业监管部门。

第五条【产业发展】行业监管部门鼓励数据开发利用和数据安全技术研究，

支持推广数据安全产品和服务，培育数据安全企业、研究和服务机构，壮大数据产业，提升数据安全保障能力，促进数据的创新应用。

工业和电信数据处理者研发提供数据开发利用新技术、新产品、新服务，应当有利于促进经济社会和行业发展，符合社会公德和伦理。

第六条【标准制定】行业监管部门推进工业和信息化领域数据开发利用和数据安全标准体系建设，组织开展行业标准制修订工作。鼓励支持企业、研究机构、高等院校、行业组织等不同主体，开展国际标准、国家标准、团体标准、企业标准制定。引导工业和电信数据处理者开展数据管理、数据安全贯标达标工作。

第二章 数据分类分级管理

第七条【分类分级方法】工业和电信数据处理者应当坚持先分类后分级，定期梳理，根据行业要求、业务需求、数据来源和用途等因素对数据进行分类和标识，形成数据分类清单。数据分类类别包括但不限于研发数据、生产运行数据、管理数据、运维数据、业务服务数据、个人信息等。工业和信息化部按照国家有关规定，根据数据遭到篡改、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、组织合法权益等造成的危害程度，将工业和电信数据分为一般数据、重要数据和核心数据三级。

第八条【一般数据】危害程度符合下列条件之一的数据为一般数据：

- （一）对公共利益或者个人、组织合法权益造成较小影响，社会负面影响小；
- （二）受影响的用户和企业数量较少、生产生活区域范围较小、持续时间较短，对企业经营、行业发展、技术进步和产业生态等影响较小；
- （三）恢复数据或消除负面影响所需付出的代价小；
- （四）其他未纳入重要数据、核心数据目录的数据。

第九条【重要数据】危害程度符合下列条件之一的数据为重要数据：

- （一）对政治、国土、军事、经济、文化、社会、科技、网络、生态、资源、核安全等构成威胁，影响海外利益、生物、太空、极地、深海、人工智能等重点

领域国家安全相关数据的安全；

(二) 对工业、电信行业发展、生产、运行和经济利益等造成影响；

(三) 造成重大数据安全事件或生产安全事故，对公共利益或者个人、组织合法权益造成严重影响，社会负面影响大；

(四) 引发的级联效应明显，影响范围涉及多个行业、区域或者行业内多个企业，或者影响持续时间长，对行业发展、技术进步和产业生态等造成严重影响；

(五) 恢复数据或消除负面影响所需付出的代价大；

(六) 经行业监管部门评估确定的其他重要数据。

第十条【核心数据】 危害程度符合下列条件之一的数据为核心数据：

(一) 对政治、国土、军事、经济、文化、社会、科技、网络、生态、资源、核安全等构成严重威胁，严重影响海外利益、生物、太空、极地、深海、人工智能等重点领域国家安全相关数据的安全；

(二) 对工业、电信行业及其重要骨干企业、关键信息基础设施、重要资源等造成严重影响；

(三) 对工业生产运营、电信和互联网运行和服务等造成重大损害，导致大范围停工停产、大面积网络与服务瘫痪、大量业务处理能力丧失等；

(四) 经工业和信息化部评估确定的其他核心数据。

第十一条【分类分级工作要求】 工业和信息化部组织制定工业和信息化领域数据分类分级、重要数据和核心数据识别认定及数据分级防护等制度规范，形成行业重要数据和核心数据具体目录并实施动态管理，指导开展数据分类分级防护工作。

地方工业和信息化主管部门、通信管理局组织开展本地区工业、电信行业数据分类分级防护及重要数据和核心数据识别认定工作，形成本地区行业重要数据和核心数据具体目录并上报工业和信息化部。

工业和电信数据处理者应当建立健全数据分类分级管理制度，将重要数据和核心数据目录报送地方工业和信息化主管部门或通信管理局，并采取措施开展数据分级防护，对重要数据进行重点保护，对核心数据在重要数据保护基础上实施更严格的管理和保护。不同级别数据同时被处理且难以分别采取保护措施的，应当按照其中级别最高的要求实施保护。

第十二条【重要数据和核心数据备案管理】工业和信息化部建立工业和信息化领域重要数据和核心数据备案管理制度，统筹建设备案管理平台。备案内容包括数据的数量、类别、处理目的和方式、使用范围、主体责任、安全保护措施等基本情况，数据提供、公开、出境、承接，以及数据安全风险、事件处置等情况。

地方工业和信息化主管部门、通信管理局应当分别对本地区工业、电信行业重要数据和核心数据备案内容进行审核，对不符合有关备案要求的，应当督促企业及时完善并重新进行备案。

工业和电信数据处理者应当按照有关要求进行备案，备案内容发生变化的，应在三个月内报备变更情况，同时对整体备案情况进行更新。

第三章 数据全生命周期安全管理

第十三条【主体责任】工业和电信数据处理者应当对数据处理活动负安全主体责任，根据数据的类型、数量、安全级别、处理方式以及对国家安全、公共利益或者个人、组织合法权益带来的影响和安全风险等，采取必要措施确保数据持续处于有效保护和合法利用的状态。

（一）建立数据全生命周期安全管理制度，针对不同级别数据，制定数据收集、存储、使用、加工、传输、提供、公开等环节的具体分级防护要求和操作规程；

（二）明确数据安全的主要负责人和责任部门，统筹负责数据处理活动的安全监督管理；

（三）合理确定数据处理活动的操作权限，严格实施人员权限管理；

(四) 制定数据安全事件应急预案，并定期进行演练；

(五) 定期对从业人员开展数据安全教育和培训；

(六) 法律、行政法规规定的其他措施。

第十四条【工作体系】涉及重要数据和核心数据的，工业和电信数据处理者应当建立覆盖本单位相关部门的数据安全工作体系，设置专门的数据安全管理责任部门，本单位党委（党组）或领导班子对数据安全负主体责任，主要负责人是数据安全第一责任人，分管数据安全的负责人是直接责任人，明确各部门数据安全职责及人员，建立常态化沟通与协作机制。

第十五条【关键岗位管理】工业和电信数据处理者应当确认数据处理关键岗位及人员，签署数据安全责任书，记录数据处理活动。

第十六条【安全同步】工业和电信数据处理者应当确保数据安全管理和技术保护手段与生产运营、业务发展同步规划、同步建设、同步运行。

第十七条【数据收集】工业和电信数据处理者收集数据应当遵循合法、正当、必要的原则，不得窃取或者以其他非法方式收集数据。

数据收集过程中，应当采取配备技术手段、签署安全协议等措施加强对数据收集人员、设备的管理，并对数据收集的时间、类型、数量、频度、流向等进行记录。

通过间接途径获取数据的，应当要求数据提供方做出数据源合法性的书面承诺，并承担相应的法律责任。

第十八条【数据存储】工业和电信数据处理者应当依据法律规定或者与用户约定的方式和期限存储数据。存储重要数据的，还应当采用校验技术、密码技术等措施进行安全存储，不得直接提供存储系统的公共信息网络访问，并实施数据容灾备份和存储介质安全管理。存储核心数据的，还应当实施异地容灾备份。

第十九条【数据使用加工】工业和电信数据处理者未经个人、单位等同意，不得使用数据挖掘、关联分析等技术手段针对特定主体进行精准画像、数据复原

等加工处理活动。利用数据进行自动化决策的，应当保证决策的透明度和结果公平合理。使用、加工重要数据和核心数据的，还应当加强访问控制，建立登记、审批机制并留存记录。

工业和电信数据处理者提供数据处理服务，涉及经营电信业务的，应当按照相关法律、行政法规规定取得电信业务经营许可。

第二十条【数据传输】工业和电信数据处理者应当根据传输的数据类型、级别和应用场景，制定安全策略并采取保护措施。传输重要数据的，还应当采取校验技术、密码技术、安全传输通道或者安全传输协议等措施，涉及跨组织机构或者使用公共信息网络进行数据传输的，应当建立登记、审批机制。跨不同数据处理主体传输核心数据的，还应当通过国家数据安全协调机制审批。

第二十一条【数据提供】工业和电信数据处理者应当依据行业数据分类分级管理要求，明确数据提供的范围、数量、条件、程序等。提供重要数据的，还应当采取数据脱敏等措施，建立审批机制。提供核心数据的，还应当通过国家数据安全协调机制审批。

工业和电信数据处理者应当事先对数据接收方的数据安全保护能力进行核实，并与数据接收方签订数据安全协议，明确数据提供的范围、使用方式、时限、用途以及相应的安全保护措施、违约责任，并督促数据接收方予以落实。

第二十二条【数据公开】工业和电信数据处理者公开数据应当真实、准确，并在公开前开展安全评估，对涉及个人隐私、个人信息、商业秘密、保密商务信息以及可能对公共利益及国家安全产生重大影响的，不得公开。

第二十三条【数据销毁】工业和电信数据处理者应当建立数据销毁策略和管理制度，明确销毁对象、流程和技术等要求，对销毁活动进行记录和留存。销毁重要数据和核心数据的，不得以任何理由、任何方式对销毁数据进行恢复。

符合以下情况之一的，工业和电信数据处理者应当销毁相应数据：

（一）因业务约定，需要销毁的；

(二) 个人依据其合法权益请求销毁的;

(三) 组织基于保护国家安全、社会公共利益目的, 且有第三方机构提供证明, 请求销毁的。

第二十四条【数据出境】 工业和电信数据处理者在中华人民共和国境内收集和产生的重要数据, 应当依照法律、行政法规要求在境内存储, 确需向境外提供的, 应当依法依规进行数据出境安全评估, 在确保安全的前提下进行数据出境, 并加强对数据出境后的跟踪掌握。核心数据不得出境。

第二十五条【数据承接】 工业和电信数据处理者因兼并、重组、破产等原因需要转移数据的, 应当明确数据承接方案, 并通过电话、短信、邮件、公告等方式通知受影响用户。涉及重要数据和核心数据的, 应当及时向所在地工业和信息化主管部门或通信管理局备案。

作为数据承接方的工业和电信数据处理者, 应当及时向所在地工业和信息化主管部门或通信管理局备案, 承担数据安全风险和保护义务, 不得违反国家有关规定及原数据处理者与用户的约定。

重要数据和核心数据没有承接方且符合销毁条件的, 工业和电信数据处理者应当依法进行数据销毁。重要数据和核心数据没有数据承接方且不符合销毁条件的, 工业和电信数据处理者应当及时上报所在地工业和信息化主管部门或通信管理局, 将数据移交至行业监管部门指定的机构进行保存。

第二十六条【委托处理】 工业和电信数据处理者委托他人开展数据处理活动的, 应当对被委托方的数据安全保护能力、资质进行核实, 确保符合国家、行业主管部门的相关要求, 并通过合同约定、现场核查等方式对被委托方落实数据安全保护措施的情况进行监督管理。委托处理重要数据和核心数据的, 还应当委托取得相应认证资质的检测评估机构对被委托方进行安全评估。

除法律、行政法规另有规定外, 未经委托方同意, 被委托方不得将数据提供给第三方。

第二十七条【安全审计】 工业和电信数据处理者应当在数据全生命周期处理

过程中，记录数据处理、权限管理、人员操作等日志。日志留存时间不少于六个月，定期进行安全审计，并形成审计报告，涉及重要数据和核心数据的，应当至少每半年进行一次。

第四章 数据安全监测预警与应急管理

第二十八条【监测预警机制】工业和信息化部统筹建立工业和信息化领域数据安全风险监测机制，建设数据安全监测预警平台，对数据泄露、违规传输、流量异常等安全风险进行监测和预警，及时组织研判重要数据和核心数据安全风险并进行预警。

地方工业和信息化主管部门、通信管理局建设数据安全监测预警平台，组织开展本地区工业、电信行业数据安全风险监测，按照有关规定及时发布预警信息，通知本地区工业和电信数据处理者及时采取应对措施。

工业和电信数据处理者应当开展数据安全风险监测，及时排查安全隐患，采取必要的措施防范数据安全风险。

第二十九条【信息上报和共享】工业和信息化部统一汇集、分析、通报工业和信息化领域数据安全风险信息，鼓励安全服务机构、行业组织、科研机构等开展数据安全风险和事件等相关信息上报和共享。

地方工业和信息化主管部门、通信管理局汇总分析本地区工业、电信行业数据安全风险和事件信息，及时将涉及重要数据和核心数据的安全风险上报工业和信息化部。

工业和电信数据处理者应当及时将自身数据安全风险情况向所在地工业和信息化主管部门或通信管理局报告。

第三十条【应急处置】工业和信息化部制定工业和信息化领域数据安全事件应急预案，组织协调重要数据和核心数据安全事件应急处置工作。

地方工业和信息化主管部门、通信管理局组织开展本地区工业、电信行业数据安全事件应急处置工作。涉及重要数据和核心数据的安全事件，应当立即上报

工业和信息化部，并及时报告事件发展和处置情况。

工业和电信数据处理者在数据安全事件发生后，应当按照应急预案，及时开展应急处置，涉及重要数据和核心数据的安全事件，应当第一时间向所在地工业和信息化主管部门或通信管理局报告。事件处置完成后应当在规定期限内形成总结报告，每年向所在地工业和信息化主管部门或通信管理局报告数据安全事件处置情况。

工业和电信数据处理者对可能损害用户合法权益的数据安全事件，应当及时告知用户，并提供减轻危害措施。

第三十一条【举报投诉处理】工业和信息化部委托相关行业组织建立工业和信息化领域数据安全违法行为投诉举报渠道，及时向地方工业和信息化主管部门、通信管理局、工业和电信数据处理者下发相关投诉举报信息。地方工业和信息化主管部门、通信管理局组织工业和电信数据处理者对举报信息进行核实和依法处理，对涉及重要数据和核心数据安全问题的，开展执法调查。

工业和电信数据处理者应当建立用户投诉处理机制，公布电子邮件、电话、传真、在线客服等便捷有效的联系方式，配备受理用户投诉的人员接收数据安全相关投诉，并自接到投诉之日起 15 个工作日内答复投诉人。

第五章 数据安全检测、评估与认证管理

第三十二条【安全能力认证】工业和信息化部建立数据安全检测、评估与认证机构管理制度，制定机构认定标准，开展机构选拔认定、资质授权、日常管理和推荐目录发布等工作。地方工业和信息化主管部门、通信管理局依据管理制度和认定标准，开展本地区工业、电信行业数据安全检测、评估与认证机构选拔认定、资质授权和管理等工作。

第三十三条【安全评估】工业和信息化部制定工业和信息化领域数据安全评估规范，指导检测评估机构开展数据安全风险评估、合规评估等工作。地方工业和信息化主管部门、通信管理局负责组织开展本地区工业、电信行业数据安全评估。

工业和电信数据处理者应当依据数据安全评估规范，开展数据安全评估及整改。

（一）对于一般数据，鼓励开展数据安全自评估，对发现的数据安全风险问题进行及时整改；

（二）对于重要数据和核心数据，应当至少每年自行或者委托推荐目录中的检测评估机构开展一次安全评估，并向所在地工业和信息化主管部门或通信管理局报告。

第六章 监督检查

第三十四条【监督检查和协助义务】工业和信息化部组织制定数据安全监测接口标准。行业监管部门对工业和电信数据处理者落实本规定要求的情况进行监督检查。工业和电信数据处理者应当配合行业监管部门依法开展监督检查，并预留检查接口。

第三十五条【数据安全审查】工业和信息化部在国家数据安全工作协调机制指导下，对影响或可能影响国家安全的工业和电信数据处理活动开展数据安全审查。

第三十六条【保密要求】行业监管部门及其委托的数据安全检测评估机构工作人员对在履行职责中知悉的个人信息和商业秘密等，应当严格保密，不得泄露、出售或者非法向他人提供。

第三十七条【约谈整改】行业监管部门在履行数据安全监督管理职责中，对未按要求进行重要数据和核心数据备案，或者发现数据处理活动存在重大安全风险或发生安全事件的，可以按照规定权限和程序对工业和电信数据处理者的法定代表人或者主要负责人进行约谈，并要求采取措施进行整改，消除隐患。

第七章 法律责任

第三十八条【信用机制】行业监管部门应当将工业和电信数据处理者落实数据安全管理工作情况纳入信用管理。对存在数据安全违法违规行为受到行政处罚

的数据处理者，按照有关规定将其列入业务经营不良名单或失信名单。

第三十九条【法律责任】对于违反本办法的，由行业监管部门依照《数据安全法》《网络安全法》等法律和相关行政法规，根据情节严重程度给予公开曝光、没收违法所得、罚款、暂停业务、停业整顿、关闭网站、吊销业务许可证或吊销营业执照等行政处罚；构成犯罪的，依法追究刑事责任。

第八章 附则

第四十条【涉密排除】涉及国家秘密信息、密码使用等数据处理活动，按照国家有关规定执行。

第四十一条【军事数据排除】涉及军事的数据处理活动，按照国家有关规定执行。

第四十二条【政务数据排除】工业和信息化领域政务数据处理活动的具体办法，由工业和信息化部另行规定。

第四十三条【国防科工、烟草领域】国防科技工业、烟草领域数据安全管理工作由国防科工局、国家烟草专卖局负责，具体制度参照本办法另行制定。

第四十四条【施行日期】本规定自 年 月 日起施行。

附件2:

起草说明

为贯彻落实《数据安全法》等法律法规，加快推动工业和信息化领域数据安全管理工作制度化、规范化，我部研究起草了《工业和信息化领域数据安全管理办法（试行）》（以下简称《管理办法》），指导督促工业和电信数据处理者依法依规开展数据处理活动，履行数据安全保护义务。有关情况说明如下：

一、《管理办法》总体考虑

《管理办法》定位为工业和信息化领域数据安全顶层设计，一是全面对接《数据安全法》要求。在工业和信息化领域对国家数据安全管理制度进行细化，明确开展数据分类分级保护、重要数据管理等工作的具体要求，为行业数据安全监管提供制度保障。二是构建工业和信息化领域数据安全监管体系。明确工业和信息化部、地方工业和信息化主管部门、地方通信管理局等管理部门的职责范围，建立权责一致的工作机制。三是明确数据保护要求。根据工业、电信行业实际情况，明确了数据全生命周期安全保护要求，指导行业企业健全数据安全管理和技术保护措施，履行保护义务。

二、《管理办法》主要内容

《管理办法》共八章四十四条，主要包括：

（一）关于行业管理职责。一是对工业数据、电信数据、工业和电信数据处理者的概念和范畴进行界定。二是明确工业和信息化部、地方工业和信息化主管部门、地方电信管理机构的监管职责。三是落实作为数据安全产业管理部门，需承担的支持技术研究和引导产业发展的责任。

（二）关于数据分类分级与重要数据安全。一是提出工业、电信数据分类分级方法，明确一般数据、重要数据、核心数据的判定条件。二是构建工业和信息化领域“部-地方-企业”三级联动的数据分类分级、重要数据和核心数据识别认定及数据分级防护等工作机制。三是建立工业、电信行业重要数据和核心数据全生命周期备案管理制度。

(三) 关于数据全生命周期安全管理。一是要求工业和电信数据处理者应当对数据处理活动负主体责任，加强数据安全。二是聚焦重要数据和核心数据建立工作体系，明确关键岗位管理要求。三是坚持“同步规划、同步建设、同步运行”原则，针对不同级别数据，从数据收集、存储、加工、传输、提供、公开、销毁、跨境、承接、委托处理等环节落实分级保护要求。

(四) 关于数据安全监测预警与应急管理。一是建立数据安全风险监测预警机制。二是开展风险信息上报和共享。三是制定数据安全事件应急预案，组织开展安全事件应急处置。四是建立针对数据安全违法行为的投诉处理机制。

(五) 关于数据安全检测评估与认证管理。一是建立数据安全检测评估、认证机构管理制度，开展检测评估、认证机构选拔认定和管理。二是制定工业和信息化领域数据安全评估规范，指导开展数据安全风险评估、合规评估。

(六) 关于监督检查。一是对工业和电信数据处理者落实数据安全保护义务进行监督检查。二是在国家数据安全工作协调机制指导下，对影响或可能影响国家安全的工业和电信数据处理活动开展数据安全审查。三是提出监督检查工作中的保密要求。

此外，《管理办法》还明确了违反本规定的法律责任，并对涉密数据、军事数据、政务数据作了排除规定。

三、重点问题的说明

(一) 关于监管范围。关于工业领域，在《管理办法》中明确列出包括原材料、装备、消费品、电子信息制造业、软件和信息技术服务业、民爆等领域，便于在实际工作中对应落实监管责任。电信行业范畴包括获得电信业务经营许可证的电信业务经营者。国防科技工业、烟草领域数据安全由国防科工局、国家烟草专卖局负责，可参照本办法另行制定管理制度。

(二) 关于与个人信息保护的关系。《数据安全法》将个人信息作为特别重要的一类数据，纳入重要数据目录和核心数据目录进行重点保护，既要遵守数据安全有关管理规定，还要遵守个人信息保护法的特别规定。《管理办法》秉承了

上述工作理念，将个人信息纳入数据全生命周期安全管理，不再单独提出个人信息保护的要求。

(十三) 网络交易监督管理方法（征求意见稿）

第一章 总则

第一条 为规范网络交易活动，维护网络交易秩序，保障网络交易各方主体合法权益，促进数字经济持续健康发展，依据相关法律、行政法规，制定本办法。

第二条 在中华人民共和国境内，通过互联网等信息网络销售商品或者提供服务的经营活动以及市场监督管理部门对其进行监督管理，适用本办法。在网络社交、网络直播等信息网络活动中销售商品或者提供服务的经营活动，适用本办法。

第三条 网络交易经营者从事经营活动，应当遵循自愿、平等、公平、诚信原则，遵守法律、法规和本办法，遵从商业道德和公序良俗，公平参与市场竞争，认真履行法定义务，积极承担主体责任，接受社会各界监督。

第四条 网络交易监督管理坚持鼓励创新、包容审慎、严守底线、线上线下一体化监管的原则。

对于网络交易新业态新模式，实行包容审慎监管，留足发展空间，同时确保商品和服务质量与交易安全。

第五条 引导网络交易经营者、网络交易行业组织、消费者权益保护组织、消费者共同参与网络交易市场治理，不断完善多元参与、有效协同、规范有序的网络交易市场治理体系。鼓励网络交易行业组织按照组织章程开展行业自律，建立健全行业规范，引导本行业经营者诚信守法经营、公平参与市场竞争。

第二章 网络交易经营者

第一节 一般规定

第六条 本办法所称网络交易经营者，是指组织、开展网络交易活动的自然人、法人和非法人组织，包括网络交易平台经营者、平台内经营者、自建网站经营者以及通过网络社交、网络直播等其他网络服务开展网络交易活动的网络交易经营者。

本办法所称网络交易平台经营者，是指在网络交易活动中为交易双方或者多方提供网络经营场所、交易撮合、信息发布等服务，供交易双方或者多方独立开展网络交易活动的法人或者非法人组织。本办法所称平台内经营者，是指通过网络交易平台开展网络交易活动的网络交易经营者。

网络社交、网络直播等其他网络服务提供者为消费者提供经营空间，并提供商品浏览、订单生成、在线支付等与完成交易有关的支持性服务的，在经营者资质审核、商品和服务信息监控、维护消费者权益、保护知识产权、信息数据提供、配合监管执法等方面应当依法履行网络交易平台经营者的责任。通过网络社交、网络直播等其他网络服务开展网络交易活动的网络交易经营者，参照适用本办法关于平台内经营者的有关规定。

第七条 网络交易经营者不得违反法律、法规、国务院决定的规定，从事无证无照经营。《电子商务法》第十条规定的可以免于办理市场主体登记情形以外的网络交易经营者，应当依法办理市场主体登记。

《电子商务法》第十条所称的“零星小额交易”是指，网络交易经营者年交易不超过 52 次且年交易额不超过所在省、自治区、直辖市上年度城镇私营单位就业人员年平均工资。同一经营者在同一平台或者不同平台开设多家网店的，各网店年交易次数、年交易额合并计算。

《电子商务法》第十条所称的“便民劳务活动”是指服务本地周边居民生活的营业性劳务活动，主要包括保洁、代厨、洗涤、缝纫、理发、搬家、配制钥匙、管道疏通、家电家具修理修配等。

第八条 网络交易经营者申请登记为个体工商户的，允许其将网络经营场所作为经营场所进行登记。对于在两个以上网络交易平台从事经营活动的，需要将其从事经营活动的所有网络经营场所向登记机关进行登记。允许将经常居住地登记为住所，个人住所所在地的县、自治县、不设区的市、市辖区市场监督管理部门为其登记机关。

第九条 网络交易经营者将网络经营场所作为经营场所进行登记的，由其入

驻的网络交易平台或者使用的网络服务的提供者为其出具网络经营场所地址证明，地址证明应当完整准确、能够独立识别并实时查验。

第十条 网络交易经营者应当在其网站首页或者从事经营活动的主页面显著位置，持续公示经营者主体信息或者该信息的链接标识。鼓励网络交易经营者链接到国家市场监督管理总局电子营业执照亮照系统，公示其营业执照信息。

已经办理市场主体登记的网络交易经营者应当公示下列信息以及与其经营业务有关的行政许可信息、实际地址、联系方式：

（一）企业应当公示其营业执照登载的统一社会信用代码（注册号）、名称、企业类型、法定代表人（负责人）、住所、注册资本（出资额）信息；

（二）个体工商户应当公示其营业执照登载的统一社会信用代码（注册号）、名称、经营者姓名、经营场所、组成形式信息；

（三）农民专业合作社应当公示其营业执照登载的统一社会信用代码（注册号）、名称、法定代表人、住所、成员出资总额信息。

依照《电子商务法》第十条规定未办理市场主体登记的经营者应当根据自身实际经营活动类型，分别公示以下自我声明以及实际地址、联系方式：

（一）“个人销售自产农副产品，依法免于办理市场主体登记”；

（二）“个人销售家庭手工业产品，依法免于办理市场主体登记”；

（三）“个人利用自己的技能从事依法无须取得许可的便民劳务活动，依法免于办理市场主体登记”；

（四）“个人从事零星小额交易活动，依法免于办理市场主体登记”。

网络交易经营者公示的信息发生变更的，应当在6个工作日内完成更新公示。

第十一条 网络交易经营者收集、使用用户的个人信息，应当取得被收集者授权同意，基于合法、正当、必要原则，明示收集、使用的目的、必要性、范围、方式，并不得采取一次概括授权方式，或者以默认授权、与其他授权捆绑、停止

安装使用等手段，强迫或者变相强迫被收集者同意收集、使用与经营活动无直接关系的信息。收集、使用生物识别信息、健康信息、财产信息、社交信息等敏感信息的，应当逐项取得被收集者授权同意。

网络交易经营者及其工作人员应当对收集的个人信息严格保密，未经被收集者授权同意，不得向包括关联方在内的任何第三方提供。

第十二条 网络交易经营者不得以下列方式欺骗、误导消费者：

（一）虚构交易；

（二）编造评价，或者教唆、诱导、胁迫他人进行虚假或者引人误解的评价；

（三）通过删除、隐匿、修改评价，或者好评前置、差评后置、混淆不同商品或者服务的评价等不正当处理手段对评价进行误导性展示；

（四）利用虚假或者使人误解的标价形式或者价格手段，欺骗、诱导消费者与其进行交易；

（五）使用虚假的广告宣传、促销方式、样品、商品或者服务说明、商品或者服务标准等；

（六）伪造或者冒用市场主体登记信息、行政许可信息；

（七）混淆商品或者服务的来源；

（八）虚构现货、虚假预订、虚假抢购等虚假营销行为；

（九）其他欺骗、误导消费者的行为。

第十三条 消费者评价中包含法律、行政法规禁止发布或者传输的信息的，网络交易经营者可以依法予以技术处理。

第十四条 未经消费者明确同意，网络交易经营者不得向其发送广告及其他商业性信息。经消费者明确同意的，应当为消费者提供显著、免费、简便的拒绝接收方式。消费者拒绝的，网络交易经营者应当立即停止发送，并不得更换名义后再次发送。

第十五条 网络交易经营者以直接捆绑或者提供多种可选项方式向消费者搭售商品或者服务的，应当以显著方式提醒消费者注意。提供多种可选项方式的，不得将搭售商品或者服务的任何选项设定为消费者默认同意，不得将消费者以往交易中选择的选项在后续独立交易中设定为消费者默认选择。

第十六条 网络交易经营者采取自动展期、自动续费等涉及消费者非主动立约的方式提供服务的，应当以显著方式提醒消费者注意。消费者自主选择有关方式的，网络交易经营者应当在全部服务期间内，为消费者提供显著、免费、简便的随时取消或者变更有关方式的选项，并在展期、续费等日期前5日以显著方式提醒消费者注意。

第十七条 网络交易经营者应当依照《消费者权益保护法》《产品质量法》等相关法律法规提供商品或服务的相关情况信息，充分保障消费者的知情权和选择权。

第十八条 网络交易经营者不得利用格式条款排除或者限缩消费者选择向有关行政部门投诉、向消费者保护组织请求调解、仲裁、诉讼等消费争议解决方式的权利。

第十九条 网络交易经营者应当按照国家市场监督管理总局、经总局授权的省级市场监督管理部门的要求，报送特定时段、特定品类、特定区域的商品或者服务的价格、销量、销售额等数据信息。

第二十条 网络交易经营者自行终止从事网络交易活动的，应当至少提前30日在其网站首页或者从事经营活动的主页面显著位置持续公示终止网络交易活动公告等有关信息，并采取合理措施保障消费者和相关经营者的合法权益。

第二十一条 通过网络社交、网络直播等其他网络服务组织、开展网络交易活动的网络交易经营者，应当以显著方式展示商品或者服务的实际经营主体、售后服务等信息，或者进行链接跳转提示。网络直播服务提供者应当为利用网络直播开展的网络交易活动提供回看功能。

第二节 网络交易平台经营者

第二十二条 网络交易平台经营者应当要求申请进入平台销售商品或者提供服务的经营者提交其身份、地址、联系方式、行政许可等真实信息，进行核验、登记，建立登记档案，并对登记档案至少每 6 个月核验更新一次。

第二十三条 网络交易平台经营者应当分别于每年 1 月 1 日至 1 月 15 日、7 月 1 日至 7 月 15 日向住所地省级市场监督管理部门报送平台内经营者的身份信息。平台内经营者的身份信息包括：

（一）已办理市场主体登记的平台内经营者的名称（姓名）、统一社会信用代码（注册号）、联系方式、网络店铺名称及网址链接等信息；

（二）未办理市场主体登记的平台内经营者的姓名、身份证件号码、实际经营地址、联系方式、网络店铺名称及网址链接、属于依法无需办理市场主体登记的具体情形的自我声明等信息。

鼓励网络交易平台经营者与市场监督管理部门建立开放数据接口等形式的自动化信息报送机制。

第二十四条 网络交易平台经营者应当为平台内经营者依法履行信息公示义务提供技术支持。平台内经营者公示的信息发生变更的，应当在 3 个工作日内将变更情况报送平台，平台应当在 3 个工作日内进行核验，完成更新公示。

第二十五条 网络交易平台经营者应当以显著方式区分标记已办理市场主体登记的经营者和未办理市场主体登记的经营者，确保消费者能够清晰辨认、直观理解、自主选择。

第二十六条 网络交易平台经营者变更平台服务协议和交易规则的，应当完整保存平台服务协议和交易规则的全部历史版本，保证经营者和消费者便利、完整地阅览和下载。

第二十七条 网络交易平台经营者应当对进入平台销售商品或者提供服务的经营者及其发布的商品或者服务信息建立检查监控制度，发现平台内经营者及其销售的商品或者提供的服务有违反市场监督管理法律、法规、规章和本办法规定情形的，应当依法采取必要处置措施，并保存有关记录。

网络交易平台经营者发现平台内经营者存在违反《电子商务法》第十二条、第十三条规定情形的，以及其它法律、法规和规章要求向市场监督管理部门报告的情形的，网络交易平台经营者应当依法向平台住所地县级以上市场监督管理部门报告。

第二十八条 网络交易平台经营者依据法律、法规、规章的规定或者服务协议和交易规则的约定，对平台内经营者采取警示、暂停服务、终止服务等处理措施的，应当自决定作出处理措施之日起 24 小时内予以公示，载明平台内经营者的网络店铺名称、违法行为、处理措施等信息。警示、暂停服务等短期处理措施应当持续公示至处理措施实施期满之日止。

第二十九条 网络交易平台经营者对平台内经营者身份信息长期保存，商品或者服务、消费支付、物流快递、退换货以及售后等交易信息的保存时间自交易完成之日起不少于 3 年。法律、行政法规另有规定的，从其规定。

第三十条 网络交易平台经营者应当自收到知识产权权利人依照《电子商务法》第四十二条发出的通知或者平台内经营者依照《电子商务法》第四十三条提交的声明后 24 小时内，在平台内经营者从事经营活动的主页面显著位置持续公示有关处理过程的基本信息；自收到知识产权权利人已经投诉或者起诉的通知后 24 小时内，在平台内经营者从事经营活动的主页面显著位置持续公示投诉或者起诉的基本信息。

网络交易平台经营者将平台内经营者的声明转送至知识产权权利人后，15 日内未收到知识产权权利人已经投诉或者起诉的通知的，应当在 24 小时内终止所采取的处理措施并撤回前款规定的公示信息。

第三十一条 网络交易平台经营者不得滥用优势地位干涉平台内经营者的自主经营，不得对平台内经营者与其他平台的商业合作进行不合理限制或者附加不合理条件。

平台内经营者可以自主选择在多个平台开展经营活动。平台与平台内经营者建立或者变更独家经营合作关系有关的事项，应当在平等基础上进行公平协商，

并通过书面形式对合作条件、双方义务、违约责任等予以明确约定，平台不得通过不合理的搜索降权、下架商品、限制经营、屏蔽店铺、提高服务收费等手段强制平台内经营者接受。平台提出建立或者变更独家经营合作关系有关的事项，造成平台内经营者损失的，应当对平台内经营者予以合理补偿。

第三十二条 网络交易平台经营者拟终止提供平台服务的，应当至少提前 3 个月在其网站主页面醒目位置予以公示并通知消费者和相关经营者，并采取必要措施保障消费者和相关经营者的合法权益。

第三十三条 网络交易平台经营者应当依法配合市场监督管理部门工作，按照要求提供与监督检查、案件调查、事故处置、消费争议处理等监管执法活动有关的平台内经营者身份信息、商品或者服务、消费支付、物流快递、退换货以及售后等交易信息以及其他数据信息。

为网络交易经营者提供宣传推广、支付结算、物流快递、网络接入、服务器托管、虚拟主机、云服务、网站网页设计制作等服务的经营者，应当及时协助市场监督管理部门依法查处网络交易违法行为，按照要求提供其掌握的有关数据信息。

市场监督管理部门发现网络交易经营者有违反市场监督管理法律、法规和规章的行为，依法要求网络交易平台经营者、其他服务提供者采取措施制止的，网络交易平台经营者、其他服务提供者应当予以配合。

第三章 监督管理

第三十四条 国家市场监督管理总局负责组织、指导全国网络交易监督管理工作，县级以上市场监督管理部门负责本行政区域内的网络交易监督管理。

第三十五条 网络交易平台经营者和自建网站经营者的违法行为，由其住所地市场监督管理部门管辖。

平台内经营者的违法行为由其实际经营地市场监督管理部门管辖，网络交易平台经营者住所地先行发现或者收到违法线索的，也可以进行管辖。对平台内经营者的消费投诉，平台内经营者实际经营地和网络交易平台经营者住所地市场监

督管理部门均有权处理。

第三十六条 网络交易平台经营者住所地和平台内经营者实际经营地市场监督管理部门应当在日常管理和执法活动中加强协同配合。网络交易平台经营者住所地省级市场监督管理部门应当根据工作需要，及时将掌握的平台内经营者的身份信息向其实际经营地省级市场监督管理部门共享。

第三十七条 市场监督管理部门应当采取必要措施保护网络交易经营者提供的信息的安全，并对其中的个人信息、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。

第三十八条 市场监督管理部门对网络交易经营者实施信用监管，将经营者的市场主体登记、行政许可、备案、资质资格认证、抽查检查结果、列入经营异常名录和严重违法失信企业名单、行政处罚等信息记入信用记录。除应当通过国家企业信用信息公示系统统一归集并依法公示上述信息中的涉企信息外，还可以通过市场监督管理部门官方网站、网络搜索引擎、经营者从事经营活动的主页面显著位置等方式公示上述信息。

第三十九条 市场监督管理部门对涉嫌违法的网络交易行为进行查处时，可以依法行使下列职权：

- （一）对与涉嫌违法的网络交易行为有关的场所进行现场检查；
- （二）查阅、复制与涉嫌违法的网络交易行为有关的合同、票据、账簿以及其他有关资料；
- （三）收集、调取与涉嫌违法的网络交易行为有关的电子数据；
- （四）询问涉嫌从事违法的网络交易行为的当事人；
- （五）向与涉嫌违法的网络交易行为有关的自然人、法人和非法人组织调查了解有关情况；
- （六）法律、法规规定可以采取的其他措施。

采取前款规定的措施，依法需要报经批准的，应当依法办理批准手续。

市场监督管理部门对网络商品交易及有关服务活动的技术监测记录资料，可以作为对违法的网络商品经营者、有关服务经营者实施行政处罚或者采取行政措施电子数据证据。

第四章 法律责任

第四十条 网络交易经营者违反本办法第十条、第二十条、第二十四条规定的，依照《电子商务法》第七十六条第一款的规定处罚。

第四十一条 网络交易平台经营者对违反本办法第十条、第二十条规定的平台内经营者未采取必要措施，或者违反本办法第二十四条规定的，依照《电子商务法》第七十六条第二款的规定处罚。

第四十二条 网络交易经营者违反本办法第十一条规定的，依照《消费者权益保护法》第五十六条的规定处罚。

第四十三条 网络交易经营者违反本办法第十二条规定的，依照《反不正当竞争法》第二十条的规定处罚。

第四十四条 网络交易经营者违反本办法第十五条规定的，依照《电子商务法》第七十七条的规定处罚。

第四十五条 网络交易经营者违反本办法第十八条规定的，依照《合同违法行为监督处理办法》《侵害消费者权益行为处罚办法》的规定处罚。

第四十六条 网络交易平台经营者违反本办法第二十二条、第二十三条、第二十七条、第二十九条规定的，依照《电子商务法》第八十条的规定处罚。

其中，网络交易平台经营者有下列情形之一的，依照《电子商务法》第八十三条的规定处罚：

（一）知道或者应当知道平台内经营者销售的商品或者提供的服务不符合保障人身、财产安全的要求，或者有其他侵害消费者合法权益行为，未采取必要措施的；

（二）对销售或者提供关系消费者生命健康的商品或者服务的平台内经营者

的资质资格未尽到审核义务，或者对消费者未尽到安全保障义务的。

第四十七条 网络交易经营者违反本办法第十三条、第十四条、第十六条、第十九条、第二十一条规定的，责令限期改正，并处一万元以下的罚款；情节严重的，处一万元以上三万元以下的罚款。

第四十八条 网络交易平台经营者违反本办法第九条、第二十五条、第二十六条、第二十八条、第三十条、第三十一条、第三十二条、第三十三条规定的，责令限期改正，并处一万元以上三万元以下的罚款。

其他服务提供者违反本办法第三十三条的，依照前款的规定处罚。

第五章 附 则

第四十九条 本办法由国家市场监督管理总局负责解释。

第五十条 本办法自 年 月 日起施行。原国家工商行政管理总局 2014 年 1 月 26 日发布的《网络交易管理办法》同时废止。

《网络交易监督管理办法（征求意见稿）》起草说明

《电子商务法》自 2019 年 1 月 1 日施行以来，全国市场监管部门大力开展法律宣传，依法推进网络交易市场监管工作，持续提升监管执法规范化水平。为更好地贯彻落实《电子商务法》，规范网络交易市场秩序，维护各方主体合法权益，促进网络交易持续健康发展，市场监管总局在修改《网络交易管理办法》（原工商总局令第 60 号）基础上起草了《网络交易监督管理办法（公开征求意见稿）》（以下简称《办法》）。现将有关起草情况说明如下。

一、《办法》的必要性和制定过程

原工商总局令第 60 号《网络交易管理办法》针对网络交易概念定义、适用范围、网络交易经营者权利责任义务、监督管理等内容作出了规定，自 2014 年 3 月 15 日施行以来，在依法加强网络交易监管执法，维护网络市场良好秩序，维护各方主体合法权益，推动网络经济快速发展等方面起到了积极作用。在《电子商务法》颁布实施后，依照法律最新规定对《网络交易管理办法》相关内容予以

修订，既是贯彻落实依法治国精神、更好履行市场监管职责的需要，又是促进数字经济发展的客观要求。

2018年9月，市场监管总局网监司组织全司力量，并抽调系统骨干人员成立起草小组，正式启动《办法》起草制定工作。前期，起草组为增强《办法》制定工作的科学性、实用性和可操作性，对规章框架、主要制度规定等进行了总体研究，并结合地方调研反映的突出问题，起草完成了《办法》初稿。2019年，召开两次系统内网监业务条线代表研讨会，就重点条款进行了研究分析。同时，先后征求了总局各业务司局、地方市场监管部门和国务院相关部门意见，并委托中国市场监管学会、工商出版社等机构召开了系统内外专家学者、网络交易经营者、消费者等各方主体代表参加的座谈会、研讨会，充分听取社会各界特别是经营者和消费者对《办法》的意见建议，在全面研究各方意见，充分吸收有益建议基础上，不断修改完善。

2020年，结合疫情期间网络交易业态新动向，聚焦网络社交、网络直播等领域规范管理的现实需要，深入研究其他服务提供者的功能角色、新业态新模式各方参与者责任义务等重点问题，进一步修改完善部分条文，努力探索符合行业发展规律和业态监管规律的监管规则。同时，针对经营者市场主体登记、平台责任和义务、各类法定公示义务等问题，在职责权限内尽力细化《电子商务法》相关规定，努力提高制度设计科学性和可操作性。近期，再次组织召开专题座谈会，征集了业界专家学者、系统内监管骨干的意见建议，进一步修改调整，形成本稿。

二、《办法》遵循的基本原则

《办法》是根据《电子商务法》相关规定，遵循促进发展、规范秩序、保障各方权益的基本理念，结合当前网络交易监管执法实际制定的。主要坚持了如下原则：

（一）科学严谨，着眼制度建设全局。严格遵循《规章制定程序条例》和总局规章制定有关规定，在《电子商务法》《消费者权益保护法》等上位法的规定范围内，对概括性规定进行细化，予以尽可能明确，审慎框定概念，严谨表述用语。基于市场监管职能，力求网络交易市场监管执法全覆盖、一体化，同时严格

按照“三定”方案确定的职责进行规定，不突破法定权限。

（二）民主立规，广泛吸纳意见建议。起草小组进行了现行法律制度的总体研究，并赴北京、上海、杭州、厦门等地进行了全面调研，从框架确立到具体条文，均源于现实需求，坚持问题导向。在起草过程中，严格按照程序要求征求了总局各司局和相关部委意见，先后组织召开多次专家研讨会、企业代表座谈会，听取了消费者组织、社会各界意见，广泛吸纳社会共识，对合理性建议进行了充分的吸收。

（三）在制度规范性和执法实践性之间力求统一。《办法》的制定着眼于落实《电子商务法》制度设计，旨在进一步完善网络交易监管规制体系，同时又必须对一线监管工作中的可操作性予以充分考量。《办法》高度关注当前网络交易监管工作现实因素，基于一线执法特点进行制度规则的具体化，从而真正实现有用、好用。

（四）在权益保护与经济效益等关系上寻找平衡。网络交易参与各方包括消费者、经营者和相关用户等多方主体，均依法享有不受侵犯的合法权益，又承担法定义务，各自履责享权是提升整体效率的基础。权益的保护尤其是消费者权益保护在网络交易监管整体制度建设中永远处于第一位，提升效率、保障发展同样是优化监管的目标追求。《办法》制定过程中力求在两者之间达致公允，实现最大平衡。

三、《办法》的基本内容

《办法》共 50 条，主要包括：

（一）网络交易监管与服务发展的基本原则。明确网络交易监管坚持鼓励创新、包容审慎、严守底线、线上线下一体化监管的原则，着眼于促进数字经济健康发展。对于网络社交、网络直播等网络交易新业态新模式，实行包容审慎监管，留足发展空间，同时确保商品和服务质量与交易安全。

（二）网络交易经营者市场主体登记。允许自然人网店经营者将网络经营场所作为经营场所依法登记为个体工商户，并明确规定了由该经营者入驻的网络交

易平台或者使用的网络服务的提供者为其出具网络经营场所地址证明。

（三）网络交易经营者信息公示。主要依照《电子商务法》规定细化了网络交易经营者身份信息公示的具体要求，特别是明确了依法免于办理市场主体登记的经营者应当持续公示其依法免于办理市场主体登记情形的自我声明、实际地址、联系方式等信息或者链接标识。

（四）网络交易信息数据报送与提供。主要规定了平台经营者应当依法向市场监管部门报送已经办理市场主体登记的平台内经营者的名称、统一社会信用代码等信息，以及依法免于办理市场主体登记的平台内经营者的姓名、身份证号、联系方式等信息。

（五）用户信息的收集使用。主要规定了网络交易经营者应当依法收集、使用消费者或者经营者信息，对其收集的消费者个人信息或者经营者的商业秘密应当严格保密等内容。

（六）具体经营行为规范。主要规定了网络交易经营者应当全面、真实、准确、及时地披露商品或者服务信息；不得以虚构交易、编造评价等方式进行虚假或者引入误解的虚假宣传；不得以不正当手段进行任何形式的搭售等。

（七）网络消费权益保护。主要规定了网络交易经营者应当依照《消费者权益保护法》《产品质量法》等相关法律法规提供商品或服务的相关情况信息，充分保障消费者知情选择权。

四、若干重要问题的说明

（一）关于《办法》名称问题

拟定名称《网络交易监督管理办法》，而非《电子商务监督管理办法》，主要基于如下考虑：一是本《办法》源自对《网络交易管理办法》的修订，并考虑到市场监管总局及网络交易监督管理机构设置进一步突出了行政监督职能，延续原名称基础上增加监督二字符符合现实情况；二是除市场监管部门以外，《电子商务法》相关规定也涉及到其他部门职责，本《办法》不是《电子商务法》唯一配套规章。三是市场监管总局、网络交易监督管理司“三定”方案均采用了“网

络交易监督管理”的统一规范表述，从规章名称宜与部门机构职责相一致的角度考虑也更加合理。

（二）关于“零星小额”判定问题

《电子商务法》规定了“零星小额交易”免于办理市场主体登记，但并未明确零星小额的含义和范围，后全国人大法工委专函授权市场监管总局研究制定有关判定标准。

经反复研究，我们认为，“零星小额”包括“零星”和“小额”两个概念要素，两者之间应是“且”的关系。如果理解为“或”，则包括“零星但是大额”的交易（如零星销售黄金珠宝、奢侈品等）和“小额但不零星”的交易（如某大型网络店铺9.9元手机壳单品年销售可达百万件），对上述两类经营者免于登记，显然不符合维护网络交易安全和保护消费者合法权益的基本要求，也将带来线上线下歧视性管理待遇等诸多问题，不仅有悖于捍卫公平竞争市场秩序的监管初心，更可能导致在保障人民群众人身财产安全方面底线失守。鉴此，我们围绕“零星且小额交易”的界定进行了认真研究，多次组织专家学者、经营者代表、消费者保护组织等进行专题座谈，并向代表性平台企业进行了支持性数据的收集调研。

经全面论证、审慎研究、反复斟酌，现稿遵循“零星小额交易是在一定程度上贴补个人花销的、偶发的、非连续性的交易行为”的立法原意，采用了“明确统一的交易次数+地区差异化交易金额”的判定框架。其中，年交易次数拟定为52次（约合每周发生1次网络交易），年交易额以其所在省、自治区、直辖市上年度城镇私营单位就业人员年平均工资为限。这主要考虑到，当前我国各地区之间网络交易发展状况很不平衡，人均可支配收入等方面尚有较大差异，在“小额”标准上有必要通过地区差异化的制度设计，来有效匹配各地经济社会发展实际，更好推动各地线上线下衔接互动、融合发展。“所在省、自治区、直辖市上年度城镇私营单位就业人员年平均工资”这一基准的研拟，主要基于以下考量：

一是目前既有的互联网领域法律法规均没有“小额”概念，但在现行民事诉讼制度中有“小额诉讼”的概念。根据《民事诉讼法》第162条，基层人民法院

和它派出的法庭审理简单民事案件，标的额为各省、自治区、直辖市上年度就业人员年平均工资 30%以下的，实行一审终审。可见，此类“小额诉讼”由于争讼金额小，即使有所错判也不致对双方权益产生大的影响，因此法律不再给予其二审的程序权利。这与《电子商务法》创设“零星小额”概念在立法精神、规范逻辑上具有高度的内在一致性：网络小额交易同样是由于价格低、货值小，即便发生纠纷也相对容易调处，更不致对消费者权益产生大的损害；加之其仅为贴补个人或者家庭生活的初衷，免于将其纳入商事登记为核心的行政管理框架，既是为民便民利民之策，也是节约行政资源之举。因此，这一小额标准是在当前法律规范体系下最宜参照的既有基准，也有利于后续行政监管和司法活动的衔接配合。在立规调研中，也有意见认为可采用税务领域“小规模纳税人”或者“个人所得税起征点”有关金额。我们对此进行了认真分析，上述观点有的将市场主体登记和依法纳税义务的发生等同看待，有的则把个人净收入与经营收入混为一谈，我们经过审慎研究并商有关主管部门，认为均不适合作为参照基准。

二是网络“零星小额”交易本身作为个体私营经济一种新的实现形式，与城镇私营单位就业人员具有更高的一致性。较之全部就业人员，采用城镇私营单位就业人员年平均工资更加贴合“零星小额”交易者个人生活收支的实际情况。同时，在网络交易经营者分布集中的北京、上海、广州、杭州等一线二线城市，城镇私营单位就业人员收入水平往往高于全部就业人员水平，从而将标准在更大范围内尽可能实现从高而定。

三是根据向部分代表性平台企业进行的支持性数据调研反馈情况看，个人网络店铺经营额呈现出明显“金字塔型”的分布特点，采用该标准已经可以让偶发交易的、贴补家用的交易用户免于登记，而对于连续经营、以此为主业的经营，又能合理纳入登记范围。这既坚持了《电子商务法》以登记为原则、免于登记为例外的规定精神，又符合线上线下公平一致原则。同时，在最大程度上赋予更多经营者免于登记的政策便利，将进一步助力复工复产，拉动居民消费，更好激发网络经济创新活力。

（三）关于删除评价问题

在起草过程中，有意见认为不允许平台删除消费评价的规定没有考虑恶意差评以及侮辱诽谤等不良有害信息的删除需要。对此，我们研究认为，这一问题在《电子商务法》第39条有明确要求，“不得删除评价”的规定并未附加任何除外情形，其旨在将平台内销售的商品或者提供的服务的“评价”全貌呈现出来，以充分实现信用约束的制度功能。相关专家学者和企业所提到的恶意差评以及侮辱诽谤的不良信息的删除权，在实践中面临平台经营者难以判断和证实是否恶意、是否不良的重大操作问题；另据了解，实践中平台内经营者因评价不实等申请平台经营者予以删除的，最终实际删除的比例不足5%。因此，对于平台经营者删除评价权限的问题，我们坚持审慎对待，规定了平台对消费者评价中包含的法律、行政法规禁止发布或者传输的信息可以依法予以技术处理。

（四）关于信息报送问题

网络交易经营者依法报送有关数据信息对于市场监管部门正常履职、保护各方主体合法权益、促进数字经济健康发展都具有不可或缺的重要性。本办法对《电子商务法》规定的平台报送平台内经营者身份信息的法定义务进行了细化，明确平台向省级市场监管部门报送平台内经营者的身份信息。同时，基于当前网络交易现实环境下，各类新设立市场主体持续快速增长，同时存续期较短，特别是依照《电子商务法》豁免登记的经营者，其生存周期尤其是活跃时间普遍较短，往往不足一个年度，若在此期间内发生违法或侵权行为，很容易直接“关门失联”，市场监管部门自始至终无法获取其身份信息，直接严重影响监管执法工作开展。因此，明确了以每年1月1日至1月15日、7月1日至7月15日为期，由平台一年两报。同时，考虑到部分平台提出希望将报送级别适当提高从而保障报送统一和报送信息的安全等意见，将报送部门的级别明确为省级市场监管部门。

（五）关于其他网络服务提供者问题

《电子商务法》并未直接规定网络社交、网络直播等其他网络服务提供者是否属于平台经营者。对此问题，我们认为应结合此类网络交易新业态的实际情况具体分析，既不能将其他网络服务提供者等同于网络交易平台经营者，也不能简单认为其他网络服务提供者就不是网络交易平台经营者。目前社会各方的基本共

识是，当其他网络服务提供者经营者提供了具有类似网络交易平台性质的服务时，即具有网络交易平台经营者属性。鉴此，明确了网络社交、网络直播等其他网络服务提供者在满足一定条件时应当依法履行网络交易平台经营者的责任。同时，积极回应社会关切，对网络直播活动的信息展示进行了特别规定，并要求平台为利用网络直播开展的网络交易活动提供直播回看功能。

（六）关于平台“二选一”问题

近年来，部分网络交易平台利用平台内经营者对其高度经营依赖性等方面形成的相对优势地位对平台内经营者和其他平台的合作进行不合理限制的情况不断出现，有关舆论称之为“二选一”问题，持续引发社会各界普遍关注。现稿基于监管实践，重点从平台优势地位、平台内经营者自主经营权、自愿平等协商原则等角度，对这一问题进行了针对性规范，主要明确了平台与平台内经营者建立或者变更独家经营合作关系有关的事项应当以书面方式明确约定，平台不得强迫平台内经营者接受等。

（七）关于细化有关程序时效问题

《电子商务法》在经营者信息定期更新与报送、知识产权通知声明程序等诸多规则中，概括规定了有关时效要求，现稿对有关时效进行了细化要求，从而提高具体执行的操作性。在时效的长短问题上，充分考虑当前经营者技术能力、实际管理需求、实施效果对时效性的要求等，反复权衡、综合研判。比如在知识产权通知声明程序中，由于可能存在正在持续的侵权行为，以24小时作为平台双向转送的时限要求，促使有关程序尽快推进。

特此说明。

五、部门规范性文件

(一) 交通运输部关于印发《交通运输政务数据共享管理办法》的通知

(交科技发〔2021〕33号)

各省、自治区、直辖市、新疆生产建设兵团交通运输厅（局、委），部属各单位，部内各司局：

现将《交通运输政务数据共享管理办法》印发给你们，请遵照执行。

交通运输部

2021年4月6日

交通运输政务数据共享管理办法

第一章 总 则

第一条 为规范交通运输政务数据共享，推动交通运输数字政府建设，加快建设交通强国，依据国务院关于政务数据共享管理要求，制定本办法。

第二条 本办法所称交通运输政务部门（以下简称政务部门），是指交通运输主管部门及法律、法规授权行使交通运输行政管理职能的事业单位和社会组织。

本办法所称交通运输政务数据，是指政务部门在履行职责过程中直接或通过第三方依法采集、产生、获取的，以电子形式记录、保存的各类非涉密数据、文件、资料和图表等。

本办法所称提供部门，是指产生和提供政务数据的政务部门。本办法所称使用部门，是指因履行职责需要使用政务数据的政务部门。

第三条 本办法用于规范交通运输部及部际、部省相关政务部门因履行职责

需要提供和使用政务数据的行为。

第四条 部科技主管部门负责管理、监督和评估政务数据共享工作，组织管理交通运输政务数据目录编制工作，组织推进部数据共享交换平台（以下简称部共享平台）政务数据接入，组织开展相关制度文件、标准规范的制修订和宣贯实施，监督部共享平台的运行。

综合交通运输大数据应用技术支持部门（以下简称技术支持部门）受部科技主管部门委托，负责部共享平台的建设运维、部共享平台政务数据目录和政务数据维护管理，并为政务数据共享和开发利用等工作提供技术支持。

提供部门负责组织开展本部门政务数据目录编制、政务数据提供和授权等相关工作，并对所提供政务数据质量负责。

使用部门依据政务数据目录申请使用政务数据、安全合规使用政务数据，并反馈使用情况。

第五条 政务数据共享应遵循以下原则：

（一）以共享为原则，不共享为例外。政务数据原则上均应共享，国家相关法律法规或政策制度明确不得共享的除外。

（二）需求导向，无偿使用。使用部门提出明确的共享需求和政务数据使用用途，提供部门应及时响应并无偿提供共享服务。

（三）统一标准，平台交换。按照国家及行业相关标准规范进行政务数据的编目、采集、存储、交换和共享工作。政务部门应基于部、省两级共享平台开展政务数据共享。

（四）建立机制，保障安全。建立健全政务数据共享管理机制。加强对政务数据共享全过程的身份鉴别、授权管理和安全保障，确保政务数据安全。

第二章 分类与要求

第六条 政务数据按共享类型分为无条件共享、有条件共享、不予共享三种类型。

可提供给所有政务部门共享使用的政务数据属于无条件共享类。

可提供给部分政务部门共享使用或仅部分内容能够提供给政务部门共享使用的政务数据属于有条件共享类。

不宜提供给其他政务部门共享使用的政务数据属于不予共享类。

第七条 政务数据共享类型划分应遵循以下要求：

（一）经脱密处理的交通运输基础设施空间和属性信息，以及运载工具基本信息、从业企业基本信息、从业人员基本信息、行政许可信息、执法案件结果信息、信用信息等基础数据是政务部门履行职责的共同需要，必须接入部共享平台实现集中汇聚、统筹管理、及时更新，供政务部门无条件共享使用。

（二）列入有条件共享类的政务数据，提供部门应明确共享条件。

（三）列入不予共享类的政务数据，提供部门应出具国家相关法律法规或政策制度依据。

第三章 目录编制与管理

第八条 政务数据目录是实现政务数据共享和业务协同的基础，是政务部门间政务数据共享的依据。

政务数据目录核心元数据包括分类、名称、提供部门、格式、信息项信息、更新周期、共享类型、共享条件、共享范围、共享方式、来源系统、安全分级等内容。政务数据目录应按照版本进行管理。

第九条 提供部门应依据相关技术规范在部共享平台编制政务数据目录，确保政务数据目录准确完整。通过合规性检测的政务数据目录方可在部共享平台发布。

政务数据目录一经发布，不得随意更改。因信息系统升级改造等原因造成数据变更，确需更改政务数据目录的，提供部门应及时在部共享平台上更新目录。数据正被使用的，提供部门应至少在数据变更前3个月进行登记。

第四章 提供与使用

第十条 凡涉及交通运输部的政务数据共享均应通过部共享平台实施，部共享平台提供联机查询、数据订阅、数据下载等共享服务。

第十一条 新建的部级信息系统、部省联网运行的信息系统，须通过部共享平台实现政务数据共享。原有跨部门、跨层级的行业政务数据共享交换系统在升级改造时，须迁移到部共享平台。

第十二条 使用部门申请共享政务数据时应明确使用用途。

申请无条件共享类政务数据的，经部共享平台身份验证通过后可自动获得授权。

申请有条件共享类政务数据的，技术支持部门应在3个工作日内完成申请信息初审；通过初审的，提供部门须在7个工作日内完成审核。拒绝共享的，提供部门应提供法律法规或政策制度依据。需提供其他证明材料的，提供部门应在共享条件中说明。

对于不予共享的政务数据，使用部门因履行职责确需使用的，由使用部门与提供部门协商解决。

第十三条 已接入部共享平台的行业外政务数据，由部科技主管部门授权使用。未接入部共享平台的行业外政务数据，使用部门向部科技主管部门提交申请，由部科技主管部门协调接入。

第十四条 提供部门可委托技术支持部门对政务数据申请进行审核，技术支持部门定期向提供部门反馈审核情况。

第十五条 提供部门应保障所提供政务数据的完整性、准确性、时效性和可用性。对使用部门反馈的政务数据质量问题，提供部门应及时予以校核并反馈。

第十六条 使用部门应依法依规使用政务数据，按照申请的使用用途将政务数据用于本部门履职需要，不得滥用、非授权使用、未经许可扩散或泄露所获取的政务数据，不得直接或以改变数据形式等方式提供给第三方，也不得用于或变

相用于其他目的。需改变使用用途的，应重新申请并获得授权。

第十七条 使用部门应在部共享平台上反馈共享政务数据使用情况，包括满足需求情况、数据质量以及使用效果。对于已授权但3个月内未使用的政务数据，授权部门可撤销授权。

第五章 监督与保障

第十八条 部科技主管部门负责建立政务数据共享监督评估制度，组织开展政务数据检查和共享评估工作。

第十九条 政务部门应遵循国家和行业网络安全管理法规、政策和制度，按照“谁管理、谁负责”和“谁使用、谁负责”的原则，建立健全政务数据安全保障机制，落实安全管理责任和数据分类分级要求，加强本部门政务数据提供渠道和使用环境的安全防护，切实保障政务数据采集、存储、传输、共享和使用安全。

第二十条 部级信息系统应在立项阶段通过部共享平台预编政务数据目录，上线试运行前在部共享平台上编制正式政务数据目录，并在试运行6个月内接入政务数据。

部共享平台提供的编目回执将作为项目立项审批、上线试运行及验收等环节重要依据。通过政务数据预编目录合规性检测的，方可下载预编目回执；通过政务数据目录合规性检测并接入数据的，方可下载正式编目回执。

申请部补助资金的省级信息化建设项目，应按照部印发的建设指南、标准规范等指导性文件，落实政务数据共享要求。

第二十一条 政务部门应保障信息资源共享工作经费，将政务数据目录编制、共享平台建设及运行维护等工作经费纳入本部门年度预算。

第二十二条 政务部门主要负责人是本部门政务数据共享工作的第一责任人。政务部门应明确本部门实施机构和工作人员。

第二十三条 政务部门有下列情形之一的，由部科技主管部门通知整改：

（一）未按要求编制和更新政务数据目录的。

(二) 未向部共享平台及时提供、更新政务数据的。

(三) 向部共享平台提供的政务数据和实际掌握数据不一致的，或提供的政务数据不符合有关规范、无法使用的。

(四) 对已发现不一致或有明显错误的政务数据，不及时校核的。

(五) 对共享获取的政务数据管理失控，致使出现滥用、非授权使用、未经许可扩散或泄漏的。

(六) 未经提供部门授权，擅自将政务数据提供给第三方或用于其他目的的。

(七) 违反本办法规定的其他行为。

第二十四条 不按本办法要求执行且通报后拒不整改的，不予安排运行维护经费，不予提供硬件资源，不予审批新建、改建、扩建项目。

第六章 附 则

第二十五条 本办法由部科技主管部门负责解释。

第二十六条 本办法自2021年4月15日起施行。2017年4月27日交通运输部印发的《交通运输政务信息资源共享管理办法（试行）》（交科技发〔2017〕58号）同时废止。涉及政务内网数据共享有关规定另行制定。

(二) 互联网个人信息安全保护指南

(2019年4月10日 公安部网络安全保卫局、北京网络行业协会、公安部第三研究所)

引 言

为有效防范侵犯公民个人信息违法行为，保障网络数据安全和公民合法权益，公安机关结合侦办侵犯公民个人信息网络犯罪案件和安全监督管理工作中掌握的情况，组织北京市网络行业协会和公安部第三研究所等单位相关专家，研究起草了《互联网个人信息安全保护指南》，供互联网服务单位在个人信息保护工作中参考借鉴。

1 范围

本文件制定了个人信息安全保护的管理机制、安全技术措施和业务流程。

适用于个人信息持有者在个人信息生命周期处理过程中开展安全保护工作参考使用。本文件适用于通过互联网提供服务的企业，也适用于使用专网或非联网环境控制和处理个人信息的组织或个人。

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

GB/T 22239 信息安全技术 网络安全等级保护基本要求（信息系统安全等级保护基本要求）

3 术语和定义

3.1 个人信息

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。

[中华人民共和国网络安全法，第七十六条（五）]

注：个人信息还包括通信通讯联系方式、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。

3.2 个人信息主体

个人信息所标识的自然人。

3.3 个人信息持有

对个人信息及相关资源、环境、管理体系等进行计划、组织、协调、控制的相关活动或行为。

3.4 个人信息持有者

对个人信息进行控制和处理的组织或个人。

3.5 个人信息收集

获得对个人信息的控制权的行为，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，以及通过共享、转让、搜集公开信息间接获取等方式。

3.6 个人信息使用

通过自动或非自动方式对个人信息进行操作，例如记录、组织、排列、存储、改编或变更、检索、咨询、披露、传播或以其他方式提供、调整或组合、限制、删除等。

3.7 个人信息删除

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。

3.8 个人信息生命周期

包括个人信息持有者收集、保存、应用、委托处理、共享、转让和公开披露、删除个人信息在内的全部生命历程。

3.9 个人信息处理系统

处理个人信息的计算机信息系统，涉及个人信息生命周期一个或多个阶段（收集、保存、应用、委托处理、共享、转让和公开披露、删除）。

4 管理机制

4.1 基本要求

个人信息处理系统的安全管理要求应满足GB/T 22239相应等级的要求。

4.2 管理制度

4.2.1 管理制度内容

a) 应制定个人信息保护的总体方针和安全策略等相关规章制度和文件，其中包括本机构的个人信息保护工作的目标、范围、原则和安全框架等相关说明；

b) 应制定工作人员对个人信息日常管理的操作规程；

c) 应建立个人信息管理制度体系，其中包括安全策略、管理制度、操作规程和记录表单；

d) 应制定个人信息安全事件应急预案。

4.2.2 管理制度制定发布

a) 应指定专门的部门或人员负责安全管理制度的制定；

b) 应明确安全管理制度的制定程序和发布方式，对制定的安全管理制度进行论证和审定，并形成论证和评审记录；

c) 应明确管理制度的发布范围，并对发文及确认情况进行登记记录。

4.2.3 管理制度执行落实

- a) 应对相关制度执行情况进行审批登记;
- b) 应保存记录文件, 确保实际工作流程与相关的管理制度内容相同;
- c) 应定期汇报总结管理制度执行情况。

4.2.4 管理制度评审改进

- a) 应定期对安全管理制度进行评审, 存在不足或需要改进的予以修订;
- b) 安全管理制度评审应形成记录, 如果对制度做过修订, 应更新所有下发的相关安全管理制度。

4.3 管理机构

4.3.1 管理机构的岗位设置

- a) 应设置指导和管理个人信息保护的工作机构, 明确定义机构的职责;
- b) 应由最高管理者或授权专人负责个人信息保护的工作;
- c) 应明确设置安全主管、安全管理各个方面的负责人, 设立审计管理员和安全管理员等岗位, 清晰、明确定义其职责范围。

4.3.2 管理机构的人员配置

- a) 应明确安全管理岗位人员的配备, 包括数量、专职还是兼职情况等; 配备负责数据保护的专门人员;
- b) 应建立安全管理岗位人员信息表, 登记机房管理员、系统管理员、数据库管理员、网络管理员、审计管理员、安全管理员等重要岗位人员的信息, 审计管理员和安全管理员不应兼任网络管理员、系统管理员、数据库管理员、数据操作员等岗位。

4.4 管理人员

4.4.1 管理人员的录用

- a) 应设立专门的部门或人员负责人员的录用工作;

- b) 应明确人员录用时对人员的条件要求，对被录用人的身份、背景和专业资格进行审查，对技术人员的技术技能进行考核；
- c) 录用后应签署相应的针对个人信息的保密协议；
- d) 应建立管理文档，说明录用人员应具备的条件（如学历、学位要求，技术人员应具备的专业技术水平，管理人员应具备的安全管理知识等）；
- e) 应记录录用人身份、背景和专业资格等，记录审查内容和审查结果等；
- f) 应记录录用人录用时的技能考核文档或记录，记录考核内容和考核结果等；
- g) 应签订保密协议，其中包括保密范围、保密责任、违约责任、协议的有效期限和责任人签字等内容。

4.4.2 管理人员的离岗

- a) 人员离岗时应办理调离手续，签署调离后个人信息保密义务的承诺书，防范内部员工、管理员因工作原因非法持有、披露和使用个人信息；
- b) 应对即将离岗人员具有控制方法，及时终止离岗人员的所有访问权限，取回其身份认证的配件，诸如身份证件、钥匙、徽章以及机构提供的软硬件设备；采用生理特征进行访问控制的，需要及时删除生理特征录入的相关信息；
- c) 应形成对离岗人员的安全处理记录(如交还身份证件、设备等的登记记录)；
- d) 应具有按照离职程序办理调离手续的记录。

4.4.3 管理人员的考核

- a) 应设立专人负责定期对接触个人信息数据工作的工作人员进行全面、严格的安全审查、意识考核和技能考核；
- b) 应按照考核周期形成考核文档，被考核人员应包括各个岗位的人员；
- c) 应对违反违背制定的安全策略和规定的人员进行惩戒；
- d) 应定期考查安全管理员、系统管理员和网络管理员其对工作相关的信息

安全基础知识、安全责任和惩戒措施、相关法律法规等的理解程度，并对考核记录进行记录存档。

4.4.4 管理人员的教育培训

a) 应制定培训计划并按计划对各岗位员工进行基本的安全意识教育培训和岗位技能培训；

b) 应制定安全教育和培训计划文档，明确培训方式、培训对象、培训内容、培训时间和地点等，培训内容包含信息安全基础知识、岗位操作规程等；

c) 应形成安全教育和培训记录，记录包含培训人员、培训内容、培训结果等。

4.4.5 外部人员访问

a) 应建立关于物理环境的外部人员访问的安全措施：

- 1) 制定外部人员允许访问的设备、区域和信息的规定；
- 2) 外部人员访问前需要提出书面申请并获得批准；
- 3) 外部人员访问被批准后应有专人全程陪同或监督，并进行全程监控录像；
- 4) 外部人员访问情况应登记备案。

b) 应建立关于网络通道的外部人员访问的安全措施：

- 1) 制定外部人员允许接入受控网络访问系统的规定；
- 2) 外部人员访问前需要提出书面申请并获得批准；
- 3) 外部人员访问时应进行身份认证；
- 4) 应根据外部访问人员的身份划分不同的访问权限和访问内容；
- 5) 应对外部访问人员的访问时间进行限制；
- 6) 对外部访问人员对个人信息的操作进行记录。

5 技术措施

5.1 基本要求

个人信息处理系统其安全技术措施应满足GB/T 22239相应等级的要求，按照网络安全等级保护制度的要求，履行安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改。

5.2 通用要求

5.2.1 通信网络安全

5.2.1.1 网络架构

a) 应为个人信息处理系统所处网络划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址；

b) 个人信息处理系统应作为重点区域部署，并设有边界防护措施。

5.2.1.2 通信传输

a) 应采用校验技术或密码技术保证通信过程中个人信息的完整性；

b) 应采用密码技术保证通信过程中个人信息字段或整个报文的保密性。

5.2.2 区域边界安全

5.2.2.1 边界防护

a) 应对跨越边界访问通信信息进行有效防护；

b) 应对非授权设备跨越边界行为进行检查或限制。

5.2.2.2 访问控制

应在个人信息处理系统边界根据访问控制策略设置访问控制规则。

5.2.2.3 入侵防范

应在个人信息处理系统边界部署入侵防护措施，检测、防止或限制从外部、内部发起的网络攻击行为。

5.2.2.4 恶意代码防范

应在个人信息处理系统的网络边界处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。

5.2.2.5 安全审计

a) 应在个人信息处理系统的网络边界、重要网络节点进行安全审计，审计应覆盖到每个用户、用户行为和安全事件；

b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功，以及个人信息范围、类型、操作方式、操作人、流转双方及其他与审计相关的信息；

c) 应对审计记录进行保护，定期备份并避免受到未预期的删除、修改或覆盖等；

d) 审计记录的留存时间应符合法律法规的要求；

e) 应能够对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析。

5.2.3 计算环境安全

5.2.3.1 身份鉴别

a) 应对登录个人信息处理系统的用户进行身份标识和鉴别，身份鉴别标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；

b) 个人信息处理系统应启用登录失败处理功能，采取诸如结束会话、限制非法登录次数和自动退出等措施；

c) 个人信息处理系统进行远程管理时，应采取措施防止身份鉴别信息在网络传输过程中被窃听；

d) 个人信息处理系统应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术

来实现，密码技术应符合国家密码主管部门规范。

5.2.3.2 访问控制

- a) 应对登录个人信息处理系统的用户分配账户和权限；
- b) 个人信息处理系统应重命名或删除默认账户，修改默认账户的默认口令；
- c) 个人信息处理系统应及时删除或停用多余的、过期的账户，避免共享账户的存在；
- d) 个人信息处理系统应进行角色划分，并授予管理用户所需的最小权限，实现管理用户的权限分离；
- e) 个人信息处理系统应由授权主体配置访问控制策略，访问控制策略应规定主体对客体的访问规则；
- f) 个人信息处理系统的访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级；
- g) 个人信息处理系统应对个人信息设置安全标记，并控制主体对有安全标记资源的访问。

5.2.3.3 安全审计

- a) 个人信息处理系统应启用安全审计功能，并且审计覆盖到每个用户，应对重要的用户行为和重要的安全事件进行审计；
- b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；
- c) 应对审计记录进行保护，进行定期备份并避免受到未预期的删除、修改或覆盖等；
- d) 审计记录的留存时间应符合法律法规的要求；
- e) 应对审计进程进行保护，防止未经授权的中断。

5.2.3.4 入侵防范

- a) 个人信息处理系统应遵循最小安装的原则, 只安装需要的组件和应用程序;
- b) 个人信息处理系统应关闭不需要的系统服务、默认共享和高危端口;
- c) 个人信息处理系统应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制;
- d) 个人信息处理系统应能够发现存在的已知漏洞, 并在经过充分测试评估后, 及时修补漏洞;
- e) 个人信息处理系统应能够检测到对重要节点的入侵行为并进行防御, 并在发生严重入侵事件时提供报警;

5.2.3.5 恶意代码防范和程序可信执行

应采取免受恶意代码攻击的技术措施或可信验证机制对系统程序、应用程序和重要配置文件/参数进行可信执行验证, 并在检测到其完整性受到破坏时采取恢复措施。

5.2.3.6 资源控制

- a) 应限制单个用户或进程对个人信息处理和存储设备系统资源的最大使用限度;
- b) 应提供重要节点设备的硬件冗余, 保证系统的可用性;
- c) 应对重要节点进行监视, 包括监视CPU、硬盘、内存等资源的使用情况;
- d) 应能够对重要节点的服务水平降低到预先规定的最小值进行检测和报警。

5.2.4 应用和数据安全

5.2.4.1 身份鉴别

- a) 个人信息处理系统应对登录的用户进行身份标识和鉴别, 该身份标识应具有唯一性, 鉴别信息应具有复杂度并要求定期更换;

b) 个人信息处理系统应提供并启用登录失败处理功能，并在多次登录后采取必要的保护措施；

c) 个人信息处理系统应强制用户首次登录时修改初始口令，当确定信息被泄露后，应提供提示全部用户强制修改密码的功能，在验证确认用户后修改密码；

d) 用户身份鉴别信息丢失或失效时，应采取技术措施保证鉴别信息重置过程的安全；

e) 应采取静态口令、动态口令、密码技术、生物技术等两种或两种以上的组合鉴别技术对用户进行身份鉴别，且其中一种鉴别技术使用密码技术来实现。

5.2.4.2 访问控制

a) 个人信息处理系统应提供访问控制功能，并对登录的用户分配账户和权限；

b) 应重命名或删除默认账户，修改默认账户的默认口令；

c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；

d) 应授予不同账户为完成各自承担任务所需的最小权限，在它们之间形成相互制约的关系；

e) 应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则；

f) 访问控制的粒度应达到主体为用户级，客体为文件、数据库表级、记录或字段级；

g) 个人信息应设置安全标记，控制主体对有安全标记资源的访问。

5.2.4.3 安全审计

a) 个人信息处理系统应提供安全审计功能，审计应覆盖到每个用户，应对重要的用户行为和重要的安全事件进行审计；

b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；

c) 应对审计记录进行保护，定期备份，并避免受到未预期的删除、修改或覆盖等；

d) 审计记录的留存时间应符合法律法规的要求；

e) 应对审计进程进行保护，防止未经授权的中断。

5.2.4.4 软件容错

a) 应提供个人信息的有效性校验功能，保证通过人机接口输入或通过通信接口输入的内容符合个人信息处理系统设定要求；

b) 应能够发现个人信息处理系统软件组件可能存在的已知漏洞，并能够在充分测试评估后及时修补漏洞；

c) 应能够在故障发生时，继续提供一部分功能，并能够实施必要的措施。

5.2.4.5 资源控制

a) 在通信双方中的一方在一段时间内未做任何响应时，另一方应能够自动结束会话；

b) 应对个人信息处理系统的最大并发会话连接数进行限制；

c) 应能够对单个用户的多重并发会话进行限制。

5.2.4.6 数据完整性

a) 应采取校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据和个人信息；

b) 应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据和个人信息。

5.2.4.7 数据保密性

a) 应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据和个人信息；

b) 应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据和个人信息。

5.2.4.8 数据备份恢复

a) 应提供个人信息的本地数据备份与恢复功能，定期对备份数据进行恢复测试，保证数据可用性；

b) 应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地；

c) 应提供重要数据处理系统的热冗余，保证系统的高可用性。

5.2.4.9 剩余信息保护

a) 应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除；

b) 应保证存有个人信息的存储空间被释放或重新分配前得到完全清除。

5.3 扩展要求

5.3.1 云计算安全扩展要求

a) 应确保个人信息在云计算平台中存储于中国境内，如需出境应遵循国家相关规定；

b) 应使用校验技术或密码技术保证虚拟机迁移过程中，个人信息的完整性，并在检测到完整性受到破坏时采取必要的恢复措施；

c) 应使用密码技术保证虚拟机迁移过程中，个人信息的保密性，防止在迁移过程中的个人信息泄露。

5.3.2 物联网安全扩展要求

物联网感知节点设备采集信息回传应采用密码技术保证通信过程中个人信息的保密性。

6 业务流程

6.1 收集

个人信息的收集行为应满足以下要求：

a) 个人信息收集前，应当遵循合法、正当、必要的原则向被收集的个人信息主体公开收集、使用规则，明示收集、使用信息的目的、方式和范围等信息；

b) 个人信息收集应获得个人信息主体的同意和授权，不应收集与其提供的服务无关的个人信息，不应通过捆绑产品或服务各项业务功能等方式强迫收集个人信息；

c) 个人信息收集应执行收集前签署的约定和协议，不应超范围收集；

d) 不应大规模收集或处理我国公民的种族、民族、政治观点、宗教信仰等敏感数据；

e) 个人生物识别信息应仅收集和使用摘要信息，避免收集其原始信息；

f) 应确保收集个人信息过程的安全性：

1) 收集个人信息之前，应有对被收集人进行身份认证的机制，该身份认证机制应具有相应安全性；

2) 收集个人信息时，信息在传输过程中应进行加密等保护处理；

3) 收集个人信息的系统应落实网络安全等级保护要求；

4) 收集个人信息时应有对收集内容进行安全检测和过滤的机制，防止非法内容提交。

6.2 保存

个人信息的保存行为应满足以下要求：

a) 在境内运营中收集和产生的个人信息应在境内存储，如需出境应遵循国家相关规定；

b) 收集到的个人信息应采取相应的安全加密存储等安全措施进行处理；

c) 应对保存的个人信息根据收集、使用目的、被收集人授权设置相应的保存时限;

d) 应对保存的个人信息在超出设置的时限后予以删除;

e) 保存信息的主要设备, 应对个人信息数据提供备份和恢复功能, 确保数据备份的频率和时间间隔, 并使用不少于以下一种备份手段:

1) 具有本地数据备份功能;

2) 将备份介质进行场外存放;

3) 具有异地数据备份功能。

6.3 应用

个人信息的应用应满足以下要求:

a) 对个人信息的应用, 应符合与个人信息主体签署的相关协议和规定, 不应超范围应用个人信息;

注: 经过处理无法识别特定个人且不能复原的个人信息数据, 可以超出与信息主体签署的相关使用协议和约定, 但应提供适当的保护措施进行保护。

b) 个人信息主体应拥有控制本人信息的权限, 包括:

1) 允许对本人信息的访问;

2) 允许通过适当方法对本人信息的修改或删除, 包括纠正不准确和不完整的数据, 并保证修改后的本人信息具备真实性和有效性;

c) 完全依靠自动化处理的画像技术应用于精准营销、搜索结果排序、个性化推送新闻、定向投放广告等增值应用, 可事先不经用户明确授权, 但应确保用户有反对或者拒绝的权利; 如应用于征信服务、行政司法决策等可能对用户带来法律后果的增值应用, 或跨网络运营者使用, 应经用户明确授权方可使用其数据;

d) 应对个人信息的接触者设置相应的访问控制措施, 包括:

1) 对被授权访问个人信息数据的工作人员按照最小授权的原则，只能访问最少够用的信息，只具有完成职责所需的最少数据操作权限；

2) 对个人信息的重要操作设置内部审批流程，如批量修改、拷贝、下载等；

3) 对特定人员超限制处理个人信息时配置相应的责任人或负责机构进行审批，并对这种行为进行记录。

e) 应对必须要通过界面（如显示屏幕、纸面）展示的个人信息进行去标识化的处理。

6.4 删除

a) 个人信息在超过保存时限之后应进行删除，经过处理无法识别特定个人且不能复原的除外；

b) 个人信息持有者如有违反法律、行政法规的规定或者双方的约定收集、使用其个人信息时，个人信息主体要求删除其个人信息的，应采取措施予以删除；

c) 个人信息相关存储设备，将存储的个人信息数据进行删除之后应采取措施防止通过技术手段恢复；

d) 对存储过个人信息的设备在进行新信息的存储时，应将之前的内容全部进行删除；

e) 废弃存储设备，应在进行删除后再进行处理。

6.5 第三方委托处理

a) 在对个人信息委托处理时，不应超出该信息主体授权同意的范围；

b) 在对个人信息的相关处理进行委托时，应对委托行为进行个人信息安全影响评估；

c) 对个人信息进行委托处理时，应签订相关协议要求受托方符合本文件；

d) 应向受托方进行对个人信息数据的使用和访问的授权；

e) 受托方对个人信息的相关数据进行处理完成之后，应对存储的个人信息数据的内容进行删除。

6.6 共享和转让

个人信息原则上不得共享、转让。如存在个人信息共享和转让行为时，应满足以下要求：

a) 共享和转让行为应经过合法性、必要性评估；

b) 在对个人信息进行共享和转让时应进行个人信息安全影响评估，应对受让方的数据安全能力进行评估确保受让方具备足够的数据安全能力，并按照评估结果采取有效的保护个人信息主体的措施；

c) 在共享、转让前应向个人信息主体告知转让该信息的目的、规模、公开范围数据接收方的类型等信息；

d) 在共享、转让前应得到个人信息主体的授权同意，与国家安全、国防安全、公共安全、公共卫生、重大公共利益或与犯罪侦查、起诉、审判和判决执行等直接相关的情形除外；

e) 应记录共享、转让信息内容，将共享、转让情况中包括共享、转让的日期、数据量、目的和数据接收方的基本情况在内的信息进行登记；

f) 在共享、转让后应了解接收方对个人信息的保存、使用情况和个人信息主体的权利，例如访问、更正、删除、注销等；

g) 当个人信息持有者发生收购、兼并、重组、破产等变更时，个人信息持有者应向个人信息主体告知有关情况，并继续履行原个人信息持有者的责任和义务，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。

6.7 公开披露

个人信息原则上不得公开披露。如经法律授权或具备合理事由确需公开披露时，应充分重视风险，遵守以下要求：

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, 与国家安全、国防安全、公共安全、公共卫生、重大公共利益或与犯罪侦查、起诉、审判和判决执行等直接相关的情形除外;

c) 公开披露个人敏感信息前, 除6.7 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) 准确记录和保存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) 不得公开披露个人生物识别信息和基因、疾病等个人生理信息;

g) 不得公开披露我国公民的种族、民族、政治观点、宗教信仰等敏感数据分析结果。

7 应急处置

7.1 应急机制和预案

a) 应建立健全网络安全风险评估和应急工作机制, 在个人信息处理过程中发生应急事件时具有上报有关主管部门的机制;

b) 应制定个人信息安全事件应急预案, 包括应急处理流程、事件上报流程等内容;

c) 应定期 (至少每半年一次) 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, 留存应急培训和应急演练记录;

d) 应定期对原有的应急预案重新评估, 修订完善。

7.2 处置和响应

a) 发现网络存在较大安全风险, 应采取措施, 进行整改, 消除隐患; 发生安

全事件时，应及时向公安机关报告，协助开展调查和取证工作，尽快消除隐患；

b) 发生个人信息安全事件后，应记录事件内容，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；

c) 应对安全事件造成的影响进行调查和评估，采取技术措施和其他必要措施，消除安全隐患，防止危害扩大；

d) 应按《国家网络安全事件应急预案》等相关规定及时上报安全事件，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；

e) 应将事件的情况告知受影响的个人信息主体，并及时向社会发布与公众有关的警示信息。

(三) 人口健康信息管理办法（试行）

第一条为规范人口健康信息的管理工作，促进人口健康信息的互联互通和共享利用，推动卫生计生事业科学发展，制定本办法。

第二条本办法适用于各级各类医疗卫生计生服务机构所涉及的人口健康信息的采集、管理、利用、安全和隐私保护工作。

第三条本办法所称人口健康信息，是指依据国家法律法规和工作职责，各级各类医疗卫生计生服务机构在服务和管理过程中产生的人口基本信息、医疗卫生服务信息等人口健康信息。

符合《中华人民共和国电子签名法》等有关法律法规规定的人口健康电子信息，与纸质文本具有同等法律效力。

第四条人口健康信息管理工作应当统筹规划、统一标准，属地管理、责权一致，保障安全、便民高效。

第五条县级以上人民政府卫生计生行政部门（含中医药行政部门，下同）是人口健康信息主管部门。国家卫生计生委负责制订全国人口健康信息发展规划和管理规范，统筹指导全国人口健康信息管理工作；县级以上地方人民政府卫生计生行政部门负责推进、指导、监督本行政区域人口健康信息管理工作。

各级各类医疗卫生计生服务机构（含中医药服务机构，下同）负责人口健康信息的采集、利用、管理、安全和隐私保护，是人口健康信息管理中的责任单位。

第六条责任单位采集、利用、管理人口健康信息应当按照法律法规的规定，遵循医学伦理原则，保证信息安全，保护个人隐私。

第七条责任单位应当根据本单位人口健康信息采集、利用和管理的情况，设立相应的人口健康信息管理部门和岗位职责，建立完善的人口健康信息质量控制管理制度，建立或利用相应的信息系统。严格执行相关标准和程序，做到标准统一、术语规范、内容准确。

第八条责任单位应当按照“一数一源、最少够用”的原则采集人口健康信息，所采集的信息应当符合业务应用和管理要求，保证服务和管理对象在本单位信息系统中身份标识的唯一性，基本数据项的一致性，所采集的信息应当严格实行信息复核程序，避免重复采集、多头采集。

第九条人口健康信息实行分级存储。责任单位按照国家统一规划，负责存储、管理工作中产生的人口健康信息，应当具备符合国家有关规定要求的数据存储、容灾备份和管理条件，建立可靠的人口健康信息容灾备份工作机制，定期进行备份和恢复检测，确保数据能够及时、完整、准确恢复，实现长期保存和历史数据的归档管理。

第十条责任单位应当结合服务和管理工作需要，及时更新与维护人口健康信息，确保信息处于最新、连续、有效状态。

不得将人口健康信息在境外的服务器中存储，不得托管、租赁在境外的服务器。

第十一条委托其他机构存储、运维人口健康信息的，委托单位承担人口健康信息的管理和安全管理责任。

受委托的存储、运维机构应当严格按照委托协议做好人口健康信息管理的技术支持，禁止超权限采集、开发和利用人口健康信息。

第十二条责任单位发生变更时，应当将所管理的人口健康信息完整、安全地移交给主管部门或承接延续其职能的机构管理，不得造成人口健康信息的损毁、丢失。

第十三条人口健康信息的利用实行分类管理，逐步实现互联互通。

人口健康信息的利用应当以提高医学研究、科学决策和便民服务水平为目的。

依法应当向社会公开的信息应当及时主动公开；涉及保密信息和个人隐私信息，不得对外提供。

第十四条责任单位应当建立人口健康信息综合利用工作制度，授权利用有关信息。

利用单位或者个人不得超出授权范围利用和发布人口健康信息。

第十五条责任单位应当为服务和管理对象提供其人口健康个案信息的查询和复制服务，并提供安全的信息查询和复制渠道。

第十六条责任单位应当做好人口健康信息安全和隐私保护工作，按照国家信息安全等级保护制度要求，加强建设人口健康信息相关系统安全保障体系，制定安全管理制度、操作规程和技术规范，保障人口健康信息安全。

