数据合规常用法律法规汇编

广州市律师协会
第十届民事法律专业委员会 编

二〇二二年一月

广州市律师协会第十届民事法律专业委员会
业务指引编撰工作小组

组　长：宋万俊

副组长：官金福　张小伟

成　员：林传富　李洁彬　闫丰华　赵琦娴　许杰民　曾雅妮　余玮玮
李燕玲　王旭虹　张雄敬　邓雪萍　杨莉　周凤婷

本编分工：

编　撰：李燕玲 王旭虹

审　稿：张雄敬 杨衡波

前　言

近年来，随着频频发生的企业因合规问题被严厉处罚的事件，标志着我国已然步入“数据合规大时代”，数据合规法律服务业务已成业界关注热点。2017 年《中华人民共和国网络安全法》施行，2021 年两部数据领域核心法律《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》出台，各层面数据立法全面启动，监管部门配套政策、各项国家标准也陆续推出。在此之际，广州市律师协会第十届民事法律专业委员会整理编辑了《数据合规法律法规汇编》，供广大企业法务部门、广大律师同行检索使用。

《数据合规法律法规汇编》全文超过 40 万字，包括了法律法规、行政法规、部门规章及规范性文件、司法解释、国家及行业标准共五大部分内容，基本保证了适用的数据法律法规相关文件的收录。若能籍此为广大企业合规、稳健发展提供帮助，为律师同行进行相关法律业务提供支持，即已达成编辑此法律法规汇编之初衷。

广州市律师协会第十届民事法律专业委员会

2022 年 1 月 28 日

目　录

一、法律法规

中华人民共和国个人信息保护法

时效性：　现行有效

发文机关：　全国人大常委会

文号：　主席令第九十一号

发文日期：　2021 年 08 月 20 日

施行日期：　2021 年 11 月 01 日

第一章　总　则

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

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

第三条　在中华人民共和国境内处理自然人个人信息的活动，适用本法。

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

（一）以向境内自然人提供产品或者服务为目的；

（二）分析、评估境内自然人的行为；

（三）法律、行政法规规定的其他情形。

第四条　个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。

个人信息的处理包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等。

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

第六条　处理个人信息应当具有明确、合理的目的，并应当与处理目的直接相关，采取对个人权益影响最小的方式。

收集个人信息，应当限于实现处理目的的最小范围，不得过度收集个人信息。

第七条　处理个人信息应当遵循公开、透明原则，公开个人信息处理规则，明示处理的目的、方式和范围。

第八条　处理个人信息应当保证个人信息的质量，避免因个人信息不准确、不完整对个人权益造成不利影响。

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

第十条　任何组织、个人不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开他人个人信息；不得从事危害国家安全、公共利益的个人信息处理活动。

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

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

第二章　个人信息处理规则

第一节　一般规定

第十三条　符合下列情形之一的，个人信息处理者方可处理个人信息：

（一）取得个人的同意；

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

所必需；

（三）为履行法定职责或者法定义务所必需；

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

（五）为公共利益实施新闻报道、舆论监督等行为，在合理的范围内处理个人信息；

（六）依照本法规定在合理的范围内处理个人自行公开或者其他已经合法公开的个人信息；

（七）法律、行政法规规定的其他情形。

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

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

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

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

个人撤回同意，不影响撤回前基于个人同意已进行的个人信息处理活动的效力。

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

产品或者服务所必需的除外。

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

（一）个人信息处理者的名称或者姓名和联系方式；

（二）个人信息的处理目的、处理方式，处理的个人信息种类、保存期限；

（三）个人行使本法规定权利的方式和程序；

（四）法律、行政法规规定应当告知的其他事项。

前款规定事项发生变更的，应当将变更部分告知个人。

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

第十八条　个人信息处理者处理个人信息，有法律、行政法规规定应当保密或者不需要告知的情形的，可以不向个人告知前条第一款规定的事项。

紧急情况下为保护自然人的生命健康和财产安全无法及时向个人告知的，个人信息处理者应当在紧急情况消除后及时告知。

第十九条　除法律、行政法规另有规定外，个人信息的保存期限应当为实现处理目的所必要的最短时间。

第二十条　两个以上的个人信息处理者共同决定个人信息的处理目的和处理方式的，应当约定各自的权利和义务。但是，该约定不影响个人向其中任何一个个人信息处理者要求行使本法规定的权利。

个人信息处理者共同处理个人信息，侵害个人信息权益造成损害

的，应当依法承担连带责任。

第二十一条　个人信息处理者委托处理个人信息的，应当与受托人约定委托处理的目的、期限、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与协助。

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

第三章　个人信息跨境提供的规则

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

（一）依照本法第四十条的规定通过国家网信部门组织的安全评估；

（二）按照国家网信部门的规定经专业机构进行个人信息保护认证；

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

（四）法律、行政法规或者国家网信部门规定的其他条件。

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

（一）处理目的已实现、无法实现或者为实现处理目的不再必要；

（二）个人信息处理者停止提供产品或者服务，或者保存期限已届满；

（三）个人撤回同意；

（四）个人信息处理者违反法律、行政法规或者违反约定处理个人信息；

（五）法律、行政法规规定的其他情形。

法律、行政法规规定的保存期限未届满，或者删除个人信息从技

术上难以实现的，个人信息处理者应当停止除存储和采取必要的安全保护措施之外的处理。

第四十八条　个人有权要求个人信息处理者对其个人信息处理规则进行解释说明。

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

第五十条　个人信息处理者应当建立便捷的个人行使权利的申请受理和处理机制。拒绝个人行使权利的请求的，应当说明理由。

个人信息处理者拒绝个人行使权利的请求的，个人可以依法向人民法院提起诉讼。

第五章　个人信息处理者的义务

第五十一条　个人信息处理者应当根据个人信息的处理目的、处理方式、个人信息的种类以及对个人权益的影响、可能存在的安全风险等，采取下列措施确保个人信息处理活动符合法律、行政法规的规定，并防止未经授权的访问以及个人信息泄露、篡改、丢失：

（一）制定内部管理制度和操作规程；

（二）对个人信息实行分类管理；

（三）采取相应的加密、去标识化等安全技术措施；

（四）合理确定个人信息处理的操作权限，并定期对从业人员进行安全教育和培训；

（五）制定并组织实施个人信息安全事件应急预案；

（六）法律、行政法规规定的其他措施。

第五十二条　处理个人信息达到国家网信部门规定数量的个人信息处理者应当指定个人信息保护负责人，负责对个人信息处理活动以及采取的保护措施等进行监督。

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

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

第五十四条　个人信息处理者应当定期对其处理个人信息遵守法律、行政法规的情况进行合规审计。

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

（一）处理敏感个人信息；

（二）利用个人信息进行自动化决策；

（三）委托处理个人信息、向其他个人信息处理者提供个人信息、公开个人信息；

（四）向境外提供个人信息；

（五）其他对个人权益有重大影响的个人信息处理活动。

第五十六条　个人信息保护影响评估应当包括下列内容：

（一）个人信息的处理目的、处理方式等是否合法、正当、必要；

（二）对个人权益的影响及安全风险；

（三）所采取的保护措施是否合法、有效并与风险程度相适应。

个人信息保护影响评估报告和处理情况记录应当至少保存三年。

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

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

（二）个人信息处理者采取的补救措施和个人可以采取的减轻危害的措施；

（三）个人信息处理者的联系方式。

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

第五十八条　提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者，应当履行下列义务：

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

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

（三）对严重违反法律、行政法规处理个人信息的平台内的产品

或者服务提供者，停止提供服务；

（四）定期发布个人信息保护社会责任报告，接受社会监督。

第五十九条　接受委托处理个人信息的受托人，应当依照本法和有关法律、行政法规的规定，采取必要措施保障所处理的个人信息的安全，并协助个人信息处理者履行本法规定的义务。

第六章　履行个人信息保护职责的部门

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

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

前两款规定的部门统称为履行个人信息保护职责的部门。

第六十一条　履行个人信息保护职责的部门履行下列个人信息保护职责：

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

（二）接受、处理与个人信息保护有关的投诉、举报；

（三）组织对应用程序等个人信息保护情况进行测评，并公布测评结果；

（四）调查、处理违法个人信息处理活动；

（五）法律、行政法规规定的其他职责。

第六十二条　国家网信部门统筹协调有关部门依据本法推进下

列个人信息保护工作：

（一）制定个人信息保护具体规则、标准；

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

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

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

（五）完善个人信息保护投诉、举报工作机制。

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

（一）询问有关当事人，调查与个人信息处理活动有关的情况;

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

（三）实施现场检查，对涉嫌违法的个人信息处理活动进行调查;

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

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

第六十四条　履行个人信息保护职责的部门在履行职责中，发现

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

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

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

履行个人信息保护职责的部门应当公布接受投诉、举报的联系方式。

第七章　法律责任

第六十六条　违反本法规定处理个人信息，或者处理个人信息未履行本法规定的个人信息保护义务的，由履行个人信息保护职责的部门责令改正，给予警告，没收违法所得，对违法处理个人信息的应用程序，责令暂停或者终止提供服务；拒不改正的，并处一百万元以下罚款；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

有前款规定的违法行为，情节严重的，由省级以上履行个人信息保护职责的部门责令改正，没收违法所得，并处五千万元以下或者上一年度营业额百分之五以下罚款，并可以责令暂停相关业务或者停业

整顿、通报有关主管部门吊销相关业务许可或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款，并可以决定禁止其在一定期限内担任相关企业的董事、监事、高级管理人员和个人信息保护负责人。

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

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

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

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

前款规定的损害赔偿责任按照个人因此受到的损失或者个人信息处理者因此获得的利益确定;个人因此受到的损失和个人信息处理者因此获得的利益难以确定的，根据实际情况确定赔偿数额。

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

第七十一条　违反本法规定，构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

第八章　附　则

第七十二条　自然人因个人或者家庭事务处理个人信息的，不适用本法。

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

第七十三条　本法下列用语的含义：

（一）个人信息处理者，是指在个人信息处理活动中自主决定处理目的、处理方式的组织、个人。

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

（三）去标识化，是指个人信息经过处理，使其在不借助额外信息的情况下无法识别特定自然人的过程。

（四）匿名化，是指个人信息经过处理无法识别特定自然人且不能复原的过程。

第七十四条　本法自2021年11月1日起施行。

中华人民共和国数据安全法

时效性：　现行有效

发文机关：　全国人大常委会

文号：　主席令第八十四号

发文日期：　2021年06月10日

施行日期：　2021年09月01日

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法，由中央军事委员会依据

本法另行制定。

第五十五条　本法自2021年9月1日起施行。

中华人民共和国民法典（节选）

时效性：　　现行有效

发文机关：　全国人民代表大会

文号：　　主席令第 45 号

发文日期：　2020 年 05 月 28 日

施行日期：　2021 年 01 月 01 日

第四编　人格权

第一章　一般规定

第九百八十九条　【人格权编的调整范围】本编调整因人格权的享有和保护产生的民事关系。

第九百九十条　【人格权类型】人格权是民事主体享有的生命权、身体权、健康权、姓名权、名称权、肖像权、名誉权、荣誉权、隐私权等权利。

除前款规定的人格权外，自然人享有基于人身自由、人格尊严产生的其他人格权益。

第九百九十一条　【人格权受法律保护】民事主体的人格权受法律保护，任何组织或者个人不得侵害。

第九百九十二条　【人格权禁止性规定】人格权不得放弃、转让或者继承。

第九百九十三条　【人格利益的许可使用】民事主体可以将自己的姓名、名称、肖像等许可他人使用，但是依照法律规定或者根据其性质不得许可的除外。

第九百九十四条　【死者人格利益保护】死者的姓名、肖像、名誉、荣誉、隐私、遗体等受到侵害的，其配偶、子女、父母有权依法请求行为人承担民事责任；死者没有配偶、子女且父母已经死亡的，其他近亲属有权依法请求行为人承担民事责任。

第九百九十五条　【人格权保护的请求权】人格权受到侵害的，受害人有权依照本法和其他法律的规定请求行为人承担民事责任。受害人的停止侵害、排除妨碍、消除危险、消除影响、恢复名誉、赔礼道歉请求权，不适用诉讼时效的规定。

第九百九十六条　【人格权责任竞合下的精神损害赔偿】因当事人一方的违约行为，损害对方人格权并造成严重精神损害，受损害方选择请求其承担违约责任的，不影响受损害方请求精神损害赔偿。

第九百九十七条　【人格权行为禁令】民事主体有证据证明行为人正在实施或者即将实施侵害其人格权的违法行为，不及时制止将使其合法权益受到难以弥补的损害的，有权依法向人民法院申请采取责令行为人停止有关行为的措施。

第九百九十八条　【认定行为人承担责任时的考量因素】认定行为人承担侵害除生命权、身体权和健康权外的人格权的民事责任，应当考虑行为人和受害人的职业、影响范围、过错程度，以及行为的目的、方式、后果等因素。

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

责任。

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

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

第一千零一条　【身份权的法律适用】对自然人因婚姻家庭关系等产生的身份权利的保护，适用本法第一编、第五编和其他法律的相关规定；没有规定的，可以根据其性质参照适用本编人格权保护的有关规定。

第二章　生命权、身体权和健康权

第一千零二条　【生命权】自然人享有生命权。自然人的生命安全和生命尊严受法律保护。任何组织或者个人不得侵害他人的生命权。

第一千零三条　【身体权】自然人享有身体权。自然人的身体完整和行动自由受法律保护。任何组织或者个人不得侵害他人的身体权。

第一千零四条　【健康权】自然人享有健康权。自然人的身心健康受法律保护。任何组织或者个人不得侵害他人的健康权。

第一千零五条　【法定救助义务】自然人的生命权、身体权、健康权受到侵害或者处于其他危难情形的，负有法定救助义务的组织或者个人应当及时施救。

第一千零六条　【人体捐献】完全民事行为能力人有权依法自主决

定无偿捐献其人体细胞、人体组织、人体器官、遗体。任何组织或者个人不得强迫、欺骗、利诱其捐献。

完全民事行为能力人依据前款规定同意捐献的，应当采用书面形式，也可以订立遗嘱。

自然人生前未表示不同意捐献的，该自然人死亡后，其配偶、成年子女、父母可以共同决定捐献，决定捐献应当采用书面形式。

第一千零七条　【禁止买卖人体细胞、组织、器官和遗体】禁止以任何形式买卖人体细胞、人体组织、人体器官、遗体。

违反前款规定的买卖行为无效。

第一千零八条　【人体临床试验】为研制新药、医疗器械或者发展新的预防和治疗方法，需要进行临床试验的，应当依法经相关主管部门批准并经伦理委员会审查同意，向受试者或者受试者的监护人告知试验目的、用途和可能产生的风险等详细情况，并经其书面同意。

进行临床试验的，不得向受试者收取试验费用。

第一千零九条　【从事人体基因、胚胎等医学和科研活动的法定限制】从事与人体基因、人体胚胎等有关的医学和科研活动，应当遵守法律、行政法规和国家有关规定，不得危害人体健康，不得违背伦理道德，不得损害公共利益。

第一千零一十条　【性骚扰】违背他人意愿，以言语、文字、图像、肢体行为等方式对他人实施性骚扰的，受害人有权依法请求行为人承担民事责任。

机关、企业、学校等单位应当采取合理的预防、受理投诉、调查

处置等措施，防止和制止利用职权、从属关系等实施性骚扰。

第一千零一十一条　【非法剥夺、限制他人行动自由和非法搜查他人身体】以非法拘禁等方式剥夺、限制他人的行动自由，或者非法搜查他人身体的，受害人有权依法请求行为人承担民事责任。

第三章　姓名权和名称权

第一千零一十二条　【姓名权】自然人享有姓名权，有权依法决定、使用、变更或者许可他人使用自己的姓名，但是不得违背公序良俗。

第一千零一十三条　【名称权】法人、非法人组织享有名称权，有权依法决定、使用、变更、转让或者许可他人使用自己的名称。

第一千零一十四条　【禁止侵害他人的姓名或名称】任何组织或者个人不得以干涉、盗用、假冒等方式侵害他人的姓名权或者名称权。

第一千零一十五条　【自然人姓氏的选取】自然人应当随父姓或者母姓，但是有下列情形之一的，可以在父姓和母姓之外选取姓氏：

（一）选取其他直系长辈血亲的姓氏；

（二）因由法定扶养人以外的人扶养而选取扶养人姓氏；

（三）有不违背公序良俗的其他正当理由。

少数民族自然人的姓氏可以遵从本民族的文化传统和风俗习惯。

第一千零一十六条　【决定、变更姓名、名称及转让名称的规定】自然人决定、变更姓名，或者法人、非法人组织决定、变更、转让名称的，应当依法向有关机关办理登记手续，但是法律另有规定的除外。

民事主体变更姓名、名称的，变更前实施的民事法律行为对其具有法律约束力。

第一千零一十七条　【姓名与名称的扩展保护】具有一定社会知名度，被他人使用足以造成公众混淆的笔名、艺名、网名、译名、字号、姓名和名称的简称等，参照适用姓名权和名称权保护的有关规定。

第四章　肖像权

第一千零一十八条　【肖像权及肖像】自然人享有肖像权，有权依法制作、使用、公开或者许可他人使用自己的肖像。

肖像是通过影像、雕塑、绘画等方式在一定载体上所反映的特定自然人可以被识别的外部形象。

第一千零一十九条　【肖像权的保护】任何组织或者个人不得以丑化、污损，或者利用信息技术手段伪造等方式侵害他人的肖像权。未经肖像权人同意，不得制作、使用、公开肖像权人的肖像，但是法律另有规定的除外。

未经肖像权人同意，肖像作品权利人不得以发表、复制、发行、出租、展览等方式使用或者公开肖像权人的肖像。

第一千零二十条　【肖像权的合理使用】合理实施下列行为的，可以不经肖像权人同意：

（一）为个人学习、艺术欣赏、课堂教学或者科学研究，在必要范围内使用肖像权人已经公开的肖像；

（二）为实施新闻报道，不可避免地制作、使用、公开肖像权人的肖像；

（三）为依法履行职责，国家机关在必要范围内制作、使用、公开肖像权人的肖像；

（四）为展示特定公共环境，不可避免地制作、使用、公开肖像权人的肖像；

（五）为维护公共利益或者肖像权人合法权益，制作、使用、公开肖像权人的肖像的其他行为。

第一千零二十一条　【肖像许可使用合同的解释】当事人对肖像许可使用合同中关于肖像使用条款的理解有争议的，应当作出有利于肖像权人的解释。

第一千零二十二条　【肖像许可使用合同期限】当事人对肖像许可使用期限没有约定或者约定不明确的，任何一方当事人可以随时解除肖像许可使用合同，但是应当在合理期限之前通知对方。

当事人对肖像许可使用期限有明确约定，肖像权人有正当理由的，可以解除肖像许可使用合同，但是应当在合理期限之前通知对方。因解除合同造成对方损失的，除不可归责于肖像权人的事由外，应当赔偿损失。

第一千零二十三条　【姓名、声音等的许可使用参照肖像许可使用】对姓名等的许可使用，参照适用肖像许可使用的有关规定。

对自然人声音的保护，参照适用肖像权保护的有关规定。

第五章　名誉权和荣誉权

第一千零二十四条　【名誉权及名誉】民事主体享有名誉权。任何组织或者个人不得以侮辱、诽谤等方式侵害他人的名誉权。

名誉是对民事主体的品德、声望、才能、信用等的社会评价。

第一千零二十五条　【新闻报道、舆论监督与保护名誉权关系问题】

行为人为公共利益实施新闻报道、舆论监督等行为，影响他人名誉的，不承担民事责任，但是有下列情形之一的除外：

（一）捏造、歪曲事实；

（二）对他人提供的严重失实内容未尽到合理核实义务；

（三）使用侮辱性言辞等贬损他人名誉。

第一千零二十六条　【认定是否尽到合理核实义务的考虑因素】认定行为人是否尽到前条第二项规定的合理核实义务，应当考虑下列因素：

（一）内容来源的可信度；

（二）对明显可能引发争议的内容是否进行了必要的调查；

（三）内容的时限性；

（四）内容与公序良俗的关联性；

（五）受害人名誉受贬损的可能性；

（六）核实能力和核实成本。

第一千零二十七条　【文学、艺术作品侵害名誉权的认定与例外】行为人发表的文学、艺术作品以真人真事或者特定人为描述对象，含有侮辱、诽谤内容，侵害他人名誉权的，受害人有权依法请求该行为人承担民事责任。

行为人发表的文学、艺术作品不以特定人为描述对象，仅其中的情节与该特定人的情况相似的，不承担民事责任。

第一千零二十八条　【名誉权人更正权】民事主体有证据证明报刊、网络等媒体报道的内容失实，侵害其名誉权的，有权请求该媒体及时

采取更正或者删除等必要措施。

第一千零二十九条　【信用评价】民事主体可以依法查询自己的信用评价；发现信用评价不当的，有权提出异议并请求采取更正、删除等必要措施。信用评价人应当及时核查，经核查属实的，应当及时采取必要措施。

第一千零三十条　【处理信用信息的法律适用】民事主体与征信机构等信用信息处理者之间的关系，适用本编有关个人信息保护的规定和其他法律、行政法规的有关规定。

第一千零三十一条　【荣誉权】民事主体享有荣誉权。任何组织或者个人不得非法剥夺他人的荣誉称号，不得诋毁、贬损他人的荣誉。

获得的荣誉称号应当记载而没有记载的，民事主体可以请求记载；获得的荣誉称号记载错误的，民事主体可以请求更正。

第六章　隐私权和个人信息保护

第一千零三十二条　【隐私权及隐私】自然人享有隐私权。任何组织或者个人不得以刺探、侵扰、泄露、公开等方式侵害他人的隐私权。

隐私是自然人的私人生活安宁和不愿为他人知晓的私密空间、私密活动、私密信息。

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

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

（二）进入、拍摄、窥视他人的住宅、宾馆房间等私密空间；

（三）拍摄、窥视、窃听、公开他人的私密活动；

（四）拍摄、窥视他人身体的私密部位；

（五）处理他人的私密信息；

（六）以其他方式侵害他人的隐私权。

第一千零三十四条　【个人信息保护】自然人的个人信息受法律保护。

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

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

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

（一）征得该自然人或者其监护人同意，但是法律、行政法规另有规定的除外；

（二）公开处理信息的规则；

（三）明示处理信息的目的、方式和范围；

（四）不违反法律、行政法规的规定和双方的约定。

个人信息的处理包括个人信息的收集、存储、使用、加工、传输、提供、公开等。

第一千零三十六条　【处理个人信息的免责事由】处理个人信息，

有下列情形之一的，行为人不承担民事责任：

（一）在该自然人或者其监护人同意的范围内合理实施的行为；

（二）合理处理该自然人自行公开的或者其他已经合法公开的信息，但是该自然人明确拒绝或者处理该信息侵害其重大利益的除外；

（三）为维护公共利益或者该自然人合法权益，合理实施的其他行为。

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

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

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

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

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

中华人民共和国生物安全法

时效性：　　现行有效

发文机关：　全国人大常委会

文号：　　主席令第五十六号

发文日期：　2020 年 10 月 17 日

施行日期：　2021 年 04 月 15 日

第一章　总　则

第一条　为了维护国家安全，防范和应对生物安全风险，保障人民生命健康，保护生物资源和生态环境，促进生物技术健康发展，推动构建人类命运共同体，实现人与自然和谐共生，制定本法。

第二条　本法所称生物安全，是指国家有效防范和应对危险生物因子及相关因素威胁，生物技术能够稳定健康发展，人民生命健康和生态系统相对处于没有危险和不受威胁的状态，生物领域具备维护国家安全和持续发展的能力。

从事下列活动，适用本法：

（一）防控重大新发突发传染病、动植物疫情；

（二）生物技术研究、开发与应用；

（三）病原微生物实验室生物安全管理；

（四）人类遗传资源与生物资源安全管理；

（五）防范外来物种入侵与保护生物多样性；

（六）应对微生物耐药；

（七）防范生物恐怖袭击与防御生物武器威胁；

（八）其他与生物安全相关的活动。

第三条　生物安全是国家安全的重要组成部分。维护生物安全应当贯彻总体国家安全观，统筹发展和安全，坚持以人为本、风险预防、分类管理、协同配合的原则。

第四条　坚持中国共产党对国家生物安全工作的领导，建立健全国家生物安全领导体制，加强国家生物安全风险防控和治理体系建设，提高国家生物安全治理能力。

第五条　国家鼓励生物科技创新，加强生物安全基础设施和生物科技人才队伍建设，支持生物产业发展，以创新驱动提升生物科技水平，增强生物安全保障能力。

第六条　国家加强生物安全领域的国际合作，履行中华人民共和国缔结或者参加的国际条约规定的义务，支持参与生物科技交流合作与生物安全事件国际救援，积极参与生物安全国际规则的研究与制定，推动完善全球生物安全治理。

第七条　各级人民政府及其有关部门应当加强生物安全法律法规和生物安全知识宣传普及工作，引导基层群众性自治组织、社会组织开展生物安全法律法规和生物安全知识宣传，促进全社会生物安全意识的提升。

相关科研院校、医疗机构以及其他企业事业单位应当将生物安全法律法规和生物安全知识纳入教育培训内容，加强学生、从业人员生物安全意识和伦理意识的培养。

新闻媒体应当开展生物安全法律法规和生物安全知识公益宣传，

对生物安全违法行为进行舆论监督，增强公众维护生物安全的社会责任意识。

第八条　任何单位和个人不得危害生物安全。

任何单位和个人有权举报危害生物安全的行为；接到举报的部门应当及时依法处理。

第九条　对在生物安全工作中做出突出贡献的单位和个人，县级以上人民政府及其有关部门按照国家规定予以表彰和奖励。

第二章　生物安全风险防控体制

第十条　中央国家安全领导机构负责国家生物安全工作的决策和议事协调，研究制定、指导实施国家生物安全战略和有关重大方针政策，统筹协调国家生物安全的重大事项和重要工作，建立国家生物安全工作协调机制。

省、自治区、直辖市建立生物安全工作协调机制，组织协调、督促推进本行政区域内生物安全相关工作。

第十一条　国家生物安全工作协调机制由国务院卫生健康、农业农村、科学技术、外交等主管部门和有关军事机关组成，分析研判国家生物安全形势，组织协调、督促推进国家生物安全相关工作。国家生物安全工作协调机制设立办公室，负责协调机制的日常工作。

国家生物安全工作协调机制成员单位和国务院其他有关部门根据职责分工，负责生物安全相关工作。

第十二条　国家生物安全工作协调机制设立专家委员会，为国家生物安全战略研究、政策制定及实施提供决策咨询。

国务院有关部门组织建立相关领域、行业的生物安全技术咨询专家委员会，为生物安全工作提供咨询、评估、论证等技术支撑。

第十三条　地方各级人民政府对本行政区域内生物安全工作负责。

县级以上地方人民政府有关部门根据职责分工，负责生物安全相关工作。

基层群众性自治组织应当协助地方人民政府以及有关部门做好生物安全风险防控、应急处置和宣传教育等工作。

有关单位和个人应当配合做好生物安全风险防控和应急处置等工作。

第十四条　国家建立生物安全风险监测预警制度。国家生物安全工作协调机制组织建立国家生物安全风险监测预警体系，提高生物安全风险识别和分析能力。

第十五条　国家建立生物安全风险调查评估制度。国家生物安全工作协调机制应当根据风险监测的数据、资料等信息，定期组织开展生物安全风险调查评估。

有下列情形之一的，有关部门应当及时开展生物安全风险调查评估，依法采取必要的风险防控措施：

（一）通过风险监测或者接到举报发现可能存在生物安全风险；

（二）为确定监督管理的重点领域、重点项目，制定、调整生物安全相关名录或者清单；

（三）发生重大新发突发传染病、动植物疫情等危害生物安全的

事件；

（四）需要调查评估的其他情形。

第十六条　国家建立生物安全信息共享制度。国家生物安全工作协调机制组织建立统一的国家生物安全信息平台，有关部门应当将生物安全数据、资料等信息汇交国家生物安全信息平台，实现信息共享。

第十七条　国家建立生物安全信息发布制度。国家生物安全总体情况、重大生物安全风险警示信息、重大生物安全事件及其调查处理信息等重大生物安全信息，由国家生物安全工作协调机制成员单位根据职责分工发布；其他生物安全信息由国务院有关部门和县级以上地方人民政府及其有关部门根据职责权限发布。

任何单位和个人不得编造、散布虚假的生物安全信息。

第十八条　国家建立生物安全名录和清单制度。国务院及其有关部门根据生物安全工作需要，对涉及生物安全的材料、设备、技术、活动、重要生物资源数据、传染病、动植物疫病、外来入侵物种等制定、公布名录或者清单，并动态调整。

第十九条　国家建立生物安全标准制度。国务院标准化主管部门和国务院其他有关部门根据职责分工，制定和完善生物安全领域相关标准。

国家生物安全工作协调机制组织有关部门加强不同领域生物安全标准的协调和衔接，建立和完善生物安全标准体系。

第二十条　国家建立生物安全审查制度。对影响或者可能影响国家安全的生物领域重大事项和活动，由国务院有关部门进行生物安全

审查，有效防范和化解生物安全风险。

第二十一条　国家建立统一领导、协同联动、有序高效的生物安全应急制度。

国务院有关部门应当组织制定相关领域、行业生物安全事件应急预案，根据应急预案和统一部署开展应急演练、应急处置、应急救援和事后恢复等工作。

县级以上地方人民政府及其有关部门应当制定并组织、指导和督促相关企业事业单位制定生物安全事件应急预案，加强应急准备、人员培训和应急演练，开展生物安全事件应急处置、应急救援和事后恢复等工作。

中国人民解放军、中国人民武装警察部队按照中央军事委员会的命令，依法参加生物安全事件应急处置和应急救援工作。

第二十二条　国家建立生物安全事件调查溯源制度。发生重大新发突发传染病、动植物疫情和不明原因的生物安全事件，国家生物安全工作协调机制应当组织开展调查溯源，确定事件性质，全面评估事件影响，提出意见建议。

第二十三条　国家建立首次进境或者暂停后恢复进境的动植物、动植物产品、高风险生物因子国家准入制度。

进出境的人员、运输工具、集装箱、货物、物品、包装物和国际航行船舶压舱水排放等应当符合我国生物安全管理要求。

海关对发现的进出境和过境生物安全风险，应当依法处置。经评估为生物安全高风险的人员、运输工具、货物、物品等，应当从指定

的国境口岸进境，并采取严格的风险防控措施。

第二十四条　国家建立境外重大生物安全事件应对制度。境外发生重大生物安全事件的，海关依法采取生物安全紧急防控措施，加强证件核验，提高查验比例，暂停相关人员、运输工具、货物、物品等进境。必要时经国务院同意，可以采取暂时关闭有关口岸、封锁有关国境等措施。

第二十五条　县级以上人民政府有关部门应当依法开展生物安全监督检查工作，被检查单位和个人应当配合，如实说明情况，提供资料，不得拒绝、阻挠。

涉及专业技术要求较高、执法业务难度较大的监督检查工作，应当有生物安全专业技术人员参加。

第二十六条　县级以上人民政府有关部门实施生物安全监督检查，可以依法采取下列措施：

（一）进入被检查单位、地点或者涉嫌实施生物安全违法行为的场所进行现场监测、勘查、检查或者核查；

（二）向有关单位和个人了解情况；

（三）查阅、复制有关文件、资料、档案、记录、凭证等；

（四）查封涉嫌实施生物安全违法行为的场所、设施；

（五）扣押涉嫌实施生物安全违法行为的工具、设备以及相关物品；

（六）法律法规规定的其他措施。

有关单位和个人的生物安全违法信息应当依法纳入全国信用信

息共享平台。

第三章　防控重大新发突发传染病、动植物疫情

第二十七条　国务院卫生健康、农业农村、林业草原、海关、生态环境主管部门应当建立新发突发传染病、动植物疫情、进出境检疫、生物技术环境安全监测网络，组织监测站点布局、建设，完善监测信息报告系统，开展主动监测和病原检测，并纳入国家生物安全风险监测预警体系。

第二十八条　疾病预防控制机构、动物疫病预防控制机构、植物病虫害预防控制机构（以下统称专业机构）应当对传染病、动植物疫病和列入监测范围的不明原因疾病开展主动监测，收集、分析、报告监测信息，预测新发突发传染病、动植物疫病的发生、流行趋势。

国务院有关部门、县级以上地方人民政府及其有关部门应当根据预测和职责权限及时发布预警，并采取相应的防控措施。

第二十九条　任何单位和个人发现传染病、动植物疫病的，应当及时向医疗机构、有关专业机构或者部门报告。

医疗机构、专业机构及其工作人员发现传染病、动植物疫病或者不明原因的聚集性疾病的，应当及时报告，并采取保护性措施。

依法应当报告的，任何单位和个人不得瞒报、谎报、缓报、漏报，不得授意他人瞒报、谎报、缓报，不得阻碍他人报告。

第三十条　国家建立重大新发突发传染病、动植物疫情联防联控机制。

发生重大新发突发传染病、动植物疫情，应当依照有关法律法规

和应急预案的规定及时采取控制措施；国务院卫生健康、农业农村、林业草原主管部门应当立即组织疫情会商研判，将会商研判结论向中央国家安全领导机构和国务院报告，并通报国家生物安全工作协调机制其他成员单位和国务院其他有关部门。

发生重大新发突发传染病、动植物疫情，地方各级人民政府统一履行本行政区域内疫情防控职责，加强组织领导，开展群防群控、医疗救治，动员和鼓励社会力量依法有序参与疫情防控工作。

第三十一条　国家加强国境、口岸传染病和动植物疫情联合防控能力建设，建立传染病、动植物疫情防控国际合作网络，尽早发现、控制重大新发突发传染病、动植物疫情。

第三十二条　国家保护野生动物，加强动物防疫，防止动物源性传染病传播。

第三十三条　国家加强对抗生素药物等抗微生物药物使用和残留的管理，支持应对微生物耐药的基础研究和科技攻关。

县级以上人民政府卫生健康主管部门应当加强对医疗机构合理用药的指导和监督，采取措施防止抗微生物药物的不合理使用。县级以上人民政府农业农村、林业草原主管部门应当加强对农业生产中合理用药的指导和监督，采取措施防止抗微生物药物的不合理使用，降低在农业生产环境中的残留。

国务院卫生健康、农业农村、林业草原、生态环境等主管部门和药品监督管理部门应当根据职责分工，评估抗微生物药物残留对人体健康、环境的危害，建立抗微生物药物污染物指标评价体系。

第四章　生物技术研究、开发与应用安全

第三十四条　国家加强对生物技术研究、开发与应用活动的安全管理，禁止从事危及公众健康、损害生物资源、破坏生态系统和生物多样性等危害生物安全的生物技术研究、开发与应用活动。

从事生物技术研究、开发与应用活动，应当符合伦理原则。

第三十五条　从事生物技术研究、开发与应用活动的单位应当对本单位生物技术研究、开发与应用的安全负责，采取生物安全风险防控措施，制定生物安全培训、跟踪检查、定期报告等工作制度，强化过程管理。

第三十六条　国家对生物技术研究、开发活动实行分类管理。根据对公众健康、工业农业、生态环境等造成危害的风险程度，将生物技术研究、开发活动分为高风险、中风险、低风险三类。

生物技术研究、开发活动风险分类标准及名录由国务院科学技术、卫生健康、农业农村等主管部门根据职责分工，会同国务院其他有关部门制定、调整并公布。

第三十七条　从事生物技术研究、开发活动，应当遵守国家生物技术研究开发安全管理规范。

从事生物技术研究、开发活动，应当进行风险类别判断，密切关注风险变化，及时采取应对措施。

第三十八条　从事高风险、中风险生物技术研究、开发活动，应当由在我国境内依法成立的法人组织进行，并依法取得批准或者进行备案。

从事高风险、中风险生物技术研究、开发活动，应当进行风险评估，制定风险防控计划和生物安全事件应急预案，降低研究、开发活动实施的风险。

第三十九条　国家对涉及生物安全的重要设备和特殊生物因子实行追溯管理。购买或者引进列入管控清单的重要设备和特殊生物因子，应当进行登记，确保可追溯，并报国务院有关部门备案。

个人不得购买或者持有列入管控清单的重要设备和特殊生物因子。

第四十条　从事生物医学新技术临床研究，应当通过伦理审查，并在具备相应条件的医疗机构内进行；进行人体临床研究操作的，应当由符合相应条件的卫生专业技术人员执行。

第四十一条　国务院有关部门依法对生物技术应用活动进行跟踪评估，发现存在生物安全风险的，应当及时采取有效补救和管控措施。

第五章　病原微生物实验室生物安全

第四十二条　国家加强对病原微生物实验室生物安全的管理，制定统一的实验室生物安全标准。病原微生物实验室应当符合生物安全国家标准和要求。

从事病原微生物实验活动，应当严格遵守有关国家标准和实验室技术规范、操作规程，采取安全防范措施。

第四十三条　国家根据病原微生物的传染性、感染后对人和动物的个体或者群体的危害程度，对病原微生物实行分类管理。

从事高致病性或者疑似高致病性病原微生物样本采集、保藏、运输活动，应当具备相应条件，符合生物安全管理规范。具体办法由国务院卫生健康、农业农村主管部门制定。

第四十四条　设立病原微生物实验室，应当依法取得批准或者进行备案。

个人不得设立病原微生物实验室或者从事病原微生物实验活动。

第四十五条　国家根据对病原微生物的生物安全防护水平，对病原微生物实验室实行分等级管理。

从事病原微生物实验活动应当在相应等级的实验室进行。低等级病原微生物实验室不得从事国家病原微生物目录规定应当在高等级病原微生物实验室进行的病原微生物实验活动。

第四十六条　高等级病原微生物实验室从事高致病性或者疑似高致病性病原微生物实验活动，应当经省级以上人民政府卫生健康或者农业农村主管部门批准，并将实验活动情况向批准部门报告。

对我国尚未发现或者已经宣布消灭的病原微生物，未经批准不得从事相关实验活动。

第四十七条　病原微生物实验室应当采取措施，加强对实验动物的管理，防止实验动物逃逸，对使用后的实验动物按照国家规定进行无害化处理，实现实验动物可追溯。禁止将使用后的实验动物流入市场。

病原微生物实验室应当加强对实验活动废弃物的管理，依法对废水、废气以及其他废弃物进行处置，采取措施防止污染。

第四十八条　病原微生物实验室的设立单位负责实验室的生物安全管理，制定科学、严格的管理制度，定期对有关生物安全规定的落实情况进行检查，对实验室设施、设备、材料等进行检查、维护和更新，确保其符合国家标准。

病原微生物实验室设立单位的法定代表人和实验室负责人对实验室的生物安全负责。

第四十九条　病原微生物实验室的设立单位应当建立和完善安全保卫制度，采取安全保卫措施，保障实验室及其病原微生物的安全。

国家加强对高等级病原微生物实验室的安全保卫。高等级病原微生物实验室应当接受公安机关等部门有关实验室安全保卫工作的监督指导，严防高致病性病原微生物泄漏、丢失和被盗、被抢。

国家建立高等级病原微生物实验室人员进入审核制度。进入高等级病原微生物实验室的人员应当经实验室负责人批准。对可能影响实验室生物安全的，不予批准；对批准进入的，应当采取安全保障措施。

第五十条　病原微生物实验室的设立单位应当制定生物安全事件应急预案，定期组织开展人员培训和应急演练。发生高致病性病原微生物泄漏、丢失和被盗、被抢或者其他生物安全风险的，应当按照应急预案的规定及时采取控制措施，并按照国家规定报告。

第五十一条　病原微生物实验室所在地省级人民政府及其卫生健康主管部门应当加强实验室所在地感染性疾病医疗资源配置，提高感染性疾病医疗救治能力。

第五十二条　企业对涉及病原微生物操作的生产车间的生物安

全管理，依照有关病原微生物实验室的规定和其他生物安全管理规范进行。

涉及生物毒素、植物有害生物及其他生物因子操作的生物安全实验室的建设和管理，参照有关病原微生物实验室的规定执行。

第六章　人类遗传资源与生物资源安全

第五十三条　国家加强对我国人类遗传资源和生物资源采集、保藏、利用、对外提供等活动的管理和监督，保障人类遗传资源和生物资源安全。

国家对我国人类遗传资源和生物资源享有主权。

第五十四条　国家开展人类遗传资源和生物资源调查。

国务院科学技术主管部门组织开展我国人类遗传资源调查，制定重要遗传家系和特定地区人类遗传资源申报登记办法。

国务院科学技术、自然资源、生态环境、卫生健康、农业农村、林业草原、中医药主管部门根据职责分工，组织开展生物资源调查，制定重要生物资源申报登记办法。

第五十五条　采集、保藏、利用、对外提供我国人类遗传资源，应当符合伦理原则，不得危害公众健康、国家安全和社会公共利益。

第五十六条　从事下列活动，应当经国务院科学技术主管部门批准：

（一）采集我国重要遗传家系、特定地区人类遗传资源或者采集国务院科学技术主管部门规定的种类、数量的人类遗传资源；

（二）保藏我国人类遗传资源；

（三）利用我国人类遗传资源开展国际科学研究合作；

（四）将我国人类遗传资源材料运送、邮寄、携带出境。

前款规定不包括以临床诊疗、采供血服务、查处违法犯罪、兴奋剂检测和殡葬等为目的采集、保藏人类遗传资源及开展的相关活动。

为了取得相关药品和医疗器械在我国上市许可，在临床试验机构利用我国人类遗传资源开展国际合作临床试验、不涉及人类遗传资源出境的，不需要批准；但是，在开展临床试验前应当将拟使用的人类遗传资源种类、数量及用途向国务院科学技术主管部门备案。