利用单位和个人应当按照授权要求，做好所涉及的人口健康信息安全和隐私保护工作。

第十七条涉及国家秘密的人口健康信息系统应当按照国家涉密信息管理的要求进行分级保护，杜绝泄密。

第十八条责任单位应当建立痕迹管理制度，任何建立、修改和访问人口健康信息的用户，都应当通过严格的实名身份鉴别和授权控制，做到其行为可管理、可控制、可追溯。

第十九条人口健康信息相关系统的信息技术产品和服务提供者应当遵守国家有关信息安全审查制度，不得中断或者以其他方式中断合理的技术支持与服务，并应当为人口健康信息在不同系统间的迁移、交互、共享提供安全与便利条件。

第二十条卫生计生行政部门应当加强对本行政区域内各责任单位人口健康信息管理工作的日常监督检查，对本行政区域内各责任单位人口健康信息综合利用工作的指导监督，提高精细化人口健康服务和管理能力。

第二十一条卫生计生行政部门建立通报制度。相关单位和个人在人口健康信息利用、人口健康信息系统建设维护和技术支持等过程中，违反本办法规定造成

不良后果的，主管部门或责任单位应当对其予以通报；情节严重、违反国家法律法规的，依照国家有关法律法规追究其法律责任。

第二十二条卫生计生行政部门建立人口健康信息管理工作责任追究制度。对于违反本办法规定的主管部门和责任单位，上级主管部门应当视情节轻重予以督导整改、通报批评、提出给予行政处分的建议；构成犯罪的，依法追究刑事责任。

第二十三条本办法自印发之日起施行。

(四) 国家健康医疗大数据标准、安全和服务管理办法（试行）

（国卫规划发〔2018〕23号）

各省、自治区、直辖市及新疆生产建设兵团卫生计生委，委机关各司局，委直属和联系单位，国家中医药局：

为加强健康医疗大数据服务管理，促进“互联网+医疗健康”发展，充分发挥健康医疗大数据作为国家重要基础性战略资源的作用，根据相关法律法规，我委研究制定了《国家健康医疗大数据标准、安全和服务管理办法（试行）》（可从国家卫生健康委员会官网下载）。现印发你们，请遵照执行。

国家卫生健康委员会

2018年7月12日

第一章 总则

第一条 为加强健康医疗大数据服务管理，促进“互联网+医疗健康”发展，充分发挥健康医疗大数据作为国家重要基础性战略资源的作用，根据《中华人民共和国网络安全法》等法律法规和《国务院促进大数据发展行动纲要》《国务院办公厅关于促进和规范健康医疗大数据应用发展的指导意见》《国务院办公厅关于促进“互联网+医疗健康”发展的意见》等文件精神，就健康医疗大数据标准、安全和服务管理，制定本办法。

第二条 我国公民在中华人民共和国境内所产生的健康和医疗数据，国家在保障公民知情权、使用权和个人隐私的基础上，根据国家战略安全和人民群众生命安全需要，加以规范管理和开发利用。

第三条 坚持以人为本、创新驱动，规范有序、安全可控，开放融合、共建共享的原则，加强健康医疗大数据的标准管理、安全管理和 service 管理，推动健康医疗大数据惠民应用，促进健康医疗大数据产业发展。

第四条 本办法所称健康医疗大数据，是指在人们疾病防治、健康管理等过程中产生的与健康医疗相关的数据。

第五条 本办法适用于县级以上卫生健康行政部门（含中医药主管部门，下同）、各级各类医疗卫生机构、相关单位及个人所涉及的健康医疗大数据的管理。

第六条 国家卫生健康委员会（含国家中医药管理局，下同）会同相关部门负责统筹规划、指导、评估、监督全国健康医疗大数据的标准管理、安全管理和 service 管理工作。县级以上卫生健康行政部门会同相关部门负责本行政区域内健康医疗大数据管理工作，是本行政区域内健康医疗大数据安全和应用管理的监管单位。

各级各类医疗卫生机构和相关企事业单位是健康医疗大数据安全和应用管理的责任单位。

第二章 标准管理

第七条 健康医疗大数据标准管理工作遵循政策引领、强化监督、分类指导、分级管理的原则。

第八条 国家卫生健康委员会负责统筹规划、组织制定全国健康医疗大数据标准，监督指导评估标准的应用工作，在已有的基础性通用性大数据标准基础上组织制定健康医疗大数据标准体系规划，负责制定、组织实施年度健康医疗大数据标准工作计划。省级卫生健康行政部门（含省级中医药主管部门）负责监督指导评估本地区健康医疗大数据标准的应用工作，依据国家健康医疗大数据标准体系规划，结合本地实际，负责指导和监督健康医疗大数据标准体系在本省域内落地执行。

第九条 国家卫生健康委员会鼓励医疗卫生机构、科研教育单位、相关企业或行业协会、社会团体等参与健康医疗大数据标准制定工作。公民、法人或者其他组织可提出制修订健康医疗大数据标准的立项建议，并提交相应标准项目建议书。

第十条 国家卫生健康委员会负责统一组织实施，择优确定健康医疗大数据

标准起草单位和负责人，提倡多方参与协作机制，由各相关单位组成协作组参与标准起草工作。

第十一条 健康医疗大数据标准起草、审查及发布的程序和要求，按照国家和行业有关规定执行。

第十二条 卫生健康行政部门应当对健康医疗大数据标准的实施加强引导和监督，充分发挥各级各类医疗卫生机构、相关企业等市场主体在标准应用实施中的积极性和主动性，建立激励和促进标准应用实施的长效管理机制。

第十三条 卫生健康行政部门应当建立相应的健康医疗大数据标准化产品生产和采购的激励约束机制，卫生健康行政部门要积极推进健康医疗大数据标准规范和测评工作，并将测评结果与医疗卫生机构评审评价挂钩。

第十四条 国家卫生健康委员会加强健康医疗大数据技术产品和服务模式的标准体系及制度建设，组织对健康医疗大数据标准应用效果评估工作，并根据评估情况，对相关标准进行组织修订或废止等。

第十五条 国家卫生健康委员会基于卫生标准管理平台，动态管理健康医疗大数据标准的开发与应用，对各级各类医疗卫生机构和企事业单位的标准应用情况进行动态监测。

第三章 安全管理

第十六条 健康医疗大数据安全管理是指在数据采集、存储、挖掘、应用、运营、传输等多个环节中的安全和管理，包括国家战略安全、群众生命安全、个人信息安全的权责管理工作。

第十七条 责任单位应当建立健全相关安全管理制度、操作规程和技术规范，落实“一把手”责任制，加强安全保障体系建设，强化统筹管理和协调监督，保障健康医疗大数据安全。

涉及国家秘密的健康医疗大数据的安全、管理和使用等，按照国家有关保密规定执行。责任单位应当建立健全涉及国家秘密的健康医疗大数据管理与使用制

度，对制作、审核、登记、拷贝、传输、销毁等环节进行严格管理。

第十八条 责任单位应当采取数据分类、重要数据备份、加密认证等措施保障健康医疗大数据安全。责任单位应当建立可靠的数据容灾备份工作机制，定期进行备份和恢复检测，确保数据能够及时、完整、准确恢复，实现长期保存和历史数据的归档管理。

第十九条 责任单位应当按照国家网络安全等级保护制度要求，构建可信的网络安全环境，加强健康医疗大数据相关系统安全保障体系建设，提升关键信息基础设施和重要信息系统的安全防护能力，确保健康医疗大数据关键信息基础设施和核心系统安全可控。健康医疗大数据中心、相关信息系统等均应开展定级、备案、测评等工作。

第二十条 健康医疗大数据相关系统的产品和服务提供者应当遵守国家有关网络安全审查制度，不得中断或者变相中断合理的技术支持与服务，并应当为健康医疗大数据在不同系统间的交互、共享和运营提供安全与便利条件。

第二十一条 责任单位应当依法依规使用健康医疗大数据有关信息，提供安全的信息查询和复制渠道，确保公民隐私保护和数据安全。

第二十二条 责任单位应当按照《中华人民共和国网络安全法》的要求，严格规范不同等级用户的数据接入和使用权限，并确保数据在授权范围内使用。任何单位和个人不得擅自利用和发布未经授权或超出授权范围的健康医疗大数据，不得使用非法手段获取数据。

第二十三条 责任单位应当建立严格的电子实名认证和数据访问控制，规范数据接入、使用 and 销毁过程的痕迹管理，确保健康医疗大数据访问行为可管、可控及服务管理全程留痕，可查询、可追溯，对任何数据泄密泄露事故及风险可追溯到相关责任单位和责任人。

第二十四条 建立健全健康医疗大数据安全管理人才培养机制，确保相关从业人员具备健康医疗大数据安全管理所要求的知识和技能。

第二十五条 责任单位应当建立健康医疗大数据安全监测和预警系统，建立

网络安全通报和应急处置联动机制，开展数据安全规范和技术规范的研究工作，不断丰富网络安全相关的标准规范体系，重点防范数据资源的集聚性风险和新技术应用的潜在性风险。发生网络安全重大事件，应当按照相关法律法规和有关要求进行报告并处置。

第四章 服务管理

第二十六条 国家卫生健康委员会负责制定健康医疗大数据应用领域相关规范、标准，建立健康医疗大数据应用诚信机制和退出机制，制定健康医疗大数据挖掘、应用的安全和管理规范。

第二十七条 责任单位实施健康医疗大数据管理和服务，应当按照法律法规和相关文件规定，遵循医学伦理原则，保护个人隐私。

第二十八条 责任单位应当根据本单位健康医疗大数据管理的需求，明确相应的管理部门和岗位，按照国家授权，实行“统一分级授权、分类应用管理、权责一致”的管理制度，并建设相应的健康医疗大数据信息系统作为技术和管理支撑。

第二十九条 责任单位采集健康医疗大数据，应当严格执行国家和行业相关标准和程序，符合业务应用技术标准和管理规范，做到标准统一、术语规范、内容准确，保证服务和管理对象在本单位信息系统中身份标识唯一、基本数据项一致，所采集的信息应当严格实行信息复核终审程序，做好数据质量管理。

第三十条 责任单位应当具备符合国家有关规定要求的数据存储、容灾备份和安全管理条件，加强对健康医疗大数据的存储管理。健康医疗大数据应当存储在境内安全可信的服务器上，因业务需要确需向境外提供的，应当按照相关法律法规及有关要求进行安全评估审核。

第三十一条 责任单位选择健康医疗大数据服务提供商时，应当确保其符合国家和行业规定及要求，具备履行相关法规制度、落实相关标准、确保数据安全的能力，建立数据安全、个人隐私保护、应急响应管理等方面管理制度。

第三十二条 责任单位委托有关机构存储、运营健康医疗大数据，委托单位

与受托单位共同承担健康医疗大数据的管理和安全责任。受托单位应当严格按照相关法律法规和委托协议做好健康医疗大数据的存储、管理与运营工作。

第三十三条 责任单位应当结合服务和管理工作需要，及时更新、甄别、优化和维护健康医疗大数据，确保信息处于最新、连续、有效、优质和安全状态。

第三十四条 责任单位发生变更时，应当将所管理的健康医疗大数据完整、安全地移交给承接延续其职能的机构或本行政区域内的卫生健康行政部门，不得造成健康医疗大数据的损毁、丢失和泄露。

第三十五条 责任单位向社会公开健康医疗大数据时，应当遵循国家有关规定，不得泄露国家秘密、商业秘密和个人隐私，不得侵害国家利益、社会公共利益和公民、法人及其他组织的合法权益。

第三十六条 责任单位应当加强健康医疗大数据的使用和服务，创造条件规范使用健康医疗大数据，推动部分健康医疗大数据在线查询。

第三十七条 国家卫生健康委员会负责按照国家信息资源开放共享有关规定，建立健康医疗大数据开放共享的工作机制，加强健康医疗大数据的共享和交换，统筹建设健康医疗大数据上报系统平台、信息资源目录体系和共享交换体系。

第五章 管理监督

第三十八条 卫生健康行政部门应当加强监督管理，对本行政区域内各责任单位健康医疗大数据安全管理工作开展日常检查，指导监督本行政区域内各责任单位数据综合利用工作，提高数据服务质量和确保安全。各级各类医疗卫生机构应当接入相应区域全民健康信息平台，传输和备份医疗健康服务产生的数据，并向卫生健康行政部门开放监管端口。

第三十九条 卫生健康行政部门应当加强监测评估，定期开展健康医疗大数据平台和服务商的稳定和安全测评及健康医疗大数据应用的安全监测评估，建立网络安全防护、系统互联共享、公民隐私保护等软件评价和安全审查保密制度。

第四十条 卫生健康行政部门会同相关部门建立健康医疗大数据安全管理

工作责任追究制度。对于违反本办法规定的单位和个人，由主管部门视情节轻重予以约谈、督导整改、诫勉、通报批评、处分或提出给予处分的建议；构成违法的，移送司法部门依法追究法律责任。

第六章 附则

第四十一条 本办法自印发之日起施行。

(五) 国家网络空间安全战略

(2016年12月27日，国家互联网信息办公室发布)

信息技术广泛应用和网络空间兴起发展，极大促进了经济社会繁荣进步，同时也带来了新的安全风险和挑战。网络空间安全（以下称网络安全）事关人类共同利益，事关世界和平与发展，事关各国国家安全。维护我国网络安全是协调推进全面建成小康社会、全面深化改革、全面依法治国、全面从严治党战略布局的重要举措，是实现“两个一百年”奋斗目标、实现中华民族伟大复兴中国梦的重要保障。为贯彻落实习近平主席关于推进全球互联网治理体系变革的“四项原则”和构建网络空间命运共同体的“五点主张”，阐明中国关于网络空间发展和安全的重大立场，指导中国网络安全工作，维护国家在网络空间的主权、安全、发展利益，制定本战略。

一、机遇和挑战

(一) 重大机遇

伴随信息革命的飞速发展，互联网、通信网、计算机系统、自动化控制系统、数字设备及其承载的应用、服务和数据等组成的网络空间，正在全面改变人们的生产生活方式，深刻影响人类社会历史发展进程。

信息传播的新渠道。网络技术的发展，突破了时空限制，拓展了传播范围，创新了传播手段，引发了传播格局的根本性变革。网络已成为人们获取信息、学习交流的新渠道，成为人类知识传播的新载体。

生产生活的新空间。当今世界，网络深度融入人们的学习、生活、工作等方面，网络教育、创业、医疗、购物、金融等日益普及，越来越多的人通过网络交流思想、成就事业、实现梦想。

经济发展的新引擎。互联网日益成为创新驱动发展的先导力量，信息技术在国民经济各行业广泛应用，推动传统产业改造升级，催生了新技术、新业态、新产业、新模式，促进了经济结构调整和经济发展方式转变，为经济社会发展注入

了新的动力。

文化繁荣的新载体。网络促进了文化交流和知识普及，释放了文化发展活力，推动了文化创新创造，丰富了人们精神文化生活，已经成为传播文化的新途径、提供公共文化服务的新手段。网络文化已成为文化建设的重要组成部分。

社会治理的新平台。网络在推进国家治理体系和治理能力现代化方面的作用日益凸显，电子政务应用走向深入，政府信息公开共享，推动了政府决策科学化、民主化、法治化，畅通了公民参与社会治理的渠道，成为保障公民知情权、参与权、表达权、监督权的重要途径。

交流合作的新纽带。信息化与全球化交织发展，促进了信息、资金、技术、人才等要素的全球流动，增进了不同文明交流融合。网络让世界变成了地球村，国际社会越来越成为你中有我、我中有你的命运共同体。

国家主权的新疆域。网络空间已经成为与陆地、海洋、天空、太空同等重要的人类活动新领域，国家主权拓展延伸到网络空间，网络空间主权成为国家主权的重要组成部分。尊重网络空间主权，维护网络安全，谋求共治，实现共赢，正在成为国际社会共识。

（二）严峻挑战

网络安全形势日益严峻，国家政治、经济、文化、社会、国防安全及公民在网络空间的合法权益面临严峻风险与挑战。

网络渗透危害政治安全。政治稳定是国家发展、人民幸福的基本前提。利用网络干涉他国内政、攻击他国政治制度、煽动社会动乱、颠覆他国政权，以及大规模网络监控、网络窃密等活动严重危害国家政治安全和用户信息安全。

网络攻击威胁经济安全。网络和信息系統已经成为关键基础设施乃至整个经济社会的神经中枢，遭受攻击破坏、发生重大安全事件，将导致能源、交通、通信、金融等基础设施瘫痪，造成灾难性后果，严重危害国家经济安全和公共利益。

网络有害信息侵蚀文化安全。网络上各种思想文化相互激荡、交锋，优秀传

统文化和主流价值观面临冲击。网络谣言、颓废文化和淫秽、暴力、迷信等违背社会主义核心价值观的有害信息侵蚀青少年身心健康，败坏社会风气，误导价值取向，危害文化安全。网上道德失范、诚信缺失现象频发，网络文明程度亟待提高。

网络恐怖和违法犯罪破坏社会安全。恐怖主义、分裂主义、极端主义等势力利用网络煽动、策划、组织和实施暴力恐怖活动，直接威胁人民生命财产安全、社会秩序。计算机病毒、木马等在网络空间传播蔓延，网络欺诈、黑客攻击、侵犯知识产权、滥用个人信息等不法行为大量存在，一些组织肆意窃取用户信息、交易数据、位置信息以及企业商业秘密，严重损害国家、企业和个人利益，影响社会和谐稳定。

网络空间的国际竞争方兴未艾。国际上争夺和控制网络空间战略资源、抢占规则制定权和战略制高点、谋求战略主动权的竞争日趋激烈。个别国家强化网络威慑战略，加剧网络空间军备竞赛，世界和平受到新的挑战。

网络空间机遇和挑战并存，机遇大于挑战。必须坚持积极利用、科学发展、依法管理、确保安全，坚决维护网络安全，最大限度利用网络空间发展潜力，更好惠及13亿多中国人民，造福全人类，坚定维护世界和平。

二、目标

以总体国家安全观为指导，贯彻落实创新、协调、绿色、开放、共享的发展理念，增强风险意识和危机意识，统筹国内国际两个大局，统筹发展安全两件大事，积极防御、有效应对，推进网络空间和平、安全、开放、合作、有序，维护国家主权、安全、发展利益，实现建设网络强国的战略目标。

和平：信息技术滥用得到有效遏制，网络空间军备竞赛等威胁国际和平的活动得到有效控制，网络空间冲突得到有效防范。

安全：网络安全风险得到有效控制，国家网络安全保障体系健全完善，核心技术装备安全可控，网络和信息运行稳定可靠。网络安全人才满足需求，全社会的网络安全意识、基本防护技能和利用网络的信心大幅提升。

开放：信息技术标准、政策和市场开放、透明，产品流通和信息传播更加顺畅，数字鸿沟日益弥合。不分大小、强弱、贫富，世界各国特别是发展中国家都能分享发展机遇、共享发展成果、公平参与网络空间治理。

合作：世界各国在技术交流、打击网络恐怖和网络犯罪等领域的合作更加密切，多边、民主、透明的国际互联网治理体系健全完善，以合作共赢为核心的网络空间命运共同体逐步形成。

有序：公众在网络空间的知情权、参与权、表达权、监督权等合法权益得到充分保障，网络空间个人隐私获得有效保护，人权受到充分尊重。网络空间的国内和国际法律体系、标准规范逐步建立，网络空间实现依法有效治理，网络环境诚信、文明、健康，信息自由流动与维护国家安全、公共利益实现有机统一。

三、原则

一个安全稳定繁荣的网络空间，对各国乃至世界都具有重大意义。中国愿与各国一道，加强沟通、扩大共识、深化合作，积极推进全球互联网治理体系变革，共同维护网络空间和平安全。

（一）尊重维护网络空间主权

网络空间主权不容侵犯，尊重各国自主选择发展道路、网络管理模式、互联网公共政策和平等参与国际网络空间治理的权利。各国主权范围内的网络事务由各国人民自己做主，各国有权根据本国国情，借鉴国际经验，制定有关网络空间的法律法规，依法采取必要措施，管理本国信息系统及本国疆域上的网络活动；保护本国信息系统和信息资源免受侵入、干扰、攻击和破坏，保障公民在网络空间的合法权益；防范、阻止和惩治危害国家安全和利益的有害信息在本国网络传播，维护网络空间秩序。任何国家都不搞网络霸权、不搞双重标准，不利用网络干涉他国内政，不从事、纵容或支持危害他国国家安全的网络活动。

（二）和平利用网络空间

和平利用网络空间符合人类的共同利益。各国应遵守《联合国宪章》关于不得使用或威胁使用武力的原则，防止信息技术被用于与维护国际安全与稳定相悖

的目的，共同抵制网络空间军备竞赛、防范网络空间冲突。坚持相互尊重、平等相待，求同存异、包容互信，尊重彼此在网络空间的安全利益和重大关切，推动构建和谐网络世界。反对以国家安全为借口，利用技术优势控制他国网络和信息系统、收集和窃取他国数据，更不能以牺牲别国安全谋求自身所谓绝对安全。

（三）依法治理网络空间

全面推进网络空间法治化，坚持依法治网、依法办网、依法上网，让互联网在法治轨道上健康运行。依法构建良好网络秩序，保护网络空间信息依法有序自由流动，保护个人隐私，保护知识产权。任何组织和个人在网络空间享有自由、行使权利的同时，须遵守法律，尊重他人权利，对自己在网络上的言行负责。

（四）统筹网络安全与发展

没有网络安全就没有国家安全，没有信息化就没有现代化。网络安全和信息化是一体之两翼、驱动之双轮。正确处理发展和安全的关系，坚持以安全保发展，以发展促安全。安全是发展的前提，任何以牺牲安全为代价的发展都难以持续。发展是安全的基础，不发展是最大的不安全。没有信息化发展，网络安全也没有保障，已有的安全甚至会丧失。

四、战略任务

中国的网民数量和网络规模世界第一，维护好中国网络安全，不仅是自身需要，对于维护全球网络安全乃至世界和平都具有重大意义。中国致力于维护国家网络空间主权、安全、发展利益，推动互联网造福人类，推动网络空间和平利用和共同治理。

（一）坚定捍卫网络空间主权

根据宪法和法律法规管理我国主权范围内的网络活动，保护我国信息设施和信息资源安全，采取包括经济、行政、科技、法律、外交、军事等一切措施，坚定不移地维护我国网络空间主权。坚决反对通过网络颠覆我国国家政权、破坏我国国家主权的一切行为。

（二）坚决维护国家安全

防范、制止和依法惩治任何利用网络进行叛国、分裂国家、煽动叛乱、颠覆或者煽动颠覆人民民主专政政权的行为；防范、制止和依法惩治利用网络进行窃取、泄露国家秘密等危害国家安全的行为；防范、制止和依法惩治境外势力利用网络进行渗透、破坏、颠覆、分裂活动。

（三）保护关键信息基础设施

国家关键信息基础设施是指关系国家安全、国计民生，一旦数据泄露、遭到破坏或者丧失功能可能严重危害国家安全、公共利益的信息设施，包括但不限于提供公共通信、广播电视传输等服务的基础信息网络，能源、金融、交通、教育、科研、水利、工业制造、医疗卫生、社会保障、公用事业等领域和国家机关的重要信息系统，重要互联网应用系统等。采取一切必要措施保护关键信息基础设施及其重要数据不受攻击破坏。坚持技术和管理并重、保护和震慑并举，着眼识别、防护、检测、预警、响应、处置等环节，建立实施关键信息基础设施保护制度，从管理、技术、人才、资金等方面加大投入，依法综合施策，切实加强关键信息基础设施安全防护。

关键信息基础设施保护是政府、企业和全社会的共同责任，主管、运营单位和组织要按照法律法规、制度标准的要求，采取必要措施保障关键信息基础设施安全，逐步实现先评估后使用。加强关键信息基础设施风险评估。加强党政机关以及重点领域网站的安全防护，基层党政机关网站要按集约化模式建设运行和管理。建立政府、行业与企业的网络安全信息有序共享机制，充分发挥企业在保护关键信息基础设施中的重要作用。

坚持对外开放，立足开放环境下维护网络安全。建立实施网络安全审查制度，加强供应链安全管理，对党政机关、重点行业采购使用的重要信息技术产品和服务开展安全审查，提高产品和服务的安全性和可控性，防止产品服务提供者和其他组织利用信息技术优势实施不正当竞争或损害用户利益。

（四）加强网络文化建设

加强网上思想文化阵地建设，大力培育和践行社会主义核心价值观，实施网络内容建设工程，发展积极向上的网络文化，传播正能量，凝聚强大精神力量，营造良好网络氛围。鼓励拓展新业务、创作新产品，打造体现时代精神的网络文化品牌，不断提高网络文化产业规模水平。实施中华优秀传统文化网上传播工程，积极推动优秀传统文化和当代文化精品的数字化、网络化制作和传播。发挥互联网传播平台优势，推动中外优秀文化交流互鉴，让各国人民了解中华优秀传统文化，让中国人民了解各国优秀文化，共同推动网络文化繁荣发展，丰富人们精神世界，促进人类文明进步。

加强网络伦理、网络文明建设，发挥道德教化引导作用，用人类文明优秀成果滋养网络空间、修复网络生态。建设文明诚信的网络环境，倡导文明办网、文明上网，形成安全、文明、有序的信息传播秩序。坚决打击谣言、淫秽、暴力、迷信、邪教等违法有害信息在网络空间传播蔓延。提高青少年网络文明素养，加强对未成年人上网保护，通过政府、社会组织、社区、学校、家庭等方面的共同努力，为青少年健康成长创造良好的网络环境。

（五）打击网络恐怖和违法犯罪

加强网络反恐、反间谍、反窃密能力建设，严厉打击网络恐怖和网络间谍活动。

坚持综合治理、源头控制、依法防范，严厉打击网络诈骗、网络盗窃、贩枪贩毒、侵害公民个人信息、传播淫秽色情、黑客攻击、侵犯知识产权等违法犯罪行为。

（六）完善网络治理体系

坚持依法、公开、透明管网治网，切实做到有法可依、有法必依、执法必严、违法必究。健全网络安全法律法规体系，制定出台网络安全法、未成年人网络保护条例等法律法规，明确社会各方面的责任和义务，明确网络安全管理要求。加快对现行法律的修订和解释，使之适用于网络空间。完善网络安全相关制度，建立网络信任体系，提高网络安全管理的科学化规范化水平。

加快构建法律规范、行政监管、行业自律、技术保障、公众监督、社会教育相结合的网络治理体系，推进网络社会组织管理创新，健全基础管理、内容管理、行业管理以及网络违法犯罪防范和打击等工作联动机制。加强网络空间通信秘密、言论自由、商业秘密，以及名誉权、财产权等合法权益的保护。

鼓励社会组织等参与网络治理，发展网络公益事业，加强新型网络社会组织建设。鼓励网民举报网络违法行为和不良信息。

（七）夯实网络安全基础

坚持创新驱动发展，积极创造有利于技术创新的政策环境，统筹资源和力量，以企业为主体，产学研用相结合，协同攻关、以点带面、整体推进，尽快在核心技术上取得突破。重视软件安全，加快安全可信产品推广应用。发展网络基础设施，丰富网络空间信息内容。实施“互联网+”行动，大力发展网络经济。实施国家大数据战略，建立大数据安全管理制度，支持大数据、云计算等新一代信息技术创新和应用。优化市场环境，鼓励网络安全企业做大做强，为保障国家网络安全夯实产业基础。

建立完善国家网络安全技术支撑体系。加强网络安全基础理论和重大问题研究。加强网络安全标准化和认证认可工作，更多地利用标准规范网络空间行为。做好等级保护、风险评估、漏洞发现等基础性工作，完善网络安全监测预警和网络安全重大事件应急处置机制。

实施网络安全人才工程，加强网络安全学科专业建设，打造一流网络安全学院和创新园区，形成有利于人才培养和创新创业的生态环境。办好网络安全宣传周活动，大力开展全民网络安全宣传教育。推动网络安全教育进教材、进学校、进课堂，提高网络媒介素养，增强全社会网络安全意识和防护技能，提高广大网民对网络违法有害信息、网络欺诈等违法犯罪活动的辨识和抵御能力。

（八）提升网络空间防护能力

网络空间是国家主权的新疆域。建设与我国国际地位相称、与网络强国相适应的网络空间防护力量，大力发展网络安全防御手段，及时发现和抵御网络入侵，

铸造维护国家网络安全的坚强后盾。

(九) 强化网络空间国际合作

在相互尊重、相互信任的基础上，加强国际网络空间对话合作，推动互联网全球治理体系变革。深化同各国的双边、多边网络安全对话交流和信息沟通，有效管控分歧，积极参与全球和区域组织网络安全合作，推动互联网地址、根域名服务器等基础资源管理国际化。

支持联合国发挥主导作用，推动制定各方普遍接受的网络空间国际规则、网络空间国际反恐公约，健全打击网络犯罪司法协助机制，深化在政策法律、技术创新、标准规范、应急响应、关键信息基础设施保护等领域的国际合作。

加强对发展中国家和落后地区互联网技术普及和基础设施建设的支持援助，努力弥合数字鸿沟。推动“一带一路”建设，提高国际通信互联互通水平，畅通信息丝绸之路。搭建世界互联网大会等全球互联网共享共治平台，共同推动互联网健康发展。通过积极有效的国际合作，建立多边、民主、透明的国际互联网治理体系，共同构建和平、安全、开放、合作、有序的网络空间。

(六) 国土资源部关于印发促进国土资源大数据应用发展实施意见的通知

(国土资发[2016]72号)

各省、自治区、直辖市国土资源主管部门，新疆生产建设兵团国土资源局，解放军土地管理局，各派驻地方的国家土地督察局，中国地质调查局及部其他直属单位，部机关各司局：

为贯彻落实《国务院关于印发促进大数据发展行动纲要的通知》(国发〔2015〕50号)精神，积极推动国土资源大数据应用发展工作，部研究制定了《关于促进国土资源大数据应用发展的实施意见》。现印发给你们，请遵照执行。

2016年7月4日

为深入贯彻落实《国务院关于印发促进大数据发展行动纲要的通知》(国发〔2015〕50号)精神，促进国土资源大数据应用发展，提升国土资源治理能力，制定本实施意见。

一、发展形势

(一) 充分认识实施国家大数据战略的重大意义。当代信息技术与经济社会的交汇融合引发了数据迅猛增长，数据已成为国家基础性战略资源。党的十八届五中全会明确提出实施国家大数据战略，《国民经济和社会发展第十三个五年规划纲要》将实施国家大数据战略作为“十三五”时期坚持创新驱动发展、培育发展新动力、拓展发展新空间的重要抓手。我国正面临从“数据大国”向“数据强国”转变的历史新机遇，充分利用数据规模优势，实现数据规模、质量和应用水平同步提升，挖掘和释放数据资源的潜在价值，有利于充分发挥数据资源战略性作用，有效提升国家竞争力。将大数据引入政府治理，推进政府数据共享开放，加强大数据分析与挖掘，建立“用数据说话、用数据决策、用数据管理、用数据创新”的管理机制，将有力促进政府从“依靠经验”的定性管理方式迈向“数据驱动”的精准治理方式。大数据发展已成为促进国家治理体系和治理能力现代化

的有效途径。

(二) 国土资源大数据是实施国家大数据战略的重要内容。国土资源数据作为基础国情信息，在国民经济和社会发展中发挥着极为重要的作用。通过国土资源调查、监测、评价和管理工作的，产生和积累了海量的基础地理、土地、地质矿产、地质环境与地质灾害防治和海洋等数据，这些数据对于各级政府部门的规划、调控、监管和社会各界开展与空间和资源相关的活动，以及满足人民群众对国土资源信息日益增长的需求具有重要的价值。推进国土资源数据共享开放，有利于促进自然资源的协调、统一管理，提升国家自然资源综合管理效能；有利于资源产权的管理与保护，促进形成公平普惠、便捷高效的民生服务体系；有利于更为准确地分析和预测经济运行状况，增强政府决策和宏观调控的针对性和时效性。国土资源大数据已成为实施国家大数据战略的重要组成部分。

(三) 国土资源大数据应用发展是新时期国土资源事业发展的迫切需要。“十三五”时期是全面建成小康社会决胜阶段。部党组提出，要把创新、协调、绿色、开放、共享的新发展理念贯彻落实到国土资源工作中，以创新理念增强国土资源事业发展新动力，以协调理念构建国土资源保护开发新格局，以绿色理念开辟国土资源永续利用新途径，以开放理念拓展国土资源合作发展新空间，以共享理念实现国土资源惠民利民新成效。做好新时期国土资源工作，迫切需要抓住实施国家大数据战略的机遇，充分利用国土资源行业密集型数据规模的优势，以国土资源数据、相关经济社会发展数据和网络数据为基础，通过数据共享开放以及对大数据的分析、挖掘与应用，创新国土资源管理方式，促进国土资源决策科学化、监管精准化、服务便利化，有效提升国土资源的管理与服务水平。

(四) 发展国土资源大数据面临着重大机遇和挑战。在部党组领导下，各级国土资源主管部门通过开展国土资源数据库的建设与应用，不断积累和丰富了海量的数据资源，基本建成全国国土资源“一张图”数据库，为提升国土资源管理与服务水平发挥了重要作用。云计算、大数据、移动互联网、物联网、数据分析挖掘等新一代信息技术的迅猛发展及其在国土资源领域的逐步推广应用，为发展国土资源大数据创造了良好的数据基础和技术条件。然而，国土资源大数据的应

用发展仍处于初级阶段，与实施国家大数据战略要求和国土资源事业发展新需求相比还存在较大差距，国土资源数据的完整性和及时性有待提高，数据共享、开放和服务还明显不足，基于数据的决策支持能力还不强，发展国土资源大数据面临着严峻的形势和挑战。抓住机遇，迎接挑战，更新发展理念，创新发展方式，着力推进国土资源大数据应用发展，已成为新时期国土资源事业发展的重要途径。

二、指导思想、基本原则和发展目标

（一）指导思想。

全面贯彻落实党的十八大和十八届三中、四中、五中全会精神及习近平总书记系列重要讲话精神，以创新、协调、绿色、开放、共享的新发展理念为指引，按照实施国家大数据战略部署，围绕“十三五”期间国土资源中心工作和主要任务，加强顶层设计和统筹协调，充分发挥国土资源大数据在国民经济和社会发展中的重要作用，大力推动大数据在国土资源工作中的创新应用，通过基于数据的科学管理、决策与服务，促进国土资源治理能力现代化。

（二）基本原则。

坚持统筹建设，共同发展。以实施国家大数据战略和国土资源管理需求为导向，加强各级国土资源主管部门数据统筹建设。坚持统一标准、统一平台，共同发展，充分发挥各数据支撑单位的特长与优势，共同推动国土资源大数据应用发展。

坚持共享开放，确保安全。建立科学规范的数据共享开放机制，大力推动国土资源数据在系统内及政府部门间的共享，稳步有序推进国土资源数据向社会开放。构建安全、规范的大数据应用发展环境，妥善处理数据开放与安全的关系，切实保障数据安全。

坚持创新发展，强化应用。充分应用云计算、互联网、大数据等现代信息技术，加大大数据应用力度，全面落实国土资源改革发展要求。以应用创新为动力，促进数据管理机制与应用模式的创新，提升数据开发利用水平，提高数据应用服

务效益。

坚持政府主导，社会参与。强化国土资源主管部门主导作用，积极探索政府推动、社会参与的大数据发展模式。充分调动市场、行业等社会力量的广泛参与，形成合力，逐步建立和营造国土资源大数据发展的良好氛围，提高大数据应用深度和广度。

（三）发展目标。

按照实施国家大数据战略的要求，立足国土资源工作发展的需要，健全国土资源数据资源体系，实现国土资源数据的充分共享和适度开放，深化国土资源大数据的创新应用，不断提高国土资源参与宏观调控、市场监管、社会治理和公共服务的精准性和有效性，促进国土资源大数据应用新业态发展，形成国土资源大数据应用发展新格局。

构建统一的国土资源数据资源体系。梳理各类国土资源数据，形成数据资源目录。汇聚整合土地、不动产、地质矿产、地质环境与地质灾害防治等各类数据，建立完善并形成内容全面、标准统一的国土资源数据资源体系，全面提升国土资源数据支撑能力。

建立国土资源数据共享开放新机制。构建统一的国土资源数据共享平台和开放平台，建立充分共享、适度开放、安全可靠的国土资源数据共享开放新机制，形成国土资源数据在系统内和政府部门间充分共享和向社会有序开放的新局面。

打造国土资源管理决策服务新模式。创新和深化大数据在国土资源形势分析、决策支持和信息服务中的应用，构建决策支持系统、智库信息化工作平台，加强国土资源信息服务，建立“用数据说话、用数据决策”的管理决策服务新模式。

培育智能化国土资源调查评价监测应用新业态。推进国土资源调查评价监测技术研发，培育智能地质调查、智慧探矿、土地智能监测等应用新业态，鼓励社会力量开发各类国土资源信息产品并提供服务，为大众创业、万众创新注入新活力。

到2018年底，在统筹规划和统一标准的基础上，丰富与完善统一的国土资源数据资源体系。初步建成国土资源数据共享平台和开放平台，实现一定范围的数据共享与开放。各级国土资源主管部门在国土资源形势分析、决策支持和信息服务等领域的大数据应用取得初步成效。

到2020年，国土资源数据资源体系得到较大丰富与完善。国土资源数据实现较为全面的共享和开放。基于数据共享的国土资源治理能力不断提高，基于数据开放的公共服务能力全面提升。国土资源大数据在资源监管和公共服务等领域得到广泛应用。国土资源大数据产业新业态初步形成。

三、主要任务

（一）持续完善国土资源数据资源体系。

国土资源数据是国土资源大数据应用发展的基石。通过建立并不断完善统一的国土资源数据资源体系，提高数据的支撑保障能力。

1.建立数据资源目录。各级国土资源主管部门要对已有各类国土资源数据进行系统、全面的梳理，摸清数据资源家底，明确各类数据的业务主管、生产单位、基本内容、数据质量、更新要求等，逐步形成横向覆盖土地、不动产、地质矿产、地质环境与地质灾害防治等各专业领域，纵向包括国家、省、市、县四级的、较为完整、准确的国土资源数据资源目录。

2.完善数据库建设与更新机制。依托各级国土资源部门组织实施的国土资源调查、评价、监测和规划等重大专项工作，建立并完善各类国土资源基础数据库和专题成果数据库，完善数据的及时汇交与更新机制。各业务管理部门要通过数据监测监管备案机制，把履行业务管理职能过程中形成的数据实时更新到数据库系统中。同时，以大数据的发展应用为目标，逐步扩展国土资源数据的内容。按照“谁产生、谁负责”的责任机制，确保国土资源数据的完整性、准确性和及时性。

3.整合集成各类国土资源数据。各级国土资源主管部门要在国土资源“一张图”基础上，强化制度机制和标准规范建设，加强对土地、不动产、地质矿产、

地质环境与地质灾害防治等相关领域的各类成果资料、基础数据、管理数据和统计数据进行有效集成。遵循“物理分散、逻辑集中”原则，将分散的海量数据汇聚整合为逻辑集中的数据资源体系，建立统一的数据管理平台与安全机制，实现对各类国土资源数据的统一管理和应用。按照国家自然资源和空间地理信息库建设的有关要求，开展相关数据库建设。

进度安排：2017年底前，全面完成国土资源数据资源梳理，形成较为完整的国土资源数据资源目录，国土资源数据资源体系得到完善。到2020年，基本形成完整和准确的国土资源数据资源体系，国土资源数据得到较大丰富与完善。

（二）全面推进国土资源系统内部信息互联互通

全面推动国土资源系统内部的互联互通和数据共享，是打破“信息孤岛”，实现国土资源相关单位之间资源整合、业务协同的重要途径，也是转变政府职能、充分发挥各有关单位作用的有效手段。

1.建立纵向覆盖四级国土资源主管部门的数据共享与交换机制。以国土资源业务专网为依托，部统一建立国土资源数据共享与交换系统，连接国家、省、市、县四级国土资源主管部门。建立健全数据共享与交换的相关制度，落实数据共享与交换相关主体的权利、责任和义务，形成国土资源系统内部数据共享与交换机制，实现土地“批、供、用、补、查、登”、矿产资源勘查与开采利用全过程、地质环境与地质灾害防治等重要数据在各级国土资源主管部门之间的在线共享与交换。

2.构建横向国土资源系统内部数据共享应用机制。在部层面，依托涉密内网，按照“物理分散、逻辑集中”原则，整合国土资源系统内部各有关单位现有分散的数据中心资源，形成布局合理、规模适度、保障有力、绿色集约的涉密内网国土资源数据中心体系。建立统一的数据共享平台，实现遥感数据、土地利用、土地规划、不动产登记、矿产资源储量、矿产资源规划、基础地质、地质环境与地质灾害防治、地质资料、科技创新成果和人力资源等基础数据、专题数据及数据产品在部机关、土地督察局及直属单位的共享使用。进一步加强基础地理、土地、地质、矿产和海洋等数据的共享和应用机制建设，促进基础地理、海洋等信息在

国土资源管理服务中的应用，构筑“测绘为基，陆海相连”的国土资源空间数据框架。网络基础设施有条件的省级和地市级国土资源主管部门，可依托本级涉密内网，根据需要建立横向连接本级各相关单位的数据共享系统，实现数据资源在同级的共享与交换。

进度安排：2018年底前，初步实现纵向覆盖四级国土资源主管部门的数据共享与交换，横向覆盖部级部分单位之间的数据共享应用。到2020年，基本实现纵向覆盖四级国土资源主管部门、横向覆盖部级和部分省级各单位之间数据的共享与交换。

（三）大力推进政府部门之间的数据共享服务。

大力推进国土资源数据与政府部门的共享服务，是发展国土资源大数据的重要内容，有利于推动数据有效利用，提升政府的服务能力和综合效能。

1.制定数据共享制度和标准。按照国家数据共享的要求，国土资源部负责制定国土资源数据共享管理办法，明晰数据共享相关主体的权利、责任和义务，形成国土资源数据共享的评估、监督和审查机制。各级国土资源主管部门依据共享管理办法，制定国土资源数据共享目录，厘清共享数据的范围、边界和使用方式，确保共享数据的质量和时效。制定数据共享、交换接口、访问接口和安全保密等标准规范。

2.开发建立国土资源数据共享平台。各级国土资源主管部门依托国家电子政务内网和外网，开发建立本级统一的国土资源数据共享平台，并与政府数据统一共享交换平台实现对接。分批次、有序开展遥感数据、土地利用现状、土地利用总体规划、土地整治规划、基本农田、农用地分等定级、矿产资源规划、矿产资源储量、矿产资源开发利用、矿产地、基础地质、地质环境与地质灾害防治、地质资料和科技创新成果等国土资源数据向政府部门提供共享服务。尤其是，加快不动产登记有关信息与住建、农业、林业、海洋等部门审批交易信息实时互通共享，以及与公安、民政、财政、税务、工商、金融、审计、统计、司法等部门的共享交换，促进部门间的业务协同。同时，依据其他政府部门的数据共享目录，建立相应的技术机制，获取其他相关部门的数据，为国土资源管理、监管和决策

提供支撑服务。

3.加强国土资源专题信息产品制作与服务。以国土资源数据资源体系为基础,加强各类国土资源数据汇聚整合,设计、开发和制作土地、地质矿产、地质环境与地质灾害防治等方面的专题信息产品,为政府部门和行业提供信息产品的线上和线下服务。

进度安排:2017年底前,编制国土资源数据共享管理办法,制定国土资源数据共享目录,开发统一的国土资源数据共享平台,研制数据共享标准规范。2018年底前,初步实现与相关政府部门之间部分数据共享,并开展国土资源信息产品服务。到2020年,数据共享制度进一步完善,基本实现与相关政府部门之间数据共享。

(四) 稳步推进国土资源数据向社会开放。

在加强安全保障和隐私保护的前提下,稳步推进国土资源数据向社会开放,推进可开放数据的社会化、市场化利用,促进数据资源的深度挖掘和应用。

1.建立数据开放制度和标准。按照国家数据开放的要求,国土资源部负责制定国土资源数据开放管理办法,形成数据开放的机制。各级国土资源主管部门依据开放管理办法,制定国土资源数据开放清单,实施分年度数据开放计划。制定数据开放、开发接口等标准规范,健全开放前保密审查机制,妥善处理数据开放与保密的关系。

2.建设全国统一的国土资源数据开放平台。依托互联网“国土资源云”基础设施,建立全国统一的国土资源数据开放平台,平台覆盖国家、省、市、县四级国土资源主管部门,并与国家政府数据统一开放平台对接。各级国土资源主管部门依据本级的数据开放清单和年度数据开放计划,通过统一的国土资源数据开放平台,开展数据的推送与开放。数据开放实行“谁推送、谁负责”的责任机制。

3.稳步推进各类国土资源数据向社会开放。各级国土资源主管部门以涉及民生保障、公共服务和市场监管等数据为重点向社会开放。有序推进土地利用规划、建设用地审批、土地征用、土地市场、土地价格、土地开发利用等土地数据集,

矿产资源规划、矿业权审批登记、矿产资源勘查资质、矿产资源开发利用、矿业权市场等矿产资源数据集，国土资源统计数据，多种比例尺基础地质图和环境地质图、地质灾害防治与地面沉降等数据集向社会开放。

4.加强公众版信息产品制作与服务。面向经济发展和社会公众的应用需求，开展土地基础数据、数字地质图件、地质环境与地质灾害调查、监测与预警等方面的标准化、普适化产品制作，形成多样化的各类公众版信息产品，以网站、报告、数据集、APP等多种形式为社会提供服务，满足广大公众对国土资源信息的需求。

5.培育国土资源数据开发利用的市场化机制。在国土资源数据向社会开放的同时，积极规范和引导各类市场主体、行业组织等社会力量广泛参与国土资源数据的开发利用，鼓励社会力量设计制作增长性、公益性、创新性信息产品，开展数据增值服务。激发创新创业活力，促进国土资源数据开发服务产业链的逐步形成。

进度安排：2018年底前，编制国土资源数据开放管理办法，制定国土资源数据开放清单，研制数据开放标准规范，建设全国统一的国土资源数据开放平台，实现部分国土资源数据向社会开放，初步形成公众版国土资源信息产品。到2020年，数据开放制度进一步完善，向社会开放的国土资源数据和专题信息产品明显丰富并基本满足社会公众的需要，国土资源数据的市场化服务机制初步形成。

（五）有效提升国土资源决策支持能力。

紧密围绕国土资源工作实际需要，推进国土资源重点领域大数据高效采集、有效整合和应用拓展，及时收集与汇聚其他行业相关数据、互联网及相关媒体信息，构建决策支持系统，为资源形势分析、管理状况监测和参与宏观调控等提供有效的决策支持服务。

1.采集与汇聚其他行业相关数据。国家级和省级国土资源主管部门、有条件的市、县级国土资源主管部门要充分利用国土资源数据共享平台，及时采集与汇聚人口、法人、税收、投融资等社会经济数据以及城市建设、交通运输、能源、

水利、环保等其他行业相关数据；利用报纸、杂志、电视、广播等传统媒体以及网络、视频、电子杂志、微信、社区、论坛、博客等新媒体，实时监测和采集土地征收、土地审批供应、矿业权审批、土地与矿业权交易、土地与矿产资源开发等方面涉及国土资源领域的民生需求、舆论热点、公众意见等数据；广泛收集和汇聚全球矿产资源数据。利用大数据智能感知技术、预处理技术和分布式虚拟技术，对上述各类结构化、半结构化、非结构化的海量数据进行智能化识别、抽取与组织，建立国土资源决策支持综合信息库和数据持续更新机制。

2.构建国土资源决策支持系统。国家级、省级国土资源主管部门和有条件的市、县级国土资源主管部门要以国土资源“一张图”、综合信息监管平台数据和决策支持综合信息库为基础，利用大数据分析、挖掘、检索和可视化等技术，建立相关知识库、模型库，构建国土资源决策支持系统，提供资源综合监管、资源勘查开发、管理状况监测、政策制定评估、扶贫开发工作和社会舆情分析等方面的专题服务。

3.开展重点领域的决策分析应用。利用国土资源决策支持系统，开展涉及社会关切、影响巨大、关乎长远等相关领域重大问题的决策分析工作。重点对国土资源行政审批、规划执行、开发利用、违法违规等开发利用过程和状况进行监测分析；对国土资源利用和管理中的基本情况、发展趋势和存在问题进行形势分析和研判；对国土资源制度改革的热点、难点问题、政策执行和调控效果、管理水平等进行分析与诊断；对网上涉及国土资源领域的民生需求、舆论热点、社会关注等情况开展舆情分析；对扶贫地区的土地利用、矿产资源、地质环境与地质灾害防治以及资源开发利用政策等进行分析、研究和评估；对全球矿产资源开发利用进行分析等。

4.建立国土资源国家智库信息化平台。按照国土资源新型智库建设的有关要求，依托决策支持系统，构建国土资源国家智库信息化平台，连接相关大专院校、科研机构 and 资深专家，汇聚和管理各类研究成果，建立国土资源战略研究成果库和专家库，形成决策知识推送、研究理念与成果分享的开放型机制，逐步形成信息化条件下的新型“互联网+”智库运行体系，提高国土资源综合研判、战略谋

划能力以及重点领域决策支持能力。

进度安排：2017年底前，完成国土资源决策综合信息库、决策支持系统和智库信息化平台的相关研究。2018年底前，基本建立国土资源决策支持综合信息库，初步建立国土资源决策支持系统和智库信息化平台，开展有关领域的决策分析。到2020年，基本建成国土资源决策支持系统和智库信息化平台，为国土资源决策提供重要支撑。

（六）加强地质环境与地质灾害分析预警与信息服务。

利用物联网、大数据等新一代数据采集与分析技术，建立智能化地质环境与地质灾害分析预警系统，整合各类地质环境与地质灾害防治数据，全面提升地质环境与地质灾害防治信息的分析与预警、决策与处置能力和信息服务水平。

1.集成与整合各类地质环境与地质灾害防治数据。利用已有的海量地质环境与地质灾害防治数据，采用大数据分析技术，开展地质灾害、地下水、矿山环境、地面沉降、地质遗迹等业务数据和动态监测数据的集成和整合，并与气象、水利、农业和环保等其他政府部门的数据进行聚合与关联分析，建立分析模型与预测模型，增强地质环境与地质灾害分析预警预报及应急指挥能力。

2.构建智能化地质环境与地质灾害分析预警系统。基于物联网和大数据技术，建立智能化地质灾害、地下水、地面沉降、矿山地质环境、地质遗迹等调查、监测数据采集、信息分析与预警系统。开展重大地质灾害快速识别、监测预警、应急处置等关键技术研发，实现重大灾害关键部位专业监测与群测群防监测数据实时自动处理和预警分析。

3.开展地质环境与地质灾害防治信息综合分析与服务。针对国家发展战略，围绕京津冀、长江经济带等重要经济区带社会经济发展规划、重大工程建设，运用大数据分析技术，开展地质环境与地质灾害防治信息综合分析和研究，提供及时、全面、准确的区域地质环境与地质灾害防治总体状况信息，为地质环境与地质灾害防治综合评价分析、资源承载力评价、地质环境与地质灾害防治管理、防治与应急指挥等各项工作提供有效的系列产品和服务。

进度安排：2018年底前，基本完成各类地质环境与地质灾害防治数据的整合集成并提供应用，建立地质环境与地质灾害调查、监测数据采集、分析和预警系统。开展地质环境与地质灾害防治信息综合分析与服务。到2020年，地质环境与地质灾害分析预警能力和信息服务水平明显提高。

（七）大力推进地质调查信息服务。

开展地质大数据建设，构建地质数据协同服务体系，深化地质大数据在调查、管理与服务等方面的创新应用，提升地质调查数据获取、分析、处理和服务能力。

1.建设地质大数据支撑平台。通过大数据等新一代信息技术的开发应用，支撑各类地质调查数据的采集、传输、处理、应用和服务。实现已积累的地质调查存量数据和正在实施的地质调查评价9大计划50项工程生产的增量数据的高效汇聚、组织、管理与共享，实现与国土资源数据共享平台的互联互通。

2.构建地质信息协同服务体系。构建由中国地质调查局主服务节点、六大区地调中心服务节点、局属专业地调单位服务节点等组成的多层次、网络化地质信息协同服务体系。各服务节点在地质大数据支撑平台的架构下，实现资源的统一汇聚、互联互通，提供全方位、多层次信息服务。

进度安排：2017年底前，完成地质大数据支撑平台建设，实现与国土资源数据共享平台互联互通，实现全国性综合服务节点与区域综合服务节点、专业综合服务节点的互联互通。到2020年，基本形成地质信息服务新模式。

（八）培育智能化国土资源调查评价监测应用新业态。

充分利用大数据技术，推进国土资源调查、评价和监测技术研发，创新工作模式，培育智能地质调查、智慧探矿、土地智能监测等应用新业态。

1.建设与完善智能地质调查体系。研发野外调查、监测、物化探、遥感、分析测试、钻探等地质工作手段的数据采集工具软件，提高数据采集效率与智能化。推进数字地质调查系统向智能化、智慧化方向发展，在地质数据快速采集、实时传输、汇聚、处理、综合、建模等方面逐步实现大数据技术支撑下的智能地质调查工作和服务模式的创新。在区域地质调查、矿产资源调查、地质灾害评价、地

下水资源调查评价等地质调查领域实现数字调查全覆盖。

2.培育智慧探矿应用新业态。紧密围绕国家资源战略与找矿需求，开发面向地质大数据的地质矿产数据处理与评价软件工具，促进共享与应用。依托地质大数据、重点实验室与业务中心等平台资源，开展重要矿种找矿专家模型、智慧探矿软件等关键技术攻关与相关系统建设，增强地质数据智能分析处理与评价预测能力。搭建地质矿产软件公共开发与应用平台，提供云端集成开发环境、高性能计算环境、应用接口与技术标准等服务。积极引导和鼓励企业、高等院校、科研机构和社会公众开展智慧探矿创新应用研究，逐步形成以数据驱动的地质矿产调查评价与智慧探矿新业态。

3.探索土地智能监测新模式。针对进一步加强土地资源数量、质量和生态监管的现实需求，重点开展面向对象的多源遥感数据快速精准校正与融合关键技术研究、面向对象的遥感数据光谱库建设、多尺度土地利用与覆被遥感自动分类规则和方法研究、多尺度土地生态退化和土地质量遥感智能化监测和评估方法研究。充分利用社会力量，研发基于大数据的多尺度和多源遥感数据自动化校正和融合作业平台，以及土地数量、质量和生态状况智能化监测和分析技术平台，提供动态更新的影像库、知识库、光谱库、应用接口与技术标准等，形成土地智能监测应用新模式。

进度安排：2017年底前，初步建立智能地质调查体系，2018年底前，初步形成智慧探矿和土地智能监测的探索性应用。到2020年，智能地质调查体系基本建立，智慧探矿和土地智能监测达到普适化水平。

推动海洋、测绘地理信息大数据应用发展。国家海洋局、国家测绘地理信息局分别研究编制大数据应用发展意见。

四、保障措施

（一）完善组织实施机制。国土资源大数据应用发展工作由部网络安全和信息化领导小组统一领导。各级国土资源主管部门要按照国土资源大数据应用发展的总体要求，建立国土资源大数据统筹与实施机制，加强与海洋局、测绘地理信

息局的沟通协作，形成职责明确、分工有序、共同推进的工作格局。各级国土资源主管部门信息办负责国土资源大数据应用发展的统筹协调和组织实施，牵头编制国土资源数据共享目录和开放清单；业务管理部门会同数据生产和保管单位负责相应主管数据共享和开放的评估、监督、审查和管理等工作；相关技术单位负责有关共享平台和开放平台、数据共享和开放的技术支撑保障工作。政策制度、标准规范和部分平台建设等工作采取统一建设模式，由部统筹规划、主导建设。数据整合、服务分发、产品制作和相关系统建设等工作，按照统一的标准规范，由各级数据生产单位、保管单位和技术单位负责实施。各责任部门和单位要细化工作计划，采取有力措施，确保各项重点任务按计划完成。

（二）健全数据管理制度。各级国土资源主管部门的业务管理部门会同相关技术单位，建立并完善国土资源数据分级分类管理办法，建立健全国土资源数据管理制度，明确数据生产和管理的责任、义务以及数据使用权限，明晰数据管理和数据使用的考核评价方式，合理界定数据的使用方式与范围，规范数据采集、保管、共享、开放和应用，保障数据一致性、准确性和权威性。

（三）强化科技人才支撑。加强国土资源大数据科研创新基地和重点实验室建设，创新人才培养机制，积极引进大数据高层次人才。加大力度培养具有计算机技术、大数据分析、国土资源管理等多学科知识的跨界复合型人才。加强职业技能人才培养，培育国土资源大数据技术和应用创新型人才。鼓励高等院校、科研机构、高新企业联合攻关。充分利用社会资源，重点加强国土资源大数据采集、存储、管理、分析、可视化、信息安全与隐私保护等领域关键技术的研发与应用。

（四）加大经费支持力度。各级国土资源主管部门要加大对大数据应用发展的经费保障力度，把大数据应用发展工作所需经费纳入年度预算，积极支持国土资源大数据的关键技术研发、重大应用示范工程和数据共享开放平台建设等。按要求管好用好已有资金，积极拓宽资金渠道，加强资金使用管理、预算绩效管理和绩效评价，提高资金使用效益。按照国务院关于政府向社会购买服务的要求，制定和完善政府购买大数据服务的配套政策，加大对政府部门和企业合作开发大数据的支持力度。

(五) 加强信息数据安全。建立健全大数据安全体系，做好顶层设计，加强对国土资源大数据的安全技术防护和安全管理，明确数据管理和维护责任单位，落实数据安全保护措施，采用安全可信产品和服务，加强日常监管。建立和完善大数据安全标准规范，加强安全监测、预警和应急处置能力。切实加强对涉及国家利益、公共安全、商业秘密、个人隐私等信息的保护。妥善处理共享开放与保障安全的关系，促进数据在安全保障、风险可控的原则下最大程度共享开放。

(七) 信息安全技术大数据交易服务安全要求（征求意见稿）

1 范围

本标准规定了数据交易服务涉及的交易参与方、交易对象和交易过程的安全要求。

本标准适用于提供数据交易服务的组织进行安全自评估，也适用于第三方机构对数据交易服务组织进行安全测评。

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 25069-2010 信息安全技术 术语

GB/T AAAA 信息技术 数据交易服务平台 交易数据描述

GB/T BBBB 信息技术 数据交易服务平台 通用功能要求

GB/T CCCC 信息安全技术 个人信息安全规范

GB/T DDDD 信息安全技术 数据出境安全评估指南

GB/T EEEE 信息安全技术 大数据服务安全能力要求

GB/T FFFF 信息安全技术 大数据安全能力成熟度模型

GB/T GGGG 信息安全技术 个人信息安全影响评估指南

GB/T 22239-2008 信息安全技术 网络安全等级保护基本要求

3 术语和定义

GB/T 25069-2010、GB/T AAAA、GB/T BBBB所确立的以及下列术语和定义适用于本文件。

3.1 数据交易 data exchange

数据供方和需方之间以数据商品作为交易对象，进行的以货币交换数据商品，或者以数据商品交换数据商品的行为。

注1：数据商品包括原始数据或加工处理后的数据衍生产品。

注2：数据交易包括以大数据或其衍生品作为数据商品的数据交易，也包括以传统数据或其衍生品作为数据商品的数据交易。

3.2 数据供方 data supplier

数据交易中提供数据的组织或个人。

3.3 数据需方 data demander

数据交易中购买和使用数据的组织或个人。

3.4 数据交易服务机构 data exchange service provider

为数据供需双方提供数据交易服务的组织。

3.5 数据交易服务平台 data exchange service platform

数据交易服务机构依赖的用来为供需双方提供数据交易的信息化平台。

3.6 在线数据交易 online data exchange

数据供方以数据调用接口的形式通过网络向数据需方交付数据的数据交易模式。

3.7 离线数据交易 offline data exchange

数据供需双方在达成数据交易协议后，由数据供方通过离线方式将数据从供方传输到需方的数据交易模式。

3.8 托管数据交易 custodian data exchange

数据供需双方在达成数据交易协议后，由供方将数据拷贝到数据交易服务机构指定的数据托管服务平台，需方在数据托管服务平台内使用数据，数据不发生转移的交易模式。

3.9 数据交易过程 data exchanging process

数据供需双方依托数据交易服务平台针对具体的数据交易对象，进行的一次完整和具体的数据交易行为。

注：数据交易过程一般分为交易申请、交易磋商、交易实施和交易退出等环节。

4 安全概述

总则

数据交易是供需双方对原始数据或加工处理后的数据依照既定交易过程进行的活动。数据交易服务参考框架如图 1 所示。数据交易涉及到数据供方、数据需方和数据交易服务机构。数据交易服务机构依托数据交易服务平台，为数据供需双方提供数据交易服务。从数据交易服务机构角度出发，数据交易过程一般包括交易申请、交易磋商、交易实施和交易结束四个环节。常见的数据交易模式包括在线模式，离线模式和托管模式。



图1 数据交易服务参考框架

数据交易安全原则

- a) 数据交易合法合规原则：数据交易应遵守我国关于数据安全相关法规、尊重社会公德，不得损害国家利益、社会公共利益和他人合法权益；
- b) 主体责任共担原则：数据供需双方及数据交易服务机构对数据交易后果负责，共同确保数据交易的安全；
- c) 数据安全防护原则：数据交易各参与方应采取数据安全保护、检测和响应等措施，防止数据丢失、损毁、泄露和篡改，确保数据安全；
- d) 个人信息保护原则：数据供需双方在进行数据交易时，应采取个人信息安全保护技术和管理措施，避免个人信息的非法收集、滥用、泄漏等安全风险，切实保护个人权益；
- e) 交易过程可控原则：应确保数据交易参与方的真实可信，交易对象合法、数据交付和资金交付过程可控，做到安全事件可追溯，安全风险可防范。

5 数据交易参与方安全要求

数据供方安全要求

数据交易服务机构应确保数据供方满足以下要求：

- a) 数据供方应为无违法违规记录的合法组织或自然人；
- b) 数据供方应完成在数据交易服务机构的注册，并经数据交易服务机构审核通过，才允许参与数据交易业务；
- c) 数据供方应证明其具备向数据需方安全交付数据的能力；
- d) 数据供方应向数据交易服务机构提供书面的安全承诺，内容包括但不限于：交易数据满足法律法规和政策要求、对交易数据质量评估说明、遵守数据交易安全原则、愿意接受数据交易服务机构安全监督、愿意对数据流通后果负责等；
- e) 数据交易服务机构应建立和执行针对数据供方的安全监管制度和流程。

数据需方安全要求

数据交易服务机构应确保数据需方满足以下要求：

- a) 数据需方为无违法违规记录的境内合法组织或自然人；
- b) 数据需方应完成在数据交易服务机构的注册，并经数据交易服务机构审核通过，才允许参与数据交易业务；
- c) 数据需方应证明其具备对交易数据实施安全保护的能力；
- d) 数据需方应提供书面的数据交易和使用安全承诺，内容包括但不限于：满足法律法规和政策要求、遵守数据交易安全原则、愿意接受数据交易服务机构安全监督、遵守与数据供方约定的数据安全要求、对所持有数据提供充分的安全保护、未经明确授权不公开或转交数据给第三方等；
- e) 数据需方应按照供需双方约定的使用目的、范围、方式和期限使用数据，禁止进行个人信息的再识别；
- f) 数据需方在按照数据交易约定方式完成数据使用后，应及时销毁交易数据；
- g) 数据交易服务机构应建立和执行针对数据需方的安全监管制度和流程。

数据交易服务机构安全要求

1 基本要求

数据交易服务机构应满足以下基本要求：

- a) 应为无违法违规记录的境内合法组织；
- b) 应得到我国行政或主管部门的授权或许可；
- c) 应具备承担数据交易服务相对应的安全保障能力；
- d) 应将从事境内数据交易服务的数据交易服务平台部署在我国境内。

2 组织安全管理要求

2.1 安全管理制度和规程

数据交易服务机构应满足以下要求：

- a) 制定数据交易服务安全管理策略，说明数据交易安全总体目标、范围、原则和安全框架等；
- b) 建立数据交易服务安全管理制度，包括但不限于：交易参与方安全管理制度、数据安全管理制度、个人信息安全保护制度等；
- c) 为数据交易管理人员或操作人员执行的管理或业务操作建立操作规程；
- d) 定期对数据交易服务安全管理策略、制度和规程进行评审，并及时进行更新。

2.2 安全相关组织机构和人员

数据交易服务机构应满足以下要求：

- a) 建立数据交易安全领导小组，由机构最高管理者或授权代表担任组长；
- b) 建立数据交易安全管理职能部门，设立安全管理负责人岗位，明确安全责任；
- c) 设立数据交易安全管理员、个人信息安全管理员等岗位，定义各个岗位的安全职责，并配备一定数量的岗位人员；
- d) 对数据交易重要岗位人员进行安全审查和技术考核，确保无违法违规记录；
- e) 与数据交易重要岗位人员签署安全保密协议，与重要岗位人员签署岗位责任协议；
- f) 对数据交易各类岗位人员制定和实施培训计划，培训内容包括安全意识、专项技能等，具备与岗位要求相适应的安全管理知识和专业技术水平；
- g) 对第三方人员进行安全管理，对于可能接触交易数据的第三方人员，应签署安全保密协议。

3 数据交易服务平台安全要求

3.1 基础要求

数据交易服务平台应满足GB/T 22239中第3级的相关安全要求。

3.2 扩展要求

3.2.1 交易数据安全保护

数据交易服务平台应满足以下要求：

- a) 分别为数据供方、需方提供安全的上传或下载接口，传输链路加密等保护措施，确保数据传输的安全；
- b) 对交易数据实施加密存储、访问控制等安全措施，防止数据泄露或非法使用；
- c) 实现数据源和数据操作的可追溯性；
- d) 在托管数据交易模式下，应为数据需方提供隔离安全环境，对数据需方在数据使用环境中运行的相关程序和产生的数据结果进行审核；
- e) 在托管数据交易模式下，应对交易数据进行安全存储和备份，确保数据的保密性、完整性和可用性。

3.2.2 交易过程安全控制

数据交易服务平台应满足以下要求：

- a) 允许对数据交易的参与方、对象、关键过程设置人工干涉；
- b) 人工干涉的内容中至少应包括：会员审核、交易审核、交易暂停、交易撤销。

3.2.3 数据交易安全审计

数据交易服务平台应满足以下要求：

- a) 对每笔数据交易操作进行记录，生成数据交易日志；
- b) 数据交易日志至少包括以下信息：交易唯一标识、交易时间、交易供方、交易需方、交易数据标识、敏感数据标签、交易价格、交易模式、交易结果等；

- c) 安全保存数据交易日志至少6个月；
- d) 只允许授权审计员访问数据交易日志，支持对数据交易日志进行查询和分析；
- e) 允许数据供方和数据需方查询与自己数据交易相关的日志信息，并允许导出。

3.2.4 数据托管服务平台安全

对于提供托管交易模式的数据交易服务机构，应该遵循GB/T EEEE要求来建设和运维数据安全托管服务平台。

4 交易对象安全

禁止交易数据

数据交易服务机构应根据我国相关法律法规，制定禁止交易的数据目录，目录至少应包括：

- a) 涉及国家秘密等受法律保护的数据；
- b) 涉及个人信息的数据，除非获得了全部个人数据主体的明示同意，或者进行了必要的去标识化处理；
- c) 涉及他人知识产权和商业秘密等权利的数据，除非取得权利人明确许可；
- d) 涉及以下内容的数据：
- e) 反对宪法所确定的基本原则的；
- f) 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；
- g) 损害国家荣誉和利益的；
- h) 煽动民族仇恨、民族歧视，破坏民族团结的；
- i) 破坏国家宗教政策，宣扬邪教和封建迷信的；
- j) 散布谣言，扰乱社会秩序，破坏社会稳定的；

- k) 散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的；
- l) 侮辱或者诽谤他人，侵害他人合法权益的；
- m) 涉及枪支弹药、爆炸物品、剧毒化学品、易制爆危险化学品和其他危险化学品、放射性物品、核材料、管制器具等能够危及人身安全和财产安全的危险物品的；
- n) 宣扬吸毒、销售毒品以及传播毒品制造配方的；
- o) 涉及传销、非法集资和非法经营等活动的；
- p) 其它法律法规明确禁止交易的数据。

数据质量要求

数据交易服务机构应确保交易数据满足以下质量要求：

- a) 应要求数据供方向数据交易服务机构提供交易数据获取渠道合法，权利清晰无争议的承诺或证明材料；
- b) 应要求数据供方向数据交易服务机构提供拥有交易数据完整相关权益的明确声明；
- c) 应要求数据供方向数据交易服务机构提供数据真实性的明确声明；
- d) 应要求数据供方向数据交易服务机构对交易数据进行分类，并对交易数据进行安全风险评估，出具安全风险评估报告；
- e) 应要求数据供方应明确交易数据的限定用途、使用范围、交易方式和使用期限；
- f) 应要求数据供方应按照GB/T AAAA要求对交易数据进行准确描述，明确数据类别等内容，描述内容满足准确性、真实性要求；
- g) 数据交易服务机构应对交易数据描述的准确性、真实性进行审核；
- h) 数据交易服务机构应对交易数据的安全风险评估报告进行审核，确保数

据可交易；

- i) 数据交易服务机构应对交易数据分类结果进行审核。

个人信息安全保护

数据交易服务机构应确保交易数据在个人信息安全保护方面满足以下要求：

- a) 涉及个人信息的交易数据，应满足GB/T CCCC第8节关于个人信息的委托处理、共享、转让、公开披露安全要求；
- b) 应要求数据供方对交易数据进行个人信息安全风险评估，提供个人信息安全风险评估报告；
- c) 数据交易服务机构应对个人信息安全风险评估报告进行审核，确保数据可交易。

5 数据交易过程安全

交易申请

数据交易服务机构应确保交易申请环节满足以下要求：

- a) 数据供方应明确界定交易数据的内容范围、使用范围，以确保符合国家相关法律法规的要求；
- b) 数据供方应按数据交易服务机构要求，提供对交易数据的概要描述，并提供样本数据；
- c) 数据交易服务机构对数据供方提供的样本数据进行内容审核，确认数据合法合规。对于不符合相关要求的，数据交易服务机构应要求数据供方处理后，重新提交样本数据进行审核；
- d) 数据需方应披露数据需求内容、数据用途，以确保符合国家相关法律法规的要求；
- e) 数据交易服务机构对数据需方的数据需求进行审核通过后，方可发布。

交易磋商

数据交易服务机构应确保交易磋商环节满足以下要求:

- a) 供需双方应对交易数据的用途、使用范围、交易方式、使用期限和交易价格等协商和约定，形成交易订单；
- b) 数据交易服务机构应依据GB/T CCCC和GB/T DDDD等标准，对交易订单从数据出境安全、个人信息保护安全等方面进行审核，确保符合相关法律法规和标准等合规性要求，撤销不符合要求的交易订单；
- c) 数据交易服务机构应对审核通过的订单进行登记备案，并对供需双方发出交易确认通知。

交易实施

数据交易服务机构应确保交易实施环节满足以下要求:

- a) 数据交易服务机构应为数据交易签订合同，明确数据内容、数据用途、交付质量、交付方式、交易金额、交易参与方安全责任、保密条款等内容；
- b) 数据交易服务机构应对交付数据进行监测和核验，如发现违法违规事件，应及时中断数据交易行为，同时依法依规进行处理；
- c) 数据交易服务机构应对交易过程中的违法违规数据具有追溯能力；
- d) 对于在线交易模式，数据交易服务机构应具备在供需双方的数据传输通路部署交易数据监控工具的能力；
- e) 对于托管交易模式，数据交易服务机构应为数据需方建立安全的数据使用环境，并分配相应的权限；
- f) 数据供方在数据需方未完全获取数据内容前，有义务保证交易数据质量和数量符合数据成交时的相关描述；
- g) 在托管数据交易模式下，数据需方在数据使用完成后，应向数据交易服务平台提供提取结果数据请求，核准后由数据交易服务平台发放给数据需方。

交易结束

数据交易服务机构应确保交易结束环节满足以下要求:

- a) 数据交付完成前, 交易服务机构应对资金进行监管, 获得数据交付和接收确认后, 资金给付数据供方;
- b) 数据交付完成后, 数据供方应及时关闭数据访问接口, 数据供方发出数据交付完成确认;
- c) 数据交付完成后, 数据需方发出数据接收完成确认;
- d) 在托管交易模式下, 数据交易服务机构应在交易结束后及时销毁残余数据, 防止数据泄露等安全隐患;
- e) 数据交易服务机构应为交易过程形成完整的交易日志并进行安全保存。

（八）国家知识产权局办公室关于印发加快推进“互联网+政务服务”工作方案的通知

局机关各部门，专利局各部门，局各直属单位：

《国家知识产权局加快推进“互联网+政务服务”工作方案》已经局“互联网+政务服务”工作领导小组审议并同意，现予印发。请各部门（单位）认真贯彻落实。

特此通知。

国家知识产权局办公室

2017年9月24日

国家知识产权局加快推进“互联网+政务服务”工作方案

按照《国务院关于进一步加快推进“互联网+政务服务”工作的指导意见》（国发〔2016〕55号）要求，为落实国务院“简政放权、放管结合、优化服务”的重大决策部署，进一步加快转变政府职能，提高透明度，切实改进政务服务质量与效率，结合我局实际，制定本方案。

一、总体要求

（一）指导思想。全面贯彻党的十八大和十八届三中、四中、五中、六中全会精神，深入贯彻习近平总书记系列重要讲话精神，牢固树立创新、协调、绿色、开放、共享发展理念，按照建设法治政府、创新政府、廉洁政府和服务型政府的要求，优化服务流程，创新服务方式，推进数据共享，做到事项管理规范、信息透明实用、网上办理高效、服务便民利企。

（二）基本原则。

坚持统筹规划。做好顶层设计，制定标准规范，预留发展空间，避免重复建设，推动政务服务平台整合，实现政务信息资源互认共享。

坚持问题导向。从解决群众反映强烈的办事难、办事慢、办事繁等问题

出发，优化办事流程，压缩办理时限，坚持实体业务大厅（包括专利受理服务大厅、代办处、快速维权中心及知识产权保护中心，下同）服务与网上服务并重，推进线上线下融合，及时回应社会关切，提供渠道多样、简便易用的政务服务。

坚持协同发展。加强协作配合，建立强有力的工作推进机制和联动机制，明确各部门、各单位目标任务、责任分工和进度要求，实现整体推进，做好制度衔接，为“互联网+政务服务”提供制度和机制保障。

坚持开放创新。运用互联网思维，创新服务模式，拓展服务渠道，开放服务资源，构建政府、公众、企业共同参与的政务服务新格局。

（三）工作要求。

1. 平台充分融合。推动实体业务大厅、网上政务平台、移动客户端、服务热线充分结合，实现线上线下一体化运行，把局门户网站打造成知识产权网上政务服务的“一张网”。

2. 上网事项全面。加快推进知识产权政务服务事项网上办理，做到“应上尽上、全程在线”，提高服务效率和透明度。

3. 服务流程便利。运用互联网思维和标准化手段，创新服务模式、拓展服务渠道、加强服务流程优化，让群众和企业少跑腿、好办事、不添堵。

4. 保障信息安全。提高信息平台（系统）的安全管理和安全防护能力。建立健全保密和密码管理、检查和审查制度（非密网），提升信息安全支撑保障水平和风险防范能力。

（四）工作目标。

2017年底前，建成高效便捷的一体化网络政务服务平台，全面公开知识产权政务服务事项，政务服务标准化、网络化水平显著提升。

2020年底前，按照国务院办公厅统一部署，实现互联网与知识产权政务服务深度融合，政务服务智慧化水平大幅提升，企业和群众办事更方便、更快捷、更有效率。

二、工作任务

（一）规范服务事项。

1. 依据法定职能全面梳理直接面向社会公众提供的具体办事服务事项，并实行编码管理，规范事项名称、条件、材料、流程、时限。逐项编制服务事项目录并归类，确保于2017年底前通过局门户网站发布。（专利局办公室牵头，条法司、审查业务管理部、初审及流程管理部和复审委按职责分别负责）

2. 规范和完善办事指南，具有政务服务事项的部门单位，按“目录化、标准化、电子化”要求，编写能够通过网络提供的各类服务事项办事指南，明确申请材料格式，提供通俗易懂的示例，告知申请、受理、审查、决定、送达的流程，积极推动、完善在线填报、在线提交和在线审查。（办公室牵头，条法司、专利局办公室、审查业务管理部、初审及流程管理部和复审委按职责分别负责）

3. 在局门户网站集中全面公开与知识产权政务服务相关的服务信息，具体包括法律法规、政策文件、通知公告、办事指南、常见问题、监督举报方式和网上可办理程度等，实行动态调整，确保线上线下信息内容准确一致。（办公室牵头，条法司、保护协调司、规划发展司、专利局办公室、审查业务管理部、初审及流程管理部和复审委按职责分别负责）

（二）创新服务方式。

4. 根据工作职责推进服务事项网上办理，重点是涉及专利申请的受理、审批、复审及专利权无效程序的相关服务事项，逐步实现网上受理、网上办理、网上反馈，做到服务事项“应上尽上、全程在线”；利用统一的政务服务资源，积极推进上述服务向移动端、热线电话等延伸，为企业和公众提供多样便捷的办事渠道。（审查业务管理部、初审及流程管理部、自动化部、专利复审委员会和检索咨询中心按职责分别负责）

5. 引入社会力量，积极利用第三方平台，开展证照寄送以及在线支付等服务。（初审及流程管理部牵头负责）

6. 依法有序开放知识产权网上政务服务资源和数据，鼓励公众、企业和社

会机构开发利用，提供多样化、创新性的便民服务。（规划发展司牵头负责，自动化部配合）

（三）夯实支撑基础。

7. 根据国务院办公厅部署要求，推动电子证照、电子公文、电子签章在政务服务中的应用，积极推动网上验证核对，避免重复提交材料和循环证明。（审查业务管理部牵头负责，初审及流程管理部 and 自动化部按职责分别负责）

8. 贯彻落实国务院办公厅有关管理制度和服务规范，加快清理修订不适应“互联网+政务服务”有关规章制度。（条法司牵头负责）

9. 将“互联网+政务服务”工作纳入干部教育培训体系，作为干部教育培训的重要内容，进一步提高我局政务工作人员的互联网思维和技能。（人事司牵头负责，人事教育部配合）

（四）平台整合共享。

10. 2017年9月底前摸清我局各类政务信息平台（系统）家底，列出清单，清理关停“不实用、可替代、已闲置”的“僵尸”信息平台（系统）。（专利局办公室牵头负责）

11. 提出平台具体建设形式和内容标准，2017年11月底前完成局政务信息平台（系统）整合共享，将局门户网站建设成为知识产权网上政务服务平台，提供一站式服务，避免重复分散建设；已经单独建设的政务服务平台（系统），应尽快在局门户网站首页设置统一入口，实现前端整合。（专利局办公室牵头负责，条法司、保护协调司、专利管理司、审查业务管理部和自动化部按职责分别负责）

12. 排查是否存在要求公众重复提交材料等情形，以及平台（系统）之间有无数据共享、业务协同等方面的障碍，尤其是在专利申请的审查及确权后相关环节、专利代理管理等方面，从而实现平台（系统）间对接联动，统一身份认证，按需共享数据，做到“单点登录、全网通办”。（条法司、审查业务管理部、初审及流程管理部、自动化部和复审委按职责分别负责）

13. 落实《政务信息资源共享管理暂行办法》的要求，按照部署和相关规定编制、维护知识产权政务信息资源目录；（专利局办公室牵头负责）积极推进向地方网上政务服务平台按需开放政务信息资源接口，促进跨地区、跨层级、跨部门互认共享。（专利局办公室牵头负责，规划发展司、自动化部配合）

14. 主动做好局网上政务服务平台与中央政府门户网站的对接。积极推进我局政务信息系统向国家电子政务内网或外网迁移，实现与国家数据共享交换平台共享数据。按《政务信息系统整合共享实施方案》的要求于每年2月底向促进大数据发展部际联席会议报告上一年度政务信息资源共享情况。（专利局办公室牵头负责，自动化部配合）

（五）强化常态监管。

15. 局门户网站作为政务服务和公开的第一平台，要不断完善信息发布机制，规范信息发布流程，避免重复审批，提高发布时效，及时归并或关闭内容更新没有保障的栏目。建立24小时值班制度，及时处理突发事件。加强协同联动，保证12小时内转载中央政府门户网站发布的重要政策信息。（专利局办公室负责）

16. 现有和新建政务服务平台应符合《“互联网+政务服务”技术体系建设指南》和《政府网站发展指引》的相关要求。各部门单位开办关停网站、微信公众号、微博、客户端等网络公开平台（下称网络公开平台）应报办公室审核。网络公开平台按照“谁主办谁负责、谁管理谁负责”的原则明确监管责任。（网络公开平台分别负责）

17. 网络公开平台应加强专题、栏目信息发布的监管，平台发布的内容不得与我国现行法律法规相冲突，提升知识产权领域原创信息的发布比例，保证信息内容的权威性和公信力，发布、转发信息时应注明信息来源、发布时间，未经核实的信息不得发布、转发；建立网站链接审批制度，严格审核把关。（网络公开平台分别负责）

18. 认真落实公文审核与保密审查同步进行的制度，对公文审批的同时对信息公开属性进行审核。信息产生部门凭保密审查依据才能发布政府信息，未经保

密审查不得发布，杜绝失泄密问题。（办公室牵头负责）

19. 按《政府网站发展指引》的要求编制政府网站监管年度报表和政务网站年度工作报表，于每年1月31日前向社会公开。（办公室牵头负责）

（六）确保平台安全。

20. 健全“互联网+政务服务”信息安全保障体系，认真落实网络安全等级保护制度，做好防攻击、防篡改、防病毒的防控措施，确保局关键信息基础设施安全。（自动化部牵头负责）

21. 修订完善网络安全管理制度，明确政务服务平台（系统）的安全责任，开展信息安全风险评估和等级保护测评等工作。健全网络安全预案，建立各方协同配合的信息安全防范、监测、通报、响应和处置机制，查补安全漏洞，做好容灾备份，提高各平台（系统）的安全防护能力。（自动化部牵头负责）

22. 加大对信息系统和涉及国家秘密、商业秘密、个人隐私等重要数据的保护力度，提升信息安全支撑保障水平和风险防范能力。（自动化部牵头负责）

（七）畅通外部监督。

23. 畅通公众监督渠道，鼓励找错纠错，优化政府网站留言收集、处理、反馈机制，进一步完善在线访谈、意见征集、网上调查等互动栏目。（办公室牵头负责，专利局办公室、规划发展司、专利管理司、审查业务管理部、自动化部和专利复审委员会分别负责）

24. 政府网站应设专人每天及时处理网民针对网站的纠错意见，在3个工作日内答复网民，除反映情况不属实等特殊情况下，所有留言办理情况均要公开。（办公室牵头负责，专利局办公室、规划发展司、专利管理司、审查业务管理部、自动化部和专利复审委员会分别负责）

三、组织保障

（一）明确组织架构。

按照国务院办公厅要求，成立局“互联网+政务服务”工作领导小组，由局

主要负责人任组长，分管政务工作的副局长和分管信息化工作的副局长任副组长，局机关各部门、专利局有关部门（专利局办公室、人事教育部、审查业务管理部、初审及流程管理部、自动化部）、及有关局属单位（专利复审委员会、知识产权出版社、专利信息中心）为成员单位，其主要负责人为组员。领导小组的职责是统筹“互联网+政务服务”工作；决定重大事项；审议涉及“互联网+政务服务”工作的重要文件等。

领导小组下设办公室，负责局“互联网+政务服务”具体事项推进工作，主要任务是建立健全工作制度及工作机制；督促工作进度；协调“互联网+政务服务”工作开展期间的人、财、物等必要保障。主任由分管政务工作的局领导担任，副主任由办公室和专利局办公室主要负责人担任，成员由有关部门单位（办公室、条法司、规划司、专利局办公室、审查业务管理部、初审及流程管理部、自动化部、复审委员会、知识产权出版社、专利信息中心）的负责人及其有关处室负责人担任。

（二）强化责任落实。

牵头部门应会同相关责任部门单位认真研究有关上级文件的要求，结合本工作方案制定各项工作任务的具体实施计划，明确责任分工、阶段任务、时间进度、负责人员及具体工作人员等内容。

具体实施计划应由牵头部门于本工作方案印发之日起10日内报领导小组办公室审核，领导小组办公室应加强对各项工作任务督促检查，定期通报工作进展，并注重发挥专家评议、第三方评估的作用，汇聚众智，改进服务。

一级 编码	信息类别	二级 编码	分类项目	公开内容	责任部门
按公文种类分类					
A01	文件发布	A0101	局令		
		A0102	局发		
		A0103	局函		
		A0104	局办发		
		A0105	局办函		
		A0106	其他		
按主题分类					
S01	政策法规	S0101	法律	由全国人大及其常委会制定并颁布的知识产权相关法律	条法司
S01	政策法规	S0102	行政法规	由国务院制定并颁布的知识产权相关行政法规	条法司
		S0103	部门规章	由市场监管总局和知识产权局颁布的部门规章	条法司
		S0104	规范性文件	除部门规章之外的知识产权相关规定、办法、通告等	局机关各部门、审查业务管理部、商标局

		S0105	政策解读	知识产权相关政策解读	局机关各部门、审查业务管理部、商标局
S02	组织机构	S0201	基本信息	局办公地址、网址、办公时间、电话、传真、电子邮箱、通讯地址、邮政编码等相关信息	办公室
		S0202	局领导	局领导简历、工作分工等相关信息	办公室、人事司
		S0203	机关职能	局职能配置、内设机构和人员编制规定	人事司
		S0204	内设机构	局机关各部门职能任务和处室设置	局机关各部门
		S0205	直属单位	专利局、商标局和其他直属单位机构设置	人事司、人教部、商标局
		S0206	社会团体	各社会团体机构设置	人事司、各社会团体
		S0207	办事机构	各地专利代办处、商标审查协作中心、商标受理窗口、商标质权登记受理点名录	初审流程部、商标局
S03	综合政务	S0301	综合事务	政务工作综合事务、财务管理、督查督办等相关信息	办公室
		S0302	政务公开	政府信息和政务公开工作信息	办公室
		S0303	电子政务及政府网站	电子政务及政府网站管理相关工作信息	办公室

		S0304	知识产权 宣传	全国知识产权宣传周、中国知识产权年会、中国专利奖评选等重大活动、中国品牌日以及新闻发布会等重要工作相关信息	办公室、运用促进司、商标局
		S0305	政策研究	软课题研究等相关信息	办公室
		S0306	其他	综合政务的其他信息	相关部门
S04	战略规划	S0401	知识产权 战略	国家知识产权战略纲要、推进计划及相关政策信息	联席办
		S0402	发展规划	知识产权事业发展规划	战略规划司
		S0403	工作要点	局年度工作要点	战略规划司
S05	知识产权 保护	S0501	保护体系	知识产权保护体系建设等相关信息	保护司
		S0502	执法信息	执法保护信息及相关数据统计、其他知识产权保护信息	保护司
S06	运用促进	S0601	行政审批 与处罚事 项	行政审批与处罚事项通知、目录等相关信息	运用促进司
		S0602	地方管理	试点示范城市、强县工程试点示范县（区）等相关信息	运用促进司
		S0603	产业促进	试点示范园区、优势示范企业等相关信息	运用促进司
		S0604	运营体系	知识产权运营服务体系建设重点城市申报通	运用促进司

				知、公示等相关信息	
		S0605	服务监管	代理机构审批、监管信息，专利代理师资格考试考务信息，知识产权服务业集聚区建设情况等等相关信息	运用促进司
		S0606	专利评奖	评选办法、评选通知、申报书、评奖公示、获奖名单等相关信息	运用促进司
S07	财政管理	S0701	财政预算	局年度预算相关信息	战略规划司
		S0702	财政决算	局年度决算相关信息	战略规划司
		S0703	收费管理	行政事业性收费和涉企收费的项目、标准等相关信息	战略规划司、运用促进司、审业部、商标局
S08	统计信息	S0801	专利统计	专利业务统计数据	战略规划司、审业部
		S0802	专利实施许可合同备案	专利实施许可合同备案统计专利数据统计、专利权质押登记信息统计	运用促进司、初审流程部
		S0803	商标统计	商标注册业务统计数据	战略规划司、商标局
		S0804	地理标志统计	地理标志保护产品、作为集体商标、证明商标注册的地理标志统计数据	战略规划司、保护司、商标局

		S0805	集成电路 布图设计	集成电路布图设计统计数据	战略规划司、初审 流程部
S09	公共服务	S0901	“放管 服”改革	知识产权领域“放管服”改革、证明事项清 单、行政许可事项清单等相关信息	公共服务司
		S0902	服务体系 建设	知识产权信息服务体系及服务平台建设等相 关信息	公共服务司
		S0903	信息传播 利用	知识产权数据开发加工制作、信息传播利用等 相关信息	公共服务司
		S0904	专利文献 服务	专利文献与信息标准、专利文献咨询、公益讲 座、专利信息传播与利用	文献部
S10	行政复议	S1001	行政复议	行政复议流程、通知等相关信息	条法司、审业部、 商标局
S11	建议提案 办理	S1101	建议提案 办理	关于全国人大代表建议和全国政协委员提案 的答复	办公室及相关答 复部门
S12	公务员招 考	S1201	公务员招 考	公务员招考计划、通知、公告等相关信息	人事司、人教部、 商标局
S13	纪检监察	S1301	廉政制度	廉洁从政制度等相关信息	机关纪委
S14	重大建设 项目	S1401	重大建设 项目	重大建设项目的批准与实施情况	战略规划司、专利 局办公室、商标局
S15	专利管理	S1501	专利申请	专利申请、审批、许可备案、质押登记、办	条法司、审业部、