境外组织、个人及其设立或者实际控制的机构不得在我国境内采集、保藏我国人类遗传资源，不得向境外提供我国人类遗传资源。

第五十七条　将我国人类遗传资源信息向境外组织、个人及其设立或者实际控制的机构提供或者开放使用的，应当向国务院科学技术主管部门事先报告并提交信息备份。

第五十八条　采集、保藏、利用、运输出境我国珍贵、濒危、特有物种及其可用于再生或者繁殖传代的个体、器官、组织、细胞、基因等遗传资源，应当遵守有关法律法规。

境外组织、个人及其设立或者实际控制的机构获取和利用我国生物资源，应当依法取得批准。

第五十九条　利用我国生物资源开展国际科学研究合作，应当依法取得批准。

利用我国人类遗传资源和生物资源开展国际科学研究合作，应当保证中方单位及其研究人员全过程、实质性地参与研究，依法分享相

关权益。

第六十条　国家加强对外来物种入侵的防范和应对，保护生物多样性。国务院农业农村主管部门会同国务院其他有关部门制定外来入侵物种名录和管理办法。

国务院有关部门根据职责分工，加强对外来入侵物种的调查、监测、预警、控制、评估、清除以及生态修复等工作。

任何单位和个人未经批准，不得擅自引进、释放或者丢弃外来物种。

第七章　防范生物恐怖与生物武器威胁

第六十一条　国家采取一切必要措施防范生物恐怖与生物武器威胁。

禁止开发、制造或者以其他方式获取、储存、持有和使用生物武器。

禁止以任何方式唆使、资助、协助他人开发、制造或者以其他方式获取生物武器。

第六十二条　国务院有关部门制定、修改、公布可被用于生物恐怖活动、制造生物武器的生物体、生物毒素、设备或者技术清单，加强监管，防止其被用于制造生物武器或者恐怖目的。

第六十三条　国务院有关部门和有关军事机关根据职责分工，加强对可被用于生物恐怖活动、制造生物武器的生物体、生物毒素、设备或者技术进出境、进出口、获取、制造、转移和投放等活动的监测、调查，采取必要的防范和处置措施。

第六十四条　国务院有关部门、省级人民政府及其有关部门负责组织遭受生物恐怖袭击、生物武器攻击后的人员救治与安置、环境消毒、生态修复、安全监测和社会秩序恢复等工作。

国务院有关部门、省级人民政府及其有关部门应当有效引导社会舆论科学、准确报道生物恐怖袭击和生物武器攻击事件，及时发布疏散、转移和紧急避难等信息，对应急处置与恢复过程中遭受污染的区域和人员进行长期环境监测和健康监测。

第六十五条　国家组织开展对我国境内战争遗留生物武器及其危害结果、潜在影响的调查。

国家组织建设存放和处理战争遗留生物武器设施，保障对战争遗留生物武器的安全处置。

第八章　生物安全能力建设

第六十六条　国家制定生物安全事业发展规划，加强生物安全能力建设，提高应对生物安全事件的能力和水平。

县级以上人民政府应当支持生物安全事业发展，按照事权划分，将支持下列生物安全事业发展的相关支出列入政府预算：

（一）监测网络的构建和运行；

（二）应急处置和防控物资的储备；

（三）关键基础设施的建设和运行；

（四）关键技术和产品的研究、开发；

（五）人类遗传资源和生物资源的调查、保藏；

（六）法律法规规定的其他重要生物安全事业。

第六十七条　国家采取措施支持生物安全科技研究，加强生物安全风险防御与管控技术研究，整合优势力量和资源，建立多学科、多部门协同创新的联合攻关机制，推动生物安全核心关键技术和重大防御产品的成果产出与转化应用，提高生物安全的科技保障能力。

第六十八条　国家统筹布局全国生物安全基础设施建设。国务院有关部门根据职责分工，加快建设生物信息、人类遗传资源保藏、菌（毒）种保藏、动植物遗传资源保藏、高等级病原微生物实验室等方面的生物安全国家战略资源平台，建立共享利用机制，为生物安全科技创新提供战略保障和支撑。

第六十九条　国务院有关部门根据职责分工，加强生物基础科学研究人才和生物领域专业技术人才培养，推动生物基础科学学科建设和科学研究。

国家生物安全基础设施重要岗位的从业人员应当具备符合要求的资格，相关信息应当向国务院有关部门备案，并接受岗位培训。

第七十条　国家加强重大新发突发传染病、动植物疫情等生物安全风险防控的物资储备。

国家加强生物安全应急药品、装备等物资的研究、开发和技术储备。国务院有关部门根据职责分工，落实生物安全应急药品、装备等物资研究、开发和技术储备的相关措施。

国务院有关部门和县级以上地方人民政府及其有关部门应当保障生物安全事件应急处置所需的医疗救护设备、救治药品、医疗器械等物资的生产、供应和调配；交通运输主管部门应当及时组织协调运

输经营单位优先运送。

第七十一条　国家对从事高致病性病原微生物实验活动、生物安全事件现场处置等高风险生物安全工作的人员，提供有效的防护措施和医疗保障。

第九章　法律责任

第七十二条　违反本法规定，履行生物安全管理职责的工作人员在生物安全工作中滥用职权、玩忽职守、徇私舞弊或者有其他违法行为的，依法给予处分。

第七十三条　违反本法规定，医疗机构、专业机构或者其工作人员瞒报、谎报、缓报、漏报，授意他人瞒报、谎报、缓报，或者阻碍他人报告传染病、动植物疫病或者不明原因的聚集性疾病的，由县级以上人民政府有关部门责令改正，给予警告；对法定代表人、主要负责人、直接负责的主管人员和其他直接责任人员，依法给予处分，并可以依法暂停一定期限的执业活动直至吊销相关执业证书。

违反本法规定，编造、散布虚假的生物安全信息，构成违反治安管理行为的，由公安机关依法给予治安管理处罚。

第七十四条　违反本法规定，从事国家禁止的生物技术研究、开发与应用活动的，由县级以上人民政府卫生健康、科学技术、农业农村主管部门根据职责分工，责令停止违法行为，没收违法所得、技术资料和用于违法行为的工具、设备、原材料等物品，处一百万元以上一千万元以下的罚款，违法所得在一百万元以上的，处违法所得十倍以上二十倍以下的罚款，并可以依法禁止一定期限内从事相应的生物

技术研究、开发与应用活动，吊销相关许可证件；对法定代表人、主要负责人、直接负责的主管人员和其他直接责任人员，依法给予处分，处十万元以上二十万元以下的罚款，十年直至终身禁止从事相应的生物技术研究、开发与应用活动，依法吊销相关执业证书。

第七十五条　违反本法规定，从事生物技术研究、开发活动未遵守国家生物技术研究开发安全管理规范的，由县级以上人民政府有关部门根据职责分工，责令改正，给予警告，可以并处二万元以上二十万元以下的罚款；拒不改正或者造成严重后果的，责令停止研究、开发活动，并处二十万元以上二百万元以下的罚款。

第七十六条　违反本法规定，从事病原微生物实验活动未在相应等级的实验室进行，或者高等级病原微生物实验室未经批准从事高致病性、疑似高致病性病原微生物实验活动的，由县级以上地方人民政府卫生健康、农业农村主管部门根据职责分工，责令停止违法行为，监督其将用于实验活动的病原微生物销毁或者送交保藏机构，给予警告；造成传染病传播、流行或者其他严重后果的，对法定代表人、主要负责人、直接负责的主管人员和其他直接责任人员依法给予撤职、开除处分。

第七十七条　违反本法规定，将使用后的实验动物流入市场的，由县级以上人民政府科学技术主管部门责令改正，没收违法所得，并处二十万元以上一百万元以下的罚款，违法所得在二十万元以上的，并处违法所得五倍以上十倍以下的罚款；情节严重的，由发证部门吊销相关许可证件。

第七十八条　违反本法规定，有下列行为之一的，由县级以上人民政府有关部门根据职责分工，责令改正，没收违法所得，给予警告，可以并处十万元以上一百万元以下的罚款：

（一）购买或者引进列入管控清单的重要设备、特殊生物因子未进行登记，或者未报国务院有关部门备案；

（二）个人购买或者持有列入管控清单的重要设备或者特殊生物因子；

（三）个人设立病原微生物实验室或者从事病原微生物实验活动；

（四）未经实验室负责人批准进入高等级病原微生物实验室。

第七十九条　违反本法规定，未经批准，采集、保藏我国人类遗传资源或者利用我国人类遗传资源开展国际科学研究合作的，由国务院科学技术主管部门责令停止违法行为，没收违法所得和违法采集、保藏的人类遗传资源，并处五十万元以上五百万元以下的罚款，违法所得在一百万元以上的，并处违法所得五倍以上十倍以下的罚款；情节严重的，对法定代表人、主要负责人、直接负责的主管人员和其他直接责任人员，依法给予处分，五年内禁止从事相应活动。

第八十条　违反本法规定，境外组织、个人及其设立或者实际控制的机构在我国境内采集、保藏我国人类遗传资源，或者向境外提供我国人类遗传资源的，由国务院科学技术主管部门责令停止违法行为，没收违法所得和违法采集、保藏的人类遗传资源，并处一百万元以上一千万元以下的罚款；违法所得在一百万元以上的，并处违法所得十

倍以上二十倍以下的罚款。

第八十一条　违反本法规定，未经批准，擅自引进外来物种的，由县级以上人民政府有关部门根据职责分工，没收引进的外来物种，并处五万元以上二十五万元以下的罚款。

违反本法规定，未经批准，擅自释放或者丢弃外来物种的，由县级以上人民政府有关部门根据职责分工，责令限期捕回、找回释放或者丢弃的外来物种，处一万元以上五万元以下的罚款。

第八十二条　违反本法规定，构成犯罪的，依法追究刑事责任；造成人身、财产或者其他损害的，依法承担民事责任。

第八十三条　违反本法规定的生物安全违法行为，本法未规定法律责任，其他有关法律、行政法规有规定的，依照其规定。

第八十四条　境外组织或者个人通过运输、邮寄、携带危险生物因子入境或者以其他方式危害我国生物安全的，依法追究法律责任，并可以采取其他必要措施。

第十章　附　则

第八十五条　本法下列术语的含义：

（一）生物因子，是指动物、植物、微生物、生物毒素及其他生物活性物质。

（二）重大新发突发传染病，是指我国境内首次出现或者已经宣布消灭再次发生，或者突然发生，造成或者可能造成公众健康和生命安全严重损害，引起社会恐慌，影响社会稳定的传染病。

（三）重大新发突发动物疫情，是指我国境内首次发生或者已经

宣布消灭的动物疫病再次发生，或者发病率、死亡率较高的潜伏动物疫病突然发生并迅速传播，给养殖业生产安全造成严重威胁、危害，以及可能对公众健康和生命安全造成危害的情形。

（四）重大新发突发植物疫情，是指我国境内首次发生或者已经宣布消灭的严重危害植物的真菌、细菌、病毒、昆虫、线虫、杂草、害鼠、软体动物等再次引发病虫害，或者本地有害生物突然大范围发生并迅速传播，对农作物、林木等植物造成严重危害的情形。

（五）生物技术研究、开发与应用，是指通过科学和工程原理认识、改造、合成、利用生物而从事的科学研究、技术开发与应用等活动。

（六）病原微生物，是指可以侵犯人、动物引起感染甚至传染病的微生物，包括病毒、细菌、真菌、立克次体、寄生虫等。

（七）植物有害生物，是指能够对农作物、林木等植物造成危害的真菌、细菌、病毒、昆虫、线虫、杂草、害鼠、软体动物等生物。

（八）人类遗传资源，包括人类遗传资源材料和人类遗传资源信息。人类遗传资源材料是指含有人体基因组、基因等遗传物质的器官、组织、细胞等遗传材料。人类遗传资源信息是指利用人类遗传资源材料产生的数据等信息资料。

（九）微生物耐药，是指微生物对抗微生物药物产生抗性，导致抗微生物药物不能有效控制微生物的感染。

（十）生物武器，是指类型和数量不属于预防、保护或者其他和平用途所正当需要的、任何来源或者任何方法产生的微生物剂、其他

生物剂以及生物毒素；也包括为将上述生物剂、生物毒素使用于敌对目的或者武装冲突而设计的武器、设备或者运载工具。

（十一）生物恐怖，是指故意使用致病性微生物、生物毒素等实施袭击，损害人类或者动植物健康，引起社会恐慌，企图达到特定政治目的的行为。

第八十六条　生物安全信息属于国家秘密的，应当依照《中华人民共和国保守国家秘密法》和国家其他有关保密规定实施保密管理。

第八十七条　中国人民解放军、中国人民武装警察部队的生物安全活动，由中央军事委员会依照本法规定的原则另行规定。

第八十八条　本法自2021年4月15日起施行。

中华人民共和国电子签名法（2019年修正）

时效性：　　现行有效

发文机关：　全国人大常委会

文号：　　主席令第二十九号

发文日期：　2019年04月23日

施行日期：　2019年04月23日

第一章　总　则

第一条　为了规范电子签名行为，确立电子签名的法律效力，维护有关各方的合法权益，制定本法。

第二条　本法所称电子签名，是指数据电文中以电子形式所含、所附用于识别签名人身份并表明签名人认可其中内容的数据。

本法所称数据电文，是指以电子、光学、磁或者类似手段生成、发送、接收或者储存的信息。

第三条　民事活动中的合同或者其他文件、单证等文书，当事人可以约定使用或者不使用电子签名、数据电文。

当事人约定使用电子签名、数据电文的文书，不得仅因为其采用电子签名、数据电文的形式而否定其法律效力。

前款规定不适用下列文书：

（一）涉及婚姻、收养、继承等人身关系的；

（二）涉及停止供水、供热、供气等公用事业服务的；

（三）法律、行政法规规定的不适用电子文书的其他情形。

第二章　数据电文

第四条　能够有形地表现所载内容，并可以随时调取查用的数据电文，视为符合法律、法规要求的书面形式。

第五条　符合下列条件的数据电文，视为满足法律、法规规定的原件形式要求：

（一）能够有效地表现所载内容并可供随时调取查用；

（二）能够可靠地保证自最终形成时起，内容保持完整、未被更改。但是，在数据电文上增加背书以及数据交换、储存和显示过程中发生的形式变化不影响数据电文的完整性。

第六条　符合下列条件的数据电文，视为满足法律、法规规定的文件保存要求：

（一）能够有效地表现所载内容并可供随时调取查用；

（二）数据电文的格式与其生成、发送或者接收时的格式相同，或者格式不相同但是能够准确表现原来生成、发送或者接收的内容；

（三）能够识别数据电文的发件人、收件人以及发送、接收的时间。

第七条　数据电文不得仅因为其是以电子、光学、磁或者类似手段生成、发送、接收或者储存的而被拒绝作为证据使用。

第八条　审查数据电文作为证据的真实性，应当考虑以下因素：

（一）生成、储存或者传递数据电文方法的可靠性；

（二）保持内容完整性方法的可靠性；

（三）用以鉴别发件人方法的可靠性；

（四）其他相关因素。

第九条　数据电文有下列情形之一的，视为发件人发送：

（一）经发件人授权发送的；

（二）发件人的信息系统自动发送的；

（三）收件人按照发件人认可的方法对数据电文进行验证后结果相符的。

当事人对前款规定的事项另有约定的，从其约定。

第十条　法律、行政法规规定或者当事人约定数据电文需要确认收讫的，应当确认收讫。发件人收到收件人的收讫确认时，数据电文视为已经收到。

第十一条　数据电文进入发件人控制之外的某个信息系统的时间，视为该数据电文的发送时间。

收件人指定特定系统接收数据电文的，数据电文进入该特定系统的时间，视为该数据电文的接收时间；未指定特定系统的，数据电文进入收件人的任何系统的首次时间，视为该数据电文的接收时间。

当事人对数据电文的发送时间、接收时间另有约定的，从其约定。

第十二条　发件人的主营业地为数据电文的发送地点，收件人的主营业地为数据电文的接收地点。没有主营业地的，其经常居住地为发送或者接收地点。

当事人对数据电文的发送地点、接收地点另有约定的，从其约定。

第三章　电子签名与认证

第十三条　电子签名同时符合下列条件的，视为可靠的电子签名：

（一）电子签名制作数据用于电子签名时，属于电子签名人专有；

（二）签署时电子签名制作数据仅由电子签名人控制；

（三）签署后对电子签名的任何改动能够被发现；

（四）签署后对数据电文内容和形式的任何改动能够被发现。

当事人也可以选择使用符合其约定的可靠条件的电子签名。

第十四条　可靠的电子签名与手写签名或者盖章具有同等的法律效力。

第十五条　电子签名人应当妥善保管电子签名制作数据。电子签名人知悉电子签名制作数据已经失密或者可能已经失密时，应当及时告知有关各方，并终止使用该电子签名制作数据。

第十六条　电子签名需要第三方认证的，由依法设立的电子认证服务提供者提供认证服务。

第十七条　提供电子认证服务，应当具备下列条件：

（一）取得企业法人资格；

（二）具有与提供电子认证服务相适应的专业技术人员和管理人员；

（三）具有与提供电子认证服务相适应的资金和经营场所；

（四）具有符合国家安全标准的技术和设备；

（五）具有国家密码管理机构同意使用密码的证明文件；

（六）法律、行政法规规定的其他条件。

第十八条　从事电子认证服务，应当向国务院信息产业主管部门提出申请，并提交符合本法第十七条规定条件的相关材料。国务院信

息产业主管部门接到申请后经依法审查，征求国务院商务主管部门等有关部门的意见后，自接到申请之日起四十五日内作出许可或者不予许可的决定。予以许可的，颁发电子认证许可证书；不予许可的，应当书面通知申请人并告知理由。

取得认证资格的电子认证服务提供者，应当按照国务院信息产业主管部门的规定在互联网上公布其名称、许可证号等信息。

第十九条　电子认证服务提供者应当制定、公布符合国家有关规定的电子认证业务规则，并向国务院信息产业主管部门备案。

电子认证业务规则应当包括责任范围、作业操作规范、信息安全保障措施等事项。

第二十条　电子签名人向电子认证服务提供者申请电子签名认证证书，应当提供真实、完整和准确的信息。

电子认证服务提供者收到电子签名认证证书申请后，应当对申请人的身份进行查验，并对有关材料进行审查。

第二十一条　电子认证服务提供者签发的电子签名认证证书应当准确无误，并应当载明下列内容：

（一）电子认证服务提供者名称；

（二）证书持有人名称；

（三）证书序列号；

（四）证书有效期；

（五）证书持有人的电子签名验证数据；

（六）电子认证服务提供者的电子签名；

（七）国务院信息产业主管部门规定的其他内容。

第二十二条　电子认证服务提供者应当保证电子签名认证证书内容在有效期内完整、准确，并保证电子签名依赖方能够证实或者了解电子签名认证证书所载内容及其他有关事项。

第二十三条　电子认证服务提供者拟暂停或者终止电子认证服务的，应当在暂停或者终止服务九十日前，就业务承接及其他有关事项通知有关各方。

电子认证服务提供者拟暂停或者终止电子认证服务的，应当在暂停或者终止服务六十日前向国务院信息产业主管部门报告，并与其他电子认证服务提供者就业务承接进行协商，作出妥善安排。

电子认证服务提供者未能就业务承接事项与其他电子认证服务提供者达成协议的，应当申请国务院信息产业主管部门安排其他电子认证服务提供者承接其业务。

电子认证服务提供者被依法吊销电子认证许可证书的，其业务承接事项的处理按照国务院信息产业主管部门的规定执行。

第二十四条　电子认证服务提供者应当妥善保存与认证相关的信息，信息保存期限至少为电子签名认证证书失效后五年。

第二十五条　国务院信息产业主管部门依照本法制定电子认证服务业的具体管理办法，对电子认证服务提供者依法实施监督管理。

第二十六条　经国务院信息产业主管部门根据有关协议或者对等原则核准后，中华人民共和国境外的电子认证服务提供者在境外签发的电子签名认证证书与依照本法设立的电子认证服务提供者签发的

电子签名认证证书具有同等的法律效力。

第四章　法律责任

第二十七条　电子签名人知悉电子签名制作数据已经失密或者可能已经失密未及时告知有关各方、并终止使用电子签名制作数据，未向电子认证服务提供者提供真实、完整和准确的信息，或者有其他过错，给电子签名依赖方、电子认证服务提供者造成损失的，承担赔偿责任。

第二十八条　电子签名人或者电子签名依赖方因依据电子认证服务提供者提供的电子签名认证服务从事民事活动遭受损失，电子认证服务提供者不能证明自己无过错的，承担赔偿责任。

第二十九条　未经许可提供电子认证服务的，由国务院信息产业主管部门责令停止违法行为；有违法所得的，没收违法所得；违法所得三十万元以上的，处违法所得一倍以上三倍以下的罚款；没有违法所得或者违法所得不足三十万元的，处十万元以上三十万元以下的罚款。

第三十条　电子认证服务提供者暂停或者终止电子认证服务，未在暂停或者终止服务六十日前向国务院信息产业主管部门报告的，由国务院信息产业主管部门对其直接负责的主管人员处一万元以上五万元以下的罚款。

第三十一条　电子认证服务提供者不遵守认证业务规则、未妥善保存与认证相关的信息，或者有其他违法行为的，由国务院信息产业主管部门责令限期改正；逾期未改正的，吊销电子认证许可证书，其

直接负责的主管人员和其他直接责任人员十年内不得从事电子认证服务。吊销电子认证许可证书的，应当予以公告并通知工商行政管理部门。

第三十二条　伪造、冒用、盗用他人的电子签名，构成犯罪的，依法追究刑事责任；给他人造成损失的，依法承担民事责任。

第三十三条　依照本法负责电子认证服务业监督管理工作的部门的工作人员，不依法履行行政许可、监督管理职责的，依法给予行政处分；构成犯罪的，依法追究刑事责任。

第五章　附　则

第三十四条　本法中下列用语的含义：

（一）电子签名人，是指持有电子签名制作数据并以本人身份或者以其所代表的人的名义实施电子签名的人；

（二）电子签名依赖方，是指基于对电子签名认证证书或者电子签名的信赖从事有关活动的人；

（三）电子签名认证证书，是指可证实电子签名人与电子签名制作数据有联系的数据电文或者其他电子记录；

（四）电子签名制作数据，是指在电子签名过程中使用的，将电子签名与电子签名人可靠地联系起来的字符、编码等数据；

（五）电子签名验证数据，是指用于验证电子签名的数据，包括代码、口令、算法或者公钥等。

第三十五条　国务院或者国务院规定的部门可以依据本法制定政务活动和其他社会活动中使用电子签名、数据电文的具体办法。

第三十六条　本法自2005年4月1日起施行。

中华人民共和国密码法

时效性：　　现行有效

发文机关：　全国人大常委会

文号：　　主席令第三十五号

发文日期：　2019 年 10 月 26 日

施行日期：　2020 年 01 月 01 日

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，维护国家安全和社会公共利益，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。

中华人民共和国电子商务法

时效性：　　现行有效

发文机关：　全国人大常委会

文号：　　主席令第 7 号

发文日期：　2018 年 08 月 31 日

施行日期：　2019 年 01 月 01 日

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、删除的申请的，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，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为电子商务提供快递物流服务，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为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：

（一）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；

（二）未在首页显著位置持续公示终止电子商务的有关信息的；

（三）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：

（一）不履行本法第二十七条规定的核验、登记义务的；

（二）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；

（三）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；

（四）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：

（一）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；

（二）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；

（三）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；

（四）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。

中华人民共和国测绘法（2017年修正）

时效性：　　现行有效

发文机关：　全国人大常委会

文号：　　主席令第67号

发文日期：　2017年04月27日

施行日期：　2017年07月01日

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年度计划，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、构筑物和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制度和技术防控体系，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。

中华人民共和国网络安全法

时效性：　　现行有效

发文机关：　全国人大常委会

文号：　　中华人民共和国主席令第五十三号

发文日期：　2016 年 11 月 07 日

施行日期：　2017 年 06 月 01 日

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：

（一）制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；

（二）采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施；

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

（四）采取数据分类、重要数据备份和加密等措施；

（五）法律、行政法规规定的其他义务。

第二十二条　网络产品、服务应当符合相关国家标准的强制性要求。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：

（一）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；

（二）定期对从业人员进行网络安全教育、技术培训和技能考核；

（三）对重要系统和数据库进行容灾备份；

（四）制定网络安全事件应急预案，并定期进行演练；

（五）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：

（一）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；

（二）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；

（三）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；

（四）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：

（一）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；

（二）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；

（三）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　因维护国家安全和社会公共秩序，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：

（一）设置恶意程序的；

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

（三）擅自终止为其产品、服务提供安全维护的。

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

第六十二条　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，并可以由有关主管部门责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处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；情节较重的，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：

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

（二）拒绝、阻碍有关部门依法实施的监督检查的；

（三）拒不向公安机关、国家安全机关提供技术支持和协助的。

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

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

第七十二条　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：

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

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

（三）网络运营者，是指网络的所有者、管理者和网络服务提供者。

（四）网络数据，是指通过网络收集、存储、传输、处理和产生的各种电子数据。

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

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。

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

时效性：　　现行有效

发文机关：　全国人大常委会

发文日期：　2012 年 12 月 28 日

施行日期：　2012 年 12 月 28 日

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

一、国家保护能够识别公民个人身份和涉及公民个人隐私的电子信息。

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

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

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

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

四、网络服务提供者和其他企业事业单位应当采取技术措施和其他必要措施，确保信息安全，防止在业务活动中收集的公民个人电子

信息泄露、毁损、丢失。在发生或者可能发生信息泄露、毁损、丢失的情况时，应当立即采取补救措施。

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

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

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

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

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

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

服务提供者应当予以配合，提供技术支持。

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

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

十二、本决定自公布之日起施行。

中华人民共和国居民身份证法（2011年修正）

时效性：　现行有效

发文机关：　全国人大常委会

文号：　主席令第51号

发文日期：　2011年10月29日

施行日期：　2012年1月1日

第一章　总　则

第一条　为了证明居住在中华人民共和国境内的公民的身份，保障公民的合法权益，便利公民进行社会活动，维护社会秩序，制定本法。

第二条　居住在中华人民共和国境内的年满十六周岁的中国公民，应当依照本法的规定申请领取居民身份证；未满十六周岁的中国公民，可以依照本法的规定申请领取居民身份证。

第三条　居民身份证登记的项目包括：姓名、性别、民族、出生日期、常住户口所在地住址、公民身份号码、本人相片、指纹信息、证件的有效期和签发机关。

公民身份号码是每个公民唯一的、终身不变的身份代码，由公安机关按照公民身份号码国家标准编制。

公民申请领取、换领、补领居民身份证，应当登记指纹信息。

第四条　居民身份证使用规范汉字和符合国家标准的数字符号填写。

民族自治地方的自治机关根据本地区的实际情况，对居民身份证

用汉字登记的内容，可以决定同时使用实行区域自治的民族的文字或者选用一种当地通用的文字。

第五条　十六周岁以上公民的居民身份证的有效期为十年、二十年、长期。十六周岁至二十五周岁的，发给有效期十年的居民身份证；二十六周岁至四十五周岁的，发给有效期二十年的居民身份证；四十六周岁以上的，发给长期有效的居民身份证。

未满十六周岁的公民，自愿申请领取居民身份证的，发给有效期五年的居民身份证。

第六条　居民身份证式样由国务院公安部门制定。居民身份证由公安机关统一制作、发放。

居民身份证具备视读与机读两种功能，视读、机读的内容限于本法第三条第一款规定的项目。

公安机关及其人民警察对因制作、发放、查验、扣押居民身份证而知悉的公民的个人信息，应当予以保密。

第二章　申领和发放

第七条　公民应当自年满十六周岁之日起三个月内，向常住户口所在地的公安机关申请领取居民身份证。

未满十六周岁的公民，由监护人代为申请领取居民身份证。

第八条　居民身份证由居民常住户口所在地的县级人民政府公安机关签发。

第九条　香港同胞、澳门同胞、台湾同胞迁入内地定居的，华侨回国定居的，以及外国人、无国籍人在中华人民共和国境内定居并被

批准加入或者恢复中华人民共和国国籍的，在办理常住户口登记时，应当依照本法规定申请领取居民身份证。

第十条　申请领取居民身份证，应当填写《居民身份证申领登记表》，交验居民户口簿。

第十一条　国家决定换发新一代居民身份证、居民身份证有效期满、公民姓名变更或者证件严重损坏不能辨认的，公民应当换领新证；居民身份证登记项目出现错误的，公安机关应当及时更正，换发新证；领取新证时，必须交回原证。居民身份证丢失的，应当申请补领。

未满十六周岁公民的居民身份证有前款情形的，可以申请换领、换发或者补领新证。

公民办理常住户口迁移手续时，公安机关应当在居民身份证的机读项目中记载公民常住户口所在地住址变动的情况，并告知本人。

第十二条　公民申请领取、换领、补领居民身份证，公安机关应当按照规定及时予以办理。公安机关应当自公民提交《居民身份证申领登记表》之日起六十日内发放居民身份证；交通不便的地区，办理时间可以适当延长，但延长的时间不得超过三十日。

公民在申请领取、换领、补领居民身份证期间，急需使用居民身份证的，可以申请领取临时居民身份证，公安机关应当按照规定及时予以办理。具体办法由国务院公安部门规定。

第三章　使用和查验

第十三条　公民从事有关活动，需要证明身份的，有权使用居民身份证证明身份，有关单位及其工作人员不得拒绝。

有关单位及其工作人员对履行职责或者提供服务过程中获得的居民身份证记载的公民个人信息，应当予以保密。

第十四条　有下列情形之一的，公民应当出示居民身份证证明身份：

（一）常住户口登记项目变更；

（二）兵役登记；

（三）婚姻登记、收养登记；

（四）申请办理出境手续；

（五）法律、行政法规规定需要用居民身份证证明身份的其他情形。

依照本法规定未取得居民身份证的公民，从事前款规定的有关活动，可以使用符合国家规定的其他证明方式证明身份。

第十五条　人民警察依法执行职务，遇有下列情形之一的，经出示执法证件，可以查验居民身份证：

（一）对有违法犯罪嫌疑的人员，需要查明身份的；

（二）依法实施现场管制时，需要查明有关人员身份的；

（三）发生严重危害社会治安突发事件时，需要查明现场有关人员身份的；

（四）在火车站、长途汽车站、港口、码头、机场或者在重大活动期间设区的市级人民政府规定的场所，需要查明有关人员身份的；

（五）法律规定需要查明身份的其他情形。

有前款所列情形之一，拒绝人民警察查验居民身份证的，依照有

关法律规定，分别不同情形，采取措施予以处理。

任何组织或者个人不得扣押居民身份证。但是，公安机关依照《中华人民共和国刑事诉讼法》执行监视居住强制措施的情形除外。

第四章　法律责任

第十六条　有下列行为之一的，由公安机关给予警告，并处二百元以下罚款，有违法所得的，没收违法所得：

（一）使用虚假证明材料骗领居民身份证的；

（二）出租、出借、转让居民身份证的；

（三）非法扣押他人居民身份证的。

第十七条　有下列行为之一的，由公安机关处二百元以上一千元以下罚款，或者处十日以下拘留，有违法所得的，没收违法所得：

（一）冒用他人居民身份证或者使用骗领的居民身份证的；

（二）购买、出售、使用伪造、变造的居民身份证的。

伪造、变造的居民身份证和骗领的居民身份证，由公安机关予以收缴。

第十八条　伪造、变造居民身份证的，依法追究刑事责任。

有本法第十六条、第十七条所列行为之一，从事犯罪活动的，依法追究刑事责任。

第十九条　国家机关或者金融、电信、交通、教育、医疗等单位的工作人员泄露在履行职责或者提供服务过程中获得的居民身份证记载的公民个人信息，构成犯罪的，依法追究刑事责任；尚不构成犯罪的，由公安机关处十日以上十五日以下拘留，并处五千元罚款，有违

法所得的，没收违法所得。

单位有前款行为，构成犯罪的，依法追究刑事责任；尚不构成犯罪的，由公安机关对其直接负责的主管人员和其他直接责任人员，处十日以上十五日以下拘留，并处十万元以上五十万元以下罚款，有违法所得的，没收违法所得。

有前两款行为，对他人造成损害的，依法承担民事责任。

第二十条　人民警察有下列行为之一的，根据情节轻重，依法给予行政处分；构成犯罪的，依法追究刑事责任：

（一）利用制作、发放、查验居民身份证的便利，收受他人财物或者谋取其他利益的；

（二）非法变更公民身份号码，或者在居民身份证上登载本法第三条第一款规定项目以外的信息或者故意登载虚假信息的；

（三）无正当理由不在法定期限内发放居民身份证的；

（四）违反规定查验、扣押居民身份证，侵害公民合法权益的；

（五）泄露因制作、发放、查验、扣押居民身份证而知悉的公民个人信息，侵害公民合法权益的。

第五章　附　则

第二十一条　公民申请领取、换领、补领居民身份证，应当缴纳证件工本费。居民身份证工本费标准，由国务院价格主管部门会同国务院财政部门核定。

对城市中领取最低生活保障金的居民、农村中有特殊生活困难的居民，在其初次申请领取和换领居民身份证时，免收工本费。对其他

生活确有困难的居民，在其初次申请领取和换领居民身份证时，可以减收工本费。免收和减收工本费的具体办法，由国务院财政部门会同国务院价格主管部门规定。

公安机关收取的居民身份证工本费，全部上缴国库。

第二十二条　现役的人民解放军军人、人民武装警察申请领取和发放居民身份证的具体办法，由国务院和中央军事委员会另行规定。

第二十三条　本法自2004年1月1日起施行，《中华人民共和国居民身份证条例》同时废止。

依照《中华人民共和国居民身份证条例》领取的居民身份证，自2013年1月1日起停止使用。依照本法在2012年1月1日以前领取的居民身份证，在其有效期内，继续有效。国家决定换发新一代居民身份证后，原居民身份证的停止使用日期由国务院决定。

二、行政法规

关健信息基础设施安全保护条例

时效性：　　现行有效

发文机关：　国务院

文号：　　国务院令第 745 号

发文日期：　2021 年 07 月 30 日

施行日期：　2021 年 09 月 01 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：

（一）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；

（二）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；

（三）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：

（一）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；

（二）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；

（三）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；

（四）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；

（五）组织网络安全教育、培训；

（六）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；

（七）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；

（八）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：

（一）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；

（二）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；

（三）未建立健全网络安全保护制度和责任制的；

（四）未设置专门安全管理机构的；

（五）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；

（六）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；

（七）专门安全管理机构未履行本条例第十五条规定的职责的；

（八）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；

（九）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；

（十）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。

信息网络传播权保护条例

时效性：　　现行有效

发文机关：　国务院

文号：　　中华人民共和国国务院令第 634 号

发文日期：　2013 年 01 月 30 日

施行日期：　2013 年 03 月 01 日

第一条　为保护著作权人、表演者、录音录像制作者（以下统称权利人）的信息网络传播权，鼓励有益于社会主义精神文明、物质文明建设的作品的创作和传播，根据《中华人民共和国著作权法》（以下简称著作权法），制定本条例。

第二条　权利人享有的信息网络传播权受著作权法和本条例保护。除法律、行政法规另有规定的外，任何组织或者个人将他人的作品、表演、录音录像制品通过信息网络向公众提供，应当取得权利人许可，并支付报酬。

第三条　依法禁止提供的作品、表演、录音录像制品，不受本条例保护。

权利人行使信息网络传播权，不得违反宪法和法律、行政法规，不得损害公共利益。

第四条　为了保护信息网络传播权，权利人可以采取技术措施。

任何组织或者个人不得故意避开或者破坏技术措施，不得故意制造、进口或者向公众提供主要用于避开或者破坏技术措施的装置或者部件，不得故意为他人避开或者破坏技术措施提供技术服务。但是，

法律、行政法规规定可以避开的除外。

第五条　未经权利人许可，任何组织或者个人不得进行下列行为：

（一）故意删除或者改变通过信息网络向公众提供的作品、表演、录音录像制品的权利管理电子信息，但由于技术上的原因无法避免删除或者改变的除外；

（二）通过信息网络向公众提供明知或者应知未经权利人许可被删除或者改变权利管理电子信息的作品、表演、录音录像制品。

第六条　通过信息网络提供他人作品，属于下列情形的，可以不经著作权人许可，不向其支付报酬：

（一）为介绍、评论某一作品或者说明某一问题，在向公众提供的作品中适当引用已经发表的作品；

（二）为报道时事新闻，在向公众提供的作品中不可避免地再现或者引用已经发表的作品；

（三）为学校课堂教学或者科学研究，向少数教学、科研人员提供少量已经发表的作品；

（四）国家机关为执行公务，在合理范围内向公众提供已经发表的作品；

（五）将中国公民、法人或者其他组织已经发表的、以汉语言文字创作的作品翻译成的少数民族语言文字作品，向中国境内少数民族提供；

（六）不以营利为目的，以盲人能够感知的独特方式向盲人提供

已经发表的文字作品；

（七）向公众提供在信息网络上已经发表的关于政治、经济问题的时事性文章；

（八）向公众提供在公众集会上发表的讲话。

第七条　图书馆、档案馆、纪念馆、博物馆、美术馆等可以不经著作权人许可，通过信息网络向本馆馆舍内服务对象提供本馆收藏的合法出版的数字作品和依法为陈列或者保存版本的需要以数字化形式复制的作品，不向其支付报酬，但不得直接或者间接获得经济利益。当事人另有约定的除外。

前款规定的为陈列或者保存版本需要以数字化形式复制的作品，应当是已经损毁或者濒临损毁、丢失或者失窃，或者其存储格式已经过时，并且在市场上无法购买或者只能以明显高于标定的价格购买的作品。

第八条　为通过信息网络实施九年制义务教育或者国家教育规划，可以不经著作权人许可，使用其已经发表作品的片断或者短小的文字作品、音乐作品或者单幅的美术作品、摄影作品制作课件，由制作课件或者依法取得课件的远程教育机构通过信息网络向注册学生提供，但应当向著作权人支付报酬。

第九条　为扶助贫困，通过信息网络向农村地区的公众免费提供中国公民、法人或者其他组织已经发表的种植养殖、防病治病、防灾减灾等与扶助贫困有关的作品和适应基本文化需求的作品，网络服务提供者应当在提供前公告拟提供的作品及其作者、拟支付报酬的标准。

自公告之日起30日内，著作权人不同意提供的，网络服务提供者不得提供其作品；自公告之日起满30日，著作权人没有异议的，网络服务提供者可以提供其作品，并按照公告的标准向著作权人支付报酬。网络服务提供者提供著作权人的作品后，著作权人不同意提供的，网络服务提供者应当立即删除著作权人的作品，并按照公告的标准向著作权人支付提供作品期间的报酬。

依照前款规定提供作品的，不得直接或者间接获得经济利益。

第十条　依照本条例规定不经著作权人许可、通过信息网络向公众提供其作品的，还应当遵守下列规定：

（一）除本条例第六条第一项至第六项、第七条规定的情形外，不得提供作者事先声明不许提供的作品；

（二）指明作品的名称和作者的姓名（名称）；

（三）依照本条例规定支付报酬；

（四）采取技术措施，防止本条例第七条、第八条、第九条规定的服务对象以外的其他人获得著作权人的作品，并防止本条例第七条规定的服务对象的复制行为对著作权人利益造成实质性损害；

（五）不得侵犯著作权人依法享有的其他权利。

第十一条　通过信息网络提供他人表演、录音录像制品的，应当遵守本条例第六条至第十条的规定。

第十二条　属于下列情形的，可以避开技术措施，但不得向他人提供避开技术措施的技术、装置或者部件，不得侵犯权利人依法享有的其他权利：

（一）为学校课堂教学或者科学研究，通过信息网络向少数教学、科研人员提供已经发表的作品、表演、录音录像制品，而该作品、表演、录音录像制品只能通过信息网络获取；

（二）不以营利为目的，通过信息网络以盲人能够感知的独特方式向盲人提供已经发表的文字作品，而该作品只能通过信息网络获取；

（三）国家机关依照行政、司法程序执行公务；

（四）在信息网络上对计算机及其系统或者网络的安全性能进行测试。

第十三条　著作权行政管理部门为了查处侵犯信息网络传播权的行为，可以要求网络服务提供者提供涉嫌侵权的服务对象的姓名（名称）、联系方式、网络地址等资料。

第十四条　对提供信息存储空间或者提供搜索、链接服务的网络服务提供者，权利人认为其服务所涉及的作品、表演、录音录像制品，侵犯自己的信息网络传播权或者被删除、改变了自己的权利管理电子信息的，可以向该网络服务提供者提交书面通知，要求网络服务提供者删除该作品、表演、录音录像制品，或者断开与该作品、表演、录音录像制品的链接。通知书应当包含下列内容：

（一）权利人的姓名（名称）、联系方式和地址；

（二）要求删除或者断开链接的侵权作品、表演、录音录像制品的名称和网络地址；

（三）构成侵权的初步证明材料。

权利人应当对通知书的真实性负责。

第十五条　网络服务提供者接到权利人的通知书后，应当立即删除涉嫌侵权的作品、表演、录音录像制品，或者断开与涉嫌侵权的作品、表演、录音录像制品的链接，并同时将通知书转送提供作品、表演、录音录像制品的服务对象；服务对象网络地址不明、无法转送的，应当将通知书的内容同时在信息网络上公告。

第十六条　服务对象接到网络服务提供者转送的通知书后，认为其提供的作品、表演、录音录像制品未侵犯他人权利的，可以向网络服务提供者提交书面说明，要求恢复被删除的作品、表演、录音录像制品，或者恢复与被断开的作品、表演、录音录像制品的链接。书面说明应当包含下列内容：