				理文件副本、办理文件备案等相关的通知公告 和政策性文件信息	初审流程部
		S1502	专利公报	发明、实用新型、外观设计专利公告等相关信息	出版社
		S1503	专利复审 无效	专利复审、无效办事指南、审查决定查询、口头审理公告、无效决定公布等相关信息	复审无效部
		S1504	电子申请	通知公告（不包括临时通知）等相关信息	审业部、初审流程部
		S1505	专利合作 条约	PCT法律法规信息及PCT国际申请实务信息等	初审流程部
S16	商标管理	S1601	商标申请	商标申请、许可备案、质押登记等信息的通知公告和政策性文件信息	商标局
		S1602	商标公告	商标公告等相关信息	商标局
		S1603	商标评审	商标评审裁定、决定文书等相关信息	商标局
		S1604	电子申请	通知公告（不包括临时通知）等相关信息	商标局
		S1605	商标合作 条约	马德里商标国际注册申请指南、马德里联盟缔约方列表、指定收取单独规费国家的收费标准等相关信息	商标局
		S1606	商标代理	商标代理机构备案信息	商标局

S17	地理标志 和官方标 志管理	S1701	地理标志	地理标志通知、公告等相关信息	保护司、商标局
		S1702	官方标志	官方标志通知、公告等相关信息	保护司
		S1703	特殊标志	特殊标志通知、公告等相关信息	保护司
		S1704	奥林匹克 标志	奥林匹克标志通知、公告等相关信息	保护司
S18	集成电路 布图设计 管理	S1801	布图设计 专有权	集成电路布图设计专有权公告等相关信息	报社
		S1802	布图设计 专有权事 务	集成电路布图设计专有权事务公告等相关信 息	报社

(九) 关于印发《国家知识产权局政府信息公开实施办法（修订）》等文件的通知

(国知办发办字〔2019〕43号)

局机关各部门，专利局各部门，商标局，局其他直属单位：

为进一步规范政府信息公开工作，根据修订后的《中华人民共和国政府信息公开条例》，结合工作实际，修订《国家知识产权局政府信息公开实施办法》《国家知识产权局政府信息公开目录》《国家知识产权局政府信息公开指南》，经局批准，现予印发，请遵照执行。

特此通知。

国家知识产权局办公室

2019年11月18日

第一章 总 则

第一条 为了保障公民、法人和其他组织依法获取国家知识产权局政府信息，充分发挥政府信息对人民群众生产、生活和经济社会活动的服务作用，根据《中华人民共和国政府信息公开条例》，结合工作实际，制定本办法。

第二条 本办法所称政府信息，是指国家知识产权局在履行行政管理职责过程中制作或者获取的，以一定形式记录、保存的信息。

第三条 国家知识产权局设立政府信息与政务公开领导小组，负责全局政务信息公开和政府信息公开的组织领导工作。

领导小组在局办公室设立政府信息公开办公室（对外称国家知识产权局政府信息公开办公室，以下简称信息公开办），具体负责政府信息公开的日常工作。

信息公开办的主要职责是：

(一) 牵头办理政府信息公开事宜；指导、协调、监督各部门单位的政府信息公开工作；

(二) 维护和更新局公开的政府信息；

(三) 组织编制政府信息公开指南、政府信息公开目录和政府信息公开工作年度报告；

(四) 组织开展对拟公开政府信息的审查；

(五) 接收、批分公民、法人或者其他组织提交的政府信息公开申请，实施统一答复；

(六) 负责局政府信息与政务公开领导小组日常工作；

(七) 负责局政府信息公开的其他工作。

局机关各部门、专利局各部门、商标局应指定一名政府信息公开工作联络员，并将名单报信息公开办备案。联络员发生变动的，应于5个工作日内将新的联络人向信息公开办报备。

第四条 公开政府信息应当坚持以公开为常态、不公开为例外，遵循公正、公平、合法、便民的原则。

第五条 应当及时、准确地公开政府信息。

发现涉及知识产权的，影响或者可能影响社会稳定、扰乱社会和经济管理秩序的虚假或者不完整信息，主办部门单位应当主动或在信息公开办要求下，在职责范围内发布准确的政府信息予以澄清。

第二章 公开的主体和范围

第六条 部门单位制作的政府信息，由制作该政府信息的部门单位负责公开；从公民、法人和其他组织获取的政府信息，由保存该政府信息的部门单位负责公开；从其他行政机关获取的政府信息，由制作或者最初获取该政府信息的行政机关负责公开。法律、法规对政府信息公开的权限另有规定的，从其规定。

国家知识产权局与其他行政机关共同制作的政府信息，由牵头制作的行政机关负责公开。

第七条 建立健全政府信息公开协调机制。公开政府信息涉及其他机关的，应当与有关机关协商、确认，保证行政机关公开的政府信息准确一致。

公开政府信息依照法律、行政法规和国家有关规定需要批准的，经批准予以公开。

第八条 依法确定为国家秘密的政府信息，法律、行政法规禁止公开的政府信息，以及公开后可能危及国家安全、公共安全、经济安全、社会稳定的政府信息，不予公开。

第九条 涉及商业秘密、个人隐私等公开会对第三方合法权益造成损害的政府信息，不得公开。但是，第三方同意公开或者国家知识产权局认为不公开会对公共利益造成重大影响的，予以公开。

第十条 局人事管理、后勤管理、内部工作流程等方面的内部事务信息，可以不予公开。

在履行行政管理职能过程中形成的讨论记录、过程稿、磋商信函、请示报告等过程性信息以及行政执法案卷信息，可以不予公开。法律、法规、规章规定上述信息应当公开的，从其规定。

第十一条 依照《中华人民共和国保守国家秘密法》以及其他法律、法规和国家有关规定，遵循“谁制作、谁公开”和“先审查、后公开”原则，政府信息公开保密审查程序与公文运转程序、信息发布程序相结合，发布政府信息应提供保密审查依据。

部门单位在制作政府信息时，应当确定该信息是否公开及公开范围、公开内容是否需要删减。对不能确定是否公开及公开范围的政府信息，应当报信息公开办审核，必要时报政府信息与政务公开领导小组审批。

国家知识产权局不能确定政府信息是否可以公开的，应当依照法律、法规和

国家有关规定报有关主管部门或者保密行政管理部门确定。

第十二条 建立健全政府信息管理动态调整机制，信息公开办和部门单位应对不予公开的政府信息进行定期评估审查，对因情势变化可以公开的政府信息应当公开。

第三章 主动公开

第十三条 对涉及公众利益调整、需要公众广泛知晓或者需要公众参与决策的政府信息应当主动公开。应当主动公开下列政府信息：

- (一) 行政法规、规章和规范性文件；
- (二) 机关职能、机构设置、办公地址、办公时间、联系方式、负责人姓名；
- (三) 国家知识产权局发展规划及相关政策，重要工作部署及实施情况；
- (四) 《中华人民共和国专利法》及其实施细则规定在专利申请、审批及复审、无效等程序中应当对外公开的信息；
- (五) 《中华人民共和国商标法》及其实施条例规定在商标申请、审查、异议及驳回复审、无效等程序中应当对外公开的信息；
- (六) 专利代理机构的审批决定、全国专利代理师资格考试的有关政策、规定；商标代理的备案信息；
- (七) 知识产权年度统计信息；
- (八) 办理行政许可和其他对外管理服务事项的依据、条件、程序以及办理结果；
- (九) 实施行政处罚、行政强制的依据、条件、程序以及本部门单位认为具有一定社会影响的行政处罚决定；
- (十) 财政预算、决算信息；
- (十一) 行政事业性收费和涉企收费项目及其依据、标准；

- (十二) 重大建设项目的批准和实施情况;
- (十三) 公务员招考的职位、名额、报考条件等事项以及录用结果;
- (十四) 法律、法规、规章和国家有关规定规定应当主动公开的其他政府信息。

第十四条 局政府信息主要按以下方式公开:

- (一) 政府门户网站, 政务微博, 政务微信公众号;
- (二) 国家知识产权局公报、文告、主管报刊等;
- (三) 新闻发布会;
- (四) 国家知识产权局业务受理大厅、商标注册大厅、客户服务中心;
- (五) 其他可以公开政府信息的方式。

第十五条 属于主动公开范围的政府信息, 由制作该政府信息的部门单位自该政府信息形成或者变更之日起20个工作日内及时公开。法律、法规对政府信息公开的期限另有规定的, 从其规定。

第四章 依申请公开

第十六条 对于公民、法人或者其他组织提出的公开申请, 经审查符合受理条件, 由信息公开办会同相关部门单位对其申请进行答复, 信息公开办负责将答复结果告知申请人。

第十七条 对于内容不明确的政府信息公开申请, 应当给予指导和释明, 并自收到申请之日起7个工作日内一次性告知申请人作出补正, 说明需要补正的事项和合理的补正期限。答复期限自收到补正的申请之日起计算。申请人无正当理由逾期不补正的, 视为放弃申请, 不再处理该政府信息公开申请。

第十八条 收到政府信息公开申请的时间, 按照下列规定确定:

- (一) 申请人当面提交政府信息公开申请的, 以提交之日为收到申请之日;

(二) 申请人以邮寄方式提交政府信息公开申请的，以局签收之日为收到申请之日；以平常信函等无需签收的邮寄方式提交政府信息公开申请的，信息公开办应当于收到申请的当日与申请人确认，确认之日为收到申请之日；

(三) 申请人通过互联网渠道提交政府信息公开申请的，信息公开办在收到申请的当日以电子邮件形式与申请人确认，确认之日为收到申请之日。

第十九条 部门单位收到信息公开办转交的政府信息公开申请后，应当在规定时限内反馈答复意见；如认为依据职责或分工不应由本部门单位答复的，应当在2个工作日内商信息公开办解决。

第二十条 依申请公开的政府信息公开会损害第三方合法权益的，负责承办的部门单位需书面征求第三方的意见。第三方应当自收到征求意见书之日起15个工作日内提出意见。第三方逾期未提出意见的，由国家知识产权局依照《中华人民共和国政府信息公开条例》的规定决定是否公开。第三方不同意公开且有合理理由的，国家知识产权局不予公开。国家知识产权局认为不公开可能对公共利益造成重大影响的，可以决定予以公开，并将决定公开的政府信息内容和理由书面告知第三方。

第二十一条 对收到的政府信息公开申请能够当场答复的，应当当场予以答复。

不能当场答复的，应当自收到申请之日起20个工作日内予以答复；需要延长答复期限的，应当经信息公开办负责人同意并告知申请人，延长的期限最长不得超过20个工作日。

征求第三方和其他机关意见所需时间不计算在前款规定的期限内。

第二十二条 申请公开的政府信息由国家知识产权局牵头与其他行政机关共同制作的，国家知识产权局收到政府信息公开申请后应当征求相关行政机关的意见，被征求意见机关应当自收到征求意见书之日起15个工作日内提出意见，逾期未提出意见的视为同意公开。

第二十三条 申请人申请公开政府信息的数量、频次明显超过合理范围，信

信息公开办可以要求申请人说明理由。信息公开办认为申请理由不合理的，告知申请人不予处理；认为申请理由合理，但是无法在20个工作日内答复申请人的，可以确定延迟答复的合理期限并告知申请人。

第二十四条 对政府信息公开申请，根据下列情况分别作出答复：

（一）所申请公开信息已经主动公开的，告知申请人获取该政府信息的方式、途径；

（二）所申请公开信息可以公开的，向申请人提供该政府信息，或者告知申请人获取该政府信息的方式、途径和时间；

（三）依据《中华人民共和国政府信息公开条例》的规定决定不予公开的，告知申请人不予公开并说明理由；

（四）经检索没有所申请公开信息的，告知申请人该政府信息不存在；

（五）所申请公开信息不属于本行政机关负责公开的，告知申请人并说明理由；能够确定负责公开该政府信息的行政机关的，告知申请人该行政机关的名称、联系方式；

（六）已就申请人提出的政府信息公开申请作出答复、申请人重复申请公开相同政府信息的，告知申请人不予重复处理；

（七）所申请公开信息属于工商、不动产登记资料等信息，有关法律、行政法规对信息的获取有特别规定的，告知申请人依照有关法律、行政法规的规定办理。

第二十五条 申请公开的信息中含有不应当公开或者不属于政府信息的内容，但是能够作区分处理的，应当向申请人提供可以公开的政府信息内容，并对不予公开的内容说明理由。

第二十六条 向申请人提供的信息，应当是已制作或者获取的政府信息。除能够作区分处理的外，需要对现有政府信息进行加工、分析的，可以不予提供。

第二十七条 申请人以政府信息公开申请的形式进行信访、投诉、举报、业

务咨询等活动，应当告知申请人不作为政府信息公开申请处理并可以告知通过相应渠道提出。

申请人提出的申请内容为要求提供政府公报、报刊、书籍等公开出版物的，可以告知获取的途径。

第二十八条 依申请公开政府信息，应当根据申请人的要求及局保存政府信息的实际情况，确定提供政府信息的具体形式；按照申请人要求的形式提供政府信息，可能危及政府信息载体安全或者公开成本过高的，可以通过电子数据以及其他适当形式提供，或者安排申请人查阅、抄录相关政府信息。

第二十九条 公民、法人或者其他组织有证据证明国家知识产权局提供的与其自身相关的政府信息记录不准确的，可以要求更正。局有权更正且审核属实的，应当予以更正并告知申请人；不属于局职能范围的，将转送有权更正的行政机关处理并告知申请人，或者告知申请人向有权更正的行政机关提出。

第三十条 依申请提供政府信息，不收取费用。但是申请人申请公开政府信息的数量、频次明显超过合理范围的，可根据国务院有关规定收取信息处理费。

第三十一条 申请公开政府信息的公民存在阅读困难或者视听障碍的，应当为其提供必要的帮助。

第三十二条 多个申请人就相同政府信息提出公开申请，且该政府信息属于可以公开的，应当将其纳入主动公开的范围。信息公开办应指导、督促制作该政府信息的部门单位调整信息公开属性。

对依申请公开的政府信息，申请人认为涉及公共利益调整、需要公众广泛知晓或者需要公众参与决策的，可以建议将该信息纳入主动公开的范围。经信息公开办审核认为属于主动公开范围的，应当及时主动公开，并指导、督促制作该政府信息的部门单位调整信息公开属性。

第五章 监督与保障

第三十三条 建立政府信息公开工作考核制度、社会评议制度和责任追究制

度，定期对政府信息公开工作进行考核、评议。

第三十四条 信息公开办应当加强对政府信息公开工作的日常指导和监督检查，对未按照要求开展政府信息公开工作的部门，予以督促整改或者通报批评；需要对负有责任的部门单位负责人和直接责任人追究责任的，依法向机关纪委提出处理建议。

公民、法人或者其他组织认为国家知识产权局未按照要求主动公开政府信息或者对政府信息公开申请不依法答复处理的，可以向信息公开办提出。经查证属实的，将对负有责任的部门单位予以督促整改或者通报批评。

第三十五条 部门单位应当在每年1月5日前向信息公开办报送上一年度工作情况。国家知识产权局应当在每年1月31日前向国务院政府信息公开工作主管部门提交上一年度政府信息公开工作年度报告并向社会公布。

第三十六条 部门单位年度报告应当包括下列内容：

- （一）局年度政务公开工作要点各项工作落实情况；
- （二）主动公开政府信息情况；
- （三）政府信息公开工作存在的主要问题及改进情况、工作建议等；
- （四）其他需要报告的事项。

第三十七条 政府信息公开工作年度报告应当包括下列内容：

- （一）主动公开政府信息的情况；
- （二）收到和处理政府信息公开申请的情况；
- （三）因政府信息公开工作被申请行政复议、提起行政诉讼的情况；
- （四）政府信息公开工作存在的主要问题及改进情况，工作考核、社会评议和责任追究结果情况；
- （五）其他需要报告的事项。

第三十八条 部门单位违反《中华人民共和国政府信息公开条例》和本办法的规定，有下列情形之一的，由信息公开办责令改正；情节严重的，对负有责任的领导人员和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：

（一）不依法履行政府信息公开职能；

（二）不及时更新公开的政府信息内容、政府信息公开指南和政府信息公开目录；

（三）违反《中华人民共和国政府信息公开条例》规定的其他情形。

第六章 附 则

第三十九条 本办法适用于局机关、专利局、商标局，局其他直属单位参照执行。

第四十条 本办法由国家知识产权局办公室负责解释。

第四十一条 本办法自印发之日起实施。原《国家知识产权局政府信息公开实施办法》同时废止。

国家知识产权局政府信息公开指南

为便利社会公众向本机关获取政府信息，规范政府信息公开申请提交和接收行为，根据《中华人民共和国政府信息公开条例》有关规定，本机关编制政府信息公开指南并实时更新。

一、本机关持有政府信息基本情况

根据《国家知识产权局职能配置、内设机构和人员编制规定》，本机关负责拟订和组织实施国家知识产权战略、保护知识产权、促进知识产权运用、知识产权的审查注册登记和行政裁决、建立知识产权公共服务体系、负责统筹协调涉外知识产权事宜、完成党中央、国务院交办的其他任务等工作。

在履行职责过程中，本机关会产生并保存以下18类政府信息：政策法规、组织机构、综合政务、战略规划、知识产权保护、运用促进、财政管理、统计信息、

公共服务、行政复议、建议提案办理、公务员招考、纪检监察、重大建设项目、专利管理、商标管理、地理标志和官方标志管理、集成电路布图设计管理等。如需了解详细情况，请点击国家知识产权局政府信息公开目录链接。

二、本机关对外发布政府信息情况

（一）本机关对外发布政府信息的渠道

1. 国家知识产权局政府门户网站。网址为：www.cnipa.gov.cn。
2. 国家知识产权局公报。获取地址为：国家知识产权局政府门户网站-政务-概况-局公报栏目。
3. 新闻发布会。每年1月、4月、7月、10月召开例行新闻发布会，地点在国家知识产权局；每年4月全国知识产权宣传周期间，在国新办召开新闻发布会，发布上一年度我国知识产权发展状况；同时，将根据知识产权重大工作进展适时召开。新闻发布会的相关情况获取地址为：国家知识产权局政府门户网站-政务-新闻发布栏目。
4. 国家知识产权局业务受理大厅。地址为：北京市海淀区西土城路6号东门。
5. 国家知识产权局商标局商标注册大厅。地址为：北京市西城区茶马南街1号。
6. 本机关还通过报刊、广播、电视、政务微博、政务微信公众号、公益咨询活动等方式发布我局的政府信息。

（二）本机关的官方出版物

1. 国家知识产权局年报。获取地址为：国家知识产权局政府门户网站-政务-概况-年度报告栏目。
2. 中国知识产权年鉴。获取方式为：各大网上书店、新华书店及相关专业书店，发行电话010-82000860转8101/8102。
3. 中国知识产权保护状况白皮书。获取地址为：国家知识产权局政府门户

网站-政务-概况-白皮书栏目。

（三）本机关的业务公告

1. 专利公报。获取地址为：国家知识产权局政府门户网站-专利公报栏目。
2. 商标公告。获取地址为：国家知识产权局政府门户网站-商标-商标公告栏目。
3. 地理标志和官方标志公告。获取地址为：国家知识产权局政府门户网站-地理标志和官方标志公告栏目。
4. 集成电路公告。获取地址为：国家知识产权局政府门户网站-集成电路公告栏目。

三、政府信息公开申请渠道

申请人向本机关提出政府信息公开申请，应当填写《国家知识产权局政府信息公开申请表》（网络平台提交时采取在线填写方式），通过以下方式向本机关提交：

（一）当面提交。联系人：国家知识产权局信访室，地址：北京市海淀区西土城路6号西门，联系电话：010-62083357，受理时间：工作日上午9：00-11：00，下午2：00-4：30。

（二）邮政寄送。收件人：国家知识产权局政府信息公开办公室；地址：北京市海淀区西土城路6号；邮编：100088。请在信封左下角注明“政府信息公开申请”字样。

（三）网络平台提交。请登录国家知识产权局政府门户网站-信息公开-依申请公开栏目在线提交。

本机关暂不受理通过电话、传真、电子邮件方式提出的申请。

四、政府信息公开工作机构情况

本机关政府信息公开工作机构为信息公开办，办公地址为：北京市海淀区西

土城路6号。有关本机关政府信息公开工作的意见建议，请联系010-62085311。

五、其他事项

（一）确认申请时间

1. 申请人当面提交政府信息公开申请的，以提交之日为收到申请之日；
2. 申请人以邮寄方式提交政府信息公开申请的，以本机关签收之日为收到申请之日；以平常信函等无需签收的邮寄方式提交政府信息公开申请的，本机关将于收到申请的当日与申请人确认，确认之日为收到申请之日；
3. 申请人通过网络平台提交政府信息公开申请的，本机关将在收到申请的当日以电子邮件形式与申请人确认，申请人收到邮件即为收到申请之日。

（二）答复申请时限

本机关收到政府信息公开申请，能够当场答复的，将当场予以答复。不能当场答复的，将于收到申请之日起20个工作日内予以答复；需要延长答复期限的，经批准后将告知申请人，延长的期限最长不超过20个工作日。

本机关征求第三方和其他机关意见所需时间不计算在前款规定的期限内。

(十) 人力资源社会保障部办公厅关于加快推进流动人员人事档案信息化建设的指导意见

(人社厅发〔2018〕102号)

各省、自治区、直辖市及新疆生产建设兵团人力资源社会保障厅(局), 各副省级城市人力资源社会保障局:

加快推进流动人员人事档案(以下简称档案)信息化建设, 是提升档案管理服务的基础工程, 是进一步简化优化档案管理服务的重要抓手。为落实《国务院关于印发<“十三五”推进基本公共服务均等化规划>的通知》(国发〔2017〕9号)、《国务院关于积极推进“互联网+”行动的指导意见》(国发〔2015〕40号)和《人力资源社会保障部关于印发“互联网+人社”2020行动计划的通知》(人社部发〔2016〕105号)等文件要求, 现就加快档案信息化建设提出如下意见。

一、总体要求

(一) 指导思想。以习近平新时代中国特色社会主义思想为指导, 坚持党管干部、党管人才原则, 全面贯彻落实党中央、国务院关于推进审批服务便民化的决策部署, 紧紧围绕深入实施人才强国战略和就业优先战略、加快推进“互联网+政务服务”的要求, 以服务用人单位和流动人员为中心, 以推动档案管理服务与信息技术、互联网技术深度融合为目标, 以“金保工程”项目建设为依托, 按照“数据向上集中、服务向下延伸、信息全国共享”的原则, 构建省级集中、全国联通的档案管理服务信息化格局, 实现档案管理服务信息化、标准化、便民化, 为提升档案公共服务能力、提高服务质量和效率提供基础保障。

(二) 基本原则。档案信息化建设应遵循以下基本原则:

坚持统筹规划, 统一标准。档案信息化建设是人力资源社会保障信息化建设的组成部分, 全国统一规划, 统筹推进。按照人力资源社会保障信息系统技术标准体系和相关工作要求, 建设统一的档案信息系统, 确保信息系统的规范性、开

放性、互融性。

坚持业务协同，信息共享。以制定部级统一规范、推进省级集中建设、实现全国联网共享为重点，减少信息孤岛，实现跨地区、跨层级业务协同以及数据交换。简化优化档案管理服务流程，升级再造信息系统，推动与人力资源社会保障领域相关信息系统之间的数据共享和业务协同。

坚持分类指导，安全有序。结合各地档案工作实际和信息化建设水平，指导制定科学合理的信息化建设工作方案，分类指导，有重点、分步骤逐步推进。注重信息安全和个人隐私保护，采取切实有效的安全防护措施，增强系统支撑能力，保证系统安全平稳运行。

(三) 工作目标。利用3年左右时间，开发统一便捷的省级档案管理服务信息系统，建设互联互通的全国档案管理服务运行平台，建立规范完整的全国档案基础信息资源库，推动档案数字化进程，满足档案管理服务在信息管理、公共服务、宏观决策等方面的要求。加快推进“互联网+公共服务”，运用大数据等新技术，打破档案信息孤岛，强化部门内外信息共享，推动协同联动，“让数据多跑路，群众少跑腿”，提升档案管理服务整体效能。

二、重点任务

(一) 统一全国档案信息化建设标准。

统一档案基本公共服务经办规范。各级人力资源社会保障部门要按照《流动人员人事档案基本公共服务经办规范》（附件1），组织档案管理服务机构梳理、细化档案公共服务经办流程，推进办事材料目录化、标准化，实现全国档案公共服务同一事项、同一流程、同一标准、同一格式。

统一档案基础信息采集规范。各级人力资源社会保障部门要组织档案管理服务机构按照《流动人员人事档案基础信息采集规范》（附件2），统一采集项目、统一指标体系、统一代码，开展档案基础信息采集工作。

统一档案数字化技术规范。鼓励和支持有条件的地区或档案管理服务机构积极开展档案数字化工作，参照《干部人事档案数字化技术规范》（GB/T

33870-2017) , 逐步建立统一规范的数字档案资源库。

(二) 建立全国统一的档案管理服务信息系统。

开发应用统一的省级档案管理服务软件。依托“金保工程”二期项目, 组织开发全国统一的软件支撑省级档案管理服务, 为各地推动档案信息化工作提供支持。省级人力资源社会保障部门要结合本地实际, 基于上述统一软件建设省级集中的档案管理服务信息系统, 支持辖区内档案管理机构开展档案基础信息采集和档案管理服务业务经办工作, 建立省级档案基础信息资源库。已建立省级集中的档案管理服务信息系统的省份, 要结合系统改造等时机逐步过渡到统一软件。

建立全国档案基础信息资源库。研究开发全国档案基础信息归集平台, 在省级档案基础信息资源库基础上, 按照“数据向上集中”的思路, 建立档案信息采集上报机制, 定期归集各地档案基础信息, 逐步过渡到实时归集, 在部级建立形成全国档案基础信息资源库, 为实现全国服务提供数据基础。

开发全国档案管理服务运行平台。基于全国档案基础信息资源库, 开发建立全国档案管理服务运行平台, 提供存档信息网上查询服务, 为流动人员和用人单位查询档案存放信息提供便利。积极推动跨地区网上远程经办模式, 逐步形成“一点存档、多点服务”的全国一体化服务格局。

(三) 推动档案数字化。支持有条件的地区开展纸质档案扫描、图像处理、数据存储备份等工作, 逐步建立数字档案资源库, 为档案“一窗式办理”提供基础。数字档案保存、上传和交换工作必须通过业务专网完成。数字档案原则上实行地市级管理, 有条件的地方可省级集中管理。

(四) 加强档案信息应用和共享。地方各级人力资源社会保障部门要充分利用档案管理服务信息系统形成的数据资源, 对流动人员数量、结构、分布、流向等开展统计分析, 逐步建立档案基本情况统计分析制度。强化档案数据资源与政务数据资源的关联分析和融合利用, 建立与人力资源社会保障持卡人员基础信息库、单位基础信息库等基础信息库的关联, 实现与就业创业、社会保障、人事人

才、劳动关系等业务信息共享，推动与教育、公安、民政、卫生健康、工商等部门资源数据互认。

三、保障支撑

（一）强化技术支持。各级人力资源社会保障部门要加强技术支持，积极探索“互联网+”模式，通过开通网上申请、后台审核、网上反馈或预约现场办理等，逐步推进档案管理服务线下向线上延伸。大力推广电子证明、电子公文、电子签章等新技术应用，提高档案管理服务的科学化和便民化水平。

（二）完善网络基础设施。各级人力资源社会保障部门要加快通信基础设施建设，实现业务专网覆盖档案管理服务机构，高速优质互联网支持档案线上经办服务。充分依托现有网络资源，为线上档案管理服务提供支撑和保障。

（三）规范安全管理。各级人力资源社会保障部门要严格按照国家信息安全等级保护制度要求，加强档案信息化安全建设。落实信息安全等级保护制度，严格做好业务专网和互联网的安全隔离，做好省级档案管理服务信息系统的应用级容灾和数据备份。建立系统安全测试、备案制度，未通过安全测试、未实行备案的档案管理服务信息系统，一律不准与全国档案基础信息资源库衔接。

四、组织实施

（一）加强组织领导。各地人力资源社会保障部门要高度重视档案信息化建设工作，将其纳入本地人力资源社会保障信息化工作总体安排，统筹规划，优先推进。省级人力资源社会保障部门要按照本指导意见要求，结合工作实际，尽快制定本地档案信息化建设工作方案，明确具体建设内容、责任主体、工作要求和完成时限。各级人力资源社会保障部门负责人力资源市场建设的行政机构主要负责档案信息化工作的统筹规划、牵头推进和督促指导，信息化综合管理机构主要负责系统规划、建设和实施，负责提供技术支持；档案管理服务机构主要负责系统建设的业务支持、具体推进。各有关机构要密切配合，通力合作，共同做好档案信息化建设工作。

（二）提供有效保障。各地人力资源社会保障部门要积极协调同级财政、发

展改革等部门，多渠道解决档案信息化建设所需经费。按照“金保工程”二期建设规划、“十三五”推进基本公共服务均等化规划等文件规定，统筹运用好“金保工程”二期项目资金、基本公共服务经费、就业补助资金、人才发展资金等，多渠道筹措系统建设和维护经费。加强对信息技术人员和业务人员的培训，确保档案信息系统在档案管理服务工作中的应用效果。

（三）明确时间要求。2018年底前，依托“金保工程”二期项目建设研究开发全国统一软件，支撑省级档案管理服务，研究全国档案基础信息归集平台、全国档案管理服务运行平台建设方案。

2019年底前，在全国范围内推广应用统一的省级档案管理服务软件，各地初步建立省级集中的档案基础信息资源库。启动全国档案基础信息归集平台和档案管理服务运行平台建设；建立全国档案基础信息归集机制。

2020年底前，进一步完善省级集中的档案基础信息资源库。依托档案基础信息归集平台，建立全国档案基础信息资源库，基本实现各级公共就业和人才服务机构档案信息采集和归集工作。建立全国档案管理服务运行平台，初步实现档案存档信息网上查询服务。

（四）强化督促检查。省级人力资源社会保障部门要抓好本地信息化建设工作方案的贯彻落实，加强工作指导和督促，确保上下联动，按时间节点推进工作，确保如期完成。要将本地档案信息化建设工作方案于2018年12月底前报我部人力资源市场司备案，同时抄送部信息中心和全国人才流动中心。今后每年年底前报送档案信息化建设工作推进情况和下一年度工作计划。我部将通过业务培训、经验交流、情况通报、专项督查、随机抽查等方式，加强对各地的工作指导和督促检查。

附件：1.流动人员人事档案基本公共服务经办规范

2.流动人员人事档案基础信息采集规范

人力资源社会保障部办公厅

2018年9月20日

(十一) 国家税务总局关于印发《全面推进政务公开工作实施办法》的通知

(税总发〔2017〕44号)

各省、自治区、直辖市和计划单列市国家税务局、地方税务局，局内各单位：

现将《全面推进政务公开工作实施办法》印发给你们，请结合实际遵照执行。

国家税务总局

2017年4月27日

为贯彻落实中共中央办公厅、国务院办公厅《关于全面推进政务公开工作的意见》（中办发〔2016〕8号）和国务院办公厅《〈关于全面推进政务公开工作的意见〉实施细则》（国办发〔2016〕80号），根据《国家税务总局关于全面推进政务公开工作的意见》（税总发〔2016〕50号），结合税务部门工作实际，制定本实施办法。

一、政务公开工作总体要求

（一）指导思想。深入推进依法行政，全面落实党中央、国务院有关政务公开决策部署和政府信息公开条例，坚持以公开为常态、不公开为例外，全面推进决策、执行、管理、服务、结果全过程公开（以下统称“五公开”），加强政策解读、回应社会关切、推进公开平台建设，保障公众知情权、参与权、表达权和监督权，增强税务部门公信力和执行力，提升税务部门治理能力。

（二）基本原则。紧紧围绕经济社会发展和人民群众关注关切，以公开促落实，以公开促规范，以公开促服务。依法依规明确税务部门政务公开的主体、内容、标准、方式、程序，加快推进权力和责任清单公开。坚持改革创新，注重精细化、可操作性，务求公开实效，让群众看得到、听得懂、能监督。以社会需求为导向，以新闻媒体为载体，推行“互联网+政务服务”，扩大公众参与，促进税务系统政务公开。

(三) 主要任务。贯彻落实“五公开”相关要求，除依法应当保密外，全面加大税务行政权力公开力度，做好税收政策法规公开，完善税收征管及税收执法公开内容，规范纳税服务公开范围，推进税务机关自身建设公开，加强政务公开全过程管理，规范税收政策解读，积极回应社会关切，推进政务公开平台建设，扩大社会公众参与，强化政务公开组织保障，不断提升税务部门政务公开水平。

(四) 工作目标。到2020年，税务部门政务公开工作总体迈上新台阶，公开内容覆盖税务行政权力运行全流程、税收征管和纳税服务全过程、税务机关自身建设全方位，政务公开制度化、标准化、信息化水平显著提升，以更加公开透明赢得社会公众更多理解、信任和支持。

二、加大税务行政权力公开力度

(一) 推进权力责任清单公开。落实国务院部门权力和责任清单编制试点决策部署，做好税务总局权责事项的梳理、清理规范和审核确认，形成税务总局基础权责清单，编制权责事项运行流程图，明确每个环节的承办机构、办理要求、办理时限等，及时向社会公开发布。建立权责清单动态管理机制，权责清单或权力运行流程图发生变化时及时更新并向社会公开发布。（政策法规司牵头落实）

(二) 推进税务行政许可公开。全面公开税务行政许可目录及指南，税务部门将税务行政许可的事项、依据、条件、数量、程序、期限以及需要提交的全部材料的目录、申请书示范文本和服务指南等在办税服务厅、税务网站予以公示，并及时做好动态调整。推进税务行政许可受理、办理进展等事项公开，提高税务行政许可办理透明度。做好行政许可决定的公示，除涉及国家秘密、商业秘密或个人隐私及其他依法不予公开的事项外，对准予税务行政许可决定书文号、项目名称、许可内容、行政相对人统一社会信用代码和许可部门等信息，各级税务机关在作出行政许可决定之日起7个工作日内完成公示。（政策法规司牵头，会同相关司局落实）

(三) 推进税务决策信息公开。对涉及纳税人切身利益、需要社会广泛知晓的征管改革、重大措施等事项的决策，除依法应当保密的外，应把公众参与、专家论证、风险评估、合法性审查、集体讨论决定确定为必经程序。在决策前应向

社会公布决策草案、决策依据，通过多渠道、全方位广泛听取各方面意见，以适当方式公布意见收集和采纳情况。决策作出后，及时全面公开决策议定事项和相关文件。（办公厅牵头，会同各司局落实）

三、做好税收政策法规公开

（一）推进政策法规内容公开。主动公开税务部门履职相关的法律、法规、规章、规范性文件，加强全国税收法规库建设，及时做好更新维护。全面公开促进深化改革、经济发展、民生改善的税收政策措施，特别是对新出台的减税降负政策措施，以及促进创业创新、保障和改善民生等税收优惠政策做好在网站发布、新媒体推送等工作，及时发布多边税收条约、避免双重征税协定、税收情报交换协定等国际税收协定。做好税收个案批复类文件公开，税收个案批复应当自作出之日起30日内，由批复机关的办公厅（室）在本级政府公报、税务机关公报、本辖区范围内公开发行的报纸或本级政府网站、本税务机关网站上公布。（政策法规司、办公厅牵头，会同相关司局落实）

（二）推进政策落实情况公开。主动公开重大政策的贯彻落实情况，重点做好政府工作报告、政府决定事项等落实情况的公开，明确执行措施、实施步骤、责任分工、监督方式，及时公布阶段成果和后续举措，确保落实到位。做好督查发现问题及整改落实情况以及对不作为、慢作为、乱作为问责情况的公开，增强抓落实的执行力。建立健全重大税收政策跟踪反馈和评估制度，注重运用第三方评估、专业机构鉴定、社情民意调查等方式，科学评估政策实施情况，全面评价政策落实效果。（办公厅牵头，会同各司局落实）

（三）推进政策清理情况公开。加大税收规章、规范性文件清理工作力度，形成文件清理长效机制。制定机关及时发布清理结果，方便社会公众查阅获取。及时在税务网站等平台上做好文件、条款的时效性标注。税务总局不定期抽查税收政策的时效性标注情况。（政策法规司、办公厅牵头，会同各司局落实）

四、完善税收征管及税收执法公开内容

（一）推进征管改革措施公开。深入贯彻《深化国税、地税征管体制改革方

案》，加大对转变税收征管方式相关措施的公开，加强事中事后管理，及时发布国税地税联合办税、纳税人分类分级管理、大企业税收管理、自然人税收管理体系等事项，重大修订事项提前在税务网站向社会公布，及时公布各项改革措施落实情况。（征管和科技发展司牵头，会同所得税司、财产和行为税司、大企业税收管理司等司局落实）

（二）推进税收数据信息公开。税务总局参与政府数据统一开放平台建设，省以上税务机关制定税收数据开放目录，优先推动民生保障、公共服务和市场监管等领域的税收数据向社会有序开放，鼓励公众、企业和社会机构开发利用。加大税收征管事项公开，主动公开纳税信用A级纳税人名单及相关信息，省以下税务机关及时发布欠税公告、非正常户公告、个体工商户定额公示（公布）公告、税务登记证件失效公告、限期申报公告、限期纳税公告、委托代征公告等。（收入规划核算司、征管和科技发展司、纳税服务司牵头，会同相关业务司局落实）

（三）推进税收执法信息公开。推行行政执法公示制度，依法及时主动向社会公开有关税收执法信息，税务人员在执法过程中要主动表明身份，接受社会监督。加大执法依据、执法过程、处理结果等税收执法信息公开。推进税务稽查随机抽查相关事项公开，向社会发布税务稽查随机抽查的依据、主体、内容、方式等事项清单。按照规定的标准和流程，做好重大税收违法案件信息公布。作出税务处理、行政处罚决定的税务机关，在案件复议诉讼期间届满或经复议诉讼最终确定效力后次月10日内，在省税务机关门户网站完成公布。（政策法规司、稽查局牵头落实）

五、规范纳税服务公开范围

（一）推进纳税人权利义务公开。积极宣传纳税人的权利和义务，重点宣传纳税人享有的申请减免税、延期申报纳税、申请行政复议、提起行政诉讼、检举和取得赔偿等权利，使纳税人全面、准确了解其法定权利和义务。公开税收执法过程中有关回避、听证等程序，保障纳税人在接受税收执法过程中的各项法定权利。（纳税服务司牵头，会同相关司局落实）

（二）推进重大服务举措公开。加大公开首问责任制、限时办结制、预约办

税制、延时服务制和24小时自助办税等便民办税服务措施。对“便民办税春风行动”、纳税服务规范、国税地税合作工作规范、出口退税工作规范等重大服务举措进行广泛宣传和深入解读。（纳税服务司牵头，会同相关司局落实）

（三）推进办税服务公开。全面公开办税服务事项，编制发布办税指南，简化优化办税流程，推行办税事项“二维码”一次性告知措施，方便纳税人办理涉税事项。依托纳税服务规范，及时更新税务网站办税指南、表证单书、软件下载等信息内容。及时发布办税日历、办税地图及服务通知等，积极为纳税人提供办税便利。拓展涉税查询功能，向社会公众提供发票信息、企业纳税信用等级等涉税信息查询服务。（纳税服务司牵头落实）

六、推进税务机关自身建设公开

（一）推进机构职能信息公开。主动公开机构设置、主要职能、本级概况等信息。加强领导信息公开，及时发布领导照片、简介、履历、分管工作等信息内容，公开内设机构负责人姓名信息。加大人事管理信息公开力度，在各级国税局机关网站上发布本级国税机关中层以上领导干部及直属单位、下一级国税机关领导班子成员任职信息。做好对外联系电话公开，及时公开纳税咨询投诉、税收违法举报、税务干部违纪举报、政府信息公开等电话信息。（人事司、办公厅牵头，会同相关司局落实）

（二）推进财政资金信息公开。税务总局及时公开国税系统经批准的预算、决算及相关文字说明，包括收入支出预算表、收入支出决算表等。部门预决算支出全部公开到功能分类款级科目，按规定公开到经济分类科目。做好“三公”经费预决算公开，公开的决算应当说明因公出国（境）团组数及人数，公务用车购置数及保有量，国内公务接待的批次人数，及“三公”经费增减变化原因等信息。（财务管理司牵头落实）

（三）推进其他政务信息公开。每年3月31日前在税务网站上发布政府信息公开年度报告。定期发布税收收入统计信息，方便社会公众查阅。做好涉税安全管理信息公开，建立预警预防信息发布和事故应急处置救援信息公开机制。按照政府采购法律法规及相关规定，做好政府采购制度、采购文件、中标或成交结果、

采购合同等公开。（办公厅、采购中心牵头落实）

七、加强政务公开全过程管理

（一）公文公开管理。各级税务机关拟制公文时，明确主动公开、依申请公开、不予公开等属性，随公文一并报批，拟不公开的，依法依规说明理由。对拟不公开的政策性文件，报批前先送本单位政务公开工作机构审查。办公厅（室）在对公文进行发文审核时，加强对公文公开属性的复核，对没有明确公开属性的，或者没有依法依规说明不公开理由的，办公厅（室）作退文处理。（办公厅牵头，会同各司局落实）

（二）会议公开管理。税务总局及省税务机关应在2017年底前，建立公众代表、专家、媒体、利益相关方等列席有关会议的制度，出台管理办法，增强决策透明度。提交会议讨论的重要改革方案和重大政策措施，应在决策前广泛听取公众意见，并将听取意见情况一并提交讨论。对涉及重大决策事项的会议议题，在制定会议方案时，应提出是否邀请有关方面人员列席会议、是否公开以及公开方式的意见，随会议方案一同报批；之前已公开征求意见的，应附意见收集和采纳情况的说明。（办公厅牵头，会同各司局落实）

（三）主动公开目录管理。全面梳理税务部门“五公开”内容、主体、时限、方式等，税务总局于2017年底前修订主动公开基本目录，2018年底前各级税务机关按照税务总局发布的目录体系，全面完成本级主动公开目录体系修订工作，并动态更新，不断提升主动公开的标准化、规范化水平。（各司局落实，办公厅汇总发布）

（四）政务公开动态管理。税务部门每年根据政务公开工作的新要求以及公众关切，明确政务公开年度工作重点，把握好公开的力度和节奏，不断拓展公开范围，细化公开内容。各级税务机关每年应对本单位不予公开的信息以及依申请公开较为集中的信息进行全面自查，发现应公开未公开的信息应当公开，可转为主动公开的应当主动公开，自查整改情况应及时向上级机关报送。各级税务机关要定期抽查，对发现的应公开未公开等问题及时督促整改。（办公厅牵头，各司局落实）

八、规范税收政策解读

(一) 明确解读主体。按照谁起草、谁解读的原则，做好政策解读工作。税务部门制定的规范性文件，文件牵头起草单位负责做好解读工作。联合发文的，牵头起草单位负责做好解读工作，其他联合发文单位做好配合工作。文件牵头起草单位负责同志是“第一解读人和责任人”，要主动发声，传递权威信息。要充分发挥各部门政策参与制定者和掌握相关政策、熟悉有关领域业务的专家学者的作用，围绕国内外舆论关切，多角度、全方位、有序有效阐释政策，着力提升解读的权威性和针对性。（各司局落实）

(二) 规范解读流程。各级税务机关要按照税收政策和解读稿同步起草、同步审批、同步发布的“三同步”要求，将经本单位负责人审定的政策解读方案和解读材料随同文件一并报送，没有解读方案和解读材料的，办公厅（室）作退文处理。文件公布前，及时做好政策吹风解读和预期引导；文件公布时，相关解读材料应与文件同步在税务网站和媒体发布；文件执行过程中，要密切跟踪舆情，分段、多次、持续开展解读，及时解疑释惑，不断增强主动性、针对性和时效性。（各司局落实）

(三) 细化解读内容。解读政策时，着重解读文件出台的背景、意义，文件内容的重点、理解的难点、必要的举例说明和落实的措施要求等，使政策内涵透明，避免误解误读。对涉及群众切身利益、影响市场预期等重要政策，各级税务机关要善于运用媒体，实事求是、有的放矢开展政策解读，做好与市场、与社会的沟通工作，及时准确传递政策意图。重视收集反馈的信息，针对市场和社会关切事项，更详细、更及时地做好政策解读，减少误解猜疑，稳定预期。（各司局落实）

(四) 丰富解读形式。要围绕国家发布的相关税收法律、法规以及税务总局发布的税收规章、规范性文件等重大税收政策，通过举行新闻发布会、吹风会、撰写解读文章、组织记者采访、发布新闻稿、开展在线访谈以及电话、传真和电子邮件答复记者问询等形式，进行信息发布和政策解读。对于一些专业性较强的政策，运用数字化、图表、音频、视频等方式，进行形象化、通俗化解读。注重

通过新闻发布会的形式开展政策解读，围绕税收工作的热点难点问题，确定新闻发布会的主题，精心准备发布材料，及时发出权威声音。税务总局每季度至少召开1次新闻发布会，主要负责人每年至少参加1次国务院新闻办公室的新闻发布会，税务总局领导每年至少参加2次国务院新闻办公室的新闻发布会；地市以上税务机关应建立新闻发言人制度，主要负责人每年对自己制定的重要政策进行解读不少于1次。（办公厅牵头，会同各司局落实）

九、积极回应社会关切

（一）明确回应责任。按照属地管理、分级负责、谁主管谁负责的原则，做好涉税舆情的回应工作。涉及税务总局的舆情，税务总局是第一回应责任主体，对于税务总局与其他政府部门联合制定政策实施中发生的涉税舆情，由税务总局相关司局牵头与相关部委协调处置。涉及各地税务机关的舆情，涉事税务机关是第一回应责任主体，同时涉及国税、地税机关的，双方均为回应责任主体。对于各地发生的重大涉税舆情，舆情发生地税务机关要依托当地党委、政府和有关部门共同做好应对处置工作。（相关司局落实）

（二）做好回应处置。建立健全涉税舆情监测、推送、分析研判、调查核实、回应反馈、评估等机制，对收集到的涉税舆情加强研判，区别不同情况，进行分类处置。对建设性意见建议，吸收采纳情况要对外公开。对群众反映的实际困难，研究解决的情况要对外公布。对群众反映的重大问题，调查处置情况要及时发布。对公众不了解情况、存在模糊认识的，要主动发布权威信息，解疑释惑，澄清事实。对错误看法，要及时发布信息进行引导和纠正。对虚假和不实信息，在及时回应的同时，将涉嫌违法的有关情况和线索移交公安机关、网络监管部门依法依规进行查处。进一步做好专项回应引导工作，重点围绕“两会”、经济数据发布和经济形势、重大改革举措、重大督查活动、重大突发事件等，做好舆情收集、研判和回应工作。（办公厅牵头落实）

（三）提升回应效果。涉及特别重大和重大突发事件的涉税舆情，要快速反应，最迟要在5个小时内发布权威信息，在24小时内举行新闻发布会，并根据工作进展情况，持续发布权威信息，主要负责人要带头主动发声，表明立场态度，

发出权威声音。针对重大涉税舆情，建立与宣传、网信等部门的快速反应和协调联动机制，及时借助媒体、网站等渠道发布准确权威信息，着力提高回应的及时性、针对性、有效性。充分利用税务特色平台、新兴媒体以及税务网站的互动功能，提升回应信息的到达率。通过购买服务、完善大数据技术支撑等方式，用好专业力量，提高舆情分析处置的信息化水平。（办公厅牵头，会同相关司局落实）

十、推进政务公开平台建设

（一）强化税务网站建设和管理。建立健全网站管理制度，完善网站日常监测机制，及时发现和解决网站运行中存在的问题。规范网站信息发布流程，做好信息公开保密审查，准确及时发布信息，发挥网站在政策解读、回应社会关切、与公众互动交流中的积极作用，使税务网站成为公众获取税务机关信息的第一来源。税务网站之间要加强协同联动，做到信息资源共享和优势互补，税务总局网站发布的税收政策和要闻，省税务机关网站应及时转载、链接，发挥税务网站集群效应。各级税务网站加强与主要新闻媒体、新闻网站、商业网站的联动，通过合办专栏专版等方式，形成传播合力，提升传播效果。（办公厅牵头落实）

（二）发挥税务特色平台作用。依托办税服务厅电子触摸屏、显示屏、公告栏、宣传资料架等设施，公开办税信息，宣传税收政策。推进12366纳税服务平台建设，完善12366税收知识库，加强热线和网站纳税咨询的衔接和整合，全面提供能听、能问、能看、能查、能约、能办的“六能”型服务。积极利用税务微博、微信和手机客户端等新兴媒体传播税务信息。税务总局网站定期发布税务公报，及时准确刊登税收规章和规范性文件，做到应登尽登，各级税务网站在明显位置提供税务公报链接，方便社会公众查阅。充分发挥中国税务报社、中国税务杂志社、中国税务出版社等税务媒体在宣传税法、解读政策等方面的积极作用，拓宽公众获取税务信息渠道。（办公厅、纳税服务司牵头，会同相关司局落实）

（三）充分利用新闻媒体平台。在立足网站、“两微一端”等自有公开平台的基础上，加强与宣传、网信等部门以及报刊、杂志、广播、电视、有新闻资质的商业网站等媒体的沟通联系。通过主动向媒体提供素材，召开媒体通气会，推荐掌握相关政策、熟悉税收业务的专家学者接受媒体访谈等方式，畅通媒体采访

渠道，更好地发挥新闻媒体的公开平台作用。积极安排中央和地方主要媒体及其新媒体负责人列席有关会议，进一步扩大政务公开的覆盖面和影响力。（办公厅牵头，会同相关司局落实）

十一、扩大社会公众参与

（一）明确公众参与事项。围绕税收中心工作，细化公众参与事项范围，让公众更大程度参与政策制定、执行和监督。税务总局重点围绕税收发展规划、税收规章、重大税收改革事项等，根据需要通过多种方式，扩大公众参与。省税务机关重点围绕年度计划、规范性文件、重要税收政策措施等决策事项，着力做好公众参与工作。市县税务机关重点围绕税收执法监管、税收优惠政策措施的执行落地，着力加强利益相关方和社会公众的参与。（各司局落实）

（二）规范公众参与方式。完善民意汇集机制，拓展公众参与方式，激发公众参与的积极性。涉及重大税收改革和公众利益的重要决策，应通过广泛征求意见、专家座谈、听证会、论证会、调查研究、咨询协商、列席会议、媒体吹风等方式扩大公众参与，充分了解纳税人和社会公众的意见建议。发挥好人大代表、政协委员、民主党派、人民团体、社会公众、新闻媒体的监督作用，积极运用第三方评估等方式，做好政策措施执行的评估和监督工作。征求意见的采纳情况应予以公布，相对集中的意见建议不予采纳的，公布时要说明理由。（各司局落实）

（三）完善公众参与渠道。在办税服务厅设立纳税服务值班岗、设置意见建议箱，做好信息的收集处理和反馈。加强纳税人需求征集工作，通过纳税人满意度调查、纳税人座谈会、入户走访等方式收集纳税人需求。不断完善税务网站意见建议征集、公众留言办理、局长信箱等互动功能，依托新闻发布会、在线访谈、局长接访等形式，扩大公众参与面。积极探索公众参与新模式，利用“两微一端”等新媒体搭建公众参与新平台，支持多渠道的信息发布和政民互动。（办公厅、纳税服务司牵头，会同相关司局落实）

十二、强化政务公开组织保障

（一）健全政务公开领导机制。各级税务机关要建立政务公开工作领导小组，

负责组织协调、指导推进、监督检查本单位政务公开工作，并成立专门的政务公开工作办事机构。将政务公开纳入重要议事日程，主要负责人亲自抓，明确一位分管负责人具体抓。主要负责人每年至少听取一次政务公开工作汇报，研究推动工作，有关情况和分管负责人工作分工应对外公布。（办公厅牵头，会同相关司局落实）

（二）完善政务公开工作机制。整合政务公开方面的力量和资源，配备政务公开专业人员，加强政务公开经费保障，为工作顺利开展创造条件。探索推行政务公开运转规范，制定政务公开工作场所建设标准、政府信息依申请公开答复范本等。健全政务公开协调机制，各级税务机关应与宣传、网信等部门紧密协作，指导协调主要媒体、重点新闻网站和主要商业网站，充分利用各媒体平台、运用全媒体手段做好政务公开工作。完善信息发布协调机制，对涉及多个部门的政府信息，应当与有关单位沟通确认，确保发布信息准确一致。（办公厅牵头落实）

（三）加强政务公开教育培训。各级税务机关要将政务公开内容纳入干部教育培训科目，加强对税务干部特别是领导干部的培训，增强公开意识，提高发布信息、解读政策、回应关切的能力。分级分层组织实施政务公开教育培训，2018年底前对税务系统政务公开工作人员轮训一遍。政务公开工作人员要加强政策理论学习和业务研究，准确把握政策精神，增强专业素养。按照税务系统人才库管理相关规定，将政务公开工作业务骨干纳入人才库管理，提高政务公开人员专业素质，提升工作水平。（办公厅牵头，会同教育中心、人事司落实）

（四）强化政务公开考评问责。将信息公开、政策解读、回应关切等政务公开工作纳入绩效考评。通过第三方评估、民意调查等方式，加强对政务公开工作的评估，并根据评估结果不断调整优化政务公开的方式方法，评估结果要作为政务公开绩效考评的重要参考。每年至少对20%以上的下级税务机关进行检查，发现问题及时督促整改。对政务公开工作推动有力、积极参与的单位和个人，按照有关规定进行表彰；对重要信息不发布、重大政策不解读、热点回应不及时，进行严肃批评、公开通报；对弄虚作假、隐瞒实情、欺骗公众，造成严重社会影响的，依法依规追究相关单位和人员责任。（办公厅牵头落实）

(十二) 教育部办公厅关于印发《教育部机关及直属事业单位教育数据管理办法》的通知

(教发厅〔2018〕1号)

部内各司局、各直属事业单位:

为加强教育部机关及直属事业单位教育数据管理工作,推进各类教育数据的规范管理、互联互通和共享公开,确保数据安全,更好地服务教育改革发展,我部制定了《教育部机关及直属事业单位教育数据管理办法》,现印发给你们,请认真贯彻执行。

教育部办公厅

2018年1月22日

第一章 总 则

第一条 为加强教育部机关及直属事业单位教育数据管理工作,推进各类教育数据的规范管理、互联互通和共享公开,确保数据安全,更好地服务教育改革发展,依据《中华人民共和国统计法》《中华人民共和国网络安全法》《中华人民共和国政府信息公开条例》《国务院关于印发政务信息资源共享管理暂行办法的通知》等相关法律法规及国家政策,特制定本办法。

第二条 本办法所称教育数据,是指教育部机关及经法律法规授权具有行政职能的直属事业单位在履行职责过程中获取的各类数字化的数据资源,包括法定统计数据 and 行政记录数据。

法定统计数据是指按照《中华人民共和国统计法》的有关规定,通过国家统计局审批备案的统计调查制度采集的数据。法定统计数据为标准时点或时段的静态数据或累计数据。

行政记录数据是指行政业务管理信息系统在履行行政管理职责过程中形成的数据资源。行政记录数据主要为动态数据。

第三条 本办法适用于教育数据的采集、储存、共享、公开和安全管理等环节。

第四条 教育数据管理的基本原则是：

（一）统筹管理，各负其责。教育数据的采集、储存、共享、公开和安全管理等工作要在教育部统筹管理、统一标准的基础上，由教育部机关及直属事业单位分头实施、各负其责。

（二）推进共享，有序公开。教育数据以共享为原则，不共享为例外。公开教育数据要依照相关法律法规，在满足社会公众知情权的前提下，有序开放公共教育数据资源。

（三）规范程序，保障安全。明确教育数据各环节的管理程序，做到教育数据管理全过程有规可依。依托国家信息安全保障体系，完善教育数据共享与公开安全机制，保护个人隐私信息，保障教育数据资源安全。

第五条 教育统计调查项目和行政业务管理信息系统的负责单位为相关数据管理的第一责任主体，应根据本办法制定本部门教育数据管理的实施细则。

第六条 教育统计调查项目和行政业务管理信息系统采集的数据由负责单位进行保密审查。审查结果报部保密办公室备案。

第二章 数据采集与存储

第七条 采集教育数据需按规定程序批准。

教育部机关和直属事业单位采集教育数据，均应经过充分论证。论证内容包括数据采集的必要性和可行性，采集数据与已有教育数据的关系，数据采集机制、经费保障等。

设立新的教育统计调查项目应将论证材料报发展规划司审核，由发展规划司报部党组会或部长专题会审议同意，并报国家统计局审批或备案后方可组织实施。部机关各司局教育统计调查项目实施方案与统计调查制度应一并报发展规划司备案。

设立行政业务管理信息系统应将系统和采集数据的论证材料报教育部网络安全和信息化领导小组办公室审核，由教育部网络安全和信息化领导小组办公室报部党组会或部长专题会审议通过后实施，系统采集的数据指标报发展规划司备案。

第八条 设立新的教育统计调查项目和行政业务管理信息系统应符合精简、高效的原则，充分考虑基层学校的承受能力，数据采集遵循“一数一源”原则。凡属于共享平台可以获取的数据，原则上不得重复采集。

第九条 因工作职能变动或其他原因，需要撤销在有效期内的统计调查项目，应报分管部领导批准，并由发展规划司报国家统计局撤销备案；已超过有效期的统计调查项目，经分管部领导批准，可自行撤销并报发展规划司备案。需要撤销业务管理信息系统的，应报分管部领导批准。

第十条 教育数据的采集要遵循国家和教育部颁布的相关标准。自然人标识遵循《学校（机构）人员基础信息代码编制规则》，学校（机构）标识遵循《学校（机构）代码管理办法》。涉及综合数据指标的应采用我部统一发布的教育统计指标定义与计算公式，不在此列的应将有关指标的定义、计算公式等报发展规划司备案。

第十一条 各教育统计调查项目和行政业务管理信息系统设置的指标如需变动，应经专家组论证后报分管部领导审核同意，并报发展规划司和教育部网络安全和信息化领导小组办公室备案。

第十二条 数据采集单位应制定数据采集的规范程序，建立数据质量核查和技术保障制度，确保数据的真实、准确、完整和及时。

第十三条 教育统计调查项目和行政业务管理信息系统均应制定完善的数据安全存储管理方案并配备必要的设施、设备，并在不同地点储存备份，确保数据存储的安全可靠。

第十四条 教育部机关及直属事业单位应当根据本部门采集的教育数据，对本部门分管业务的发展状况进行数据分析，提供必要的数据监测信息、咨询意见

和决策建议。

第三章 数据共享

第十五条 本办法所称数据共享，是指政务部门间教育数据的共享。包括教育部机关及直属事业单位间教育数据的共享，教育部和其他政务部门间的数据共享。

第十六条 教育数据资源共享分为无条件共享、有条件共享、不予共享等三种类型。

无条件共享数据是指可提供给所有部机关、直属事业单位和其他政务部门共享使用的教育数据资源。

有条件共享数据是指可提供给相关部机关、直属事业单位和其他相关政务部门共享使用或依双方协议提供共享使用的教育数据资源。

不予共享数据是指不宜提供给部机关及直属事业单位和其他政务部门共享使用的教育数据。

第十七条 凡列入不予共享类的教育数据资源，必须有法律、行政法规或党中央、国务院政策依据。

第十八条 共享数据的生产和提供部门应按照“谁主管，谁提供，谁负责”的原则，及时提供、维护和更新共享数据，保障数据的完整性、准确性，确保所提供的共享数据与本部门的数据一致。在向使用部门提供共享数据时，需明确数据的共享范围和用途。

第十九条 因履行职责需要使用共享数据的部门，应按照“谁经手，谁使用，谁管理，谁负责”的原则，依法依规使用共享数据，加强共享数据使用的全过程管理。

第二十条 使用部门需共享数据时，应向数据提供方提出明确的共享需求和用途，提供部门应及时响应并无偿提供共享服务。共享各类数据的基本流程如下：

属于无条件共享类的数据资源，使用部门在共享平台上直接获取；

属于有条件共享类的数据资源，使用部门通过共享平台向提供部门提出申请，提供部门应在10个工作日内予以答复，使用部门按答复意见使用共享数据，对不予共享的，提供部门应说明理由。

第二十一条 涉及国家秘密、商业秘密和个人隐私的教育数据资源，使用部门和提供部门应当签订教育数据资源共享安全保密协议，按照约定方式共享数据资源。

第二十二条 使用部门获得的共享数据仅限内部使用，如需对外提供或发布，应当向提供部门提出书面申请，经同意后，方可对外提供或发布。使用部门未经授权，不得将获取的共享数据资源挪作他用，不得以任何方式用于社会有偿服务或其他商业活动，并对共享数据资源的滥用、非授权使用、未经许可的扩散以及泄露等行为及后果承担全部责任。

第二十三条 使用部门对获取的共享数据有疑义或发现有明显错误的，应及时反馈给提供部门予以校核。

第四章 数据公开

第二十四条 本办法所称数据公开，是指依照相关法律法规向社会公众公开教育数据。教育数据资源公开分为主动公开、依申请公开、不予公开等三种类型。

教育统计调查项目和行政管理信息系统负责部门应依照《中华人民共和国统计法》《教育部信息公开指南》，结合本部门工作实际，科学确定本单位教育数据的资源公开属性，并及时做好数据公开工作。

第二十五条 公开数据不得泄露国家秘密、商业秘密和个人隐私，切实维护数据资源主体的合法权益。经权利人同意公开或者不公开可能对公共利益造成重大影响的涉及商业秘密、个人隐私的数据资源，可予以公开。

第二十六条 主动公开类数据均应通过公开平台开放数据资源，并可通过年鉴、光盘等专门出版物形式公开数据。依申请公开类的数据资源，应依据《教育部信息公开指南》要求提供。

第五章 教育政务信息资源目录

第二十七条 教育部实行教育政务信息资源目录管理制度。教育政务信息资源目录包括教育信息资源的分类、责任方、格式、属性、更新时限、共享类型、共享方式、公开类型、公开方式、使用要求等内容。教育政务信息资源目录是信息资源共享、公开和业务协同的基础和依据。

第二十八条 负责教育数据生产的部机关及直属事业单位，应按照《政务信息资源目录编制指南（试行）》要求和统一标准，编制、审核、发布本部门《教育政务信息资源目录》，并确保其准确、完整、合规。

第二十九条 各单位《教育政务信息资源目录》应按要求及时报送发展规划司，由发展规划司汇总并报分管部领导审定，形成《教育部教育政务信息资源目录》。

第三十条 负责教育数据生产的部机关及直属事业单位，应建立本部门资源目录更新维护制度，每年应当至少进行一次全面维护。如资源目录要素内容发生调整或可共享与公开的教育数据资源出现变化时，应当在7个工作日内进行数据资源目录的更新操作，并报发展规划司备案，及时纳入到《教育部教育政务信息资源目录》中。

第三十一条 部机关及直属事业单位新设立教育统计调查项目或行政管理信息系统时，应在上报项目立项申请前预编项目《教育政务信息资源目录》，作为项目审批要件。项目建成后，应将项目《教育政务信息资源目录》及时纳入《教育部教育政务信息资源目录》中，作为项目验收的必要条件。

第六章 数据资源共享、公开平台

第三十二条 教育部设立统一的教育数据资源共享交换平台，用于支撑教育数据的共享交换，管理《教育部教育政务信息资源目录》。共享平台应按照涉密信息系统分级保护要求，依托国家电子政务外网进行建设和管理。

第三十三条 无条件共享数据资源必须依据整合共建原则，通过接入共享平台实现基础数据的统筹管理与维护。部机关及直属事业单位可通过共享平台直接

获取并使用共享数据。共享平台接入国家数据共享交换平台，其他政务部门可通过国家数据共享交换平台获取并使用共享数据。

第三十四条 教育部设立教育数据资源公开平台，面向社会公众提供教育数据服务。公开平台应按照国家互联网及网络安全等相关法律法规及政策建设和管理。部机关及直属事业单位可通过公开平台面向社会公开教育数据资源。

第三十五条 教育统计调查项目和行政管理业务信息系统责任单位负责本部门系统与共享平台的联通保障工作，并按照《教育部教育政务信息资源目录》向共享平台和公开平台提供相应的教育数据资源。

第三十六条 教育部教育管理信息中心作为技术支撑部门，负责共享平台与国家数据共享交换平台的联通工作和教育部教育数据公开平台的管理维护工作。

第七章 数据安全

第三十七条 教育部机关及直属事业单位设立的教育统计调查项目和行政管理业务信息系统，均应根据有关法律法规，制定涵盖数据采集、存储、共享、公开、使用等全过程的数据安全管理办法，开展数据风险评估，确定数据共享、公开类型，明确责任人，落实安全管理责任制。教育管理信息中心负责共享平台和公开平台的安全防护工作，确保教育数据安全。

第三十八条 教育部网络安全和信息化领导小组办公室负责制定教育数据网络安全管理制度，指导督促教育数据采集、存储、共享、使用全过程的网络安全保障工作，组织开展教育数据安全风险评估和安全管理审查。

第三十九条 共享数据涉及国家秘密、商业秘密和个人隐私的，提供部门和使用部门应当遵守有关保密的法律法规，在数据共享工作中分别承担相应的安全保障责任。

第八章 监督与保障

第四十条 发展规划司和教育部网络安全和信息化领导小组办公室分别负责教育统计调查项目和教育行政业务管理信息系统的核准与检查监督工作，并对

核准与检查监督项目或系统发出通知单。

第四十一条 发展规划司和教育部网络安全和信息化领导小组办公室对不符合国家及本办法有关规定的申请项目和系统，不予立项，财务部门不予安排运维经费。正在运行实施的项目与系统，如有不符合本办法规定的情况，应按检查通知单要求限期整改，对经反复催促仍未按规定完成整改的，在部内予以通报。

第九章 附 则

第四十二条 本办法由发展规划司和教育部网络安全和信息化领导小组办公室负责解释。

第四十三条 本办法自2018年1月22日起施行。

(十三) 信息安全技术 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、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；

（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；

（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；

(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。

（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。

附件2

关于《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）》的起草说明

一、起草背景

近年来，我国个人信息保护力度不断加大，但App个人信息收集使用规则、目的、方式和范围仍存在不明确的地方，部分环节仍存漏洞，个人信息保护面临诸多问题和挑战。党中央、国务院高度重视App个人信息保护治理工作，党的十

十九届五中全会明确提出，维护人民根本利益，保障国家数据安全，加强个人信息保护。国家互联网信息办公室、工业和信息化部、公安部、市场监管总局持续深入开展App违法违规收集使用个人信息治理工作，工业和信息化部连续两年开展App侵害用户权益专项整治行动，社会反映热烈，取得阶段性明显成效。

考虑到App治理是一项具有长期性、复杂性的系统治理工作，有必要将近年来成熟的经验做法和管理措施转换为制度性规范文件。同时，为强化App个人信息保护管理的系统性、整体性和协同性，在总结专项治理工作经验基础上，起草形成了《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）》（以下简称《征求意见稿》），并向社会公开征求意见。

二、关于起草的主要情况和把握要点

《征求意见稿》在国家互联网信息办公室的统筹指导下，由工业和信息化部会同公安部、市场监管总局联合制定完成。起草过程中，就重点问题组织有关单位和专家学者进行了专题研究，并听取了百度、阿里巴巴、腾讯、字节跳动、美团、拼多多、京东、滴滴、新浪微博、快手、小米、华为、OPPO、vivo、360、捷兴信源、梆梆等主要互联网企业、终端企业和安全企业的意见建议。

制定过程中，重点把握“三个坚持”：一是坚持以人民为中心的发展思想。贯彻党的十九届五中全会要求，落实以人民为中心的发展思想，坚持人民利益至上，严格规范App个人信息处理活动，增强人民群众安全感和获得感。二是坚持问题导向。立足前期专项治理工作基础，聚焦用户投诉举报反映强烈的突出问题，将近两年来已经成熟的经验做法和管理措施制度化，为规范App个人信息处理活动提供可靠制度保障。三是坚持落实主体责任。明确细化了App开发运营者、分发平台、第三方服务提供者等主体在App个人信息处理活动中应当履行的主体责任义务。

三、关于《征求意见稿》的主要内容

《征求意见稿》共计二十条，界定了适用范围和监管主体；确立了“知情同意”“最小必要”两项重要原则；细化了App开发运营者、分发平台、第三方服

务提供者、终端生产企业、网络接入服务提供者五类主体责任义务；提出了投诉举报、监督检查、处置措施、风险提示等四方面规范要求，主要内容如下：

一是界定适用范围和明确监管主体。在适用范围方面，《征求意见稿》明确了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。在监管主体方面，《征求意见稿》明确了App个人信息保护的联合工作机制，国家互联网信息办公室会同工业和信息化部、公安部、市场监管总局健全完善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，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。（第一条至第五条）

二是明确“知情同意”“最小必要”两项重要原则。《征求意见稿》“知情同意”规定，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，并明确了“六项应当”要求。“最小必要”规定，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，并提出了“六项不得”要求。（第六条和第七条）

三是规范关键环节主体责任义务。《征求意见稿》对App治理的全链条、全主体、全流程予以规范，规定了App开发运营者、App分发平台、App第三方服务提供者、移动智能终端生产企业和网络接入服务提供者在App个人信息保护方面的具体义务。（第八条至第十二条）

四是细化违规处置流程和具体措施。《征求意见稿》明确从事个人信息处理活动的有关主体违反要求的，依次按照通知整改、社会公告、下架处置、断开接入、信用管理流程进行处置，并明确具体时间期限要求。特别提出，对未按要求完成整改或反复出现问题、采取技术对抗等违规情节严重的App，将对其进行直接下架；且下架后的App在40个工作日内不得通过任何渠道再次上架的管理要求。此外，监督管理部门将指导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。（第十六和第十七

条)

此外,《征求意见稿》还对违反本规定行为的法律责任、保密义务等作了规定。(第十八和第十九条)

(十四) 常见类型移动互联网应用程序必要个人信息范围规定

本文件规定了地图导航、网络约车、即时通信等38类常见类型App必要个人信息范围。必要个人信息是指保障App基本功能正常运行所必须的个人信息，缺少该信息App无法提供基本功能服务。只要用户同意收集必要个人信息，App不得拒绝用户安装使用。

1.地图导航类:

基本功能服务: 定位和导航。

必要个人信息: 位置信息。

2.网络约车类:

基本功能服务: 预约汽车出行。

必要个人信息:

(1) 注册用户手机号码或其他真实身份信息 (App提供者提供多种选项, 由用户选择其一) 。

(2) 乘车人出发地、到达地、位置信息、行踪轨迹。

3.即时通信类:

基本功能服务: 提供文字、图片、语音、视频等即时通信服务。

必要个人信息:

(1) 注册用户手机号码或其他真实身份信息 (App提供者提供多种选项, 由用户选择其一) 。

(2) 账号信息: 账号、联系人账号列表。

4.网络社区类:

基本功能服务: 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：注册用户手机号码或其他真实身份信息（App提供者提供多种选项，由用户选择其一）。

5.网络支付类:

基本功能服务：收款人或付款人依托公共网络远程发起支付指令，由支付机构提供货币资金转移服务（如支付、提现、转账等）。

必要个人信息：

（1）注册用户手机号码或其他真实身份信息（App提供者提供多种选项，由用户选择其一）。

（2）付款人姓名、证件类型和号码、证件有效期限、证件影印件、银行卡号码、银行预留手机号码。

（3）收款人姓名、银行卡号码。

6.网上购物类:

基本功能服务：购买商品。

必要个人信息：

（1）注册用户手机号码或其他真实身份信息（App提供者提供多种选项，由用户选择其一）。

（2）收货人姓名、地址、联系电话。

（3）支付信息。

7.餐饮外卖类:

基本功能服务：购买餐饮。

必要个人信息：

（1）注册用户手机号码或其他真实身份信息（App提供者提供多种选项，由用户选择其一）。

(2) 收货人姓名、地址、联系电话。

(3) 支付信息。

8. 快递物流类:

基本功能服务: 包裹、印刷品等物品的快递寄收件。

必要个人信息:

(1) 寄件人真实姓名、地址、联系电话。

(2) 收件人姓名、地址、联系电话。

9. 交通票务类:

基本功能服务: 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:

(1) 注册用户手机号码或其他真实身份信息(App提供者提供多种选项,由用户选择其一)。

(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)。

(4) 支付信息。

10. 婚恋相亲类:

基本功能服务: 婚恋相亲。

必要个人信息:

(1) 注册用户手机号码或其他真实身份信息(App提供者提供多种选项,由用户选择其一)。

(2) 婚恋相亲人的性别、年龄、婚姻状况。

11.求职招聘类:

基本功能服务: 职位信息查询和求职简历投递。

必要个人信息:

(1) 注册用户手机号码或其他真实身份信息 (App提供者提供多种选项, 由用户选择其一) 。

(2) 求职者提供的简历。

12.网络借贷类:

基本功能服务: 通过互联网平台实现的个人消费贷款。

必要个人信息:

(1) 注册用户手机号码或其他真实身份信息 (App提供者提供多种选项, 由用户选择其一) 。

(2) 借款人姓名、证件类型和号码、证件有效期限、证件影印件、银行卡号码。

13.房屋租售类:

基本功能服务: 个人房源信息发布、房屋出租或买卖。

必要个人信息:

(1) 注册用户手机号码或其他真实身份信息 (App提供者提供多种选项, 由用户选择其一) 。

(2) 房源基本信息: 房屋地址、面积/户型、期望售价或租金。

14.二手车交易类:

基本功能服务: 二手车买卖。

必要个人信息:

(1) 注册用户手机号码或其他真实身份信息 (App提供者提供多种选项, 由用户选择其一) 。

(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。

15.问诊挂号类:

基本功能服务: 在线问诊、挂号。

必要个人信息:

(1) 注册用户手机号码或其他真实身份信息 (App提供者提供多种选项, 由用户选择其一) 。

(2) 患者姓名、证件类型和号码。

(3) 患者预约挂号的医院、科室。

16.旅游服务类:

基本功能服务: 旅游产品订购。

必要个人信息:

(1) 注册用户手机号码或其他真实身份信息 (App提供者提供多种选项, 由用户选择其一) 。

(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。

17.酒店服务类:

基本功能服务: 酒店预订。

必要个人信息:

(1) 注册用户手机号码或其他真实身份信息 (App提供者提供多种选项, 由用户选择其一) 。

(2) 住宿人姓名、联系方式, 入住、退房时间, 入住酒店名称。

18.网络游戏类:

基本功能服务: 通过网络提供游戏产品和服务。

必要个人信息: 注册用户手机号码或其他真实身份信息 (App提供者提供多种选项, 由用户选择其一) 。

19.学习教育类:

基本功能服务: 在线辅导、网络课堂等。

必要个人信息: 注册用户手机号码或其他真实身份信息 (App提供者提供多种选项, 由用户选择其一) 。

20.本地生活类:

基本功能服务: 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: 注册用户手机号码或其他真实身份信息 (App提供者提供多种选项, 由用户选择其一) 。

21.女性健康类:

基本功能服务: 女性经期管理、备孕育儿、美容美体等健康管理服务。

必要个人信息:

(1) 注册用户手机号码或其他真实身份信息 (App提供者提供多种选项, 由用户选择其一) 。

(2) 用于健康管理的历史信息。

22.用车服务类:

基本功能服务: 共享单车、共享汽车、租赁汽车等服务。

必要个人信息:

(1) 注册用户手机号码或其他真实身份信息 (App提供者提供多种选项, 由用户选择其一) 。

(2) 使用共享汽车、租赁汽车服务用户的证件类型和号码, 驾驶证影印件。

23.投资理财类:

基本功能服务: 股票、期货、基金、债券等相关投资理财服务。

必要个人信息:

(1) 注册用户手机号码或其他真实身份信息 (App提供者提供多种选项, 由用户选择其一) 。

(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。

(3) 投资理财用户资金账户、银行卡号码。

24.手机银行类:

基本功能服务: 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:

(1) 注册用户手机号码或其他真实身份信息 (App提供者提供多种选项, 由用户选择其一) 。

(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、银行预留手机号码。

(3) 收款人姓名、银行卡号码。

25.邮箱网盘类:

基本功能服务: 邮箱、云盘等。

必要个人信息: 注册用户手机号码或其他真实身份信息 (App提供者提

供多种选项，由用户选择其一）。

26.远程会议类:

基本功能服务：通过网络提供音频或视频会议。

必要个人信息：注册用户手机号码或其他真实身份信息（App提供者提供多种选项，由用户选择其一）。

27.网络直播类:

基本功能服务：向公众持续提供实时视频、音频、图文等形式信息服务。

必要个人信息：无须个人信息，即可使用基本功能服务。

28.在线影音类:

基本功能服务：影视、音乐播放和下载。

必要个人信息：无须个人信息，即可使用基本功能服务。

29.短视频类:

基本功能服务：不超过一定时长的视频搜索、播放。

必要个人信息：无须个人信息，即可使用基本功能服务。

30.新闻资讯类:

基本功能服务：新闻资讯的浏览、搜索。

必要个人信息：无须个人信息，即可使用基本功能服务。

31.运动健身类:

基本功能服务：运动记录、健身管理等服务。

必要个人信息：无须个人信息，即可使用基本功能服务。

32.浏览器类:

基本功能服务：浏览互联网信息资源。

必要个人信息：无须个人信息，即可使用基本功能服务。

33.输入法类：

基本功能服务：文字、符号等输入。

必要个人信息：无须个人信息，即可使用基本功能服务。

34.安全管理类：

基本功能服务：查杀病毒、清理恶意插件、修复漏洞、清理优化、骚扰拦截、权限管理等。

必要个人信息：无须个人信息，即可使用基本功能服务。

35.电子图书类：

基本功能服务：电子图书阅读。

必要个人信息：无须个人信息，即可使用基本功能服务。

36.拍摄美化类：

基本功能服务：拍摄、美颜、滤镜等。

必要个人信息：无须个人信息，即可使用基本功能服务。

37.应用商店类：

基本功能服务：App下载和管理。

必要个人信息：无须个人信息，即可使用基本功能服务。

38.实用工具类：

基本功能服务：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、协同办公等。

必要个人信息：无须个人信息，即可使用基本功能服务。

(十五) 互联网个人信息安全保护指南

为有效防范侵犯公民个人信息违法行为，保障网络数据安全和公民合法权益，公安机关结合侦办侵犯公民个人信息网络犯罪案件和安全监督管理工作中掌握的情况，组织北京市网络行业协会和公安部第三研究所等单位相关专家，研究起草了《互联网个人信息安全保护指南》，供互联网服务单位在个人信息保护工作中参考借鉴。

1 范围

本文件制定了个人信息安全保护的管理机制、安全技术措施和业务流程。

适用于个人信息持有者在个人信息生命周期处理过程中开展安全保护工作参考使用。本文件适用于通过互联网提供服务的企业，也适用于使用专网或非联网环境控制和处理个人信息的组织或个人。

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

GB/T 22239 信息安全技术 网络安全等级保护基本要求（信息系统安全等级保护基本要求）

3 术语和定义

3.1 个人信息

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。

[中华人民共和国网络安全法，第七十六条（五）]

注：个人信息还包括通信通讯联系方式、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。

3.2 个人信息主体

个人信息所标识的自然人。

3.3 个人信息持有

对个人信息及相关资源、环境、管理体系等进行计划、组织、协调、控制的相关活动或行为。

3.4 个人信息持有者

对个人信息进行控制和处理的组织或个人。

3.5 个人信息收集

获得对个人信息的控制权的行为，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，以及通过共享、转让、搜集公开信息间接获取等方式。

3.6 个人信息使用

通过自动或非自动方式对个人信息进行操作，例如记录、组织、排列、存储、改编或变更、检索、咨询、披露、传播或以其他方式提供、调整或组合、限制、删除等。

3.7 个人信息删除

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。

3.8 个人信息生命周期

包括个人信息持有者收集、保存、应用、委托处理、共享、转让和公开披露、

删除个人信息在内的全部生命历程。

3.9 个人信息处理系统

处理个人信息的计算机信息系统，涉及个人信息生命周期一个或多个阶段（收集、保存、应用、委托处理、共享、转让和公开披露、删除）。

4 管理机制

4.1 基本要求

个人信息处理系统的安全管理要求应满足GB/T 22239相应等级的要求。

4.2 管理制度

4.2.1 管理制度内容

a) 应制定个人信息保护的总体方针和安全策略等相关规章制度和文件，其中包括本机构的个人信息保护工作的目标、范围、原则和安全框架等相关说明；

b) 应制定工作人员对个人信息日常管理的操作规程；

c) 应建立个人信息管理制度体系，其中包括安全策略、管理制度、操作规程和记录表单；

d) 应制定个人信息安全事件应急预案。

4.2.2 管理制度制定发布

a) 应指定专门的部门或人员负责安全管理制度的制定；

b) 应明确安全管理制度的制定程序和发布方式，对制定的安全管理制度进行论证和审定，并形成论证和评审记录；

c) 应明确管理制度的发布范围，并对发文及确认情况进行登记记录。

4.2.3 管理制度执行落实

a) 应对相关制度执行情况进行审批登记；

b) 应保存记录文件，确保实际工作流程与相关的管理制度内容相同；

c) 应定期汇报总结管理制度执行情况。

4.2.4 管理制度评审改进

a) 应定期对安全管理制度进行评审，存在不足或需要改进的予以修订；

b) 安全管理制度评审应形成记录，如果对制度做过修订，应更新所有下发的相关安全管理制度。

4.3 管理机构

4.3.1 管理机构的岗位设置

a) 应设置指导和管理个人信息保护的工作机构，明确定义机构的职责；

b) 应由最高管理者或授权专人负责个人信息保护的工作；

c) 应明确设置安全主管、安全管理各个方面的负责人，设立审计管理员和安全管理员等岗位，清晰、明确定义其职责范围。

4.3.2 管理机构的人员配置

a) 应明确安全管理岗位人员的配备，包括数量、专职还是兼职情况等；配备负责数据保护的专门人员；

b) 应建立安全管理岗位人员信息表，登记机房管理员、系统管理员、数据库管理员、网络管理员、审计管理员、安全管理员等重要岗位人员的信息，审计管理员和安全管理员不应兼任网络管理员、系统管理员、数据库管理员、数据操作员等岗位。

4.4 管理人员

4.4.1 管理人员的录用

a) 应设立专门的部门或人员负责人员的录用工作；

b) 应明确人员录用时对人员的条件要求，对被录用人的身份、背景和专业

资格进行审查，对技术人员的技术技能进行考核；

c) 录用后应签署相应的针对个人信息的保密协议；

d) 应建立管理文档，说明录用人员应具备的条件（如学历、学位要求，技术人员应具备的专业技术水平，管理人员应具备的安全管理知识等）；

e) 应记录录用人身份、背景和专业资格等，记录审查内容和审查结果等；

f) 应记录录用人录用时的技能考核文档或记录，记录考核内容和考核结果等；

g) 应签订保密协议，其中包括保密范围、保密责任、违约责任、协议的有效期限和责任人签字等内容。

4.4.2 管理人员的离岗

a) 人员离岗时应办理调离手续，签署调离后个人信息保密义务的承诺书，防范内部员工、管理员因工作原因非法持有、披露和使用个人信息；

b) 应对即将离岗人员具有控制方法，及时终止离岗人员的所有访问权限，取回其身份认证的配件，诸如身份证件、钥匙、徽章以及机构提供的软硬件设备；采用生理特征进行访问控制的，需要及时删除生理特征录入的相关信息；

c) 应形成对离岗人员的安全处理记录(如交还身份证件、设备等的登记记录)；

d) 应具有按照离职程序办理调离手续的记录。

4.4.3 管理人员的考核

a) 应设立专人负责定期对接触个人信息数据工作的工作人员进行全面、严格的安全审查、意识考核和技能考核；

b) 应按照考核周期形成考核文档，被考核人员应包括各个岗位的人员；

c) 应对违反违背制定的安全策略和规定的人员进行惩戒；

d) 应定期考查安全管理员、系统管理员和网络管理员其对工作相关的信息

安全基础知识、安全责任和惩戒措施、相关法律法规等的理解程度，并对考核记录进行记录存档。

4.4.4 管理人员的教育培训

a) 应制定培训计划并按计划对各岗位员工进行基本的安全意识教育培训和岗位技能培训；

b) 应制定安全教育和培训计划文档，明确培训方式、培训对象、培训内容、培训时间和地点等，培训内容包含信息安全基础知识、岗位操作规程等；

c) 应形成安全教育和培训记录，记录包含培训人员、培训内容、培训结果等。

4.4.5 外部人员访问

a) 应建立关于物理环境的外部人员访问的安全措施：

- 1) 制定外部人员允许访问的设备、区域和信息的规定；
- 2) 外部人员访问前需要提出书面申请并获得批准；
- 3) 外部人员访问被批准后应有专人全程陪同或监督，并进行全程监控录像；
- 4) 外部人员访问情况应登记备案。

b) 应建立关于网络通道的外部人员访问的安全措施：

- 1) 制定外部人员允许接入受控网络访问系统的规定；
- 2) 外部人员访问前需要提出书面申请并获得批准；
- 3) 外部人员访问时应进行身份认证；
- 4) 应根据外部访问人员的身份划分不同的访问权限和访问内容；
- 5) 应对外部访问人员的访问时间进行限制；
- 6) 对外部访问人员对个人信息的操作进行记录。

5 技术措施

5.1 基本要求

个人信息处理系统其安全技术措施应满足GB/T 22239相应等级的要求，按照网络安全等级保护制度的要求，履行安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改。

5.2 通用要求

5.2.1 通信网络安全

5.2.1.1 网络架构

a) 应为个人信息处理系统所处网络划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址；

b) 个人信息处理系统应作为重点区域部署，并设有边界防护措施。

5.2.1.2 通信传输

a) 应采用校验技术或密码技术保证通信过程中个人信息的完整性；

b) 应采用密码技术保证通信过程中个人信息字段或整个报文的保密性。

5.2.2 区域边界安全

5.2.2.1 边界防护

a) 应对跨越边界访问通信信息进行有效防护

b) 应对非授权设备跨越边界行为进行检查或限制。

5.2.2.2 访问控制

应在个人信息处理系统边界根据访问控制策略设置访问控制规则。

5.2.2.3 入侵防范

应在个人信息处理系统边界部署入侵防护措施，检测、防止或限制从外部、内部发起的网络攻击行为。

5.2.2.4 恶意代码防范

应在个人信息处理系统的网络边界处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。

5.2.2.5 安全审计

a) 应在个人信息处理系统的网络边界、重要网络节点进行安全审计，审计应覆盖到每个用户、用户行为和安全事件；

b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功，以及个人信息范围、类型、操作方式、操作人、流转双方及其他与审计相关的信息；

c) 应对审计记录进行保护，定期备份并避免受到未预期的删除、修改或覆盖等；

d) 审计记录的留存时间应符合法律法规的要求；

e) 应能够对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析。

5.2.3 计算环境安全

5.2.3.1 身份鉴别

a) 应对登录个人信息处理系统的用户进行身份标识和鉴别，身份鉴别标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；

b) 个人信息处理系统应启用登录失败处理功能，采取诸如结束会话、限制非法登录次数和自动退出等措施；

c) 个人信息处理系统进行远程管理时，应采取措施防止身份鉴别信息在网络传输过程中被窃听；

d) 个人信息处理系统应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术

来实现，密码技术应符合国家密码主管部门规范。

5.2.3.2 访问控制

- a) 应对登录个人信息处理系统的用户分配账户和权限；
- b) 个人信息处理系统应重命名或删除默认账户，修改默认账户的默认口令；
- c) 个人信息处理系统应及时删除或停用多余的、过期的账户，避免共享账户的存在；
- d) 个人信息处理系统应进行角色划分，并授予管理用户所需的最小权限，实现管理用户的权限分离；
- e) 个人信息处理系统应由授权主体配置访问控制策略，访问控制策略应规定主体对客体的访问规则；
- f) 个人信息处理系统的访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级；
- g) 个人信息处理系统应对个人信息设置安全标记，并控制主体对有安全标记资源的访问。

5.2.3.3 安全审计

- a) 个人信息处理系统应启用安全审计功能，并且审计覆盖到每个用户，应对重要的用户行为和重要的安全事件进行审计；
- b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；
- c) 应对审计记录进行保护，进行定期备份并避免受到未预期的删除、修改或覆盖等；
- d) 审计记录的留存时间应符合法律法规的要求；
- e) 应对审计进程进行保护，防止未经授权的中断。

5.2.3.4 入侵防范

- a) 个人信息处理系统应遵循最小安装的原则, 只安装需要的组件和应用程序;
- b) 个人信息处理系统应关闭不需要的系统服务、默认共享和高危端口;
- c) 个人信息处理系统应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制;
- d) 个人信息处理系统应能够发现存在的已知漏洞, 并在经过充分测试评估后, 及时修补漏洞;
- e) 个人信息处理系统应能够检测到对重要节点的入侵行为并进行防御, 并在发生严重入侵事件时提供报警;