（一）服务对象的姓名（名称）、联系方式和地址；

（二）要求恢复的作品、表演、录音录像制品的名称和网络地址；

（三）不构成侵权的初步证明材料。

服务对象应当对书面说明的真实性负责。

第十七条　网络服务提供者接到服务对象的书面说明后，应当立即恢复被删除的作品、表演、录音录像制品，或者可以恢复与被断开的作品、表演、录音录像制品的链接，同时将服务对象的书面说明转送权利人。权利人不得再通知网络服务提供者删除该作品、表演、录音录像制品，或者断开与该作品、表演、录音录像制品的链接。

第十八条　违反本条例规定，有下列侵权行为之一的，根据情况承担停止侵害、消除影响、赔礼道歉、赔偿损失等民事责任；同时损害公共利益的，可以由著作权行政管理部门责令停止侵权行为，没收

违法所得，非法经营额5万元以上的，可处非法经营额1倍以上5倍以下的罚款；没有非法经营额或者非法经营额5万元以下的，根据情节轻重，可处25万元以下的罚款；情节严重的，著作权行政管理部门可以没收主要用于提供网络服务的计算机等设备；构成犯罪的，依法追究刑事责任：

（一）通过信息网络擅自向公众提供他人的作品、表演、录音录像制品的；

（二）故意避开或者破坏技术措施的；

（三）故意删除或者改变通过信息网络向公众提供的作品、表演、录音录像制品的权利管理电子信息，或者通过信息网络向公众提供明知或者应知未经权利人许可而被删除或者改变权利管理电子信息的作品、表演、录音录像制品的；

（四）为扶助贫困通过信息网络向农村地区提供作品、表演、录音录像制品超过规定范围，或者未按照公告的标准支付报酬，或者在权利人不同意提供其作品、表演、录音录像制品后未立即删除的；

（五）通过信息网络提供他人的作品、表演、录音录像制品，未指明作品、表演、录音录像制品的名称或者作者、表演者、录音录像制作者的姓名（名称），或者未支付报酬，或者未依照本条例规定采取技术措施防止服务对象以外的其他人获得他人的作品、表演、录音录像制品，或者未防止服务对象的复制行为对权利人利益造成实质性损害的。

第十九条　违反本条例规定，有下列行为之一的，由著作权行政

管理部门予以警告，没收违法所得，没收主要用于避开、破坏技术措施的装置或者部件；情节严重的，可以没收主要用于提供网络服务的计算机等设备；非法经营额5万元以上的，可处非法经营额1倍以上5倍以下的罚款；没有非法经营额或者非法经营额5万元以下的，根据情节轻重，可处25万元以下的罚款；构成犯罪的，依法追究刑事责任：

（一）故意制造、进口或者向他人提供主要用于避开、破坏技术措施的装置或者部件，或者故意为他人避开或者破坏技术措施提供技术服务的；

（二）通过信息网络提供他人的作品、表演、录音录像制品，获得经济利益的；

（三）为扶助贫困通过信息网络向农村地区提供作品、表演、录音录像制品，未在提供前公告作品、表演、录音录像制品的名称和作者、表演者、录音录像制作者的姓名（名称）以及报酬标准的。

第二十条　网络服务提供者根据服务对象的指令提供网络自动接入服务，或者对服务对象提供的作品、表演、录音录像制品提供自动传输服务，并具备下列条件的，不承担赔偿责任：

（一）未选择并且未改变所传输的作品、表演、录音录像制品；

（二）向指定的服务对象提供该作品、表演、录音录像制品，并防止指定的服务对象以外的其他人获得。

第二十一条　网络服务提供者为提高网络传输效率，自动存储从其他网络服务提供者获得的作品、表演、录音录像制品，根据技术安

排自动向服务对象提供，并具备下列条件的，不承担赔偿责任：

（一）未改变自动存储的作品、表演、录音录像制品；

（二）不影响提供作品、表演、录音录像制品的原网络服务提供者掌握服务对象获取该作品、表演、录音录像制品的情况；

（三）在原网络服务提供者修改、删除或者屏蔽该作品、表演、录音录像制品时，根据技术安排自动予以修改、删除或者屏蔽。

第二十二条　网络服务提供者为服务对象提供信息存储空间，供服务对象通过信息网络向公众提供作品、表演、录音录像制品，并具备下列条件的，不承担赔偿责任：

（一）明确标示该信息存储空间是为服务对象所提供，并公开网络服务提供者的名称、联系人、网络地址；

（二）未改变服务对象所提供的作品、表演、录音录像制品；

（三）不知道也没有合理的理由应当知道服务对象提供的作品、表演、录音录像制品侵权；

（四）未从服务对象提供作品、表演、录音录像制品中直接获得经济利益；

（五）在接到权利人的通知书后，根据本条例规定删除权利人认为侵权的作品、表演、录音录像制品。

第二十三条　网络服务提供者为服务对象提供搜索或者链接服务，在接到权利人的通知书后，根据本条例规定断开与侵权的作品、表演、录音录像制品的链接的，不承担赔偿责任；但是，明知或者应知所链接的作品、表演、录音录像制品侵权的，应当承担共同侵权责

任。

第二十四条　因权利人的通知导致网络服务提供者错误删除作品、表演、录音录像制品，或者错误断开与作品、表演、录音录像制品的链接，给服务对象造成损失的，权利人应当承担赔偿责任。

第二十五条　网络服务提供者无正当理由拒绝提供或者拖延提供涉嫌侵权的服务对象的姓名（名称）、联系方式、网络地址等资料的，由著作权行政管理部门予以警告；情节严重的，没收主要用于提供网络服务的计算机等设备。

第二十六条　本条例下列用语的含义：

信息网络传播权，是指以有线或者无线方式向公众提供作品、表演或者录音录像制品，使公众可以在其个人选定的时间和地点获得作品、表演或者录音录像制品的权利。

技术措施，是指用于防止、限制未经权利人许可浏览、欣赏作品、表演、录音录像制品的或者通过信息网络向公众提供作品、表演、录音录像制品的有效技术、装置或者部件。

权利管理电子信息，是指说明作品及其作者、表演及其表演者、录音录像制品及其制作者的信息，作品、表演、录音录像制品权利人的信息和使用条件的信息，以及表示上述信息的数字或者代码。

第二十七条　本条例自2006年7月1日起施行。

征信业管理条例

时效性：　　现行有效

发文机关：　国务院

文号：　　中华人民共和国国务院令第631号

发文日期：　2013年01月21日

施行日期：　2013年03月15日

第一章　总　则

第一条　为了规范征信活动，保护当事人合法权益，引导、促进征信业健康发展，推进社会信用体系建设，制定本条例。

第二条　在中国境内从事征信业务及相关活动，适用本条例。

本条例所称征信业务，是指对企业、事业单位等组织（以下统称企业）的信用信息和个人的信用信息进行采集、整理、保存、加工，并向信息使用者提供的活动。

国家设立的金融信用信息基础数据库进行信息的采集、整理、保存、加工和提供，适用本条例第五章　规定。

国家机关以及法律、法规授权的具有管理公共事务职能的组织依照法律、行政法规和国务院的规定，为履行职责进行的企业和个人信息的采集、整理、保存、加工和公布，不适用本条例。

第三条　从事征信业务及相关活动，应当遵守法律法规，诚实守信，不得危害国家秘密，不得侵犯商业秘密和个人隐私。

第四条　中国人民银行（以下称国务院征信业监督管理部门）及其派出机构依法对征信业进行监督管理。

县级以上地方人民政府和国务院有关部门依法推进本地区、本行业的社会信用体系建设，培育征信市场，推动征信业发展。

第二章　征信机构

第五条　本条例所称征信机构，是指依法设立，主要经营征信业务的机构。

第六条　设立经营个人征信业务的征信机构，应当符合《中华人民共和国公司法》规定的公司设立条件和下列条件，并经国务院征信业监督管理部门批准：

（一）主要股东信誉良好，最近3年无重大违法违规记录；

（二）注册资本不少于人民币5000万元；

（三）有符合国务院征信业监督管理部门规定的保障信息安全的设施、设备和制度、措施；

（四）拟任董事、监事和高级管理人员符合本条例第八条规定的任职条件；

（五）国务院征信业监督管理部门规定的其他审慎性条件。

第七条　申请设立经营个人征信业务的征信机构，应当向国务院征信业监督管理部门提交申请书和证明其符合本条例第六条规定条件的材料。

国务院征信业监督管理部门应当依法进行审查，自受理申请之日起60日内作出批准或者不予批准的决定。决定批准的，颁发个人征信业务经营许可证；不予批准的，应当书面说明理由。

经批准设立的经营个人征信业务的征信机构，凭个人征信业务经

营许可证向公司登记机关办理登记。

未经国务院征信业监督管理部门批准，任何单位和个人不得经营个人征信业务。

第八条　经营个人征信业务的征信机构的董事、监事和高级管理人员，应当熟悉与征信业务相关的法律法规，具有履行职责所需的征信业从业经验和管理能力，最近3年无重大违法违规记录,并取得国务院征信业监督管理部门核准的任职资格。

第九条　经营个人征信业务的征信机构设立分支机构、合并或者分立、变更注册资本、变更出资额占公司资本总额5%以上或者持股占公司股份5%以上的股东的，应当经国务院征信业监督管理部门批准。

经营个人征信业务的征信机构变更名称的，应当向国务院征信业监督管理部门办理备案。

第十条　设立经营企业征信业务的征信机构，应当符合《中华人民共和国公司法》规定的设立条件，并自公司登记机关准予登记之日起30日内向所在地的国务院征信业监督管理部门派出机构办理备案，并提供下列材料：

（一）营业执照；

（二）股权结构、组织机构说明；

（三）业务范围、业务规则、业务系统的基本情况；

（四）信息安全和风险防范措施。

备案事项发生变更的，应当自变更之日起30日内向原备案机构

办理变更备案。

第十一条　征信机构应当按照国务院征信业监督管理部门的规定，报告上一年度开展征信业务的情况。

国务院征信业监督管理部门应当向社会公告经营个人征信业务和企业征信业务的征信机构名单，并及时更新。

第十二条　征信机构解散或者被依法宣告破产的，应当向国务院征信业监督管理部门报告，并按照下列方式处理信息数据库：

（一）与其他征信机构约定并经国务院征信业监督管理部门同意，转让给其他征信机构；

（二）不能依照前项规定转让的，移交给国务院征信业监督管理部门指定的征信机构；

（三）不能依照前两项规定转让、移交的，在国务院征信业监督管理部门的监督下销毁。

经营个人征信业务的征信机构解散或者被依法宣告破产的，还应当在国务院征信业监督管理部门指定的媒体上公告，并将个人征信业务经营许可证交国务院征信业监督管理部门注销。

第三章　征信业务规则

第十三条　采集个人信息应当经信息主体本人同意，未经本人同意不得采集。但是，依照法律、行政法规规定公开的信息除外。

企业的董事、监事、高级管理人员与其履行职务相关的信息，不作为个人信息。

第十四条　禁止征信机构采集个人的宗教信仰、基因、指纹、血

型、疾病和病史信息以及法律、行政法规规定禁止采集的其他个人信息。

征信机构不得采集个人的收入、存款、有价证券、商业保险、不动产的信息和纳税数额信息。但是，征信机构明确告知信息主体提供该信息可能产生的不利后果，并取得其书面同意的除外。

第十五条　信息提供者向征信机构提供个人不良信息，应当事先告知信息主体本人。但是，依照法律、行政法规规定公开的不良信息除外。

第十六条　征信机构对个人不良信息的保存期限，自不良行为或者事件终止之日起为5年；超过5年的，应当予以删除。

在不良信息保存期限内，信息主体可以对不良信息作出说明，征信机构应当予以记载。

第十七条　信息主体可以向征信机构查询自身信息。个人信息主体有权每年两次免费获取本人的信用报告。

第十八条　向征信机构查询个人信息的，应当取得信息主体本人的书面同意并约定用途。但是，法律规定可以不经同意查询的除外。

征信机构不得违反前款规定提供个人信息。

第十九条　征信机构或者信息提供者、信息使用者采用格式合同条款取得个人信息主体同意的，应当在合同中作出足以引起信息主体注意的提示，并按照信息主体的要求作出明确说明。

第二十条　信息使用者应当按照与个人信息主体约定的用途使用个人信息，不得用作约定以外的用途，不得未经个人信息主体同意

向第三方提供。

第二十一条　征信机构可以通过信息主体、企业交易对方、行业协会提供信息，政府有关部门依法已公开的信息，人民法院依法公布的判决、裁定等渠道，采集企业信息。

征信机构不得采集法律、行政法规禁止采集的企业信息。

第二十二条　征信机构应当按照国务院征信业监督管理部门的规定，建立健全和严格执行保障信息安全的规章制度，并采取有效技术措施保障信息安全。

经营个人征信业务的征信机构应当对其工作人员查询个人信息的权限和程序作出明确规定，对工作人员查询个人信息的情况进行登记，如实记载查询工作人员的姓名，查询的时间、内容及用途。工作人员不得违反规定的权限和程序查询信息，不得泄露工作中获取的信息。

第二十三条　征信机构应当采取合理措施，保障其提供信息的准确性。

征信机构提供的信息供信息使用者参考。

第二十四条　征信机构在中国境内采集的信息的整理、保存和加工，应当在中国境内进行。

征信机构向境外组织或者个人提供信息，应当遵守法律、行政法规和国务院征信业监督管理部门的有关规定。

第四章　异议和投诉

第二十五条　信息主体认为征信机构采集、保存、提供的信息存

在错误、遗漏的，有权向征信机构或者信息提供者提出异议，要求更正。

征信机构或者信息提供者收到异议，应当按照国务院征信业监督管理部门的规定对相关信息作出存在异议的标注，自收到异议之日起20日内进行核查和处理，并将结果书面答复异议人。

经核查，确认相关信息确有错误、遗漏的，信息提供者、征信机构应当予以更正；确认不存在错误、遗漏的，应当取消异议标注；经核查仍不能确认的，对核查情况和异议内容应当予以记载。

第二十六条　信息主体认为征信机构或者信息提供者、信息使用者侵害其合法权益的，可以向所在地的国务院征信业监督管理部门派出机构投诉。

受理投诉的机构应当及时进行核查和处理，自受理之日起30日内书面答复投诉人。

信息主体认为征信机构或者信息提供者、信息使用者侵害其合法权益的，可以直接向人民法院起诉。

第五章　金融信用信息基础数据库

第二十七条　国家设立金融信用信息基础数据库，为防范金融风险、促进金融业发展提供相关信息服务。

金融信用信息基础数据库由专业运行机构建设、运行和维护。该运行机构不以营利为目的，由国务院征信业监督管理部门监督管理。

第二十八条　金融信用信息基础数据库接收从事信贷业务的机构按照规定提供的信贷信息。

金融信用信息基础数据库为信息主体和取得信息主体本人书面同意的信息使用者提供查询服务。国家机关可以依法查询金融信用信息基础数据库的信息。

第二十九条　从事信贷业务的机构应当按照规定向金融信用信息基础数据库提供信贷信息。

从事信贷业务的机构向金融信用信息基础数据库或者其他主体提供信贷信息，应当事先取得信息主体的书面同意，并适用本条例关于信息提供者的规定。

第三十条　不从事信贷业务的金融机构向金融信用信息基础数据库提供、查询信用信息以及金融信用信息基础数据库接收其提供的信用信息的具体办法，由国务院征信业监督管理部门会同国务院有关金融监督管理机构依法制定。

第三十一条　金融信用信息基础数据库运行机构可以按照补偿成本原则收取查询服务费用，收费标准由国务院价格主管部门规定。

第三十二条　本条例第十四条、第十六条、第十七条、第十八条、第二十二条、第二十三条、第二十四条、第二十五条、第二十六条适用于金融信用信息基础数据库运行机构。

第六章　监督管理

第三十三条　国务院征信业监督管理部门及其派出机构依照法律、行政法规和国务院的规定，履行对征信业和金融信用信息基础数据库运行机构的监督管理职责，可以采取下列监督检查措施：

（一）进入征信机构、金融信用信息基础数据库运行机构进行现

场检查，对向金融信用信息基础数据库提供或者查询信息的机构遵守本条例有关规定的情况进行检查；

（二）询问当事人和与被调查事件有关的单位和个人，要求其对与被调查事件有关的事项作出说明；

（三）查阅、复制与被调查事件有关的文件、资料，对可能被转移、销毁、隐匿或者篡改的文件、资料予以封存；

（四）检查相关信息系统。

进行现场检查或者调查的人员不得少于2人，并应当出示合法证件和检查、调查通知书。

被检查、调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。

第三十四条　经营个人征信业务的征信机构、金融信用信息基础数据库、向金融信用信息基础数据库提供或者查询信息的机构发生重大信息泄露等事件的，国务院征信业监督管理部门可以采取临时接管相关信息系统等必要措施，避免损害扩大。

第三十五条　国务院征信业监督管理部门及其派出机构的工作人员对在工作中知悉的国家秘密和信息主体的信息，应当依法保密。

第七章　法律责任

第三十六条　未经国务院征信业监督管理部门批准，擅自设立经营个人征信业务的征信机构或者从事个人征信业务活动的，由国务院征信业监督管理部门予以取缔，没收违法所得，并处5万元以上50万元以下的罚款；构成犯罪的，依法追究刑事责任。

第三十七条　经营个人征信业务的征信机构违反本条例第九条规定的，由国务院征信业监督管理部门责令限期改正，对单位处2万元以上20万元以下的罚款；对直接负责的主管人员和其他直接责任人员给予警告，处1万元以下的罚款。

经营企业征信业务的征信机构未按照本条例第十条规定办理备案的，由其所在地的国务院征信业监督管理部门派出机构责令限期改正；逾期不改正的，依照前款规定处罚。

第三十八条　征信机构、金融信用信息基础数据库运行机构违反本条例规定，有下列行为之一的，由国务院征信业监督管理部门或者其派出机构责令限期改正，对单位处5万元以上50万元以下的罚款；对直接负责的主管人员和其他直接责任人员处1万元以上10万元以下的罚款；有违法所得的，没收违法所得。给信息主体造成损失的，依法承担民事责任；构成犯罪的，依法追究刑事责任：

（一）窃取或者以其他方式非法获取信息；

（二）采集禁止采集的个人信息或者未经同意采集个人信息；

（三）违法提供或者出售信息；

（四）因过失泄露信息；

（五）逾期不删除个人不良信息；

（六）未按照规定对异议信息进行核查和处理；

（七）拒绝、阻碍国务院征信业监督管理部门或者其派出机构检查、调查或者不如实提供有关文件、资料；

（八）违反征信业务规则，侵害信息主体合法权益的其他行为。

经营个人征信业务的征信机构有前款所列行为之一，情节严重或者造成严重后果的，由国务院征信业监督管理部门吊销其个人征信业务经营许可证。

第三十九条　征信机构违反本条例规定，未按照规定报告其上一年度开展征信业务情况的，由国务院征信业监督管理部门或者其派出机构责令限期改正；逾期不改正的，对单位处2万元以上10万元以下的罚款；对直接负责的主管人员和其他直接责任人员给予警告，处1万元以下的罚款。

第四十条　向金融信用信息基础数据库提供或者查询信息的机构违反本条例规定，有下列行为之一的，由国务院征信业监督管理部门或者其派出机构责令限期改正，对单位处5万元以上50万元以下的罚款；对直接负责的主管人员和其他直接责任人员处1万元以上10万元以下的罚款；有违法所得的，没收违法所得。给信息主体造成损失的，依法承担民事责任；构成犯罪的，依法追究刑事责任：

（一）违法提供或者出售信息；

（二）因过失泄露信息；

（三）未经同意查询个人信息或者企业的信贷信息；

（四）未按照规定处理异议或者对确有错误、遗漏的信息不予更正；

（五）拒绝、阻碍国务院征信业监督管理部门或者其派出机构检查、调查或者不如实提供有关文件、资料。

第四十一条　信息提供者违反本条例规定，向征信机构、金融信

用信息基础数据库提供非依法公开的个人不良信息，未事先告知信息主体本人，情节严重或者造成严重后果的，由国务院征信业监督管理部门或者其派出机构对单位处2万元以上20万元以下的罚款；对个人处1万元以上5万元以下的罚款。

第四十二条　信息使用者违反本条例规定，未按照与个人信息主体约定的用途使用个人信息或者未经个人信息主体同意向第三方提供个人信息，情节严重或者造成严重后果的，由国务院征信业监督管理部门或者其派出机构对单位处2万元以上20万元以下的罚款；对个人处1万元以上5万元以下的罚款；有违法所得的，没收违法所得。给信息主体造成损失的，依法承担民事责任；构成犯罪的，依法追究刑事责任。

第四十三条　国务院征信业监督管理部门及其派出机构的工作人员滥用职权、玩忽职守、徇私舞弊，不依法履行监督管理职责，或者泄露国家秘密、信息主体信息的，依法给予处分。给信息主体造成损失的，依法承担民事责任；构成犯罪的，依法追究刑事责任。