5.2.3.5 恶意代码防范和程序可信执行

应采取免受恶意代码攻击的技术措施或可信验证机制对系统程序、应用程序和重要配置文件/参数进行可信执行验证, 并在检测到其完整性受到破坏时采取恢复措施。

5.2.3.6 资源控制

- a) 应限制单个用户或进程对个人信息处理和存储设备系统资源的最大使用限度;
- b) 应提供重要节点设备的硬件冗余, 保证系统的可用性;
- c) 应对重要节点进行监视, 包括监视CPU、硬盘、内存等资源的使用情况;
- d) 应能够对重要节点的服务水平降低到预先规定的最小值进行检测和报警。

5.2.4 应用和数据安全

5.2.4.1 身份鉴别

- a) 个人信息处理系统应对登录的用户进行身份标识和鉴别, 该身份标识应具有唯一性, 鉴别信息应具有复杂度并要求定期更换;

b) 个人信息处理系统应提供并启用登录失败处理功能，并在多次登录后采取必要的保护措施；

c) 个人信息处理系统应强制用户首次登录时修改初始口令，当确定信息被泄露后，应提供提示全部用户强制修改密码的功能，在验证确认用户后修改密码；

d) 用户身份鉴别信息丢失或失效时，应采取技术措施保证鉴别信息重置过程的安全；

e) 应采取静态口令、动态口令、密码技术、生物技术等两种或两种以上的组合鉴别技术对用户进行身份鉴别，且其中一种鉴别技术使用密码技术来实现。

5.2.4.2 访问控制

a) 个人信息处理系统应提供访问控制功能，并对登录的用户分配账户和权限；

b) 应重命名或删除默认账户，修改默认账户的默认口令；

c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；

d) 应授予不同账户为完成各自承担任务所需的最小权限，在它们之间形成相互制约的关系；

e) 应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则

f) 访问控制的粒度应达到主体为用户级，客体为文件、数据库表级、记录或字段级；

g) 个人信息应设置安全标记，控制主体对有安全标记资源的访问。

5.2.4.3 安全审计

a) 个人信息处理系统应提供安全审计功能，审计应覆盖到每个用户，应对重要的用户行为和重要的安全事件进行审计；

b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；

c) 应对审计记录进行保护，定期备份，并避免受到未预期的删除、修改或覆盖等；

d) 审计记录的留存时间应符合法律法规的要求；

e) 应对审计进程进行保护，防止未经授权的中断。

5.2.4.4 软件容错

a) 应提供个人信息的有效性校验功能，保证通过人机接口输入或通过通信接口输入的内容符合个人信息处理系统设定要求；

b) 应能够发现个人信息处理系统软件组件可能存在的已知漏洞，并能够在充分测试评估后及时修补漏洞；

c) 应能够在故障发生时，继续提供一部分功能，并能够实施必要的措施。

5.2.4.5 资源控制

a) 在通信双方中的一方在一段时间内未做任何响应时，另一方应能够自动结束会话；

b) 应对个人信息处理系统的最大并发会话连接数进行限制；

c) 应能够对单个用户的多重并发会话进行限制。

5.2.4.6 数据完整性

a) 应采取校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据和个人信息；

b) 应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据和个人信息。

5.2.4.7 数据保密性

a) 应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据和个人信息；

b) 应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据和个人信息。

5.2.4.8 数据备份恢复

a) 应提供个人信息的本地数据备份与恢复功能，定期对备份数据进行恢复测试，保证数据可用性；

b) 应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地；

c) 应提供重要数据处理系统的热冗余，保证系统的高可用性。

5.2.4.9 剩余信息保护

a) 应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除；

b) 应保证存有个人信息的存储空间被释放或重新分配前得到完全清除。

5.3 扩展要求

5.3.1 云计算安全扩展要求

a) 应确保个人信息在云计算平台中存储于中国境内，如需出境应遵循国家相关规定；

b) 应使用校验技术或密码技术保证虚拟机迁移过程中，个人信息的完整性，并在检测到完整性受到破坏时采取必要的恢复措施；

c) 应使用密码技术保证虚拟机迁移过程中，个人信息的保密性，防止在迁移过程中的个人信息泄露。

5.3.2 物联网安全扩展要求

物联网感知节点设备采集信息回传应采用密码技术保证通信过程中个人信息的保密性。

6 业务流程

6.1 收集

个人信息的收集行为应满足以下要求：

a) 个人信息收集前，应当遵循合法、正当、必要的原则向被收集的个人信息主体公开收集、使用规则，明示收集、使用信息的目的、方式和范围等信息；

b) 个人信息收集应获得个人信息主体的同意和授权，不应收集与其提供的服务无关的个人信息，不应通过捆绑产品或服务各项业务功能等方式强迫收集个人信息；

c) 个人信息收集应执行收集前签署的约定和协议，不应超范围收集；

d) 不应大规模收集或处理我国公民的种族、民族、政治观点、宗教信仰等敏感数据；

e) 个人生物识别信息应仅收集和使用摘要信息，避免收集其原始信息；

f) 应确保收集个人信息过程的安全性：

1) 收集个人信息之前，应有对被收集人进行身份认证的机制，该身份认证机制应具有相应安全性；

2) 收集个人信息时，信息在传输过程中应进行加密等保护处理；

3) 收集个人信息的系统应落实网络安全等级保护要求；

4) 收集个人信息时应有对收集内容进行安全检测和过滤的机制，防止非法内容提交。

6.2 保存

个人信息的保存行为应满足以下要求：

a) 在境内运营中收集和产生的个人信息应在境内存储，如需出境应遵循国家相关规定；

b) 收集到的个人信息应采取相应的安全加密存储等安全措施进行处理；

c) 应对保存的个人信息根据收集、使用目的、被收集人授权设置相应的保存时限；

d) 应对保存的个人信息在超出设置的时限后予以删除；

e) 保存信息的主要设备，应对个人信息数据提供备份和恢复功能，确保数据备份的频率和时间间隔，并使用不少于以下一种备份手段：

1) 具有本地数据备份功能；

2) 将备份介质进行场外存放；

3) 具有异地数据备份功能。

6.3 应用

个人信息的应用应满足以下要求：

a) 对个人信息的应用，应符合与个人信息主体签署的相关协议和规定，不应超范围应用个人信息；

注：经过处理无法识别特定个人且不能复原的个人信息数据，可以超出与信息主体签署的相关使用协议和约定，但应提供适当的保护措施进行保护。

b) 个人信息主体应拥有控制本人信息的权限，包括：

1) 允许对本人信息的访问；

2) 允许通过适当方法对本人信息的修改或删除，包括纠正不准确和不完整的数据，并保证修改后的本人信息具备真实性和有效性；

c) 完全依靠自动化处理的画像技术应用于精准营销、搜索结果排序、个性化推送新闻、定向投放广告等增值应用，可事先不经用户明确授权，但应确保

用户有反对或者拒绝的权利；如应用于征信服务、行政司法决策等可能对用户带来法律后果的增值应用，或跨网络运营者使用，应经用户明确授权方可使用其数据；

d) 应对个人信息的接触者设置相应的访问控制措施，包括：

1) 对被授权访问个人信息数据的工作人员按照最小授权的原则，只能访问最少够用的信息，只具有完成职责所需的最少的数据操作权限；

2) 对个人信息的重要操作设置内部审批流程，如批量修改、拷贝、下载等；

3) 对特定人员超限制处理个人信息时配置相应的责任人或负责机构进行审批，并对这种行为进行记录。

e) 应对必须要通过界面（如显示屏幕、纸面）展示的个人信息进行去标识化的处理。

6.4 删除

a) 个人信息在超过保存时限之后应进行删除，经过处理无法识别特定个人且不能复原的除外；

b) 个人信息持有者如有违反法律、行政法规的规定或者双方的约定收集、使用其个人信息时，个人信息主体要求删除其个人信息的，应采取措施予以删除；

c) 个人信息相关存储设备，将存储的个人信息数据进行删除之后应采取措施防止通过技术手段恢复；

d) 对存储过个人信息的设备在进行新信息的存储时，应将之前的内容全部进行删除；

e) 废弃存储设备，应在进行删除后再进行处理。

6.5 第三方委托处理

a) 在对个人信息委托处理时，不应超出该信息主体授权同意的范围；

b) 在对个人信息的相关处理进行委托时，应对委托行为进行个人信息安全

影响评估；

- c) 对个人信息进行委托处理时，应签订相关协议要求受托方符合本文件；
- d) 应向受托方进行对个人信息数据的使用和访问的授权；
- e) 受托方对个人信息的相关数据进行处理完成之后，应对存储的个人信息数据的内容进行删除。

6.6 共享和转让

个人信息原则上不得共享、转让。如存在个人信息共享和转让行为时，应满足以下要求：

- a) 共享和转让行为应经过合法性、必要性评估；
- b) 在对个人信息进行共享和转让时应进行个人信息安全影响评估，应对受让方的数据安全能力进行评估确保受让方具备足够的数据安全能力，并按照评估结果采取有效的保护个人信息主体的措施；
- c) 在共享、转让前应向个人信息主体告知转让该信息的目的、规模、公开范围数据接收方的类型等信息；
- d) 在共享、转让前应得到个人信息主体的授权同意，与国家安全、国防安全、公共安全、公共卫生、重大公共利益或与犯罪侦查、起诉、审判和判决执行等直接相关的情形除外；
- e) 应记录共享、转让信息内容，将共享、转让情况中包括共享、转让的日期、数据量、目的和数据接收方的基本情况在内的信息进行登记；
- f) 在共享、转让后应了解接收方对个人信息的保存、使用情况和个人信息主体的权利，例如访问、更正、删除、注销等；
- g) 当个人信息持有者发生收购、兼并、重组、破产等变更时，个人信息持有者应向个人信息主体告知有关情况，并继续履行原个人信息持有者的责任和义务，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。

6.7 公开披露

个人信息原则上不得公开披露。如经法律授权或具备合理事由确需公开披露时，应充分重视风险，遵守以下要求：

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，与国家安全、国防安全、公共安全、公共卫生、重大公共利益或与犯罪侦查、起诉、审判和判决执行等直接相关的情形除外；

c) 公开披露个人敏感信息前，除6.7 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) 准确记录和保存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) 不得公开披露个人生物识别信息和基因、疾病等个人生理信息；

g) 不得公开披露我国公民的种族、民族、政治观点、宗教信仰等敏感数据分析结果。

7 应急处置

7.1 应急机制和预案

a) 应建立健全网络安全风险评估和应急工作机制，在个人信息处理过程中发生应急事件时具有上报有关主管部门的机制；

b) 应制定个人信息安全事件应急预案，包括应急处理流程、事件上报流程等内容；

c) 应定期（至少每半年一次）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，留存应急培训和应急演练记录；

d) 应定期对原有的应急预案重新评估，修订完善。

7.2 处置和响应

a) 发现网络存在较大安全风险，应采取措施，进行整改，消除隐患；发生安全事件时，应及时向公安机关报告，协助开展调查和取证工作，尽快消除隐患；

b) 发生个人信息安全事件后，应记录事件内容，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；

c) 应对安全事件造成的影响进行调查和评估，采取技术措施和其他必要措施，消除安全隐患，防止危害扩大；

d) 应按《国家网络安全事件应急预案》等相关规定及时上报安全事件，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；

e) 应将事件的情况告知受影响的个人信息主体，并及时向社会发布与公众有关的警示信息。

(十六) 信息安全技术 数据出境安全评估指南

前 言

本标准按照GB/T 1.1-2009的规则起草。

本标准由全国信息安全标准化技术委员会（SAC/TC260）提出并归口。

本标准起草单位：上海华东电信研究院、工业和信息化部电信研究院、公安部第一研究所、阿里巴巴（北京）软件服务有限公司、北京大学互联网发展研究中心、中国电子技术标准化研究院、中国电子信息产业发展研究院、国家信息技术安全研究中心、深圳市腾讯计算机系统有限公司、阿里云计算有限公司、蚂蚁金服、国信优易数据有限公司。

本标准主要起草人：覃庆玲、洪延青、魏薇、张郁安、张媛媛、姜宇泽、陈诗洋、魏亮、韩煜、何延哲、郭晓雷、陈淦萍、李海涛、王洁萍、周波、李程远、赵冉冉、李克鹏、王昕、赵会敏、周润松、刘俊河、白晓媛、代威、贾思琪、邵华、杨国威、范洛鋤、王梦寅、柳雁军、顾伟、杨思磊、赵然、田申、乔建雄、马宁、唐一鸿、王秉正、王肃、胡影、张振涛、庞妹、郭建楠等。

引 言

近年来，随着互联网的蓬勃发展，数据流动无处不在。数据流动所产生的经济价值和社会价值凸显，这一过程中的安全风险也随之增加，国家安全、经济发展、社会公共利益、个人隐私受到严重威胁，防范数据泄露和滥用所产生的风险日益紧迫。

本标准规定了数据出境安全评估流程、评估要点、评估方法等内容，国家网信部门、行业主管部门以及网络运营者按照本指南对其向境外提供的个人信息和重要数据进行主管部门评估和安全自评估，发现存在的安全问题和风险，及时采取措施，确保个人信息和重要数据合法流动的同时，避免其对国家安全、经济发展、社会公共利益和个人信息主体权益造成不利影响。

1 范围

本标准提出了个人信息和重要数据出境的安全评估流程、要点和方法。

本标准适用于网络运营者开展的个人信息和重要数据出境安全自评估，以及国家网信部门、行业主管部门组织开展的个人信息和重要数据出境安全评估。

2 安全自评估规范性引用文件

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 AAAAA-AAAA 信息安全技术 个人信息安全规范

GB/T 20984-2007 信息安全技术 信息安全风险评估规范

3 术语和定义

GB/T AAAAA-AAAA 《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 网络运营者 network operator

网络的所有者、管理者和网络服务提供者。

3.2 境内运营 domestic operation

网络运营者在中华人民共和国境内开展业务，提供产品或服务的活动。

注1：未在中华人民共和国境内注册的网络运营者，但在中华人民共和国境内开展业务，或向中华人民共和国境内提供产品或服务的，属于境内运营。判断网络运营者是否在中华人民共和国境内开展业务，或向中华人民共和国境内提供产品或服务的参考因素包括但不限于：使用中文；以人民币作为结算货币；向中国境内配送物流等。

注2: 中华人民共和国境内的网络运营者仅向境外机构、组织或个人开展业务、提供商品或服务, 且不涉及境内公民个人信息和重要数据的, 不视为境内运营。

3.3 个人信息 personal data

以电子或以其他方式记录的能够单独或与其他信息结合识别自然人身份的各种信息, 如姓名、出生日期、身份证号、个人账号信息、住址、电话号码、指纹、虹膜等。

注: 关于个人信息的范围和类别可参考《信息安全技术 个人信息安全规范》附录A

3.4 个人敏感信息 personal sensitive information

指一旦泄露、披露或滥用可能危害人身和财产安全、损害个人名誉和身心健康、导致歧视性待遇等的个人信息。通常情况下, 身份证号、银行卡号、健康记录、生物识别等属于个人敏感信息。

注: 关于个人敏感信息的范围和类别可参考《信息安全技术 个人信息安全规范》附录B。

3.5 重要数据 important data

相关组织、机构和个人在境内收集、产生的不涉及国家秘密, 但与国家安全、经济发展以及公共利益密切相关的数据(包括原始数据和衍生数据)。

注1: 具体范围见附录A。

注2: 经政府信息公开渠道合法公开的, 不再属于重要数据。

3.6 加工处理 data processing

针对个人信息和重要数据实施的操作, 包括个人信息和重要数据的收集、存储、访问、修改、转让、披露、匿名化、去标识化、恢复、删除、销毁等。

3.7 数据出境 data cross-border transfer

网络运营者通过网络等方式，将其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，通过直接提供或开展业务、提供服务、产品等方式提供给境外的机构、组织或个人的一次性活动或连续性活动。

注1：以下情形属于数据出境：

- a) 向本国境内，但不属于本国司法管辖或未在境内注册的主体提供个人信息和重要数据；
- b) 数据未转移存储至本国以外的地方，但被境外的机构、组织、个人访问查看的（公开信息、网页访问除外）；
- c) 网络运营者集团内部数据由境内转移至境外，涉及其在境内运营中收集和产生的个人信息和重要数据的。

注2：非在境内运营中收集和产生的个人信息和重要数据经由本国出境，未经任何变动或加工处理的，不属于数据出境。

注3：非在境内运营中收集和产生的个人信息和重要数据在境内存储、加工处理后出境，不涉及境内运营中收集和产生的个人信息和重要数据的，不属于数据出境。

3.8 数据出境安全风险 risk of data cross-border transfer

数据出境可能对国家安全、经济发展、社会公共利益和个人合法权益带来的风险。

3.9 安全自评估 self assessment

网络运营者依照相关国家法律法规和标准的规定，自行组织或委托网络安全服务机构对数据出境开展安全评估。

3.10 主管部门评估 competent authority assessment

国家网信部门、行业主管部门依照相关国家法律法规和标准的规定组织对数据出境开展主管部门评估。

3.11 数据脱敏处理 data masking

对个人信息和重要数据通过脱敏规则进行数据变形处理，降低其敏感程度。

3.12 个人信息主体同意 consent of personal information subject

个人信息主体通过书面声明或主动做出肯定性动作，对其个人信息出境做出明确授权的行为。

4 评估流程

4.1 评估总体流程

数据出境安全评估首先评估数据出境目的；数据出境目的不具有合法性、正当性和必要性，不得出境。在此基础上评估数据出境安全风险，将数据出境及再转移后被泄露、损毁、篡改、滥用等风险有效地降至最低限度。具体流程如图 1。

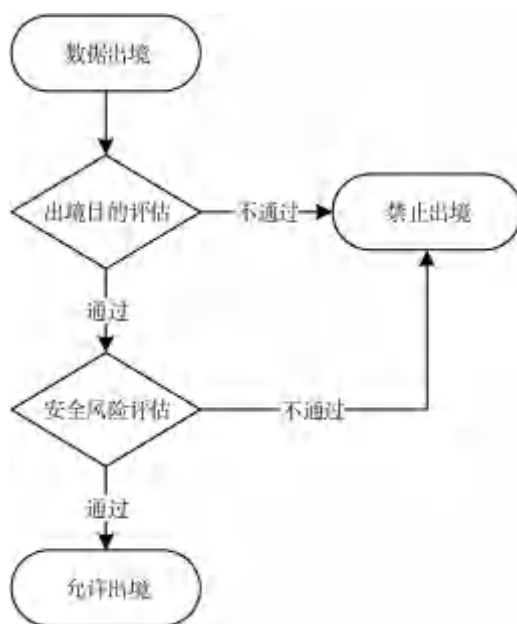


图 1 数据出境安全评估总体流程

4.2 安全自评估流程

4.2.1 概述

在数据出境安全自评估启动后，数据出境安全自评估工作组审查数据出境计划，对个人信息与重要数据依照流程进行评估，并形成评估报告。

数据出境满足上报要求的，评估报告应按要求报送国家网信部门、行业主管部门。

数据出境需获得国家网信部门、行业主管部门同意的，应在数据出境前将评估报告按要求报送国家网信部门、行业主管部门，并获得其同意。

对评估结果为可以出境的，依照出境计划进行出境，对评估结果禁止出境的，提出出境计划修改建议，业务部门修改出境计划，降低数据出境安全风险后，重新进行评估。

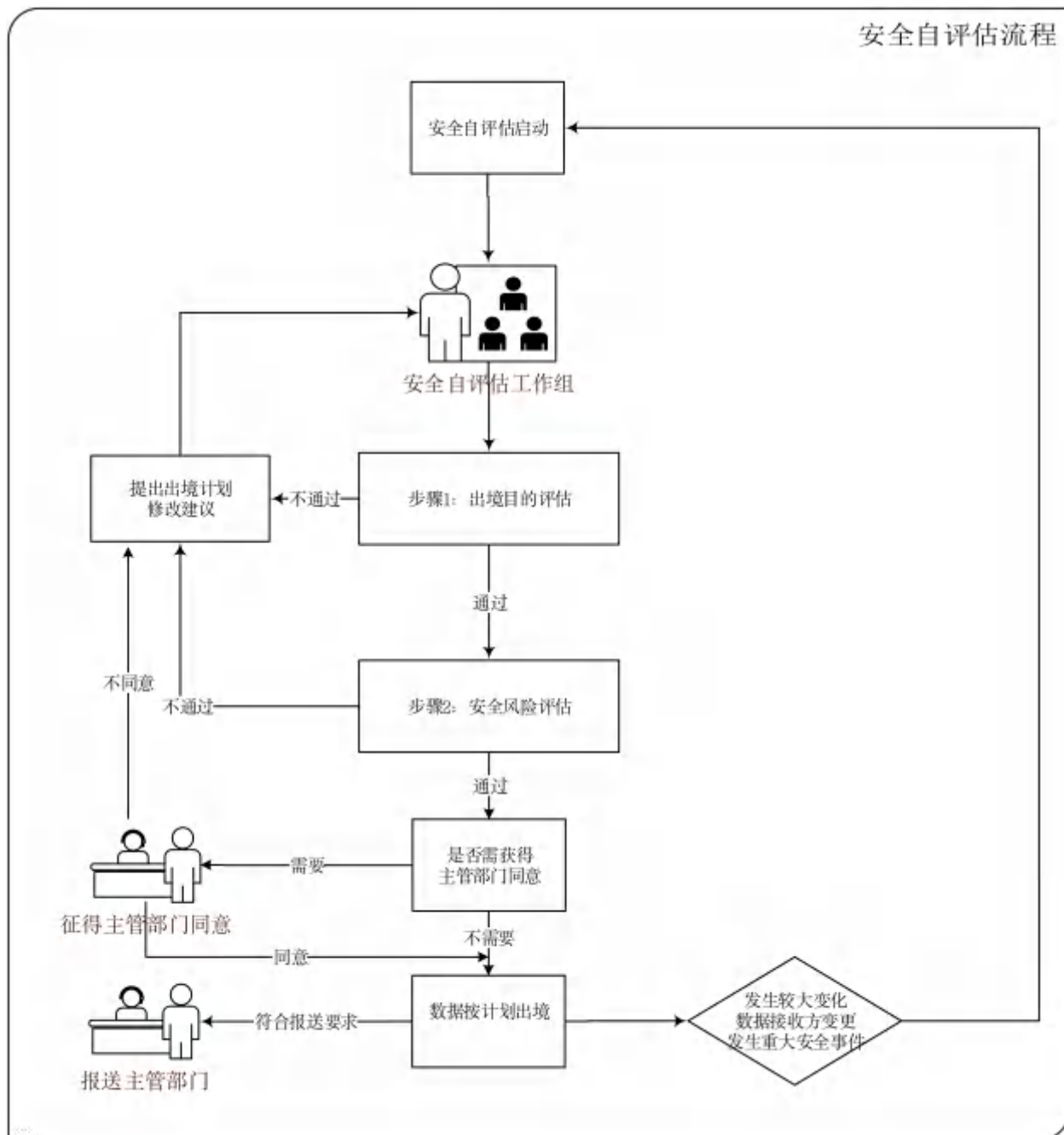


图 2 安全自评估流程

4.2.2 安全自评估启动条件

网络运营者应每年开展安全自评估，满足以下条件之一时启动评估：

- a) 涉及数据出境的；
- b) 关键信息基础设施运营者进行数据出境之前的；

- c) 已完成数据出境安全自评估的产品或业务所涉及的个人信息和重要数据出境，在目的、范围、类型、数量等方面发生较大变化、数据接收方变更或发生重大安全事件的；
- d) 按照行业主管或者监管部门要求启动的。

注1：当网络运营者的数据出境满足连续出境的条件时，视为一次出境行为，免于重复评估；

注2：连续出境是指数据出境的目的、接收方相同，范围、类型、数量不发生较大变化，且两次数据出境间隔不超过一年的。

注3：数据出境涉及多方主体的如：云服务、转包服务等，根据数据出境发起方，确定安全自评估责任主体。如：云服务客户主动要求云服务提供商进行数据出境的，由云服务提供商配合云服务客户开展安全自评估，且由云服务客户承担相应责任。如云服务提供商主动要求进行数据出境的，由云服务提供商配合云服务提供商开展安全自评估，且由云服务提供商承担相应责任。

4.2.3 安全自评估工作组

网络运营者应建立数据出境安全自评估工作组，工作组主要包含法务、政策、安全、技术、管理相关专业人员。数据出境安全自评估工作组应负责审查业务部门提交的数据出境计划，并定期对数据出境情况开展检查、抽查。

4.2.4 制定数据出境计划

网络运营者有数据出境需求的业务部门应制定数据出境计划，计划的内容包括但不限于：

- a) 涉及个人信息情况，包括个人信息的类型、数量、范围和敏感程度等；
- b) 涉及重要数据情况，包括重要数据的类型、数量和范围等；
- c) 涉及的信息系统情况；

- d) 数据发送方安全保护能力;
- e) 数据接收方安全保护能力及其所在的国家或地区的基本情况。

4.2.5 安全自评估要点及方法

网络运营者需按照本标准第 5 章中的评估要点及附录 B 中的评估方法进行安全自评估。经评估, 数据出境计划不满足出境目的评估中合法性、正当性和必要性要求的或数据出境安全风险评估中的出境安全风险为高或极高的, 个人信息和重要数据不得出境。

4.2.6 安全自评估报告

网络运营者在完成数据出境安全自评估后, 应形成安全自评估报告。安全自评估报告内容应包括但不限于: 安全自评估对象基本情况、安全自评估组织实施情况、安全自评估结果、数据出境安全风险点、检查修正建议。安全自评估报告应至少保存 2 年, 并在如下情况下将安全自评估报告上报行业主管部门, 行业主管部门不明确的, 报国家网信部门。

- a) 关键信息基础设施运营者开展的安全自评估;
- b) 一年内出境的个人信息数量达到国家网信部门、行业主管部门上报要求的;
- c) 包含核设施、生物化学、国防军工、人口健康等领域数据, 大型工程活动、海洋环境敏感地理信息数据, 以及其他重要数据的;
- d) 涉及关键信息基础设施的安全缺陷、具体安全防护措施等网络安全信息的;
- e) 其他可能影响国家安全、经济发展和社会公共利益的。

4.2.7 检查修正

如果安全自评估结果为禁止出境的, 网络运营者应采用相关措施降低数据出境安全风险, 并修正数据出境计划, 重新开展安全自评估。

注：可用于降低数据出境安全风险的措施包括但不限于：精简出境数据内容、使用技术手段处理数据降低敏感程度、提升数据发送方安全保障能力、限定数据接收方的处理活动、更换数据保护水平更高的接收方、选择政治法律环境保障能力较高地区的数据接收方等。在网络运营者进行相应调整后，可重新对数据出境进行安全风险安全自评估。

4.3 主管部门评估流程

4.3.1 概述

在数据出境主管部门评估启动之后，国家网信部门、行业主管部门确定主管部门评估范围，制定主管部门评估方案，并成立主管部门评估工作组。

网络运营者按要求向主管部门评估工作组提交相关材料，材料包括安全自评估报告以及相关证明资料等。

主管部门评估工作组根据主管部门评估方案，通过远程检测、现场检查等方式进行主管部门评估并形成主管部门评估报告。

专家委员会对主管部门评估工作组做出的主管部门评估报告、安全自评估报告进行审议并给出是否同意数据出境的建议。

国家网信部门、行业主管部门根据专家委员会建议做出决定。

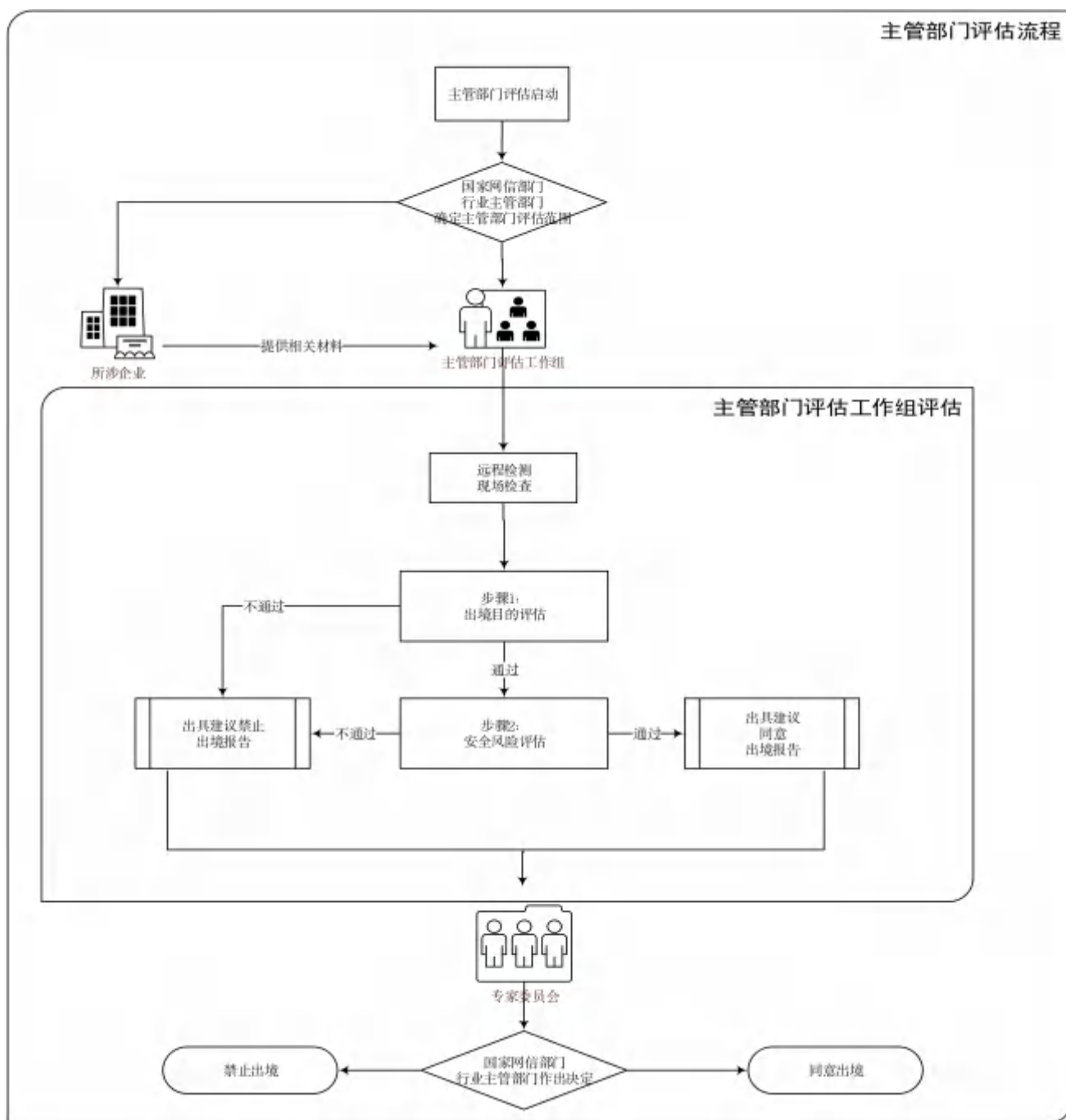


图 3 主管部门评估流程

4.3.2 主管部门评估启动条件

国家网信部门、行业主管部门根据数据出境类型、数量、范围、重要程度等，酌情组织开展主管部门评估。具有下列情形之一的，国家网信部门、行业主管部门可启动主管部门评估：

- a) 一年内出境的个人信息数量达到国家网信部门、行业主管部门上报要求

的；

- b) 包含核设施、生物化学、国防军工、人口健康等领域数据，大型工程活动、海洋环境、敏感地理信息数据，以及其他重要数据的；
- c) 涉及关键信息基础设施的安全缺陷、具体安全防护措施等网络安全信息的；
- d) 关键基础设施运营者数据出境的；
- e) 其他可能影响国家安全、经济发展和社会公共利益的；
- f) 大量用户投诉、举报的；
- g) 全国性行业协会建议的；
- h) 其他经国家网信部门、行业主管部门认定有必要启动主管部门评估的。

注：数据出境涉及多方主体的，如：云服务等，根据数据出境发起方，确定主管部门评估责任主体。

4.3.3 制定主管部门评估方案

主管部门评估启动后，国家网信部门、行业主管部门制定主管部门评估方案，主管部门评估方案的内容包括但不限于：

- a) 确定主管部门评估对象：国家网信部门、行业主管部门可以根据网络运营者提交的安全自评报告、全国性行业协会建议、大量用户的投诉举报，按程序确定主管部门评估对象。
- b) 成立主管部门评估工作组：确定主管部门评估对象后国家网信部门、行业主管部门与网络安全服务机构成立主管部门评估工作组。
- c) 制定主管部门评估程序与方法：主管部门评估工作组根据网络运营者提交的评估报告制定主管部门评估程序与方法。

4.3.4 主管部门评估工作组

主管部门评估方案制定后，国家网信部门、行业主管部门成立数据出境主管部门评估工作组，主管部门评估工作组根据评估方案，通过远程检测、现场检查的方式负责对主管部门评估对象的出境情况开展评估，形成主管部门评估报告。

4.3.5 主管部门评估要点及方法

主管部门评估工作组可参考本标准第5章中的评估要点及附录B中的评估方法进行主管部门评估。经评估，数据出境计划不满足出境目的评估中合法性、正当性和必要性要求的或数据出境安全风险评估中的出境安全风险为高或极高的，个人信息和重要数据不得出境。

4.3.6 主管部门评估报告

主管部门评估工作组完成对数据出境计划的主管部门评估后，应形成主管部门评估报告，且应包括但不限于如下内容：

- a) 数据出境主管部门评估结果及理由；
- b) 数据出境重大风险点；
- c) 数据出境计划检查修正建议。

4.3.7 专家委员会审议

国家网信部门、行业主管部门组织成立包括网络安全专家、数据安全专家以及所在行业专家等的专家委员会，专家委员会负责对企业提交的安全自评估报告和主管部门评估报告进行研讨分析，给出是否同意数据出境的建议。

4.3.8 形成主管部门评估结论

国家网信部门、行业主管部门结合主管部门评估报告以及专家委员会建议做出是否同意数据出境的决定，并书面告知被评估主体。

4.3.9 主管部门安全检查

国家网信部门、行业主管部门可根据安全自评估结果、主管部门评估结论，结合网络运营者数据出境情况，定期对网络运营者开展的数据出境进行安全检

查，形成检查结果及整改建议并书面告知被检查主体。

5 评估要点

5.1 出境目的

数据出境计划中出境目的应同时满足合法性、正当性和必要性的要求：

a) 合法性包括以下情况：

- 1) 不属于法律法规明令禁止的；
- 2) 不属于国家网信部门、公安部门、安全部门等有关部门认定不能出境的。

注1：拨打国际及漫游电话、发送国际电子邮件、进行国际即时通信、通过互联网进行跨境交易以及其他个人主动行为，视为个人信息主体已经同意。

注2：将合法向社会公开披露的个人信息出境，视为个人信息主体已经同意。

注3：网络运营者在取得个人信息主体同意前，应将数据出境目的、类型、数据接收方情况及数据出境可能存在的风险，网络运营者的联系人及其联系方式等信息明确告知个人信息主体。

注4：当网络运营者隐私规则发生变更、数据出境目的、范围、类型、数量发生较大变化、数据接收方发生变更或数据出境风险发生较大变化时应重新取得个人信息主体同意。

b) 正当性包括以下情况：

- 1) 个人信息主体已同意的。虽未经个人信息主体同意但是危及公民生命财产安全等紧急情况除外；
- 2) 不违反相关主管部门规定的。

c) 必要性包括以下任一种或几种情况：

- 1) 履行合同义务所必需的；

- 2) 同一机构、组织内部开展业务所必需的；
- 3) 我国政府部门履行公务所必需的；
- 4) 履行我国政府与其他国家和地区、国际组织签署的条约、协议所必需的；
- 5) 其他维护网络空间主权和国家安全、经济发展、社会公共利益和保护公民合法利益需要的。

5.2 安全风险

5.2.1 概述

评估数据出境计划的安全风险，应综合考虑出境数据的属性和数据出境发生安全事件的可能性及影响程度：

a) 数据属性：

- 1) 个人信息的属性，包括类型、数量、范围、敏感程度和技术处理情况等；
- 2) 重要数据的属性，包括类型、数量、范围和技术处理情况等；
- 3) 当数据出境同时包含个人信息和重要数据时，应同时满足上述两条评估要求。

b) 数据出境发生安全事件的可能性及影响程度：

- 1) 发送方数据出境的技术和管理能力；
- 2) 数据接收方的安全保护能力、采取的措施；
- 3) 数据接收方所在国家或区域的政治法律环境。

5.2.2 个人信息属性评估要点

5.2.2.1 类型和敏感程度

应识别个人信息中所包含的信息类型，并判断其是否涉及个人敏感信息。个

人信息的类型参照 GB/T AAAAA-AAAA 《信息安全技术 个人信息安全规范》附录 A；个人信息的敏感程度参照 GB/T AAAAA-AAAA 《信息安全技术 个人信息安全规范》附录 B。

5.2.2.2 数量

应评估所涉及的个人信息主体数量以及所涉及的主要人群的群体特征，当数据出境涉及的个人信息主体数量达到或超过一定量级时，个人信息会出现数据汇集后的衍生价值。

5.2.2.3 范围

应评估出境个人信息范围是否符合最小化原则：

- a) 向境外传输的个人信息应与出境目的相关的业务功能有直接关联。直接关联是指没有该信息的参与，相应功能无法实现；
- b) 向境外自动传输的个人信息频率应是和数据出境目的相关的业务功能所必需的频率；
- c) 向境外传输的个人信息数量应是和数据出境目的相关的业务功能所必需的数量。

5.2.2.4 技术处理情况

应评估个人信息技术处理情况：

- a) 是否在数据出境前使用技术措施对个人信息进行了数据脱敏处理；
- b) 数据脱敏效果是否有效可靠，达到了合理程度的不可还原。

5.2.3 重要数据属性评估要点

5.2.3.1 类型

应评估识别重要数据的类型，重要数据类型见附录 A：《重要数据识别指南》。

5.2.3.2 数量

应评估重要数据出境数量，重要数据数量影响其所蕴含的社会、经济价值，数量越大，发生泄漏、披露或滥用时，对国家安全、经济发展和社会公共利益造成的危害越大。

5.2.3.3 范围

重要数据出境范围应符合最小化原则：

- a) 向境外传输的数据应与出境目的相关的业务功能应有直接关联。即没有该信息的参与，相应功能无法实现；
- b) 向境外自动传输的数据频率应是和数据出境目的相关的业务功能所必需的频率；
- c) 向境外传输的数据数量应是和数据出境目的相关的业务功能所必需的数量。

5.2.3.4 技术处理情况

应评估重要数据技术处理情况：

- a) 是否使用技术措施对重要数据进行了数据脱敏处理；
- b) 数据脱敏效果是否有效可靠，达到了合理程度的不可还原。

5.2.4 数据发送方的安全保护能力

5.2.4.1 管理制度保障能力

应评估发送方管理制度保障能力：

- a) 安全管理制度
 - 1) 应具备数据出境安全管理体系，包括但不限于：安全策略、管理制度、数据出境安全操作流程；
 - 2) 安全策略管理文件中应包含：总体目标、原则、总体框架等；

- 3) 安全管理制度中应对出境数据的数量、范围、类型及其敏感程度等进行描述;
- 4) 数据出境安全操作流程应包括: 数据出境计划、数据出境安全评估报告等。

b) 人员管理

- 1) 应在组织内部指定数据出境安全管理人员, 并确保其履行相应职责, 包括但不限于: 数据出境的审计、评估报告的编写与提交、配合主管部门监督检查、处理有关纠纷等;
- 2) 应在组织内部建立数据出境相关人员的培训和考核机制。

c) 合同约束

- 1) 应约定数据接收方的数据处理目的、方式和采取的安全措施;
- 2) 应约定数据接收方配合数据发送方对数据出境活动进行调查;
- 3) 应约定在未获得数据发送方的授权前提下, 数据接收方不得对数据进行公开披露及再转移;
- 4) 应约定数据接收方使用、留存数据的合法周期及超出合法周期后数据接收方应对数据采取的处理措施如: 删除、销毁等;
- 5) 应约定数据接收方配合数据发送方响应个人信息主体的请求, 如: 访问、更正、删除等。

d) 审计机制

- 1) 应对数据出境安全策略、管理制度、出境操作流程以及安全措施的有效性进行审计, 并形成审计结果;
- 2) 审计结果应能支持事件的处置、应急响应和事后调查;
- 3) 应防止非授权访问、篡改或删除审计记录。

e) 应急处置

- 1) 应制定数据出境安全事件应急预案，应急预案应包含应急处置、安全事件告知和上报等相关内容；
- 2) 应定期组织内部相关人员进行应急响应培训和应急演练；
- 3) 当发生数据出境安全事件时，启动应急预案。如：数据接收方发生数据泄露、损毁、滥用等安全事件时；
- 4) 当发生数据出境安全事件时，应及时将数据出境安全事件的相关情况告知受影响方；难以逐一告知时，应采取合理、有效的方式发布有关的警示信息；
- 5) 当发生数据出境安全事件时，应按照国家有关规定及时向国家网信部门或行业主管部门上报数据出境安全事件，上报内容包括但不限于：安全事件发生的时间、数据类型、数量、范围、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；
- 6) 应根据相关法律法规变化情况，以及事件处置情况，及时更新应急响应预案。

f) 申诉管理

- 1) 应建立针对数据出境的申诉管理机制和跟踪流程；
- 2) 应在合理的时间内，对申诉进行响应；
- 3) 应公开申诉的渠道和机制。

5.2.4.2 技术手段保障能力

应评估发送方技术手段保障能力：

- a) 应具备在数据出境传输时采取相应安全措施的能力，如加密传输等；
- b) 应具备针对数据安全事件的预防、检测及响应能力；

- c) 应具备整体的数据安全技术防护体系，保障所传输数据的保密性、完整性和可用性；
- d) 应具备数据传输过程中实施身份鉴别和访问控制的能力，防止数据接收方或第三方非授权访问和调取数据；
- e) 应具备保留数据发送日志的能力，日志内容包括但不限于：数据发送的时间、类型、数量、范围、方式、接收方，数据发送日志至少保存 2 年；
- f) 应具备对数据发送、传输、销毁等各阶段进行审计的能力；
- g) 应对数据出境传输的安全措施定期评估，及时发现并修复安全漏洞；
- h) 若数据出境过程中存在经由第三国中转的，应采取相关技术手段保障数据在中转过程中不被非法访问或调取。

5.2.5 数据接收方的安全保护能力

5.2.5.1 主体背景情况

应评估接收方主体背景情况：

- a) 应判断数据接收方是否具有真实有效的主体资质证明；
- b) 应判断数据接收方是否出现过数据安全相关事件，是否进行了及时有效的处置；
- c) 涉及重要数据出境的，应能获得数据接收方的股东构成或主管部门等背景信息。

5.2.5.2 管理制度保障能力

应评估接收方管理制度保障能力：

- a) 安全管理制度
 - 1) 应依据业务需求和数据安全合规要求，制定并执行数据安全管理的方针和策略；

- 2) 应建立数据接收、保存、使用、传输、销毁等阶段的的安全管理制度, 提出各阶段的安全管理要求;
- 3) 应建立数据安全风险的预防、发现、应急处置、问责机制等。

b) 人员管理

- 1) 应在组织内部指定数据安全机构和人员, 并确保其履行数据安全保护职责;
- 2) 处理数据的人员应具备专业的数据安全知识和技能, 能够理解并严格执行数据安全合规要求。

c) 审计机制

- 1) 应对数据安全策略、管理制度、操作流程以及安全措施的有效性进行审计, 并形成审计结果;
- 2) 审计结果应能支持事件的处置、应急响应和事后调查;
- 3) 应防止非授权访问、篡改或删除审计记录。

d) 应急处置

- 1) 应制定涉及接收数据安全事件的应急预案, 应急预案应包含应急处置、安全事件告知和上报等相关内容;
- 2) 应定期组织内部相关人员进行应急响应培训和应急演练;
- 3) 当发生涉及接收数据的安全事件时, 启动应急预案, 并及时告知数据发送方;
- 4) 应根据相关法律法规变化情况, 以及事件处置情况, 及时更新应急响应预案。

5.2.5.3 技术手段保障能力

应评估接收方技术手段保障能力:

- a) 应具备针对数据安全事件的预防、检测及响应能力;
- b) 应具备整体的数据安全技术防护体系,保障所接收数据的保密性、完整性和可用性;
- c) 应具备数据处理过程中实施身份鉴别和访问控制的能力;
- d) 应具备保留数据接收日志的能力,日志内容包括但不限于数据接收的时间、数据类型、数量、范围、方式、发送方,数据接收日志至少保存 2 年;
- e) 应具备对数据接收、保存、使用、传输、销毁等各阶段进行审计的能力;
- f) 应具备对数据存储介质安全管理,及对数据进行备份和恢复的能力。

5.2.6 数据接收方所在国家或区域的政治法律环境

5.2.6.1 个人信息

涉及个人信息出境时,对数据接收方所在国家或地区的政治法律环境的评估包括:

- a) 该国家或地区现行的个人信息保护法律法规及普遍适用的标准情况;
- b) 该国家或地区加入的区域或全球性的个人信息保护方面的组织,以及所做出的具有约束力的承诺;
- c) 该国家或地区落实个人信息保护的机制,如:是否具备负责个人信息保护的执法机构和相关司法机构等。

5.2.6.2 重要数据

涉及重要数据出境时,对数据接收方所在国家或地区的政治法律环境评估包括:

- a) 该国家或地区在数据安全方面现行的法律法规及普遍适用的标准情况;
- b) 该国家或地区主管数据安全的执法机构和相关司法机构等;
- c) 该国家或地区的执法机构、司法机构等部门调取数据的权力和法律程序;

- d) 该国家或地区与其他国家或地区之间是否缔结有关数据流通、共享等方面的双边或多边协定，包括在执法、监管等方面数据流通、共享的双多边协定。

(规范性附录)
重要数据识别指南

《重要数据识别指南》中的重要数据是指相关组织、机构和个人在境内收集、产生的不涉及国家秘密，但与国家安全、经济发展以及公共利益密切相关的数据(包括原始数据和衍生数据)，一旦未经授权披露、丢失、滥用、篡改或销毁，或汇聚、整合、分析后，可能造成以下后果：

- a) 危害国家安全、国防利益，破坏国际关系；
- b) 损害国家财产、社会公共利益和个人合法利益；
- c) 影响国家预防和打击经济与军事间谍、政治渗透、有组织犯罪等；
- d) 影响行政机关依法调查处理违法、渎职或涉嫌违法、渎职行为；
- e) 干扰政府部门依法开展监督、管理、检查、审计等行政活动，妨碍政府部门履行职责；
- f) 危害国家关键基础设施、关键信息基础设施、政府系统信息系统安全；
- g) 影响或危害国家经济秩序和金融安全；
- h) 可分析出国家秘密或敏感信息；
- i) 影响或危害国家政治、国土、军事、经济、文化、社会、科技、信息、生态、资源、核设施等其它国家安全事项。

根据上述定义和行业（领域）主管部门相关规定，指南提出了各行业(领域)重要数据的范围。各行业（领域）主管部门应结合实际，明确本行业（领域）重要数据定义、范围或判定依据；并根据行业（领域）发展变化，及时更新或替换本指南中相关内容。

本指南不影响中国在《世贸组织协定》等国际协定项下义务的执行。

A.1 石油天然气

主管部门：国家发展改革委、能源局。

重要数据包括但不限于：

- a) 价值类，包括表示资源金额等信息；
- b) 生产量类，包括各类生产量等信息；
- c) 销售量类，包括各类销售量等信息；
- d) 施工作业量类，包括各类施工作业量等信息；
- e) 安全与环保类，包括计量管理、节能管理、劳保用品、危险作业区、质量控制等信息；
- f) 储备类，包括储备数量、储备设施位置、坐标等信息。

A.2 煤炭

主管部门：国家发展改革委、能源局。

重要数据包括但不限于：

- a) 行业基本情况，主要包括企业数量、企业分布、企业类型、从业人员数量、从业人员分布等；
- b) 行业经济情况，主要包括行业的资产、负债、收入、利润、主要经济指标、行业资金紧张程度等；
- c) 行业采购情况，主要包括原材料的采购量、采购金额、采购价格以及采购周期等；
- d) 行业生产情况，主要包括行业的产值、生产投入、劳动生产率、产能以及产能影响因素等；
- e) 行业销售情况，主要包括行业市场规模、销售投入、人均销售水平、主要产品销售价格等；
- f) 行业投资情况，主要包括行业新建项目数量、投资额、资金来源等。

A.3 石化

主管部门：能源局。

重要数据包括但不限于：

- a) 国家石油、石化工业年度和中、长期发展规划的主要经济技术指标和重大政策措施；
- b) 石化工业重要生产物资年度进口计划和未分配的控制外汇金额。

A.4 电力

主管部门：国家发展改革委、能源局。

重要数据包括但不限于：

A.4.1 发电厂相关信息

- a) 火电厂的用煤量、水电厂的耗水量等信息；
- b) 发电机组数据，包括火电、水电等发电机组可靠性指标数据等信息；
- c) 电厂内变电站的开关数据，包括厂站名、开关类型、电抗值、母线电压、投入时间、退出时间等信息。

A.4.2 输配电信息

- a) 实际负荷、预测负荷等信息；
- b) 输变电设备可靠性指标，包括电压等级、统计百台年数、故障率、故障次数、故障停运时间、修复时间、计检率、计检平均时间等信息；
- c) 输电线路信息，包括线路段号、侧地名、侧开关号、并联号、侧省名、调度权、线路长度、导线型号、地线型号、安全电流、控制电流、导线

排列、正序电阻等；

d) 线损消耗、影响线路状态的环境信息等。

A.4.3 建设运维信息

a) 装机容量、发电量、供应量等信息；

b) 同比环比增减量等信息；

c) 电力各系统配置信息，包括配电自动化系统、生产管理系统、停电管理系统、高级量测体系、电能质量监控系统、用户能效管理系统等；

d) 电力各系统运行信息，包括电压、电流、频率、波形等；

e) 电力系统实时状态监控、电力系统巡检、电力调度等信息；

f) 可靠性统计分析信息，包括可用系数、强迫停运率、平均无故障可用小时、故障率、修复率等。

A.4.4 其他信息

a) 电力各系统资产、配套安防系统相关信息；

b) 未发布的电网/电厂规划图等；

c) 城市电网管线分布图文资料；

d) 电网地理坐标信息；

e) 能够有助于入侵攻击电力基础设施的其他信息。

A.5 通信

主管部门：工业和信息化部。

重要数据包括但不限于：

A.5.1 规划建设类数据

主要包括电信网和互联网网络及信息系统在规划及建设环节产生的重要数据，如规划设计及建设方案、灾难备份系统设计与建设方案、设备地理位置、网络拓扑结构、线路路由走向、设备资产采购清单等。

A.5.2 运行维护类数据

主要包括网络及信息系统运维过程中产生、收集的重要数据，如设备及软件配置信息、IP地址分配信息及内外网转换信息、网络流量流向信息、网络及系统运行状态信息、网络及系统运行维护日志、以及系统用户资料信息等。

A.5.3 安全保障类数据

- a) 网络与信息安全管理数据，如网络安全预警监测信息、系统及数据访问操作日志、安全审计记录、网络安全应急预案、违法有害信息监测处置相关数据、用户访问互联网日志数据、用户计费数据和上网记录等个人通信数据；
- b) 应急通信数据，如应急通信系统规划、建设、运行相关信息等；应急通信事件分级信息和应急预案，重大活动行动方案、保障预案信息、应急通信装备物资储备、保障队伍部署等。

A.5.4 无线电数据

- a) 国家重要行业如交通运输、渔业、海洋系统、航空、航天、军事、广播电视等行业使用的涉及国家主权、安全的无线电频率和台站信息；
- b) 卫星通信信息主要是指使用卫星进行通信所涉及的相关信息，主要包括卫星地面站基建、卫星地面站灾备、卫星通信用户等信息；
- c) 蜂窝移动通信基站位置、蜂窝移动通信基站基建、蜂窝移动通信基站灾

备、蜂窝移动通信基站收发能力等信息；

- d) 无线电监测信息主要指开展无线电监测工作所涉及的相关信息，主要包括无线电监测站地理位置、天线配置、设备能力等监测设施信息，以及监测信号样本、频段扫描数据、频率时间占用度等电磁环境信息；
- e) 上述信息中已纳入国际电信联盟（ITU）国际频率登记总表（Master International Frequency Register, MIFR）内的信息除外；国家无线电管理机构正在向或需向 ITU 进行申报的无线电网络数据除外。

A.5.5 统计分析类数据

主要包括：根据网络及信息系统运行、用户网络行为等过程中直接产生、收集的重要数据，以及统计分析得到的数据，如行业和企业运行情况、用户网络行为习惯分析信息、行业或业务发展预测信息等。

A.5.6 其他通信数据

- a) 关键基础设施网络威胁原数据；
- b) 通信内容、信令、记录等数据；
- c) 基础核心技术、核心设备主要性能参数、网络信息安全整体防护能力。

A.6 电子信息

主管部门：工业和信息化部。

重要数据包括但不限于：

- a) 产业运行数据，主要包括：尚未公开的规模以上电子信息产业企业数量、产值、销售收入、利润等基本情况，尚未公开的产业新在建项目数量、项目可行性报告、投资额、资金来源等投资情况，及尚未公开的电子信息产品进出口贸易情况；
- b) 产业发展数据，主要包括：尚未公开的产业发展规划、发展重点、近期国家级和部重点的研发支持项目等；

- c) 电子信息百强企业业务数据，主要包括：尚未公开的企业业务发展决策、投融资决策，及企业产值、销售收入、利润、研发投入、研发人员数量等内容；
- d) 电子信息产品基础硬件的型号、重要参数、源代码和目标、技术方案、实验数据、检测报告、重要工艺技术等全部技术资料；
- e) 国防军事领域、政务领域和公共服务领域等在关键领域或重要行业中各类电子信息设备的销售信息和使用信息，例如购买方名单、交易价格、交易数量、采购周期、采购产品型号、应用领域、产品去向、更换频率等；
- f) 在关键领域或重要行业中电子信息产品在使用过程中的运行、保养和维修信息，例如使用信号波段、频率等设备运行参数，设备故障频率、故障原因、解决方案、使用寿命等维修记录；
- g) 在关键领域或重要行业中电子信息产品在使用过程中采集、存储、管理和分析的涉及政府秘密、商业秘密和个人隐私的信息。包括地理地貌、气候环境、卫星轨道、军事部署等相关信息，企业、单位决定不宜公开的商业资料以及个人隐私包括个人身份信息、财产信息、健康信息等。

A.7 钢铁

主管部门：工业和信息化部。

重要数据包括但不限于：

A.7.1 钢铁产业的实力、潜力及竞争力信息

- a) 重点区域或企业的生产安排、炼钢配比、规模、产量、生产设备与技术水平、采购计划、物流配送、能耗等信息；
- b) 企业重点产品批量进入石油、化工等重点领域和新兴领域的信息；
- c) 大型客户采购钢铁的品种、频次、吨数等信息。

A.7.2 国防军用和国民经济建设发展所需钢材、优特钢产业等实力信息

涉及冶金、能源、交通、建筑、桥梁、机械、电子等国民经济建设发展所需先进钢铁材料及其制品的信息。

A.7.3 国家产业发展及外部环境掌控、应对相关信息

- a) 钢铁市场行情的预测和动态监测方面的信息；
- b) 钢铁行业未公开的政策文件、布局安排、军民配置分配、统计数字等相关信息。

A.8 有色金属

主管部门：工业和信息化部。

重要数据包括但不限于：

A.8.1 有色金属产业的实力、潜力及竞争力信息

- a) 重点企业的生产安排、规模、产量、生产设备与技术水平、采购计划、物流配送、能耗、销售去向、贸易谈判等信息；
- b) 大型客户采购有色金属的品种、频次、吨数等数据。

A.8.2 国防军工和国民经济建设发展所需有色金属信息

有色金属产品的名称、科研、勘察开采计划，生产能力、工艺技术路线，全部技术资料，企业名称、产地、产量、产能、储备、消费去向等信息及统计信息。

A.8.3 国家有色金属产业发展及外部环境掌控、应对信息

有色金属市场行情的预测和动态监测方面的信息。

A.9 装备制造

主管部门：工业和信息化部。

重要数据包括但不限于：

A.9.1 投资信息

生产安全保障类装备和高技术关键装备，如军事、航空航天装备等的投资信息；

A.9.2 重要装备出厂后工程活动信息

国民经济、国防施工等重要领域装备长时间或大范围生产活动相关信息。

A.10 化学工业

主管部门：工业和信息化部。

重要数据包括但不限于：

- a) 国家主要化工产品生产能力、储备情况等统计信息，重大化工进出口项目相关信息；
- b) 重要地区化工经济项目协议、项目、计划以及军用化学品出口相关信息等；
- c) 剧毒化学品、易爆危险化学品的道路运输、水路运输、航空运输等相关信息；
- d) 生产、储存危险化学品的单位，其作业场所设置通信、报警装置、警卫保护措施等相关信息；
- e) 机构出具的对化工企业的安全生产条件进行评价的报告；
- f) 新建、改建、扩建生产、储存危险化学品的建设项目，及新建、改建、扩建储存、装卸危险化学品的港口建设项目信息；
- g) 化工厂房平面图、化学品存储库房分布、库场面积、容量、年度用量、来源等资料；
- h) 企业生产、储存的剧毒化学品、易致爆危险化学品的数量、流向等相关信息。

A.11 国防军工

主管部门：国防科工局。

其重要数据包括但不限于：

- a) 采购元器件、软件、型号材料、工控设备测试仪器的名称、数量、来源、途径、代理商等信息；
- b) 军工科研生产单位内部名称、地理位置、建设计划、安防规划、保密等级、警卫保护、厂房图纸、库房容积、储备情况等信息。

A.12 其它工业

主管部门：工业和信息化部。

重要数据包括但不限于：

- a) 战争及临时宣布的紧急备战时期，全国及各大地区军用产品的运输、储备计划和执行情况；
- b) 处于世界先进水平，且对国民经济具有重要影响的工业研究开发项目、计划；
- c) 具有国际水平和重大经济效益的科研成果中的核心部分；
- d) 全国输油、输气管线及战备油库的坐标；
- e) 全国石油库存的分布、统计数字及有关资料；
- f) 涉及国防军工生产的发供用电规划、计划和统计资料；
- g) 工业科技发展重点任务中与安全相关的关键科技内容。

A.13 地理信息

主管部门：国土资源部（国家测绘地理信息局、国家海洋局）。

重要数据包括但不限于：

A.13.1 重要目标地理信息

- a) 标注国家或地区重要安全警卫目标、设施和关键基础设施信息的遥感影像；
- b) 国家或地区重要安全警卫目标、设施的带有位置精度信息的实景影像；
- c) 分辨率和位置精度优于遥感影像公开使用要求的影像；
- d) 大于 1:5 万（含）比例尺海图及其数字化成果；
- e) 大于 1:5 万（含）比例尺地形图及其数字化成果；
- f) 未经审核发布的重要地理信息，包括国界、国家海岸线长度；领土、领海、毗连区、专属经济区面积；国家海岸滩涂面积、岛礁数量和面积；国家版图的重要特征点，地势、地貌分区位置；国务院测绘地理信息行政主管部门商国务院其他军地有关部门确定的其他重要自然和人文地理实体的位置、高程、深度、面积、长度等地理信息；
- g) 地理信息分析数据，包括能源、金属、非金属等主要矿物的地理分布情况及开采储量、设计储量、远景储量等储量信息，尤其是与国家安全密切相关的矿产情况。

A.13.2 标识有下列内容的（对社会公众开放的除外）地理信息

- a) 专用铁路及站内火车线路、铁路编组站，专用公路；
- b) 未经国家有关部门批准公开发布的与地理相关的重大经济建设信息等；
- c) 未公开的机场（含民用、军民合用机场）和机关、单位的信息；
- d) 国家法律法规、部门规章禁止公开的其他内容。

A.13.3 标识有下列目标具体形状及属性的（用于公共服务的设施可以标注名称）地理信息

- a) 大型水利设施、电力设施、通信设施、石油和燃气设施、重要战略物资储备库、气象台站、降雨雷达站和水文观测站（网）等涉及国家经济命

脉，对人民生产、生活有重大影响的民用设施；

- b) 监狱、看守所、拘留所、强制隔离戒毒所等与公共安全相关的单位；
- c) 公开机场的内部结构及运输能力属性；
- d) 渡口的内部结构及属性；
- e) 国家法律法规、部门规章禁止公开的其他内容相关形状和属性。

A.13.4 标识有下列内容属性的地理信息

- a) 高压电线、通信线、管道的属性；
- b) 国家法律法规、部门规章禁止公开的其他内容相关属性；
- c) 水库库容、输电线路电压等精确数据，桥梁、渡口、隧道的结构形式和河底性质，未经公开的港湾、港口、沿海潮浸地带的详细数据；
- d) 重要桥梁的限高、限宽、净空、载重量和坡度属性，重要隧道的高度和宽度属性，公路的路面铺设材料属性；
- e) 江河的通航能力、水深、流速、底质属性，水库的库容属性，拦水坝的构筑材料 and 高度属性，水源的性质属性，沼泽的水深和泥深属性。

A.13.5 特殊测绘信息

- a) 国家重力控制点成果、加密重力测量成果，航空重力测量成果、海洋重力测量成果以及小于 5' × 5' 分辨率的平均重力异常和似大地水准面成果等各类计算衍生产品；
- b) 军事禁区的磁力测量数据和我国海域磁力测量数据及其衍生品；
- c) 境内优于 25 米网络的数字高程模型、数字地表模型数据。

A.13.6 公开地图数据

按照2015年12月颁布的《地图管理条例》（国务院第664号令），互联网地图服务单位应当将存放地图数据的服务器设在中华人民共和国境内，并将互联网服务单位收集、使用、提供的用户位置相关信息存放在中华人民共和国境内。

A.13.7 北斗卫星导航信息

- a) 北斗卫星导航系统的灾备和服务能力等数据；
- b) 北斗卫星导航系统生成和服务的高精度位置数据；
- c) 北斗卫星导航用户名录、属性、装备识别号（ID）及短信息服务内容等数据。

A.14 民用核设施

民用核设施主管部门：国防科工局和能源局。

民用核设施安全监管部门：环境保护部（国家核安全局）。

重要数据包括但不限于：

A.14.1 民用核设施安全监管信息

- a) 管理部门对于建造、装料、运行、退役等活动审批中涉及到的关键设计资料、运行参数等；
- b) 未公布的全国辐射环境监测原始信息。

A.14.2 民用核设施运行信息

- c) 核燃料生产、加工、贮存和后处理设施、放射性废物处理设施中涉及到的关键技术电子资料，如关键设备设计图纸、制造工艺等信息；
- d) 核动力厂（核电站、核热电厂、核供气供热厂等）的产能，核燃料年度采购处置数量及处置信息，业务信息系统中重要业务统计信息，日常运维管理信息（如重大核电厂运行异常大事件、停堆换料或检修等）；
- e) 其他反应堆（研究堆、实验堆、临界装置等）的使用信息、核燃料年度

采购处置数量及处置信息，业务信息系统中重要业务数据统计信息，日常运维管理的信息（如停堆换料或检修等）；

- f) 核燃料生产、加工、贮存和后处理设施的年度处理能力、年度处理记录、原料采购、产品销售等相关统计信息、业务系统中的业务信息；
- g) 放射性废物处理和处置设施的年度处理能力、年度处理记录、原料采购、产品销售等相关统计信息，业务系统中的业务信息；
- h) 核动力厂、反应堆、核燃料加工处理等机构为满足监管要求建立的通信网络相关信息，以及上报的停堆换料或检修等信息；
- i) 对核设施工况参数进行监控而使用的核设施数据采集系统形成的信息。

A.14.3 核设施产业发展信息

- a) 我国核原料矿产分布、储量等信息；
- b) 国家发展规划中关于民用核设施的发展规划信息；
- c) 民用核设施科研中的试验或测试数据。

注：依据我国有关法律法规以及参加的国际公约，以上信息中已公开的除外。

A.15 交通运输

主管部门：国家交通战备办公室、交通运输部、国家铁路局、中国铁路总公司。

重要数据包括但不限于：

A.15.1 含有下列内容，或通过汇聚分析能印证、推论出下列信息的数据

交通运输相关的信息通信系统部署信息、无线电频谱（有公开标准、依照国家公约、国内法律法规规定的除外）。

A.15.2 以下各个具体领域的属性数据单点可被测定或公开，但集中批量的数据泄露可能会危害国家安全、军事行动或反恐安全

- a) 关键铁路线路图、车站布局、轨道分布、仓储数据等资料;
- b) 涉外交通运输工程施工建设过程中的地理、水文、技术资料、统一口径等数据。

A.16 邮政快递

主管部门：邮政局。

重要数据包括但不限于：

- a) 与客户签署保密协议或协议中保密条款约定的不能共享使用的信息;
- b) 邮政服务过程中的名址、联系电话、数量金额等信息;
- c) 邮政企业、快递企业的运单数据，如收寄物品的名称、规格、数量、重量、收寄时间、寄件人和收件人名址、联系电话，以及寄递过程中的实时位置、位置轨迹、车辆、人员等信息;
- d) 邮政企业、快递企业收集的上下游用户相关名址数据，涵盖企业、个人客户的客户名单、客户姓名或单位名称、网址或地址、联系电话等信息;
- e) 收寄邮件、快件时登记的上下游用户实名身份证件信息;
- f) 通过大数据分析得到涉及特定个体用户数据，如姓名、住址、身份证号、联系方式等;
- g) 有助于黑客实施攻击邮政行业的数据，与基础设施、网络、系统等方面相关的材料，包括但不限于系统架构设计说明文档、基础设施的布局和建设文档、网络架构设计文档、IP 地址分配文档、主要软硬件类型、维护人员信息、维护用户帐号和密码等。

A.17 水利

主管部门：水利部。

重要数据包括但不限于：

- a) 水情信息拍报电码;
- b) 未经国际防汛抗旱总指挥部批准公布, 可能造成重大灾情的水、旱情信息及预报成果;
- c) 大型及防洪重点水库运行管理资料;
- d) 大型水利水电、水利枢纽、跨流域调水等重要工程项目的规划、项目建议书、可行性研究、初步设计、施工、竣工验收报告、图纸等资料及系统水文分析成果;
- e) 省、流域机构水利发展的中、长期计划;
- f) 七大江河流域及重要地区水的中、长期供求计划;
- g) 涉及对外技术合作和水利工程合作项目的未公开出版的科技成果、资料;
- h) 反映大、中型水库移民生活困的资料及水库移民专项资金的年度计划;
- i) 水文、水质年鉴、水情年报、水情资料汇编和水文公报 (含水质通报、水资源公报等) ;
- j) 传输网络中的实时水文与工程运行信息;
- k) 省际水事纠纷及水事违法案件、水土保持重要案件的正式资料;
- l) 水利行政主管部门发布前的水利统计年鉴、资料汇编;
- m) 全国江河湖泊水文观测数据, 统计整编和分析的水文数据等。

A.18 人口健康

主管部门: 卫生计生委。

重要数据包括但不限于:

- a) 在药品和避孕药具不良反应报告和监测过程中获取的个人隐私、患者和报告者信息;
- b) 突发公共卫生事件与传染病疫情监测过程中获取的传染病病人及其家

属、密切接触者的个人隐私和相关疾病、流行病学信息等；

- c) 医疗机构和健康管理服务机构保管的个人电子病历、健康档案等各类诊疗、健康数据信息；
- d) 人体器官移植医疗服务中人体器官捐献者、接受者和人体器官移植手术申请人的个人信息；
- e) 人类辅助生殖技术服务中精子、卵子捐献者和使用者以及人类辅助生殖技术服务申请人的个人信息；
- f) 计划生育服务过程中涉及的个人隐私；
- g) 个人和家族的遗传信息；
- h) 生命登记信息。

A.19 金融

主管部门：人民银行。

重要数据包括但不限于：

A.19.1 金融机构安全信息

- a) 新产品研发方案以及研发过程中产生的相关记录和数据；
- b) 技术方案、电路设计、计算机软件、源代码和目标码、数据库、研究开发记录、技术报告、检测报告、实验数据、实验结果、图纸等技术文档；
- c) 产品销售信息、市场调研信息、市场营销计划、财务资料、业务分析研究成果等经营资料；
- d) 客户名单、客户身份资料、客户交易记录等客户资料；
- e) 内部安全保卫制度、操作细节、银行业务使用的密押、编制方案及专用暗记、代号、指令密码；
- f) 其他一经泄露会对各金融机构安全和利益造成损害的信息。

A.19.2 自然人、法人和其他组织金融信息

- a) 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；
- b) 账户信息。包括银行结算账户和支付账户的信息。主要要素为：账号名称、账号、账户类型、账户开立时间、开户机构、绑定账户信息、账户验证信息（含客户身份外部渠道验证信息）、账户映射的敏感介质信息（如银行卡有效期、验证码、磁道信息等）、账户余额、账户交易情况等；
- c) 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；
- d) 自然人、法人和其他组织金融交易信息。包括银行业金融机构、证券业金融机构、保险业金融机构、交易及结算类金融机构、非银行支付机构等各类金融机构办理业务时获取的自然人、法人和其他组织交易信息；
- e) 身份信息。包括个人身份信息和单位身份信息。其中个人身份信息包括个人姓名、性别、国籍、民族、身份证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。单位身份信息包括单位名称、统一社会信用代码、类型、法定代表人（负责人）姓名及身份证件号码、经营场所、联系方式等；
- f) 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；
- g) 在与自然人、法人和其他组织建立业务关系过程中获取、保存的其他自然人、法人和组织信息。

A.19.3 中央银行、金融监管部门、外汇管理部门工作中产生的不涉及国家秘密的工作秘密。

A.20 征信

主管部门：人民银行。

重要数据包括以下内容：

- a) 法院生效判决、裁定、调解和执行信息；
- b) 欠缴税收信息；
- c) 欠缴劳动及社会保障保险信息；
- d) 行政事业性收费、政府性基金欠费信息；
- e) 公共事业欠费信息；
- f) 信用卡还款情况、贷款偿还情况；
- g) 企业和个人与金融机构以外的市场主体发生融资授信关系产生的信息，包括商业信用信息、民间借贷信息和水电费欠费信息等。

A.21 食品药品

监管部门：食品药品监管总局。

重要数据包括但不限于：

- a) 涉及国家战略安全的药品在药品审批过程中提交的药品实验数据，例如在动物模型上进行的药理、毒理、稳定性、药代动力学等试验数据，在人体中进行的临床试验数据，以及与药品的生产流程、生产设施有关的试验数据；
- b) 第二类、第三类医疗器械临床试验数据/报告；
- c) 食品安全溯源标识信息，包括产品名称、执行标准。药品溯源标识信息，包括追溯编码、产品名称、执行标准、配料、生产工艺、标签标识；
- d) 食品药品安全重大（紧急）信息。包括事件发生时间、地点、当前状况、危害程度、先期处置、发展趋势、事件进展、后续应对措施、调查详情、原因分析；

- e) 大宗粮食加工品（含大米、小麦粉等）抽检监测信息。

A.22 统计

主管部门：统计局。

重要数据包括但不限于：

A.22.1 人口

- a) 人口普查的资料（包括姓名、性别、年龄、民族、户口登记状况、受教育程度、行业、迁移流动、社会保障、婚姻、生育、死亡、住房情况等）；
- b) 人口普查中获得的能够识别或者推断单个普查对象身份的资料。

A.22.2 经济

- a) 全国国内生产总值（GDP）初步核算数；
- b) 全国规模以上工业总产值及增加值、主要财务指标；
- c) 全国单位国内生产总值（GDP）能耗及其降低率；
- d) 各省、自治区、直辖市单位地区生产总值能耗及其降低率、固定资产投资额、社会消费品零售总额等；
- e) 各省、自治区、直辖市粮食、棉花总产量；
- f) 全国粮食、棉花总产量；
- g) 各省、自治区、直辖市工业生产者出厂价格指数及主要分类指数、购进价格指数及主要分类指数；
- h) 全国工业生产者出厂价格指数及主要分类指数、购进价格指数及主要分类指数；
- i) 全国及各省、自治区、直辖市主要工业产品产量；
- j) 全国及各省、自治区、直辖市房地产开发投资额、销售额、销售面积、建筑业总产值、增加值；

- k) 全国及各省、自治区、直辖市农林牧渔业总产值、农业生产资料价格指数、商品零售价格指数、固定资产投资价格指数及主要分类指数；
- l) 全国及各省、自治区、直辖市煤炭等能源消费总量及其增长率；
- m) 全国及各省、自治区、直辖市农村居民人均现金收入、人均纯收入、人均可支配收入、人均生活消费支出等；
- n) 全国及各省、自治区、直辖市城镇居民人均可支配收入、人均消费支出；
- o) 全国及各省、自治区、直辖市居民人均可支配收入、人均消费支出；
- p) 其它与国家安全和经济利益密切相关的重要统计数据及统计分析材料；
- q) 其它与全国或较大区域（一省或数省）社会秩序和经济秩序密切相关的重要统计数据及统计分析材料。

A.23 气象

主管部门：气象局。

重要数据包括但不限于：

- a) 我国气象卫星原始资料；
- b) 为国家保密任务或者军事部门保密任务专门设置的气象台站的观测气象数据；
- c) 为作战、军事演习和训练、国防科研实验等任务专门提供的气象数据；
- d) 为高科技或者特殊科学试验研究获得的空间大气监测数据；
- e) 为国家或者军事部门保密任务专门统计整编和分析的重要气象数据；
- f) 通过非国际交换途径获得的各种国外气象数据；
- g) 我国未参加国际交换的地面气象、高空气象、气象辐射、大气成分、天气雷达、气象卫星数据及相应元数据，我国未公布的数值预报产品；
- h) 专项、专业气象数据，包括海洋气象、空间天气、历史气候代用数据、

气象灾害数据、航空气象数据、交通气象数据、科学试验考察数据及相应元数据。

i) 环境保护

主管部门：环境保护部。

重要数据包括但不限于：

- a) 未公布的长时间系列各行业（领域）环境污染的重要污染源监测数据和危害程度以及重大污染事故情况；
- b) 未公布的长时间系列大、中城市供水水源的水质资料及主要江湖、河段水质监测资料及监测系统信息；
- c) 未公布的长时间系列城市空气质量监测资料及相应监测系统信息；
- d) 未公布的全国土壤污染监测或调查数据。

A.24 广播电视

主管部门：国家新闻出版广电总局。

重要数据包括但不限于：

- a) 广播电视安全播出运维、应急保障、调度指挥等信息材料；
- b) 广播电视监测监管系统产生的相关数据；
- c) 广播电视台产生业务相关系统网络拓扑、安全运维类信息以及不宜公开的报道方案、媒体资源类文件等信息资料；
- d) 广播电视无线和卫星传输覆盖网系统配置、播出参数及台站位置信息等重要数据；
- e) 全国直播卫星用户信息。

A.25 海洋环境

主管部门：国家海洋局。

重要数据包括但不限于：

- a) 海底地形、海洋水文、海洋气象、水声环境和海洋物理场等观测和统计整编数据；
- b) 领海内的温盐、水声、底质、潮汐、海流实测数据和相关成果；
- c) 未公布的海洋生态环境监测数据。

A.26 电子商务

主管部门：商务部。

重要数据包括但不限于：

- a) 个人在电子商务平台的注册信息，包括姓名、性别、年龄、住址、婚姻、学历、职业、收入、账户、联系方式等；
- b) 企业在电子商务平台的注册信息，包括企业名称、住址、证照编号、经营范围、账户、联系方式等；
- c) 电子商务交易记录以及相关的个人消费习惯及偏好和企业经营数据等；
- d) 电子商务交易记录以及相关的个人消费习惯及偏好和企业经营数据等；
- e) 电子商务交易各方的信用记录和信用评价信息；
- f) 电子商务平台企业的经营数据；
- g) 电子商务相关服务信息，包括支付和融资信息、物流信息等；
- h) 对上述数据进行加工形成的涉及国计民生的全国或区域经济运行、行业发展情况的统计分析报告等。

A.27 其它

重要数据涉及范围众多，本指南仅列出部分行业（领域）重要数据部分范围或内容，其它重要数据可依据下列规则判断、识别：

- a) 企事业单位掌握的能够反映国家某行业（领域）整体情况的数据，且该

行业（领域）与国家安全、社会公共利益密切相关；

- b) 反映能够导致某行业（领域）发生系统性风险的企事业单位总体运行状况的数据，以及一旦完整性、保密性、可用性遭破坏即能显著影响这些单位稳定运行的各种数据；
- c) 反映不可更改或长时间保持稳定的自然、经济、社会特征的数据，如地理位置、地貌特征、矿区位置、民族基因特性等；
- d) 在各类数据集合并过程中能起到识别、关联、连接作用的数据，如地理位置、身份证号、手机号、法人代码；
- e) 各行业主管部门在重大规划、计划、决策中所依赖或从本行业（领域）的企事业单位调取的部分数据；
- f) 行政机关、执法机关在履职、执法过程中收集、产生的可能影响国家安全、社会公共利益或存在大量个人隐私的信息；
- g) 单条或少量信息不会影响国家安全或社会公共利益，但覆盖较大范围或较长时间，一旦出境会带来危害或影响的某些信息集合；
- h) 单条或少量信息不会影响国家安全或社会公共利益，但涉及某些重要区域或时期，一旦出境会带来危害或影响的某些信息集合；
- i) 关键信息基础设施的系统设计、安全防护计划和策略方案，及其单元或设备选型、配置、软件等属性信息和脆弱性信息等；以及包括密码技术在内的其它与国家安全相关的单元、装置、设备、系统或计划、设计能力和缺陷信息；
- j) 与意识形态、舆情等有关的文化安全相关信息；

行业（领域）主管部门可根据行业（领域）发展、评估实践，判断是否存在其它重要数据并及时更新指南。

(规范性附录)

个人信息和重要数据出境安全风险评估方法

A.28 评估个人信息出境对个人权益产生的影响等级

A.28.1 个人信息类型和敏感程度

个人信息因其敏感程度、出境后的处理目的等不同，对个人权益可能造成的影响有所不同，出境后的个人敏感信息如出现泄露、毁损、篡改或滥用等情形时，对个人合法权益造成的影响通常高于非敏感类个人信息。

A.28.2 个人信息数量

个人信息数量越大，或涉及特定群体的个人信息数量越多，当安全事件发生时，对个人权益造成的影响会随之增加，甚至影响国家安全、经济发展和社会公共利益。

A.28.3 个人信息范围

个人信息范围超出与出境目的相关联的最小集时，将会对个人权益造成额外影响。

A.28.4 个人信息技术处理情况

网络运营者可在满足业务需求的前提下，对拟出境的个人信息采取去标识化等数据脱敏处理措施，并应采取技术和管理措施单独存储去标识化后个人信息，与可用于恢复标识的信息分别存储。经技术处理后的个人信息能有效降低数据出境安全风险。

个人信息经技术处理无法识别特定个人且不能复原的，不属于个人信息出境情形。

A.28.5 个人权益影响等级判定

评估个人权益受影响等级时，首先，需要对其关键要素个人信息敏感程度进行分析，初步判定影响等级；其次，根据个人信息数量、个人信息范围、技术处

理情况等要素对影响等级进行进一步修正，使其更加准确。除以上修正要素外，评估时还可以根据实际情形加入相应的修正要素，如某个特定年龄、职业的群体个人信息，是否对个人权益形成额外影响等。

为了方便分析和计算，个人权益受影响等级的判定方法可参考下表：

表 B.1 个人权益受影响等级判定表

关键要素 敏感程度	影响等级	修正要素		
		数量	范围	技术处理情况
个人敏感信息为主	3	一年内涉及出境的个人信息累计大于主管部门规定的大量个人信息时，影响等级可增加 1。	如果出境个人信息超出满足出境目的最小集，则影响等级可增加 1。	使用技术措施对涉及出境的个人信息进行去标识化处理，能有效防止识别出个人的，影响等级可减去 1。
包含少量个人敏感信息（如个人敏感信息占个人信息中的比例小于 50%）	2			
仅为个人信息，不包含个人敏感信息	1			

A.29 评估重要数据出境对国家安全、社会公共利益产生的影响等级

A.29.1 重要数据类型

重要数据出境后如出现泄露、毁损、篡改或滥用等情形，将损害国家安全、经济发展和社会公共利益。

A.29.2 重要数据数量

重要数据数量越大，其所蕴含的社会、经济价值越高，发生泄漏、毁损、篡改或滥用时，对国家安全、经济发展和社会公共利益危害程度越大。

A.29.3 重要数据范围

重要数据超出与出境目的相关联的最小集时，将会对国家安全、经济发展和社会公共利益造成额外的影响。

A.29.4 重要数据技术处理情况

重要数据在出境前，网络运营者应对其采取数据脱敏处理等措施，并对数据脱敏处理的效果进行验证，使其不能被还原为原始数据。脱敏处理后的重要数据能适度降低出境带来的安全风险。

A.29.5 国家和社会公共利益受影响等级判定

评估国家和社会公共利益受影响等级时，首先，需要明确关键要素重要数据内容，以及其影响等级；其次，根据重要数据数量、重要数据范围和技术处理等要素对影响等级进行进一步修正，使其更加准确。除以上修正要素外，评估时还可以根据实际的情形加入相应的修正要素，如重要数据的生成时间、数据源特点，是否可与其他信息汇聚对国家安全、经济发展和社会公共利益形成额外影响等。

为了方便分析和计算，国家安全、经济发展和社会公共利益受影响等级的判定方法可参考下表：

表 B.2 国家安全、经济发展和社会公共利益受影响等级判定表

关键要素	影响等级	修正要素		
重要数据类别		数量	范围	技术处理情况
识别出的重要数据	4	出境的重要数据属于主管部门规定的大量数据时，影响等级可增加 1。	如果出境重要数据超出满足出境目的的最小集，则影响等级可增加 1。	使用技术措施对重要数据进行数据脱敏处理，且处理后的数据不能被还原为原始数据，影响等级可减去 1。

A.30 评估安全事件的可能性等级

A.30.1 评估发送方的安全保障能力等级

根据数据发送方技术保障要求和管理保障要求的实施情况，将保障能力等级划分为高、中、低三个等级，对保障能力等级的赋值可参考下表：

表 B.3 发送方安全保障能力赋值

类别	保障能力等级	具体描述
管理制度保	高	发送方具备完备且有效的管理制度、人员管理、合同约定、

障能力		审计、应急处置、申诉管理、安全事件告知和报告等机制，能够有效保护数据安全，能有效防止数据泄露、毁损、篡改、滥用等事件发生，或事件发生后造成的影响可以忽略。。
	中	发送方具备基本的管理制度、人员管理、合同约定、审计、应急处置、申诉管理、安全事件告知和报告等机制，管理方式有待提升，但存在发生数据泄露、毁损、篡改、滥用事件的可能性，且会造成一定范围和程度的影响。
	低	发送方缺乏有效的管理制度、人员管理、合同约定、审计、应急处置、申诉管理、安全事件告知和报告等机制，管理手段缺失严重，数据被泄露、毁损、篡改、滥用等的可能性很高或事件已发生，且会造成严重影响。
技术手段保障能力	高	发送方在数据出境环节采用了较先进和完善的数据安全技术，完全落实了 5.2.4.2 中的安全要求，并建立数据出境日志留存机制，能够有效保护数据出境过程安全，如果被威胁利用，造成的损害可以忽略。
	中	发送方在数据出境环节采用了相应的数据安全技术，基本落实 5.2.4.2 中的安全要求，或日志留存机制不够完整，如果被威胁利用，将造成一般损害。
	低	发送方在数据出境环节未落实 5.2.4.2 中的安全要求，或采用的安全技术存在重大缺陷，或未建立日志留存机制，无法有效保护数据安全，如果被威胁利用，将造成完全损害。

A.30.2 评估接收方的安全保障能力等级

根据数据接收方对技术保障要求和管理保障要求的实施情况，将保障能力等级划分为高、中、低三个等级，对保障能力等级的赋值可参考下表：

表 B.4 接收方安全保障能力赋值

类别	保障能力等级	具体描述
主体资格	高	数据接收方资质完备齐全，股东构成或主管部门关系清晰，接收的数据与数据接收方业务完全契合。
	中	数据接收方资质相对齐全，股东构成或主管部门相对清晰，接收的数据与数据接收方业务基本契合。
	低	数据接收方缺乏合法资质或资质不真实，或接收的数据与数据接收方业务存在较大差异，或发生过数据安全相关事件且未得到有效处置。
管理制度保障能力	高	数据接收方的组织机构健全、制度流程完备、人员能力良好、审计和应急处置机制有效，能有效防止数据泄露、毁损、篡改、滥用等事件发生，或事件发生后造成的影响可

		以忽略。
		数据接收方提供权威、有效的数据安全合规证明以保证其达到了 5.2.5.2 中管理保障要求。
	中	数据接收方的组织机构基本健全、制度流程较规范、人员能力一般，审计和应急处置机制基本有效，但存在发生数据泄露、毁损、篡改、滥用事件的可能性，且会造成一定范围和程度的影响。
	低	数据接收方的组织机构不健全、制度流程缺失、人员能力较差、缺乏审计和应急处置机制，数据被泄露、毁损、篡改、滥用等的可能性很高或事件已发生，且会造成严重影响。
技术手段保障能力	高	数据接收方具备较先进和完善的数据安全技术能力，落实了 5.2.5.3 中的安全要求，能够有效保护数据安全，如果被威胁利用，造成的损害可以忽略。
		数据接收方提供权威、有效的数据安全合规证明以保证其达到了 5.2.5.3 中的技术保障要求。
	中	数据接收方具备一定的数据安全技术能力，基本落实 5.2.5.3 中的安全要求，如果被威胁利用，将造成一般损害。
	低	数据接收方未落实 5.2.5.3 中的技术保障要求，或采取的安全技术存在重大缺陷，无法有效保护数据安全，如果被威胁利用，将造成完全损害。

A.30.3 评估接收方所在国家或区域的政治法律环境

A.30.3.1 评估个人信息接收方所在国家或地区的政治法律环境

个人信息接收方所在国家或区域的政治法律环境评估是指对该国家或地区现行的个人信息保护法律法规情况，该国家或地区加入的区域或全球性的个人信息保护方面的组织以及所做出的具有约束力的承诺，该国家或地区落实个人信息保护的机制进行评估，依据各方面水平的高低，将保障能力等级划分为高、中、低三个等级，对保障能力等级的赋值可参考下表：

表 B.5 个人信息接收方所在国家或地区的政治法律环境赋值

类别	保障能力等级	具体描述
数据接收方所在国家或地区的政治法律环境	高	个人信息保护方面的法律法规较为成熟且已形成体系化，广泛使用了标准作为法律法规的补充，保障了个人信息主体的各项权利，有专门个人信息保护机构，同时具备完备、有效、多层次的救济渠道。

	中	个人信息保护方面的法律法规标准基本齐备，保障了个人信息主体的部分权利，有个人信息保护相关部门，具备相应的行政、司法救济渠道。
	低	个人信息保护方面的法律法规标准欠缺或不完备，个人仅能通过司法救济渠道维护权利。

A.30.3.2 评估重要数据接收方所在国家或地区的政治法律环境

重要数据接收方所在国家或区域的政治法律环境评估是指对评估重要数据接收方所在国家或地区的数据安全方面现行的法律法规情况，该国家或地区落实数据安全的机构，该国家或地区的行政机关、司法机构等执法部门调取数据的规范法律程序，该国家或地区与其他国家或地区之间有关数据流通、共享等方面的双边或多边协定进行评估。依据各方面水平的高低，将保障能力等级划分为高、中、低三个等级，对保障能力等级的赋值可参考下表：

表 B.6 重要数据接收方所在国家或地区的政治法律环境赋值

类别	保障能力等级	具体描述
数据接收方所在国家或地区的政治法律环境	高	网络安全或数据安全方面的法律法规完备，主管或监管部门具备较强的监督和执法能力，数据安全事件发生后具备有效的追责和监督机制。执法机构和司法机构调取数据的权力受法律的约束，且做到了公开透明，且近期不存在相关的负面案例。
	中	网络安全或数据安全方面的法律法规标准基本完备，主管或监管框架初步成型，对数据安全事件主要依靠行政监督。执法机构和司法机构调取数据需要遵循一定的程序。
	低	网络安全或数据安全方面的法律法规标准欠缺或不完备，主管或监管部门不清晰或缺乏相应能力，缺乏在数据安全事件发生后有效追责的机制。执法机构和司法机构调取数据的权力基本不受约束，或近期存在相关的负面案例。

A.30.4 安全事件可能性等级判定

安全事件的可能性与发送方安全保障能力、接收方安全保障能力以及接收方所在国家或地区的法律环境有关，根据上述要素的分析与赋值，为了方便分析和计算，安全事件的可能性等级判定方法可参考下表：

表 B.7 安全事件可能性等级判定表

可能性等级	主要判定条件	修正条件
3	发送方管理保障能力、技术保障能力、接收方背景情况、管理保障能力、技术保障能力任何一项赋值为“低”的。	政治法律环境赋值为“高”的，可能性等级可减 1。
2	发送方管理保障能力、技术保障能力、接收方背景情况、管理保障能力、技术保障能力赋值有“中”和“高”的。	政治法律环境赋值为“低”的，可能性等级可加 1。
1	发送方管理保障能力、技术保障能力、接收方背景情况、管理保障能力、技术保障能力所有项赋值均为“高”的。	

如果在某些数据出境活动的评估过程中不涉及接收方背景情况、管理保障能力、技术保障能力、接收方所在国家或地区等要素，表B.7中的判定条件可将相关要素视为不适用项，不纳入判定条件的考虑范围，仅对需评估的要素按表B.7中进行判定，得出相应的安全事件可能性等级。

A.31 安全风险综合评估

安全风险综合评估是根据国家安全、经济发展、社会公共利益和个人权益受影响程度以及安全事件可能性两方面进行综合评价，分析数据出境活动整体的安全风险级别，安全风险级别划分为极高、高、中、低四个等级，对风险级别的判定可参考下表。

表 B.8 安全风险级别判定参考表

影响程度等级	安全事件可能性等级		
	1	2	3
≥5	高	极高	极高
4	中	高	高
3	低	中	高
2	低	中	中
1	低	低	中

参 考 文 献

- [1] ISO/IEC 27000-2013 信息安全管理体系统概述和术语
- [2] ISO/IEC 27001-2013 信息安全管理体系统 要求
- [3] ISO/IEC 27002-2013 信息安全管理实用规则
- [4] ISO/IEC 27003-2013 信息安全管理体系统实施指南
- [5] GB/T 22239-2008 信息安全技术 信息体系统安全等级保护基本要求
- [6] GB/T 25070-2010 信息安全技术信息体系统等级保护安全设计技术要求
- [7] NIST Special Publication 800-53 联邦信息体系统和组织的安全和隐私控制
- [8] GB/T 20984-2007 信息安全技术 信息安全风险评估规范

(十七) 车联网（智能网联汽车）网络安全标准体系建设指南（征求意见稿）

前 言

车联网（智能网联汽车）作为汽车、电子、信息通信等深度融合的新兴产业生态，已成为推动制造业高质量发展，加速经济转型，构建新发展格局的重要动力，呈现蓬勃发展的良好态势。与此同时，伴随车联网全方位跨域互联、融合开放和多样化业务应用等新技术新业务的加速推进，车联网（智能网联汽车）网络安全需求更为多样复杂，“人-车-路-网-云”各环节安全风险更为突出，亟需加快建立健全车联网（智能网联汽车）网络安全保障体系，为车联网安全健康发展提供支撑。

为落实《中华人民共和国网络安全法》《新能源产业汽车发展规划（2021-2035年）》《车联网（智能网联汽车）产业发展行动计划》等相关法律和政策要求，在已初步构建国家车联网产业标准体系基础上，面向车联网终端与设施安全、网联通信安全、数据安全、应用服务安全、安全保障与支撑等方面需求，工业和信息化部组织编制了《车联网（智能网联汽车）网络安全标准体系建设指南》（以下简称《标准体系建设指南》），加强标准化工作顶层设计，指导标准制定有序开展，推动构建系统、科学、规范的车联网（智能网联汽车）网络安全标准体系，支撑和保障车联网产业高质量发展。

一、总体要求

（一）指导思想

全面贯彻习近平新时代中国特色社会主义思想 and 党的十九大精神，贯彻落实党中央、国务院关于促进车联网产业发展的部署要求，推动制造强国和网络强国建设，着力构建车联网（智能网联汽车）网络安全标准体系，指导标准统筹规划，系统推进网络安全标准研制，注重与智能网联汽车、信息通信、电子产品和服务等相关标准体系的协调和衔接，促进强化标准落地实施，为保障车联网产业安全可持续发展提供标准支撑。

（二）基本原则

统筹规划，全面布局。结合车联网产业发展及网络安全现状特点，加强统筹协调，整体规划覆盖汽车、通信等领域的车联网（智能网联汽车）网络安全标准体系，合理布局网络安全标准建设重点，满足车联网（智能网联汽车）网络安全管理和行业保障需求。

共性先立，急用先行。立足车联网（智能网联汽车）从测试示范走向先导应用和规模化部署的发展实际，着眼车联网（智能网联汽车）重要环节网络安全需求，合理安排标准制修订工作进度，加快基础、共性和关键技术标准等重要和急需标准项目的研究制定。

加强协作，协同发展。聚集整车及关键设备、云服务平台、汽车电子零部件、信息通信、网络安全等相关产业链主体，加强标准研制过程中的交流合作，凝聚共识，加速标准创新研制。以信息服务、车路协同、自动驾驶等安全典型应用场景为牵引，强化重点标准的宣标贯标与落地实施。

（三）建设目标

到 2023 年底，初步构建起车联网（智能网联汽车）网络安全标准体系，重点研究基础共性、终端与设施安全、网联通信安全、数据安全、应用服务安全、安全保障与支撑等重点行业标准和国家标准，完成 50 项以上重点急需安全标准的制修订工作。

到 2025 年，形成较为完备的车联网（智能网联汽车）网络安全标准体系，完成 100 项以上重点标准，提升标准对细分领域的覆盖程度，加强标准服务能力，提高标准应用水平，支撑车联网产业安全发展。

二、建设思路

（一）建设思路

在《国家车联网产业标准体系建设指南》整体框架基础上，结合车联网（智能网联汽车）网络安全工作实际需求，统筹规划、突出重点、急用先行、循序渐进，进一步明确安全标准建设的对象和重点内容，建立统一协调的标准体系框架，指导车联网（智能网联汽车）网络安全标准化建设。

（二）技术架构图

车联网（智能网联汽车）网络安全标准体系从车联网基本构成要素出发，针对车载联网设备、基础设施、网络通信、数据信息、平台应用、车联网服务等关键环节，提出覆盖终端与设施安全、网联通信安全、数据安全、应用服务安全、安全保障与支撑等方面的技术架构，见图 1。



图 1 车联网（智能网联汽车）网络安全技术架构图

三、建设内容

（一）标准体系框架

车联网（智能网联汽车）网络安全标准体系框架包括总体与基础共性、终端与设施安全、网联通信安全、数据安全、应用服务安全、安全保障与支撑等六个部分，主要反映标准体系各部分的组成关系，见图 2。



图 2 车联网（智能网联汽车）网络安全标准体系框架图

总体与基础共性标准包括术语和定义、总体架构、密码应用等三类；终端与设施安全标准包括车载设备安全、车端安全、路侧通信设备安全和测试场设施安全等四类；网联通信安全包括通信安全、身份认证等两类；数据安全包括通用要求、分类分级、出境安全、个人信息保护、应用数据安全等五类；应用服务安全包括平台安全、应用程序安全、服务安全等三类；安全保障与支撑类标准包括风

险评估、安全监测与应急管理、安全能力评估等三类。

（二）重点标准化领域及方向

车联网（智能网联汽车）网络安全标准体系框架主要包括以下内容：

1. 总体与基础共性标准

总体与基础共性标准主要规范车联网（智能网联汽车）网络安全的总体性、通用性和指导性标准，包括术语和定义、总体架构、密码应用等三类标准。

术语和定义标准用于统一车联网（智能网联汽车）网络安全主要概念，为车联网安全相关标准中的术语和定义提供依据支撑。

总体架构标准制定车联网（智能网联汽车）网络安全总体架构要求，明确和界定防护对象、防护措施、防护策略，指导企业体系化开展网络安全防护工作。

密码应用标准主要规范车联网（智能网联汽车）密码应用通用要求，明确数字证书格式、数字证书应用、设备密码应用等方面要求。

2. 终端与设施安全标准

终端与设施安全标准主要规范车联网终端和基础设施等相关安全要求，包括车载设备安全、车端安全、路侧通信设备安全和测试场设施安全等四类标准。

车载设备安全标准主要针对智能网联汽车的关键智能设备和组件提出安全防护与检测要求，主要包括汽车信息感知设备、电子控制单元、车载计算平台，以及车载智能交互设备、车载智能网关、车载 OBU 设备、车联网智能通信终端等安全标准。

车端安全标准在车联网（智能网联汽车）总体安全架构要求基础上，以保障车辆安全、稳定、可靠运行为核心，主要针对车辆及车载系统通信、软硬件安全等，从系统和整车层面提出安全防护与检测要求。

路侧通信设备安全标准主要针对联网路侧设备安全问题，以保障路侧设备通信安全、稳定、可靠运行为核心，提出网络安全防护与检测要求。

测试场设施安全标准主要对汽车测试场地设施提出安全防护与检测要求。

3. 网联通信安全标准

网联通信安全标准主要规范 V2X 通信网络安全、身份认证等相关安全要求，包括通信安全、身份认证等两类标准。

通信安全标准重点针对车内总线通信、LTE-V2X 通信、5G LTE 通信，以及应用于车联网的蜂窝移动通信（4G/5G）、卫星通信、无线射频识别、车内无线局域网、BLE、Zigbee 等安全技术，提出安全防护与检测要求。

身份认证标准主要规范车联网（智能网联汽车）数字身份认证相关的证书应用接口、证书管理系统、安全认证技术及测试方法、关键部件轻量级认证等技术要求。

4. 数据安全标准

数据安全标准主要规范智能网联汽车、车联网平台、车载应用服务等数据安全和个人信息保护要求，包括通用要求、分类分级、出境安全、个人信息保护、应用数据安全等五类标准。

通用要求主要用于规范车联网（智能网联汽车）可采集和处理的数据类型、范围、质量、颗粒度等通用要求，包括数据最小化采集、数据安全存储、数据加密传输、数据安全共享等标准。

分类分级标准主要用于指导车联网（智能网联汽车）数据分类分级保护，制定数据分类分级的维度、方法、示例等，明确重要数据类型和安全保护要求。

数据出境安全标准主要用于规范车联网（智能网联汽车）行业依法依规落实数据出境安全要求，包括数据出境安全评估要点、评估方法等标准。

个人信息保护标准主要用于规范车联网（智能网联汽车）用户个人信息保护机制及相关技术要求，明确用户敏感数据和个人信息保护的场景、规则、技术方法，包括匿名化、去标识化、数据脱敏、异常行为识别等标准。

应用数据安全标准主要用于规范车联网（智能网联汽车）相关应用所开展的

数据采集和处理使用等活动，包括车联网平台、网约车、车载应用程序等数据安全标准。

5.应用服务安全标准

应用服务安全标准主要规范车联网（智能网联汽车）应用服务平台和应用程序的安全要求，以及典型业务应用服务场景下的安全要求，包括平台安全、应用程序安全和服务安全等三类标准。

平台安全标准主要规范车联网云平台、业务应用平台和服务、信息服务平台、远程升级（OTA）服务平台、边缘计算平台、电动汽车远程信息服务与管理等安全防护及检测要求。

应用程序安全标准主要规范车联网（智能网联汽车）应用程序等安全防护与检测要求。

服务安全标准主要规范车联网（智能网联汽车）典型业务服务场景下的安全要求，包括 OTA、汽车远程诊断、高级辅助驾驶、高级自动驾驶、车路协同等服务安全要求。

6.安全保障与支撑标准

安全保障与支撑标准主要规范车联网（智能网联汽车）网络安全管理与支撑相关的安全要求，包括风险评估、安全监测与应急管理、安全能力评估等三类标准。

风险评估标准主要用于明确车联网（智能网联汽车）网络安全风险分类与安全等级划分，规范安全风险评估流程和方法，提出车联网（智能网联汽车）服务平台、整车网络安全风险评估规范等相关要求。

安全监测与应急管理标准用于规范车联网（智能网联汽车）网络安全监测、数据安全监测、应急管理、网络安全漏洞分类分级、安全事件追踪溯源等相关要求，以及安全管理平台接口、车联网业务 HI 接口、车联网卡实名登记数据采集接口等相关规范。

安全能力评估标准主要规范车联网（智能网联汽车）相关企业安全防护措施

部署及安全服务实施，提出网络安全成熟度模型、数据安全成熟度模型、安全能力成熟度评价准则、评估实施方法、机构能力认定、道路车辆信息安全工程等相关要求。

四、组织实施

（一）推进标准研制。在国家制造强国建设领导小组车联网产业发展专项委员会指导下，按照《标准体系建设指南》明确的标准研制路径，组织整车企业、车联网平台企业、汽车电子零部件供应商、基础电信企业、互联网企业、网络安全企业、科研院所、高校等相关单位，有序推进标准研制工作，注重车联网（智能网联汽车）网络安全标准化工作与网络安全防护最新研究成果、行业最佳实践的有机结合。

（二）实施动态更新。实施动态更新机制，跟踪车联网（智能网联汽车）技术和应用的发展趋势，结合网络安全相关法律法规的最新要求，通过持续强化行业间的协调、协作，适时修订《标准体系建设指南》，形成适应车联网技术和产业发展的网络安全标准体系。

（三）加强宣贯实施。充分发挥地方主管部门、标准化组织、行业协会和专业机构的作用，组织开展标准的宣标贯标和技术研讨活动，通过培训、咨询、论坛等方式推进标准的宣贯实施。组织开展贯标试点优秀企业和案例的遴选，形成最佳实践，促进标准应用推广。

（四）加强交流合作。加强与国际标准化组织的交流与合作，积极参与联合国世界车辆法规协调论坛（UN/WP29）、国际标准化组织（ISO）、国际电信联盟（ITU）、国际电工技术委员会（IEC）、国际自动化工程师学会（SAE）、第三代合作伙伴计划（3GPP）、欧洲电信标准化协会（ETSI）、欧洲标准化委员会（CEN）等国际组织活动及国际标准研制。促进国内标准与国际接轨，推动国内标准向国际标准转化。

附件

车联网（智能网联汽车）网络安全相关标准项目明细表

总序号	分序号	标准名称	标准号/计划号	状态
100总体与基础共性				
101术语和定义				
1.	1.	车联网网络安全通用术语和定义		待制定
102总体架构				
2.	1.	车联网网络安全总体架构		待制定
103密码应用				
3.	1.	车联网数字证书格式通用	GB/T 37376-2019	已发布
4.	2.	智能网联汽车数字证书应用技术要求		待制定
5.	3.	车联网密码应用通用要求		待制定
6.	4.	智能网联汽车商用密码应用技术要求		待制定
7.	5.	车联网通信设备密码应用技术要求		待制定
200终端与设施安全				
201车载设备安全				
8.	1.	汽车网关信息安全技术要求及试验方法	20191070-T-339	制定中
9.	2.	车载信息交互系统信息安全技术要求及试验方法	20191069-T-339	制定中
10.	3.	汽车电子控制单元网络安全防护技术要求		待制定
11.	4.	汽车信息感知设备网络安全技术要求		待制定
12.	5.	车载计算平台网络安全技术要求		待制定
13.	6.	车联网网络关键设备安全通用技术及检测要求		待制定
14.	7.	车联网网络关键设备安全技术及检测要求 车载智能交互设备		待制定
15.	8.	车联网网络关键设备安全技术及检测要求 车载智能网关设备		待制定
16.	9.	车联网网络关键设备安全技术及检测要求 车载OBU设备		待制定
17.	10.	车联网网络关键设备安全技术及检测要求 车联网智能通信终端（VBOX）		待制定
202车载安全				
18.	1.	汽车电子系统网络安全指南	GB/T 38628-2020	已发布
19.	2.	汽车信息安全通用技术要求	20191065-T-339	制定中
20.	3.	电动汽车充电系统信息安全技术要求	20192313-T-339	制定中

21.	4.	汽车软件升级通用技术要求	CQCCPZ0013-2021	制定中
22.	5.	汽车整车信息安全技术要求及试验方法	CQCCPZQ0014-2021	制定中
23.	6.	汽车网络安全域及防护层级化定义		待制定
24.	7.	汽车网络安全通用测试与评价方法		待制定
25.	8.	车载总线系统网络安全技术要求		待制定
26.	9.	车载以太网网络安全技术要求		待制定
27.	10.	汽车诊断接口网络安全技术要求		待制定
28.	11.	车用安全芯片网络安全技术要求		待制定
29.	12.	车载操作系统及应用软件安全防护要求		待制定
30.	13.	汽车电子外部接口网络安全技术要求		待制定
203路侧通信设备安全				
31.	1.	车联网网络关键设备安全技术及检测要求 路侧无线通信设备		待制定
204测试场设施安全				
32.	1.	智能网联汽车自动驾驶能力测试场地设施网络安全技术要求		待制定
300网联通信安全				
301通信安全				
33.	1.	车联网无线通信安全技术指南	YD/T 3750-2020	已发布
34.	2.	基于公众电信网的联网汽车信息安全技术要求	YD/T 3737-2020	已发布
35.	3.	基于LTE的车联网通信安全技术要求	YD/T 3594-2019	已发布
36.	4.	基于5G V2X的车联网无线通信安全技术要求		待制定
37.	5.	车联网网络安全接入技术要求		待制定
38.	6.	面向车联网的卫星通信安全技术要求		待制定
39.	7.	车联网汽车安全类通信专用短程通信接口规范		待制定
302身份认证				
40.	1.	基于LTE的车联网无线通信技术 安全证书技术要求	2019-0021T-YD	制定中
41.	2.	基于LTE的车联网无线通信技术 安全证书管理系统技术要求	2020-CCSA-36	制定中
42.	3.	基于LTE的车联网无线通信技术 安全认证测试方法	2019-0022T-YD	制定中
43.	4.	电子驾驶证安全技术要求		待制定
44.	5.	车联网数字证书应用接口规范		待制定
45.	6.	基于PKI的车联网应用服务安全认证体系框架		待制定
46.	7.	车联网关键部件轻量级认证通用技术要求		待制定

47.	8.	智能网联汽车数字身份及认证通用规范		待制定
400 数据安全				
401通用要求				
48.	1.	智能网联汽车数据通用要求		待制定
49.	2.	智能网联汽车数据安全共享模型与规范		待制定
50.	3.	智能网联汽车数据安全共享参考架构		待制定
51.	4.	信息安全技术 网联汽车 采集数据的安全要求		待制定
52.	5.	车联网数据安全保护能力参考框架		待制定
402分类分级				
53.	1.	车联网信息服务 数据安全技术要求	YD/T 3751-2020	已发布
403数据出境安全				
54.	1.	车联网数据跨境流动安全管理要求		待制定
55.	2.	车联网数据跨境流动安全评估规范		待制定
404个人信息保护				
56.	1.	车联网信息服务 用户个人信息保护要求	YD/T 3746-2020	已发布
57.	2.	基于移动互联网的汽车用户数据应用与保护技术要求	2018-0182T-YD	制定中
58.	3.	基于移动互联网的汽车用户数据应用与保护评估方法	2018-0183T-YD	制定中
59.	4.	车联网用户个人信息合规检测要求		待制定
405应用数据安全				
60.	1.	信息安全技术 网络预约汽车服务数据安全指南	20205164-T-469	制定中
61.	2.	网络预约出租汽车服务平台数据安全防护要求	2017-0938T-YD	制定中
62.	3.	车联网信息服务 数据安全保护能力评估规范	2020-1317T-YD	制定中
63.	4.	车联网应用服务 数据脱敏实施方法		待制定
500 应用服务安全				
501 平台安全				
64.	1.	车联网信息服务平台安全防护技术要求	YD/T 3752-2020	已发布
65.	2.	车联网信息服务平台安全防护检测要求	2021-0192T-YD	制定中
66.	3.	电动汽车远程服务与管理系统信息安全技术要求及试验方法	20191066-T-339	制定中
67.	4.	车联网云平台安全防护技术要求及检测要求		待制定
68.	5.	车联网服务平台通信安全保障技术要求		待制定
69.	6.	车联网服务平台安全接入技术要求		待制定
70.	7.	车联网远程监控平台网络安全技术要求		待制定
502 应用程序安全				

71.	1.	车联网APP安全技术及测试要求		待制定
503 服务安全				
72.	1.	车联网OTA升级网络安全技术及测试方法		待制定
73.	2.	车联网部件和系统外部信息交互通用安全技术要求		待制定
74.	3.	车联网应用服务平台与车载终端交互安全技术要求		待制定
75.	4.	车联网汽车远程诊断网络安全技术要求		待制定
76.	5.	车联网高级辅助驾驶应用网络安全技术要求		待制定
77.	6.	车联网车路协同服务网络安全技术规范		待制定
78.	7.	车联网高级自动驾驶应用网络安全技术要求		待制定
600 安全保障与支撑				
601 风险评估				
79.	1.	车联网网络安全风险评估规范		待制定
80.	2.	车联网网络安全风险分类指南		待制定
602 安全监测与应急管理				
81.	1.	车联网网络安全管理平台接口规范		待制定
82.	2.	车联网企业侧安全管理平台通用技术要求		待制定
83.	3.	车联网网络安全应急管理要求		待制定
84.	4.	汽车网络安全应急响应管理指南		待制定
85.	5.	车联网系统漏洞分类分级指南		待制定
86.	6.	车联网业务 HI接口总体技术要求		待制定
87.	7.	车联网业务 HI接口技术实施要求		待制定
88.	8.	车联网业务 HI接口测试方法		待制定
89.	9.	车联网卡实名登记数据采集接口规范-电信企业		待制定
90.	10.	车联网卡实名登记数据采集接口规范-车辆生产企业		待制定
603 安全能力评估				
91.	1.	车联网网络安全能力成熟度模型		待制定
92.	2.	车联网网络安全能力成熟度评价准则		待制定
93.	3.	车联网网络安全能力成熟度评估实施方法		待制定
94.	4.	车联网网络安全服务机构能力认定准则		待制定
95.	5.	车联网供应链安全风险管理体系指南		待制定
96.	6.	道路车辆 网络安全工程		待制定
97.	7.	道路车辆 网络安全工程审核指南		待制定

(十八) 网络数据安全标准体系建设指南（征求意见稿）

前言

随着信息技术和人类生产生活交汇融合，全球数据呈现爆发增长、海量聚集的特点，大数据产业正值活跃发展期，技术演进和应用创新并行加速推进，数据资源已成为国家基础战略性资源和社会生产的创新要素。当前，我国电信和互联网行业高速发展，汇聚大量网络数据，在释放数字经济发展潜力、促进数字经济加快成长的同时，面临严峻的安全风险。这要求我们深刻认识网络数据安全的重要性和紧迫性，坚持安全与发展并重，积极应对复杂严峻的安全风险与挑战，加速构建网络数据安全保障体系。

“安全发展、标准先行”，标准化工作是保障网络数据安全的重要基础。为落实《中华人民共和国网络安全法》《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》《电信和互联网用户个人信息保护规定》等法律法规要求，指导电信和互联网行业网络数据安全标准化工作，工业和信息化部组织制定了《网络数据安全标准体系建设指南》（以下简称《建设指南》）。《建设指南》充分发挥标准的顶层设计和基础引领作用，为保障电信和互联网行业网络数据安全、促进网络数据合理有序流动、助力数字经济高质量发展提供有力支撑。

一、建设思路及目标

（一）总体思路

以习近平新时代中国特色社会主义思想为指导，全面贯彻党的十九大和十九届二中、三中、四中全会精神，落实《中华人民共和国网络安全法》《全国人民代表大会常务委员会关于加强网络信息保护的決定》《电信和互联网用户个人信息保护规定》等法律法规要求，充分发挥标准在保障网络数据安全、推动行业健康有序发展中的支撑和引领作用，有效建立电信和互联网行业网络数据安全标准体系。加强标准的统筹规划，做好与国家标准、相关领域行业标准的衔接工作，鼓励创新技术成果向标准转化，强化标准的实施与应用，加强标准的国际交流与合作，提升标准对网络数据安全保护的整体支撑作用，为数字经济高质量发展保驾护航。

（二）基本原则

统筹规划，全面布局。结合电信和互联网行业技术、产业发展现状及特点，发挥政府主管部门在顶层设计、组织协调和政策制定等方面的重要作用，制定政府引导和市场驱动相结合的标准体系建设方案，建立适合电信和互联网行业整体情况的网络数据安全标准体系。

基础先立，急用先行。从网络数据安全管理工作重点和难点出发，确定网络数据安全标准体系建设的重点领域，加快基础共性、关键技术、安全管理类标准的研究制定。在此基础上，综合考虑相关重要领域的网络数据安全现状及面临的风险和挑战，加快推进急需标准项目的研究制定。

多方参与，协同合作。在标准制定过程中聚集电信运营企业、互联网企业、设备提供商、安全企业、科研院所、高校等产业界、学术界多方力量，充分凝聚共识，研究制定网络数据安全相关标准，完善标准研制、应用的全生命周期管理。统筹运用行业资源，充分发挥企业在技术创新、产品开发、示范引领等标准研究与应用方面的主体作用，组织协调相关单位积极参与国际标准的制定、交流与合作。

（三）建设目标

到2021年，初步建立网络数据安全标准体系，有效落实网络数据安全管理工作，基本满足行业网络数据安全保护需要，推进标准在重点企业、重点领域中的应用，研制网络数据安全行业标准20项以上。

到2023年，健全完善网络数据安全标准体系，标准技术水平、应用水平和国际化水平显著提高，有力促进行业网络数据安全保护能力提升，研制网络数据安全行业标准50项以上。

二、建设内容

（一）网络数据安全标准体系框架

网络数据安全标准体系包括基础共性、关键技术、安全管理、重点领域四大类标准。基础共性标准包括术语定义、数据安全框架、数据分类分级，相关标准为各类标准提供基础性支撑。关键技术标准从数据采集、传输、存储、处理、交换、销毁等数据全生命周期维度对数据安全关键技术进行规范。安全管理标准从网络数据安全保护的管理视角出发，指导行业有效落实法律法规关于网络数据安全工作的要求，包括数据安全规范、数据安全评估、监测预警与处置、应急响应与灾难备份、安全能力认证等。重点领域标准结合相关领域的实际情况和具体要求，指导行业有效开展重点领域网络数据安全保护工作。网络数据安全标准体系框架如图1所示。

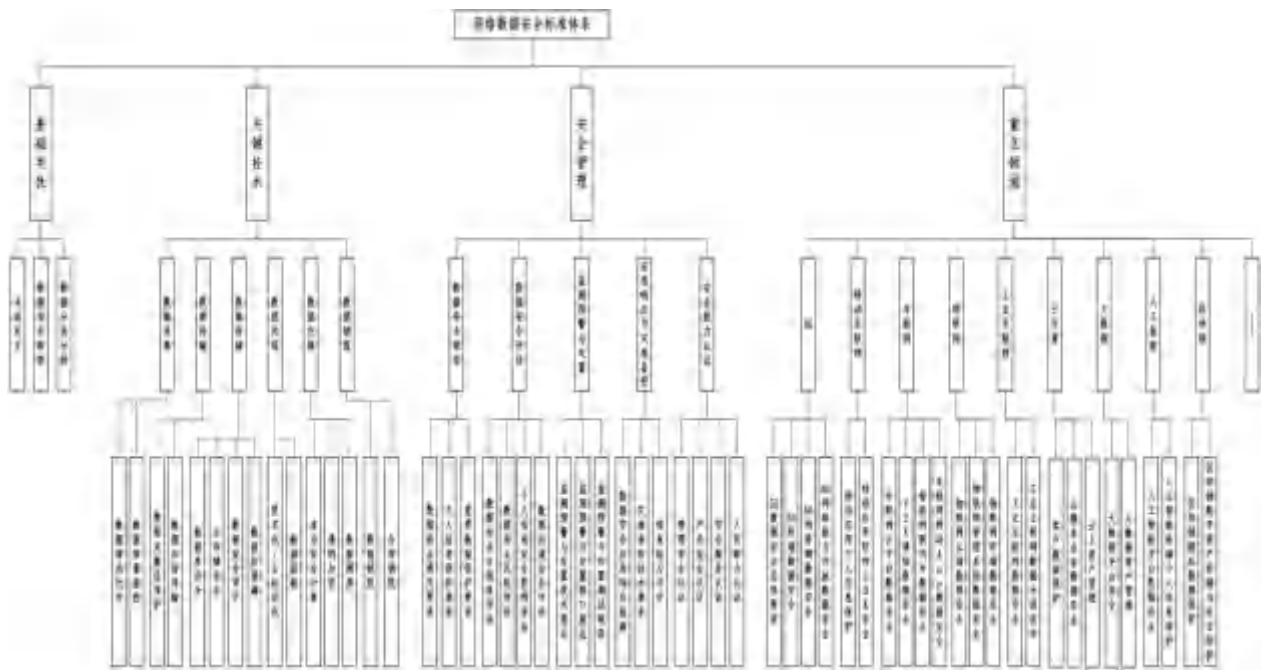


图1 网络数据安全标准体系框架

(二) 重点标准化领域及方向

1.基础共性标准

基础共性标准是网络数据安全保护的基础性、通用性、指导性标准，包括术语定义、数据安全框架、数据分类分级等标准。基础共性标准子体系如图2所示。

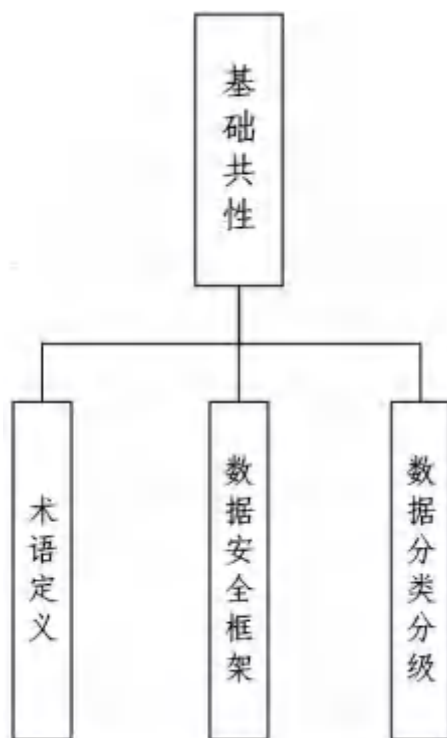


图2 基础共性标准子体系

1.1 术语定义

术语定义用于规范网络数据安全相关概念，为其它部分标准的制定提供支撑，包括技术、规范、应用领域的相关术语、概念定义、相近概念之间的关系等。

1.2 数据安全框架

数据安全框架标准包括网络数据安全体系框架以及各部分参考框架，以明确和界定网络数据安全的角色、职责、边界、各部分的层级关系和内在联系。

1.3 数据分类分级

数据分类分级标准用于指导对网络数据分类分级，给出数据分类分级的基本原则、维度、方法、示例等，为数据安全分类、分级保护提供依据，为数据安全

规范、数据安全评估等方面的标准制定提供支撑。

2. 关键技术标准

关键技术标准从采集、传输、存储、处理、交换、销毁等全生命周期环节出发，对网络数据安全的关键技术进行规范。关键技术标准子体系如图3所示。

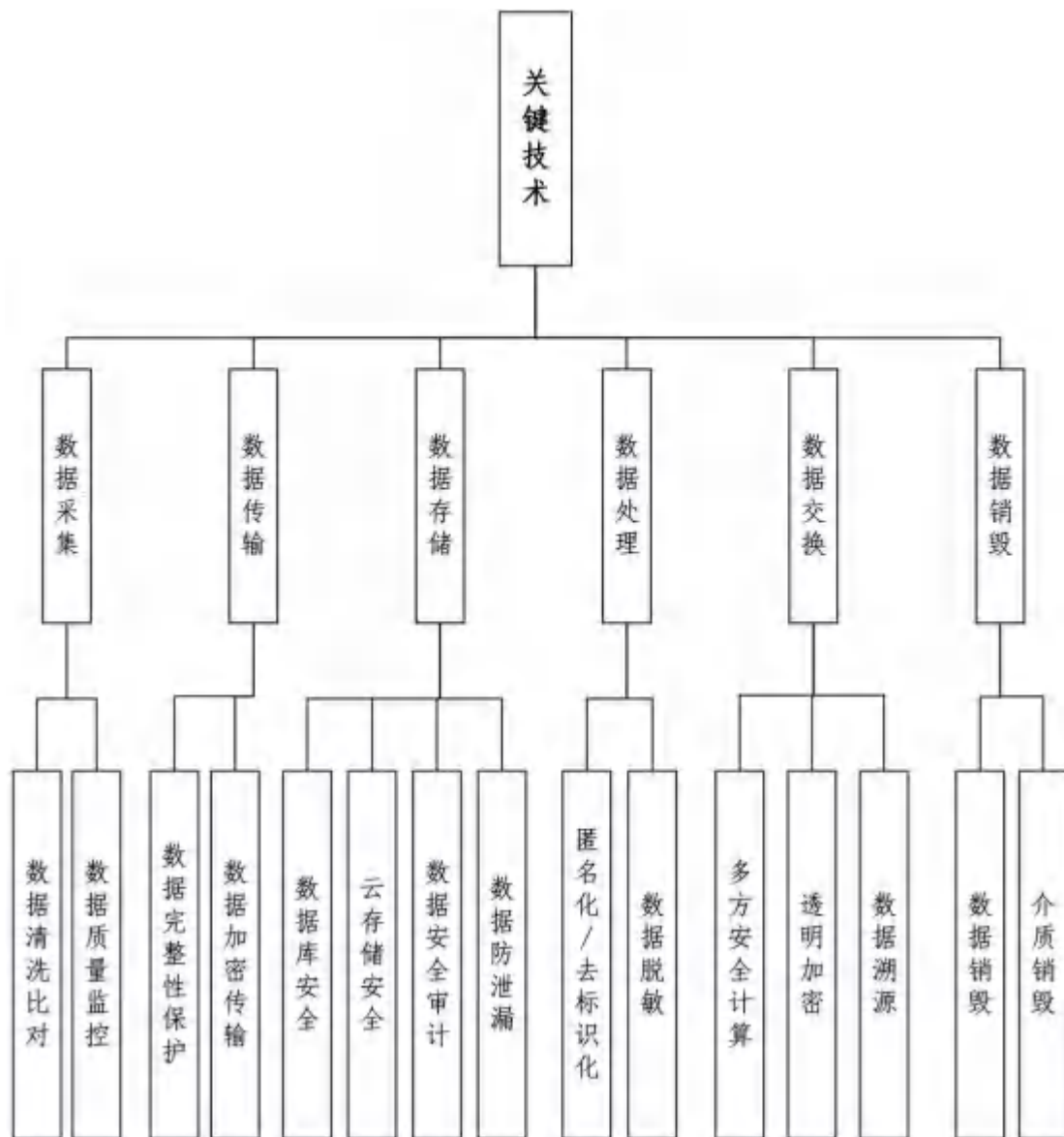


图3 关键技术标准子体系

2.1 数据采集

数据采集标准用于规范数据采集格式、数据标签、数据审查校验等方面相关技术要求，有效提升数据质量，主要包括数据清洗比对、数据质量监控等标准。

2.2 数据传输

数据传输标准用于规范数据传输过程中可以标准化的功能架构、安全协议及其他安全相关技术要求，主要包括数据完整性保护、数据加密传输等标准。

2.3 数据存储

数据存储标准用于规范存储平台安全机制、数据安全存储方法、安全审计、安全防护技术等相关技术要求，主要包括数据库安全、云存储安全、数据安全审计、数据防泄漏等标准。

2.4 数据处理

数据处理标准用于规范敏感数据、个人信息的保护机制及相关技术要求，明确敏感数据保护的场景、规则、技术方法，主要包括匿名化/去标识化、数据脱敏等标准。

2.5 数据交换

数据交换标准用于规范数据安全交换模型、角色权责定义、安全管控技术框架，并明确数据溯源模型、过程和方法，支撑数据安全共享、审计和监管，主要包括多方安全计算、透明加密、数据溯源等标准。

2.6 数据销毁

数据销毁标准用于规范数据销毁和介质销毁的安全机制和技术要求，确保存储数据永久删除、不可恢复，主要包括数据销毁、介质销毁等标准。

3.安全管理标准

安全管理标准从网络数据安全框架的管理视角出发，指导行业落实法律法规以及政府主管部门的管理要求，包括数据安全规范、数据安全评估、监测预警与处置、应急响应与灾难备份、安全能力认证等。安全管理标准子体系如图4所示。

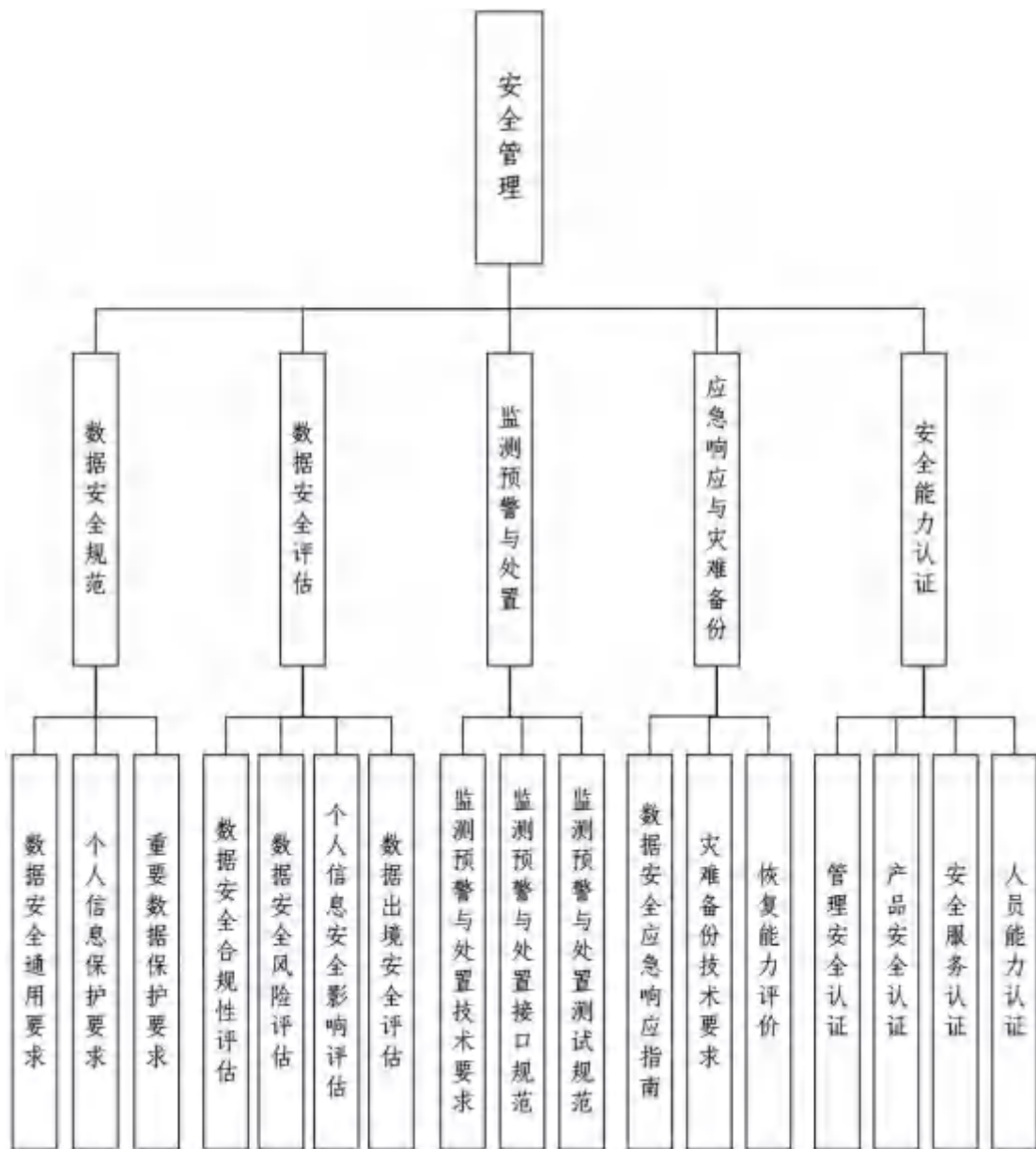


图4 安全管理标准子体系

3.1 数据安全规范

数据安全规范标准用于落实细化相关法律法规对网络数据安全保护的要求，对行业开展数据安全管理工作提供指导和规范，主要包括数据安全通用要求、个人信息保护要求、重要数据保护要求等标准。

3.2 数据安全评估

数据安全评估标准用于指导行业落实网络数据安全评估的要求，明确评估的基本概念、要素关系、分析原理、评估方法、实施流程、实施要点和工作形式等要素，指导行业规范开展网络数据安全评估工作，主要包括数据安全合规性评估、

数据安全风险评估、个人信息安全影响评估、数据出境安全评估等标准。

3.3 监测预警与处置

监测预警与处置标准从政府主管部门监管需求的视角出发，明确数据安全监测预警与处置系统及其技术要求，结合数据的敏感度、量级、流向以及账号权限等进行综合分析，实时动态追踪数据安全风险，主要包括监测预警与处置方面的技术要求、接口规范、测试规范等标准。

3.4 应急响应与灾难备份

应急响应与灾难备份标准用于规范数据安全事件的应急响应管理、处置措施，规范灾难备份及恢复工作的目标和原则、技术要求以及实施方法，主要包括数据安全应急响应指南、灾难备份技术要求、恢复能力评价等标准。

3.5 安全能力认证

安全能力认证标准用于规范组织及人员数据安全保障能力、产品与服务数据安全保护水平、数据安全服务能力等相关认证要求，用于指导网络运营者与安全服务机构提升自身的安全能力、服务能力，主要包括管理安全认证、产品安全认证、安全服务认证、人员能力认证等标准。

4. 重点领域标准

在基础共性标准、关键技术标准、安全管理标准的基础上，结合新一代信息技术发展情况，重点在5G、移动互联网、车联网、物联网、工业互联网、云计算、大数据、人工智能、区块链等重点领域进行布局，并结合行业发展情况，逐步覆盖其他重要领域。结合重点领域自身发展情况和网络数据安全保护需求，制定相关网络数据安全标准。重点领域安全标准子体系如图5所示。

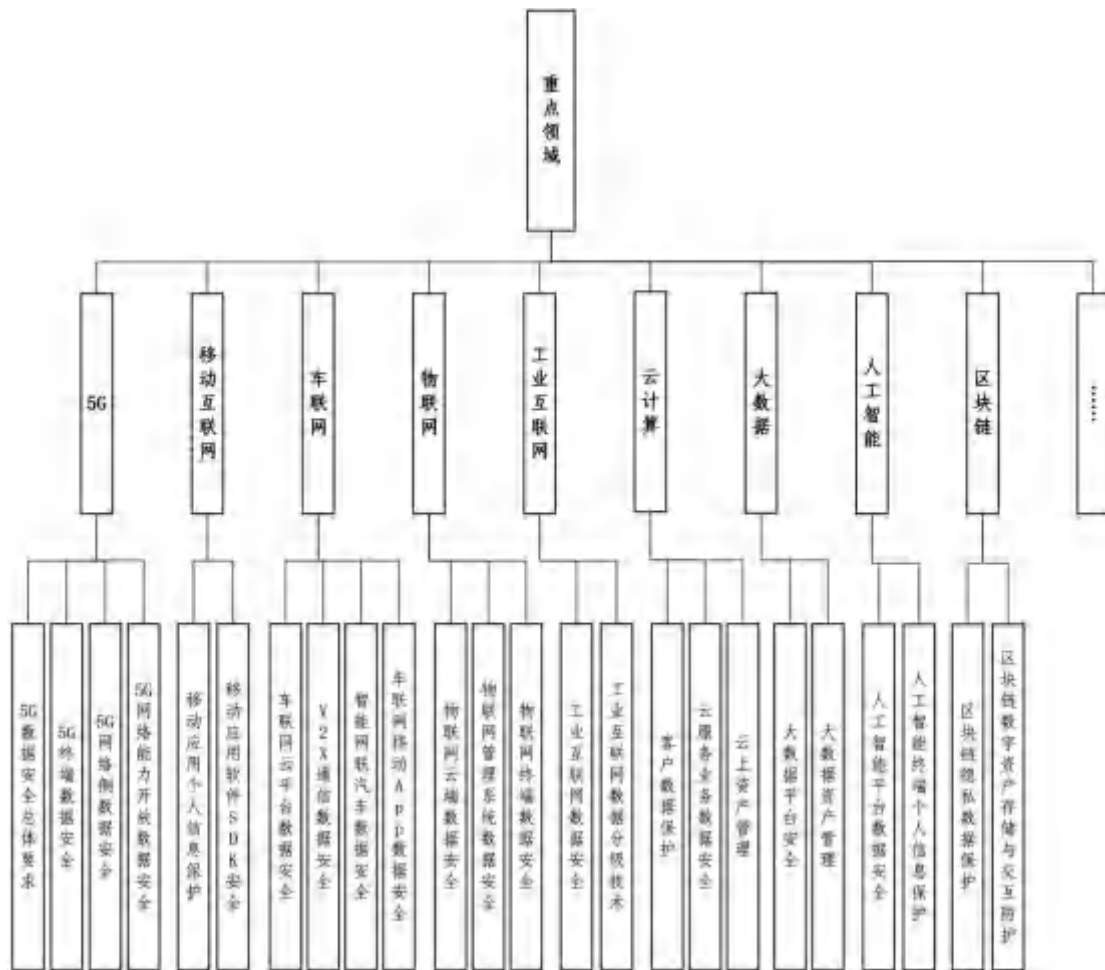


图5 重点领域标准子体系

4.1 5G

5G 安全机制在满足通用安全要求基础上，为不同业务场景提供差异化安全服务，适应多种网络接入方式及新型网络架构，保护用户个人隐私，并支持提供开放的安全能力。5G领域的网络数据安全标准主要包括5G数据安全总体要求、5G终端数据安全、5G网络侧数据安全、5G网络能力开放数据安全等。

4.2 移动互联网

传统的移动互联网安全主要包括终端安全、网络安全和应用安全等方面。随着开放生态体系下移动操作系统的普遍应用和数据的大规模流动，移动互联网的数据安全风险进一步凸显。移动互联网领域的网络数据安全标准主要包括移动应用个人信息保护、移动应用软件SDK安全等。

4.3 车联网

车联网安全覆盖车内、车与车、车与路、车与人、车与服务平台的全方位连接和数据交互过程，数据安全和隐私保护贯穿于车联网的各个环节。车联网领域的网络数据安全标准主要包括车联网云平台数据安全、V2X通信数据安全、智能网联汽车数据安全、车联网移动App数据安全等。

4.4 物联网

物联网安全涵盖物联网的感知层、传输层、应用层，涉及服务端安全、终端安全和通信网络安全等方面，数据安全贯穿于其中的各个环节。物联网领域的网络数据安全标准主要包括物联网云端数据安全保护、物联网管理系统数据安全保护、物联网终端数据安全保护等。

4.5 工业互联网

工业互联网安全重点关注控制系统、设备、网络、数据、平台、应用程序安全 and 安全管理等。工业互联网领域的网络数据安全标准主要包括工业互联网数据安全保护、工业互联网数据分级技术等。

4.6 云计算

云计算安全以云主机安全为核心，涵盖网络安全、数据安全、应用安全、安全管理、业务安全等方面。云计算领域的网络数据安全标准主要包括客户数据保护、云服务业务数据安全、云上资产管理等。

4.7 大数据

大数据安全覆盖数据全生命周期管理各环节，涵盖对大数据平台运行安全功能保障及以数据为对象进行资产管理等。大数据领域的网络数据安全标准主要包括大数据平台安全、大数据资产管理等。

4.8 人工智能

人工智能安全覆盖个人信息安全、算法安全、数据安全、网络安全等。人工智能领域的网络数据安全标准主要包括人工智能平台数据安全、人工智能终端个人信息保护等。

4.9 区块链

区块链安全包括应用服务的安全性、系统设计的安全性（包含智能合约、共识机制）、基础组件的安全性（包含网络通信、数据安全、密码技术）三个维度。区块链领域的网络数据安全标准主要包括区块链隐私数据保护、区块链数字资产存储与交互保护等。

五、组织实施

一是实施动态更新。实施动态更新完善机制，随着经济社会数字化转型持续推进、数据安全认知与实践水平的提高，结合数据安全相关法律法规的最新要求，适时滚动修订《建设指南》。

二是推进标准研制。组织中国通信标准化协会及相关电信运营企业、互联网企业、设备提供商、安全企业、科研院所、高校等单位，按照《标准指南》明确的标准研制路径，有序推进行业标准研制工作，注重网络数据安全标准化工作与网络数据安全保护最新研究成果、行业最佳实践的有机结合。

三是加强宣贯实施。充分发挥标准化组织、行业协会作用，组织相关专家开展标准研讨活动，通过培训、咨询、论坛等手段推进标准的宣贯。积极组织开展标准试点示范，形成最佳实践，促进标准在业界的应用推广。

四是加强国际交流合作。加强与国际标准化组织的交流与合作，积极参与国际电信联盟（ITU）、国际标准化组织（ISO）、国际电工技术委员会（IEC）等国际标准化组织活动及国际标准研制。积极促进国内标准与国际接轨，推动国内先进标准向国际标准转化。

附件1 术语定义

1、网络数据

通过网络收集、存储、传输、处理和产生的各种电子数据。

2、重要数据

我国机构和个人在境内收集、产生的不涉及国家秘密，但与国家安全、经济发展以及公共利益密切相关的数据。

3、个人信息

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。

4、数据出境

网络运营者通过网络等方式，将其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，通过直接提供或开展业务、提供服务、产品等方式提供给境外机构、组织或个人的一次性活动或连续性活动。

5、数据全生命周期

数据从产生，经过数据采集、数据传输、数据存储、数据处理（包括计算、分析、可视化等）、数据交换，直至数据销毁等各种生存形态的演变过程。

6、数据交换

为满足不同平台或应用间数据资源的传送和处理需要，依据一定的原则，采取相应的技术，实现不同平台和应用间数据资源的流动过程。

7、数据清洗

对数据进行重新审查和校验的过程，目的在于删除重复信息、纠正存在的错误，处理无效值和缺失值，并提供数据一致性。

8、数据质量监控

从数据的完整性、准确性、一致性和及时性等方面，对采集数据的质量进行识别、度量、监控、预警的过程。

9、数据完整性

数据没有遭受以未经授权方式所作的更改或破坏的特性。

10、大数据平台

采用分布式存储和计算技术，提供大数据的访问和处理，支持大数据应用安全高效运行的软硬件集合，包括监测大数据的存储、输入/输出、操作控制等大数据服务软硬件基础设施。

11、安全审计

对事件进行记录和分析，并针对特定事件采取相应比较的动作。

12、数据防泄露

通过一定的技术手段，防止机构的指定数据或信息资产以违反安全策略规定的形式流出机构的一种策略。

13、匿名化

通过对于个人信息的技术处理，使得个人信息主体无法被识别，且处理后的信息不能被复原的过程。

14、去标识化

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。

15、数据脱敏

对某些敏感信息通过脱敏规则进行数据的变形，实现敏感隐私数据的可靠保护。

16、安全多方计算

多个数据所有者在互不信任的情况下进行协同计算，输出计算结果，并保证

任何一方均无法得到除应得的计算结果之外的其他任何信息。

17、透明加密

通过监控应用程序对文件的操作，在打开文件时自动对密文进行解密，在写文件时自动将内存中的明文加密写入存储介质，从而保证存储介质上的文件始终处于加密状态。

18、数据篡改

数据被篡改、增加或删除，造成数据破坏。

19、数据溯源

记录原始数据在整个生命周期内(从产生、传播到消亡)的演变信息和演变处理内容。

附件2 网络数据安全相关标准项目明细表

序号	标准名称	标准号/计划号	所属组织	状态
基础共性				
术语定义				
1.	《信息安全技术 术语》		SAC/TC260	征求意见稿
2.	《电信数据服务平台 第2部分：术语及参考模型》	2018-2321T-YD	CCSA	征求意见稿
数据安全框架				
3.	《信息安全技术 大数据安全参考框架》		SAC/TC260	研究项目
4.	《信息技术 安全技术 隐私保护框架》		SAC/TC260	研究项目
数据分类分级				
5.	《信息安全技术 数据安全分类分级实施指南》		SAC/TC260	研究项目
6.	《电信和互联网服务 用户个人信息保护 定义及分类》	YD/T 2781-2014	CCSA	已发布
7.	《电信和互联网服务 用户个人信息保护 分级指南》	YD/T 2782-2014	CCSA	已发布
8.	《电信运营商 大数据安全管控分类分级技术要求》	2018-0162T-YD	CCSA	征求意见稿
9.	《基础电信企业数据分类分级方法》	2019-0216T-YD	CCSA	征求意见稿
10.	《电信和互联网物联网业务数据分类分级方法》		CCSA	拟制定
关键技术				
数据采集				
11.	《使用cookie进行互联网数据采集的安全性要求》	2013-2498T-YD	CCSA	报批稿
12.	《公共安全大数据 数据采集与预处理》	2019-CCSA-08	CCSA	草案
数据传输				
13.	《信息安全技术 电子文档加密与签名消息语法》	GB/T 31503-2015	SAC/TC260	已发布
14.	《信息安全技术 XML数字签名语法与处理规范》		SAC/TC260	征求意见稿
数据存储				
15.	《信息安全技术 信息系统安全审计产品技术要求和测试评价方法》	GB/T 20945-2013	SAC/TC260	已发布
16.	《信息安全技术 网络存储安全技术要求》		SAC/TC260	报批稿
17.	《信息安全技术 数据库管理系统安全技术要求》		SAC/TC260	报批稿
18.	《通信存储介质 (SSD) 加密安全技术	YD/T 2390-2011	CCSA	已发布

	要求》			
19.	《电信网数据泄露防护系统 (DLP) 技术要求》	2018-1785T-YD	CCSA	报批稿
20.	《大数据环境下数据库审计系统技术要求》	2019-0743T-YD	CCSA	草案
21.	《电信网和互联网数据安全日志审计规范》		CCSA	拟制定
22.	《电信网和互联网数据生命周期日志通用要求》		CCSA	拟制定
数据处理				
23.	《信息安全技术 个人信息去标识化指南》	GB/T 37964-2019	SAC/TC260	报批稿
24.	《电信大数据平台数据脱敏实施方法》	2019-0215T-YD	CCSA	报批稿
25.	《面向互联网应用的健康医疗数据应用脱敏技术要求》	2019-0302T-YD	CCSA	报批稿
数据交换				
26.	《信息安全技术 数据交易服务安全要求》	GB/T 37932-2019	SAC/TC260	报批稿
27.	《信息安全技术 政务信息共享 数据安全技术要求》		SAC/TC260	征求意见稿
28.	《互联网基础资源支撑系统信息数据共享接口技术要求》	2018-0180T-YD	CCSA	报批稿
29.	《通信行业数据开放共享安全管理要求》	2017-0302T-YD	CCSA	草案
30.	《网络环境下应用数据流通安全要求》	2019-0742T-YD	CCSA	草案
31.	《数据安全流通平台技术要求》		CCSA	拟制定
数据销毁				
安全管理				
数据安全规范				
32.	《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》	GB/Z 28828-2012	SAC/TC260	已发布
33.	《信息安全技术 个人信息安全规范》	GB/T 35273-2017	SAC/TC260	报批稿
34.	《信息安全技术 个人信息工程指南》		SAC/TC260	征求意见稿
35.	《信息安全技术 个人信息告知同意指南》		SAC/TC260	征求意见稿
36.	《信息安全技术 数据安全基本要求》		SAC/TC260	征求意见稿
37.	《信息安全技术 移动互联网应用 (App) 收集个人信息基本规范》		SAC/TC260	草案
38.	《信息安全技术 个人可识别信息 (PII) 处理者在公有云中保护PII的实践指南》		SAC/TC260	草案

39.	《电信网和互联网用户个人电子信息保护通用技术要求和管埋要求》	2018-1784T-YD	CCSA	送审稿
40.	《基础电信企业重要数据识别指南》	2019-0217T-YD	CCSA	草案
41.	《电信和互联网服务 用户个人信息保护技术要求》	20173806-T-339	CCSA	草案
42.	《电信和互联网服务 用户个人信息保护技术要求 电子商务服务》	YD/T 3105-2016	CCSA	已发布
43.	《电信和互联网服务 用户个人信息保护技术要求 移动应用商店》	YD/T 3106-2016	CCSA	已发布
44.	《电信和互联网服务 用户个人信息保护技术要求 即时通信服务》	YD/T 3327-2018	CCSA	已发布
45.	《电信和互联网服务 用户个人信息保护技术要求 基础电信服务》	2018-1688T-YD	CCSA	草案
46.	《电信和互联网服务 用户个人信息保护技术要求 出行服务》	2018-1687T-YD	CCSA	草案
数据安全评估				
47.	《信息安全技术 数据库管理系统安全评估准则》		SAC/TC260	报批稿
48.	《信息安全技术 数据出境安全评估指南》		SAC/TC260	送审稿
49.	《信息安全技术 个人信息安全影响评估指南》		SAC/TC260	报批稿
50.	《信息安全技术 大数据业务安全风险控制实施指南》		SAC/TC260	研究项目
51.	《互联网新技术新业务安全评估要求 大数据技术应用与服务》	2017-0298T-YD	CCSA	报批稿
52.	《电信和互联网数据安全风险评估实施方法》	2018-1669T-YD	CCSA	报批稿
53.	《电信网和互联网数据安全要求》	2019-0218T-YD	CCSA	送审稿
54.	《电信网和互联网数据安全评估规范》	2019-0219T-YD	CCSA	征求意见稿
55.	《电信网和互联网数据安全评估实施技术要求》	2019-0220T-YD	CCSA	征求意见稿
56.	《电信网和互联网数据安全评估服务机构能力认定准则》		CCSA	拟制定
监测预警与处置				
57.	《网络安全威胁数据报送接口要求》	2016-1069T-YD	CCSA	报批稿
应急响应与灾难备份				
58.	《信息安全技术 灾难恢复服务要求》	GB/T 36957-2018	SAC/TC260	已发布
59.	《信息安全技术 存储介质数据恢复服务要求》	GB/T 31500-2015	SAC/TC260	已发布

60.	《第三方灾备数据交换技术要求》	YD/T 2393-2011	CCSA	已发布
61.	《电信网和互联网灾难备份及恢复实施指南》	2017-1024T-YD	CCSA	草案
62.	《电信和互联网数据安全事件应急响应实施指南》		CCSA	拟制定
安全能力认证				
63.	《信息安全技术 大数据服务安全能力要求》	GB/T 35274-2017	SAC/TC260	已发布
64.	《信息安全技术 灾难恢复服务能力评估准则》	GB/T 37046-2018	SAC/TC260	已发布
65.	《信息安全技术 数据备份与恢复产品技术要求与测试评价方法》	GB/T 29765-2013	SAC/TC260	已发布
66.	《信息安全技术 数据安全能力成熟度模型》	GB/T 37988-2019	SAC/TC260	报批稿
67.	《信息安全技术 数据安全能力成熟度模型》		SAC/TC260	草案
68.	《面向互联网的数据安全能力技术框架》	YD/T 3644-2020	CCSA	已发布
69.	《电信网和互联网第三方安全服务能力评定准则》	2018-1783T-YD	CCSA	草案
重点领域				
5G				
70.	《5G移动通信网 安全技术要求》	2018-2367T-YD	CCSA	报批稿
71.	《5G数据安全总体技术要求》		CCSA	拟制定
移动互联网				
72.	《信息安全技术 移动智能终端数据存储安全技术要求与测试评价方法》	GB/T 34977-2017	SAC/TC260	已发布
73.	《信息安全技术 移动智能终端个人信息保护技术要求》	GB/T 34978-2017	SAC/TC260	已发布
74.	《信息安全技术 移动互联网安全审计产品技术要求》		SAC/TC260	征求意见稿
75.	《移动互联网环境下个人信息共享技术导则》	YD/T 3411-2018	CCSA	已发布
76.	《移动浏览器个人信息保护技术要求》	YD/T 3367-2018	CCSA	已发布
77.	《移动智能终端上的个人信息保护技术要求》	YD/T 3082-2016	CCSA	已发布
78.	《移动互联网环境下个人数据共享评估和测试方法》	2016-1933T-YD	CCSA	报批稿
79.	《移动应用软件个人信息保护要求和评估方法》	2019-1132T-YD	CCSA	征求意见稿
80.	《移动应用软件SDK安全技术要求和测试方法》		CCSA	拟制定

81.	《移动应用软件SDK安全指南》		CCSA	拟制定
82.	《移动应用商店数据安全要求》		CCSA	拟制定
车联网				
83.	《车联网信息服务 数据安全技术要求》	2017-0926T-YD	CCSA	报批稿
84.	《车联网信息服务 用户个人信息保护要求》	2017-0959T-YD	CCSA	送审稿
85.	《基于移动互联网的汽车用户数据应用与保护技术要求》	2018-0182T-YD	CCSA	征求意见稿
86.	《基于移动互联网的汽车用户数据应用与保护评估方法》	2018-0183T-YD	CCSA	草案
87.	《网络预约出租汽车服务平台数据安全防护要求》	2017-0938T-YD	CCSA	草案
物联网				
88.	《信息安全技术 物联网数据传输安全技术要求》	GB/T 37025-2018	SAC/TC260	已发布
89.	《基于区块链的物联网数据交换与共享技术分析》	2017B73	CCSA	报批稿
90.	《基于区块链的安全可信物联网数据通信架构》	2018-2359T-YD	CCSA	草案
工业互联网				
91.	《信息安全技术 工业控制系统信息安全分级规范》	GB/T 36324-2018	SAC/TC260	已发布
92.	《信息安全技术 工业控制系统网络审计产品安全技术要求》		SAC/TC260	报批稿
93.	《工业互联网数据安全保护要求》	2018-1369T-YD	CCSA	征求意见稿
94.	《工业互联网安全能力成熟度评估规范》	2018-1395T-YD	CCSA	征求意见稿
云计算				
95.	《信息安全技术 政府网站云计算服务安全指南》	GB/T 38249-2019	SAC/TC 260	已发布
96.	《信息安全技术 云计算安全参考架构》	GB/T 35279-2017	SAC/TC 260	已发布
97.	《信息安全技术 云计算服务安全能力评估方法》	GB/T 34942-2017	SAC/TC 260	已发布
98.	《信息安全技术 云计算服务安全指南》	GB/T 31167-2014	SAC/TC 260	已发布
99.	《信息安全技术 云计算服务安全能力要求》	GB/T 31168-2014	SAC/TC 260	已发布
100.	《云计算安全框架》	YD/T 3148-2016	CCSA	已发布
101.	《公有云服务安全防护要求》	YD/T 3157-2016	CCSA	已发布
102.	《公有云服务安全防护检测要求》	YD/T 3158-2016	CCSA	已发布
103.	《面向云服务的数据安全标记规范》	YD/T 3470-2019	CCSA	已发布

104.	《云服务用户数据保护能力参考框架》	2018-1796T-YD	CCSA	报批稿
105.	《云服务用户数据保护能力评估方法第1部分：公有云》	2018-1797T-YD	CCSA	报批稿
106.	《云服务用户数据保护能力评估方法第2部分：私有云》	2019-0209T-YD	CCSA	报批稿
107.	《电信和互联网云服务业务数据分类分级方法》		CCSA	拟制定
大数据				
108.	《信息安全技术 大数据安全管理指南》	GB/T 37973-2019	SAC/TC260	报批稿
109.	《信息安全技术 电信领域大数据安全防护实现指南》		SAC/TC260	草案
110.	《大数据平台安全管理产品安全技术要求研究》		SAC/TC260	研究项目
111.	《电信运营商的大数据应用业务安全技术要求》	YD/T 3472-2019	CCSA	已发布
112.	《电信和互联网大数据平台安全防护要求》	2017-0929T-YD	CCSA	报批稿
113.	《电信和互联网大数据平台安全防护检测要求》	2018-1782T-YD	CCSA	报批稿
114.	《大数据处理平台安全基线要求 应用及基础设施平台》	2017-0297T-YD	CCSA	征求意见稿
115.	《电信网和互联网数据资产梳理规范》		CCSA	拟制定
人工智能				
116.	《移动智能终端人工智能应用的个人信息保护技术要求及评估方法》	2019-0745T-YD	CCSA	草案
117.	《人工智能服务平台数据安全要求和评估方法》	2019-0031T-YD	CCSA	草案
区块链				
118.	《区块链开发平台网络与数据安全技术要求》	2017-1054T-YD	CCSA	报批稿
119.	《基于区块链的边缘云网络数据共享机制研究》	2019B62	CCSA	草案
120.	《金融交易中的区块链智能合约与分布式账本安全技术研究》	2019B32	CCSA	草案

(十九) APP 违法违规收集使用个人信息自评估指南

本指南主要用于 App 运营者对其他收集使用个人信息的情况进行自查自纠。App 运营者应遵守《[网络安全法](#)》、《[消费者权益保护法](#)》等法律要求，参考个人信息保护国家标准，持续提升个人信息保护水平。

一、隐私政策文本

评估项 1：隐私政策的独立性、易读性

评估点	评估标准
1. 是否有隐私政策	在 App 界面中能够找到隐私政策, 包括通过弹窗、文本链接、常见问题 (FAQs) 等形式。
2. 隐私政策是否单独成文	隐私政策以单独成文的形式发布, 而不是作为用户协议, 用户说明等文件中的一部分存在。
3. 隐私政策是否易于访问	进入 App 主功能界面后, 通过 4 次以内的点击, 能够访问到隐私政策, 且隐私政策链接位置突出、无遮挡。
4. 隐私政策是否易于阅读	隐私政策文本文字显示方式 (字号、颜色、行间距等) 不会造成阅读困难。

评估项 2：清晰说明各项业务功能及所收集个人信息类型

评估点	评估标准
5. 是否明示收集个人信息的业务功能	隐私政策中应当将收集个人信息的业务功能逐项列举, 不应使用“等、例如”字样。 注: 业务功能是指 App 面向个人用户所提供的一类完整的服务, 如地图导航、网络约车、网上购物、即时通讯、网络支付等。
6. 业务功能与所收集个人信息类型是否一一对应	隐私政策中对每个业务功能都应说明其所收集的个人信息类型, 不应出现多个业务功能对应一类个人信息的情况。
7. 是否明示各项业务功能所收集的个人信息类型	每个业务功能在说明其所收集的个人信息类型时, 应在隐私政策中逐项列举, 不应使用“等、例如”等方式概括说明。
8. 是否显著标识个人敏感信息类型	隐私政策应对个人敏感信息类型进行显著标识 (如字体加粗、标星号、下划线、斜体、颜色等)。 注: 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) 未成年人的个人信息等。(该定义见 GB/T 35273《个人信息安全规范》3.2 节)

评估项 3：清晰说明个人信息处理规则及用户权益保障

评估点	评估标准
9. App 运营者的基本情况	隐私政策应对 App 运营者基本情况描述，至少包括： 1、公司名称； 2、注册地址； 3、个人信息保护相关负责人联系方式。
10. 个人信息存储和超期处理方式	隐私政策应对个人信息存放地域（国内、国外）；存储期限（法律规定范围内最短期限或明确的期限）、超期处理方式进行明确说明。
11. 个人信息的使用规则	如果 App 运营者将个人信息用于用户画像、个性化展示等，隐私政策中应说明其应用场景和可能对用户产生的影响。
12. 个人信息出境情况	如果存在个人信息出境情况，隐私政策中应将出境个人信息类型逐项列出并显著标识（如字体加粗、标星号、下划线、斜体、颜色等）。
13. 个人信息安全保护措施和能力	隐私政策中应对 App 运营者在个人信息保护方面采取的措施和具备的能力进行说明，如身份鉴别、数据加密、访问控制、恶意代码防范、安全审计等。
14. 对外共享、转让、公开披露个人信息规则	如果存在个人信息对外共享、转让、公开披露等情况，隐私政策中应明确一下内容： 1、对外共享、转让、公开披露个人信息的目的； 2、涉及的个人信息类型； 3、接受方类型或身份。
15. 用户权利保障机制	隐私政策中应对一下用户操作方法提供明确说明： 1、个人信息查询； 2、个人信息更正； 3、个人信息删除； 4、用户账户注销； 5、撤回已同意的授权。
16. 用户申诉渠道和反馈机制	隐私政策中至少提供一下一种投诉渠道： 1、电子邮件； 2、电话； 3、传真； 4、在线客服； 5、在线表格。
17. 隐私政策时效	应明确标识隐私政策发布、生效或更新日期。
18. 隐私政策更新	如果发生业务功能变更、个人信息出境情况变更、使用目的变更、个人信息保护相关负责人联络方式变更等情形时，隐私政策应进行相应修订，并通过电子邮件、信函、电话、推送通知等方式及时告知用户。

评估项 4：不应在隐私政策等文件中设置不合理条款

评估点	评估标准
19. 隐私政策等文件是否存在免责等不合理条款	App 运营者不应在用户协议、服务协议、隐私政策等文件中出现免除自身责任、加重用户责任、排除用户主要权利条款。 注：免除自身责任是指App运营者免除其依照法律规定应当负有的强制性法定义务； 加重用户责任是指App运营者要求用户在法律规定的义务范围之外承担责任或损失； 排除用户主要权利是指App运营者排除用户依照法律规定或者依照合同的性质通常应当享有的主要权利。

二、App 收集使用个人信息行为

评估项 5：收集个人信息应明示收集目的、方式、范围

评估点	评估标准
20. 是否向用户明示收集、使用个人信息的目的、方式、范围	1、在用户安装、注册或首次开启 App 时，应主动提醒用户阅读隐私政策。 2、当App打开系统权限时（不包括用户自行在系统设置中打开权限的情况），App应当说明该权限将收集个人信息的目的。 3、收集个人敏感信息时，App应通过弹窗提示等明显方式向用户明示收集、使用个人信息的目的、方式、范围。
21. 若使用 Cookie 及其同类技术收集个人信息，是否向用户明示	当使用 Cookie 等同类技术（包括脚本、Clickstream、Web 信标、Flash Cookie、内嵌 Web 链接、sdk 等）收集个人信息时，应向用户明示所收集个人信息的目的、类型。
22. 若存在嵌入第三方代码插件收集个人信息的功能，是否向用户明示	如果通过嵌入第三方代码、插件等方式将个人信息传输至第三方服务器，应通过弹窗提示等方式明确告知用户。

评估项 6：收集使用个人信息应经用户自主选择同意，不应存在强制捆绑授权行为

评估点	评估标准
23. 收集个人信息前是否征得用户自主选择同意	App 收集个人信息前应提供由用户主动选择同意或不同意的选项，不同意应仅影响与所拒绝提供个人信息相关的业务功能。
24. 是否存在将多项业务功能和权限打包，要求用户一揽子接受的情形	1、不应通过捆绑 App 多项业务功能的方式，要求用户一次性接受并授权同意多项业务功能收集个人信息的请求。 2、根据用户主动填写、点击、勾选等自主行为，作为产品或服务的业务功能开启或开始收集个人信息的条件。

评估项 7：收集个人信息应满足必要性要求

评估点	评估标准
25. 实际收集的个人信息类型是否超出隐私政策所述范围	各业务功能实际收集的个人信息类型应与隐私政策所描述内容一致，不应超出隐私政策所述范围。
26. 收集与业务功能有关的非必要信息，是否经用户自主选择同意	当 App 运营者收集的个人信息超出必要信息范围时，应向用户明示所收集个人信息目的并经用户自主选择同意。 注1：必要信息指与基本业务功能直接相关，缺少该信息则基本业务功能无法实现的信息。 注2：自主选择同意是指个人信息主体通过书面声明或主动做出肯定性动作，对其个人信息进行待处理做出明确授权的行为。肯定性动作包括个人信息主体主动做出声明（电子过纸质形式）、主动勾选、主动点击“同意”“注册”“发送”“拨打”、主动填写或提供等。
27. 是否收集与业务功能无关的个人信息	App 不应收集与业务功能无关系的个人信息。
28. 是否在用户明确拒绝后继续索要权限、打扰用户	对于用户明确拒绝使用、关闭或退出的特定业务功能，App 不应再次询问用户是否打开该业务功能或相关系统权限。
29. App 更新是否更改系统权限设置	App 更新升级后，不应更改原有的系统权限设置。

三、App 运营则对用户授权权利的保障

评估项 8：支持用户注销账号、更正或删除个人信息

评估点	评估标准
30. 是否支持用户注销账号	App 应提供注销账号的途径（如在线功能界面、客服电话等），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。
31. 是否支持用户查询、更正或删除个人信息	App 应提供查询更正、删除个人信息的途径。

评估项 9：及时反馈用户申诉

评估点	评估标准

32. 是否及时反馈用户申诉	App 运营者应妥善处理并及时反馈用户申诉, 原则上在 15 天内回复处理意见或结果。

(二十) 中央网信办关于印发《国家网络安全事件应急预案》的通知

(中网办发文〔2017〕4号)

各省、自治区、直辖市、新疆生产建设兵团党委网络安全和信息化领导小组，中央和国家机关各部委、各人民团体：

《国家网络安全事件应急预案》已经中央网络安全和信息化领导小组同意，现印发给你们，请认真组织实施。

中央网络安全和信息化领导小组办公室

2017年1月10日

1 总则

1.1 编制目的

建立健全国家网络安全事件应急工作机制，提高应对网络安全事件能力，预防和减少网络安全事件造成的损失和危害，保护公众利益，维护国家安全、公共安全和社会秩序。

1.2 编制依据

《中华人民共和国突发事件应对法》、《中华人民共和国网络安全法》、《国家突发公共事件总体应急预案》、《突发事件应急预案管理办法》和《信息安全技术信息安全事件分类分级指南》（GB/Z 20986-2007）等相关规定。

1.3 适用范围

本预案所指网络安全事件是指由于人为原因、软硬件缺陷或故障、自然灾害等，对网络和信息系统或者其中的数据造成危害，对社会造成负面影响的事件，可分为有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障、灾害性事件和其他事件。

本预案适用于网络安全事件的应对工作。其中，有关信息内容安全事件的应对，另行制定专项预案。

1.4 事件分级

网络安全事件分为四级：特别重大网络安全事件、重大网络安全事件、较大网络安全事件、一般网络安全事件。

(1) 符合下列情形之一的，为特别重大网络安全事件：

①重要网络和信息系统的遭受特别严重的系统损失，造成系统大面积瘫痪，丧失业务处理能力。

②国家秘密信息、重要敏感信息和关键数据丢失或被窃取、篡改、假冒，对国家安全和社会稳定构成特别严重威胁。

③其他对国家安全、社会秩序、经济建设和公共利益构成特别严重威胁、造成特别严重影响的网络安全事件。

(2) 符合下列情形之一且未达到特别重大网络安全事件的，为重大网络安全事件：

①重要网络和信息系统的遭受严重的系统损失，造成系统长时间中断或局部瘫痪，业务处理能力受到极大影响。

②国家秘密信息、重要敏感信息和关键数据丢失或被窃取、篡改、假冒，对国家安全和社会稳定构成严重威胁。

③其他对国家安全、社会秩序、经济建设和公共利益构成严重威胁、造成严重影响的网络安全事件。

(3) 符合下列情形之一且未达到重大网络安全事件的，为较大网络安全事件：

①重要网络和信息系统的遭受较大的系统损失，造成系统中断，明显影响系统效率，业务处理能力受到影响。

②国家秘密信息、重要敏感信息和关键数据丢失或被窃取、篡改、假冒，对

国家和社会稳定构成较严重威胁。

③其他对国家安全、社会秩序、经济建设和公众利益构成较严重威胁、造成较严重影响的网络安全事件。

(4) 除上述情形外，对国家安全、社会秩序、经济建设和公众利益构成一定威胁、造成一定影响的网络安全事件，为一般网络安全事件。

1.5 工作原则

坚持统一领导、分级负责；坚持统一指挥、密切协同、快速反应、科学处置；坚持预防为主，预防与应急相结合；坚持谁主管谁负责、谁运行谁负责，充分发挥各方面力量共同做好网络安全事件的预防和处置工作。

2 组织机构与职责

2.1 领导机构与职责

在中央网络安全和信息化领导小组（以下简称“领导小组”）的领导下，中央网络安全和信息化领导小组办公室（以下简称“中央网信办”）统筹协调组织国家网络安全事件应对工作，建立健全跨部门联动处置机制，工业和信息化部、公安部、国家保密局等相关部门按照职责分工负责相关网络安全事件应对工作。必要时成立国家网络安全事件应急指挥部（以下简称“指挥部”），负责特别重大网络安全事件处置的组织指挥和协调。

2.2 办事机构与职责

国家网络安全应急办公室（以下简称“应急办”）设在中央网信办，具体工作由中央网信办网络安全协调局承担。应急办负责网络安全应急跨部门、跨地区协调工作和指挥部的事务性工作，组织指导国家网络安全应急技术支撑队伍做好应急处置的技术支撑工作。有关部门派负责相关工作的司局级同志为联络员，联络应急办工作。

2.3 各部门职责

中央和国家机关各部门按照职责和权限，负责本部门、本行业网络和信息系

统网络安全事件的预防、监测、报告和应急处置工作。

2.4 各省（区、市）职责

各省（区、市）网信部门在本地区党委网络安全和信息化领导小组统一领导下，统筹协调组织本地区网络和信息系统的网络安全事件的预防、监测、报告和应急处置工作。

3 监测与预警

3.1 预警分级

网络安全事件预警等级分为四级：由高到低依次用红色、橙色、黄色和蓝色表示，分别对应发生或可能发生特别重大、重大、较大和一般网络安全事件。

3.2 预警监测

各单位按照“谁主管谁负责、谁运行谁负责”的要求，组织对本单位建设运行的网络和信息系统的开展网络安全监测工作。重点行业主管或监管部门组织指导做好本行业网络安全监测工作。各省（区、市）网信部门结合本地区实际，统筹组织开展对本地区网络和信息系统的开展安全监测工作。各省（区、市）、各部门将重要监测信息报应急办，应急办组织开展跨省（区、市）、跨部门的网络安全信息共享。

3.3 预警研判和发布

各省（区、市）、各部门组织对监测信息进行研判，认为需要立即采取防范措施的，应当及时通知有关部门和单位，对可能发生重大及以上网络安全事件的信息及时向应急办报告。各省（区、市）、各部门可根据监测研判情况，发布本地区、本行业的橙色及以下预警。

应急办组织研判，确定和发布红色预警和涉及多省（区、市）、多部门、多行业的预警。

预警信息包括事件的类别、预警级别、起始时间、可能影响范围、警示事项、应采取的措施和时限要求、发布机关等。

3.4 预警响应

3.4.1 红色预警响应

(1) 应急办组织预警响应工作，联系专家和有关机构，组织对事态发展情况进行跟踪研判，研究制定防范措施和应急工作方案，协调组织资源调度和部门联动的各项准备工作。

(2) 有关省（区、市）、部门网络安全事件应急指挥机构实行24小时值班，相关人员保持通信联络畅通。加强网络安全事件监测和事态发展信息搜集工作，组织指导应急支撑队伍、相关运行单位开展应急处置或准备、风险评估和控制工作，重要情况报应急办。

(3) 国家网络安全应急技术支撑队伍进入待命状态，针对预警信息研究制定应对方案，检查应急车辆、设备、软件工具等，确保处于良好状态。

3.4.2 橙色预警响应

(1) 有关省（区、市）、部门网络安全事件应急指挥机构启动相应应急预案，组织开展预警响应工作，做好风险评估、应急准备和风险控制工作。

(2) 有关省（区、市）、部门及时将事态发展情况报应急办。应急办密切关注事态发展，有关重大事项及时通报相关省（区、市）和部门。

(3) 国家网络安全应急技术支撑队伍保持联络畅通，检查应急车辆、设备、软件工具等，确保处于良好状态。

3.4.3 黄色、蓝色预警响应

有关地区、部门网络安全事件应急指挥机构启动相应应急预案，指导组织开展预警响应。

3.5 预警解除

预警发布部门或地区根据实际情况，确定是否解除预警，及时发布预警解除信息。

4 应急处置

4.1 事件报告

网络安全事件发生后，事发单位应立即启动应急预案，实施处置并及时报送信息。各有关地区、部门立即组织先期处置，控制事态，消除隐患，同时组织研判，注意保存证据，做好信息通报工作。对于初判为特别重大、重大网络安全事件的，立即报告应急办。

4.2 应急响应

网络安全事件应急响应分为四级，分别对应特别重大、重大、较大和一般网络安全事件。I级为最高响应级别。

4.2.1 I 级响应

属特别重大网络安全事件的，及时启动I级响应，成立指挥部，履行应急处置工作的统一领导、指挥、协调职责。应急办24小时值班。

有关省（区、市）、部门应急指挥机构进入应急状态，在指挥部的统一领导、指挥、协调下，负责本省（区、市）、本部门应急处置工作或支援保障工作，24小时值班，并派员参加应急办工作。

有关省（区、市）、部门跟踪事态发展，检查影响范围，及时将事态发展变化情况、处置进展情况报应急办。指挥部对应对工作进行决策部署，有关省（区、市）和部门负责组织实施。

4.2.2 II 级响应

网络安全事件的II级响应，由有关省（区、市）和部门根据事件的性质和情况确定。

(1) 事件发生省（区、市）或部门的应急指挥机构进入应急状态，按照相关应急预案做好应急处置工作。

(2) 事件发生省（区、市）或部门及时将事态发展变化情况报应急办。应急办将有关重大事项及时通报相关地区和部门。

(3) 处置中需要其他有关省（区、市）、部门和国家网络安全应急技术支

撑队伍配合和支持的，商应急办予以协调。相关省（区、市）、部门和国家网络安全应急技术支撑队伍应根据各自职责，积极配合、提供支持。

（4）有关省（区、市）和部门根据应急办的通报，结合各自实际有针对性地加强防范，防止造成更大范围影响和损失。

4.2.3 Ⅲ级、Ⅳ级响应

事件发生地区和部门按相关预案进行应急响应。

4.3 应急结束

4.3.1 I 级响应结束

应急办提出建议，报指挥部批准后，及时通报有关省（区、市）和部门。

4.3.2 II 级响应结束

由事件发生省（区、市）或部门决定，报应急办，应急办通报相关省（区、市）和部门。

5 调查与评估 特别重大网络安全事件由应急办组织有关部门和省（区、市）进行调查处理和总结评估，并按程序上报。重大及以下网络安全事件由事件发生地区或部门自行组织调查处理和总结评估，其中重大网络安全事件相关总结调查报告报应急办。总结调查报告应对事件的起因、性质、影响、责任等进行分析评估，提出处理意见和改进措施。

事件的调查处理和总结评估工作原则上在应急响应结束后30天内完成。

6 预防工作

6.1 日常管理

各地区、各部门按职责做好网络安全事件日常预防工作，制定完善相关应急预案，做好网络安全检查、隐患排查、风险评估和容灾备份，健全网络安全信息通报机制，及时采取有效措施，减少和避免网络安全事件的发生及危害，提高应对网络安全事件的能力。

6.2 演练

中央网信办协调有关部门定期组织演练，检验和完善预案，提高实战能力。

各省（区、市）、各部门每年至少组织一次预案演练，并将演练情况报中央网信办。

6.3 宣传

各地区、各部门应充分利用各种传播媒介及其他有效的宣传形式，加强突发网络安全事件预防和处置的有关法律、法规 and 政策的宣传，开展网络安全基本知识和技能的宣传活动。

6.4 培训

各地区、各部门要将网络安全事件的应急知识列为领导干部和有关人员的培训内容，加强网络安全特别是网络安全应急预案的培训，提高防范意识及技能。

6.5 重要活动期间的预防措施

在国家重要活动、会议期间，各省（区、市）、各部门要加强网络安全事件的防范和应急响应，确保网络安全。应急办统筹协调网络安全保障工作，根据需要要求有关省（区、市）、部门启动红色预警响应。有关省（区、市）、部门加强网络安全监测和分析研判，及时预警可能造成重大影响的风险和隐患，重点部门、重点岗位保持24小时值班，及时发现和处置网络安全事件隐患。

7 保障措施

7.1 机构和人员

各地区、各部门、各单位要落实网络安全应急工作责任制，把责任落实到具体部门、具体岗位和个人，并建立健全应急工作机制。

7.2 技术支撑队伍

加强网络安全应急技术支撑队伍建设，做好网络安全事件的监测预警、预防防护、应急处置、应急技术支援工作。支持网络安全企业提升应急处置能力，提供应急技术支援。中央网信办制定评估认定标准，组织评估和认定国家网络安全

应急技术支撑队伍。各省（区、市）、各部门应配备必要的网络安全专业技术人才，并加强与国家网络安全相关技术单位的沟通、协调，建立必要的网络安全信息共享机制。

7.3 专家队伍

建立国家网络安全应急专家组，为网络安全事件的预防和处置提供技术咨询和决策建议。各地区、各部门加强各自的专家队伍建设，充分发挥专家在应急处置工作中的作用。

7.4 社会资源

从教育科研机构、企事业单位、协会中选拔网络安全人才，汇集技术与数据资源，建立网络安全事件应急服务体系，提高应对特别重大、重大网络安全事件的能力。

7.5 基础平台

各地区、各部门加强网络安全应急基础平台和管理平台建设，做到早发现、早预警、早响应，提高应急处置能力。

7.6 技术研发和产业促进

有关部门加强网络安全防范技术研究，不断改进技术装备，为应急响应工作提供技术支撑。加强政策引导，重点支持网络安全监测预警、预防防护、处置救援、应急服务等方向，提升网络安全应急产业整体水平与核心竞争力，增强防范和处置网络安全事件的产业支撑能力。

7.7 国际合作

有关部门建立国际合作渠道，签订合作协定，必要时通过国际合作共同应对突发网络安全事件。

7.8 物资保障

加强对网络安全应急装备、工具的储备，及时调整、升级软硬件工具，不断增强应急技术支撑能力。

7.9 经费保障

财政部门为网络安全事件应急处置提供必要的资金保障。有关部门利用现有政策和资金渠道，支持网络安全应急技术支撑队伍建设、专家队伍建设、基础平台建设、技术研发、预案演练、物资保障等工作开展。各地区、各部门为网络安全应急工作提供必要的经费保障。

7.10 责任与奖惩

网络安全事件应急处置工作实行责任追究制。

中央网信办及有关地区和部门对网络安全事件应急管理中作出突出贡献的先进集体和个人给予表彰和奖励。

中央网信办及有关地区和部门对不按照规定制定预案和组织开展演练，迟报、谎报、瞒报和漏报网络安全事件重要情况或者应急管理工作中有其他失职、渎职行为的，依照相关规定对有关责任人给予处分；构成犯罪的，依法追究刑事责任。

8 附则

8.1 预案管理

本预案原则上每年评估一次，根据实际情况适时修订。修订工作由中央网信办负责。

各省（区、市）、各部门、各单位要根据本预案制定或修订本地区、本部门、本行业、本单位网络安全事件应急预案。

8.2 预案解释

本预案由中央网信办负责解释。

8.3 预案实施时间

本预案自印发之日起实施。

附件：

1. 网络安全事件分类
2. 名词术语
3. 网络和信息系统的损失程度划分说明

附件1

网络安全事件分类

网络安全事件分为有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障、灾害性事件和其他网络安全事件等。

(1) 有害程序事件分为计算机病毒事件、蠕虫事件、特洛伊木马事件、僵尸网络事件、混合程序攻击事件、网页内嵌恶意代码事件和其他有害程序事件。

(2) 网络攻击事件分为拒绝服务攻击事件、后门攻击事件、漏洞攻击事件、网络扫描窃听事件、网络钓鱼事件、干扰事件和其他网络攻击事件。

(3) 信息破坏事件分为信息篡改事件、信息假冒事件、信息泄露事件、信息窃取事件、信息丢失事件和其他信息破坏事件。

(4) 信息内容安全事件是指通过网络传播法律法规禁止信息，组织非法串联、煽动集会游行或炒作敏感问题并危害国家安全、社会稳定和公众利益的事件。

(5) 设备设施故障分为软硬件自身故障、外围保障设施故障、人为破坏事故和其他设备设施故障。

(6) 灾害性事件是指由自然灾害等其他突发事件导致的网络安全事件。

(7) 其他事件是指不能归为以上分类的网络安全事件。

附件2

名词术语

一、重要网络与信息系统

所承载的业务与国家安全、社会秩序、经济建设、公众利益密切相关的网络和信息系统。

(参考依据:《信息安全技术信息安全事件分类分级指南》(GB/Z 20986-2007))

二、重要敏感信息

不涉及国家秘密,但与国家安全、经济发展、社会稳定以及企业和公众利益密切相关的信息,这些信息一旦未经授权披露、丢失、滥用、篡改或销毁,可能造成以下后果:

- a) 损害国防、国际关系;
- b) 损害国家财产、公共利益以及个人财产或人身安全;
- c) 影响国家预防和打击经济与军事间谍、政治渗透、有组织犯罪等;
- d) 影响行政机关依法调查处理违法、渎职行为,或涉嫌违法、渎职行为;
- e) 干扰政府部门依法公正地开展监督、管理、检查、审计等行政活动,妨碍政府部门履行职责;
- f) 危害国家关键基础设施、政府信息系统安全;
- g) 影响市场秩序,造成不公平竞争,破坏市场规律;
- h) 可推论出国家秘密事项;
- i) 侵犯个人隐私、企业商业秘密和知识产权;
- j) 损害国家、企业、个人的其他利益和声誉。

(参考依据:《信息安全技术云计算服务安全指南》(GB/T31167-2014))