第八章　附则

第四十四条　本条例下列用语的含义：

（一）信息提供者，是指向征信机构提供信息的单位和个人，以及向金融信用信息基础数据库提供信息的单位。

（二）信息使用者，是指从征信机构和金融信用信息基础数据库获取信息的单位和个人。

（三）不良信息，是指对信息主体信用状况构成负面影响的下列

信息：信息主体在借贷、赊购、担保、租赁、保险、使用信用卡等活动中未按照合同履行义务的信息，对信息主体的行政处罚信息，人民法院判决或者裁定信息主体履行义务以及强制执行的信息，以及国务院征信业监督管理部门规定的其他不良信息。

第四十五条　外商投资征信机构的设立条件，由国务院征信业监督管理部门会同国务院有关部门制定，报国务院批准。

境外征信机构在境内经营征信业务，应当经国务院征信业监督管理部门批准。

第四十六条　本条例施行前已经经营个人征信业务的机构，应当自本条例施行之日起6个月内，依照本条例的规定申请个人征信业务经营许可证。

本条例施行前已经经营企业征信业务的机构，应当自本条例施行之日起3个月内，依照本条例的规定办理备案。

第四十七条　本条例自2013年3月15日起施行。

计算机信息网络国际联网安全保护管理办法

时效性：　　现行有效

发文机关：　国务院

文号：　　国务院令第588号

发文日期：　2011年01月08日

施行日期：　2011年01月08日

第一章　总　则

第一条　为了加强对计算机信息网络国际联网的安全保护，维护公共秩序和社会稳定，根据《中华人民共和国计算机信息系统安全保护条例》、《中华人民共和国计算机信息网络国际联网管理暂行规定》和其他法律、行政法规的规定，制定本办法。

第二条　中华人民共和国境内的计算机信息网络国际联网安全保护管理，适用本办法。

第三条　公安部计算机管理监察机构负责计算机信息网络国际联网的安全保护管理工作。

公安机关计算机管理监察机构应当保护计算机信息网络国际联网的公共安全，维护从事国际联网业务的单位和个人的合法权益和公众利益。

第四条　任何单位和个人不得利用国际联网危害国家安全、泄露国家秘密，不得侵犯国家的、社会的、集体的利益和公民的合法权益，不得从事违法犯罪活动。

第五条　任何单位和个人不得利用国际联网制作、复制、查阅和

传播下列信息：

（一）煽动抗拒、破坏 宪法和法律、行政法规实施的；

（二）煽动颠覆国家政权，推翻社会主义制度的；

（三）煽动分裂国家、破坏国家统一的；

（四）煽动民族仇恨、民族歧视，破坏民族团结的；

（五）捏造或者歪曲事实，散布谣言，扰乱社会秩序的；

（六）宣扬封建迷信、淫秽、色情、赌博、暴力、凶杀、恐怖，教唆犯罪的；

（七）公然侮辱他人或者捏造事实诽谤他人的；

（八）损害国家机关信誉的；

（九）其他违反 宪法和法律、行政法规的。

第六条　任何单位和个人不得从事下列危害计算机信息网络安全的活动：

（一）未经允许，进入计算机信息网络或者使用计算机信息网络资源的；

（二）未经允许，对计算机信息网络功能进行删除、修改或者增加的；

（三）未经允许，对计算机信息网络中存储、处理或者传输的数据和应用程序进行删除、修改或者增加的；

（四）故意制作、传播计算机病毒等破坏性程序的；

（五）其他危害计算机信息网络安全的。

第七条　用户的通信自由和通信秘密受法律保护。任何单位和个

人不得违反法律规定，利用国际联网侵犯用户的通信自由和通信秘密。

第二章　安全保护责任

第八条　从事国际联网业务的单位和个人应当接受公安机关的安全监督、检查和指导，如实向公安机关提供有关安全保护的信息、资料及数据文件，协助公安机关查处通过国际联网的计算机信息网络的违法犯罪行为。

第九条　国际出入口信道提供单位、互联单位的主管部门或者主管单位，应当依照法律和国家有关规定负责国际出入口信道、所属互联网络的安全保护管理工作。

第十条　互联单位、接入单位及使用计算机信息网络国际联网的法人和其他组织应当履行下列安全保护职责：

（一）负责本网络的安全保护管理工作，建立健全安全保护管理制度；

（二）落实安全保护技术措施，保障本网络的运行安全和信息安全；

（三）负责对本网络用户的安全教育和培训；

（四）对委托发布信息的单位和个人进行登记，并对所提供的信息内容按照本办法第五条进行审核；

（五）建立计算机信息网络电子公告系统的用户登记和信息管理制度；

（六）发现有本办法第四条、第五条、第六条、第七条所列情形之一的，应当保留有关原始记录，并在24小时内向当地公安机关报告；

（七）按照国家有关规定，删除本网络中含有本办法第五条内容的地址、目录或者关闭服务器。

第十一条　用户在接入单位办理入网手续时，应当填写用户备案表。备案表由公安部监制。

第十二条　互联单位、接入单位、使用计算机信息网络国际联网的法人和其他组织（包括跨省、自治区、直辖市联网的单位和所属的分支机构），应当自网络正式联通之日起30日内，到所在地的省、自治区、直辖市人民政府公安机关指定的受理机关办理备案手续。

前款所列单位应当负责将接入本网络的接入单位和用户情况报当地公安机关备案，并及时报告本网络中接入单位和用户的变更情况。

第十三条　使用公用账号的注册者应当加强对公用账号的管理，建立账号使用登记制度。用户账号不得转借、转让。

第十四条　涉及国家事务、经济建设、国防建设、尖端科学技术等重要领域的单位办理备案手续时，应当出具其行政主管部门的审批证明。

前款所列单位的计算机信息网络与国际联网，应当采取相应的安全保护措施。

第三章　安全监督

第十五条　省、自治区、直辖市公安厅（局），地（市）、县（市）公安局，应当有相应机构负责国际联网的安全保护管理工作。

第十六条　公安机关计算机管理监察机构应当掌握互联单位、接入单位和用户的备案情况，建立备案档案，进行备案统计，并按照国

家有关规定逐级上报。

第十七条　公安机关计算机管理监察机构应当督促互联单位、接入单位及有关用户建立健全安全保护管理制度。监督、检查网络安全保护管理以及技术措施的落实情况。

公安机关计算机管理监察机构在组织安全检查时，有关单位应当派人参加。公安机关计算机管理监察机构对安全检查发现的问题，应当提出改进意见，作出详细记录，存档备查。

第十八条　公安机关计算机管理监察机构发现含有本办法第五条所列内容的地址、目录或者服务器时，应当通知有关单位关闭或者删除。

第十九条　公安机关计算机管理监察机构应当负责追踪和查处通过计算机信息网络的违法行为和针对计算机信息网络的犯罪案件，对违反本办法第四条、第七条规定的违法犯罪行为，应当按照国家有关规定移送有关部门或者司法机关处理。

第四章　法律责任

第二十条　违反法律、行政法规，有本办法第五条、第六条所列行为之一的，由公安机关给予警告，有违法所得的，没收违法所得，对个人可以并处5000元以下的罚款，对单位可以并处1.5万元以下的罚款；情节严重的，并可以给予6个月以内停止联网、停机整顿的处罚，必要时可以建议原发证、审批机构吊销经营许可证或者取消联网资格；构成违反治安管理行为的，依照 治安管理处罚法的规定处罚；构成犯罪的，依法追究刑事责任。

第二十一条　有下列行为之一的，由公安机关责令限期改正，给予警告，有违法所得的，没收违法所得；在规定的限期内未改正的，对单位的主管负责人员和其他直接责任人员可以并处5000元以下的罚款，对单位可以并处1.5万元以下的罚款；情节严重的，并可以给予6个月以内的停止联网、停机整顿的处罚，必要时可以建议原发证、审批机构吊销经营许可证或者取消联网资格。

（一）未建立安全保护管理制度的；

（二）未采取安全技术保护措施的；

（三）未对网络用户进行安全教育和培训的；

（四）未提供安全保护管理所需信息、资料及数据文件，或者所提供内容不真实的；

（五）对委托其发布的信息内容未进行审核或者对委托单位和个人未进行登记的；

（六）未建立电子公告系统的用户登记和信息管理制度的；

（七）未按照国家有关规定，删除网络地址、目录或者关闭服务器的；

（八）未建立公用账号使用登记制度的；

（九）转借、转让用户账号的。

第二十二条　违反本办法第四条、第七条规定的，依照有关法律、法规予以处罚。

第二十三条　违反本办法第十一条、第十二条规定，不履行备案职责的，由公安机关给予警告或者停机整顿不超过6个月的处罚。

第五章　附　则

第二十四条　与香港特别行政区和台湾、澳门地区联网的计算机信息网络的安全保护管理，参照本办法执行。

第二十五条　本办法自1997年12月30日起施行。

中华人民共和国计算机信息网络国际联网管理暂行规定

时效性：　　已被修改

发文机关：　国务院

文号：　　国务院令[第 195 号]

发文日期：　1996 年 02 月 01 日

施行日期：　1996 年 02 月 01 日

第一条　为了加强对计算机信息网络国际联网的管理，保障国际计算机信息交流的健康发展，制定本规定。

第二条　中华人民共和国境内的计算机信息网络进行国际联网，应当依照本规定办理。

第三条　本规定下列用语的含义是：

（一）计算机信息网络国际联网（以下简称国际联网），是指中华人民共和国境内的计算机信息网络为实现信息的国际交流，同外国的计算机信息网络相联接。

（二）互联网络，是指直接进行国际联网的计算机信息网络；互联单位，是指负责互联网络运行的单位。

（三）接入网络，是指通过接入互联网络进行国际联网的计算机信息网络；接入单位，是指负责接入网络运行的单位。

第四条　国家对国际联网实行统筹规划、统一标准、分级管理、促进发展的原则。

第五条　国务院经济信息化领导小组（以下简称领导小组），负责协调、解决有关国际联网工作中的重大问题。

领导小组办公室按照本规定制定具体管理办法，明确国际出入口信道提供单位、互联单位、接入单位和用户的权利、义务和责任，并负责对国际联网工作的检查监督。

第六条　计算机信息网络直接进行国际联网，必须使用邮电部国家公用电信网提供的国际出入口信道。

任何单位和个人不得自行建立或者使用其他信道进行国际联网。

第七条　已经建立的互联网络，根据国务院有关规定调整后，分别由邮电部、电子工业部、国家教育委员会和中国科学院管理。

新建互联网络，必须报经国务院批准。

第八条　接入网络必须通过互联网络进行国际联网。

拟建立接入网络的单位，应当报经互联单位的主管部门或者主管单位审批；办理审批手续时，应当提供其计算机信息网络的性质、应用范围和所需主机地址等资料。

第九条　接入单位必须具备下列条件：

（一）是依法设立的企业法人或者事业法人；

（二）具有相应的计算机信息网络、装备以及相应的技术人员和管理人员；

（三）具有健全的安全保密管理制度和技术保护措施；

（四）符合法律和国务院规定的其他条件。

第十条　个人、法人和其他组织（以下统称用户）使用的计算机或者计算机信息网络，需要进行国际联网的，必须通过接入网络进行国际联网。

前款规定的计算机或者计算机信息网络，需要接入接入网络的，应当征得接入单位的同意，并办理登记手续。

第十一条　国际出入口信道提供单位、互联单位和接入单位，应当建立相应的网络管理中心，依照法律和国家有关规定加强对本单位及其用户的管理，做好网络信息安全管理工作，确保为用户提供良好、安全的服务。

第十二条　互联单位与接入单位，应当负责本单位及其用户有关国际联网的技术培训和管理教育工作。

第十三条　从事国际联网业务的单位和个人，应当遵守国家有关法律、行政法规，严格执行安全保密制度，不得利用国际联网从事危害国家安全、泄露国家秘密等违法犯罪活动，不得制作、查阅、复制和传播妨碍社会治安的信息和淫秽色情等信息。

第十四条　违反本规定第六条、第八条和第十条规定的，由公安机关或者公安机关根据国际出入口信道提供单位、互联单位、接入单位的意见，给予警告、通报批评、责令停止联网，可以并处15000元以下的罚款。

第十五条　违反本规定，同时触犯其他有关法律、行政法规的，依照有关法律、行政法规的规定予以处罚；构成犯罪的，依法追究刑事责任。

第十六条　与台湾、香港、澳门地区的计算机信息网络的联网，参照本规定执行。

第十七条　本规定自发布之日起施行。

中华人民共和国计算机信息系统安全保护条例

时效性：　　现行有效

发文机关：　国务院

文号：　　国务院令第588号

发文日期：　2011年01月08日

施行日期：　2011年01月08日

第一章　总　则

第一条　为了保护计算机信息系统的安全，促进计算机的应用和发展，保障社会主义现代化建设的顺利进行，制定本条例。

第二条　本条例所称的计算机信息系统，是指由计算机及其相关的和配套的设备、设施（含网络）构成的，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、检索等处理的人机系统。

第三条　计算机信息系统的安全保护，应当保障计算机及其相关的和配套的设备、设施（含网络）的安全，运行环境的安全，保障信息的安全，保障计算机功能的正常发挥，以维护计算机信息系统的安全运行。

第四条　计算机信息系统的安全保护工作，重点维护国家事务、经济建设、国防建设、尖端科学技术等重要领域的计算机信息系统的安全。

第五条　中华人民共和国境内的计算机信息系统的安全保护，适用本条例。

未联网的微型计算机的安全保护办法，另行制定。

第六条　公安部主管全国计算机信息系统安全保护工作。

国家安全部、国家保密局和国务院其他有关部门，在国务院规定的职责范围内做好计算机信息系统安全保护的有关工作。

第七条　任何组织或者个人，不得利用计算机信息系统从事危害国家利益、集体利益和公民合法利益的活动，不得危害计算机信息系统的安全。

第二章　安全保护制度

第八条　计算机信息系统的建设和应用，应当遵守法律、行政法规和国家其他有关规定。

第九条　计算机信息系统实行安全等级保护。安全等级的划分标准和安全等级保护的具体办法，由公安部会同有关部门制定。

第十条　计算机机房应当符合国家标准和国家有关规定。

在计算机机房附近施工，不得危害计算机信息系统的安全。

第十一条　进行国际联网的计算机信息系统，由计算机信息系统的使用单位报省级以上人民政府公安机关备案。

第十二条　运输、携带、邮寄计算机信息媒体进出境的，应当如实向海关申报。

第十三条　计算机信息系统的使用单位应当建立健全安全管理制度，负责本单位计算机信息系统的安全保护工作。

第十四条　对计算机信息系统中发生的案件，有关使用单位应当在24小时内向当地县级以上人民政府公安机关报告。

第十五条　对计算机病毒和危害社会公共安全的其他有害数据的防治研究工作，由公安部归口管理。

第十六条　国家对计算机信息系统安全专用产品的销售实行许可证制度。具体办法由公安部会同有关部门制定。

第三章　安　全　监　督

第十七条　公安机关对计算机信息系统安全保护工作行使下列监督职权：

（一）监督、检查、指导计算机信息系统安全保护工作；

（二）查处危害计算机信息系统安全的违法犯罪案件；

（三）履行计算机信息系统安全保护工作的其他监督职责。

第十八条　公安机关发现影响计算机信息系统安全的隐患时，应当及时通知使用单位采取安全保护措施。

第十九条　公安部在紧急情况下，可以就涉及计算机信息系统安全的特定事项发布专项通令。

第四章　法律　责　任

第二十条　违反本条例的规定，有下列行为之一的，由公安机关处以警告或者停机整顿：

（一）违反计算机信息系统安全等级保护制度，危害计算机信息系统安全的；

（二）违反计算机信息系统国际联网备案制度的；

（三）不按照规定时间报告计算机信息系统中发生的案件的；

（四）接到公安机关要求改进安全状况的通知后，在限期内拒不改进的；

（五）有危害计算机信息系统安全的其他行为的。

第二十一条　计算机机房不符合国家标准和国家其他有关规定的，或者在计算机机房附近施工危害计算机信息系统安全的，由公安机关会同有关单位进行处理。

第二十二条　运输、携带、邮寄计算机信息媒体进出境，不如实向海关申报的，由海关依照《中华人民共和国海关法》和本条例以及其他有关法律、法规的规定处理。

第二十三条　故意输入计算机病毒以及其他有害数据危害计算机信息系统安全的，或者未经许可出售计算机信息系统安全专用产品的，由公安机关处以警告或者对个人处以5000元以下的罚款、对单位处以1　5万元以下的罚款；有违法所得的，除予以没收外，可以处以违法所得1至3倍的罚款。

第二十四条　违反本条例的规定，构成违反治安管理行为的，依照《中华人民共和国治安管理处罚法》的有关规定处罚；构成犯罪的，依法追究刑事责任。

第二十五条　任何组织或者个人违反本条例的规定，给国家、集体或者他人财产造成损失的，应当依法承担民事责任。

第二十六条　当事人对公安机关依照本条例所作出的具体行政行为不服的，可以依法申请行政复议或者提起行政诉讼。

第二十七条　执行本条例的国家公务员利用职权，索取、收受贿赂或者有其他违法、失职行为，构成犯罪的，依法追究刑事责任；尚不构成犯罪的，给予行政处分。

第五章　附　则

第二十八条　本条例下列用语的含义：

计算机病毒，是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码。

计算机信息系统安全专用产品，是指用于保护计算机信息系统安全的专用硬件和软件产品。

第二十九条　军队的计算机信息系统安全保护工作，按照军队的有关法规执行。

第三十条　公安部可以根据本条例制定实施办法。

第三十一条　本条例自发布之日起施行。

互联网信息服务管理办法

时效性：　　现行有效

发文机关：　国务院

文号：　　国务院令第588号

发文日期：　2011年01月08日

施行日期：　2011年01月08日

第一条　为了规范互联网信息服务活动，促进互联网信息服务健康有序发展，制定本办法。

第二条　在中华人民共和国境内从事互联网信息服务活动，必须遵守本办法。

本办法所称互联网信息服务，是指通过互联网向上网用户提供信息的服务活动。

第三条　互联网信息服务分为经营性和非经营性两类。

经营性互联网信息服务，是指通过互联网向上网用户有偿提供信息或者网页制作等服务活动。

非经营性互联网信息服务，是指通过互联网向上网用户无偿提供具有公开性、共享性信息的服务活动。

第四条　国家对经营性互联网信息服务实行许可制度；对非经营性互联网信息服务实行备案制度。

未取得许可或者未履行备案手续的，不得从事互联网信息服务。

第五条　从事新闻、出版、教育、医疗保健、药品和医疗器械等互联网信息服务，依照法律、行政法规以及国家有关规定须经有关主管部门审核同意的，在申请经营许可或者履行备案手续前，应当依法

经有关主管部门审核同意。

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

（一）有业务发展计划及相关技术方案；

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

（三）服务项目属于本办法第五条规定范围的，已取得有关主管部门同意的文件。

第七条　从事经营性互联网信息服务，应当向省、自治区、直辖市电信管理机构或者国务院信息产业主管部门申请办理互联网信息服务增值电信业务经营许可证（以下简称经营许可证）。

省、自治区、直辖市电信管理机构或者国务院信息产业主管部门应当自收到申请之日起60日内审查完毕，作出批准或者不予批准的决定。予以批准的，颁发经营许可证；不予批准的，应当书面通知申请人并说明理由。

申请人取得经营许可证后，应当持经营许可证向企业登记机关办理登记手续。

第八条　从事非经营性互联网信息服务，应当向省、自治区、直辖市电信管理机构或者国务院信息产业主管部门办理备案手续。办理备案时，应当提交下列材料：

（一）主办单位和网站负责人的基本情况；

（二）网站网址和服务项目；

（三）服务项目属于本办法第五条规定范围的，已取得有关主管部门的同意文件。

省、自治区、直辖市电信管理机构对备案材料齐全的，应当予以备案并编号。

第九条　从事互联网信息服务，拟开办电子公告服务的，应当在申请经营性互联网信息服务许可或者办理非经营性互联网信息服务备案时，按照国家有关规定提出专项申请或者专项备案。

第十条　省、自治区、直辖市电信管理机构和国务院信息产业主管部门应当公布取得经营许可证或者已履行备案手续的互联网信息服务提供者名单。

第十一条　互联网信息服务提供者应当按照经许可或者备案的项目提供服务，不得超出经许可或者备案的项目提供服务。

非经营性互联网信息服务提供者不得从事有偿服务。

互联网信息服务提供者变更服务项目、网站网址等事项的，应当提前30日向原审核、发证或者备案机关办理变更手续。

第十二条　互联网信息服务提供者应当在其网站主页的显著位置标明其经营许可证编号或者备案编号。

第十三条　互联网信息服务提供者应当向上网用户提供良好的服务，并保证所提供的信息内容合法。

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

户账号、互联网地址或者域名、主叫电话号码等信息。

互联网信息服务提供者和互联网接入服务提供者的记录备份应当保存60日，并在国家有关机关依法查询时，予以提供。

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

（一）反对 宪法所确定的基本原则的；

（二）危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一的；

（三）损害国家荣誉和利益的；

（四）煽动民族仇恨、民族歧视，破坏民族团结的；

（五）破坏国家宗教政策，宣扬邪教和封建迷信的；

（六）散布谣言，扰乱社会秩序，破坏社会稳定的；

（七）散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的；

（八）侮辱或者诽谤他人，侵害他人合法权益的；

（九）含有法律、行政法规禁止的其他内容的。

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

第十七条　经营性互联网信息服务提供者申请在境内境外上市或者同外商合资、合作，应当事先经国务院信息产业主管部门审查同意；其中，外商投资的比例应当符合有关法律、行政法规的规定。