附件3

网络和信息系统损失程度划分说明

网络和信息系统损失是指由于网络安全事件对系统的软硬件、功能及数据的破坏,导致系统业务中断,从而给事发组织所造成的损失,其大小主要考虑恢复系统正常运行和消除安全事件负面影响所需付出的代价,划分为特别严重的系统损失、严重的系统损失、较大的系统损失和较小的系统损失,说明如下:

a) 特别严重的系统损失：造成系统大面积瘫痪，使其丧失业务处理能力，或系统关键数据的保密性、完整性、可用性遭到严重破坏，恢复系统正常运行和消除安全事件负面影响所需付出的代价十分巨大，对于事发组织是不可承受的；

b) 严重的系统损失：造成系统长时间中断或局部瘫痪，使其业务处理能力受到极大影响，或系统关键数据的保密性、完整性、可用性遭到破坏，恢复系统正常运行和消除安全事件负面影响所需付出的代价巨大，但对于事发组织是可承受的；

c) 较大的系统损失：造成系统中断，明显影响系统效率，使重要信息系统或一般信息系统业务处理能力受到影响，或系统重要数据的保密性、完整性、可用性遭到破坏，恢复系统正常运行和消除安全事件负面影响所需付出的代价较大，但对于事发组织是完全可以承受的；

d) 较小的系统损失：造成系统短暂中断，影响系统效率，使系统业务处理能力受到影响，或系统重要数据的保密性、完整性、可用性遭到影响，恢复系统正常运行和消除安全事件负面影响所需付出的代价较小。

(二十一) 国家互联网信息办公室关于《个人信息和重要数据出境安全评估办法（征求意见稿）》公开征求意见的通知

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权益，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：

- （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、个人合法权益带来的风险;

(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。

(二十二) 工业和信息化部办公厅关于印发《电信和互联网行业提升网络数据安全保护能力专项行动方案》的通知

近年来，随着国家大数据发展战略加快实施，大数据技术创新与应用日趋活跃，产生和集聚了类型丰富多样、应用价值不断提升的海量网络数据，成为数字经济发展的关键生产要素。与此同时，数据过度采集滥用、非法交易及用户数据泄露等数据安全问题日益凸显，做好电信和互联网行业（以下简称行业）网络数据安全保护管理尤为迫切。为积极应对新形势新情况新问题，切实做好新中国成立70周年网络数据安全保障工作，全面提升行业网络数据安全保护能力，制定本方案。

一、总体要求

以习近平新时代中国特色社会主义思想为指导，全面贯彻党的十九大和十九届二中、三中全会精神，严格落实《网络安全法》《全国人民代表大会常务委员会关于加强网络信息保护的決定》《互联网信息服务管理办法》等法律法规，坚持维护数据安全与促进数据开发利用并重，坚持数据分类分级保护，坚持充分发挥政府引导作用、企业主体作用和社会监督作用，立足我部行业网络数据安全监管职责，开展为期一年的行业提升网络数据安全保护能力专项行动（以下简称专项行动），加快推动构建行业网络数据安全综合保障体系，为建设网络强国、助力数字经济发展提供有力保障和重要支撑。

二、工作目标

（一）通过集中开展数据安全合规性评估、专项治理和监督检查，督促基础电信企业和重点互联网企业强化网络数据安全全流程管理，及时整改消除重大数据泄露、滥用等安全隐患，2019年10月底前完成全部基础电信企业（含专业公司）、50家重点互联网企业以及200款主流App数据安全检查，圆满完成新中国成立70周年等重大活动网络数据安全保障工作。

（二）基本建立行业网络数据安全保障体系。网络数据安全制度标准体系进一步完善，形成行业网络数据保护目录，制定15项以上行业网络数据安全标准规范，贯标试点企业不少于20家；行业网络数据安全管理和技木支撑平台基本建成，

遴选网络数据安全技术创新示范项目不少于30个；基础电信企业和重点互联网企业网络数据安全管理体系有效建立。

三、重点任务

（一）加快完善网络数据安全制度标准

1.强化网络数据安全管理制度设计。梳理对标《网络安全法》《电信和互联网用户个人信息保护规定》等法律法规要求，加快建立网络数据分类分级保护、数据安全风险评估、数据安全事件通报处置、数据对外提供使用报告等制度。部署电信和互联网企业按照法律法规要求，开展数据安全管理制度对标工作，健全完善企业内部网络数据安全全生命周期安全管理制度。

2.完善网络数据安全标准体系。推动出台行业《网络数据安全标准体系建设指南》，加快完善行业网络数据安全标准体系。制定出台行业重要数据识别指南、网络数据安全防护等重点标准，遴选企业开展贯标试点。指导中国通信标准化协会成立网络数据安全标准专项工作组，加快推动网络数据安全相关标准制定工作。

（二）开展合规性评估和专项治理

3.开展网络数据安全风险评估。出台网络数据安全合规性评估要点，依托互联网新技术新业务安全评估机制，部署基础电信企业（含专业公司）和重点互联网企业结合重点业务类型和场景，开展网络数据安全合规性自评估工作，提升企业网络数据安全风险防范能力。针对物联网、车联网、卫星互联网、人工智能等新技术新应用带来的重大互联网数据安全问题，及时开展行业评估和跨部门联合评估工作。

4.深化App违法违规专项治理。持续推进App违法违规收集使用个人信息专项治理行动，组织第三方评测机构开展App安全滚动式评测，对在网络数据安全和用户信息保护方面存在违法违规行为的App及时进行下架和公开曝光。组织开展应用商店安全责任专项部署，督促应用商店落实App运营者真实身份信息验证、应用程序安全检测、违法违规App下架等责任。创新工作模式，引导鼓励第三方机构开展App数据安全认证，探索推动应用商店等明确标识并优先推荐通过

认证的App。

5.强化网络数据安全监督执法。将企业网络数据安全责任落实情况、数据安全合规性评估落实情况作为重点内容，纳入2019年网络信息安全“双随机一公开”检查和基础电信企业网络与信息安全责任考核检查，采取远程测试、实地检查等方式开展监督检查，督促问题整改。持续开展数据泄露等网络数据安全和用户信息安全事件监测跟踪与执法调查，对违法违规行为及时采取约谈、公开曝光、行政处罚等措施，将处罚结果纳入电信业务经营不良名单或失信名单。

（三）强化行业网络数据安全

6.稳步实施网络数据资源“清单式”管理。开展电信和重点互联网企业网络数据资源调研摸底，依据网络数据重要敏感程度和泄露滥用可能造成的危害，研究形成行业网络数据保护目录，并选取重点企业开展试点应用。指导督促试点企业建立内部网络数据清单和数据分类分级管理制度，对列入目录的网络数据实施重点保护。

7.明确企业网络数据安全职能部门。指导电信和重点互联网企业加强内部网络数据安全组织保障，推动设立或明确网络数据安全管理部门和专职人员，负责承担企业内部网络数据安全管理工作，督促协调企业内部各相关主体和环节严格落实操作权限管理、日志记录和安全审计、数据加密、数据脱敏、访问控制、数据容灾备份等数据安全保护措施，组织开展数据安全岗位人员法律法规、知识技能等培训。

8.强化网络数据对外合作安全管理。落实《工业和信息化部关于加强基础电信企业数据安全规范清理数据对外合作工作的通知》等相关管理要求，督促企业定期开展网络数据对外合作业务专项排查，及时发现问题消除隐患。研究明确利用行业网络数据进行大数据开发应用的数据安全管理要求，督促企业开展合作方数据安全保障能力动态评估，充分依托合同约束、信用管理等手段强化合作方管理，切实提升网络数据共享安全管理水平。

9.加强行业网络数据安全应急管理。落实工业和信息化部相关应急预案要求，

指导企业进一步健全完善企业网络数据安全事件应急处置机制，开展应急演练，落实重大网络数据安全事件报告、调查追责、向社会公告等要求。在新中国成立70周年等重大活动保障期间，明确企业数据安全重要岗位职责要求，强化应急响应，及时处置网络数据安全突发情况。

（四）创新推动网络数据安全技术防护能力建设

10. 加强网络数据安全技术手段建设。加快建设行业网络数据安全管理和技术支撑平台，支撑开展行业数据备案管理、事件通报、溯源核查、技术检测和安全认证等工作，提升网络数据安全监管技术支撑保障能力。指导企业加大网络数据安全技术投入，加快完善数据防攻击、防窃取、防泄漏、数据备份和恢复等安全技术保障措施，提升企业网络数据安全保障能力。

11. 推动网络数据安全技术创新发展。推动成立大数据安全联盟，打造网络数据安全技术交流、联合攻关和试点应用平台。组织开展网络数据安全最佳实践案例征集和试点示范项目评选，加大技术研发、成果转化和解决方案的支持力度，促进网络数据安全先进技术创新和产品服务应用推广。制定发布网络数据安全产业发展白皮书。

12. 加强专业支撑队伍建设。成立行业网络数据安全专家委员会，为网络数据安全政策标准制定、关键技术研究、重大网络数据安全风险评估、网络数据安全示范项目评审等提供决策支撑。委托中国信息通信研究院、中国电子信息产业发展研究院、中国电子技术标准化研究院、中国互联网协会、中国通信标准化协会等单位开展面向行业的网络数据安全法律法规和政策标准宣贯、技能培训和测试检查。

（五）强化社会监督和宣传交流

13. 强化社会监督和行业自律。依托中国互联网协会12321网络不良与垃圾信息举报受理中心，建立网络数据违法违规行为举报平台，及时受理用户投诉举报。强化行业自律，指导中国互联网协会联合基础电信企业、重点互联网企业、第三方机构等签署网络数据安全自律公约，引导企业自觉履行数据安全保护义务，努力提高数据安全保护水平。

14.加强宣传展示和国际交流。充分利用中国互联网大会、中国国际大数据产业博览会、国家网络安全宣传周等，指导相关单位举办网络数据安全论坛，开展网络数据安全主题宣传日等活动，促进网络数据安全管理和技术经验交流，提升全行业数据安全意识。加强数据安全国际交流合作，利用世界互联网大会、中欧数字经济与网络安全会议等，积极开展数据安全管理经验交流和信息共享。

四、工作安排

（一）工作部署阶段（2019年7月）。部制定印发专项行动方案，组织开展宣贯部署，向各单位、各企业制定印发工作任务清单，明确各项任务时间节点和工作要求。

（二）重点保障阶段（2019年8-10月）。部组织完成电信和重点互联网企业网络数据资源调研摸底，明确数据安全合规性评估要点，指导完成各省级基础电信企业和重点互联网企业重点环节数据安全合规性评估，持续开展App违法违规收集使用个人信息专项治理，组织完成对重点企业网络数据安全责任落实情况的监督检查和隐患整改，全力做好新中国成立70周年网络数据安全保障工作。

（三）长效建设阶段（2019年11月-2020年5月）。总结固化新中国成立70周年网络数据安全保障工作经验，重点围绕关键制度、重点标准、技术手段、示范项目、支撑队伍等方面，加快推进完成重点任务举措，推动建立网络数据安全长效管理机制。

（四）总结提升阶段（2020年6-7月）。各单位、各企业梳理总结专项行动完成情况、工作成效及问题，形成工作总结报部（网络安全管理局）。部组织对专项行动工作情况进行总结通报，对典型经验做法进行推广，巩固相关工作成效。

五、工作要求

（一）加强组织领导。各单位要充分认识加快提升行业网络数据安全保护能力的重要性和紧迫性，结合本单位实际，精心组织，周密部署，迅速行动，确保专项行动顺利开展。部网络安全管理局牵头做好专项行动总体部署、推进落实、督导检查等工作；各地通信管理局结合实际，组织开展属地网络数据安全能力提升专项行动各项工作。

(二) 明确任务分工。各企业要明确责任部门 and 责任人, 对照任务清单, 坚持问题导向, 逐一细化工作措施和责任分工, 做到措施到位、责任到人, 确保专项行动各项任务落实到位、取得实效。中国信息通信研究院、中国电子信息产业发展研究院、中国电子技术标准化研究院、人民邮电报社、中国互联网协会、中国通信标准化协会等单位要做好相关支撑保障工作。

(三) 强化监督检查。部和各地通信管理局组织对各单位、各企业专项行动落实情况进行督导检查, 指导督促基础电信企业和互联网企业进一步落实相关制度标准要求, 健全完善企业网络数据安全合规管理体系, 对存在问题及时督促整改。

(四) 加强宣传通报。各单位、各企业要建立信息通报机制, 及时总结专项行动进展和成效, 每月底前将工作进展情况、取得成效、问题和建议报部网络安全管理局。大力宣传专项行动新进展、新动态及典型经验做法, 营造全行业重视网络数据安全、自觉维护网络数据安全的良好氛围, 推动专项行动扎实开展。

(二十三) 交通运输部办公厅关于印发《网络预约出租汽车监管信息交互平台运行管理办法》的通知

(交办运〔2018〕24号)

各省、自治区、直辖市、新疆生产建设兵团交通运输厅（局、委）：

经交通运输部同意，现将《网络预约出租汽车监管信息交互平台运行管理办法》印发给你们。请结合各地实际，认真贯彻执行。

附件：网络预约出租汽车监管信息交互平台数据传输质量测评指标及计算方式

交通运输部办公厅

2018年2月13日

第一章 总 则

第一条 为加强网络预约出租汽车监管信息交互平台（简称网约车监管信息交互平台）的运行管理工作，规范数据传输，提高网约车行业监管效能，营造良好的营商环境，根据《网络预约出租汽车经营服务管理暂行办法》（交通运输部 工业和信息化部 公安部 商务部 工商总局 质检总局 国家网信办令2016年第60号）等相关规定，制定本办法。

第二条 本办法所称网约车监管信息交互平台，包括交通运输部网约车监管信息交互平台（简称部级平台），省、自治区交通运输主管部门网约车监管信息交互平台（简称省级平台），直辖市、设区的市级交通运输主管部门网约车监管平台（简称城市监管平台）。

第三条 网约车监管信息交互平台数据传输、运行维护、数据质量测评等工作，适用本办法。

第四条 交通运输部指导各级网约车监管信息交互平台的运行管理等工作。

各省、自治区交通运输主管部门负责省级平台运行管理，并指导和监督本行

政区域内的网约车监管信息交互平台运行管理工作。

直辖市、设区的市级交通运输主管部门（简称城市交通运输主管部门）负责本城市的网约车监管信息交互平台使用、运行和维护管理工作。

各网约车平台公司按照相关规定，负责规范本企业网约车平台的运行管理和数据传输工作。

第二章 数据传输

第五条 各城市交通运输主管部门应当通过网约车监管信息交互平台及时录入网约车平台公司、车辆、驾驶员相关许可信息；将运政信息系统与网约车监管信息交互平台对接，实时传输更新相关许可信息。

第六条 网约车平台公司在取得相应《网络预约出租汽车经营许可证》后，应自次日零时起向部级平台传输相关基础静态信息以及订单信息、经营信息、定位信息、服务质量信息等运营数据。

第七条 网约车平台公司应加强对数据信息的规范化管理，所传输的网约车运营服务相关数据，应直接接入网约车监管信息交互平台，不得通过第三方平台或系统直接传输。

第八条 网约车平台公司数据传输至部级平台后，由部级平台将数据实时转发至相关省级平台及城市监管平台，各地交通运输主管部门不得要求网约车平台公司向省级平台或城市监管平台重复传输。

第九条 网约车监管信息交互平台所接收的运营信息数据，在线保存期限不少于6个月。

第十条 网约车平台公司应建立健全数据传输工作机制，指定专人负责数据传输工作，明确与网约车监管信息交互平台对接工作的责任人、业务人员与系统技术人员，并告知相关网约车监管信息交互平台运行维护单位。上述人员信息发生变动的，应及时告知。

第十一条 网约车平台公司因系统改造、服务器迁移等可预见原因，需要暂停网约车平台运行的，应提前72小时告知相关网约车监管信息交互平台运行维

护单位。

第十二条 因自然灾害、安全生产事故等不可预见的突发事件造成系统故障，无法正常传输数据的，网约车平台公司应及时告知相关网约车监管信息交互平台运行维护单位，并采取有效处置措施，尽快恢复系统正常运行。系统故障排除后，网约车平台公司应当及时将漏传数据补传，并提交处理情况书面报告。

第十三条 网约车平台公司在技术接入和数据传输过程中，存在可能危害部级平台系统安全的，部级平台运行维护单位有权暂停技术接入和数据传输；造成损失的，依法追究相关责任。

第三章 传输质量要求

第十四条 网约车平台公司应保证传输数据的完整性、规范性、及时性、真实性等，确保数据传输质量。

第十五条 传输数据质量满足以下方面要求：

（一）数据完整性：网约车平台公司传输的数据应符合《网络预约出租汽车监管信息交互平台总体技术要求（暂行）》相关要求，确保其基础静态信息、订单信息、经营信息、定位信息、服务质量信息等相关数据字段内容齐全完整，不遗漏信息及字段。

（二）数据规范性：网约车平台公司传输的数据字段内容在元素名称、字段名称、数据类型、字段长度、取值范围、数据精度、编码规则等应符合《网络预约出租汽车监管信息交互平台总体技术要求（暂行）》相关要求。

（三）数据及时性：网约车平台公司基础静态信息变更的，应于变更后 24 小时内将信息传输至部级平台；订单信息、经营信息、服务质量信息等应实时传输，延迟不得超过 300 秒；定位信息实时传输延迟不得超过 60 秒。

（四）数据真实性：网约车平台公司传输的数据内容应真实有效，基础静态信息、订单信息、经营信息、定位信息、服务质量信息间应当相互关联，相互关联数据之间的逻辑关系应正确、真实和完整。

第四章 传输质量测评

第十六条 部级平台对网约车平台公司数据传输质量情况定期开展测评，测评内容包括但不限于数据完整性、规范性、及时性、真实性等方面。网络预约出租汽车监管信息交互平台数据传输质量测评指标及计算方式见附件，具体测评指标和计算方法将根据行业发展情况予以更新。

第十七条 数据传输质量测评工作分为月度、年度测评，月度、年度测评周期为每自然月、自然年。

第十八条 网约车平台公司数据传输质量测评结果由部级平台定期向社会进行公布，年度测评结果纳入出租汽车企业服务质量信誉考核内容。

第五章 运行维护

第十九条 各地交通运输主管部门应明确网约车监管信息交互平台使用的责任人及联系人，并告知部级平台运行维护单位，要加强网约车监管信息交互平台登录账号的申请开通管理，并督促使用人员妥善保管账号信息，定期更换密码。

第二十条 各地交通运输主管部门应当加强系统网络安全管理，根据有关法律法规及标准实施网络安全等级保护，定期开展安全排查，对于发现的安全风险和漏洞，要及时整改，防止信息数据发生泄漏、毁损或者丢失。

第二十一条 部级、省级、城市等各级平台应当建立平台系统运行管理和故障应急处理机制，对本系统的运行情况进行7×24小时实时监测，发现系统故障及时处理。

第二十二条 各地交通运输主管部门可根据网约车行业联合监管的需要，与其他管理部门相关信息系统进行技术对接，实现信息共享。

第二十三条 网络链路维护按照分级管理的原则，由部级、省级、城市等各级平台共同开展。部、省（区）间的网络链路由部级、省级平台共同维护；省（区）内网络链路由省级平台、城市监管平台负责维护。

第六章 附 则

第二十四条 开展私人小客车合乘业务的，按照各地有关规定传输数据信息。

第二十五条 中国交通通信信息中心作为部级平台的运行维护单位，负责实施部级平台的运行维护及数据传输管理等工作，确保部级平台系统安全稳定运行。

第二十六条 本办法由交通运输部运输服务司负责解释。

第二十七条 本办法自 2018 年 3 月 1 日起施行，有效期 3 年。

附件

网络预约出租汽车监管信息交互平台

数据传输质量测评指标及计算方式

测评项	测评内容及要求	测评指标及计算方式
数据完整性	根据已许可城市数据传输情况，测评网约车平台公司已获许可但未进行数据传输的情况	城市数据传输缺失率 = 未传输数据的城市个数/应传输城市总数
	根据数据接口缺失情况，测评各项数据内容完整情况	数据接口缺失率 = 缺失数据接口项/应传输的数据接口项总数
	根据数据项字段缺失情况，测评各项数据各字段完整情况	数据项字段缺失率 = 缺失关键数据字段的数据条数/数据总条数
数据规范性	测评各项数据各字段数据是否符合有关要求，任意一条数据存在不符合规范要求的字段即为本条数据记录不规范	数据不规范率 = 不规范的数据记录条数/报送数据记录总条数
数据及时性	基础静态信息延迟不得超过24小时	基础静态信息数据延迟率 = 延迟传输时间超过24小时的基础静态信息数据记录条数/报送基础静态信息数据记录总条数

	订单信息、经营信息、服务质量信息等动态数据延迟不得超过300秒	$\text{动态数据延迟率} = \frac{\text{延迟传输时间超过300秒的动态数据数据记录条数}}{\text{报送动态数据数据记录总条数}}$
	定位信息传输延迟不得超过60秒	$\text{定位数据延迟率} = \frac{\text{延迟传输时间超过60秒的定位信息数据记录条数}}{\text{报送定位信息数据记录总条数}}$
数据真实性	测评订单发起、订单撤消、经营支付信息是否具备正确的关联关系。以订单发起信息为基准，存在不具备关联关系的数据记录即为缺失。	$\text{订单发起数据关联缺失率} = \frac{\text{不具备关联关系的订单发起数据记录条数}}{\text{订单发起数据记录总条数}}$
	测评车辆基本信息、驾驶员基本信息与经营支付信息是否具备正确的关联关系。以经营支付信息为基准，存在不具备关联关系的数据记录即为缺失。	$\text{经营支付数据关联缺失率} = \frac{\text{不具备关联关系的经营支付数据记录条数}}{\text{经营支付数据记录总条数}}$

(二十四) 工业和信息化部关于加强车联网网络安全和数据安全工作的通知

工信部网安〔2021〕134号

各省、自治区、直辖市及新疆生产建设兵团工业和信息化主管部门，各省、自治区、直辖市通信管理局，中国电信集团有限公司、中国移动通信集团有限公司、中国联合网络通信集团有限公司，有关智能网联汽车生产企业、车联网服务平台运营企业，有关标准化技术组织：

车联网是新一代网络通信技术与汽车、电子、道路交通运输等领域深度融合的新兴产业形态。智能网联汽车是搭载先进的车载传感器、控制器、执行器等装置，并融合现代通信与网络技术，实现车与车、路、人、云端等智能信息交换、共享，具备复杂环境感知、智能决策、协同控制等功能，可实现“安全、高效、舒适、节能”行驶的新一代汽车。在产业快速发展的同时，车联网安全风险日益凸显，车联网安全保障体系亟须健全完善。为推进实施《新能源汽车产业发展规划（2021-2035年）》，加强车联网网络安全和数据安全管理工作，现将有关事项通知如下：

一、网络安全和数据安全基本要求

（一）落实安全主体责任。各相关企业要建立网络安全和数据安全管理制度，明确负责人和管理机构，落实网络安全和数据安全保护责任。强化企业内部监督管理，加大资源保障力度，及时发现并解决安全隐患。加强网络安全和数据安全宣传、教育和培训。

（二）全面加强安全保护。各相关企业要采取管理和技术措施，按照车联网网络安全和数据安全相关标准要求，加强汽车、网络、平台、数据等安全保护，监测、防范、及时处置网络安全风险和威胁，确保数据处于有效保护和合法利用状态，保障车联网安全稳定运行。

二、加强智能网联汽车安全防护

(三) 保障车辆网络安全。智能网联汽车生产企业要加强整车网络安全架构设计。加强车内系统通信安全保障，强化安全认证、分域隔离、访问控制等措施，防范伪装、重放、注入、拒绝服务等攻击。加强车载信息交互系统、汽车网关、电子控制单元等关键设备和部件安全防护和安全检测。加强诊断接口（OBD）、通用串行总线（USB）端口、充电端口等的访问和权限管理。

(四) 落实安全漏洞管理责任。智能网联汽车生产企业要落实《网络产品安全漏洞管理规定》有关要求，明确本企业漏洞发现、验证、分析、修补、报告等工作程序。发现或获知汽车产品存在漏洞后，应立即采取补救措施，并向工业和信息化部网络安全威胁和漏洞信息共享平台报送漏洞信息。对需要用户采取软件、固件升级等措施修补漏洞的，应当及时将漏洞风险及修补方式告知可能受影响的用户，并提供必要技术支持。

三、加强车联网网络安全防护

(五) 加强车联网网络设施和网络系统安全防护能力。各相关企业要严格落实网络安全分级防护要求，加强网络设施和网络系统资产管理，合理划分网络安全域，加强访问控制管理，做好网络边界安全防护，采取防范木马病毒和网络攻击、网络侵入等危害车联网安全行为的技术措施。自行或者委托检测机构定期开展网络安全符合性评测和风险评估，及时消除风险隐患。

(六) 保障车联网通信安全。各相关企业要建立车联网身份认证和安全信任机制，强化车载通信设备、路侧通信设备、服务平台等安全通信能力，采取身份认证、加密传输等必要的技术措施，防范通信信息伪造、数据篡改、重放攻击等安全风险，保障车与车、车与路、车与云、车与设备等场景通信安全。鼓励相关企业、机构接入工业和信息化部车联网安全信任根管理平台，协同推动跨车型、跨设施、跨企业互联互通。

(七) 开展车联网安全监测预警。国家加强车联网网络安全监测平台建设，开展网络安全威胁、事件的监测预警通报和安全保障服务。各相关企业要建立网络安全监测预警机制和技术手段，对智能网联汽车、车联网服务平台及联网系统开展网络安全相关监测，及时发现网络安全事件或异常行为，并按照规定留存相

关的网络日志不少于 6 个月。

(八) 做好车联网安全应急处置。智能网联汽车生产企业、车联网服务平台运营企业要建立网络安全应急响应机制，制定网络安全事件应急预案，定期开展应急演练，及时处置安全威胁、网络攻击、网络侵入等网络安全风险。在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照《公共互联网网络安全突发事件应急预案》等规定向有关主管部门报告。

(九) 做好车联网网络安全防护定级备案。智能网联汽车生产企业、车联网服务平台运营企业要按照车联网网络安全防护相关标准，对所属网络设施和系统开展网络安全防护定级工作，并向所在省（区、市）通信管理局备案。对新建网络设施和系统，应当在规划设计阶段确定网络安全防护等级。各省（区、市）通信管理局会同工业和信息化主管部门做好定级备案审核工作。

四 、加强车联网服务平台安全防护

(十) 加强平台网络安全管理。车联网服务平台运营企业要采取必要的安全技术措施，加强智能网联汽车、路侧设备等平台接入安全，主机、数据存储系统等平台设施安全，以及资源管理、服务访问接口等平台应用安全防护能力，防范网络侵入、数据窃取、远程控制等安全风险。涉及在线数据处理与交易处理、信息服务业务等电信业务的，应依法取得电信业务经营许可。认定为关键信息基础设施的，要落实《关键信息基础设施安全保护条例》有关规定，并按照国家有关标准使用商用密码进行保护，自行或者委托商用密码检测机构开展商用密码应用安全性评估。

(十一) 加强在线升级服务（OTA）安全和漏洞检测评估。智能网联汽车生产企业要建立在线升级服务软件包安全验证机制，采用安全可信的软件。开展在线升级软件包网络安全检测，及时发现产品安全漏洞。加强在线升级服务安全校验能力，采取身份认证、加密传输等技术措施，保障传输环境和执行环境的网络安全。加强在线升级服务全过程的网络安全监测和应急响应，定期评估网络安全状况，防范软件被伪造、篡改、损毁、泄露和病毒感染等网络安全风险。

(十二) 强化应用程序安全管理。智能网联汽车生产企业、车联网服务平台

运营企业要建立车联网应用程序开发、上线、使用、升级等安全管理制度，提升应用程序身份鉴别、通信安全、数据保护等安全能力。加强车联网应用程序安全检测，及时处置安全风险，防范恶意应用程序攻击和传播。

五、加强数据安全保护

（十三）加强数据分类分级管理。按照“谁主管、谁负责，谁运营、谁负责”的原则，智能网联汽车生产企业、车联网服务平台运营企业要建立数据管理台账，实施数据分类分级管理，加强个人信息与重要数据保护。定期开展数据安全风险评估，强化隐患排查整改，并向所在省（区、市）通信管理局、工业和信息化主管部门报备。所在省（区、市）通信管理局、工业和信息化主管部门要对企业履行数据安全保护义务进行监督检查。

（十四）提升数据安全技术保障能力。智能网联汽车生产企业、车联网服务平台运营企业要采取合法、正当方式收集数据，针对数据全生命周期采取有效技术保护措施，防范数据泄露、毁损、丢失、篡改、误用、滥用等风险。各相关企业要强化数据安全监测预警和应急处置能力建设，提升异常流动分析、违规跨境传输监测、安全事件追踪溯源等水平；及时处置数据安全事件，向所在省（区、市）通信管理局、工业和信息化主管部门报告较大及以上数据安全事件，并配合开展相关监督检查，提供必要技术支持。

（十五）规范数据开发利用和共享使用。智能网联汽车生产企业、车联网服务平台运营企业要合理开发利用数据资源，防范在使用自动化决策技术处理数据时，侵犯用户隐私权和知情权。明确数据共享和开发利用的安全管理和责任要求，对数据合作方数据安全保护能力进行审核评估，对数据共享使用情况进行监督管理。

（十六）强化数据出境安全管理。智能网联汽车生产企业、车联网服务平台运营企业需向境外提供在中华人民共和国境内收集和产生的重要数据的，应当依法依规进行数据出境安全评估并向所在省（区、市）通信管理局、工业和信息化主管部门报备。各省（区、市）通信管理局会同工业和信息化主管部门做好数据出境备案、安全评估等工作。

六、健全安全标准体系

（十七）加快车联网安全标准建设。加快编制车联网网络安全和数据安全标准体系建设指南。全国通信标准化技术委员会、全国汽车标准化技术委员会等要加快组织制定车联网防护定级、服务平台防护、汽车漏洞分类分级、通信交互认证、数据分类分级、事件应急响应等标准规范及相关检测评估、认证标准。鼓励各相关企业、社会团体制定高于国家标准或行业标准相关技术要求的企业标准、团体标准。

特此通知。

工业和信息化部

2021年9月15日

(二十五) 信息安全技术 汽车采集数据的安全要求

1 范围

本文件规定了对汽车采集数据进行传输、存储和出境等处理活动的安全要求。

本文件适用于汽车制造商开展汽车的设计、生产、销售、使用、运维，也适用于主管监管部门、第三方评估机构等对汽车采集数据处理活动进行监督、管理和评估。不适用于警车、消防车、救护车、工程救险车等执行紧急任务时的汽车采集数据，以及装置有专用设备或器具的作业车辆在封闭场所内从事作业活动时的汽车采集数据。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 7258 机动车
运行安全技术条
件GB/T 25069 信
息安全技术 术语

GB/T 35273 信息安全技术 个人信息安全规范

3 术语和定义

GB 7258、GB/T 25069、GB/T 35273界定的以及下列术语和定义适用于本文件。

汽 车 vehicle

由动力驱动、用于载运人员货物的非轨道承载的车辆。

汽车采集数据 vehicle collected data

通过汽车传感设备、控制单元采集的数据，以及对其进行加工后产生的数据。

注：不包含通过网络或物理接口获取的其他系统或设备的数据。

远程信息服务平台 telematics service platform

用于车辆管理或者提供信息服务的远程系统。

4 汽车采集数据内容

汽车采集数据主要包括：

a) 车外数据：通过摄像头、雷达等传感器从汽车外部环境采集的道路、建筑、地形、交通参与者等数据，以及对其进行加工后产生的数据；

注 1：交通参与者是指参与交通活动的人，包括机动车、非机动车、其他交通工具的驾驶员与乘员，以及其他参与交通活动相关的人员。

注 2：车外数据可能包含人脸、车牌等个人信息以及车辆流量、物流等法律法规标准所规定的重要数据。

b) 座舱数据：通过摄像头、红外传感器、指纹传感器、麦克风等传感器从汽车座舱采集的数据，以及对其进行加工后产生的数据；

注 3：座舱数据可能包含驾驶员和乘员的人脸、声纹、指纹、心律等敏感个人信息。

注 4：座舱数据不包括对汽车采集数据处理产生的操控记录数据。

c) 运行数据：通过车速传感器、温度传感器、轴转速传感器、压力传感器等从动力系统、底盘系统、车身系统、舒适系统等电子电气系统采集的数据；

注 5：运行数据包含整车控制数据、运行状态数据、系统工作参数、操控记

录数据等。

- d) 位置轨迹数据: 基于卫星定位、通信网络等各种方式获取的汽车定位和途经路径相关的数据。

5 传输要求

- 5.1 未经个人信息主体单独同意, 汽车不应通过网络向外传输包含其个人信息的车外数据, 已进行匿名化处理的视频、图像数据除外。

注 1: 匿名化处理包括对视频、图像中可识别个人身份的人脸、车牌等信息进行擦除等, 确保无法利用视频、图像数据识别个人身份。

注 2: 通过网络向外传输是指通过移动通信网络、无线局域网、充电桩接口等方式, 向位于车外的设备、系统传输。

- 5.2 汽车不应通过网络向外传输座舱数据。

- 5.3 满足以下条件的, 可作为上述条款的例外情形。

- a) 为实现 5.1 所述匿名化处理功能, 需要通过远程信息服务平台实时执行匿名化处理操作的情形, 但应确保原始数据传输到平台后不用于其他目的, 并在匿名化处理后得到删除。
- b) 为实现语音识别等直接服务于驾驶人或乘员的功能, 需要通过远程信息服务平台实时配合处理座舱数据的情形, 但应征得驾驶人同意授权, 且确保功能实现后即时删除原始数据及处理结果。
- c) 为实现用户远程监控车内外情况、使用云盘存储用户数据等直接服务于用户的功能, 需要通过网络向用户终端设备传输数据或使用远程信息服务平台存储数据的情形, 但应在传输以及存储时采取加密等措施, 确保用户数据只能由用户终端设备访问, 在其他设备以及远程信息服务平台上无法访问。

d) 道路运输车辆、运营车辆依据相关行政管理要求向外传输座舱数据的情形。

e) 道路交通事故发生后按执法部门要求向外传输数据的情形。

6 存储要求

6.1 车外数据、位置轨迹数据在远程信息服务平台等车外位置中保

6.2 存时间均不应超过 14 天。满足以下条件的数据，可作为上述条款的例外。

a) 为优化行驶安全功能而存储的特定场景数据，但每车每天不应超过 3 个连续时间的数据片段，每个片段不应超过 2 分钟。

b) 符合 5.3 c)要求，用户传输到远程信息服务平台的数据。

c) 由采集训练数据的专用采集车辆或在特定区域行驶的专用测试车辆采集的数据，但车辆外部应有“测试车辆”或“数据采集车辆”及所属单位的显著标识，且驾驶人员为具备授权的特定人员。新能源汽车、道路运输车辆、网络预约出租汽车依据相关行政管理要求进行存储的数据。

d) 用于生产经营的汽车产生的，生产经营者可控的位置轨迹数据。

7 数据出境要求

7.1 车外数据、座舱数据、位置轨迹数据不应出境；运行数据如需出境，应当通过国家网信部门组织开展的数据出境安全评估。

7.2 汽车制造商应为主管监管部门开展数据出境情况的抽查工作提供技术手段，包括传输的数据格式、便于读取的数据展示方式等。

8 其他要求

- 8.1 汽车制造商应对整车的数据安全负责，全面掌握其生产的整车所含各零部件采集、传输数据情况，对零部件供应商处理汽车采集数据的行为进行约束和监督，并将汽车采集数据向外传输的完整情况对用户披露。
- 8.2 为执行相关行政管理要求采集的数据应仅用于行政管理要求明确规定的目的。

(二十六) 信息安全技术 网络预约汽车服务数据安全指南

1、范围

本文件给出了网络预约汽车服务运营者开展服务时数据收集、存储、使用、共享、公开披露、删除的数据类型、范围、方式和条件，以及数据安全要求。

本文件适用于网络预约汽车服务运营者加强数据安全保护，也适用于国家主管部门、第三方评估机构等对网络预约汽车服务数据活动进行监督、管理和评估。

2、规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 信息安全技术 术语

GB/T 35273 信息安全技术 个人信息安全规范

GB/T AAAAA 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GB/T BBBBB 信息安全技术 网络
数据处理安全规范

GB/T CCCCC 信息安全技术 个人信息收集告知同意指南

1 术语和定义

GB/T 25069和GB/T 35273界定的以及下列术语和定义适用于本文件。

1.1

网络预约汽车服务数据 online car-booking service data

任何以电子或者非电子形式对网络预约出租汽车（简称“网约车”）
服务和网络预约巡

游出租汽车（简称“出租车”）服务产生的信息的记录。包括乘客数
据、驾驶员数据、车辆 数据及服务过程中产生和收集的其

他数据。

1.2

企业订单 enterprise order

乘客所属企业与网络预约汽车服务运营者建立合作关系，乘客在所属企业设定的范围内

产生的乘车费用由所属企业承担的订单。

1.3

行程录音录像 trip audio and video

在网络预约汽车服务过程中,通过车载设备或者驾驶员App收集的车内录音录像数据及

其衍生数据。

注：衍生数据包括从视频中抽取的音频和图像等。

1.4

用户 user

使用网络预约汽车服务的个人，通常包括乘客和驾驶员。乘客包括叫车人和实际乘车人。以下缩略语适用于本文本：

App 移动互联网应用程序（mobile Internet application）

2 概述

2.1 总则

网络预约汽车服务的个人信息保护按照 GB/T 35273 的规定执行，数据安全保护按照GB/T BBBB 的规定执行。

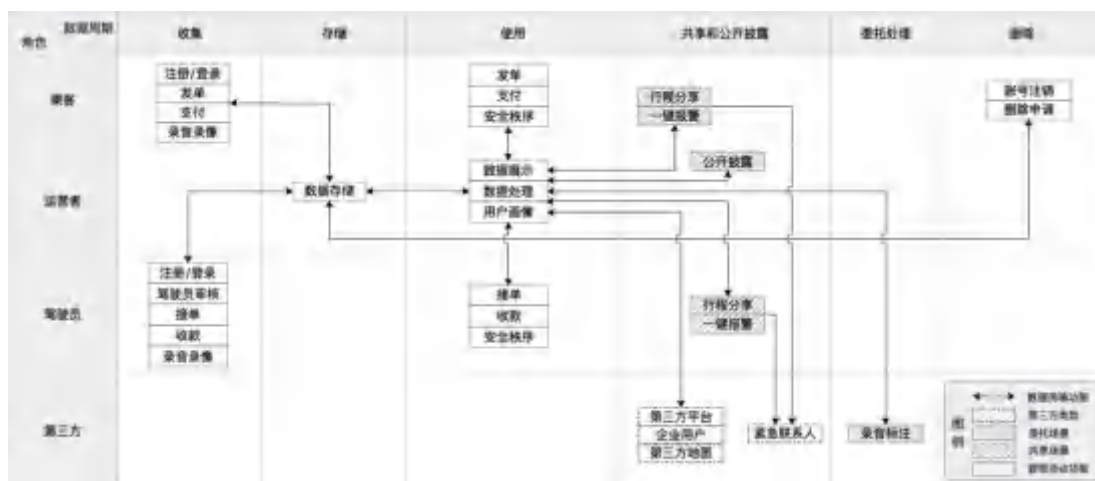
2.2 网络预约汽车服务组成

网络预约汽车服务仅包括网络预约出租汽车（简称“网约车”）服务和网络预约巡游出租汽车（简称“出租车”）服务。网络预约汽车服务的参与相关方包括用户、运营者和第三方。

2.3 网络预约汽车服务数据活动

一次完整的网络预约汽车服务活动，主要包括乘客和驾驶员注

册、网络预约汽车服务运营者对驾驶员资质审核、乘客发单、订单匹配、驾驶员接单、行程服务、网络预约汽车服务运营者对安全秩序的维护、支付收款、用户评价等。



网络预约汽车服务的数据活动及其角色和功能如图 1 所示。

图1 网络预约汽车服务数据活动及其角色和功能

2.4 网络预约汽车服务数据安全风险

网络预约汽车服务数据主要面临如下安全风险：

- 在数据收集活动中，网络预约汽车服务运营者过度收集乘客和驾驶员的个人信息或者过度索取移动智能终端操作系统权限的风险；
- 在数据传输、存储和使用活动中，网络预约汽车服务运营者未采取充分安全保护措施，如因链路监听、攻击拖库和权限不当等带来的数据泄露或滥用风险；
- 在数据共享和公开披露活动中，网络预约汽车服务运营者未经用户同意或者超出必要限度与第三方共享数据或对外公开披露数据的风险。

2.5 网络预约汽车服务数据分类分级

网络预约汽车服务数据类别包括个人信息、车辆行驶数据、统计数据和匿名化数据，依据数据的敏感程度、重要性、保护要求以及一旦泄露、丢失、破坏造成的危害程度等因素分为4个等级，详见附录A。

3 数据收集

3.1 数据收集通用要求

数据收集的通用要求包括：

- a) 网络预约汽车服务运营者在收集用户个人信息前，应告知用户并征得用户同意；
- b) 用户拒绝提供网络预约汽车服务最小必要个人信息以外的个人信息时，网络预约汽车服务运营者不应拒绝提供网络预约汽车服务；
- c) 用户拒绝提供网络预约汽车服务可选业务功能对应的最小必要个人信息时，网络预约汽车服务运营者可拒绝提供对应可选业务功能服务，但不应拒绝提供网络预约汽车服务。

3.2 网络预约汽车服务最小必要个人信息

6.2.1 乘客最小必要个人信息

网络预约汽车服务通过App收集的乘客最小必要个人信息按照GB/T AAAAA附录A.2的规定执行；网络预约汽车安装有车载设备的，收集的个人信息包括行程录音录像。

注：网络预约汽车服务接入到第三方平台时，乘客通过第三方平台提供的服务发单的，乘客个人信息的收集要求适用于第三方平台。

6.2.2 驾驶员最小必要个人信息

网络预约汽车服务运营者收集的驾驶员最小必要个人信息范围见表1。

表1 驾驶员必要个人信息

业务功能	最小必要信息	收集目的及使用要求
用户注册	手机号码	用于标识驾驶员用户和保障账号信息安全
	账号信息：账号、口令	
背景审核	身份证或者其他身份证明	用于审核是否符合法律法规规定的驾驶员资格
	面部识别特征	
	车辆信息：车辆号牌、车身颜色、品牌型号、车辆识别代号	

	驾驶证	
	行驶证	

表1 (续)

业务功能	最小必要信息	收集目的及使用要求
背景审核	车辆保险	用于审核是否符合法律法规规定的驾驶员资格
	信用记录	
	是否有相关犯罪记录	
	网络预约出租汽车驾驶员证（仅网约车收集）	
	网络预约出租汽车运输证（仅网约车收集）	
	车辆监督卡（仅出租车收集）	
接单并运送乘客	位置信息	用于确定用户当前位置，匹配订单。
	行程轨迹	记录驾驶员服务行为，用于核实服务过程、解决司乘纠纷。
	订单信息：出发地、目的地、订单时间、订单里程、订单金额	
	日志信息	
安全秩序	录音录像	用于核实处理涉及用户重要人身财产安全的订单纠纷，预防订单中违法犯罪行为的发生。
	驾驶行为信息	用于加强对驾驶员的驾驶行为监督，提升出行安全
收款	使用何种方式支付	用于用户使用第三方支付方式对约车订单收款
	银行卡号	用于驾驶员提现
风险控制	通讯设备信息	用于防控运营风险

3.3 网络预约汽车服务可选业务功能的最小必要个人信息

在网络预约汽车服务过程中，网络预约汽车服务运营者会提供一些允许用户自主选择是否使用的业务功能。本文件列举了网络预约汽车服务中典型可选业务功能，以及这些业务功能对应收集的最小必要个人信息，典型可选业务功能及对应收集的最小必要个人信息范围见附录B。

3.4 网络预约汽车服务最小必要系统权限

网络预约汽车服务最小必要系统权限要求包括：

- a) 为保证服务正常开展，乘客App需向乘客申请移动终端操作系统位置信息权限，采集位置信息频率每秒不应超过一

次；

b) 为保证服务正常开展, 驾驶员App需向驾驶员申请移动终端操作系统位置信息、麦克风和相机权限, 采集位置信息频率每秒不应超过一次。

3.5 告知同意

6.5.1 叫车人告知同意

叫车人告知同意按照GB/T CCCCC的规定执行。

6.5.2 代叫车告知同意

代叫车告知同意要求包括:

- a) 用户通过代叫车功能为他人代叫车的, 网络预约汽车服务运营者应提示叫车人收集使用实际乘车人个人信息的情况, 并取得代叫车人已告知并征得实际乘车人同意的确认;
- b) 收集录音录像信息的, 网络预约汽车服务运营者应通过短信、车内语音播报或其他方式告知实际乘车人录音录像收集情况。

6.5.3 同乘人告知同意

乘客叫车后, 有同行共同乘车的, 叫车人宜告知同乘人网络预约汽车服务运营者收集使用个人信息的情况, 并征得同乘人的同意。

6.5.4 录音录像信息收集的告知同意

网络预约汽车服务运营者收集行程录音录像信息时, 应当制定单独录音录像信息收集协议, 向用户告知录音录像信息收集方式、时间、使用用途、存储规则等内容, 行程录音录像信息收集协议应征得乘客和驾驶员双方的同意, 录音信息收集协议范式模板见附录C。

6.5.5 使用目的变更告知同意

使用目的变更告知同意要求包括:

- a) 网络预约汽车服务运营者变更个人信息使用目的，将网络预约汽车服务运营者收集、产生的个人信息用于其他业务类型，应在变更前告知用户变更使用目的的个人信息类型、变更后的使用目的，征得用户明示同意；
- b) 网络预约汽车服务运营者对用户使用网络预约汽车过程中的违规行为、纠纷记录等进行加工处理，将分析结果用于其他业务类型的风险控制前，应告知用户。

4 数据存储

数据传输和存储安全要求包括：

- a) 网络预约汽车服务运营者通过互联网传输个人信息时，应采用加密等安全措施；
- b) 网络预约汽车服务运营者应将乘客和驾驶员的个人身份信息、面部识别特征和行程录音录像数据分开存储；
- c) 网络预约汽车服务运营者不宜将行程轨迹和行程录音录像数据存储办公终端中，宜在有安全防护措施的服务器端存储。

注：采用密码技术时宜遵循密码管理相关国家标准。

5 数据使用

5.1 数据访问控制措施

数据访问控制措施要求包括：

- a) 网络预约汽车服务运营者宜采取数据分级策略，将数据分级与数据访问权限进行关联标识，访问权限应明确数据查询、更正、删除、下载等操作，定义不同级别数据访问和访问权限申请审批流程；
- b) 网络预约汽车服务运营者应对访问乘客和驾驶员个人信息的权限进行控制。不为投诉处理人员配置非需求触发访问

乘客和驾驶员订单信息的权限，投诉处理场景数据使用安全保护要求见附录D。

5.2 个人信息的展示

个人信息展示要求包括：

- a) 订单匹配后，网络预约汽车服务运营者向乘客和驾驶员展示对方个人信息用于身份核验时，所展示的个人信息应以满足核验需求为限，可向乘客展示的驾驶员信息包括驾驶员姓氏、头像、实时位置、车辆信息、评价信息，向驾驶员展示的乘客信息包括乘客手机号码最后四位、评价信息；
- b) 网络预约汽车服务运营者通过界面展示乘客和驾驶员个人信息的（如显示屏幕），应对需展示的个人信息的采取去标识化处理，为去标识化信息提供查看完整信息功能的，应对查看行为留存审计日志，去标识化规则见附录E；
- c) 乘客和驾驶员使用行程分享功能将其行程分享给亲友时，向亲友分享的信息包括分享人手机号码、驾驶员姓氏、驾驶员头像、出发地、目的地、实时位置和车辆信息；
- d) 订单匹配后，网络预约汽车服务运营者为乘客和驾驶员提供电话沟通渠道时，应使用虚拟号码；
- e) 订单完成后，网络预约汽车服务运营者为用户保留纠纷处理的联系通道（例如物品遗失沟通）时，应使用虚拟号码；
- f) 驾驶员可以选单的业务类型，应对用户评价内容进行限制，不应用户发布与网络预约汽车服务无关的评价内容；
- g) 网络预约汽车服务运营者向乘客、驾驶员展示对方给出的评价内容时，应延时、匿名提供。

5.3 用户画像的使用

用户画像的使用要求包括：

- a) 网络预约汽车服务运营者根据用户性别、年龄、饮酒情况或者其他信息进行用户画像，制定派单策略时，应以保护乘客

和驾驶员人身和财产安全为原则，尊重用户合法权利；

b) 网络预约汽车服务运营者不应滥用大数据分析等技术手段，基于用户消费记录、消费偏好等设置不公平的交易条件，侵犯用户合法权益。

5.4 驾驶员信用记录的使用

a) 网络预约汽车服务运营者建立驾驶员信用记录用于管理驾驶员的，驾驶员注销账号后，对于驾驶员在服务过程中产生的违反法律法规、违反平台规则的信用记录，以及低于初始分的信用记录，网络预约汽车服务运营者可以持续保存；

b) 驾驶员注销账号后重新注册的，对于驾驶员在服务过程中产生的违反法律法规、违反平台规则的信用记录，以及低于初始分的信用记录，网络预约汽车服务运营者可以恢复。

6 数据的共享、公开披露

6.1 数据共享

9.1.1 数据共享通用要求

数据共享通用要求包括：

- a) 网络预约汽车服务运营者与第三方数据共享按照GB/T BBBB的5.10规定执行；
- b) 不应向无业务需要的第三方共享网络预约汽车服务数据。

9.1.2 紧急情况数据共享

紧急情况数据共享要求包括：

- a) 用户设置的紧急联系人或者其他亲友以用户人身安全存在重大风险为由，要求查询用户的行程信息和位置信息的，网络预约汽车服务运营者的工作人员应先尝试拨打用户联系电话，在无法联系到用户的紧急情况下，可以向进线人提供相应的行程信息和位置信息。如联系到用户，则应依照用户要求进行处理；

- b) 网络预约汽车服务运营者宜为用户提供开启或者关闭紧急联系人查询信息授权的功能。用户事先开启紧急联系人查询用户个人信息授权的，紧急联系人要求获取用户个人信息时，网络预约汽车服务运营者可以直接提供；
- c) 在用户使用一键报警或者其他紧急情况下，网络预约汽车服务运营者可以向用户设置的紧急联系人共享其行程信息、位置信息和报警情况。

9.1.3 企业订单数据共享

企业订单数据共享要求包括：

- a) 网络预约汽车服务运营者应与企业用户约定企业订单中乘客个人信息的共享规则，在征得乘客明示同意后，可向乘客所属企业共享的个人信息包括：乘客姓名、乘客手机号码、出发地、目的地和支付信息；
- b) 乘客在企业订单过程中发生安全事件，人身财产安全受到损害或者威胁的，乘客所属企业向网络预约汽车服务运营者索要乘客行程中安全事件信息的，可以予以提供。

9.1.4 第三方地图数据共享

网络预约汽车服务接入第三方地图服务，为乘客和驾驶员提供路径规划、导航服务时，在征得乘客明示同意后，可共享通讯设备信息、实时位置和路线规划信息，不应共享乘客或驾驶员的手机号码及身份信息。

9.1.5 第三方平台数据共享

网络预约汽车服务接入到第三方平台时，乘客通过第三方平台提供的服务发单的，网络预约汽车服务运营者与第三方平台应约定在服务中共享的个人信息类型，不应超出约定范围共享个人信息。在征得乘客和驾驶员明示同意后，第三方平台数据共享要求包括：

- a) 订单匹配后，第三方平台可向网络预约汽车服务运营者共享乘客的用户标识符、手机号码、发单城市、出发地、目的地

和通讯设备信息；

b) 订单匹配后，网络预约汽车服务运营者可向第三方平台共享驾驶员的用户标识符、手机号码、姓氏、实时位置、完成订单量、车辆信息和评价信息；

c) 网络预约汽车服务运营者和第三方平台作为支付渠道的一方可向另一方共享乘客支付信息；

d) 乘客申请发票时，第三方平台可向网络预约汽车服务运营者共享电子发票投递所需的电子邮箱或纸质发票邮寄所需的收件人信息；

e) 处理乘客或者驾驶员投诉时，网络预约汽车服务运营者和第三方平台可共享必要的乘客和驾驶员的身份信息及投诉记录信息。

6.2 违法违规信息的公开披露

网络预约汽车服务运营者公开披露违法违规信息时，应对乘客或者驾驶员的身份信息进行去标识化处理，去标识化规则见附录B。

7 典型场景数据安全保护措施

7.1 行程录音录像数据安全通用要求

行程录音录像数据是网络预约汽车服务中敏感的个人信息，网络预约汽车服务运营者应制定行程录音录像数据安全管理规范重点保护，明确行程录音录像数据生命周期中收集、传输、存储、使用、披露和销毁等环节的安全控制措施。行程录音录像数据安全管理范式模板见附录F。

7.2 行程录音录像的收集

对网络预约汽车服务运营者行程录音录像的收集要求包括：

- a) 行程录音通过驾驶员App或车载设备收集，行程录像通过车载设备收集，宜优先使用车载设备收集录音；
- b) 驾驶员App生成的行程录音文件应在上传完成后删除，不应在移动终端留存；
- c) 车载设备应采取必要的安全防护，防范非授权访问，禁用

或屏蔽调试接口，防范物理接口分析入侵。

7.3 行程录音录像的存储

对网络预约汽车服务运营者行程录音录像的存储要求包括：

- a) 收集的行程录音录像数据存储时间不宜超过7天，当乘客或驾驶员有尚未解决完毕的纠纷时，对应的行程录音录像数据可以适当延长保存期限，在纠纷处理完毕且超过约定存储时限的应删除；
- b) 宜为乘客和驾驶员提供已完成订单的行程录音录像删除服务，对无纠纷和投诉等需求的订单行程录音录像删除申请在取得乘客和驾驶员确认后予以处理。

7.4 行程录音录像的使用

对网络预约汽车服务运营者行程录音录像的使用要求包括：

- a) 网络预约汽车服务运营者应与用户明确约定行程录音录像的使用用途，并严格按照约定用途使用行程录音录像，不应超出约定用途使用行程录音录像；
- b) 应对行程录音采取技术措施使录音可识别录音内容但无法识别用户身份，如对音频信息的基频进行改变等；
- c) 应对行程录像采取技术措施对乘客和驾驶员面部识别特征模糊化处理，如采取检测技术在视频中定位乘客面部位置，对面部识别特征遮挡处理等。

注：当投诉处理必须要使用行程录音录像中用原始音频基频和面部识别特征时，可不采取音频基频改变和面部识别特征遮挡等处理措施。

7.5 行程录音录像的共享

对网络预约汽车服务运营者行程录音录像的共享要求包括：

- a) 除依据法律法规规定或经用户明示同意，网络预约汽车服务运营者不应向第三方共享行程录音录像；
- b) 网络预约汽车服务运营者在向第三方共享行程录音录

像时，应经过审批，并采用加密等保护措施；

c) 网络预约汽车服务运营者宜配备专用终端设备用于行程录音录像数据的共享输出，并留存记录。

注：采用密码技术时宜遵循密码管理相关国家标准。

7.6 行程录音的委托处理

对网络预约汽车服务运营者行程录音的委托标注处理要求包括：

- a) 委托行为用于提升录音准确识别能力增强行程安全风险处置水平；
- b) 委托行为不应超出已征得用户授权同意的使用范围；
- c) 应对委托行为进行个人信息安全影响评估，经评估风险可控后进行委托行为；
- d) 将行程录音提供给受委托方前，应采取以下保护措施：
 - 1) 向受委托方提供行程录音时，不应提供行程录音所属用户的个人身份信息；
 - 2) 在满足处理需求的前提下，筛选并删除行程录音中描述个人身份信息的内容；
 - 3) 将行程录音分割为最小听音分片并打散，使之无法重新组装还原为原始文件；
 - 4) 将行程录音切片随机分发给不同的标注人员，避免切片还原为原始文件；
 - 5) 仅允许标注人员通过流式播放听音，通过技术措施防范行程录音被下载。
- e) 应对受委托方进行监督，方式包括但不限于：
 - 1) 通过合同等方式规定受委托方的责任和义务；
 - 2) 发现受委托方未充分履行安全责任和义务时，及时停止委托行为，并要求受委托方删除行程录音。

附录 A

(资料性)

网络预约汽车服务数据分类分级

A.1 网络预约汽车服务数据类别范围

网络预约汽车服务数据包括个人信息、车辆行驶数据、统计数据和匿名化数据。具体数据类别范围如下：

- a) 个人信息，网络预约汽车服务运营者在网络预约汽车服务过程中收集使用的个人信息，个人信息详细分类参照GB/T 35273附录A；
- b) 车辆行驶数据，网络预约汽车服务运营者在网络预约汽车服务过程中收集的与车辆行驶有关的数据，包括车辆行驶速度、违章处罚情况等；
- c) 统计数据，网络预约汽车服务运营者对收集的个人信息、车辆行驶数据等进行统计分析后得出的汇总数据，包括用户数、订单量和里程总数等；
- d) 匿名化数据，网络预约汽车服务运营者对收集的个人信息进行匿名化处理后得出的数据，包括匿名化后的订单信息、行驶轨迹等。

A.2 网络预约汽车服务数据分级

网络预约汽车服务运营者宜对数据进行分级标识或列出清单，数据分级应综合考虑数据的敏感程度、重要性、保护要求以及一旦泄露、丢失、破坏造成的危害程度等因素；对行踪轨迹、面部识别特征、行程录音录像等敏感数据应在在数据分级中从高考虑。根据数据重要程度、敏感度和泄露后带来的危害宜将数据划分为以下4级：

- a) 第1级：可完全公开使用的数据。包括可以通过公开途径获取的数据，例如网络预约汽车服务运营者通过官网、

公众号等公开渠道发布的统计数据等。

b) 第2级：可在较大范围内供访问使用的数据。例如不能标识个人身份的数据，在履行必要申请审批后用于统计分析。

c) 第3级：在较小范围内供访问使用的数据，如果未经授权披露，可能会对数据主体造成较高程度的损害。例如可以直接标识个人身份的数据，限于履行工作岗位职责的人员访问使用。

d) 第4级：仅在极小范围内且在严格限制条件下供访问使用的数据，如果未经授权披露，可能会对数据主体造成严重程度的损害。例如行程录音录像，当发生投诉时才能授权访问查询。

附 录 B

(规范性)

典型可选业务功能及对应收集的最小必要个人信息

表B.1给出了乘客App典型可选业务功能及对应收集的最小必要个人信息。

表B.1 乘客 App 典型可选业务功能及对应收集的最小必要个人信息

典型可选业务功能	对应收集的最小必要个人信息	收集目的及使用要求
代叫车	实际乘车人姓名、电话号码	用于驾驶员联系实际乘车人，接实际乘车人上车
添加紧急联系人	紧急联系人姓名、电话号码	当乘客使用一键报警功能或者遇到其他紧急情况时，用于将相应情况通知紧急联系人。
添加常用地址	家的地址、公司地址	用于乘客更快捷输入订单出发地、目的地
在线沟通	虚拟号码通话录音、在线沟通内容记录	用于核实事实，处理用户纠纷
评价	评价内容	用于解决纠纷，建立用户信用评价机制
客服	乘客与投诉处理人员的沟通内容	用于记录纠纷处理情况
开具发票	发票信息、纸质发票收集收件人信息、电子发票收集电子邮箱	用于开具发票

表B.2给出了驾驶员App典型可选业务功能及对应收集的最小必要个人信息。

表B.2 驾驶员 App 典型可选业务功能及对应收集的最小必要个人信息

典型可选业务功能	对应收集的最小必要个人信息	收集目的及使用要求
添加紧急联系人	紧急联系人姓名、电话号码	当驾驶员使用一键报警功能或者遇到其他紧急情况时，网络预约汽车服务运营者将相应情况通知紧急联系人
在线沟通	虚拟号码通话录音、在线沟通内容记录	用于核实事实，处理用户纠纷
评价	评价内容	用于解决纠纷，建立用户信用评价机制
客服	驾驶员与投诉处理人员的沟通内容	用于记录纠纷处理情况

注 1：用户拒绝提供可选业务功能及对应最小必要个人信息的，只影响用户使用相应的可选业务功能，不应影响用户使用其他业务功能。

注 2: 可选业务功能收集最小必要个人信息以外的个人信息, 应允许用户自主选择是否提供。用户拒绝提供的, 不影响用户使用可选业务功能。

注 3: 网络预约汽车服务运营者通过调用通讯录收集紧急联系人姓名、电话号码的, 应允许用户拒绝开启通讯录权限, 以手动输入紧急联系人姓名、电话号码。

注 4: 本附录仅列举了较为典型的网络预约汽车服务乘客 App 及驾驶员 App 的可选业务功能, 各网络预约汽车服务乘客 App 及驾驶员 APP 提供的可选业务功能可能会有所差别, 本表格未予明确的可选业务功能, 可以根据需要实现的服务目的判断其最小必要个人信息范围。

附 录 C

(资料性)

行程录音收集协议范式模板

为提升XXXX服务产品安全能力、更好地处理XXXX服务的司乘纠纷，XXXX服务上线录音功能。本协议将向您说明XXXX服务收集使用录音信息的情况，请您务必认真阅读本协议，在确认充分了解后慎重决定是否同意本协议。您点击同意后，本协议生效，对您及XXXX均具有法律约束力。

您同意本协议后，使用XXXX服务时，XXXX将通过软件或硬件设备录取您后续全部行程中的车内环境声音信息（包括您及车上人员交谈或肢体动作产生的声音），且后续行程不再做单独提示。受技术条件影响，XXXX各项服务在不同城市上线录音功能的时间不同，具体以XXXX显示的录音状态为准。

录音将通过XXXX驾驶员App或其他具备录音功能的软件或硬件进行。录音仅在驾驶员、乘客均同意的情况下开启。如乘客使用的App版本未及时更新，无法对录音进行授权，则录音不开启。

录音起始时间：

录音自订单行程开始时起（预约订单自驾驶员到达乘客出发地时起），至行程结束后适当时间停止（具体以驾驶员App显示的录音状态为准）。乘客自进入车辆后至离开车辆时，将同时被采集录音信息；

其他上线录音功能的服务的录音起始时间以XXXXApp另行告知为准。

如您是代他人叫车，在代叫车前请务必告知被代叫车人行程内录音信息收集情况，并征得被代叫车人同意后，方可为其叫车。

为保障用户的隐私，录音将实时上传至XXXX服务器，用户无法自行下载、调取或播放录音。

6、录音信息将用于以下明确列明的使用场景：

a)作为服务运营者处理用户纠纷的依据；

- b)为维护用户人身安全等重大合法利益,或情况紧急又很难得到用户同意的;
- c)用于抽查检测用户是否存在违反平台用户规则的行为;
- d)用于系统分析,设计、开发、应用保护用户安全的辅助工具或产品。

XXXX将严格保护用户个人信息安全,除以下情况外,我们不会向其他人共享您的录音信息:

相关机关依据法定程序取;

用户持法律文件依法取。

录音保存期限为7日。如遇差评、投诉、尚未处理完毕的纠纷等,将适当延长录音保存期限。

用户使用的手机等硬件设备故障、网络状态不稳定、App版本过旧以及不可抗力等因素均可能导致录音失败,您对此表示理解,如遇此类问题,XXXX不需承担责任。

X将严格按照本协议约定收集使用用户录音信息。本协议对相关内容未作明确约定的,以XXXX《个人信息保护及隐私政策》约定为准。

附录 D

(规范性)

投诉处理场景数据安全保护要求

人员安全管理

对网络预约汽车服务运营者投诉处理人员安全管理要求包括：

在投诉处理人员上岗前签署保密协议，声明对用户个人信息保护相关要求；

对投诉处理人员开展必要的安全培训，培训内容包括但不限于：网络安全法律法规、社会工程学、网络安全管理制度，通过考核方可上岗；

对投诉处理系统访问权限执行严格的申请审批控制，仅对履行投诉处理服务岗位职责的人员开放权限，在投诉处理人员工作岗位调整或离职时，及时关闭撤销所拥有的系统权限。

账号安全管理

对网络预约汽车服务运营者投诉处理系统账户安全管理要求包括：

定义并维护投诉处理系统人员账号信息，对投诉处理人员岗位职责、角色和业务类型进行定义说明，对不同岗位、角色、业务类型投诉处理人员数据访问范围进行限定；

采取多因素身份验证措施，防止身份冒用和账号共享，同一投诉处理人员不能在不同终端上同时登录，对投诉处理人员登录投诉处理系统网络地址进行限定。

工单有效期限限制

网络预约汽车服务运营者根据业务需要限定已处理完成的投诉工单有效期，及时关闭投诉处理人员已处理完成订单数据的权限。

数据防泄漏

网络预约汽车服务运营者投诉处理系统应采取页面安全水印技术，对投诉处

理人员的操作行为进行监控，防止系统数据泄露。

安全审计

网络预约汽车服务运营者应部署自动化审计系统，收集、记录和监测个人信息查询、更正、删除及下载等处理活动，包括但不限于以下内容：

审计日志内容包括：账号、网络地址、操作时间、操作行为、操作结果等；

根据审计数据进行统计分析，支持生成审计报表；

根据审计数据分析挖掘个人信息违规查询、违规下载、违规外发等异常行为，并通过实时告警通知安全管理人员进行处置。

注：网约预约汽车服务运营者其他业务场景下的人员安全管理、账号安全管理、数据防泄漏和安全审计等数据安全保护措施参照投诉处理场景相关要求执行。

附录 E

(资料性)

网络预约汽车服务数据去标识化规则

表E.1给出了网络预约汽车服务数据去标识化规则。

表E.1 网络预约汽车服务数据去标识化规则

序号	数据类型	去标识化规则	备注
1	姓名	展示第一个字，后面都隐藏。如：张*	
2	手机号码	显示前 3 位，后 4 位，中间隐藏。如： 188****8888	
3	固定电话号码	显示前 3 位，后 4 位，中间隐藏。如：010****8888	
4	地址信息	显示省/市/县区信息，街道地址隐藏。如：山东省 青岛市市南区**街道**	
5	坐标信息	显示前 3 位，后 3 位隐藏。如：经度 113.***、 纬度 22.4***	在 App 中可对乘客和驾驶员展示未脱敏位置信息
6	车辆号牌	显示前 3 位和最后 1 位，中间 3 位隐藏。如：京 A8***8	
7	发动机号码	显示前 3 位和最后 2 位，中间 2 位隐藏。如： 888**8K	
8	车辆识别代号	显示前 13 位和最后 1 位，中间 3 位隐藏。 如LSGJR88U88K88***8	
9	身份证号	显示前 3 位，后 2 位，中间隐藏，如： 110*****33	

附录 F
(资料性)

行程录音录像数据安全规范模板

行程录音录像安全规范模板包括行程录音录像保护的目、范围、依据、术语定义、安全要求、处罚措施和维护更新等内容。

表 F.1 给出了行程录音录像数据安全规范模板。

表F.1 行程录音录像数据安全规范模板

行程录音录像数据安全规范模板	编写要求
1、目的 1 行程录音录像数据为敏感个人信息，应采用安全管理和技术措施进行重点保护。 1 为了保护行程录音录像数据，降低信息资产被泄露或破坏的风险，特制定本规范，保证用户个人信息不受侵害。	说明本规范的制定的目的
2、适用范围 1 本规范适用于任何与行程录音录像数据有关的行为，包括行程录音录像数据生命周期中的收集、传输、存储、使用、披露、销毁等环节的安全控制。	说明本规范的适用范围或适用场景
3、规范依据 1 《中华人民共和国网络安全法》 1 《信息安全技术 个人信息安全规范》(GB/T35273—2020)	列举本规范制定时依据的国家法律法规
4、术语定义 1 网络预约汽车服务过程中，通过车载录像设备收集的行程录音录像数据或者通过App收集的行程录音数据，及其衍生数据。 1 安全区域：为满足查询行程录音录像信息安全要求设立的物理封闭区域（例如某层楼或某房间）称为安全区域。	对本规范中出现的名词术语进行定义说明

5、行程录音录像数据安全要求 本要求围绕行程录音录像数据的生命周期各环节提出, 根据此要求执行行程录音录像数据安全工作。在不违反以下原则的情况下, 可以根据业务场景进行安全要求的细化。 (1) 行程录音录像数据收集 a) 采集行程录音录像数据必须通过乘客同意; b) 行程录音录像数据自产生之时起需全程加密。加密要求如下: 密码算法…… 密钥长度…… c) 不得留存未加密行程录音录像数据; …… (2) 行程录音录像数据传输 在传输行程录音录像数据时, 应遵守以下安全要求: a) 在进行行程录音录像传输时, 链路应加密; b) 禁止使用第三方网盘、即时聊天工具等方式传输行程录音录像数据; ……	详细说明行程录音录像数据在收集、传输、存储、使用、披露及删除销毁环节应采取的安全措施。

表F.1 (续)

行程录音录像数据安全管理范式模版	编写要求
(3) 行程录音录像数据存储 线上存储应符合以下要求: a) 行程中录音录像文件应加密存储在独立的存储集群; b) 严格控制存储集群访问权限, 必须获得相应的授权后才可以访问; …… 线下存储应符合以下要求: c) 保存行程录音录像数据的介质 (例如纸质文件、光盘等) 应当保存在有锁的柜子中或独立的封闭区域 (如档案室等), 并留存使用记录; …… (4) 行程录音录像数据使用 a) 使用行程录音录像数据必须经过审批; b) 行程录音录像应接入水印标识; c) 必须在安全区域内访问行程录音录像数据; d) 禁止利用右键、下载工具等方法下载行程录音录像数据; e) 访问行程录音录像数据的人员必须签署保密协议, 并向访问人员提供回执确认; f) 除法律规定的情形外, 行程录音录像数据不得向第三方提供, 对第三方提供前必须经过XXXX审批; …… (5) 行程录音录像数据披露 a) 不得擅自通过各种媒介对外披露 (包括但不限于亲友、客户及第三方合作方) 披露工作中接触到行程录音录像数据; b) 对外披露行程录音录像数据必须经过XXX部门审批; ……	

(6) 行程录音录像数据删除销毁 a) 行程录音录像保存的期限：默认存储X天，有差评投诉保存X天，有重大投诉保存至投诉工单关闭； b) 行程录音录像数据在使用完毕后应进行删除； c) 包含行程录音录像数据的纸质文件应通过碎纸机销毁； 	
6、安全区域及终端安全要求 (1) 安全区域物理安全要求 行程录音录像的查询使用在封闭的安全区域内完成，安全区域应至少采取以下安全保护措施： a) 安全区域出入口安排专人值守并配置电子门禁系统，控制、鉴别和记录出入的人员； b) 安全区域与外部连接的通风口、窗户等通道部署防盗报警装置； c) 电子门禁系统与警报系统联动或具备警报功能，并采取指纹或人脸识别等技术进行身份核实防范身份冒用； d) 配置视频监控系统，对人员活动行为进行全方位监控； e) 对进入物理区域的人员随身携带的物品进行限制，禁止携带手机、相机、录音笔、优盘等电子设备； f) 配备专门的安全运营人员，对物理区域的运行进行安全审计，采取措施包括但不限于： 1) 根据物理区域安全管理要求监督进入员工行为，如身份核验、禁止携带物品的监督提醒； 2) 采取定时和不定时巡查，对发现的异常、告警和故障等及时记录并上报，采取必要的纠正措施； 3) 抽检视频监控和门禁记录，排查违规行为和安全隐患。	详细说明安全区域及终端设备应采取的安全措施。

表F.1 (续)

行程录音录像数据安全规范式模版	编写要求
(2) 安全区域内终端设备安全要求 用于行程录音录像查询使用的终端设备采取必要的技术防护措施，包括但不限于： a) 网络准入控制：对终端设备进行身份认证、安全检查，非授权设备禁止访问行程录音和行程录像信息； b) 网络行为监控：对终端设备文件操作访问、上网行为、网络协议等进行管控和审计，禁止具备即时通讯、公有云存储等与录音录像无关的互联网应用，防止外发、泄露行程录音和行程录像信息泄露； c) 网络防病毒：及时更新系统补丁并采取恶意代码防护措施，防范病毒、木马、蠕虫、间谍软件等恶意程序传播感染； d) 端口管控：对终端设备的通用串行总线和蓝牙等外部连接进行管控，防范非法外联，设置专用听音设备，禁止随意插拔更换。 	
7、处罚措施 1 明令禁止违反该制度规定的行为，具体的处罚措施包括： a) 通报批评：..... b) 警告：..... c) 解除劳动关系：..... d) 移交司法机关：..... 1 鼓励对违反本规范要求违规使用行程录音录像数据的行为进行检举。 	详细说明违反本规范对相关人员的处罚措施，可列举说明各类处罚条款。
8、维护更新 1 本规范由.....制定和解释。 1 本规范自公布之日起施行，员工有义务及时阅读，了解行程录音录像数据安全要求，并遵照执行。 	

参 考 文 献

【1】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

【2】《中华人民共和国网络安全法》2016 年 11 月 7 日第十二届全国人民代表大会常务委员会第二十四次会议通过

【3】《全国人大常委会关于维护互联网安全的决定》 2000 年 12 月 28 日第九届全国人民代表大会常务委员会第十九次会议通过

【4】《全国人大常委会关于加强网络信息保护的决定》 2012 年 12 月 28 日第十一届全国人民代表大会常务委员会第三十次会议通过

【5】《中华人民共和国电子商务法》 2018 年 8 月 31 日第十三届全国人民代表大会常务委员会第五次会议通过

【6】《电信和互联网用户个人信息保护规定》2013 年 7 月 16 日中华人民共和国工业和信息化部令第 24 号公布，自 2013 年 9 月 1 日起施行

【7】《移动互联网应用程序信息服务管理规定》2016 年 6 月 28 日国家互联网信息办公室发布，自 2016 年 8 月 1 日起实施

【8】《网络交易管理办法》经中华人民共和国国家工商行政管理总局局务会审议通过，自2014 年 3 月 15 日起施行

【9】《网络预约出租汽车经营服务管理暂行办法》2016 年 7 月 14 日经交通运输部第 15 次部务会议通过，并经工业和信息化部、公安部、商务部、工商总局、质检总局、国家网信办同意，自 2016 年 11 月 1 日起施行

【10】《中华人民共和国刑法修正案（七）》 2009 年 2 月 28 日第十一届全国人民代表大会常务委员会第七次会议通过

【11】《中华人民共和国刑法修正案（九）》 2015 年 8 月 29 日第十二届全国人民代表大会常务委员会第十六次会议通过

(二十七) 国家地名和区划数据库管理办法（试行）

第一章 总则

第一条 为规范国家地名和区划数据库的使用、维护、更新，确保数据完整、规范、准确、有效，数据库管理系统安全高效运行，更好地为我国经济社会发展和国防建设服务，方便群众生产生活，根据有关法规及规定，制定本办法。

第二条 本办法所称国家地名和区划数据库，是指以地理信息系统和数据库技术等为基础，对地名和行政区划、行政区域界线等数据的采集、录（导）入、存储、处理、分析、应用的计算机管理系统，由国家、省（自治区、直辖市）、市（自治州、地区、盟）、县（市、市辖区）四级数据库组成，使用统一的软件平台，其中国家级数据库存储全国范围的数据，省、市、县三级数据库各存储本行政区域内的数据。

第三条 国家地名和区划数据库管理工作内容包括：

- （一）采集、审核、录（导）入数据；
- （二）更新、补充、修改数据；
- （三）按时限报送数据；
- （四）定期进行数据备份；
- （五）硬件设备配置及管理维护；
- （六）软件研发、配备、升级及运行维护；
- （七）数据管理和应用；
- （八）安全保密管理。

第四条 国家地名和区划数据库运行管理执行以下标准：

- （一）《地名分类与类别代码编制规则》（GB / T18521-2001）；
- （二）《国家地名数据库代码编制规则》（民地办发〔2010〕1号）；

(三) 《国家地名数据库建设指导意见》（民办发〔2006〕4号）；

(四) 第二次全国地名普查试点工作规程（修订版）。

第二章 工作职责

第五条 县级以上各级人民政府行政区划和地名主管部门（以下简称主管部门）负责本级地名和区划数据库的使用、更新维护、运行管理、开发应用及配套建设。

第六条 民政部负责制定国家地名和区划数据库建设规划，研究制定有关法规和技术标准；组织开发应用各种比例尺的图形库数据；组织研发数据库管理系统软件和软件升级；省级数据库建设的技术指导、上报数据审核和检查验收；组织开展技术培训；负责国家数据库数据的汇总、修改、管理应用和安全保密等工作。

第七条 省级主管部门负责本行政区域内各级数据库建设的组织协调、技术指导、业务培训、上报数据审核、督促检查；本级数据库数据的修改、关联、汇总上报、管理应用及安全保密等工作。

第八条 市级主管部门负责本行政区域内县级数据库建设的技术指导、业务培训、上报数据审核、检查验收；本级数据库数据的采集、录（导）入、修改、关联、核对、汇总上报、管理应用及安全保密等工作。

第九条 县级主管部门负责本行政区域内的地名和行政区划、行政区域界线等数据的采集、录（导）入、修改、关联、核对、汇总上报、管理应用，业务培训及安全保密等工作。

第三章 数据采集、更新、报送

第十条 数据库数据分为专题地名和行政区划属性数据、空间图形数据和多媒体数据。

(一) 专题地名和行政区划属性数据是指反映地名、行政区划、行政区域界线的文字、数字等相关数据。

1.地名：包括自然地理实体和人文地理实体的名称、地理位置及附属信息。自然地理实体包括海域、水系、陆地地形等；人文地理实体包括各级行政区域及非行政区域、群众自治组织、居民点、具有地名意义的交通运输设施、水力电力通信设施、纪念地与旅游胜地、建筑物、单位等。

2.行政区划：包括行政区划概况、沿革、人口、面积、经济、城建等数据。

3.行政区域界线：包括行政区域界线协议书、界桩登记表、界线联检成果及会议纪要，边界纠纷处理协议，平安边界建设成果等。

（二）空间图形数据是指不同比例尺的矢量地图和遥感影像、行政区域界线矢量数据；地名标志、界桩等矢量数据。

（三）多媒体数据是指描述地理实体、地名标志、界桩的图像、视频、音频等数据；描述界线的有关文件扫描图等。

第十一条 各级主管部门应协调相关部门，建立地名和区划数据采集机制，按照有关技术标准和时限要求，统一做好数据采集、入库工作。

第十二条 数据更新坚持准确规范、上下联动的原则。数据发生变更的，应在20个工作日内完成数据更新工作，县级主管部门每年1、4、7、10月，市级主管部门每年2、5、8、11月，省级主管部门每年6、12月分别将更新数据汇总审核后以安全方式报送。

第十三条 数据增加、修改、更新、删除，应当履行审批备案制度，由审批的主管部门建立纸质和电子档案，永久保存。

第四章 数据共享使用

第十四条 地名和区划数据分为基础数据、政务数据和公共数据，分别按不同权限、面向不同对象、以不同形式进行共享使用。

第十五条 基础数据是指数据库内的全部数据，主要面向民政系统（地名主管部门）、军队有关部门，在专用计算机或内部保密专网上共享或以文件交换方式提供使用，与政务网、互联网进行物理隔离。

第十六条 政务数据是指经筛选并通过保密审核的数据，主要面向政府部门，供浏览查阅，不能下载保存，不同用户授予不同权限，使用环境与互联网逻辑隔离。

第十七条 公共数据是指经筛选并脱密处理的数据，面向社会公众，通过互联网、问路电话、触摸屏等平台提供相关信息。

第十八条 政务数据和公共数据须依程序审批后共享使用，具体程序为：

（一）主管部门结合地名更新和公共服务需求，定期编制地名和区划数据共享目录，并通过公共平台或门户网站公布共享目录、使用权限、共享方式及相关要求；

（二）使用部门对照目录，根据需要向主管部门提出书面申请，明确使用目的、数据范围、有关需求等内容；

（三）主管部门审查后，经过脱密处理，授权使用部门使用并对其进行监督。

第五章 运行维护

第十九条 各级主管部门须配备数据采集设备、专用保密计算机及存储设备，有条件的可配备专用机房及监控、防水、防火、防尘、防电磁、防辐射、防雷击等配套设施，定期检查系统运行情况，并制定故障恢复预案，做到有备无患。

第二十条 各级主管部门应采取安全访问权限控制措施，严格执行身份验证制度，防止未经授权用户访问数据库。未经批准，任何人不得对后台数据库进行数据更改操作。确需后台操作的，必须经批准，并事先对数据库进行备份，详细记录数据更改情况并存档备查。

第二十一条 各级主管部门应建立安全存储机制，保证数据安全，每年6、12月对数据进行多份、异质备份，检查备份数据存储介质，并填写数据备份管理日志。

第二十二条 各级主管部门要指派专职人员负责数据采集和系统管理，建立岗前培训制度，定期组织技术培训；管理人员调离岗位时须移交全部相关资料，确保数据库运行不受人员更替影响。

第二十三条 各级主管部门要结合自身实际制定责任分工制度、系统维护制度、运行操作规程、档案管理制度和情况反馈机制。

第二十四条 各级主管部门要向同级人民政府积极争取，将建库、更新、维护、升级等经费作为专项经费纳入年度财政预算，也可以向企事业单位有偿提供数据公共产品，其收益用于数据库全面建设，收费标准和收费办法按照国家有关规定执行。

第二十五条 民政部定期组织数据库管理系统软件升级。地方各级主管部门根据统一部署做好相应升级工作。

第六章 安全保密

第二十六条 国家地名和区划数据库中的涉密信息，严格遵守国家有关保密规定进行管理。

第二十七条 严格专机专用，严禁接入互联网，专用存储处理设备不能与其他计算机交叉使用，不得在联网计算机上安装运行数据库软件和处理数据；专用计算机须安装正版杀毒软件并定期查杀病毒，严格控制移动介质使用，数据上报前要进行杀毒处理。

第二十八条 专用计算机及存储处理设备出现故障，应到保密部门指定的维修单位进行维修，如送其他单位，须经本部门主管领导批准，并由专人进行现场监督；报废设备和过期数据应到保密部门指定单位进行销毁。

第二十九条 与其他单位合作建库，利用数据开展功能拓展应用，须经省级以上主管部门批准，审查其保密资质并签订保密协议，同时对数据进行脱密处理。

第三十条 加强涉密人员的保密教育。定期开展信息安全和保密教育，提高安全意识、防范意识和责任意识，确保数据安全可靠，数据库管理系统安全有序运行。

第三十一条 因管理失职或者处置不当而泄露涉密信息，有关部门和相关责任人应当承担相应的法律责任。

第七章 附则

第三十二条 各省、自治区、直辖市人民政府主管部门可结合自身实际，制定相应的管理细则。

(二十八) 交通运输部办公厅关于推进交通运输行业数据资源开放共享的实施意见

(交办科技[2016]113号)

各省、自治区、直辖市、新疆生产建设兵团及计划单列市交通运输厅（局、委），部属各单位，部内各司局：

为贯彻落实国家关于促进大数据发展和政务信息资源共享管理有关要求，充分挖掘交通运输行业数据资源价值，实现用数据说话、用数据决策、用数据管理、用数据创新，提升行业治理能力和服务水平，促进行业提质增效与转型升级，现提出如下实施意见。

一、总体要求

（一）指导思想。

深入贯彻落实党的十八大和十八届三中、四中、五中全会精神，按照党中央、国务院决策部署，遵循以目录管理数据资产、以共享促进数据融合、以开放实现数据增值的总体思路，坚持需求导向和问题导向，加强统筹协调，激发市场活力，着力突破交通运输大数据发展机制与技术障碍，提升行业数据资源开发利用价值，为打造精准治理、多方协作的行业治理模式，构建贴近需求、便捷高效的运输服务体系提供有力支撑，促进安全便捷、畅通高效、绿色智能的现代综合交通运输体系建设。

（二）基本原则。

统筹协调、联合推进。加强管理与技术体系统筹，强化行业数据资源治理，推动各类平台有效对接，打破部门分割和行业壁垒，政企合作，上下联动，共同推进数据资源开放共享。

需求导向、互利共赢。以跨部门、跨地区、跨领域业务协同需求为导向，注重盘活整合现有资源，实现行业数据资源有效共享。以提升综合交通服务品质为导向，推动行业数据资源向社会开放，充分释放行业数据红利，实现多方共赢。

激发活力、创新应用。创新行业数据资源开发利用模式，激活数据增值能力，引导鼓励企业和社会机构开展交通运输服务大数据创新应用，推动交通运输服务联动创新、融合创新、万众创新。

规范有序、保障安全。统一数据资源开放共享标准，完善相关业务规则，规范数据资源全生命周期管理，提升行业数据质量。妥善处理创新发展与保障安全的关系，强化大数据技术背景下的安全防护。

（三） 实施目标。

通过3-5年时间，实现以下目标：

1. 建立健全行业数据资源开放共享体制机制，基本建成协调联动、高效运转的行业数据资源管理体系。
2. 完善行业数据资源开放共享技术体系，建立互联互通的行业数据资源开放共享平台。
3. 围绕科学决策、精准治理、便捷服务等重点需求，开展一批跨部门、跨地区、跨领域协同应用的试点示范。

二、主要任务和措施

（一） 健全行业数据资源开放共享管理体系。

1.完善组织管理体系。明确承担部综合交通运输数据资源管理及促进应用服务职能的机构，加强行业数据资源交换共享、对外开放和开发利用等工作统筹。完善地方交通运输数据资源管理相关职能，强化数据资产管理，确保部省、省际间数据资源共享交换机制有效运行。

2.加强管理制度建设。贯彻落实国家政务信息资源共享管理有关要求，制定交通运输数据资源共享交换管理制度，厘清各单位各部门数据管理、维护及共享交换的职责、权利和义务，明确数据资源共享交换范围和工作程序，推动行业数据资源共享共用。

3.研究建立目录体系。以行业协同性、综合性业务需求为重点，梳理行业数

据资源，制定行业数据资源分级分类标准，按照行业内“共享为原则、不共享为例外”研究制定数据资源共享目录。在保障信息安全和个人隐私的基础上，合理界定数据资源权属，研究制定公共数据开放目录，建立健全目录定期更新发布机制。

4.健全监督考评机制。完善信息化建设项目管理制度，在项目立项、验收等环节，加强对数据资源建设和开放共享方案的审核。研究建立行业数据资源开放共享考评机制，将评估结果作为信息化投入的重要参考，加强对行业数据资源开放共享效能的激励和约束。

（二）完善行业数据资源开放共享技术体系。

5.加强开放共享标准规范建设。研究完善行业信息数据标准体系，加快信息资源核心元数据、信息资源标识符编码规则、信息平台互联共享、空间信息应用共享交换等基础性数据标准制修订，进一步加强标准执行的监督管理。

6.建立数据资源目录服务系统。研究制定行业数据资源目录服务系统建设指南，推动行业数据资源目录服务体系建设，开展存量数据资源著录工作，实现基于目录的数据资产管理，确保行业数据资源底数清、情况明。

7.完善数据资源共享交换平台。加快部省两级数据资源共享交换平台建设，建立各业务数据资源共享交换主干通道，形成行业统一的数据资源共享交换体系，并接入国家数据共享交换平台，实现行业数据资源共享交换，推动信息系统互联互通。

8.推动公共数据开放平台建设。加快各级交通运输公共数据开放平台建设，并接入国家数据统一开放平台，促进行业公共数据对外开放，支持大数据产品及增值服务的社会化开发。

（三）开展行业数据资源开放共享示范应用。

9.推动跨部门数据资源共享示范应用。结合行业数据资源共享交换平台建设，开展水路领域数据资源共享交换应用示范。推进部、省、市、县四级道路运输管理信息系统互联互通。加快推进交通运输信用信息管理系统建设，逐步实现行业

信用信息归集共享。在交通运行协调、综合行政执法等领域，进一步推动跨部门数据共享和业务协同应用示范。依托国家和行业统一的数据资源共享平台，开展与公安、海关、安监、旅游、气象、测绘等部门的跨部门数据资源共享应用示范。

10.推进跨地区数据资源共享示范应用。加快推进京津冀交通信息共享机制建设，在路政执法、运政执法、高速公路运行及应急管理等领域开展业务协同示范。落实长江经济带发展要求，深入推进长江航运信息资源整合工作，推动长三角地区交通运输数据资源共享交换示范。支持西部地区交通运输跨省数据资源开放共享应用。

11.推动交通运输大数据创新应用。依托行业统一的数据资源开放共享平台，以及物流、运政、海事等专业数据资源共享平台，促进行业数据资源和社会数据资源整合共享，鼓励企业和社会机构创新应用，支持建立促进创新应用的开放式技术平台，提升综合交通出行及物流信息服务能力和品质。引导社会优质资源参与交通旅游服务大数据应用开发，推进交通旅游服务大数据创新应用。

（四）保障行业数据资源开放共享规范有序。

12.完善业务规则。进一步完善行业管理业务规则，着力促进业务流程再造，明确跨部门、跨地区、整体性、协同性业务对数据资源的开放共享需求，以业务需求驱动数据资源开放共享，以数据资源开放共享促进业务流程优化和管理模式创新。

13.提升数据质量。推动交通运输基础设施与数据采集系统同步建设、同步养护，从源头保障数据完整性和及时性。各级交通运输主管部门应进一步加强数据运维与质量管控，切实保障数据准确性和一致性。

14.加强数据安全。落实数据安全有关法规制度，加强数据采集、传输、存储、使用、开发等关键环节的安全防护。加强行业重要数据资源容灾备份，提升重要数据容灾恢复能力。细化界定行业涉密信息内容，依法加强对涉及国家秘密、个人隐私和商业秘密数据的保护。

三、加强组织实施

(一) 强化协调领导。

各级交通运输主管部门要高度重视，落实“一把手”责任制，细化分解各项工作任务，合理安排工作计划，加大协调监督力度，加强实施工作的集中统筹，主动推进各项工作，确保各项任务落实到位。

(二) 确保制度执行。

各级交通运输主管部门要认真贯彻国家、行业和本部门制定实施的数据资源开放共享规章制度，将其落实到信息化建设、管理、运维等各个环节，确保各项规章制度执行有力，避免有规不依、执规不严。

(三) 保障资金投入。

各级交通运输主管部门应统筹安排好相关经费，保证各项工作有效投入。依托各地交通运输“十三五”规划，推动数据资源目录服务系统、数据资源共享交换平台、公共数据开放平台、开放共享示范应用等任务有序开展。

(四) 加强督查评估。

各级交通运输主管部门要加强督促检查，将工作推进落实情况列入年度工作目标考核，并纳入“十三五”相关规划的中期评估。

交通运输部办公厅

2016年8月25日

(二十九) 信息安全技术 个人信息安全规范

1 范围

本标准规范了开展收集、保存、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。

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可参见附录 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。

注 2：关于个人敏感信息的判定方法和类型可参见附录 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

有权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，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：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

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，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（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）。

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、经济状况、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。

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。如地图导航、网络约车、即时通讯、社区社交、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，个人信息处理活动对个人信息主体合法权益造成损害时应承担责任。

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、规则等，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

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业务功能；
- c) 不应从非法渠道获取个人信息；
- d) 不应收集法律法规明令禁止收集的个人信息；
- e) 不应大规模收集我国公民的种族、民族、政治观点、宗教信仰等个人敏感信息。

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，产品或服务的业务功能无法实现；
- 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 不强迫接受多项业务功能

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) 不应以改善服务质量、提升个人信息主体体验、研发新产品、增强安全性等为由，强迫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：

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，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、使用个人信息业务功能时，个人信息控制者可通过隐私政策的形式，实现向个人信息主体的告知；产品或服务提供多项收集、使用个人信息业务功能的，除隐私政策外，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：符合本标准5.3和5.4a)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，并确保个人信息主体的明示同意是其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；

c) 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；

d) 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 隐私政策

对个人信息控制者的要求包括：

a) 应制定隐私政策，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；

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) 隐私政策所告知的信息应真实、准确、完整；

c) 隐私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) 隐私政策应公开发布且易于访问，例如，在网站主页、移动应用程序安装页、本标准附录C.4中给出的交互式功能界面等显著位置设置链接；

e) 隐私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) 在本条a) 所载事项发生变化时，应及时更新隐私政策并重新告知个人信息主体。

注1：隐私政策的内容可参考附录D。

注2：在个人信息主体首次打开产品或服务、注册账号等情形时，宜通过弹窗等形式主动向其展示隐私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，使个人信息主体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；

注：隐私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，不应将其视为本条中的合同。

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，例如发现、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 个人信息的保存

6.1 个人信息保存时间最小化

对个人信息控制者的要求包括:

a) 个人信息保存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) 超出上述个人信息保存期限后, 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;

b) 存储个人生物识别信息时, 应采用技术措施确保信息安全后再进行存储, 例如将个人生物识别信息的原始信息和摘要分开存储, 或仅收集、存储、使用摘要信息。

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:

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本标准 10.1。

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，应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。

注：加工处理而产生的个人信息属于个人敏感信息的，对其处理应符合本标准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) 侵害保护公民、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) 除为达到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信息的选项。

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程度的能力。

7.6 基于不同业务目的所收集的个人信息的汇聚融合

对个人信息控制者的要求包括：

a) 遵守本标准7.3的要求；

b) 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，支持通过人工方式对个人信息主体投诉情形进行复核。

7.8 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。

7.9 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。

7.10 个人信息删除

对个人信息控制者的要求包括：

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。

7.11 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按同意的个人信息处理。

7.12 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，且该方法应简便易操作；

b) 宜直接设置便捷的注销功能交互式页面，及时响应个人信息主体注销请求；

c) 受理注销账号请求后，需要人工处理的，应在承诺时限内（原则上不超过十五天）完成核查和处理；

d) 注销过程进行身份核验需要个人信息主体重新提供的个人信息不应多于注册、使用等服务环节收集的个人信息；

e) 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

作记录作为必要注销条件等；

f) 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；

g) 个人信息主体注销账户后，应及时删除其个人信息或做匿名化处理。

注：因法律规规定需要留存的个人信息应妥善保管，不能将其再次应用于业务场景。

7.13 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。

7.14 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本标准第7.8至7.13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) 宜直接在产品或服务提供的界面中设置专门的功能或选项，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性方法，以保护个人信息主体的合法权益；

e) 以下情况可不响应个人信息主体基于本标准7.8至7.13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；

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。

7.15 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。

8 个人信息的委托处理、共享、转让、公开披露

8.1 委托处理

委托处理个人信息时，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本标准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, 确保受委托者达到本标准10.4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本标准7.8至7.13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保存相关个人信息。

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保存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(例如更改口令、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的个人信息。

8.2 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8.2 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) 准确记录和保存个人信息的共享、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（例如更改口令、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保存、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。

8.3 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，个人信息控制者应：

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。

8.4 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，应充分重视风险，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8.4 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) 准确记录和保存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。

8.5 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。

8.6 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。

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、使用个人信息的授权同意，则个人信息控制者与该第三方为共同个人信息控制者。

8.7 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本标准8.1和8.6的，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，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，并妥善留存、及时更新，以供个人信息主体查询、使用；
- g) 应督促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) 涉及第三方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、小程序等）的，宜：
 - 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。

8.8 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。

9 个人信息安全事件处置

9.1 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：

- 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带来严重危害的，如个人敏感信息的泄露，照本标准9.2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。

9.2 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。

10 组织的管理要求

10.1 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、定期更新隐私政策和相关规程；

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。

10.2 个人信息安全工程

开发具有处理个人信息功能的产品和服务时, 个人信息控制者宜根据有关国家标准在需求、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。

10.3 个人信息处理活动记录

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 (例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;
- c) 与个人信息处理各环节相关的信息系统、组织或人员。

10.4 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、导致歧视性待遇等;
- 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。

10.5 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, 防止个人信息的泄露、损毁、丢失、篡改。

10.6 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，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）或在隐私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隐私政策和相关规程。

10.7 安全审计

对个人信息控制者的要求包括：

a) 应对隐私政策、相关规程和安全措施的有效性进行审计；

b) 应采取建立自动化审计系统等方式，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 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、电子邮箱等

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、面部特征等

网络身份标识信息 个人信息主体账号、IP 地址、邮箱地址及与前述有关的密码、口令、口令保护答案、个人信息主体个人数字证书等

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产生的相关信息，及体重、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

银行账号、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）儿童的个人信息和自然人的隐私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的示例。

表B.1 个人敏感信息举例

个人财产信息

银行账号、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，以及与个人身体健康状况产生的相关信息等

个人生物识别信息 个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部识别特征等

个人身份信息 身份证、军官证、护照、驾驶证、工作证、社保卡、居住证等

网络身份标识信息 个人信息主体账号、口令、口令保护答案、个人信息主体个人数字证书等的组合

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

20附录 C

(资料性附录)

实现个人信息主体自主意愿的方法

保障个人信息主体自主意愿包括两个方面：一是不强迫个人信息主体接受多项业务功能；二是保障个人信息主体对个人信息收集、使用的知情权和授权同意的权利。个人信息控制者，尤其是移动应用程序运营者，可通过以下方式实现：

C.1 区分基本业务功能和扩展业务功能

保障个人信息主体选择同意的权利，首先需划分产品或服务的基本业务功能和扩展业务功能，划分的方法如下：

a)应根据个人信息主体选择、使用所提供产品或服务的根本期待和最主要的需求，划定产品或服务的基本业务功能；

注1：个人信息主体之所以识别或挑选某项产品或服务，主要依据个人信息控制者对所提供产品或服务开展的市场推广和商业定位、产品或服务本身的名称、在应用商店中的描述、所属的应用类型等因素。因此，个人信息控制者应根据一般个人信息主体对上述因素的最可能的认识和理解，而非自身想法来确定个人信息主体的主要需求和期待来划定基本业务功能。一般来说，如果产品或服务不提供基本业务功能，个人信息主体将不会选择使用该产品或服务。

注2：随着产品或服务的迭代、拓展、升级等，基本业务功能可能需要随之重新划分。个人信息控制者仍应根据一般个人信息主体最可能的认识和理解，来重新划定基本业务功能。但个人信息控制者不应短时间内大范围改变基本业务功能和扩展业务功能的划分。在重新划分后，个人信息控制者应再次告知并征得个人信息主体对基本业务功能收集、使用其个人信息的明示同意。

b) 不应将改善服务质量、提升个人信息主体体验、研发新产品单独作为基本业务功能；

c) 将产品或服务所提供的基本业务功能之外的其他功能，划定为扩展业务功能。

C.2 基本业务功能的告知和明示同意基本业务功能的告知和明示同意的实现方法如下：

a) 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），应通过交互界面或设计（如弹窗、文字说明、填写框、提示条、提示音等形式），向个人信息主体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作出肯定性动作（如勾选、点击“同意”或“下一步”等）征得其明示同意；

注：当产品或服务所提供的基本业务功能无需一次性全部开启时，应根据个人信息主体的具体使用行为逐步开启基本业务功能，并即时完成本条a)的告知要求。

b) 个人信息主体不同意收集基本业务功能所必要收集的个人信息，个人信息控制者可拒绝向个人信息主体提供该业务功能；

c) 本条a) 所要求的交互界面或设计应方便个人信息主体再次访问及更改其同意的范围。

注：上述要求的实现方式可参考附录C.4。

C.3 扩展业务功能的告知和明示同意

21 扩展业务功能的告知和明示同意的实现方法如下：

a) 在扩展业务功能首次使用前，应通过交互界面或设计（如弹窗、文字说明、填写框、提示条、提示音等形式），向个人信息主体逐一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) 个人信息主体不同意收集扩展业务功能所必要收集的个人信息，个人信息控制者不应反复征求个人信息主体的同意。除非个人信息主体主动选择开启扩展功能，在24小时内向个人信息主体征求同意的次数不应超过一次；

c) 个人信息主体不同意收集扩展业务功能所必要收集的个人信息，不应拒绝提供基本业务功能或降低基本业务功能的服务质量；

d) 本条a) 所要求的交互界面或设计应方便个人信息主体再次访问及更改其同意的范围。

注：上述要求的实现方式可参考附录C.4。

C.4 交互式功能界面设计

个人信息控制者可参考以下模板设计交互式功能界面，保障个人信息主体能充分行使其选择同意的权利。该功能界面应在个人信息控制者开始收集个人信息前，如产品安装过程中，或个人信息主体首次使用产品或服务时，或个人信息主体注册账号时，由个人信息控制者主动向个人信息主体提供。如以填写纸质材料收集个人信息的，个人信息控制者可以参考以下模板内容设计表格，以保障个人信息主体能行使选择同意的权利。

22功能界面模板 说明

1、为向个人信息主体清晰展示收集个人信息的目的、种类等，并分情形征得个人信息主体同意。建议个人信息控制者采用分阶段、分窗口、分屏幕等方式向个人信息主体展示左侧模板中的功能界面。

2、个人信息控制者需明确定义其产品（或服务）的基本业务功能，识别其所需收集的个人信息。

3、左侧模板中的赋值需要个人信息控制者根据实际情形给出，且内容应清楚明白易懂，不应使用概括性、模糊性语句描述所收集的个人信息。

4、个人信息控制者可结合实际的产品（或服务）形态，考虑适宜、便捷等因素实现左侧模板中的功能。

5、个人信息控制者在实现左侧功能界面时，“勾选处”不应采用预填写的方式。

23功能界面模板 说明

6、扩展业务功能的基本业务功能之外的其他功能，常见的扩展业务功能如：基本业务功能基础上的一些衍生服务或新型业务、提高产品（或服务）的使用体验的附加功能（如语音识别、图片识别、地理定位等）、提升产品（或服务）的安全机制的扩展功能等（如收集密保邮箱、指纹等）。

7、扩展业务功能一般具有可选择、可退订、不影响基本业务等特点，个人信息控制者在识别扩展业务功能时需要充分分析其是否具备这些特点，不应将扩展业务功能等同于基本业务功能，强迫收集个人信息。

8、在此页面中，综合个人信息主体主动填写的个人信息项和同意自动采集的个人信息项，个人信息控制者可即时展示个人信息主体可使用的扩展功能。

9、个人信息控制者应告知个人信息主体再次访问该功能界面的方法，保障个人信息主体撤回授权同意的权利。

24功能界面模板 说明

10、与第三方共享、转让和公开披露的情形可能因业务功能复杂的原因变得多样化。个人信息控制者可酌情在此页面增加共享、转让、公开披露的场景，或在个人信息主体使用过程中以弹窗等形式单独告知，并征得同意。

11、数据安全能力指个人信息控制者保护个人信息保密性、完整性和可用性的能力，个人信息控制者可以通过开展相关的国家标准合规工作证明其数据安全能力，并将相关证明以链接形式向个人信息主体展示。

12、个人信息控制者应向个人信息主体提供针对处理规则的答疑渠道，如果个人信息主体不认可其处理规则，可以选择不继续使用该产品（或服务）。

13、应向个人信息主体告知与个人信息控制者联系的方式。

14、应明示隐私政策的链接，以便个人信息主体查阅。

25附 录 D

(资料性附录)

隐私政策模板

发布隐私政策是个人信息控制者遵循公开透明原则的重要体现，是保证个人信息主体知情权的重要手段，还是约束自身行为和配合监督管理的重要机制。隐私政策应清晰、准确、完整地描述个人信息控制者的个人信息处理行为。

隐私政策模版 编写要求

本政策仅适用于XXXX的XXXX产品或服务，包括……。

最近更新日期：XXXX年XX月。

如果您有任何疑问、意见或建议，请通过以下联系方式与我们联系：

电子邮件：

电 话：

传 真：

该部分为适用范围。包含隐私政策所适用的产品或服务范围、所适用的个人信息主体类型、生效及更新时间等。

本政策将帮助您了解以下内容：

业务功能一的个人信息收集使用规则

业务功能二的个人信息收集使用规则

我们如何保护您的个人信息 您的权利我们如何处理儿童的个人信息

您的个人信息如何在全球范围转移本政策如何更新

如何联系我们

深知个人信息对您的重要性，并会尽全力保护您的个人信息安全可靠。我们致力于维持您对我们的信任，恪守以下原则，保护您的个人信息：权责一致原则、

目的明确原则、选择同意原则、最小必要原则、确保安全原则、主体参与原则、公开透明原则等。同时，承诺，我们将按业界成熟的安全标准，采取相应的安全保护措施来保护您的个人信息。请在使用我们的产品（或服务）前，仔细阅读并了解本《隐私政策》。该部分为隐私政策的重点说明，是隐私政策的一个要点摘录。目的是使个人信息主体快速了解隐私政策的主要组成部分、个人信息控制者所做声明的核心要旨。

26业务功能一的个人信息收集使用规则

1、我们收集哪些您的个人信息

我们提供的业务功能需要依赖部分信息才得以运行。您选择使用该项业务功能，则需要向我们提供或允许我们收集的必要信息包括：……共计XX类个人信息。

您可自主选择向我们提供或允许我们收集下列信息：……共计XX类个人信息。这些信息并非该业务功能运行所必需，但这些信息对改善服务质量、研发新产品或服务等有非常重要的意义。我们不会强制要求您提供这些信息，您如拒绝不会对使用该业务功能产生不利影响。

在您使用该业务功能时，我们的App会向您申请下列与个人信息相关的系统权限：……共计XX项系统权限。如果您不授权，将会导致我们无法提供该业务

功能。除上述权限之外，您可自主选择是否额外授予App其他的系统权限。

2、我们如何使用您的个人信息

对于必要的个人信息，我们会用来提供该项业务功能，包括……我们也会使用上述信息来维护和改进本项业务功能，开发新的业务功能等。对于非必要的个人信息，我们会用于以下用途，包括……

3、我们如何委托处理、共享、转让、公开披露您的个人信息

(1) 委托处理

本业务功能中某些具体的模块或功能由外部供应商提供。例如我们会聘请服务提供商来协助我们提供客户支持。对我们委托处理个人信息的公司、组织和个

人，我们会与其签署严格的保密协定，要求他们按照我们的要求、本隐私政策以及其他任何相关的保密和安全措施来处理个人信息。

(2) 共享

我们不会与本公司以外的任何公司、组织和个人分享您的个人信息，除非获得您的明确同意。目前，我们会在以下情形中，向您征求您对共享个人信息的授权同意：

a)了解此情形中目前涉及的公司、组织和个人，请点击此处。【提供超链接】

b)了解此情形中目前涉及的公司、组织和个人，请点击此处。【提供超链接】

c)了解此情形中目前涉及的公司、组织和个人，请点击此处。【提供超链接】

我们可能会根据法律法规规定，或按政府主管部门的强制性要求，对外共享您的个人信息。

(3) 转让

我们不会将您的个人信息转让给任何公司、组织和个人，但以下情况除外：

1、详细列举收集和使用个人信息的业务功能，不应使用概括性语言。

2、根据不同业务功能，分别列出各业务功能所收集的个人信息类型。

3、明确描述哪些类型的个人信息属于特定业务功能所必需的。

4、收集身份证、护照、驾照等法定证件信息和个人生物识别信息时，应专门提醒个人信息主体此次收集活动涉及的信息，并说明处理目的、处理规则。

5、不应使用概括性语言综述所收集个人信息，如“我们收集您的身份等相关信息”此类描述，而应明确写明“我们收集您的姓名、电话号码、地址信息”。

6、说明个人信息在使用过程中涉及的地理区域，如个人信息存储和备份的地域，个人信息传输过程中涉及的地域范围；如果个人信息存在跨境传输情况，需单独列出或重点标识。

7、根据个人信息的使用情况，注明不同类型个人信息预计的保留时间（如：

自收集日期开始5年内) 以及需要删除或销毁的截止日期 (如: 2019年12月31日或个人信息主体注销账户时) 。

8、确需改变信息收集和使用的目的, 应当说明会征得个人信息主体的同意。

9、个人信息控制者说明是否需要共享、转让个人信息, 并详细描述需要共享、转让的个人信息类型和原因、个人信息的接收方、对接收方的约束和管理准则、接收方使用人信息的目的、个人信息共享、转让过程中的安全措施, 及共享、转让个人信息是否对个人信息主体带来高危风险。

10、个人信息控制者说明是否需要公开披露个人信息, 并详细描述需要公开披露的个人信息类型、原因、是否对个人信息主体带来高危风险。

11、说明何种情况下个人信息控制者会不经过个人信息主体同意, 共享、转让和公开披露数据, 如响应执法机关和政府机构的要求、进行个人信息安全审计、保护个人信息主体免受遭受欺诈和严重人身伤害等。

27隐私政策模版 编写要求

a) 在获取明确同意的情况下转让: 获得您的明确同意后, 我们会向其他方转让您的个人信息;

b) 在涉及合并、收购或破产清算时, 如涉及到个人信息转让, 我们会在要求新的持有您个人信息的公司、组织继续受此隐私政策的约束, 否则我们将要求该公司、组织重新向您征求授权同意。

(4) 公开披露

我们仅会在以下情况下, 公开披露您的个人信息:

a) 获得您明确同意后;

b) 基于法律的披露: 在法律、法律程序、诉讼或政府主管部门强制性要求的情况下, 我们可能会公开披露您的个人信息。

28隐私政策模版 编写要求

业务功能二的个人信息收集使用规则

我们如何保护您的个人信息

(一) 我们已使用符合业界标准的安全防护措施保护您提供的个人信息，防止数据遭到未经授权访问、公开披露、使用、修改、损坏或丢失。我们会采取一切合理可行的措施，保护您的个人信息。例如，……

(二) 我们已经取得了以下认证：……

(三) 我们的数据安全能力：……

(四) 我们会采取一切合理可行的措施，确保未收集无关的个人信息。我们只会在达成本政策所述目的所需的期限内保留您的个人信息，除非需要延长保留期或受到法律的允许。

(五) 我们将定期更新并公开安全风险、个人信息安全影响评估等报告的有关内容。您可通过以下方式获得……

(六) 互联网环境并非百分之百安全，我们将尽力确保或担保您发送给我们的任何信息的安全性。如果我们的物理、技术、或管理防护设施遭到破坏，导致信息被非授权访问、公开披露、篡改、或毁坏，导致您的合法权益受损，我们将承担相应的法律责任。

(七) 在不幸发生个人信息安全事件后，我们将按照法律法规的要求，及时向您告知：安全事件的基本情况、可能的影响、我们已采取或将要采取的处置措施、您可自主防范和降低风险的建议、对您的补救措施等。我们将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您，难以逐一告知个人信息主体时，我们会采取合理、有效的方式发布公告。同时，我们还将按照监管部门要求，主动上报个人信息安全事件的处置情况。

1、详细说明个人信息控制者对个人信息进行安全保护的措施。包括但不限于个人信息完整性保护措施，个人信息传输、存储和备份过程的加密措施，个人信息访问、使用的授权和审计机制，个人信息的保留和删除机制等。

2、目前遵循的个人信息安全协议和取得的认证。包含个人信息控制者目前

主动遵循的国际或国内的个人信息安全法律、法规、标准、协议等，以及个人信息控制者目前已取得的个人信息安全相关的权威独立机构认证。

3、应描述提供个人信息后可能存在的安全风险。

4、应表明在发生个人信息安全事件后，个人信息控制者将承担法律责任。

5、应表明在发生个人信息安全事件后，将及时告知个人信息主体。您的权利按照中国相关的法律、法规、标准，以及其他国家、地区的通行做法，我们保障您对自己的个人信息行使以下权利：

（一）访问您的个人信息

您有权访问您的个人信息，法律法规规定的例外情况除外。如果您想行使数据访问权，可以通过以下方式自行访问：……如果您无法通过上述链接访问这些个人信息，您可随时使用我们的Web 表单联系，或发送电子邮件至……我们将在30天内回复您的访问请求。对于您在使用我们的产品或服务过程中产生的其他个人信息，只要我們不需要过多投入，我们会向您提供。如果您想行使数据访问权，请发送电子邮件至……

（二）更正您的个人信息

当您发现我们处理的关于您的个人信息有错误时，您有权要求我们作出更正。您可以通过“（一）访问您的个人信息”中罗列的方式提出更正申请。如果您无法通过上述链接更正这些个人信息，您可以随时使用我们的Web 表单联系或发送电子邮件至……我们将在30天内回复您的更正请求。

（三）删除您的个人信息

在以下情形中，您可以向我们提出删除个人信息的请求：

- 1、如果我们处理个人信息的行为违反法律法规；
- 2、如果我们收集、使用您的个人信息，却未征得您的同意；
- 3、如果我们处理个人信息的行为违反了与您的约定；
- 4、如果您不再使用我们的产品或服务，或您注销了账号；

5、如果我们不再为您提供产品或服务。若我们决定响应您的删除请求，我们还将同时通知从我们获得您的个人信息的实体，要求其及时删除，除非法律法规另有规定，或这些实体获得您的独立授权。当您从我们的服务中删除信息后，我们可能不会立即在备份系统中删除相应的信息，但会在备份更新时删除这些信息。

（四）改变您授权同意的范围

每个业务功能需要一些基本的个人信息才能得以完成。对于额外收集的个人信息的使用，您可以随时给予或收回您的授权同意。您可以通过以下方式自行操作：

当您收回同意后，我们将不再处理相应的个人信息。但您收回同意的决定，不会影响此前基于您的授权而开展的个人信息处理。如果您不想接受我们给您发送的商业广告，您随时可通过以下方式取消：……

（五）个人信息主体注销账户

您随时可注销此前注册的账户，您可以通过以下方式自行操作：……在注销账户之后，我们将停止为您提供产品或服务，并依据您的要求，删除您的个人信息，法律法规另有规定的除外。

（六）个人信息主体获取个人信息副本

您有权获取您的个人信息副本，您可以通过以下方式自行操作：……

在技术可行的前提下，例如数据接口匹配，我们还可按您的要求，直接将您的个人信息副本传输给您指定的第三方。

（七）约束信息系统自动决策

在某些业务功能中，我们可能仅依据信息系统、算法等在内的非人工自动决策机制做出决定。如果这些决定显著影响您的合法权益，您有权要求我们作出解释，我们也将提供适当的救济方式。

（八）响应您的上述请求

为保障安全，您可能需要提供书面请求，或以其他方式证明您的身份。我们可能会先要求您验证自己的身份，然后再处理您的请求。我们将在三十天内作出答复。如您不满意，还可以通过以下途径投诉：……

1、说明个人信息主体对其个人信息拥有何种权利，内容包括但不限于：信息收集、使用和公开披露时允许个人信息主体选择的个人信息范围，个人信息主体所具备的访问、更正、删除、获取等控制权限，个人信息主体隐私偏好设置，个人信息主体可以选择的通信和广告偏好，个人信息主体不再使用服务后撤回同意和注销账号的渠道、个人信息主体进行维权的有效渠道等。

2、对于需要自行配置或操作（如对所使用的软件、浏览器、移动终端等进行配置和操作）以达到访问、更正、删除、撤回同意等目的，个人信息控制者应对配置和操作的过程进行详细说明，说明方式易于个人信息主体理解，必要时提供技术支持的渠道（客服电话、在线客服等）。

3、如果个人信息主体行使权利的过程产生费用，需明确说明收费的原因和依据。

4、如果个人信息主体提出行使权利的需求后需要较长时间才能响应，需明确说明响应的时间节点，以及无法短时间内响应的原因。

5、如果个人信息主体行使权利的过程需要再次验证身份，需明确说明验证身份的原因，并采取适当的控制措施，避免验证身份过程中造成的个人信息泄露。

6、如果个人信息控制者拒绝个人信息主体对个人信息进行访问、更正、删除、撤回同意等的要求，需明确说明拒绝的原因和依据。

隐私政策模版 编写要求

对于您合理的请求，我们原则上不收取费用，但对多次重复、超出合理限度的请求，我们将视情收取一定成本费用。对于那些无端重复、需要过多技术手段（例如，需要开发新系统或从根本上改变现行惯例）、给他人合法权益带来风险或者非常不切实际（例如，涉及备份磁带上存放的信息）的请求，我们可能会予以拒绝。

在以下情形中，我们将无法响应您的请求：

- 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同意的；
- 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。隐私政策模版 编写要求

我们如何处理儿童的个人信息

我们的产品、网站和服务主要面向成人。如果没有父母或监护人的同意，儿童不应创建自己的个人信息主体账户。对于经父母同意而收集儿童个人信息的情况，我们只会在受到法律允许、父母或监护人明确同意或者保护儿童所必要的情况下使用或公开披露

此信息。尽管当地法律和习俗对儿童的定义不同，但我们将不满 14 周岁的任何人均视为儿童。如果我们发现自己在未事先获得可证实的父母同意的情况下收集了儿童的个人信息，则会设法尽快删除相关数据。如果产品或服务主要面向儿童，如有必要，隐私政策可以单独成章，或者单独成文，并突出征得监护人同意或监护人权利的条款。

您的个人信息如何在全球范围转移

原则上，我们在中华人民共和国境内收集和产生的个人信息，将存储在中华人民共和国境内。由于我们通过遍布全球的资源和服务提供产品或服务，这意

意味着，在获得您的授权同意后，您的个人信息可能会被转移到您使用产品或服务所在国家/地区的境外管辖区，或者受到来自这些管辖区的访问。此类管辖区可能设有不同的数据保护法，甚至未设立相关法律。在此类情况下，我们会确保您的个人信息得到在中华人民共和国境内足够同等的保护。例如，我们会请求您对跨境转移个人信息的同意，或者在跨境数据转移之前实施数据去标识化等安全举措。如果因业务需求、政府和司法监管要求存在跨境信息传输情况，需详细说明需要进行跨境传输的数据类型，以及跨境传输遵守的标准、协议和法律机制（合同等）。

本政策如何更新

我们的隐私政策可能变更。未经您明确同意，我们不会削减您按照本隐私政策所应享有的权利。我们会在本页面上发布对本政策所做的任何变更。对于重大变更，我们还会提供更为显著的通知（包括对于某些服务，

我们会通过电子邮件发送通知，说明隐私政策的具体变更内容）。本政策所指的重大变更包括但不限于：

1、我们的服务模式发生重大变化。如处理个人信息的目的、处理的个人信息类型、个人信息的使用方式等；

2、我们在所有权结构、组织架构等方面发生重大变化。如业务调整、破产并购等引起的所有者变更等；

3、个人信息共享、转让或公开披露的主要对象发生变化；

4、您参与个人信息处理方面的权利及其行使方式发生重大变化；

5、我们负责处理个人信息安全的责任部门、联络方式及投诉渠道发生变化时；

6、个人信息安全影响评估报告表明存在高风险时。我们还会将本政策的旧版本存档，供您查阅。个人信息控制者在隐私政策发生重大变化时，需及时更新隐私政策，并说明使用何种方式及时通知个人信息主体。通常情况下采取的通知方式如：个人信息主体登录信息系统时、更新信息系统版本并在个人信息主体使

用时弹出窗口、个人信息主体使用信息系统时直接向个人信息主体推送通知、向个人信息主体发送邮件、短信等。

如何联系我们如果您对本隐私政策有任何疑问、意见或建议，通过以下方式与我们联系：……我们设立了个人信息保护专职部门（或个人信息保护专员），您可以通过以下方式与其联系：……

一般情况下，我们将在三十天内回复。如果您对我们的回复不满意，特别是我们的个人信息处理行为损害了您的合法权益，您还可以通过以下外部途径寻求解决方案：……

1、个人信息控制者需要明确给出处理个人信息安全问题相关反馈、投诉的渠道，如个人信息安全责任部门的联系方式、地址、电子邮箱、个人信息主体反馈问题的表单等，并明确个人信息主体可以收到回应的时间。

2、个人信息控制者需给出外部争议解决机构及其联络方式，以应对与个人信息主体出现无法协商解决的争议和纠纷。外部争议解决机构通常为：个人信息控制者所在管辖区的法院、认证个人信息控制者隐私政策的独立机构、行业自律协会或政府相关管理机构等。

(三十) 个人信息安全影响评估指南

前 言

本标准依据 GB/T 1.1-2009 给出的规则起草。

本标准由全国信息安全标准化技术委员会 (SAC/TC 260) 提出并归口。

本标准的附录 A 是资料性附录。

本标准起草单位：

本标准主要起草人：

引 言

本标准是《个人信息安全规范》的配套标准，将借鉴美、欧等国家和地区在个人信息安全影响评估（国际上习惯称为隐私影响评估（PIA））方面最新的法律规定、制度设计、实践做法，以国内现有立法、行政法规、标准要求为出发点，提出科学有效符合、信息化发展需要、具有明确实施指导意义的个人信息安全影响评估指南。指南将针对机构、企业提出个人信息安全影响评估的基本框架、方法和流程，供其自评估使用，同时为国家主管部门、第三方测评机构等开展个人信息安全监管、检查、评估等工作提供的指导和依据。

1. 范围

本标准规定了个人信息安全影响评估的基本概念、框架、方法和流程。

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。同时为国家主管部门、第三方测评机构等开展个人信息安全监管、检查、评估等工作提供的指导和依据。

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 35273-2017 信息安全技术 个人信息安全规范

3. 术语

GB/T 25069-2010、GB/T 35273-2017 确立的以及下列术语适用于本标准。

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是个人信息控制者实施风险管理的重要组成部分，旨在发现、处置和持续监控个人信息处理过程中的安全风险。一般情况下，个人信息控制者必须在收集和处理个人信息前开展个人信息安全影响评估，明确个人信息保护边界，根据评估结果实施适当的安全控制措施，降低收集和处理个人信息的过程对个人信息主体权益造成的影响；另外，个人信息控制者还需按照要求定

期开展个人信息安全影响评估，根据业务现状、威胁环境、法律法规、标准要求等情况持续修正个人信息保护边界，调整安全控制措施，使个人信息处理过程处于风险可控的状态。

4.2 评估价值

通常情况下，实施个人信息安全影响评估可以达到以下目的。

- a) 识别对个人权益造成的影响，安全风险和相关的责任。
- b) 为产品和业务设计阶段的个人信息保护理念落地提供支撑。
- c) 评审新上线信息系统在处理个人信息时的安全风险。
- d) 向个人信息主体提供加强个人信息安全的建议。
- e) 维护和更新信息系统新增功能可能对所处理个人信息安全的影响。
- f) 向相关方共享安全风险并采取风险处置措施。
- g) 向合规部门反馈证据。

个人信息安全影响评估通常被视为一种预警机制，它为组织提供一种安全风险发现方法，用于发现个人信息的处理过程中存在的安全风险，继而帮助组织在项目实际处理之前实施预防措施和专项保护措施，如果安全风险的影响非常严重且无法预防或保护，整个项目都可能被撤销。因此，个人信息安全影响评估有助于在早期识别个人信息安全问题，通过尽早考虑个人信息安全问题降低时间管理成本、法律费用以及潜在的媒体或公众担忧。

个人信息安全影响评估不仅是简单的合规性检查，还可以帮助组织在持续合规性审计或调查中证明其遵守了相关个人信息与数据保护法律、法规和标准要求。如果发生个人信息安全风险或违规事件，个人信息安全影响评估报告可提供证据证明组织已经采取适当措施试图阻止上述情况发生，这可以有助于减轻、甚至免除相关责任和名誉损失。此外，恰当的个人信息安全影响评估还可以向组织的用户或民众证明，该组织尊重他们的隐私并会回应他们所担忧的个人信息安全问题，用户或民众更倾向于信任执行个人信息安全影响评估的组织。

信任建立在透明的基础上，而个人信息安全影响评估是一项提倡开放式交流、共同认知及透明度的纪律性活动。执行个人信息安全影响评估流程的组织可以向其员工和承包商证明，组织将严肃对待个人信息保护问题，也期望他们能够采取相同的处理方式。此外，通过个人信息安全影响评估，组织还可以对员工进行个人信息保护教育，使之警惕可能导致组织受损的个人信息安全问题。此外，个人信息安全影响评估还是肯定组织本身价值的一种方式，可看作是尽职调查的一种形式，从而减少客户审计次数。

4.3 评估报告的使用对象

个人信息安全影响评估报告应能支持以下功能：

a) 提供清单，确保特定的相关方始终了解已识别的受影响部门、受影响环境及受影响部门的周期性个人信息安全风险（包括固有风险和已经得到减缓的风险）。

b) 作为一种持续性工作追踪机制，用于追踪改善和/或解决已识别为存在个人信息安全风险的行动/任务。同时，需要对评估报告信息的分发或发布的敏感性进行明确评估和分类（私有、机密、公开等）。

基于这些功能，个人信息安全影响评估报告可以给个人信息主体、个人信息控制者、监管机构、组织的合作伙伴或服务商带来以下帮助：

对于个人信息主体，个人信息安全影响评估是一种工具，可确保个人信息主体的个人信息得到有效保护。

对于个人信息控制者，评估报告的使用场景可能包括以下方面：

a) 个人信息安全影响评估是一种工具，用于管理个人信息安全风险、提升意识、建立责任制度；确保组织内部处理个人信息的风险可视性、管理潜在风险与影响；

b) 在项目初始阶段执行个人信息安全影响评估流程，有助于更加透彻地理解个人信息保护要求，确保在职能与非职能要求中加入个人信息保护要求（可实现、可行、可追踪），进而为产品或服务设计与交付提供风险维度的决策依据；

c) 在产品或服务交付后，产品功能、互联网安全环境、法律法规变更时，对个人信息安全影响评估结果进行审核和修订，有助于组织及时跟踪产品或服务的安全风险，及时防范或弥补，避免对组织或用户带来更大的损失。

对于监管机构，个人信息安全影响评估报告可提供证据，证明某组织遵守适用法律、法规和标准要求。此外，如发生个人信息方面的违规、投诉等情况，个人信息安全影响评估可提供组织已进行尽职调查的相关证据。

对于组织的合作伙伴或服务商，个人信息安全影响评估是一种工具，用于评估个人信息处理者正在处理个人信息的方式是否会对个人信息安全带来不良影响，同时也可以作为合同义务的履行证据。

4.4 评估责任主体

通常，应由组织内部的安全职能部门对程序或信息系统执行个人信息安全影响评估流程，或者由客户组织或非政府组织对流程、信息系统或程序进行个人信息安全影响评估。

一般情况下，确保执行个人信息安全影响评估流程的责任首先应由负责保护个人信息的人员承担，或者由研发可能对隐私造成影响的新技术、服务或其他提案的项目经理承担。

应由最高级别的个人信息安全影响评估管理员负责确保评估流程的执行及结果的质量。经指派负责进行个人信息安全影响评估的人员可选择自行执行评估流程，或请求其他内部和/或外部相关方提供帮助，或将个人信息安全影响评估流程外包给独立第三方，上述方法都有各自的优缺点，可适当搭配使用。

当由组织自行进行个人信息安全影响评估时，监管机构和客户可以要求独立审计机构来核证评估活动的合理性。

组织应确保其已经明确个人信息安全风险管理的责任，包括个人信息安全风险流程的执行与维护，以及确保所有控制措施的适当性与有效性等。组织应指定人员负责个人信息安全风险框架的制定、执行与维护，安全控制措施的维护，以及相关个人信息安全影响和风险相关的报告。

4.5 评估规模

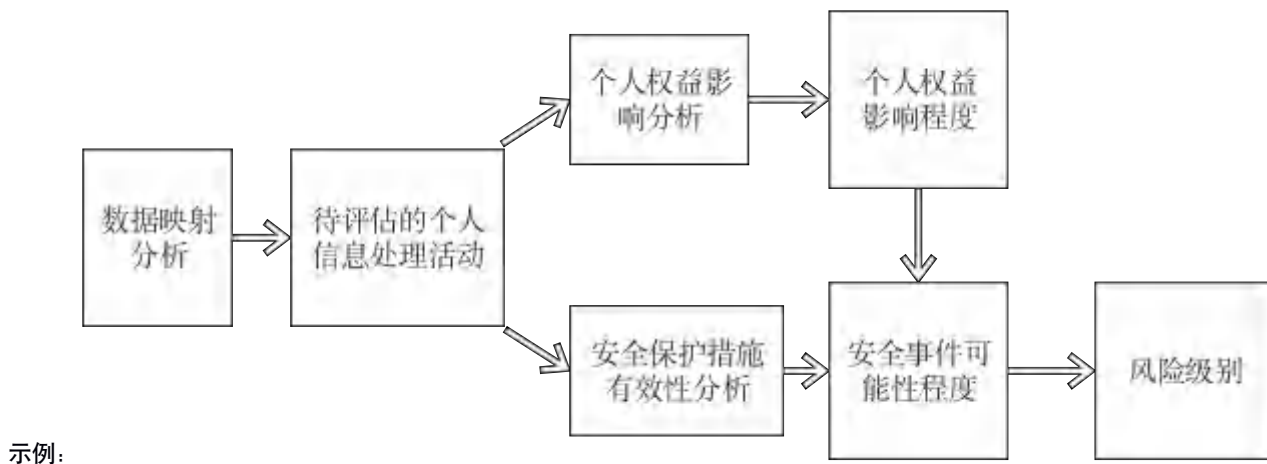
个人信息安全影响评估的规模往往取决于受到影响的个人信息主体范围和程度。如果影响的对象仅为组织内部员工时，可以仅针对员工的典型代表开展小规模的评价；如果政府部门希望为公民福利建议一个新的标识符管理系统，则需要实施一个更大范围的个人信息安全影响评估活动，同时涵盖外部的相关方。

通常，组织还会对其业务处理的个人信息实施自评估，以满足法律法规的需要，其中，个人信息的总量、类别、敏感程度、涉及个人信息主体的数量，能访问个人信息的人员等都会成为影响实际评估规模的重要因素。

中小企业实施个人信息安全影响评估时，应把握适当的评估规模，评估宜由相应的安全管理岗位人员完成，而非聘用专职从事个人信息安全影响评估的人员，选取外部专家进行评估也是一种可行路径。

4.6 评估原理

个人信息安全影响评估的基本原理如下图。



示例：图 1 评估原理示意图

评估前，对个人信息控制者的个人信息处理过程进行全面的调研，形成清晰的数据清单及数据映射图表。同时结合个人信息处理的具体场景，初步判定所处理的个人信息哪些属于个人敏感信息，梳理出待评估的个人信息处理活动。

评估过程中，首先，分析个人信息处理活动对个人权益造成的影响，并判定

相应的影响程度；其次，对个人信息处理活动涉及的特点、安全措施、相关方、规模等进行分析，判定相应影响相关安全事件发生的可能性。最后，综合分析影响程度和可能性两个要素，得出风险等级，并给出相应的改进建议，最终形成评估报告。

4.7 实施流程

介绍个人信息安全影响评估的基本实施流程包括：评估准备阶段、必要性分析阶段、数据映射分析阶段、个人权益影响分析阶段、安全事件可能性分析阶段、风险分析阶段、评估报告阶段、风险处置和持续改进阶段、评估报告发布阶段。

4.8 评估活动

在评估过程中，所采用的基本评估方法，包括但不限于以下三种：

访谈：指评估人员对信息系统相关人员进行谈话，以促进对信息系统中个人信息保护措施设计和实施情况的了解、分析或取证。访谈的对象为个人或团体，如产品经理、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、人力资源人员和用户等。

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。

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。测试的对象为机制和活动，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。

4.9 评估工作形式

个人信息安全影响评估分为自评估和检查评估两种形式，个人信息安全影响评估应以自评估为主，自评估和检查评估相互结合，相互补充。

自评估是指个人信息控制者自行发起对其个人信息处理行为的评估，自评估可以由本机构组织专门负责评估、审计的部门和角色开展，也可以委托外部专业机构开展评估工作。

检查评估是指个人信息控制者的上级机构组织或由国家职能部门依法开展的个人信息安全影响评估工作。检查评估也可以委托外部评估技术服务支持，应要求外部机构的评估结果对检查机构负责。

6 评估流程

6.1 必要性分析

组织应在新的产品或服务的开发、启动、发布等环节分析针对其开展新的个人信息安全影响评估工作的必要性，如有必要，则需要确定评估责任人员，界定评估范围、边界和评估的适用性，评估所依赖的技术文档，评估工具与计划流程，评估需调研人员，评估报告的种类与发布形式等。必要时，可以专门编制必要性分析报告，以推动组织内部按计划开展个人信息安全影响评估工作。

通常情况下，出现本标准第 6 章的情形时可开展新的或更新个人信息安全影响评估程序。

6.2 评估准备工作

准备阶段的工作主要包括：组建评估团队、制定评估计划、确定评估对象和范围、相关方咨询等。

注：6.2.1 组建评估团队

组织应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，组织还应指定人员负责签署评估报告。

评估人应定义风险准则，确保高级管理层认可该用于评价风险严重程度的风险标准。该标准可能以现有标准要求所示内容为基础，或者由组织单独制定（以及评估影响程度及各等级风险的标准）。此外，评估人还应确认风险接受标准并确保管理层认可该标准。

风险准则应反映组织的价值、目标与资源。在制定风险准则时，评估人应考虑以下因素：

- a) 影响个人信息保护的法律与监管因素；
- b) 外部因素，如行业准则、职业标准、公司政策与客户协议；
- c) 由具体应用预先决定的因素、或者在特定用例情境下预先决定的因素；
- d) 会影响信息系统设计及相关个人信息保护要求的其他因素。

组织管理层应分别从个人信息主体的视角和组织的视角出发审视个人信息安全风险。为制定用于评价个人信息安全风险重要程度的规则，评估人应回答以下问题：

a) 用于评估对个人信息主体与组织的影响程度的标准是什么？（例如，识别水平、泄露的个人信息敏感程度、受影响的个人信息主体的数量、组织影响程度）。

b) 用于评估可能性的标准是什么？（例如，支持资产的漏洞、风险源利用漏洞的能力。）

c) 用于评估影响程度的标尺？

d) 用于评估可能性的标尺？

e) 用于评价风险的各种组合（影响程度与可能性）的重要程度？尤其重要的是，风险接受标准是什么？

f) 适用于应对各种情况的策略是什么？尤其重要的是，用于确认风险是可接受的策略是什么？

g) 处理个人信息优势将对策略产生怎样的影响？

注：上述准则应与组织内部使用的其他风险标准保持一致，同时，每次使用准则时应考虑是否有改进机会。

应综合以上考虑和问题，基于以下内容定义风险准则：

a) 对产品、服务或系统使用者的伤害。此类伤害包括身体、经济、名誉损失，家庭生活被打扰或陷入尴尬境地。此外，当考虑个人信息安全风险对个人的影响时，组织应考虑不同类型的个人信息，例如人身信息、位置与空间信息、行为信息、通信内容、数据与图像信息、思想感情信息、以及交际信息；

b) 法律与监管要求，以及合同义务；

c) 相关方的期望与看法，对商誉及名誉的负面影响；

d) 个人信息可用性、机密性及完整性在运营方面的重要性；

e) 信息处理的战略价值，如信息处理产生现有价值和未来的机遇。

应清楚规定是否会进行公众咨询、个人信息安全影响评估报告将提交给谁、个人信息安全影响评估的名义预算及时间段、是否会公布评估报告或摘要。个人信息安全影响评估的最低要求应取决于法律或监管限制、或者组织认定的个人信息安全风险重要程度。

如有必要评估人应申请团队支持，例如由 ICT 部门、相关业务单位、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大力支持，管理层应确保为个人信息安全影响评估团队配置必要资源。

注：6.2.2 制定评估计划

评估计划应考虑待进行的评估活动的范围、如有必要应允许迭代进行，包括个人信息安全影响评估报告的迭代。当评估涉及大量资源时这一做法尤为有效，但针对复杂程度较低的小型提案时，非必要流程。此外，计划还应考虑到待评估提案中断的情况。

计划应清楚规定完成个人信息安全影响评估报告须进行的工作、相关工作具体由评估团队中的哪些成员负责、评估计划表、以及如果进行咨询、咨询的进行方式。计划应说明在某些具体情况下为什么咨询相关方是非常重要的、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）。

评估人完成评估计划的编制后，应评估执行成本、向组织的高级管理层申请

基本预算及人力资源。根据具体计划，可能会上调高级管理层最初设定的名义预算，或者，负责进行个人信息安全影响评估报告的人员可能需要根据可用预算修订评估计划。

组织应为个人信息安全影响评估报告配置合适资源。具体操作时应考虑以下方面：

- 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：6.2.3 确定评估对象和范围

应从以下三个方面描述评估的对象和范围。

- a) 描述系统需求信息，包括但不限于：
 - 1) 处理个人信息的类型目的；
 - 2) 对当前或未来将获得信息系统支持的业务流程的描述；
 - 3) 针对信息系统定义的职能要求清单及其义务或执行水平；
 - 4) 信息安全目标；

5) 关于数据收集方式、收集对的数据的说明。说明中应阐明谁将有权访问个人信息，包括个人信息主体访问权限的相关参数；

6) 如果预定与第三方共享信息系统或其中的个人信息，则应就信息系统或个人信息的共享人、以及共享目的提供详细信息及相关建议；

- 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) 按部分和接口划分的数据流示意图;
 - 5) 个人信息周期的数据流示意图, 例如个人信息的生成、应用、转移和处理;
 - 6) 描述在什么时间通知个人信息主体、以及什么时间取得个人信息主体同意的 workflows;
 - 7) 定义已连接个人信息主体及已转移数据字段的接口清单;
 - 8) 关于端口、协议、APIs、及加密的详细信息。
- 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在现场运行、外部托管、抑或云外包, 以及具体位置;
 - 3) 支持概念, 非常重要的一点是列示参与信息系统支持的第三方名称、他们拥有的个人信息访问权限的大小、以及从哪些位置可以访问个人信息;
 - 4) 记录概念及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媒介的处置。

描述上述内容的方式可以有以下几种: 可用于为评估执行人员提供必要的背景信息、可归入评估报告中、或者在咨询相关方时可用作简报。项目说明中应提供一些背景信息 (例如执行项目的原因、目标市场的构成、所描述的技术、服务、系统或其他提案影响隐私的具体方式、将处理的个人信息以及用于处理个人信息的平台)。项目说明中应指明项目的负责人及重要的里程碑事件, 尤其应说明在什么时候制定可影响项目设计方案的决策。

注: 62.4 相关方咨询

相关方包括但不限于：

- 1) 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；
- 2) 个人信息主体；
- 3) 消费者代表；
- 4) 分包商；
- 5) 业务合作伙伴；
- 6) 系统开发人员；
- 7) 系统运维人员；
- 8) 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、实现评估解决安全风险的目标，评估执行负责人应详细确认与进入评估程序的流程、或者正在处理中的个人信息的保护具有利益关系、或受上述两者影响的内部或外部相关方。相关方可以是拥有或可能获取个人信息访问权限的所有个人信息主体。

评估人应确认相关方的各个种类、然后具体确认各类相关方中的具体个人，个人应尽可能具有代表性。个人信息的范围与规模，对于确定恰当的相关方非常重要。如果正在执行的是大型政府项目，可能存在许多相关方。在这种情况下，社会利益群体，例如消费者代表可能被确认为相关方，另外还需确认处理个人信息、以及为个人信息主体的相关方。相反，一些小型的商业流程，可能不需要确认这样宽泛的相关方清单。

制定咨询计划应明确不同的相关方所受影响、后果（如果已知）、以及所采取的管理措施等相关问题。计划中还应包含咨询规模及计划表，内容包括但不限于：

- a) 与相关方合作识别并评估个人信息安全影响；
- b) 就评估报告草案咨询相关方意见以确认报告草案是否充分反映他们对有

关问题的关注。

c) 将咨询的相关方的数量与范围，个人信息安全影响程度、安全事件的可能性、以及可能受到影响的个人信息主体数量进行假设。

例如，如果风险的波及范围仅限于某一个组织的员工，则咨询范围仅限于该组织员工和/或其代表。然而，如果预期风险将影响到国家内的每一个人，组织应广泛咨询外部相关方的意见。如果，最初组织认为仅有少量相关方可能受到影响，但后续认识到受影响人员的数量可能要大得多且风险也要大得多，则组织应根据情况修订其咨询计划并尽力咨询大量相关方的意见。

相关方的反馈意见所确认的问题可能与风险感知有关、而非实际风险，但不应忽略这些意见、而是应该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。

对于许多独立、但却非常相似的项目而言，如果能够重复使用咨询结果，咨询相关方意见所造成的潜在重要影响可能降至最低。如果预计许多项目面临类似的个人信息保护问题，重复使用适用咨询结果可以为咨询设计提供有用信息。咨询范围不应过于宽泛，在合理判断下可实现对咨询结果的重复利用。对于新项目中的新问题，以递增方式进行咨询，有助于规避不当影响。

可根据领域专项准则，按市场领域调整相关方。在同一市场领域中的组织，可使用领域特有的准则作为基准来评估和应对隐私与安全风险。此类准则应与本文件原则保持一致，应基于特定市场领域的常见业务流程与服务明确风险和控制措施。

对于中小企业而言，咨询相关方的意见所带来的利益、可能与所消耗的时间和成本不成比例。对此类企业而言，当他们能够参考相应准则时，领域专项准则的理念可以改善个人信息安全影响评估的全面性及品质。

6.3 数据映射分析

组织应针对个人信息控制者的个人信息处理过程进行全面的调研，形成清晰的数据清单及数据映射图表（可参考附录 B 表 B-1 和表 B-2）。数据映射分析阶

段需结合个人信息处理的具体场景，初步判定所处理的个人信息哪些属于个人敏感信息。

调研内容包括个人信息收集、存储、使用、对外提供、废弃环节涉及的目的和具体实现方式，以及个人信息处理过程涉及的资源和相关方（如策略和规程、合同和协议、内部信息系统、个人信息处理者、第三方、交易平台经营者、外部服务供应商、云服务商等）（可参考附录 B 表 B-3），调研过程中应考虑已下线系统、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，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。一般情况下个人敏感信息处理活动和普通个人信息处理活动不归于同一类。

6.4 个人权益影响分析

个人权益影响分析一般指根据不同的个人信息处理活动，分析其是否存在对个人信息主体权益产生影响。个人权益影响概括可分为“影响个人自主决定权”、“引发差别性待遇”、“个人名誉受损或遭受精神压力”、“个人财产受损”四个维度：

a) 影响个人自主决定权。如，被强迫执行不愿执行的操作、缺乏相关知识或缺少相关渠道更正个人信息、无法选择推送广告的种类、被蓄意推送影响个人价值观判断的资讯、个人人身自由受限、可能引发人身伤害等；

b) 引发差别性待遇。如，因疾病、婚史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。如，被他人冒用身份、公开不愿为人知的事实（生活习惯、以往经历等），被频繁骚扰、监视追踪等；

d) 个人财产受损。如，账户被盗、遭受诈骗、勒索等。

组织应根据本标准 5.3 所述过程识别的数据映射分析结果及梳理得到的个人信息处理活动，通过查阅支撑性文档、检查个人信息处理过程、测试相应的处理

机制等方法，分析个人信息在数据流程以及个人信息处理活动全生命周期的范围内，评价组织的个人信息保护策略的执行情况、相关法律法规与政策标准的符合性情况，并审视是否存在侵害个人信息主体权益的风险。

注：支撑性文档包括（但不限于）各类需求和设计文档、管理制度和记录、数据库表单结构说明、个人信息保护协议等。

个人权益影响分析过程一般包含对个人信息处理过程弱点分析、问题确认，以及影响分析三个阶段。

在个人信息处理过程弱点分析阶段，组织应参照与国家有关法律法规和政策标准要求，依据数据映射分析与个人信息处理活动结果，对个人信息处理过程进行全生命周期、全流程的分析，识别个人信息处理过程中可能存在的薄弱环节。个人信息处理过程弱点分析应至少包含以下内容：

- 个人敏感信息的判定是否准确；
- 收集个人信息的目的是否正当、合法；
- 从第三方获得的数据是否得到正式的处理授权；
- 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；
- 是否定义了个人信息最小元素集，是否收集了过多的个人信息；
- 是否提供便捷有效的个体参与的机制；
- 变更目的处理对个人信息主体产生的影响；
- 接收个人信息的第三方是否会变更目的使用个人信息；
- 去标识化（匿名化、假名化等）后的个人信息是否能够被识别；
- 是否提供及时有效的安全事件通知机制和应急处置机制；

- 是否提供有效的投诉和维权渠道等。

在个人信息处理活动问题分析阶段，组织应依据个人信息处理过程弱点分析的结果，对各弱点的潜在问题进行深入挖掘分析，寻找归纳引起弱点出现的根本性问题。个人信息处理活动问题分析应该至少包含以下内容：

- 私自变更目的使用数据；
- 散播不准确的数据或不完整的误导性数据；
- 诱导或强迫个人提供过多个人信息；
- 过多地追踪或监视个人行为造成影响；
- 意料之外的数据披露对个人造成影响；
- 无根据地限制个人控制其个人信息的行为等。

在个人权益影响分析阶段，组织应结合前两阶段的弱点分析与问题归纳结果，综合组织的个人信息处理活动各环节涉及的个人信息特征、敏感程度，分析上述弱点与问题对个人权益可能造成的影响，及其严重程度。个人权益影响程度评估可参考本标准附录 A.1。

实施个人权益影响分析时可参考附录 B 表 B-4。

6.5 安全事件可能性分析

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，也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。为简化安全事件可能性的分析过程，将与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。如，所处网络环境、与其他系统的交互方式、采取的加密、授权、访问控制、审计、备份等技术措施；

b) 处理流程规范性。如，个人信息收集的规范性、个人信息保存的周期、个人信息使用的限制、个人信息对外提供的授权、个人信息保护机构设置合理性、收到的个人信息处理相关的投诉等；

c) 参与人员与第三方。如，人员资格审核情况及具备的技能、涉及处理个人信息人员的安全意识、人员职责有效履行的情况、第三方处理个人信息过程的可控性等；

d) 安全态势及处理规模。如，近期内遭受网络攻击或发生安全事件的情况、近期内收到过的安全相关的警示信息、当前或预计处理个人信息的规模、频率等。

组织应该对以上维度的相应内容进行充分了解，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 5.4 中对个人权益影响分析的不同维度，从以上四方面导致安全事件发生的可能性进行综合评价，得到安全事件发生的可能性。安全事件可能性等级评估可参考本标准附录 A.2。

实施安全事件可能性分析时可参考附录 B 表 B-5。

6.6 风险分析

示例：进行风险分析时，首先，应根据个人信息处理活动的目的、状态、相关个人信息的敏感程度，同时考虑个人信息主体数量、群体特征等要求，评价对个人权益影响的程度等级；其次，应根据个人信息处理活动涉及的特点、已实施的安全措施、相关方、处理规模等要素，同时考虑具备的事件处置经验、用户习惯、及预防性措施等，评价安全事件发生的可能性等级。最后，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。其中，风险分析的具体过程和风险等级的判定可参考附录 A.3。

风险分析的实施过程可参考附录 B 表 B-6。

6.7 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（应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。

6.8 风险处置和持续改进

根据评估结果，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，严重风险应立即处置，高风险应限期内处置，中风险应在权衡影响和成本后处置，低风险可选择接受。

个人信息控制者应持续跟踪风险处置的落实情况，评估剩余风险，将风险控制可在接受的范围内。此外，应将评估结果用于下一次个人信息安全影响评估工作。

6.9 评估报告发布

公开发布个人信息安全影响评估报告是促进自合规、配合监管、增加客户信任的重要方式，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，但其内容通常应不少于以下方面：收集和处理个人信息的必要性和给个人带来的益处、收集和处理的个人信息类型（个人敏感信息需单独强调）、个人信息处理的例外情况（法律法规规定）、合规性分析的概况、评估过程和结果概况、已实施和将要实施的风险处置措施概况、对个人信息主体的建议、实施评估责任部门或人员的联系方式和解答疑问的渠道等。

7 评估实施

7.1 合规性差距评估

注：7.1.1 整体合规性差距评估

个人信息控制者可根据所参考的个人信息保护相关法律、法规、政策及标准，直接分析当前执行的个人信息处理活动与其条款的差距（可参考附录 B 表 B-7）。该评估方式的应用场景包括但不限于以下情形：

- a) 产品或服务年度整体评估；

- b) 新产品或新服务（不限技术平台）设计阶段评估；
- c) 新产品或服务（不限技术平台）上线初次评估；
- d) 法律法规、政策、标准、外部环境等出现重变化时重新评估；
- e) 业务模式、信息系统、运行环境等发生重大变更重新评估；
- f) 发生重大个人信息安全事件后重新评估；
- f) 发生收购、兼并、重组等情形时。

对于合规差距分析过程中发现个人信息处理活动与法律、法规、政策、标准等的条款存在合规性差距的，可根据需要按照本标准第 5 章内容，启动相应的个人信息安全影响评估工作，评估该差距对个人信息主体权益可能造成的影响和风险。

注：7.1.2 局部合规性差距评估

个人信息控制者可根据所参考的个人信息保护相关法律、法规、政策及标准，对当前执行的个人信息处理活动中的部分子活动与相对对应条款的差距进行分析（可参考附录 B 表 B-7）。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时评估；
- b) 法律、法规、政策、标准出现部分变化时评估；
- c) 业务模式、信息系统、运行环境等发生变化时评估。

对于合规差距分析过程中发现个人信息处理活动与法律、法规、政策、标准等的条款存在合规性差距的，可根据需要按照本标准第 5 章内容，启动相应的个人信息安全影响评估工作，评估该差距对个人信息主体权益可能造成的影响和风险。

7.2 典型个人信息处理活动影响评估

注：7.2.1 典型评估场景

示例：通常情况下，涉及以下针对个人信息处理活动时，应实施个人信息安全影响评估：

- a) 个人信息出境前评估；
- b) 个人信息处理目的变更前评估；
- c) 个人信息委托处理、转让、共享或公开披露前或范围发生变化时评估；
- d) 个人信息匿名化和去标识化效果评估；
- e) 其他情形，包括但不限于：
 - 1) 需要对去标识化后的数据重标识使用时；
 - 2) 通过购买、从合作伙伴获得方式收集、使用个人信息时；
 - 3) 使用“征得同意例外”条款收集、使用个人信息时；
 - 4) 使用“默许同意”方式收集个人信息时；
 - 5) 对政府、监管部门、司法部门提供个人信息前；
 - 6) 出现用户申诉且纠纷未解决时。

注：7.2.2 个人信息出境安全评估

个人信息出境场景的评估可参照 GB/T XXXX《信息安全技术 数据出境安全评估指南》中的相应内容。

注：7.2.3 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，则不会为个人权益带来额外影响，无需再次告知用户并征得其明示同意。判断时是否有直接或合理的关联应至少需要考虑如下因素：

- a) 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的理解程度；

b) 个人信息收集时的场景，包括个人信息主体和个人信息控制者之间的关系、商品或服务的范围及使用的商标和名称、个人信息主体使用商品或服务的方式、商品或服务为个人信息主体提供的便利等；

c) 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，以及为提供商品或服务，或改进或推广商品或服务，可预见到的将被使用到的个人信息的类型。

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，应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。

注：7.2.4 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：

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。

评估个人信息匿名化和去标识化效果时，应充分考虑以下要素：

a) 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；

b) 匿名化后的个人信息是否为统计型结果；

c) 去标识化后的个人信息是否能够达到满足使用目的的最小元素集；

- d) 匿名化和去标识化后的个人信息使用场景；
- e) 数据处理者的安全保障能力；
- f) 能否在公开渠道或数据交易机构获得类似的个人信息；
- g) 未经处理保留的个人信息类型和内容的特殊性。

注：7.2.5 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，应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：

- a) 个人信息的类型、数量、敏感程度等；
- b) 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，并得到个人信息主体的明示授权同意；
- c) 数据发送方的安全管理保障和安全技术保障能力；
- d) 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）；
- e) 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；
- f) 个人信息是否进行过去标识化处理；
- g) 发生个人信息安全事件后的补救措施；
- h) 数据接收方所能响应个人信息主体请求的范围，如：访问、更正、删除等。

注：7.2.6 个人信息安全事件影响评估

发生个人信息安全事件后，组织应及时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。评估影响时，应充分考虑以下因素：

- a) 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；
- b) 发生事件的信息系统状况，对其他互联系统的影响；

- c) 已采取或将要采取的处置措施及措施的有效性;
- d) 对个人信息主体权益造成的直接影响和长期影响;
- e) 向个人信息主体告知事件的方式和内容;
- f) 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。

7.3 可能产生高风险的个人信息处理活动影响评估

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，也应开展个人信息安全影响评估，可能产生高风险的场景包括但不限于：

- a) 涉及对个人信息主体评价、打分等直接画像行为，如进行负面标识、预测健康状态等;
- 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;
- 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;
- d) 收集的个人敏感信息数量、比重较多，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;
- e) 数据处理的规模较大，如涉及 50 万人以上、持续时间久、在某个特定群体的占比高、涵盖的地理区域广泛或较集中等;
- 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;
- 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、文化水平偏低人群、寻求庇护人群等;
- h) 创新型技术或解决方案的应用，如生物特征识别、IoT、人工智能等;
- i) 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。

判断个人信息处理活动是否与上述情形相关，可在进行数据映射分析、合规性差距分析等过程中进行识别，一旦涉及上述情形，可针对以上场景评估影响和风险，同时应重视个人信息主体代表等相关方的咨询工作，保障评估的准确性。

(资料性附录)
个人信息安全影响评估参考方法

A.1 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原则见下表。

示例：表 A.1 个人权益影响程度判定原则

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难度。如付出额外成本、无法使用应提供的服务、造成误解、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、产生厌烦和恼怒情绪等。	低

以定性方式为例，可从“影响个人自主决定权”、“引发差别性待遇”、“个人名誉受损和遭受精神压力”、“个人财产受损”四个维度，依据本标准表 A.1 的判定原则，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下表。

示例：表 A.2 影响程度判定表

影响类别	影响程度判定原则	影响描述	影响程度
影响个人自主决定权	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。	如个人人身自由受限、遭受人身伤害。	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，被强迫执行违反个人意愿的操作、被蓄意推送资讯影响个人价值观判断、可能引发个人人身自由受限或遭受人身伤害。	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难度。	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
	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。	低
引发差别性待遇	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，因信息泄露造成歧视性对待以致被用人单位解除劳动关系。	严重

影响类别	影响程度判定原则	影响描述	影响程度
	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, 造成对个人合法权利的歧视性待遇、造成对个人公平交易权的损害 (无法全部或部分使用应提供的产品或服务)。	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难度。	如, 造成误解、为使用应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
	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, 被打扰、产生厌烦和恼怒的情绪等。	低
个人名誉受损和遭受精神压力	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, 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
	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, 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
	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难度。	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
	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, 被频繁打扰、产生厌烦和恼怒情绪等。	低
个人财产受损	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, 遭受金融诈骗、资金被盗用、征信信息受损等。	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难度。	如, 社会信用受损, 为获取金融产品或服务需付出额外的成本等。	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, 因个人信息更正而需执行额外的流程 (或提供额外的证明性材料) 等。	低

评估过程中, 可先分析对某一个个人信息主体造成的影响程度, 再根据处理活动的特征、群体性特征等要素修正影响等级, 修正的条件可参考下表。

示例: 表 A.2 影响程度修正表

修正前影响程度	修正条件	修正后影响程度
严重	无	无
高	个人信息处理活动涉及个人敏感信息, 且涉及的个人信息主体超过 10 万人。	严重
	个人信息处理活动涉及的个人信息主体超过 500 万人。	严重
	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。	严重

修正前影响程度	修正条件	修正后影响程度
	其他不可控因素，如个人信息出境后保存地的法律、政策多变等。	严重
中	个人信息处理活动涉及个人敏感信息，且涉及的个人信息主体超过 500 万人。	严重
	个人信息处理活动涉及个人敏感信息，且涉及的个人信息主体超过 10 万人。	高
	个人信息处理活动涉及的个人信息主体超过 500 万人。	高
	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。	高
	其他不可控因素，如个人信息出境后保存地的法律、政策多变等。	高
低	个人信息处理活动涉及的个人信息主体超过 500 万人。	中
	对个人信息主体造成困扰的频率过高时。	中

以半定量或定量方式为例，可根据个人权益受损对个人信息控制者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。

A.2 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原则见下表。

示例：表 A.3 安全事件可能性等级判定原则

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”、“安全态势及处理规模”等方面，依据本标准表 A.3 的判定原则，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下表。

示例：表 A.4 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量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，或收到了大量相关的投诉，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围无任何限制，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，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，或已在合作方已经发生，或收到过权威机构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。	
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。	中
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。	
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。	
威胁引发的相关安全事件已经同领域其他组织发现，或在专业机构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的保护个人信息安全。	低
该个人信息处理行为为非常态业务行为，个人信息处理行为符合规范，几乎没有出现关于该行为的投诉。	
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机构所预测。

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，再根据个人信息控制者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，修正的条件可参考下表。

示例：表 A.4 可能性级别修正表

修正前可能性等级	修正条件	修正后可能性等级
很高	对相关的投诉有处置的经验，并得到了个人信息主体认同。	高/中
	针对安全事件的特征提前实施了有效的安全措施，或根据安全预警的内容及时提升了安全防护水平。	高/中
高	对相关的投诉有处置的经验，并得到了个人信息主体认同。	中
	针对安全事件的特征提前实施了有效的安全措施，或根据安全预警的内容及时提升了安全防护水平。	中
中	已实施了处理相关投诉问题的解决方案。	低
	针对安全事件的特征提前实施了有效的安全措施。	低
低	无	无

A.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，可参考下表。

示例：表 A.5 风险等级判定表

示例：风险等级		示例：可能性级别			
		示例：低	示例：中	示例：高	示例：很高
示例：响应级	示例：严重	示例：中	示例：高	示例：严重	示例：严重

别	示例：高	示例：中	示例：中	示例：高	示例：严重
	示例：中	示例：低	示例：中	示例：中	示例：高
	示例：低	示例：低	示例：低	示例：中	示例：中

(资料性附录)

个人信息安全影响评估常用工具表

示例：表 B-1 基于系统组件的个人信息映射表

组件名	该功能是否收集、使用、存储个人信息	个人信息的类型	收集个人信息的方法	收集/使用个人信息的原因	实施的安全控制措施

示例：表 B-2 基于个人信息生命周期的个人信息映射表

序号	个人信息的类型	涉及的信息系统组件	收集			存储		使用		对外提供		废弃
			目的	方法	控制措施	存储位置	控制措施	方式	控制措施	对象	控制措施	控制措施

示例：表 B-3 个人信息保护相关方关系表

个人信息类型	个人信息主体涉及的主要群体	涉及的个人 信息控制者		涉及的个人 信息处理者		需要对外提 供的第三方		涉及的其他相关机构（交 易平台经营者、外部服务 供应商、云服务商等）		涉及的其他 情形（如跨境 传输等）
		对象	责任部 门和人 员	对象	约束和 监管机 制	对象	约束和 监管机 制	对象	约束和监管 机制	保护机制

示例：表 5-4 个人权益影响分析表

个人信息处理活动	是否涉及个人敏感信息	识别脆弱点	情况描述	发现证据	个人信息处理活动存在的问题	对个人权益产生的影响
处理活动 A	敏感/非敏感	个人敏感信息的判定是否准确				
		收集个人信息的目的是否正当、合法				
		从第三方获得的数据是否得到正式的处理授权				
		新设个人信息处理目的是否超出原有目的				
		个人信息受让方采取的个人 信息保护措施的有效性				
		公开披露个人信息对个人权 益造成的影响				
处理活动 B						

示例：表 B-5 安全事件可能性分析表

个人信息处理活动	涉及的信息系统组件	是否涉及个人敏感信息	对个人权益的影响	已实施的措施	相应证据	可能发生的安全事件	安全事件发生的可能性
处理活动 A		敏感/非敏感	影响个人自主决定权				
			引发差别性待遇				
			个人名誉受损或遭受精神压力				
			个人财产受损				
处理活动 B							

示例：表 B-6 风险分析过程表

个人信息处理活动	对个人权益的影响	影响程度	安全事件可能性	风险等级	风险处置建议	风险涉及的相关方
处理活动 A	影响个人自主决定权					
	引发差别性待遇					
	个人名誉受损或遭受精神压力					
	个人财产受损					
处理活动 B						

示例：表 B-7 合规差距分析表

条款编号	条款内容	分析内容	处理活动 A	处理活动 B	处理活动 C
1.1		个人信息处理活动描述			
		合规性差距分析			
		对个人权益产生的影响			
1.2		个人信息处理活动描述			
		合规性差距分析			
		对个人权益产生的影响			

(三十一) 信息安全技术 大数据安全管理指南

ICS 点击此处添加 ICS 号
点击此处添加中国标准文献分类号



中华人民共和国国家标准

GB/T XXXXX—XXXX

信息安全技术 大数据安全管理指南

Information Security Technology — Big Data Security Management Guide

点击此处添加与国际标准一致性程度的标识

(征求意见稿)

(本稿完成日期：2017 年 3 月 21 日)

XXXX—XX—XX 发布

XXXX—XX—XX 实施

中华人民共和国国家质量监督检验检疫总局 发布
中国国家标准化管理委员会

GB/T XXXX—XXXX

I

GB/T XXXXX—XXXX

目 次

前 言.....	III
引 言.....	IV
信息安全技术 大数据安全管理指南.....	1
1 范围.....	1
2 规范性引用文件.....	1
3 术语、定义和缩略语.....	1
3.1 术语和定义.....	1
3.2 缩略语.....	2
4 大数据安全管理原则.....	2
4.1 原则1 - 职责明确原则.....	2
4.2 原则2 - 意图合规原则.....	2
4.3 原则3 - 质量保障原则.....	2
4.4 原则4 - 数据最小化原则.....	2
4.5 原则5 - 责任不随数据转移原则.....	3
4.6 原则6 - 最小授权原则.....	3
4.7 原则7 - 数据保护原则.....	3
4.8 原则8 - 可审计原则.....	3
5 大数据安全管理基本概念.....	3
5.1 概述.....	3
5.2 大数据安全管理方法.....	3
6 制定大数据安全目标、战略和策略.....	4
7 明确大数据安全管理角色与责任.....	4
7.1 概述.....	4
7.2 数据安全管理团队的职责.....	5
7.3 职能部门的职责.....	5
7.4 明确大数据主要活动安全管理责任.....	5
8 管理大数据安全风险.....	8
8.1 概述.....	8
8.2 评估大数据风险.....	8
8.3 选择安全保护措施.....	9
8.4 制订安全计划.....	10
9 管理大数据平台运行安全.....	10
附录A 电信行业数据分类分级示例.....	12
附录B 国家基础数据.....	14
附录C 生命科学大数据风险分析示例.....	15
附录D 大数据安全风险.....	16
参考文献.....	17

GB/T XXXXX—XXXX

前 言

本标准按照 GB/T 1.1-2009 给出的规则起草。

本标准由全国信息安全标准化技术委员会（SAC/TC260）提出并归口。

本标准起草单位：四川大学、中国电子技术标准化研究院、中国移动有限公司、深圳市腾讯计算机系统有限公司、清华大学、阿里云计算有限公司、广州赛宝认证中心服务有限公司、中电长城网际系统应用有限公司、华为技术有限公司、成都超维计算中心有限公司、陕西省信息化工程研究院、银联智慧信息服务（上海）有限公司、北京华宇软件股份有限公司、中国电子科技网络信息安全有限公司等单位。

本标准主要起草人：xxx。

GB/T XXXXX—XXXX

引 言

大数据技术的发展和影响影响着国家的治理模式、企业的决策架构、商业的业务策略以及个人的生活方式。我国大数据仍处于起步发展阶段，各地发展大数据积极性高，行业应用得到快速推广，市场规模迅速扩大。在面向大量用户的应用和服务中，从数据收集的角度，数据收集者希望能获得更多的信息，以提供更加丰富、高效的个性化服务。随着大数据的应用，大量数据集中，新技术不断涌现和应用，使数据面临新的安全风险，随着大数据的应用和分析，数据价值不断提升，安全受到高度重视。

而拥有大量数据的企业的管理和技术水平参差不齐，有不少企业缺乏技术、运维等方面的专业安全人员，容易因数据平台和计算平台的脆弱性遭受网络攻击，导致数据泄露。数据信息泄露的主要途径包括：一是外部攻击者利用系统和平台的漏洞入侵获取数据；二是掌握数据的机构或其合作商内部人员主动泄露数据；三是掌握数据的机构或其合作商内部人员与外部攻击者勾结盗取数据。从数据泄露的途径来看，关键是要加强掌握数据的机构和其合作商的技术和管理能力的建设，加强数据收集、存储、使用、分发等环节的技术和管理措施，制定规范和制度。

本标准指导拥有、处理大数据的政府部门、企业、事业单位、非盈利机构等组织做好大数据的安全管理、风险评估等工作，有效、安全地应用大数据，采用有效技术和管理措施保障数据安全。

GB/T XXXXX—XXXX

信息安全技术 大数据安全管理指南

1 范围

本标准组织的的大数据安全提供指导，本标准提出大数据安全管理基本原则、大数据安全管理基本概念和大数据安全风险过程。本标准提出大数据的数据收集、数据存储、数据使用、数据分发、数据删除等主要阶段的基本概念和管理要求。本标准规范了组织内部不同大数据角色的安全职责。

本标准适用于所有的组织，包括企业、政府部门、非盈利机构等。

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 25069—2010 信息安全技术 术语
- GB/T 7072—2002 信息分类和编码的基本原则与方法
- GB/T 20529.1—2006 企业信息分类编码导则 第一部分：原则与方法
- GB/T 31167—2014 信息安全技术 云计算服务安全指南
- GB/T XXXXX—XXXX 信息安全技术 大数据服务安全能力要求
- GB/T XXXXX—XXXX 信息安全技术 个人信息安全规范

3 术语、定义和缩略语

GB/T 32400-2015中界定的以及下列术语和定义适用于本文件。

3.1 术语和定义

（引用国内在研的大数据标准，根据本标准需求添加所需术语）

3.1.1

大数据 big data

具有数量巨大、种类繁多、流动速度快、且特征多变等特性，并且难以用传统数据体系结构进行有效处理的数据集。

注：国际上，大数据的4个特征普遍不加修饰地直接用volume、variety、velocity和variability予以表述，并分别赋予了它们在大数据语境下的定义：

- a)数量 volume: 数据集的规模。
- b)多样性 variety: 数据来源、领域或类型多样。
- c)速度 velocity: 单位时间的数据流量。
- d)多变性 variability: 大数据其他特征，即数量、速度和多样性等特征都处于多变状态。

GB/T XXXXX—XXXX

3.1.2

大数据平台 big data platform

采用分布式存储和计算技术，提供大数据的访问和处理，支持大数据应用安全高效运行，包括监视大数据的存储、输入输出操作控制等大数据服务功能的软硬件集合。

3.1.3

组织 organization

由作用不同的个体为实施共同的业务目标而建立的结构。组织可以是一个企业、事业单位、政府部门等。

[GB/T 20984-2007]

3.2 缩略语

下列缩略语适用于本文件。

4 大数据安全管理原则

4.1 原则 1 - 职责明确原则

- a) 根据数据规模、数据重要性、组织规模等因素，组织可成立安全管理团队，安全管理团队为组织数据及使用安全负责。
- b) 组织应明确组织内部不同角色的数据安全管理职责。
- c) 组织应明确大数据生命周期各活动的实施主体及安全责任。

4.2 原则 2 - 意图合规原则

对数据的收集、使用需基于法律依据。组织应制定相关流程确保数据的收集和使用方式没有违反任何法律法规，包括法律法规、合同条款等。组织需要确保履行需要承担的内部的和外部的责任，包括但不限于：

- a) 确保所有数据集和数据流的安全；
- b) 正确处理个人信息、重要信息；
- c) 实施了合理的跨组织数据保留的策略和实践；
- d) 理解数据相关的法律义务，并确保组织履行了这些义务。

4.3 原则 3 - 质量保障原则

组织应：

- a) 实施适当的措施确保数据的准确性、相关性、完整性和时效性。
- b) 建立控制机制定期检查收集和存储的数据的质量。

4.4 原则 4 - 数据最小化原则

组织应采取适当的措施最小化大数据生命周期各活动涉及的数据。

4.5 原则 5 - 责任不随数据转移原则

- a) 当前控制数据的组织应对数据负责，当数据转移给其他组织时，责任不随数据转移而转移。

GB/T XXXXX—XXXX

- b) 组织在数据转移前，需对数据进行风险评估，确保数据转移后的风险可承受，方可转移数据，并对数据转移给其他组织所造成的数据安全事件承担安全责任。
- c) 组织在数据转移前，需确保通过合同或其他诸如强制的内部策略等明确界定了接收方接收的数据范围和要求，确保其提供同等或更高的数据保护水平。

4.6 原则6 - 最小授权原则

- a) 在保证组织业务功能完整实现的基础上应赋予数据活动中各角色最小的操作权限，确保非法用户或异常操作所造成的损失最小。
- b) 所有角色只能使用所授权范围内的数据，非授权范围内的数据使用必须进行授权审批。

4.7 原则7 - 数据保护原则

- a) 组织需对数据进行分类分级，对不同安全级别的数据实施恰当的安全保护措施。
- b) 组织应确保处理大数据处理平台及应用的安全控制措施和策略有效，保护数据的完整性、保密性和可用性，确保数据在整个生命周期里，免遭诸如未经授权访问、破坏、篡改、泄露或丢失等风险。
- c) 组织应解决风险评估和安全检查中所发现的风险和脆弱性，并对数据安全防护措施不当所造成的安全事件承担责任。

4.8 原则8 - 可审计原则

对数据进行修改、查询、导出、删除等操作时，组织需要记录相应的操作，记录应可追溯可审查。

5 大数据安全管理基本概念

5.1 概述

大数据面临一些新的安全风险，如数据关联分析可能暴露个人隐私，大数据的新特性使得传统的安全机制不能满足安全要求，大数据恶意使用可能会给公共利益、国家安全等带来严重损害等。

大数据安全管理用来实现和维护数据保密性、完整性、可用性、可核查性、真实性和可靠性的过程。大数据安全管理与IT安全管理相似，主要功能包括：

- a) 确定组织的数据安全目标、战略和策略；
- b) 确定组织的数据安全要求；
- c) 识别并分析对组织数据的安全威胁；
- d) 识别并分析组织数据安全风险；
- e) 规定合适的防护措施；
- f) 监督防护措施的实施与运行；
- g) 检测并及时响应数据安全事件。

5.2 大数据安全管理方法

组织应系统分析和识别大数据安全要求，并采用系统的安全技术和运行管理措施保护大数据安全。大数据安全管理应包括以下活动：

- a) 制定大数据安全策略；
- b) 明确组织中大数据安全管理的角色和责任；
- c) 风险管理；

GB/T XXXXX—XXXX

- d) 配置管理；
- e) 变更管理；
- f) 应急响应和灾难恢复；
- g) 安全意识培训；
- h) 大数据平台运行安全管理。

6 制定大数据安全目标、战略和策略

组织应明确拟使用大数据达成的目标，如利用大数据提升组织的竞争力等；应确定实现目标采用的策略；并制定计划实施的策略。

组织宜采用分层目标、战略和策略结构。总体目标指组织根据自身的业务特点建立大数据收集、使用的整体目标、战略和策略。基于总体的大数据目标、战略和策略，组织制定总体的大数据安全目标、战略和策略。各个部门应该根据自身特点，制定适用于部门具体安全需求的数据安全目标、战略和策略。如图1所示。

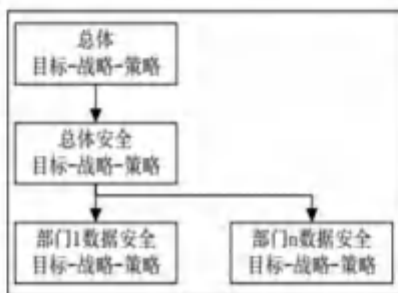


图1 目标、战略和策略层次结构

数据安全目标、战略和策略可以使用自然语言阐述，也可以使用机器语言表示，应该包括以下几个方面：

- a) 保密性；
- b) 完整性；
- c) 可用性；
- d) 可核查性；
- e) 真实性；
- f) 可靠性。

目标、战略和策略要规定组织的数据安全等级、接受风险的阈值和应急需求。

7 明确大数据安全管理角色与责任

7.1 概述

大数据安全管理角色包括组织内部的安全管理团队和职能部门。安全管理团队对组织的大数据安全全面负责。职能部门是根据业务需求对数据进行收集、分析或使用的具体部门，负责数据收集、分析或使用等的技术实现。职能部门对本部门收集或使用的数据安全负责，细化数据在收集、分析或使用等阶段的安全要求，并推动落实。

GB/T XXXX—XXXX

7.2 数据安全团队的职责

安全管理团队的具体职责有：

- 应确定各种数据的分类分级初始值，制定数据分类分级指南；
- 应综合考虑相关的法律法规、政策、标准、大数据分析技术当前水平、组织所处行业特殊性等，综合评估数据安全分析，制定数据安全基本要求；
- 建立相应的数据安全监督机制，监视数据安全机制的有效性；
- 负责组织的大数据安全过程，并对外部相关方（如：国家安全的主管部门、数据主体等）负责；
- 对于组织的数据使用，大数据安全管理团队具有相应的权力、职责和管理责任。

7.3 职能部门的职责

职能部门在履行其职能时会生成、收集不同数据，持久保存数据并进行分析，职能部门可能涉及一个或多个大数据主要阶段，根据涉及的阶段履行相应安全职责。

职能部门需要配合安全管理团队来保障数据安全，职能部门的主要职责有：

- 确定本部门数据的最终分级；
- 根据本部门涉及的大数据主要阶段，明确和细化本部门数据在收集、存储、使用等过程中的具体安全要求，并有效实施；
- 配合安全管理团队处置安全事件；
- 根据要求安全使用数据。

7.4 明确大数据主要活动实施部门安全管理责任

7.4.1 大数据主要活动基本概念

从数据进入组织的大数据平台开始，以数据被删除结束，数据主要包含数据收集、数据存储、数据使用、数据分发以及数据删除几个活动，即：

- 数据收集：该阶段使数据进入组织的大数据生态环境，比如保存在大数据平台。
- 数据存储：该阶段指将数据持续存储在存储介质上。
- 数据使用：组织通过该阶段的活动作出基于数据的决策，以便更好地履行组织的职责或实现组织的目标。使用的数据可以是组织内部持久保存的数据，也可以是以数据流方式接入分析平台的实时数据流。
- 数据分发：组织可以在满足相关规定的情况下将数据使用活动中生成的报告、分析结果等分发给其他组织，也可以将组织内部的数据适当处理后销售给其他组织。
- 数据删除：当组织决定不再使用特定数据时，组织可以删除该数据。

不同活动之间可能存在数据流，从而存在一定的安全风险，组织需要确保安全策略、规程和安全要求到位，满足大数据的安全保护要求。

7.4.1.1 收集

收集活动包括数据获取或创建过程，数据收集方式包括但不限于：

- 网络数据采集：通过网络爬虫或公开API等方式获取数据。
- 从其他组织获取数据：通过线上或线下等方式获得数据。
- 通过传感器获取：传感器包括温度传感器、电视、汽车、摄像头等公共和个人的智能设备。
- 系统数据：组织内部的系统运行过程中产生的业务数据，以及各种系统、程序和服务运行产生的大量运维和日志数据等。

GB/T XXXX—XXXX

收集活动的主要操作包括：发现数据源、收集数据、生成数据、缓存数据、创建元数据、数据转换、数据验证、数据清理、数据聚合等。

7.4.1.2 存储

数据存储指将数据持久保存在大数据平台，存储的数据包括采集的数据、分析结果数据等。存储系统可以是关系数据库、非关系数据库等，应支持对不同数据类型和数据格式的数据存储；且提供多种数据访问接口，如文件系统接口、数据库接口等，直到数据被删除之前，存储的数据均可被组织合便使用。

在某些情况下，组织将使用第三方的数据存储平台保存数据，此时组织失去对存储基础设施的部分控制权，组织应充分考虑这种方式存在的安全风险。

组织即使能对存储系统中的数据进行有效控制，但可能并不是数据的拥有者，组织不是数据控制者的原因有：知识产权、法律问题（如个人信息或健康数据处理相关法律）等。这种情况下，组织仍需承担数据的管理责任。

存储活动的主要操作包括：数据编解码、数据加解密、数据持久存储、数据备份、数据更新、数据访问等。

7.4.1.3 使用

数据使用活动包括利用数据预处理、数据分析和数据可视化等技术从原始数据中提取信息，提炼出有用知识，支撑组织根据数据作出合理的决策等操作。

数据预处理指对收集的数据进行提取、转换和去噪等处理。原始数据格式和数据类型众多，通过数据提取和转换操作，复杂的数据可以转换为简单的结构化数据，便于对数据进行分析。数据去噪过程删除噪声数据，避免对分析过程产生不利影响。数据分析指从大数据中抽取有用信息或发现有价值的模式的过程。可视化指通过使用统计图、统计表、报告等多种方式展示数据的过程。数据可视化帮助组织更好地理解数据。

使用活动的主要操作包括：数据查询、数据读取、数据索引、批处理、交互式处理、流处理、数据统计分析、数据预测分析、数据关联分析、数据可视化、生成分析报告。

7.4.1.4 分发

数据分发活动将原始数据、处理过的数据、分析的结果等不同形式的数据传递给外部实体或组织内部的其他部门。数据分发包括线上或线下等多种方式。

数据分发的原因包括但不限于：

- a) 组织内部部门间的数据交换；
- b) 需要为外部生成报告，例如政府机关；
- c) 企业与企业间的数据交换，客户需要使用报告等；
- d) 数据被出售给一个广告代理或调查公司；
- e) 数据是该组织发布的业务的一部分，例如业务数据；

数据分发涉及的主要操作包括：数据传输、数据脱敏、数据交换、数据交易、数据共享。

7.4.1.5 删除

删除活动指删除组织的大数据平台或租用的第三方大数据存储平台上的数据及其副本，如果数据来自外部实时数据流，还应断开与实时数据流的链接。

数据需要被删除的原因包括但不限于：

- a) 为了减少数据泄露的风险，避免数据被不适当的分发或使用。
- b) 删除不相关或不正确的数据，数据与最初使用目的不再相关，或数据不正确。
- c) 满足客户要求删除其数据的要求，但可能存在法律法规需要保留数据，如和健康相关的数据。

数据删除活动的主要操作包括：删除元数据、删除原始数据及其副本、断开与外部实时数据流的链接。

7.4.2 大数据主要活动职责

GB/T XXXXX—XXXX

7.4.2.1 数据收集

实施部门应：

- a) 定义采集数据目的和用途，明确数据采集源和采集数据范围。
- b) 遵循意图合规原则，确保数据收集的合法性、正当性和必要性，且只采集满足业务所需的最小数据集。
- c) 遵守质量保障原则，制定数据质量保障的策略、规程和要求。
- d) 对数据采集环境、采集设施和采集技术采取必要的安全管控措施。
- e) 遵循数据保护原则，对收集数据进行分类分级标识，并对不同类别和级别的数据实施相应的安全管理策略和保障措施。