第十八条　国务院信息产业主管部门和省、自治区、直辖市电信管理机构，依法对互联网信息服务实施监督管理。

新闻、出版、教育、卫生、药品监督管理、工商行政管理和公安、国家安全等有关主管部门，在各自职责范围内依法对互联网信息内容实施监督管理。

第十九条　违反本办法的规定，未取得经营许可证，擅自从事经营性互联网信息服务，或者超出许可的项目提供服务的，由省、自治区、直辖市电信管理机构责令限期改正，有违法所得的，没收违法所得，处违法所得3倍以上5倍以下的罚款；没有违法所得或者违法所得不足5万元的，处10万元以上100万元以下的罚款；情节严重的，责令关闭网站。

违反本办法的规定，未履行备案手续，擅自从事非经营性互联网信息服务，或者超出备案的项目提供服务的，由省、自治区、直辖市电信管理机构责令限期改正；拒不改正的，责令关闭网站。

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

第二十一条　未履行本办法第十四条规定的义务的，由省、自治

区、直辖市电信管理机构责令改正；情节严重的，责令停业整顿或者暂时关闭网站。

第二十二条　违反本办法的规定，未在其网站主页上标明其经营许可证编号或者备案编号的，由省、自治区、直辖市电信管理机构责令改正，处5000元以上5万元以下的罚款。

第二十三条　违反本办法第十六条规定的义务的，由省、自治区、直辖市电信管理机构责令改正；情节严重的，对经营性互联网信息服务提供者，并由发证机关吊销经营许可证，对非经营性互联网信息服务提供者，并由备案机关责令关闭网站。

第二十四条　互联网信息服务提供者在其业务活动中，违反其他法律、法规的，由新闻、出版、教育、卫生、药品监督管理和工商行政管理等有关主管部门依照有关法律、法规的规定处罚。

第二十五条　电信管理机构和其他有关主管部门及其工作人员，玩忽职守、滥用职权、徇私舞弊，疏于对互联网信息服务的监督管理，造成严重后果，构成犯罪的，依法追究刑事责任；尚不构成犯罪的，对直接负责的主管人员和其他直接责任人员依法给予降级、撤职直至开除的行政处分。

第二十六条　在本办法公布前从事互联网信息服务的，应当自本办法公布之日起60日内依照本办法的有关规定补办有关手续。

第二十七条　本办法自公布之日起施行。

三、部门规章及规范性文件

汽车数据安全管理若干规定（试行）

时效性：　　现行有效

发文机关：　国家互联网信息办公室、国家发展和改革委员会、工业和信息化部、公安部、交通运输部

文号：　　国家互联网信息办公室、国家发展和改革委员会、工业和信息化部、公安部、交通运输部令第 7 号

发文日期：　2021 年 08 月 16 日

施行日期：　2021 年 10 月 01 日

第一条　为了规范汽车数据处理活动，保护个人、组织的合法权益，维护国家安全和社会公共利益，促进汽车数据合理开发利用，根据《中华人民共和国网络安全法》、《中华人民共和国数据安全法》等法律、行政法规，制定本规定。

第二条　在中华人民共和国境内开展汽车数据处理活动及其安全监管，应当遵守相关法律、行政法规和本规定的要求。

第三条　本规定所称汽车数据，包括汽车设计、生产、销售、使用、运维等过程中的涉及个人信息数据和重要数据。

汽车数据处理，包括汽车数据的收集、存储、使用、加工、传输、提供、公开等。

汽车数据处理者，是指开展汽车数据处理活动的组织，包括汽车制造商、零部件和软件供应商、经销商、维修机构以及出行服务企业等。

个人信息，是指以电子或者其他方式记录的与已识别或者可识别的车主、驾驶人、乘车人、车外人员等有关的各种信息，不包括匿名化处理后的信息。

敏感个人信息，是指一旦泄露或者非法使用，可能导致车主、驾驶人、乘车人、车外人员等受到歧视或者人身、财产安全受到严重危害的个人信息，包括车辆行踪轨迹、音频、视频、图像和生物识别特征等信息。

重要数据是指一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能危害国家安全、公共利益或者个人、组织合法权益的数据，包括：

（一）军事管理区、国防科工单位以及县级以上党政机关等重要敏感区域的地理信息、人员流量、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。

网络产品安全漏洞管理规定

时效性：　　现行有效

发文机关：　工业和信息化部,国家互联网信息办公室,公安部

文号：　　工信部联网安〔2021〕66号

发文日期：　2021年07月12日

施行日期：　2021年09月01日

第一条　为了规范网络产品安全漏洞发现、报告、修补和发布等行为，防范网络安全风险，根据《中华人民共和国网络安全法》，制定本规定。

第二条　中华人民共和国境内的网络产品（含硬件、软件）提供者和网络运营者，以及从事网络产品安全漏洞发现、收集、发布等活动的组织或者个人，应当遵守本规定。

第三条　国家互联网信息办公室负责统筹协调网络产品安全漏洞管理工作。工业和信息化部负责网络产品安全漏洞综合管理，承担电信和互联网行业网络产品安全漏洞监督管理。公安部负责网络产品安全漏洞监督管理，依法打击利用网络产品安全漏洞实施的违法犯罪活动。

有关主管部门加强跨部门协同配合，实现网络产品安全漏洞信息实时共享，对重大网络产品安全漏洞风险开展联合评估和处置。

第四条　任何组织或者个人不得利用网络产品安全漏洞从事危害网络安全的活动，不得非法收集、出售、发布网络产品安全漏洞信息；明知他人利用网络产品安全漏洞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。

第五条　网络产品提供者、网络运营者和网络产品安全漏洞收集平台应当建立健全网络产品安全漏洞信息接收渠道并保持畅通，留存网络产品安全漏洞信息接收日志不少于6个月。

第六条　鼓励相关组织和个人向网络产品提供者通报其产品存在的安全漏洞。

第七条　网络产品提供者应当履行下列网络产品安全漏洞管理义务，确保其产品安全漏洞得到及时修补和合理发布，并指导支持产品用户采取防范措施：

（一）发现或者获知所提供网络产品存在安全漏洞后，应当立即采取措施并组织对安全漏洞进行验证，评估安全漏洞的危害程度和影响范围；对属于其上游产品或者组件存在的安全漏洞，应当立即通知相关产品提供者。

（二）应当在2日内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相关漏洞信息。报送内容应当包括存在网络产品安全漏洞的产品名称、型号、版本以及漏洞的技术特点、危害和影响范围等。

（三）应当及时组织对网络产品安全漏洞进行修补，对于需要产品用户（含下游厂商）采取软件、固件升级等措施的，应当及时将网络产品安全漏洞风险及修补方式告知可能受影响的产品用户，并提供必要的技术支持。

工业和信息化部网络安全威胁和漏洞信息共享平台同步向国家网络与信息安全信息通报中心、国家计算机网络应急技术处理协调中

心通报相关漏洞信息。

鼓励网络产品提供者建立所提供网络产品安全漏洞奖励机制，对发现并通报所提供网络产品安全漏洞的组织或者个人给予奖励。

第八条　网络运营者发现或者获知其网络、信息系统及其设备存在安全漏洞后，应当立即采取措施，及时对安全漏洞进行验证并完成修补。

第九条　从事网络产品安全漏洞发现、收集的组织或者个人通过网络平台、媒体、会议、竞赛等方式向社会发布网络产品安全漏洞信息的，应当遵循必要、真实、客观以及有利于防范网络安全风险的原则，并遵守以下规定：

（一）不得在网络产品提供者提供网络产品安全漏洞修补措施之前发布漏洞信息；认为有必要提前发布的，应当与相关网络产品提供者共同评估协商，并向工业和信息化部、公安部报告，由工业和信息化部、公安部组织评估后进行发布。

（二）不得发布网络运营者在用的网络、信息系统及其设备存在安全漏洞的细节情况。

（三）不得刻意夸大网络产品安全漏洞的危害和风险，不得利用网络产品安全漏洞信息实施恶意炒作或者进行诈骗、敲诈勒索等违法犯罪活动。

（四）不得发布或者提供专门用于利用网络产品安全漏洞从事危害网络安全活动的程序和工具。

（五）在发布网络产品安全漏洞时，应当同步发布修补或者防范

措施。

（六）在国家举办重大活动期间，未经公安部同意，不得擅自发布网络产品安全漏洞信息。

（七）不得将未公开的网络产品安全漏洞信息向网络产品提供者之外的境外组织或者个人提供。

（八）法律法规的其他相关规定。

第十条　任何组织或者个人设立的网络产品安全漏洞收集平台，应当向工业和信息化部备案。工业和信息化部及时向公安部、国家互联网信息办公室通报相关漏洞收集平台，并对通过备案的漏洞收集平台予以公布。

鼓励发现网络产品安全漏洞的组织或者个人向工业和信息化部网络安全威胁和漏洞信息共享平台、国家网络与信息安全信息通报中心漏洞平台、国家计算机网络应急技术处理协调中心漏洞平台、中国信息安全测评中心漏洞库报送网络产品安全漏洞信息。

第十一条　从事网络产品安全漏洞发现、收集的组织应当加强内部管理，采取措施防范网络产品安全漏洞信息泄露和违规发布。

第十二条　网络产品提供者未按本规定采取网络产品安全漏洞补救或者报告措施的，由工业和信息化部、公安部依据各自职责依法处理；构成《中华人民共和国网络安全法》第六十条规定情形的，依照该规定予以处罚。

第十三条　网络运营者未按本规定采取网络产品安全漏洞修补或者防范措施的，由有关主管部门依法处理；构成《中华人民共和国网络安

全法》第五十九条规定情形的，依照该规定予以处罚。

第十四条　违反本规定收集、发布网络产品安全漏洞信息的，由工业和信息化部、公安部依据各自职责依法处理；构成《中华人民共和国网络安全法》第六十二条规定情形的，依照该规定予以处罚。

第十五条　利用网络产品安全漏洞从事危害网络安全活动，或者为他人利用网络产品安全漏洞从事危害网络安全的活动提供技术支持的，由公安机关依法处理；构成《中华人民共和国网络安全法》第六十三条规定情形的，依照该规定予以处罚；构成犯罪的，依法追究刑事责任。

第十六条　本规定自2021年9月1日起施行。

网络交易监督管理办法

时效性：　　现行有效

发文机关：　国家市场监督管理总局

文号：　　国家市场监督管理总局令第37号

发文日期：　2021年03月15日

施行日期：　2021年05月01日

第一章　总　则

第一条　为了规范网络交易活动，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，根据有关法律、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（以下简称通过网络）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、规章和商业道德、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。

第五条　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。

县级以上地方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工作。

第六条　市场监督管理部门引导网络交易经营者、网络交易行业组织、消费者组织、消费者共同参与网络交易市场治理，推动完善多元参与、有效协同、规范有序的网络交易市场治理体系。

第二章　网络交易经营者

第一节　一般规定

第七条　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、网络直播等网络服务提供者为经营者提供网络经营场所、商品浏览、订单生成、在线支付等网络交易平台服务的，应当依法履行网络交易平台经营者的义务。通过上述网络交易平台服务开展网络交易活动的经营者，应当依法履行平台内经营者的义务。

第八条　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。除《中华人民共和国电子商务法》第十条规定的不需要进行登记的情形外，网络交易经营者应当依法办理市场主体登记。

个人通过网络从事保洁、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依法无须取得许可的便民劳务活动，依照《中华人民共和国电子商务法》第十条的规定不需要进行登记。

个人从事网络交易活动，年交易额累计不超过10万元的，依照《中华人民共和国电子商务法》第十条的规定不需要进行登记。同一经营者在同一平台或者不同平台开设多家网店的，各网店交易额合并计算。个人从事的零星小额交易须依法取得行政许可的，应当依法办理市场主体登记。

第九条　仅通过网络开展经营活动的平台内经营者申请登记为个体工商户的，可以将网络经营场所登记为经营场所，将经常居住地登记为住所，其住所所在地的县、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。同一经营者有两个以上网络经营场所的，应当一并登记。

第十条　平台内经营者申请将网络经营场所登记为经营场所的，由其入驻的网络交易平台为其出具符合登记机关要求的网络经营场所相关材料。

第十一条　网络交易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，损害国家利益和社会公共利益，违背公序良

俗的商品或者服务。

第十二条　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如实公示下列营业执照信息以及与其经营业务有关的行政许可等信息，或者该信息的链接标识：

（一）企业应当公示其营业执照登载的统一社会信用代码、名称、企业类型、法定代表人（负责人）、住所、注册资本（出资额）等信息；

（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、名称、经营者姓名、经营场所、组成形式等信息；

（三）农民专业合作社、农民专业合作社联合社应当公示其营业执照登载的统一社会信用代码、名称、法定代表人、住所、成员出资总额等信息。

依照《中华人民共和国电子商务法》第十条规定不需要进行登记的经营者应当根据自身实际经营活动类型，如实公示以下自我声明以及实际经营地址、联系方式等信息，或者该信息的链接标识：

（一）“个人销售自产农副产品，依法不需要办理市场主体登记”；

（二）“个人销售家庭手工业产品，依法不需要办理市场主体登记”；

（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，依法不需要办理市场主体登记”；

（四）“个人从事零星小额交易活动，依法不需要办理市场主体登记”。

网络交易经营者公示的信息发生变更的，应当在十个工作日内完成更新公示。

第十三条　网络交易经营者收集、使用消费者个人信息，应当遵循合法、正当、必要的原则，明示收集、使用信息的目的、方式和范围，并经消费者同意。网络交易经营者收集、使用消费者个人信息，应当公开其收集、使用规则，不得违反法律、法规的规定和双方的约定收集、使用信息。

网络交易经营者不得采用一次概括授权、默认授权、与其他授权捆绑、停止安装使用等方式，强迫或者变相强迫消费者同意收集、使用与经营活动无直接关系的信息。收集、使用个人生物特征、医疗健康、金融账户、个人行踪等敏感信息的，应当逐项取得消费者同意。

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，除依法配合监管执法活动外，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。

第十四条　网络交易经营者不得违反《中华人民共和国反不正当竞争法》等规定，实施扰乱市场竞争秩序，损害其他经营者或者消费者合法权益的不正当竞争行为。

网络交易经营者不得以下列方式，作虚假或者引人误解的商业宣

传，欺骗、误导消费者：

（一）虚构交易、编造用户评价；

（二）采用误导性展示等方式，将好评前置、差评后置，或者不显著区分不同商品或者服务的评价等；

（三）采用谎称现货、虚构预订、虚假抢购等方式进行虚假营销；

（四）虚构点击量、关注度等流量数据，以及虚构点赞、打赏等交易互动数据。

网络交易经营者不得实施混淆行为，引人误认为是他人商品、服务或者与他人存在特定联系。

网络交易经营者不得编造、传播虚假信息或者误导性信息，损害竞争对手的商业信誉、商品声誉。

第十五条　消费者评价中包含法律、行政法规、规章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。

第十六条　网络交易经营者未经消费者同意或者请求，不得向其发送商业性信息。

网络交易经营者发送商业性信息时，应当明示其真实身份和联系方式，并向消费者提供显著、简便、免费的拒绝继续接收的方式。消费者明确表示拒绝的，应当立即停止发送，不得更换名义后再次发送。

第十七条　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。

第十八条　网络交易经营者采取自动展期、自动续费等方式提供服务的，应当在消费者接受服务前和自动展期、自动续费等日期前五日，以显著方式提请消费者注意，由消费者自主选择；在服务期间内，应当为消费者提供显著、简便的随时取消或者变更的选项，并不得收取不合理费用。

第十九条　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，保障消费者的知情权和选择权。

第二十条　通过网络社交、网络直播等网络服务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及其实际经营主体、售后服务等信息，或者上述信息的链接标识。

网络直播服务提供者对网络交易活动的直播视频保存时间自直播结束之日起不少于三年。

第二十一条　网络交易经营者向消费者提供商品或者服务使用格式条款、通知、声明等的，应当以显著方式提请消费者注意与消费者有重大利害关系的内容，并按照消费者的要求予以说明，不得作出含有下列内容的规定：

（一）免除或者部分免除网络交易经营者对其所提供的商品或者服务应当承担的修理、重作、更换、退货、补足商品数量、退还货款和服务费用、赔偿损失等责任；

（二）排除或者限制消费者提出修理、更换、退货、赔偿损失以及获得违约金和其他合理赔偿的权利；

（三）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；

（四）排除或者限制消费者依法变更或者解除合同的权利；

（五）规定网络交易经营者单方享有解释权或者最终解释权；

（六）其他对消费者不公平、不合理的规定。

第二十二条　网络交易经营者应当按照国家市场监督管理总局及其授权的省级市场监督管理部门的要求，提供特定时段、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。

第二十三条　网络交易经营者自行终止从事网络交易活动的，应当提前三十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、必要、及时的措施保障消费者和相关经营者的合法权益。

第二节　网络交易平台经营者

第二十四条　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，并至少每六个月核验更新一次。

网络交易平台经营者应当对未办理市场主体登记的平台内经营者进行动态监测，对超过本办法第八条第三款规定额度的，及时提醒其依法办理市场主体登记。

第二十五条　网络交易平台经营者应当依照法律、行政法规的规定，向市场监督管理部门报送有关信息。

网络交易平台经营者应当分别于每年1月和7月向住所地省级市场监督管理部门报送平台内经营者的下列身份信息：

（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、实际经营地址、联系方式、网店名称以及网址链接等信息；

（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、网店名称以及网址链接、属于依法不需要办理市场主体登记的具体情形的自我声明等信息；其中，对超过本办法第八条第三款规定额度的平台内经营者进行特别标示。

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。

第二十六条　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，应当在三个工作日内将变更情况报送平台，平台应当在七个工作日内进行核验，完成更新公示。

第二十七条　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。

第二十八条　网络交易平台经营者修改平台服务协议和交易规则的，应当完整保存修改后的版本生效之日前三年的全部历史版本，并保证经营者和消费者能够便利、完整地阅览和下载。

第二十九条　网络交易平台经营者应当对平台内经营者及其发

布的商品或者服务信息建立检查监控制度。网络交易平台经营者发现平台内的商品或者服务信息有违反市场监督管理法律、法规、规章，损害国家利益和社会公共利益，违背公序良俗的，应当依法采取必要的处置措施，保存有关记录，并向平台住所地县级以上市场监督管理部门报告。

第三十条　网络交易平台经营者依据法律、法规、规章的规定或者平台服务协议和交易规则对平台内经营者违法行为采取警示、暂停或者终止服务等处理措施的，应当自决定作出处理措施之日起一个工作日内予以公示，载明平台内经营者的网店名称、违法行为、处理措施等信息。警示、暂停服务等短期处理措施的相关信息应当持续公示至处理措施实施期满之日止。

第三十一条　网络交易平台经营者对平台内经营者身份信息的保存时间自其退出平台之日起不少于三年；对商品或者服务信息，支付记录、物流快递、退换货以及售后等交易信息的保存时间自交易完成之日起不少于三年。法律、行政法规另有规定的，依照其规定。

第三十二条　网络交易平台经营者不得违反《中华人民共和国电子商务法》第三十五条的规定，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，干涉平台内经营者的自主经营。具体包括：

（一）通过搜索降权、下架商品、限制经营、屏蔽店铺、提高服务收费等方式，禁止或者限制平台内经营者自主选择在多个平台开展经营活动，或者利用不正当手段限制其仅在特定平台开展经营活动；

（二）禁止或者限制平台内经营者自主选择快递物流等交易辅助服务提供者；

（三）其他干涉平台内经营者自主经营的行为。

第三章　监督管理

第三十三条　县级以上地方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身份信息与其实际经营地的省级市场监督管理部门共享。

第三十四条　市场监督管理部门在依法开展监督检查、案件调查、事故处置、缺陷消费品召回、消费争议处理等监管执法活动时，可以要求网络交易平台经营者提供有关的平台内经营者身份信息，商品或者服务信息，支付记录、物流快递、退换货以及售后等交易信息。网络交易平台经营者应当提供，并在技术方面积极配合市场监督管理部门开展网络交易违法行为监测工作。

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（以下简称其他服务提供者），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，提供其掌握的有关数据信息。法律、行政法规另有规定的，依照其规定。