7.4.2.2 数据存储

实施部门应：

- a) 首先对存储的数据进行分类分级，非涉密数据根据本标准的分级要求进行分级。
 - 1) 数据应先分类再分级；
 - 2) 不同类别的数据应分开存储，并采取物理或逻辑隔离机制；
 - 3) 组织根据自身需求，可对组织数据进行内部分类和分级，例如将敏感数据进一步划分为一般敏感和重要敏感数据。
- b) 遵守数据保护原则，按照标准 GB/T XXXXX-XXXX 中 6.3 的要求，主要考虑以下几个方面：
 - 1) 存储架构安全；
 - 2) 逻辑存储安全；
 - 3) 存储访问控制；
 - 4) 数据副本安全；
 - 5) 数据归档安全；
 - 6) 数据时效性管理。
- c) 建立数据存储冗余策略和管理制度，及数据备份与恢复操作过程规范。

7.4.2.3 数据使用

实施部门应：

- a) 依据国家个人信息和重要数据保护的法律法规要求建立数据使用正当性原则，明确数据使用和分析处理的目的和范围。
- b) 建立数据使用的内部责任制度，保证在数据使用声明的目的和范围内对受保护的数据进行使用和分析处理。
- c) 遵守最小授权原则，提供细粒度访问控制机制，限定数据使用过程中可访问的数据范围和使用目的。
- d) 遵守数据保护原则，按照标准 GB/T XXXXX-XXXX 中 6.4 的要求，主要考虑以下几个方面：
 - 1) 分布式处理安全；
 - 2) 数据分析安全；
 - 3) 数据加密处理；
 - 4) 数据脱敏处理；
 - 5) 数据溯源。
- e) 遵守可审计原则，记录和管理数据使用操作。
- f) 对数据分析结果的风险进行合规性评估，避免分析结果输出中包含可恢复的敏感数据。

7.4.2.4 数据分发

实施部门应：

- a) 遵守责任不随数据转移原则，对数据分发后产生的数据安全事件承担必要的安全责任。

GB/T XXXXX—XXXX

- b) 在数据分发前,对数据进行风险评估,确保数据分发后的风险可承受,方可分发数据,并通过合同明确数据接收方的数据保护责任。
- c) 在数据分发前,对数据的敏感性进行评估,根据评估结果对需要分发的敏感信息进行脱敏操作。
- d) 遵守可审计原则,记录时间、分发需求、数据接收方等相关信息。
- e) 提供有效的数据共享访问控制机制,明确不同机构或部门、不同身份与目的的用户的权限,保证访问控制的有效性。
- f) 建立大数据公开的审核制度,严格审核发布信息符合相关法律法规要求,明确数据公开内容、权限和适用范围,信息发布者与使用者的权利与义务,定期审查公开发布的信息中是否含有非公开信息,一经发现,立即删除。
- g) 评估数据传输安全风险,明确数据传输安全要求。

7.4.2.5 数据删除

实施部门应:

- a) 立即删除超出收集阶段明确的数据留存期限的相关数据;对留存期限有明确规定的,按相关规定执行。
- b) 在删除数据可能会影响执法机构调查取证时,采取适当的存储和屏蔽措施。
- c) 依照数据分类分级建立相应的数据销毁机制,明确销毁方式和销毁要求。
- d) 遵守审计原则,建立数据销毁策略和管理制度,明确销毁数据范围和流程,记录数据删除的操作时间、操作人、操作方式、数据内容等相关信息。

8 管理大数据安全风险

8.1 概述

风险管理主要包括以下四种不同的活动:

- a) 在总体安全策略环境内确定适合于组织的大数据风险管理战略;
- b) 根据风险评估结果,选用适当的防护措施;
- c) 形成安全策略,必要时更新总体安全策略;
- d) 根据批准的安全策略,制订安全计划以实现保护措施。

8.2 评估大数据风险

大数据风险评估可关注以下内容:

- a) 安全事件发生的概率
 - 1) 实施不利行为的因素
 - 潜在攻击方具有的资源、科学与技术专长、访问设施与设备的能力、动机等,常见的攻击方有个人、组织、国家等;
 - 潜在攻击方窃取、利用和滥用数据的意图;
 - 大数据访问、存储和分析所需资源;
 - 直接访问数据或窃取数据的概率;
 - 发起攻击、利用大数据技术、基础设施和数据集的经济能力;
 - 攻击的成本与收益。
 - 2) 系统的脆弱点
 - 大数据存储、处理等基础软件和基础设施的脆弱性;
 - 识别和限制数据访问和使用分析技术的能力;

GB/T XXXXX—XXXX

- 大数据相关系统的脆弱性。
- 3) 恶意利用所需的科学专业知识和技能
 - 数据和结果分析需要使用的技能、专业知识；
 - 数据使用和结果分析需要的技术和设备；
 - 利用系统脆弱性需要的技能、技术专长和知识。
- b) 后果
 - 1) 事件发生的后果
 - 造成的经济损失、名誉损失等；
 - 持续时间；
 - 影响的规模；
 - 事件恢复的时间、代价等。
 - 2) 存在的应对措施
 - 应对脆弱性的措施；
 - 防止或减轻后果的措施；
 - 防止或控制滥用大数据和大数据技术的措施。

附录C给出了生命科学大数据风险评估的具体案例。

8.3 选择安全保护措施

8.3.1 选择措施

根据8.2节的风险评估方法，评估大数据的安全风险，选择使风险降低到可接受水平的保护措施。

选择安全保护措施包含以下步骤：

- a) 分类分级组织大数据；
- b) 选择适当的保护措施。

组织应采用数据分类分级保护的方法对数据先分类，后分级，最后实施分级保护。

8.3.2 数据分类分级

8.3.2.1 数据分类分级原则

数据分类分级应满足以下原则：

- a) 科学性：按照数据的多维特征及其相互间客观存在的逻辑关联进行科学和系统化的分类，按照数据安全需求确定数据的安全等级。
- b) 稳定性：应以数据最稳定的特征和属性为依据制定分类和分级方案。
- c) 实用性：数据分类要确保每个类目下要有数据，不设没有意义的类目，数据类目划分要符合对数据分类的普遍认识。数据分级要确保分级结果能够为数据保护提供有效信息，应提出分级安全要求。
- d) 扩展性：数据分类和分级方案在总体上应具有概括性和包容性，能够实现各种类型数据的分类和分级，以及满足将来可能出现的数据类型和安全需求。

8.3.2.2 数据分类方法

数据分类方法宜参照标准 GB/T 7072—2002 中的 6 实施，由组织根据数据主体、主题、业务等不同的属性进行分类。

8.3.2.3 数据分级方法

组织应对已有数据或新收集的数据进行分级，数据分级时需要组织的业务部门领导、业务专家、安全专家等共同确定。政府数据分级参照GB/T 31167-2014中6.3执行，将非涉密数据分为公开、敏感数据，个人数据按照GB/T *****《个人信息安全规范》中的**，识别和确认个人敏感信息。

GB/T XXXXX—XXXX

组织可根据法律法规、业务、组织职能、市场需求等，对敏感数据进一步分级，以提供相应的安全管理和技术措施。

B.3.2.4 数据分级保护要求

组织应按照图2所示的数据分级步骤分级数据。附录A提供运营商对数据分级的实践案例。

涉密信息的处理、保存、传输、利用按国家保密法规执行。

组织应根据搜集、存储和使用的数据范围，结合自身行业特点制定组织的数据分类分级规范，规范应包含但不限于以下内容：

- 数据分类方法及指南；
- 数据分级详细清单，包含每类数据的初始安全级别；
- 数据分级保护的安全要求。

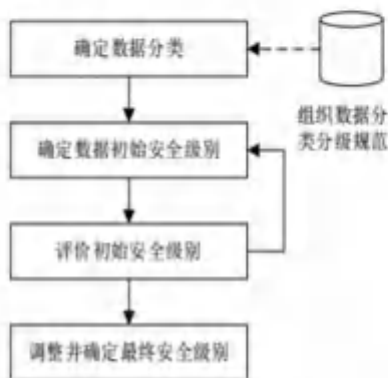


图2 数据分级实施步骤

B.4 制订安全计划

大数据安全计划阐述大数据的安全要求、已采用或拟采用的安全保护措施。大数据安全计划应包括以下内容：

- 大数据平台安全体系结构和设计；
- 数据收集、使用的目的、范围、手段等；
- 数据分类分级及安全要求；
- 大数据不同阶段的保护措施，大数据支撑平台的保护措施；
- 数据不同角色的职责分配；
- 大数据安全相关的安全意识培训等。

9 管理大数据平台运行安全

大数据平台运行安全是大数据安全的基础，大数据平台的运行安全管理目的是确保大数据平台安全持续满足要求。大数据平台运行安全应满足标准GB/T XXXXX—XXXX中7.4的要求。

组织应制定重大变更管理流程，主要活动包括：

- 标识重大变更；
- 重大变更的安全风险评估；
- 重大变更申请及批准流程；
- 重大变更中不同角色的职责。

GB/T XXXX—XXXX

大数据平台的重大变更包括但不限于以下变更：

- a) 鉴别（包括身份鉴别和数据源鉴别）和访问控制措施的变更；
- b) 数据存储实现方法的变更；
- c) 大数据平台中软件代码的更新；
- d) 备份机制和流程的变更；
- e) 安全措施的替换、撤除；
- f) 已部署商业硬件产品的替换；
- g) 数据源的变更，如增加、删除数据源；
- h) 分析算法、分析方式的变更。

GB/T XXXXX—XXXX

附录 A 电信行业数据分类分级示例

a) 数据分类

将全公司业务支撑域系统（B域）、网络支撑域系统（O域）、管理信息域系统（M域）、信令/DPI数据系统、业务管理平台等五大领域的的数据，分为以下四类。

类别	子类及范围
（A类）用户身份相关数据	（A1）用户身份和标识信息： （A1-1）自然人身份标识、（A1-2）网络身份标识、（A1-3）用户基本资料、（A1-4）实体身份证明、（A1-5）用户私密资料 （A2）用户网络身份鉴权信息： （A2-1）密码及关联信息
（B类）用户服务内容数据	（B1）服务内容和资料数据： （B1-1）服务内容数据、（B1-2）联系人信息
（C类）用户服务衍生数据	（C1）用户服务使用数据： （C1-1）业务订购关系、（C1-2）服务记录和日志、（C1-3）消费信息和账单、（C1-4）位置数据、（C1-5）违规记录数据 （C2）设备信息： （C2-1）设备标识、（C2-2）设备资料
（D类）企业运营管理数据（企业运营管理数据依据其商业价值，分为“核心”，“重要”，“一般”，“公开”四类数据。）	（D1）企业管理数据： （D1-1）：企业内部核心管理数据、（D1-2）：企业内部重要管理数据、（D1-3）：企业内部一般管理数据、（D1-4）：市场核心经营类数据、（D1-5）：市场重要经营类数据、（D1-6）：市场一般经营类数据、（D1-7）：企业公开披露信息、（D1-8）：企业上报信息 （D2）业务运营数据： （D2-1）：重要业务运营服务数据、（D2-2）：一般业务运营服务数据、（D2-3）：业务运营服务数据、（D2-4）：数字内容业务运营数据 （D3）网络运维数据： （D3-1）：网络设备及IT系统密码及关联信息、（D3-2）：核心网络设备及IT系统资源数据、（D3-3）：重要网络设备及IT系统资源数据、（D3-4）：一般网络设备及IT系统资源数据、（D3-5）：公开网络设备及IT系统资源数据、（D3-6）：公开网络设备及IT系统支撑据 （D4）合作伙伴数据： （D4-1）：渠道基础数据、（D4-2）：CP/SP基础数据*

数据分级如下表所示：

类别	定位	子类及范围
第4级	极敏感级	（A1-4）实体身份证明、（A1-5）用户私密资料、（A2-1）用户密码及关联信息、（D1-1）企业内部核心管理数据、（D1-4）市场核心经营类数据、（D3-1）网络设备及IT系统密码及关联信息、（D3-2）核心网络设备及IT系统资源类数据

GB/T XXXXX—XXXX

第3级	敏感级	(A1-1) 自然人身份标识、(A1-2) 网络身份标识、(A1-3) 用户基本资料、(B1-1) 服务内容数据、(B1-2) 联系人信息、(C1-2) 服务记录和日志、(C1-4) 位置数据、(D1-2) 企业内部重要管理数据、(D1-5) 市场重要经营类数据、(D1-8) 企业上报信息、(D2-1) 重要业务运营服务数据、(D3-2) 重要网络设备及IT系统资源类数据、(D4-1) 渠道基础数据、(D4-2) CP/SP基础数据
第2级	较敏感级	(C1-3) 消费信息和账单、(C2-1) 终端设备标识、(C2-2) 终端设备资料、(D1-3) 企业内部一般管理数据、(D1-6) 市场一般经营类数据、(D2-2) 一般业务运营服务数据、(D3-3) 一般网络设备及IT系统资源类数据、(D3-6)：网络设备及IT系统支撑数据
第1级	低敏感级	(C1-1) 业务订购关系、(C1-5) 违规记录数据、(D1-7) 企业公开披露信息、(D2-3) 业务运营服务数据、(D2-4) 数字内容业务运营数据、(D3-5)：公开网络设备及IT系统资源类数据

GB/T XXXXX—XXXX

附录B 国家基础数据

国家基础数据包含以下五类：

- **自然资源和空间地理基础数据：**包括基础地理与区划综合信息、遥感影像综合信息、全国自然资源综合信息、全国遥感资源环境动态监测综合信息、自然灾害监测预警和突发事件应急响应综合信息、资源安全动态评估预警综合信息、可持续发展和地区经济综合信息、生态环境评估综合信息、重大基础设施及生态工程监测综合信息。
- **人口基础数据：**人的状况和基础性信息,主要涉及包括教育、公安、民政、劳动和社会保障、人口和计划生育等信息。
- **法人单位基础数据** 与法人单位密切相关的数据,它代表了法人单位的基本状态与特征,具有跨业务系统共享需求基础。法人单位基本信息包含组织机构代码、组织机构名称、机构类型、机构住所、法定代表人姓名、经营或业务范围、注册资本或开办资金金额、注册资本或开办资金币种、成立日期、注册或登记机构名称、注册或登记号等。
- **宏观经济基础数据** 包括金融、税收、统计等基础信息以及消费、投资、进出口以及经济运行、节能减排、知识产权等方面的业务信息。
- **文化信息基础数据：**以国家物质和非物质文化遗产信息、少数民族传统文化、国家重要文物、国家档案信息等为主要内容的数据。

GB/T XXXX—XXXX

附录 C 生命科学大数据风险分析示例

表 C-1 展示了以下 3 个场景下生命科学大数据风险评估案例：

- 场景 1：使用生物大数据来设计针对特定人群的病毒
- 场景 2：误导传染信息、传染病监视系统
- 场景 3：利用大数据技术破坏现有的病原体检测能力

表 C-1 3 种典型场景下生命科学大数据风险分析

应用场景			场景 1	场景 2	场景 3
概 率	攻击方		具有充分资源的组织或国家、内部人员。这些攻击方技术先进。具有大量攻击所需资源、数据和所需软件。	熟悉计算机的个人、组织等。	技术上先进、能访问所需软件和数据、具有所需的资金支持。
	数据仓库、软件、网络基础设施的脆弱性		能使用公开访问的数据和分析软件。	报告机制和数据库的开放访问	开放访问数据和一些分析软件
	需 要 专 业 知 识 和 技 能	能利用系统的脆弱性	无	报告系统的访问，无特殊的技能要求	无
		使用大数据分析来设计有害的生物代理	需要特殊的技能：微生物基因组学、分子生物学、生物信息学	无	需要特殊技能：生物信息、分子生物学、微生物基因
后 果	经济、政治体系、社会、健康、环境和农业方面产生严重后果		后果很严重，造成人员伤亡或引发疾病、受到当地或国际社区的攻击，合规问题。	后果为中到高：损害人员健康、农业、环境等。	后果严重：不能检测危险的病原体感染。
	是否具有足够的应对措施		无足够应对措施。可能的技术措施有：访问控制、组织的内部措施、个人的措施。	无。IP 地址跟踪。	无。IP 地址跟踪、访问控制、组织的内部措施。
风险发生的概率			不太可能	近期是可能的	有可能

GB/T XXXXX—XXXX

附录 D 大数据安全风险

1. 大数据恶意使用给个人信息保护或国家安全带来损害

由于缺乏风险评估所需的必要信息，评估类似大数据等新兴技术的风险比较困难。随着大数据技术的进步，收集信息的不断丰富，数据共享标准的制定，大数据分析可以发现更多、更深入的关联关系。

例如通过关联分析用户在社交网站中写入的信息，智能手机显示的位置信息等多种数据，可以识别到自然人，挖掘出个人信息。利用大数据技术和不同的生命科学相关大数据，可以开发针对特定人群的生物病毒，给该群体的生命安全产生重大威胁。

2. 数据交易增加数据管理难度

由于大数据交换和交易具有便捷、快速、隐蔽的特性，监管大数据在不同数据控制者的处理过程非常困难。当发生数据泄露或个人数据保护问题时难以定位事件源，即责任方难以追溯，是其中最大的风险之一。

3. 数据不准确给机构的利益带来损失

网络的数据并非都可信，这主要反映在伪造的数据和失真的数据两个方面。有人可能通过伪造数据来制造假象，进而对数据分析人员进行诱导；或者数据在传播中逐步失真，这可使大数据分析和预测得出无意义或错误的结果，给组织、国家带来重大损失。

4. 大数据增加访问控制实现难度

访问控制是实现数据受控共享的有效手段，由于大数据可能被用于多种不同场景，其访问控制需求十分突出。难以预设角色，实现角色划分。由于大数据应用范围广泛，它通常要来自不同组织或部门、不同身份与目的的用户所访问，实施访问控制是基本需求。然而，在大数据的场景下，有大量的用户需要实施权限管理，且用户具体的权限要求未知。面对未知的大量数据和用户，预先设置角色十分困难。

同时，难以预知每个角色的实际权限。面对大数据，安全管理员可能无法准确为用户指定其可以访问的数据范围，而且这样做效率不高。

5. 数据聚集增加遭受网络攻击风险

为了从数据中挖掘有价值的信息，需要将不同的数据源进行汇聚和关联分析，数据汇聚增加了遭受网络攻击的风险。大数据系统本身是一个复杂系统，使得大数据系统不可避免存在一些安全脆弱点，成功的网络攻击导致数据被窃取、破坏后造成更加严重的损失。

6. 数据共享的安全风险

很难预先知道安全分享数据，才能既保证敏感信息不被泄露，又保证数据的正常使用。真实数据不是静态的，并且随着时间的变化而变化。数据规模在不断增加，分析技术不断发展，很难准确评估数据共享的风险，因此很难对数据进行充分的访问控制，存在敏感信息泄露的风险。

GB/T XXXX—XXXX

参 考 文 献

- [1] NIST Special Publication 1500-1, NIST Big Data Interoperability Framework: Volume 1, Definitions Final Version 1, September 2015
- [2] NIST Special Publication 1500-2, NIST Big Data Interoperability Framework: Volume 2, Big Data Taxonomies Final Version 1, September 2015
- [3] NIST Special Publication 1500-4, NIST Big Data Interoperability Framework: Volume 4, Security and Privacy Requirements Final Version 1, September 2015
- [4] NIST Special Publication 1500-6, NIST Big Data Interoperability Framework: Volume 6, Reference Architecture Final Version 1, September 2015
- [5] Editor draft of ISO/IEC 20547-1, Big data - Reference architecture - Part 1: Framework and application process, May 2, 2016
- [6] 4th Working Draft of ISO/IEC 20547-3, Big data - Reference architecture - Part 3: Reference architecture, January 23, 2016
- [7] 2nd Editors Draft of ISO/IEC 20547-4, Big data - Reference architecture - Part 4: Security and Privacy Fabric, January 5, 2016
- [8] Committee Draft of ISO/IEC 20546, Big data - Overview and Vocabulary, March, 2016
- [9] ITU-T Y.3600, Big data - Cloud Computing based requirements and capabilities, November, 2015
- [10] ENISA Big Data Security - Good Practices and recommendations on the security of Big data systems, December, 2015
- [11] ICO Big data and data protection Version 1.0, July 28, 2014
- [12] GB/T 7072—2002 信息分类和编码的基本原则与方法
- [13] GB/T 20529.1—2006 企业信息分类编码导则 第一部分：原则与方法
- [14] 贵州省《政府数据 数据分类分级指南》（试行）
- [15] ISO/IEC DIS 38505-1, Information Technology — Governance of IT — Part 1: The application of ISO/IEC 38500 to the governance of data
- [16] A Joint AAAS-FBI-UNICRI Project, National and Transnational Security Implications of Big Data in the Life Sciences
- [17] GB/T 19715.1-2005/ISO/IEC TR13335-1:1996. 信息技术 信息技术安全管理指南 第1部分：信息技术安全概念和模型.
- [18] GB/T 19715.2-2005/ISO/IEC TR13335-2:1997. 信息技术 信息技术安全管理指南 第2部分：管理和规划信息技术安全.

专业服务提供者是提供专业服务的组织。这个角色可能由公司内的一个内部组织扮演，或者由外部公司执行。这些外部公司或者是被转包方，或者和专业服务公司签订了合同，也可能是公司的竞争者。

客户的定义是人员或者组织，他们曾经雇用服务公司执行服务或者最近正在雇用服务公司。顾客有一个子类付款客户，描述了负责交付专业服务费的当事人，另一个子类接受服务的客户是接受专业服务的当事人。

7.1.3 关于专业服务角色和关系的例子

这一章中的实例是一个名为“Whole Shebang Professional Services”的专业服务公司。表 7-2、7-3、7-4 提供了关于专业服务人员角色、组织角色和关系的例子。表 7-2 提供了人员角色的一些例子。“Rob Mathews”是一个人员客户，人员客户的意思是他作为个人而不是作为一个组织的一部分来雇用专业服务公司。“Phil Williams”是一个客户联络员，“Pete Waters”是一个供应商的联络员，“Joe Witherspoon”是一个雇员。表中接下来的三行展示了可以提供服务的不同的专业人员，即“Sol Isiter”、“Spi Hay”和“Joe Nowitall”。

表 7-2 专业服务人员角色

人员角色	人员姓名
客户（人员客户）	Rob Mathews
联络员（供应商联络员）	Pete Waters
联络员（客户联络员）	Phil Williams
雇员	Joe Witherspoon
专业人员（律师）	Sol Isiter
专业人员（会计）	Spi Hay
专业人员（顾问）	Joe Nowitall

表 7-3 提供了专业服务提供者中的组织角色的例子。“Whole Shebang Professional Services”是一个提供包括法律、会计和一些咨询服务在内的所有专业服务类型的公司。根据表 7-3，“Whole Shebang Professional Services”是三个分部的上级组织，即“Whole Shebang Law Office”，“Whole Shebang Accounting”和“Whole Shebang Consulting”。“XYZ Accounting Services”是另一个专业服务提供商，它不是内部组织，可以成为服务转包商。所有这些公司还扮演着专业服务提供商和内部组织的角色。“Everything Manufacturing”是一个组织型的客户，“ABC Printing”是一个供应商。

表 7-3 专业服务当事人角色

组织角色	组织名称
专业服务提供者 内部组织 上级组织	Whole Shebang Professional Services
专业服务提供者 内部组织 分支机构	Whole Shebang Law Offices
专业服务提供者 内部组织 分支机构	Whole Shebang Accounting
专业服务提供者 内部组织 分支机构	Whole Shebang Consulting
客户（组织客户）	Everything Manufacturing
专业服务提供者	XYZ Accounting Services
供应商	ABC Printing

表 7-4 提供了一些关于什么角色与什么关系有关的补充信息。例如：前两行显示了“Everything Manufacturing”是公司两个内部组织，即“Whole Shebang Law Offices”和“Whole Shebang Accounting”的一个客户。“Phil Williams”是“Everything Manufacturing”的联络员。“Rob Mathews”是“Whole Shebang Professional Services”的客户，“ABC Printing”是“Whole Shebang Professional Services”的供应商，其中一位负责供应的联络员是“Pete Waters”。表 7-4 说明“Joe Witherspoon”是“Whole Shebang Professional Services”的一个雇员。“Sol Isiter”，“Sipi Hay”和“Joe Nowitall”都是能够提供各种服务的专业人员，其中“Sol Isiter”偶尔在“Whole Shebang”工作，而其他两个专业人员为其他公司工作。所以“Sol Isiter”具有专业人员和受雇人员的角色，而“Sipi Hay”和“Joe Nowitall”既有专业人员和签约人的角色，还和他们各自的公司有“组织联系关系”。

表 7-4 专业服务当事人关系

当事人之间的关系	提供服务的当事人名称	接受服务的当事人名称
客户关系	Everything Manufacturing	Whole Shebang Law Offices
客户关系	Everything Manufacturing	Whole Shebang Accounting
组织联系关系（客户联系关系）	Phil Williams	Everything Manufacturing
客户关系	Rob Mathews	Whole Shebang Professional Services
供应商关系	ABC Printing	Whole Shebang Professional Services
组织联系关系（供应商联系关系）	Pete Waters	ABC Manufacturing
雇用	Joe Witherspoon	Whole Shebang Professional Services
雇用	Sol Isiter	Whole Shebang Professional Services
组织联系关系（签约人）	Sipi Hay	Weknow Accounting Services
组织联系关系（签约人）	Joe Nowitall	Joe Nowitall, Inc.

7.2 专业服务产品

从专业服务组织的定义来看，它们注重出售服务。这些组织可能按时间收费，也可能向客户提供已经预先规定好的基于交付结果的服务。另外，这些公司可能出售某些物品来辅助它们所提供的服务，比如应用软件。

7.2.1 专业服务产品模型

图 7.2 为专业服务组织提供了一个修正的产品定义。这个模型是卷 I 中的一些通用模型、产品类别（VI-3-2）和产品特征（VI-3-4），做了一些特定的缩小修改而成的。产品实体又进一步划分为服务和货物子类。服务可能是基于交付结果的服务或者是时间和原材料服务。交付结果的定义是预先定好的作为雇用或者雇用项目的结果为客户生产的工作产品。时间和原材料服务是一个由根据时间和材料收费的专业服务公司提供的标准服务。一个基于时间和材料的服务的例子是一个公司提供的“会计审计”，它依照标准价格为每个小时的审计收费。

为了提供每种专业服务产品，每个产品可能需要一种或多种技能。因此，如果要交付一种或多种产品，可能需要每一种技能类型，反之亦然，这样就需要相关实体产品交付技能需求。例如，在交付有关数据体系结构开发的标准专业服务时，可能需要“数据体系结构”、“数据建模”和“简化”这些技能类型。如果这个产品被出售，这些信息就会帮助确定需要哪些专业人员。

产品特征和产品特征类别实体适用于专业服务，因为在某些服务中可能存在一些差异和特征。

产品可以按多种方式分类，如按服务所属行业（产品行业类别）分类，例如出售属于“管理产品”类的“存货管理即时服务”。产品还可以按其所属的技能产品类别（技能产品分类）进行分类，例如“数据仓库就绪性评估”属于“数据仓库供应”技能产品类别。

表 7-5 显示了可能在专业服务企业内存在的产品例子，以“Whole Shebang Professional Services”内部为例。这些服务代表了可能提供的专业服务类型，比如“商标注册服务”、“簿记”、“会计审计”和“数据体系结构”，一般来说，这些服务有相关的标准计费。随着时间推移这个价格会根据市场需求而发生变化。卷 I 中的产品价格模型（VI-3-7）可以提供这些信息。

交付结果是即将生产的预定好的工作产品，比如专利、内部审计，或者是一个企业数据模型或一个数据库设计。同一个类型的服务可能被定义为基于交付结果的服务，时间和原材料服务或是同时属于两者（这个实体的两个实例），到底属于哪种服务取决于专业服务提供者怎样包装他们的服务。请注意这些产品可能由正在被建模的公司提供，也可能由其他公司提供，如表中最后一行所示。这个表显示了用于辅助服务的商品，比如小册子或者软件。

特征则显示了可能的变化或者可能包含在专业服务中的选择，比如在“Whole Shebang Law Offices”提供的商标注册服务中存在着注册一个商标还是两个商标的选择，因为对于这种

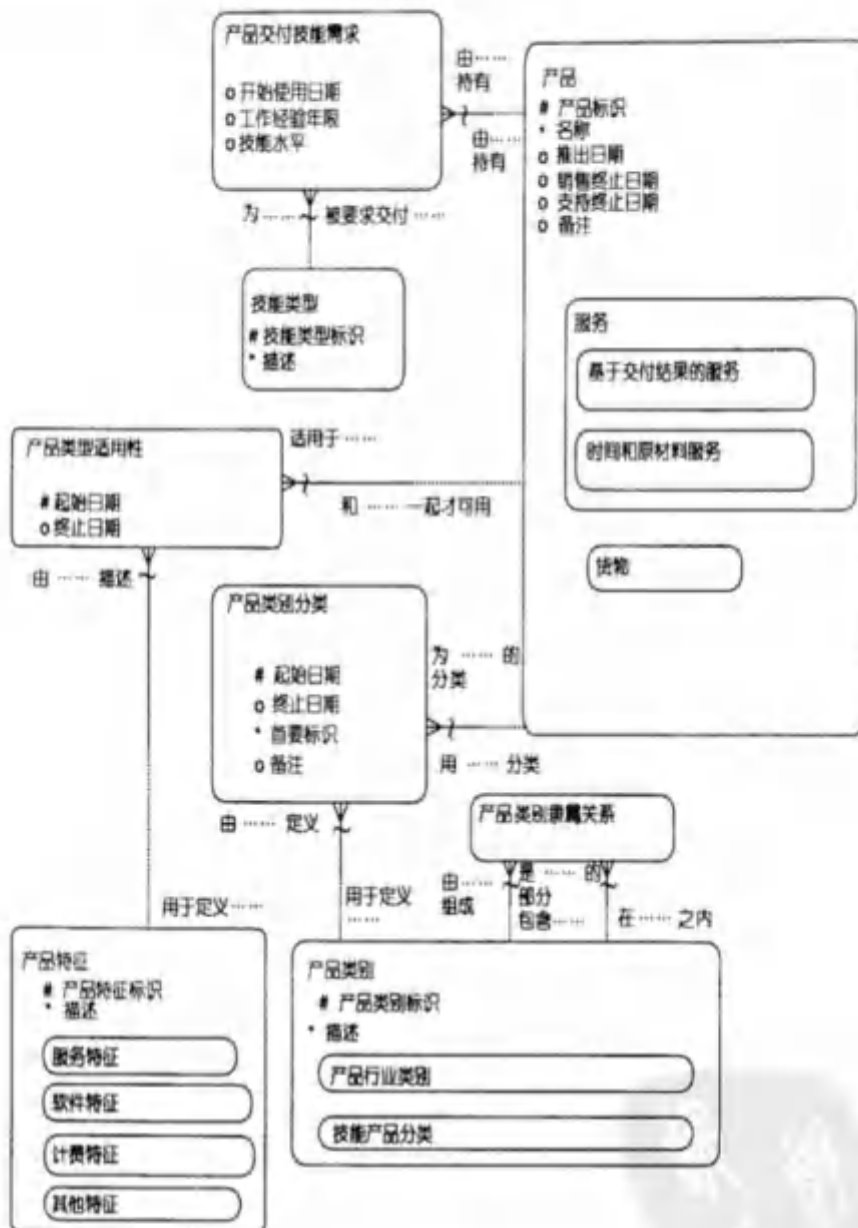


图 7-2 专业服务产品

服务，这两种选择的费用有所不同。这个例子中，提供的服务类型发生了变化，因此它属于服务特征的一个例子。“两周一次”、“一个月一次”都是计费特征的例子。“包含源代码”是软件特征的一个例子，软件特征是“Whole Shebang Accounting 软件”的产品可能具有的特点。

表 7-5 专业服务产品

提供服务的组织	产品类型	产品名称	产品特性
Whole Shebang Law Offices	时间和原材料服务	商标注册服务	一个商标注册两个商标注册
Whole Shebang Law Offices	基于交付结果的服务	为一个产品提供专利	
Whole Shebang Law Offices	货物	Whole Shebang 关于专利的小册子	
Whole Shebang Accounting	时间和原材料服务	簿记	双端计费月计费
Whole Shebang Accounting	基于交付结果的服务	为中等大小公司提供的会计审计	法定代理
Whole Shebang Accounting	货物	Whole Shebang 会计软件	包含源代码
Whole Shebang Consulting	时间和原材料服务	数据体系结构开发	
Whole Shebang Consulting	基于交付结果的服务	企业数据模型	
Whole Shebang Consulting	货物	Whole Shebang CASP 工具	
其他咨询事务所	基于交付结果的服务	数据库设计评审	

7.2.2 其他产品模型的适用性

产品模型 V1:3-5 的供应者和生产者，可能用来记录哪些组织供应哪些类型的服务、交付结果和货物。在追踪其他专业服务组织提供的服务时，这个模型发挥其作用，简化了转包合同的安排。供应方购货时也可以使用这个模型。

其他产品模型不包括库存项目存储模型，V1:3-6。因为专业服务公司主要处理服务和交付结果。当然也可以利用这些结构来存储供应品，然而在大多数情况下，公司并不想也没有办法使这个模型有使用的价值。

产品价格模型，V1:3-7，一般对一些例外情况起作用。在价格成分中除了价格属性还应该有利率属性来存储专业服务供应的标准利率。

产品成本数据模型，V1:3-8，的适用性很强，因为不论专业人员是来自服务公司还是来自其他公司，知道他们的服务成本都是很重要的。还有，确定服务公司是否会为每个供应者（或者专业服务公司）存储各个服务类型的成本信息也是重要的。如果公司只存储自己公司所提供服务的成本信息，那么我们感兴趣的关系应该是预计产品成本和产品的关系，而不是预计产品成本与供应商产品的关系。

7.2.3 专业服务产品关联

因为服务常常由其他服务组成，产品关联数据模型，V1:3-9a~3-9b，有一定的适用性。如图 7-3 所示，它与 V1:3-9a~3-9b 还是有一些不同。实体行销包取代了图 3-9a 中的产品构成，行销包用来记录把多个服务集中到一个服务包中。这样做很合适，因为服务和交付结果可能包含其他交付结果。比如一个管理咨询战略规划服务可能由一个管理战略规划、一个管理建议报告和一系列的商业模型组成。“使用的数量”和“使用说明”属性被去掉了，因为这些属性对有形的装配物品更重要。



图 7-3 专业服务产品关联

产品替代实体被去掉了，因为服务一般不处理一个服务或者交付结果替代其他服务或者交付结果的问题。产品取代是适用的，因为服务可能被其他专业服务产品供应所取代。产品补充

适用于专业服务组织。比如一个法律公司提供的“商标注册”检索服务可能是“商标检索”服务的补充。然而，产品不要因此适用于销售商品的公司，但是它可能不适用于专业服务公司。

7.3 订单

像大多数行业一样，专业服务公司也从他们的客户处获得订单。然而，它们经常被称为“雇用”，因为是客户雇用了公司的服务。所以卷1中的订购数据模型也许应该做些修改后再使用。

在这一节中提出的雇用模型应该适用于公司的销售方面，而卷1中的标准订购模型可以用于公司的购买方面。例如用于购买设备和/或供应品。当从公司向客户提供的雇用服务中捕获信息时，会用到下面的雇用模型。当从其他服务组织向公司提供的雇用服务中捕获信息时也会用到这个模型，因为在专业服务公司内转包是一个非常常见的业务。

本节由那些捕获关于特定的雇用服务和全部专业服务协议信息的模型组成。这一节中会扩展卷1中的需求、请求和报价数据模型（VI:4.9-4.11），因为它们也是专业服务公司的重要信息需求。雇用数据模型以卷1中的订单数据模型（VI:4.1-4.8）为基础，而且要存储关于执行时间和原材料任务的合约的信息，或者存储在项目雇用中关于交付具体结果的合约的信息。有的时候雇用被称为“工作的描述”。协议数据模型捕获有关两方或多方当事人之间的协议的信息，这个协议一般能控制这些确定的雇用服务。

7.3.1 专业服务需求

在专业服务组织中，需求、请求和报价都是交易中不可缺少的部分。卷1中的模型适用性非常强，然而本章中的模型会对这些数据结构做进一步的扩展。

图7.4中，需求实体保存关于客户的需要（客户需求）的信息，还保存关于专业服务企业需要的信息（内部需求）。需求实体使得组织能够任意存储它的客户的需求和企业本身所具有的需求，比如那些已经被专业服务公司给了其他组织的转包需求。

每个需求也可能表现为资源需求、项目需求或者产品需求。资源需求或者代表对客户的需求，或者代表专业服务企业聘用专业人员的需求，聘用的形式是基于合同或者雇用。这种需求也被认为是对临时或者永久“人员安排”的需求。项目需求是基于交付结果的需求，它是通过工作计划提交一个特定结果或者项目的需求。比如一个客户可能需要专业服务公司来提供一个销售分析数据仓库。产品需求中保存针对专业服务企业可提供的具体预定义产品的需求。举个例子，专业服务组织可能会提供“商标注册”标准服务。在这种情况下，该需求实体会针对这个标准产品保存相应的需求。

资源需求保存每种技能类型需要的技能，要把留住工作机会需要这些技能类型。工作经历年限和技能水平使得所需要的技能有确定的等级规范。这与专业人员可能有什么技能相对应（见人力资源模型，VI:9.11）。项目需求保存交付结果类型需要的交付结果来定义这些需求所希望的结果。每个产品需求可能需要一个确定的预先定义好的专业服务公司的产品，而且可能会根据期望特征做进一步的改进。

每一个需求都可能要在某个设施中用到，比如一个要在某个建筑中做地基的资源的需求或者一个客户的法人代表所需要的销售分析解决方案。

需求实体可能有许多需求场景，包括有需求的当事人、满足需求的当事人、寻找满足需求当事人的人（招聘人员或者职务管理员），和/或者那些应客户请求从事工作的人。

在需求被执行、被支持、被管理、被出售期间，每个需求有许多需求状态：需求状态可以是“活动的”，“非活动的”，“等待用户认可”，“取消”，“被其他的企业履行”，或者“停止”（意思是企业停止出售）。

对每个需求，可能需要存储描述，即对需求的解释；需求创建日期，即需求首次起源于何时；需求提出日期，即何时需要完成需求；预算估计，即要完成需求估计需要的花费；原因，即为什么要设立这些需求。对于资源需求，还有一些属性：职位数目，即有多少个就业机会（比如可能需要两个技能作家顾问）；需求开始日期，即何时开始需要（人力）资源；需求结束日期，即何时就不再需要这些资源；职责，即（人力）资源的责任。

需求实体可能递归地和那些可以存储需求细节的更低级需求有关。比如，一个数据库项目需求可能由以下更多的详细需求组成：对一个企业数据库的需求，对一个确定的销售分析数据集的需求，对一个财政分析数据集的需求。递归需求分解的一个例子是：设有一个总体资源需求，它需要一个系统顾问和一个技术文书与员顾问，这样产生了两个更低一级的需求。在后一种情况下，可能会有几个专业人士适合这个需求。

需求常常涉及到与客户和/或转包商的通信往来，以了解他们之间能否达成一致。每个需求都可能有一些需求通信来跟踪需求，还会有一些专业人员从事与需求有关的活动。需求通信表明了哪些通信事件（为了需求活动）和需求有关，这些通信事件可能和一个特定的专业人员有关，这个专业人员很可能是去帮助履行需求的人。需要跟踪的重要需求活动包括“提交履历”、“销售会议”、“访问调查”和“提案”。根据公司的需求，他们可能将提案作为一个单独的实体进行跟踪——比如在卷1中的报价实体——或者如果关于它们的报价信息只有很少的话，他们可能在需求活动实体中跟踪提案。

表7.6给出了一些图7.4中的需求数据模型内可能会包含的一些信息实例。“Whole Shebang Law Offices”跟踪每个需求和相关的活动。比如，一个项目需求是“易惹麻烦的经销商”的“诉讼”需求，这个经销商又遇到了麻烦。交付的结果是那些关于怎样进一步处理事情的建议和这件事情的解决方法。Whole Shebang Law Offices安排了与这个需求有关的活动，安排与Sol Ister和潜在客户在1999年12月19日举行，1999年12月27日提出了一个议案。根据这个公司和它的需要，这个提议也许就是固有的实体而且和这个公司的需要有关，或者因为在这种情况下这个提议不需要什么细节，所以这个提议被看成是需求通信的一种类型。

Whole Shebang Accounting有一个客户需要一个纳税申报单，这个纳税申报单表示有标准价格的标准产品。客户想通过纳税申报单确保能得到Whole Shebang的收益背后的立场特征，并且在税务监查时提供建议。跟踪需求的通信包括会议和要去处理的口头合约。

Whole Shebang Consulting记录了一个依据合同雇用了一个数据模型师的资源需求。这个数据模型师的候选人必须有数据建模、简化、数据库设计的技能。请注意每个需求通信都可能与一个专业人员有关，也可能没有。和数据建模合同有关的面试活动展现了致力于不同的需求通信的不同专业人员。

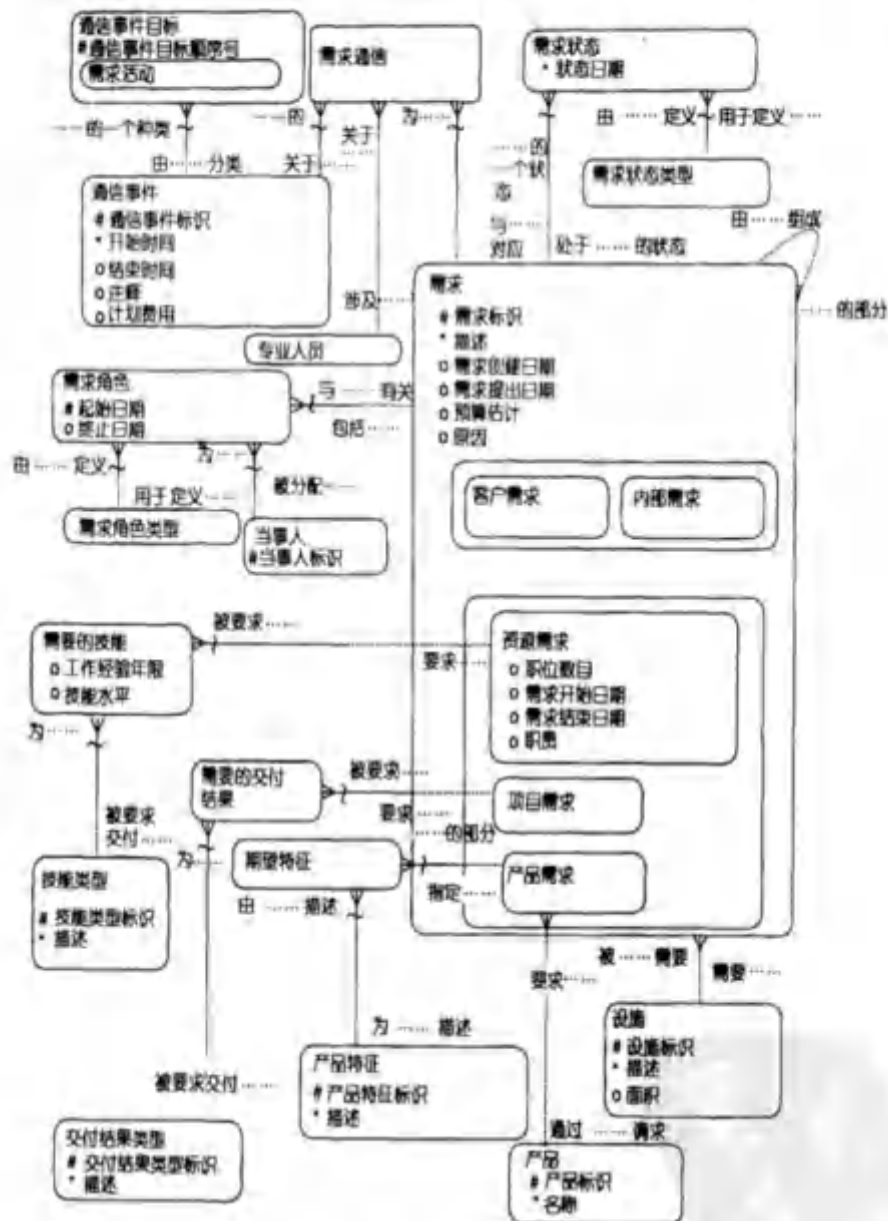


图 7-4 专业服务需求

表中最后一个需求描绘了 ABC Consumer 公司的客户需求，即需要一个销售分析系统。这个分析系统有数据转化程序的结果、销售分析用户界面、终端用户报告，特别地，它还具有报告能力。这个需求是从 ABC Consumer 公司的账目管理人员的销售要求中得来的。

(三十二) 个人金融信息保护技术规范

(银发〔2020〕45号)

《个人金融信息保护技术规范》(JR/T 0171-2020, 以下简称《规范》) 金融行业标准已经全国金融标准化技术委员会审查通过, 现予以发布, 并就有关事项通知如下:

一、金融业机构可结合实际按照《规范》加强个人金融信息全生命周期技术管理, 强化风险识别和监控, 建立健全风险事件处置机制, 保障个人金融信息主体合法权益。

二、行业协会可根据工作需要按照《规范》加强个人金融信息保护行业自律管理, 建立健全自律检查、违规约束、投诉处理等机制, 定期向人民银行报送相关情况。

请人民银行副省级城市中心支行以上分支机构将本通知告知辖区内分支机构和金融业机构。

附件: 个人金融信息保护技术规范

Personal financial information protection technical specification

目次

前言

引言

1 范围

2 规范性引用文件

3 术语和定义

4 个人金融信息概述

5 安全基本原则

6安全技术要求

7安全管理要求

附录A （资料性附录） 信息屏蔽

参考文献

前言

本标准按照GB/T 1.1-2009给出的规则起草。

本标准由中国人民银行提出。

本标准由全国金融标准化技术委员会（SAC/TC 180）归口。

本标准起草单位：中国人民银行科技司、中国人民银行郑州中心支行、北京银联金卡科技有限公司、中国银行股份有限公司、中国银联股份有限公司、网联清算有限公司、浙江蚂蚁小微金融服务集团股份有限公司、拉卡拉支付股份有限公司、中国金融电子化公司、中国人民银行武汉分行、中国工商银行股份有限公司、中国农业银行股份有限公司、中国建设银行股份有限公司、中国平安保险（集团）股份有限公司、北京中金国盛认证有限公司、北京软件产品质量检测检验中心、中金金融认证中心有限公司、信息产业信息安全测评中心、华泰证券股份有限公司、中国人民保险集团股份有限公司、财付通支付科技有限公司、中国支付清算协会、中国互联网金融协会、建信金融科技有限责任公司。

本标准主要起草人：李伟、李兴锋、张宏基、关晓辉、刘雨露、汤沁、郭琳净、赵战勇、熊继承、渠韶光、孟飞宇、高强裔、陈聪、居崑、陈雪秀、公丽丽、徐艳姣、牛小伟、王欢、展昭、强群力、郭林、杨萌、陈俊、李意、冯坚坚、唐凌、黄本涛、魏猛、刘琼瑶、赵旭、孙垚、周利华、母延燕、王家炜、张扬、蔡嘉勇、刘洋、孙鹏亮、聂丽琴、刘力慷、牛跃华、陈伟、王秀君、任凤丽、谢宗晓、董亚南、张旭刚、刘健、董晶晶、张嵩、于晓雪、吴永强、陆家有、石竹君、于沛、侯晓晨、田然、王泽航、何伟明、梁伟韬。

引言

个人金融信息是个人信息在金融领域围绕账户信息、鉴别信息、金融交易信息、个人身份信息、财产信息、借贷信息等方面的扩展与细化，是金融业机构在提供金融产品和服务的过程中积累的重要基础数据，也是个人隐私的重要内容。个人金融信息一旦泄露，不但会直接侵害个人金融信息主体的合法权益、影响金融业机构的正常运营，甚至可能会带来系统性金融风险。为加强个人金融信息安全管理，指导各相关机构规范处理个人金融信息，最大程度保障个人金融信息主体合法权益，维护金融市场稳定，编制本标准。

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/T 22239-2019 信息安全技术 网络安全等级保护基本要求

GB/T 25069-2010 信息安全技术 术语

GB/T 31186.2-2014 银行客户基本信息描述规范 第2部分：名称

GB/T 31186.3-2014 银行客户基本信息描述规范 第3部分：识别标识

GB/T 35273-2017 信息安全技术 个人信息安全规范

JR/T 0068-2020 网上银行系统信息安全通用规范

JR/T 0071 金融行业信息系统信息安全等级保护实施指引

JR/T 0092-2019 移动金融客户端应用软件安全管理规范

JR/T 0149-2016 中国金融移动支付 支付标记化技术规范

JR/T 0167-2018 云计算技术金融应用规范 安全技术要求

3 术语和定义 GB/T 25069-2010、GB/T 35273-2017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 financial industry institutions

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 personal financial information

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/T 35273-2017，定义3.1。

3.3 支付敏感信息 payment sensitive information

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 personal financial information subject

个人金融信息所标识的自然人。

注：改写GB/T 35273-2017，定义3.3。

3.5 个人金融信息控制者 personal financial information controller

有权决定个人金融信息处理目的、方式等的机构。

注：改写GB/T 35273-2017，定义3.4。

3.6 收集 collect

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。

3.7 公开披露 public disclosure

向社会或不特定群体发布信息的行为。

3.8 转让 transfer of control

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。

3.9 共享 sharing

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。

3.10 个人金融信息安全影响评估 personal financial information security impact assessment

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。

3.11 支付账号 payment account

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。

3.12 支付标记 payment token (Token)

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。

3.13 磁道数据 track data

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。

3.14 卡片验证码 card verification number; CVN

对磁条信息合法性进行验证的代码。

3.15 卡片验证码2 card verification number 2; CVN2

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。

3.16 动态口令 one-time-password (OTP) , dynamic password

基于时间、事件等方式动态生成的一次性口令。

3.17 短信动态密码 SMS dynamic code

短信验证码 SMS code

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。

3.18 客户法定名称 customer's legal name

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/T 31186.2-2014，定义3.2。

3.19 证件类识别标识 legal discriminating ID

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。

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/T 31186.3-2014，定义3.2。

3.20 未经授权的查看 unauthorized reading

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 unauthorized altering

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 explicit consent

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/T 35273-2017，定义3.6。

3.23 匿名化 anonymization

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/T 35273-2017，定义3.13。

3.24 去标识化 de-identification

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/T 35273-2017，定义3.14。

3.25 删除 delete

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/T 35273-2017，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。

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。

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/T 35273-2017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：

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：

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（CVN1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。

应用程序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/T 0149-2016）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，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。

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/T 0167-2018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/T 22239-2019、JR/T 0071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。

6.2.2 Web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/T 0092-2019、JR/T 0068-2020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。

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；

--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 and 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；

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，应立即调整并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。

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）。

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/T 35273-2017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。

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。

附录A

(资料性附录)

信息屏蔽

信息屏蔽指对某些敏感信息通过既定规则屏蔽（或截词）全部（或部分）敏感信息，实现对敏感信息展示的可靠保护。通过信息屏蔽可使信息本身的安全等级降级，从而可以在开发、测试和其他非生产环境以及外包或云计算环境中安全地使用脱敏后的信息集。借助信息屏蔽（或截词）技术，屏蔽敏感信息，并使屏蔽的信息保留其原始个人金融信息格式和属性，以确保应用程序可在使用脱敏个

人金融信息的开发与测试过程中正常运行。

注：截词的目的在于永久删除某条信息的某个数据段，仅存储部分数据（如仅保留银行卡卡号不超过前六位和后四位数）。

对外输出的任何个人金融信息原则上应事先做屏蔽（或截词）等脱敏处理（已经获得用户明示同意以及根据法律法规要求需要对外输出的信息除外），脱敏处理包括但不限于：

--模糊化：指通过隐藏（或截词）局部信息令该个人金融信息无法完整显示，包括但不限于：

具体名称ID化（如：以12345代替客户法定名称或ID），具体ID哈希化，金额、笔数去绝对值化（如：区间分段、个位数及小数点取整等）、星号模糊化；

信息隐藏规则（缺省）：显示前1/3和后1/3（向下取整），其他用*号代替，这样保留了部分信息，并且保证了信息的长度不变性，对信息持有者更易辨别，如手机、身份证号码等。

--不可逆：指无法通过样本信息倒推真实信息的方法，包括但不限于：

使用匿名、差分隐私等技术对真实信息进行处理，使其无法被识别，且处理后的信息不能被复原；

不应通过信息拼接、关联得到完整的敏感信息记录；

不应通过局部占比的信息得到全量信息。

针对特定类型信息的隐藏规则示例详见表A.1。

表A.1个人金融信息隐藏规则及示例

敏感信息类型

信息范围

展示规范

银行卡信息

银行卡卡号

显示前6位 + * (实际位数) + 后4位。如: 622575*****1496

个人信息信息

1) 身份证号码、军官证号码、护照号码

使用缺省信息隐藏规则, 如隐藏出生日期, 身份证号码屏蔽后6位

2) 客户法定名称 (姓名)

隐藏部分字符

3) 手机号码

除区号外, 至少隐藏中间四位

大陆: 显示前3位 + **** + 后4位。如: 137****9050

香港、澳门: 显示前2位 + **** + 后2位。如: 90****85

台湾: 显示前2位 + **** + 后3位。如: 90****856

其他海外地区: 使用缺省隐藏规则

4) 固定电话号码

推荐的规范: 显示区号和后2位

敏感信息类型

信息范围

展示规范

5) 电子邮箱

@前面的字符显示前3位, 3位后显示3个*, @后面完整显示如: con***@111.com

如果少于三位, 则全部显示, @前加***, 例如tt@111.com则显示为tt***@111.com

参考文献

- [1]GB/T 13016-2018 标准体系构建原则和要求
- [2]GB/T 13017-2018 企业标准体系表编制指南
- [3]GB/T 18336.1-2015 信息技术 安全技术 信息技术安全评估准则 第1部分: 简介和一般模型
- [4]GB/T 25000.10-2016 系统与软件工程 系统与软件质量要求和评价 (SQuaRE) 第10部分: 系统与软件质量模型
- [5]GB/T 26237.1-2010 信息技术 生物特征识别数据交换格式 第1部分: 框架
- [6]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
- [7]GM/Z 0001-2013 密码术语
- [8]JR/T 0061-2011 银行卡名词术语
- [9]JR/T 0088.1-2012 中国金融移动支付 应用基础 第1部分: 术语
- [10]JR/T 0156-2017 移动终端支付可信环境技术规范
- [11]ISO/IEC 19785-2: 2006 Information technology-Common biometric exchange formats framework-Part 2: Procedures for the operation of the biometric registration authority
- [12]ISO/IEC 27018: 2014 Information technology-security techniques-Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
- [13]ISO/IEC 29100: 2011 Information technology-Security techniques-Privacy framework

[14]中国人民银行.中国人民银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（银发[2011]17号），2011-01-21

[15]中国人民银行.中国人民银行关于银行业金融机构进一步做好客户个人金融信息保护工作的通知（银发〔2012〕80号），2012-03-27

[16]征信业管理条例（国务院令 第631号），2013-01-21

[17]中国人民银行.中国人民银行关于进一步加强银行卡风险管理的通知（银发〔2016〕170号），2016-06-13

[18]中国人民银行.中国人民银行关于印发《中国人民银行金融消费者权益保护实施办法》的通知（银发〔2016〕314号），2016-12-14

[19]中国人民银行.中国人民银行关于印发《金融科技（FinTech）发展规划（2019-2021年）》的通知（银发〔2019〕209号），2019-08-19

[20]金融机构客户身份识别和客户身份资料及交易记录保存管理办法（中国人民银行 中国银行业监督管理委员会 中国证券监督管理委员会 中国保险监督管理委员会令〔2007〕第2号），2007-06-21

(三十三) 公开征求对《工业和信息化领域数据安全风险信息报送与共享工作指引（试行）（征求意见稿）》的意见

为贯彻落实《[中华人民共和国数据安全法](#)》等法律法规，加强工业和信息化领域数据安全风险信息获取、分析、研判和预警工作，及时掌握工业和信息化领域数据安全整体态势，提高数据安全风险处置能力，工业和信息化部研究起草了《工业和信息化领域数据安全风险信息报送与共享工作指引（试行）（征求意见稿）》（见附件），拟以规范性文件形式印发，现面向社会公开征求意见。如有意见或建议，请于2022年1月22日前反馈。

传真：010-66069561

邮箱：zhanghong@miit.gov.cn

地址：北京市西城区西长安街13号工业和信息化部网络安全管理局（邮编：100804）。请在信封上注明“《工业和信息化领域数据安全风险信息报送与共享工作指引（试行）（征求意见稿）》意见反馈”。

工业和信息化部

2021年12月22日

附件：工业和信息化领域数据安全风险信息报送与共享工作指引（试行）

第一章 总则

第一条 为加强工业和信息化领域数据安全风险信息获取、分析、研判和预警工作，及时掌握工业和信息化领域数据安全整体态势，提高数据安全风险处置能力，根据《中华人民共和国数据安全法》等法律法规，制定本指引。

第二条 本指引所称数据安全风险信息，是指通过检测、评估、信息搜集、授权监测等手段获取的，包括但不限于数据泄露、数据篡改、数据滥用、违规传输、非法访问、流量异常等数据安全风险：

（一）数据泄露，包括但不限于数据被恶意获取，或者转移、发布至不安全环境等相关风险；

(二) 数据篡改, 包括但不限于造成数据破坏的修改、增加、删除等相关风险;

(三) 数据滥用, 包括但不限于数据超范围、超用途、超时间使用等相关风险;

(四) 违规传输, 包括但不限于数据未按照有关规定擅自进行传输等相关风险;

(五) 非法访问, 包括但不限于数据遭未经授权访问等相关风险;

(六) 流量异常, 包括但不限于数据流量规模异常、流量内容异常等相关风险;

(七) 其他信息, 包括由相关政府部门组织授权监测的暴露在互联网上的数据库、大数据平台等数据资产信息, 以及有关单位掌握的威胁数据安全的其他风险信息等。

第三条 本指引所称风险信息报送, 是指有关单位向工业和信息化部、地方工业和信息化主管部门、地方通信管理局报送数据安全风险信息的行为。

第四条 本指引所称风险信息共享, 是指经工业和信息化部、地方工业和信息化主管部门、地方通信管理局审核、授权后, 向有关部门、单位告知风险提示的行为。

第五条 风险信息报送与共享工作坚持“及时、客观、准确、真实、完整”的原则, 不得迟报、瞒报、谎报。

第二章 组织机构及职责

第六条 工业和信息化部指导、监督工业和信息化领域数据安全风险信息报送与共享工作。具体工作由工业和信息化部网络安全管理局(以下简称网安局)会同各相关业务司局共同开展。其中, 网安局统筹协调风险信息报送与共享工作, 各相关业务司局负责参与风险信息评估、研判、处置等工作。

第七条 地方工业和信息化主管部门负责本地区工业领域数据安全风险

信息报送与共享工作。

地方通信管理局负责本地区电信和互联网领域数据安全风险信息报送与共享工作。

第八条 工业和信息化部（网安局）组织建设、运行工业和信息化领域数据安全风险信息报送与共享平台（以下简称平台），收集、汇总数据安全风险信息，并发布、通报风险提示。

第九条 工业和信息化部选择有条件的部属单位作为支撑单位，负责运行维护平台，并支撑工业和信息化部（网安局）开展风险信息报送与共享工作。

第三章 风险信息报送

第十条 工业和信息化部（网安局）鼓励部系统各单位、安全企业、数据处理者、科研院所、行业组织等单位（以下简称风险报送单位）开展风险信息报送，遴选支撑服务能力强、技术水平高、报送信息质量优的单位建立风险直报单位名录，并实施名录动态管理。

地方工业和信息化主管部门、地方通信管理局应当组织开展本地区风险报送单位遴选、推荐等工作，建立本地区风险报送单位名录，并加强名录管理。

第十一条 风险直报单位应当通过平台直接向工业和信息化部（网安局）报送数据安全风险信息。其他风险报送单位应当通过平台及时向所在地工业和信息化主管部门、通信管理局报送掌握的工业、电信和互联网领域数据安全风险信息。

第十二条 地方工业和信息化主管部门、地方通信管理局应当组织开展本地区风险信息报送工作，审核研判本地区收到的风险信息，及时向工业和信息化部（网安局）报送涉及重要数据和核心数据的、跨地区的或者可能造成重大事件的相关风险信息，并每半年向工业和信息化部（网安局）报送风险信息报送工作总结。

第四章 风险信息研判与共享

第十三条 工业和信息化部（网安局）组织支撑单位对部级平台收到的风

险信息进行评估和研判，对于确认的风险信息开展共享和通报，达到应急标准的，应当同时启动应急预案。

支撑单位对风险信息进行分类、研判、整理，及时分析总结风险信息报送与共享情况，并向工业和信息化部（网安局）报送。

第十四条 工业和信息化部（网安局）根据数据安全风险影响范围等情况，分别开展以下风险信息共享和通报工作：

（一）对于可能影响社会公众的风险信息，可通过部网站等渠道通报；

（二）对于区域性的风险信息，通报至有关地方工业和信息化主管部门或者地方通信管理局；

（三）对于能够确定具体通报单位的，同时向该单位主体及其所在地工业和信息化主管部门或者通信管理局通报；

（四）工业和信息化部（网安局）加强数据安全态势分析，不定期通报行业数据安全情况。

第十五条 地方工业和信息化主管部门、地方通信管理局应当及时接收工业和信息化部（网安局）发送的数据安全风险信息，并指导、督促相关单位开展风险处置。应当及时研判分析本地区数据安全风险信息，并将相关信息通报至相关单位进行处置。

第十六条 数据处理者接到通报信息后，应当及时处置风险，并按要求反馈处置情况。

第五章 保障措施

第十七条 工业和信息化部（网安局）组建数据安全风险分析专家组，为风险信息报送与共享工作提供技术咨询和决策支持。

第十八条 工业和信息化部（网安局）每年对风险报送单位报送信息的数量、质量等进行评比，对表现突出的单位予以鼓励。

第十九条 地方工业和信息化主管部门、地方通信管理局、风险报送单位

应当指定风险信息报送与共享工作联络员，报工业和信息化部（网安局）备案。联络员和联络方式发生变化时，应当在 5 个工作日内报送变更情况。应当加强数据安全风险信息报送与共享工作保障，对表现突出的风险报送单位予以鼓励。

第二十条 参与风险信息报送与共享工作的相关机构和人员应当对获悉的信息承担保密义务，不得泄露或者非法向他人提供。

第二十一条 地方工业和信息化主管部门、地方通信管理局应当参照本指引，建立完善本地区工业、电信和互联网领域数据安全风险信息报送和共享工作机制。

第二十二条 本指引自发布之日起实施。

附件 1：风险信息报送模板

数据安全风险信息

xx 年 xx 月 xx 日，xx (风险报送单位) 发现 xx 公司 (风险所在单位) xx 系统存在数据安全风险。有关情况如下。

一、风险基本情况

(一) 风险类别和级别

风险类别1： 风险级别2：

(二) 风险涉及数据情况

涉及数据类型3： 涉及数据级别4：

涉及数据量： (暂时无法确定的可写暂不确定)

(三) 风险产生时间

xx 年xx 月 xx 日 (暂时无法确定的可写暂不确定)

(四) 风险范围

影响地区： 影响单位： 影响行业：

¹ 参考本指引第二条所列举的风险类型。

² 风险级别分为高危、中危、低危。其中，高危风险主要指涉及重要数据或核心数据的，或者涉及数据量大、影响区域范围广的风险，中危风险主要指涉及数据量较少、影响范围较小的风险，低危风险主要指造成轻微影响的风险。

³ 数据类型参考《工业和信息化领域数据安全管理办法（试行）》中列举的主要类型，可在此基础上进行细分类。

⁴ 数据级别包括核心数据、重要数据、一般数据。

(五) 风险概述

简要概述风险情况

(五) 其他风险相关信息

系统名称:

系统域名:

IP 地 址 :

端 口 :

风 险 URL:

IP 所属地区:

IP 所属运营商:

ICP 备案号:

二、风险分析

描述风险产生原因、发现方式、验证情况及风险后果影响, 并提供截图等证明。

三、风险处置建议

针对风险提出处置建议。

四、风险报送单位

单位名称:

联系人及联系方式:

附件 2：风险信息报送工作总结模板

数据安全风险信息报送工作总结

XX 年 XX 月至 XX 月，XX（主管部门）数据安全风险信息报送工作总结如下。

一、风险报送基本情况

（一）风险类型与级别情况

报送的风险包括数据泄露 XX 起，数据篡改 XX 起，数据滥用 XX 起，……。其中，高危风险 XX 起，中危风险 XX 起，低危风险 XX 起。

（二）风险地域分布情况

报送的风险涉及 XX 等共 XX 个城市，风险数量最多的前三位城市分别是 XX（XX 起）、XX（XX 起）、XX（XX 起）。高危风险最多的前三位城市分别是 XX（XX 起）、XX（XX 起）、XX（XX 起）。

其中，跨地区的风险有 XX 起，主要涉及 XX 等地区。

（三）风险行业分布情况

报送的风险涉及 XX 等共 XX 个行业，风险数量最多的前三位行业分别是 XX（XX 起）、XX（XX 起）、XX（XX 起）。高危风险最多的前三位行业分别是 XX（XX 起）、XX（XX 起）、XX（XX 起）。

（四）风险涉及数据情况

报送的风险涉及 XX 等数据类型。其中，涉及 XX 类的有 XX 起，……，涉及 XX 类的有 XX 起；涉及核心数据的有 XX 起，涉及重要数据的有 XX 起，涉及一般数据的有 XX 起。已研判确定存在风险的数据量是 XX。

（五）风险通报处置情况

已通报 XX 家企业进行风险处置，XX 家已完成处置。

二、存在的问题

三、下一步工作计划及建议

附件：风险报送与处置情况汇总表

序号	风险报送 时间	风险名称	风险类别 与级别	风险所在 单位	风险处置 情况	风险报送 单位

附件 3

工业和信息化领域数据安全风险报送单位申报要求

申报工业和信息化领域数据安全风险报送单位,应当符合 下列基本条件:

一、在中华人民共和国境内注册成立,取得独立法人资格; 二、遵守中华人民共和国法律法规和相关规定,在信用中

国的查询信息中无不良记录,5年内无违法违规记录,对国家安全、社会秩序、公共利益不构成威胁;

三、注册资金在 500 万元人民币以上,组织管理结构和产权关系明晰,独立经营核算;

四、从事数据安全相关工作 3 年以上,在工业、电信和互联网数据安全领域有一定的综合实力和技术优势,有固定的场所和必要的设施,具备必要的数据安全风险发现、分析、研判、处置等技术能力和业务积累;

五、具有 2 年以上数据安全相关工作经历的技术团队人员不少于 20 人,其中取得数据安全、网络安全、计算机等相关专业资质证书的人员不少于 10 人,相关人员 5 年内无违法违规记录;

六、支持提供 7×24 小时风险研判、应急处置等相关服务;

七、自愿签订承诺书,严格遵守相关要求。自觉接受工业和信息化部(网络安全管理局)监督和指导。发生违法违规行为或违约行为的,将自动撤销风险报送单位资格,5 年内不得重新申请。

附件 4

工业和信息化领域数据安全风险报送单位承诺书

工业和信息化部网络安全管理局：

我单位申报工业和信息化领域数据安全风险报送单位，严格遵守相关工作要求，并自愿作出以下承诺：

一、不以非法方式开展数据安全风险监测、检测等工作；二、不以非法方式收集数据安全相关风险信息；

三、及时报送所发现的数据安全风险，未经主管部门确认，不得擅自披露风险；

四、对报送信息的客观性、准确性、真实性、完整性负责；五、对报送信息内容负有保密责任，所报送的信息内容不

涉及国家秘密、个人隐私信息和其他敏感信息；

六、支持提供 7×24 小时风险研判、应急处置等相关服务；七、存在责任落实不到位、造成重大安全事件、严重违法

违规等行为的，将妥善处理善后事宜。

我单位对违反上述承诺导致的后果承担全部法律责任。

单位负责人：

(加盖公章)

xx 年 xx 月 xx 日

(三十四) 中国银保监会关于印发监管数据安全管理办法（试行）的通知

(银保监发〔2020〕43号)

各银保监局，机关各部门，各会管单位：

为切实加强监管数据安全管理工作，防范监管数据安全风险，我会制定了《中国银保监会监管数据安全管理办法（试行）》，现予以印发，请遵照执行。

2020年9月23日

第一章 总 则

第一条 为规范银保监会监管数据安全管理工作，提高监管数据安全保护能力，防范监管数据安全风险，依据《中华人民共和国网络安全法》《中华人民共和国银行业监督管理法》《中华人民共和国保险法》《工作秘密管理暂行办法》等法律法规及有关规定，制定本办法。

第二条 本办法所称监管数据是指银保监会在履行监管职责过程中，依法定期采集，经监管信息系统记录、生成和存储的，或经银保监会各业务部门认定的数字、指标、报表、文字等各类信息。

本办法所称监管信息系统是指以满足监管需求为目的开发的，具有数据采集、处理、存储等功能的信息系统。

第三条 本办法所称监管数据安全是指监管数据在采集、处理、存储、使用等活动（以下简称监管数据活动）中，处于可用、完整和可审计状态，未发生泄露、篡改、损毁、丢失或非法使用等情况。

第四条 银保监会及受托机构开展监管数据活动，适用本办法。

本办法所称受托机构是指受银保监会委托或委派，为银保监会提供监管数据采集、处理或存储服务的企事业单位。

第五条 开展监管数据活动，必须遵守相关法律法规。任何单位和个

人对在监管数据活动中知悉的国家秘密、工作秘密、商业秘密和个人信息，应当依照相关规定予以保密。

第六条 银保监会建立健全监管数据安全协同管理体系，推动银保监会有关业务部门、各级派出机构、受托机构等共同参与监管数据安全保护工作，加强培训教育，形成共同维护监管数据安全的良好环境。

第二章 工作职责

第七条 监管数据安全实行归口管理，建立统筹协调、分工负责的管理机制。

银保监会统计信息部门是归口管理部门，负责统筹监管数据安全管理工作。银保监会各业务部门负责本部门监管数据安全管理工作。

第八条 归口管理部门具体职责包括：

- （一）制定监管数据安全工作规则和管理流程；
- （二）制定监管数据安全技术防护措施；
- （三）组织实施监管数据安全评估和监督检查。

第九条 各业务部门具体职责包括：

- （一）规范本部门监管数据安全使用，明确具体工作要求，落实相关责任；
- （二）组织开展本部门监管数据安全管理工作；
- （三）协助归口管理部门实施监管数据安全监督检查。

第三章 监管数据采集、存储和加工处理

第十条 监管数据的采集应按照安全、准确、完整和依法合规的原则进行，避免重复、过度采集。

第十一条 监管数据应通过监管工作网或金融专网进行传输。因客观条件限制需要通过物理介质、互联网或其它网络传输的，应经归口管理部门评估同意。

第十二条 监管数据应存储在银保监会机房，并具有完备的备份措施。确有

必要存储在受托机构机房的，应经归口管理部门评估同意。

第十三条 监管数据存储期限、存储介质管理应按照国家 and 银保监会有关规定执行。

第十四条 监管数据的加工处理应在监管工作权限或受托范围内进行。未经归口管理部门同意，任何单位和个人不得将代码、接口、算法模型和开发工具等接入监管信息系统。

第十五条 监管数据采集、传输、存储、加工处理、转移交换、销毁，以及用于系统开发测试等活动，应根据监管数据类型和管理要求采取分级分类安全防护措施。

第四章 监管数据使用

第十六条 监管数据仅限于银保监会履行监管工作职责使用。纪检监察、司法、审计等党政机关为履行工作职责需要使用监管数据时，按照有关规定办理。

第十七条 监管数据的使用行为应通过管理和技术手段确保可追溯。监管数据用于信息系统开发测试以及对外展示时，应经过脱敏处理。

第十八条 使用未公开披露的监管数据，原则上应在不可连接互联网的台式机或笔记本等银保监会工作机中进行。因客观条件限制需采取虚拟专用网络等方式使用监管数据时，应经归口管理部门评估同意。

第十九条 因工作需要下载的监管数据，仅可存储于银保监会的工作机中。承载监管数据的使用介质应妥善保管，防止数据泄露。

第二十条 在使用监管数据过程中产生的加工数据、汇总结果等信息应视同监管数据进行安全管理。

第二十一条 监管数据对外披露应由指定业务部门按照有关规定和流程实施。

第二十二条 各业务部门因工作需要向非党政机关单位、个人提供监管数据时，应充分评估数据安全风险，经本部门主要负责人同意后实施，必要时与对方

签订备忘录和保密协议并报归口管理部门备案。

与境外监管机构或国际组织共享监管数据时，应由国际事务部门依照银保监会签署的监管合作谅解备忘录、合作协议等约定或其他有关工作安排进行管理。

法律法规另有规定的，从其规定。

第二十三条 各业务部门因工作需要和系统下线停用监管数据时，应及时对其采取封存或销毁措施。

第五章 监管数据委托服务管理

第二十四条 各业务部门监管数据采集涉及受托机构提供服务时，应事先与归口管理部门沟通并会签同意。受托机构的技术服务方案，应通过归口管理部门的安全评估。技术服务方案发生变更的，应事先报归口管理部门进行安全评估。

安全评估不通过的，不得开展委托服务或建立委派关系。

第二十五条 为银保监会提供监管数据服务的受托机构，应满足以下基本条件：

（一）具备从事监管数据工作所需系统的自主研发及运维能力；

（二）具备相关信息安全管理资质认证；

（三）拥有自主产权或已签订长期租赁合同的机房；

（四）网络和信息系統具备有效的安全保护和稳定运行措施，三年内未发生网络安全重大事件；

（五）具备有效的监管数据安全保护措施，能够保障银保监会各部门对监管数据的访问和控制；

（六）具有监管数据备份体系、应急组织体系和业务连续性计划。

第二十六条 银保监会通过与受托机构签订协议，确立监管数据委托服务关系。协议应明确服务项目、期限、安全管理责任和终止事由等内容。

银保监会通过委派方式确立监管数据服务关系的，应下达委派任务书。

第二十七条 因有关政策调整导致原委托或委派事项无需继续履行，或发现受托机构监管数据服务出现重大安全问题的，银保监会有权终止委托或委派关系。

委托或委派关系终止时，受托机构应及时、完整地移交监管数据，并销毁因委托或委派事项而获取的监管数据，不得保留相关数据备份等内容。

第六章 监督管理

第二十八条 各业务部门及受托机构应按照监管数据安全工作规则定期开展自查，发现监管数据安全缺陷、漏洞等风险时，应立即采取补救措施。

第二十九条 归口管理部门应定期对各业务部门及受托机构开展监管数据安全评估检查工作。

各业务部门及受托机构对于评估和检查中发现的问题应制定整改措施，及时整改，并向归口管理部门报送整改报告。

第三十条 各业务部门及受托机构发生以下监管数据重大安全风险事项时，应立即采取应急处置措施，及时消除安全隐患，防止危害扩大，并于48小时内向归口管理部门报告。

- (一) 监管数据发生泄露或非法使用；
- (二) 监管数据发生损毁或丢失；
- (三) 承载监管数据的信息系统或网络发生系统性故障造成服务中断4小时以上；
- (四) 承载监管数据的信息系统或网络遭受非法入侵、发生有害信息或计算机病毒的大规模传播等破坏；
- (五) 监管数据安全事件引发舆情；
- (六) 《网络安全重大事件判定指南》列明的其他影响监管数据安全的网络安全重大事件。

辖区发生以上监管数据重大安全风险事项时，各银保监局应立即采取补救措

施，并于48小时内向银保监会归口管理部门报告。

第三十一条 归口管理部门应建立监管数据安全事件通报工作机制，及时通报监管数据安全事件。

第七章 附 则

第三十二条 涉密监管数据按照国家和银保监会保密管理有关规定进行管理。

第三十三条 各银保监局承担辖区监管数据安全管理工作，参照本办法制定辖区监管数据安全管理办法，明确职责和管理要求，强化监管数据安全保护。

第三十四条 本办法自印发之日起施行。

六、行业规范

(一) 应用商店 App 个人信息收集使用上架审核和管理规范（征求意见稿）

1 范围

应用商店、应用市场、分发网站等分发平台运营者对申请上架的移动应用程序收集使用个人信息的合规性审核以及日常管理，小程序、快应用、H5 页面等新业态网络应用程序的分发、接入平台运营者对所分发和接入的应用程序进行个人信息处理行为规范性审核和安全管理，（以下称“平台运营者”）适用本标准。

2 审核管理规则

平台运营者应当依照有关法律法规、国家标准的强制性要求以及本标准，制定、公开移动应用程序个人信息处理行为审核管理规则，并为移动应用程序开发者和社会公众提供便捷获取的途径。

3 开发者基本信息审核

平台运营者在受理移动应用程序进入平台的申请时，应当要求开发者至少提交并核实以下信息：

- a) 移动应用程序的名称、包名、版本号、更新日期、基本功能服务等基本信息；
- b) 移动应用程序开发者的姓名或者名称、个人信息保护负责人或者机构的联系方式；
- c) 用户隐私协议全文文本，涉及为儿童提供服务的，还宜提交单独的儿童个人信息保护协议；
- d) 开发者未提供上述信息或者提供虚假信息的，平台运营者应当拒绝其移

动应用程序上架。

4 隐私协议审核

隐私协议有下列情形之一的，平台运营者应当拒绝移动应用程序进入本平台：

- a) 未提示用户阅读隐私协议；
- b) 以默认选择同意隐私协议的方式征求用户意见；
- c) 未完整、详细、逐项列出收集的个人信息类别、说明收集的必要性、实现的服务或使用目的；
- d) 未完整、详细、逐项说明申请权限所实现的服务或使用目的、用户能否拒绝授权、不可拒绝的理由；
- e) 未完整、详细、逐项列出嵌入的 SDK 名称、包名、开发者名称、嵌入目的、收集的个人信息类型、使用的系统权限；
- f) 隐私协议中存在免除个人信息保护相关主要义务、排除用户主要个人信息权益等不合理情形。

5 申请和调用权限审核

移动应用程序申请或者调用权限，有下列情形之一的，平台运营者应当拒绝移动应用程序进入本平台：

- a) 在用户未使用任何功能时（如：App 启动过程中）申请或者调用权限；
- b) 在用户使用功能过程中，申请或者调用与实现当前功能无关的权限；
- c) 因用户不同意打开非必要权限而拒绝提供服务；
- d) 在用户拒绝打开非必要权限后，频繁征求用户同意，干扰用户正常使用；
- e) 在申请权限时，未同步告知用户其目的，或者告知的目的与实际情况不

符;

- f) 仅以改善服务质量、提升用户体验、定向推送信息、研发新产品等非功能性需求为由，强制要求用户打开权限。

6 个人信息处理行为审核

移动应用程序收集使用个人信息，有下列情形之一的，平台运营者应当拒绝移动应用程序进入本平台：

- a) 以捆绑多项功能、捆绑必要与非必要个人信息等方式，诱导、强迫用户一次性授权同意个人信息处理规则，例如进入App 或注册登录时强制要求用户同意隐私协议全部条款；
- b) 收集的个人信息超出实现功能的最小必要范围，包括收集个人信息的类型、频率、数量、方式、精度、场景等；
- c) 因用户不同意收集非必要个人信息而拒绝提供服务；
- d) 未经用户自主选择，默认开启非基本功能服务收集个人信息；
- e) 在用户拒绝收集非必要个人信息后，频繁征求用户同意，干扰用户正常使用；
- f) 在收集敏感个人信息时，未向用户同步告知其目的；
- g) 仅以改善服务质量、提升用户体验、定向推送信息、研发新产品等非功能性需求为由，强制要求用户同意收集个人信息；
- h) 收集了个人信息但未提供声称的功能；
- i) 未向用户提供有效的查询、更正、删除以及撤回同意收集个人信息的途径；
- j) 具有定向推送信息功能的，未向用户提供关闭定向推送信息的选项；
- k) 具有注册账号功能的，未提供有效的用户账号注销功能，或者为注销用户账号设置不必要或者不合理条件。

7 审核记录与异议反馈

平台运营者应当建立移动应用程序审核记录档案，记录移动应用程序未通过审核的原因，并为移动应用程序开发者提供意见反馈渠道。

8 存量移动应用程序审核与管理

平台运营者应当对存量移动应用程序首次版本更新时按照上述要求进行审核，审核不通过的应当将其从平台中清退。

移动应用程序在本标准发布后 180 日内未进行更新的，平台运营者应当通知其在 30 日内重新申请

进入平台。未在规定期限内进行申请的，平台经营者应当在 7 日内将其从平台中清退。

9 版本更新审核

移动应用程序更新版本涉及个人信息处理活动发生明显变化的，如打开的可收集个人信息权限发生变更、收集范围或者目的发生变化，以及其他对用户个人信息权益造成影响的，平台运营者应当依照进入平台程序对其进行审核。

10 个人信息处理公示

平台运营者应当在下载页面清晰、全面地展示移动应用程序收集使用个人信息的下列情况：

- a) 移动应用程序的基本服务类型、开发者名称、官方网站链接、个人信息保护机构或者负责人的联系电话和邮箱；
- b) 隐私协议；
- c) 收集个人信息的具体类别、所实现业务功能或使用目的；
- d) 系统权限名称、所实现业务功能或使用目的；

- e) 嵌入的 SDK 名称、所实现业务功能或使用目的、收集个人信息类型和使用的系统权限;
- f) 移动应用程序曾用名称;
- g) 平台运营者及有关监管部门的个人信息问题投诉、举报渠道。

11 个人信息安全标识

平台运营者应当通过设置不同颜色、形状图标等方式对移动应用程序的个人信息收集使用情况进行显著标识, 可提供的标识包括但不限于:

- a) 对移动应用程序收集个人信息类型数量、申请系统权限数量进行显著标识;
- b) 对有关部门发布的, 涉及政务和民生领域的移动应用程序标识“官方”字样, 并在用户搜索时 优先展示;
- c) 向移动应用程序开发者提供用户年龄群体标识选择功能。面向儿童服务的移动应用程序, 用户点击标识后展示儿童隐私保护协议。

12 个人信息安全管理

平台运营者应当采取下列措施指导督促移动应用程序开发者提升个人信息保护的意识和能力, 确保审核工作公平公正:

- a) 对移动应用程序开发者进行个人信息保护方面的知识和技能培训, 督促移动应用程序开发者加强安全责任意识;
- b) 确保移动应用程序审核流程、审核标准、展示样式等的一致性, 不得根据开发者身份、市场地位等因素区别对待;
- c) 建立移动应用程序开发者信用档案, 对其产品频繁出现个人信息收集使用问题的开发者, 及时进行警告, 并向消费者发布个人信息安全警示; 对产品被有关监管部门通报 5 次以上或者下架3 次以上的开发者, 5 年内不得从事移动应用程序开发和运营。

13 违法违规移动应用程序处理

平台运营者应当采取下列措施，处理用户反映和有关主管部门通报的个人信息收集使用问题：

- a) 对用户举报的本平台移动应用程序违法违规收集使用个人信息的问题，在 5 个工作日内向用户回复受理情况；
- b) 经核验用户反映问题属实的，督促移动应用程序开发者在 15 个工作日内进行整改，拒不整改或者未在规定时间内按照要求整改的，将其清退；
- c) 对有关监管部门认定存在违法违规收集使用个人信息的移动应用程序，配合采取督促整改、清退等措施；
- d) 每季度对移动应用程序审核情况、问题移动应用程序处置情况进行汇总分析，并报告所在地省级网信部门。

(二) 移动智能端个人信息保护指南（征求意见稿）

1 敏感权限调用提示

移动应用程序前后台使用麦克风、摄像头、位置等敏感权限时，移动智能终端在屏幕特定位置持续、显著地提示用户。用户点击提示标识时，移动智能终端展示正在使用敏感权限的移动应用程序名称，并为用户提供权限调整功能。

2 敏感操作行为提示

移动应用程序前后台读取剪切板、通讯录、短信、通话记录、日历、设备、行为信息、应用列表、系统相册以及读取或者删除其他移动应用程序私有存储目录文件等进行敏感操作或者调用敏感权限时，移动智能终端采取有效措施向用户提示上述敏感操作行为。

用户安装来源不明移动应用程序时，移动智能终端向用户提醒可能存在的风险及其规避风险的措施。

3 提示设置

移动智能终端应当就敏感权限调用提示和敏感操作行为提示提供便捷设置途径。移动智能终端操作系统默认开启提示功能，用户可自主选择关闭提示功能，并可针对每项敏感权限和操作单独设置。

4 访问控制措施

移动智能终端应当依照最小必要原则，按照下列要求提供细粒度数据访问控制措施，强化用户对个人信息控制能力：

- a) 在无需开启“存储”等权限的情况下，用户可以直接选取允许移动应用程序访问的照片、音视频等；
- b) 在无需开启“通讯录”权限的情况下，用户可以直接选取允许移动应用程序访问的特定联系人；

c) 移动应用程序读取地理位置时，向用户提供精确位置和粗略位置选项；

d) 在无需开启“读取通话记录”权限的情况下，用户可以直接选取允许移动应用程序访问的通话记录。

5 自启动行为控制

移动智能终端应当将移动应用程序自启动、被关联启动功能默认设置为关闭状态。在移动应用程序首次自启动、关联启动其他应用时弹窗提示用户，并为用户提供是否同意开启该功能的选项。

6 设备识别码控制

移动智能终端应当通过以下途径为用户提供便捷的设备识别码控制功能：

支持用户手动重置设备识别码或者提供设备识别码随机化的机制；

a) 提供设备识别码定期自动重置功能；

b) 提供是否允许移动应用程序读取设备识别码并用于追踪目的的选项，并将其设置为默认关闭状态；

c) 禁止 App 获取不可变更的设备识别码，如 MAC 地址、手机 IMEI 号等。

7 权限控制

移动智能终端应当遵循最小必要原则，为用户提供便捷的细粒度权限控制功能：

a) 位置、摄像头、麦克风、通讯录、短信、日历等敏感权限为用户提供“单次授权”选项；

b) 除位置、摄像头、麦克风、通讯录、短信、日历权限为移动应用程序提供服务所必需外，不得为用户提供“始终允许”的授权方

式;

c) 将读取应用程序列表、剪切板、手机号码、照片附加信息、行为信息以及屏幕截图等权限默认设置为拒绝或者关闭状态, 在开启时需要单独获得用户明确同意, 并向用户提供“仅使用期间允许、单次授权、拒绝”多种控制选项。

8 敏感权限自动重置

移动智能终端应当将用户 3 个月内未使用的移动应用程序开启的敏感系统权限重置为禁止状态, 并为用户提供手动关闭自动重置功能的选项。

9 存储空间管理

移动智能终端应当采取有效措施, 将移动应用程序对存储空间的访问范围限定在私有存储目录的文件以及用户授权的公共存储区文件, 并禁止移动应用程序将私有存储目录中的文件设置为全局可访问。

10 个人信息处理记录和展示

移动智能终端应当记录并展示移动应用程序收集使用敏感个人信息行为, 并为用户提供便捷的查询途径, 记录和展示的行为包括:

- a) 移动应用程序调用位置、通讯录、公共存储区、录音、拍摄、读取短信、通话记录、行为信息、日历、设备信息等敏感系统权限的行为;
- b) 自启动、关联启动和被关联启动的行为;
- c) 读取应用程序列表、剪切板、屏幕截图、系统相册等其他获取敏感个人信息的行为。

移动智能终端记录、保存使用上述权限和行为的次数、具体时间, 保存期限不少于 7 天, 并允许用户自行设置保存期限。

11 预装移动应用程序个人信息处理记录和展示

移动智能终端预装移动应用程序的敏感行为和系统权限控制机制应当与第三方移动应用程序保持一致，不得为预装移动应用程序进行默认授权或者削减安全管理措施。

● 关于国瓴

“国之重器，高屋建瓴。不忽细微，善于解剖，必有证据。”国瓴律师事务所是一家由上海交通大学凯原法学院校友发起创立，致力于科技改变法律、让“律师成为守护庭院的最后一道篱笆”“在法律中寻获时代问题答案”“为伙伴创造价值”的精品律师事务所。

国瓴律师事务所设有“国瓴研究院”和“上海交通大学凯原法学院国瓴公益基金”。

在资本市场和非资本市场领域，在民法典时代和互联网时代，国瓴律师深耕产业，教学相长，提供专业化、跨界化、本土化、国际化复杂问题解决方案，为企业上市、并购重组、数据与知识产权、合规与股权激励、私募股权、银行保险与大资管、婚姻家庭与家族信托、不良资产处置、争议解决、刑事辩护等法律领域提供智慧解决方案。

上海市秀文路898号西子国际中心2号楼3层 邮编：201199

上海市华山路1389弄14号 邮编：200030

电话 (Tel) : 86-21-33883626 传真 (Fax) : 86-21-34127367 网址 (Website) www.guolinglaw.com