市场监督管理部门发现网络交易经营者有违法行为，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。

第三十五条　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，可以依法采取下列措施：

（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、账簿等有关资料；

（三）收集、调取、复制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，应当办理批准手续。

市场监督管理部门对网络交易违法行为的技术监测记录资料，可以作为实施行政处罚或者采取行政措施的电子数据证据。

第三十六条　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。

第三十七条　市场监督管理部门依法对网络交易经营者实施信用监管，将网络交易经营者的注册登记、备案、行政许可、抽查检查结果、行政处罚、列入经营异常名录和严重违法失信企业名单等信息，通过国家企业信用信息公示系统统一归集并公示。对存在严重违法失

信行为的，依法实施联合惩戒。

前款规定的信息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途径公示。

第三十八条　网络交易经营者未依法履行法定责任和义务，扰乱或者可能扰乱网络交易秩序，影响消费者合法权益的，市场监督管理部门可以依职责对其法定代表人或者主要负责人进行约谈，要求其采取措施进行整改。

第四章　法律责任

第三十九条　法律、行政法规对网络交易违法行为的处罚已有规定的，依照其规定。

第四十条　网络交易平台经营者违反本办法第十条，拒不为入驻的平台内经营者出具网络经营场所相关材料的，由市场监督管理部门责令限期改正；逾期不改正的，处一万元以上三万元以下罚款。

第四十一条　网络交易经营者违反本办法第十一条、第十三条、第十六条、第十八条，法律、行政法规有规定的，依照其规定；法律、行政法规没有规定的，由市场监督管理部门依职责责令限期改正，可以处五千元以上三万元以下罚款。

第四十二条　网络交易经营者违反本办法第十二条、第二十三条，未履行法定信息公示义务的，依照《中华人民共和国电子商务法》第七十六条的规定进行处罚。对其中的网络交易平台经营者，依照《中华人民共和国电子商务法》第八十一条第一款的规定进行处罚。

第四十三条　网络交易经营者违反本办法第十四条的，依照《中

华人民共和国反不正当竞争法》的相关规定进行处罚。

第四十四条　网络交易经营者违反本办法第十七条的，依照《中华人民共和国电子商务法》第七十七条的规定进行处罚。

第四十五条　网络交易经营者违反本办法第二十条，法律、行政法规有规定的，依照其规定；法律、行政法规没有规定的，由市场监督管理部门责令限期改正；逾期不改正的，处一万元以下罚款。

第四十六条　网络交易经营者违反本办法第二十二条的，由市场监督管理部门责令限期改正；逾期不改正的，处五千元以上三万元以下罚款。

第四十七条　网络交易平台经营者违反本办法第二十四条第一款、第二十五条第二款、第三十一条，不履行法定核验、登记义务，有关信息报送义务，商品和服务信息、交易信息保存义务的，依照《中华人民共和国电子商务法》第八十条的规定进行处罚。

第四十八条　网络交易平台经营者违反本办法第二十七条、第二十八条、第三十条的，由市场监督管理部门责令限期改正；逾期不改正的，处一万元以上三万元以下罚款。

第四十九条　网络交易平台经营者违反本办法第二十九条，法律、行政法规有规定的，依照其规定；法律、行政法规没有规定的，由市场监督管理部门依职责责令限期改正，可以处一万元以上三万元以下罚款。

第五十条　网络交易平台经营者违反本办法第三十二条的，依照《中华人民共和国电子商务法》第八十二条的规定进行处罚。

第五十一条　网络交易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。

第五十二条　网络交易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，网络交易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。

第五十三条　对市场监督管理部门依法开展的监管执法活动，拒绝依照本办法规定提供有关材料、信息，或者提供虚假材料、信息，或者隐匿、销毁、转移证据，或者有其他拒绝、阻碍监管执法行为，法律、行政法规、其他市场监督管理部门规章有规定的，依照其规定；法律、行政法规、其他市场监督管理部门规章没有规定的，由市场监督管理部门责令改正，可以处五千元以上三万元以下罚款。

第五十四条　市场监督管理部门的工作人员，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。

第五十五条　违反本办法规定，构成犯罪的，依法追究刑事责任。

第五章　附　则

第五十六条　本办法自2021年5月1日起施行。2014年1月26

日原国家工商行政管理总局令第60号公布的《网络交易管理办法》同时废止。

交通运输政务数据共享管理办法

时效性：　　现行有效

发文机关：　交通运输部

文号：　　交科技发〔2021〕33号

发文日期：　2021年04月06日

施行日期：　2021年04月15日

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。

常见类型移动互联网应用程序必要个人信息范围规定

时效性：　　现行有效

发文机关：　国家互联网信息办公室秘书局、工业和信息化部办公厅、公安部办公厅、国家市场监督管理总局

文号：　　国信办秘字〔2021〕14 号

发文日期：　2021 年 03 月 12 日

施行日期：　2021 年 05 月 01 日

第一条　为了规范移动互联网应用程序（App）收集个人信息行为，保障公民个人信息安全，根据《中华人民共和国网络安全法》，制定本规定。

第二条　移动智能终端上运行的 App 存在收集用户个人信息行为的，应当遵守本规定。法律、行政法规、部门规章和规范性文件另有规定的，依照其规定。

App 包括移动智能终端预置、下载安装的应用软件，基于应用软件开放平台接口开发的、用户无需安装即可使用的小程序。

第三条　本规定所称必要个人信息，是指保障 App 基本功能服务正常运行所必需的个人信息，缺少该信息 App 即无法实现基本功能服务。具体是指消费侧用户个人信息，不包括服务供给侧用户个人信息。

第四条　App 不得因为用户不同意提供非必要个人信息，而拒绝用户使用其基本功能服务。

第五条　常见类型 App 的必要个人信息范围：

（一）地图导航类，基本功能服务为“定位和导航”，必要个人信

息为：位置信息、出发地、到达地。

（二）网络约车类，基本功能服务为“网络预约出租汽车服务、巡游出租汽车电召服务”，必要个人信息包括：

1.注册用户移动电话号码；

2.乘车人出发地、到达地、位置信息、行踪轨迹；

3.支付时间、支付金额、支付渠道等支付信息（网络预约出租汽车服务）。

（三）即时通信类，基本功能服务为“提供文字、图片、语音、视频等网络即时通信服务”，必要个人信息包括：

1.注册用户移动电话号码；

2.账号信息：账号、即时通信联系人账号列表。

（四）网络社区类，基本功能服务为“博客、论坛、社区等话题讨论、信息分享和关注互动”，必要个人信息为：注册用户移动电话号码。

（五）网络支付类，基本功能服务为“网络支付、提现、转账等功能”，必要个人信息包括：

1.注册用户移动电话号码；

2.注册用户姓名、证件类型和号码、证件有效期限、银行卡号码。

（六）网上购物类，基本功能服务为“购买商品”，必要个人信息包括：

1.注册用户移动电话号码；

2.收货人姓名（名称）、地址、联系电话；

3.支付时间、支付金额、支付渠道等支付信息。

（七）餐饮外卖类，基本功能服务为“餐饮购买及外送”，必要个人信息包括：

1.注册用户移动电话号码；

2.收货人姓名（名称）、地址、联系电话；

3.支付时间、支付金额、支付渠道等支付信息。

（八）邮件快件寄递类，基本功能服务为“信件、包裹、印刷品等物品寄递服务”，必要个人信息包括：

1.寄件人姓名、证件类型和号码等身份信息；

2.寄件人地址、联系电话；

3.收件人姓名（名称）、地址、联系电话；

4.寄递物品的名称、性质、数量。

（九）交通票务类，基本功能服务为“交通相关的票务服务及行程管理（如票务购买、改签、退票、行程管理等）”，必要个人信息包括：

1.注册用户移动电话号码；

2.旅客姓名、证件类型和号码、旅客类型。旅客类型通常包括儿童、成人、学生等；

3.旅客出发地、目的地、出发时间、车次/船次/航班号、席别/舱位等级、座位号（如有）、车牌号及车牌颜色（ETC 服务);

4.支付时间、支付金额、支付渠道等支付信息。

（十）婚恋相亲类，基本功能服务为“婚恋相亲”，必要个人信息

包括：

1.注册用户移动电话号码；

2.婚恋相亲人的性别、年龄、婚姻状况。

（十一）求职招聘类，基本功能服务为“求职招聘信息交换”，必要个人信息包括：

1.注册用户移动电话号码；

2.求职者提供的简历。

（十二）网络借贷类，基本功能服务为“通过互联网平台实现的用于消费、日常生产经营周转等的个人申贷服务”，必要个人信息包括：

1.注册用户移动电话号码；

2.借款人姓名、证件类型和号码、证件有效期限、银行卡号码。

（十三）房屋租售类，基本功能服务为“个人房源信息发布、房屋出租或买卖”，必要个人信息包括：

1.注册用户移动电话号码；

2.房源基本信息：房屋地址、面积/户型、期望售价或租金。

（十四）二手车交易类，基本功能服务为“二手车买卖信息交换”，必要个人信息包括：

1.注册用户移动电话号码；

2.购买方姓名、证件类型和号码；

3.出售方姓名、证件类型和号码、车辆行驶证号、车辆识别号码。

（十五）问诊挂号类，基本功能服务为“在线咨询问诊、预约挂号”，必要个人信息包括：

1.注册用户移动电话号码；

2.挂号时需提供患者姓名、证件类型和号码、预约挂号的医院和科室；

3.问诊时需提供病情描述。

（十六）旅游服务类，基本功能服务为“旅游服务产品信息的发布与订购”，必要个人信息包括：

1.注册用户移动电话号码；

2.出行人旅游目的地、旅游时间；

3.出行人姓名、证件类型和号码、联系方式。

（十七）酒店服务类，基本功能服务为“酒店预订”，必要个人信息包括：

1.注册用户移动电话号码；

2.住宿人姓名和联系方式、入住和退房时间、入住酒店名称。

（十八）网络游戏类，基本功能服务为“提供网络游戏产品和服务”，必要个人信息为：注册用户移动电话号码。

（十九）学习教育类，基本功能服务为“在线辅导、网络课堂等”，必要个人信息为：注册用户移动电话号码。

（二十）本地生活类，基本功能服务为“家政维修、家居装修、二手闲置物品交易等日常生活服务”，必要个人信息为：注册用户移动电话号码。

（二十一）女性健康类，基本功能服务为“女性经期管理、备孕育儿、美容美体等健康管理服务”，无须个人信息，即可使用基本功能

服务。

（二十二）用车服务类，基本功能服务为“共享单车、共享汽车、租赁汽车等服务”，必要个人信息包括：

1.注册用户移动电话号码；

2.使用共享汽车、租赁汽车服务用户的证件类型和号码，驾驶证件信息；

3.支付时间、支付金额、支付渠道等支付信息；

4.使用共享单车、分时租赁汽车服务用户的位置信息。

（二十三）投资理财类，基本功能服务为“股票、期货、基金、债券等相关投资理财服务”，必要个人信息包括：

1.注册用户移动电话号码；

2.投资理财用户姓名、证件类型和号码、证件有效期限、证件影印件；

3.投资理财用户资金账户、银行卡号码或支付账号。

（二十四）手机银行类，基本功能服务为“通过手机等移动智能终端设备进行银行账户管理、信息查询、转账汇款等服务”，必要个人信息包括：

1.注册用户移动电话号码；

2.用户姓名、证件类型和号码、证件有效期限、证件影印件、银行卡号码、银行预留移动电话号码；

3.转账时需提供收款人姓名、银行卡号码、开户银行信息。

（二十五）邮箱云盘类，基本功能服务为“邮箱、云盘等”，必要

个人信息为：注册用户移动电话号码。

（二十六）远程会议类，基本功能服务为“通过网络提供音频或视频会议”，必要个人信息为：注册用户移动电话号码。

（二十七）网络直播类，基本功能服务为“向公众持续提供实时视频、音频、图文等形式信息浏览服务”，无须个人信息，即可使用基本功能服务。

（二十八）在线影音类，基本功能服务为“影视、音乐搜索和播放”，无须个人信息，即可使用基本功能服务。

（二十九）短视频类，基本功能服务为“不超过一定时长的视频搜索、播放”，无须个人信息，即可使用基本功能服务。

（三十）新闻资讯类，基本功能服务为“新闻资讯的浏览、搜索”，无须个人信息，即可使用基本功能服务。

（三十一）运动健身类，基本功能服务为“运动健身训练”，无须个人信息，即可使用基本功能服务。

（三十二）浏览器类，基本功能服务为“浏览互联网信息资源”，无须个人信息，即可使用基本功能服务。

（三十三）输入法类，基本功能服务为“文字、符号等输入”，无须个人信息，即可使用基本功能服务。

（三十四）安全管理类，基本功能服务为“查杀病毒、清理恶意插件、修复漏洞等”，无须个人信息，即可使用基本功能服务。

（三十五）电子图书类，基本功能服务为“电子图书搜索、阅读”，无须个人信息，即可使用基本功能服务。

（三十六）拍摄美化类，基本功能服务为“拍摄、美颜、滤镜等”，无须个人信息，即可使用基本功能服务。

（三十七）应用商店类，基本功能服务为“App 搜索、下载”，无须个人信息，即可使用基本功能服务。

（三十八）实用工具类，基本功能服务为“日历、天气、词典翻译、计算器、遥控器、手电筒、指南针、时钟闹钟、文件传输、文件管理、壁纸铃声、截图录屏、录音、文档处理、智能家居助手、星座性格测试等”，无须个人信息，即可使用基本功能服务。

（三十九）演出票务类，基本功能服务为“演出购票”，必要个人信息包括：

1.注册用户移动电话号码；

2.观演场次、座位号（如有）；

3.支付时间、支付金额、支付渠道等支付信息。

第六条　任何组织和个人发现违反本规定行为的，可以向相关部门举报。

相关部门收到举报后，应当依法予以处理。

第七条　本规定自 2021 年 5 月 1 日起施行。

互联网用户公众账号信息服务管理规定

时效性：　　现行有效

发文机关：　国家互联网信息办公室

发文日期：　2021 年 01 月 22 日

施行日期：　2021 年 02 月 22 日

第一章　总则

第一条　为了规范互联网用户公众账号信息服务，维护国家安全和公共利益，保护公民、法人和其他组织的合法权益，根据《中华人民共和国网络安全法》《互联网信息服务管理办法》《网络信息内容生态治理规定》等法律法规和国家有关规定，制定本规定。

第二条　在中华人民共和国境内提供、从事互联网用户公众账号信息服务，应当遵守本规定。

第三条　国家网信部门负责全国互联网用户公众账号信息服务的监督管理执法工作。地方网信部门依据职责负责本行政区域内互联网用户公众账号信息服务的监督管理执法工作。

第四条　公众账号信息服务平台和公众账号生产运营者应当遵守法律法规，遵循公序良俗，履行社会责任，坚持正确舆论导向、价值取向，弘扬社会主义核心价值观，生产发布向上向善的优质信息内容，发展积极健康的网络文化，维护清朗网络空间。

鼓励各级党政机关、企事业单位和人民团体注册运营公众账号，生产发布高质量政务信息或者公共服务信息，满足公众信息需求，推动经济社会发展。

鼓励公众账号信息服务平台积极为党政机关、企事业单位和人民团体提升政务信息发布、公共服务和社会治理水平，提供充分必要的技术支持和安全保障。

第五条　公众账号信息服务平台提供互联网用户公众账号信息服务，应当取得国家法律、行政法规规定的相关资质。

公众账号信息服务平台和公众账号生产运营者向社会公众提供互联网新闻信息服务，应当取得互联网新闻信息服务许可。

第二章　公众账号信息服务平台

第六条　公众账号信息服务平台应当履行信息内容和公众账号管理主体责任，配备与业务规模相适应的管理人员和技术能力，设置内容安全负责人岗位，建立健全并严格落实账号注册、信息内容安全、生态治理、应急处置、网络安全、数据安全、个人信息保护、知识产权保护、信用评价等管理制度。

公众账号信息服务平台应当依据法律法规和国家有关规定，制定并公开信息内容生产、公众账号运营等管理规则、平台公约，与公众账号生产运营者签订服务协议，明确双方内容发布权限、账号管理责任等权利义务。

第七条　公众账号信息服务平台应当按照国家有关标准和规范，建立公众账号分类注册和分类生产制度，实施分类管理。

公众账号信息服务平台应当依据公众账号信息内容生产质量、信息传播能力、账号主体信用评价等指标，建立分级管理制度，实施分级管理。

公众账号信息服务平台应当将公众账号和内容生产与账号运营管理规则、平台公约、服务协议等向所在地省、自治区、直辖市网信部门备案；上线具有舆论属性或者社会动员能力的新技术新应用新功能，应当按照有关规定进行安全评估。

第八条　公众账号信息服务平台应当采取复合验证等措施，对申请注册公众账号的互联网用户进行基于移动电话号码、居民身份证号码或者统一社会信用代码等方式的真实身份信息认证，提高认证准确率。用户不提供真实身份信息的，或者冒用组织机构、他人真实身份信息进行虚假注册的，不得为其提供相关服务。

公众账号信息服务平台应当对互联网用户注册的公众账号名称、头像和简介等进行合法合规性核验，发现账号名称、头像和简介与注册主体真实身份信息不相符的，特别是擅自使用或者关联党政机关、企事业单位等组织机构或者社会知名人士名义的，应当暂停提供服务并通知用户限期改正，拒不改正的，应当终止提供服务；发现相关注册信息含有违法和不良信息的，应当依法及时处置。

公众账号信息服务平台应当禁止被依法依约关闭的公众账号以相同账号名称重新注册；对注册与其关联度高的账号名称，还应当对账号主体真实身份信息、服务资质等进行必要核验。

第九条　公众账号信息服务平台对申请注册从事经济、教育、医疗卫生、司法等领域信息内容生产的公众账号，应当要求用户在注册时提供其专业背景，以及依照法律、行政法规获得的职业资格或者服务资质等相关材料，并进行必要核验。

公众账号信息服务平台应当对核验通过后的公众账号加注专门标识，并根据用户的不同主体性质，公示内容生产类别、运营主体名称、注册运营地址、统一社会信用代码、联系方式等注册信息，方便社会监督查询。

公众账号信息服务平台应当建立动态核验巡查制度，适时核验生产运营者注册信息的真实性、有效性。

第十条　公众账号信息服务平台应当对同一主体在本平台注册公众账号的数量合理设定上限。对申请注册多个公众账号的用户，还应当对其主体性质、服务资质、业务范围、信用评价等进行必要核验。

公众账号信息服务平台对互联网用户注册后超过六个月不登录、不使用的公众账号，可以根据服务协议暂停或者终止提供服务。

公众账号信息服务平台应当健全技术手段，防范和处置互联网用户超限量注册、恶意注册、虚假注册等违规注册行为。

第十一条　公众账号信息服务平台应当依法依约禁止公众账号生产运营者违规转让公众账号。

公众账号生产运营者向其他用户转让公众账号使用权的，应当向平台提出申请。平台应当依据前款规定对受让方用户进行认证核验，并公示主体变更信息。平台发现生产运营者未经审核擅自转让公众账号的，应当及时暂停或者终止提供服务。

公众账号生产运营者自行停止账号运营，可以向平台申请暂停或者终止使用。平台应当按照服务协议暂停或者终止提供服务。

第十二条　公众账号信息服务平台应当建立公众账号监测评估

机制，防范账号订阅数、用户关注度、内容点击率、转发评论量等数据造假行为。

公众账号信息服务平台应当规范公众账号推荐订阅关注机制，健全技术手段，及时发现、处置公众账号订阅关注数量的异常变动情况。未经互联网用户知情同意，不得以任何方式强制或者变相强制订阅关注其他用户公众账号。

第十三条　公众账号信息服务平台应当建立生产运营者信用等级管理体系，根据信用等级提供相应服务。

公众账号信息服务平台应当建立健全网络谣言等虚假信息预警、发现、溯源、甄别、辟谣、消除等处置机制，对制作发布虚假信息的公众账号生产运营者降低信用等级或者列入黑名单。

第十四条　公众账号信息服务平台与生产运营者开展内容供给与账号推广合作，应当规范管理电商销售、广告发布、知识付费、用户打赏等经营行为，不得发布虚假广告、进行夸大宣传、实施商业欺诈及商业诋毁等，防止违法违规运营。

公众账号信息服务平台应当加强对原创信息内容的著作权保护，防范盗版侵权行为。

平台不得利用优势地位干扰生产运营者合法合规运营、侵犯用户合法权益。

第三章　公众账号生产运营者

第十五条　公众账号生产运营者应当按照平台分类管理规则，在注册公众账号时如实填写用户主体性质、注册地、运营地、内容生产

类别、联系方式等基本信息，组织机构用户还应当注明主要经营或者业务范围。

公众账号生产运营者应当遵守平台内容生产和账号运营管理规则、平台公约和服务协议，按照公众账号登记的内容生产类别，从事相关行业领域的信息内容生产发布。

第十六条　公众账号生产运营者应当履行信息内容生产和公众账号运营管理主体责任，依法依规从事信息内容生产和公众账号运营活动。

公众账号生产运营者应当建立健全选题策划、编辑制作、发布推广、互动评论等全过程信息内容安全审核机制，加强信息内容导向性、真实性、合法性审核，维护网络传播良好秩序。

公众账号生产运营者应当建立健全公众账号注册使用、运营推广等全过程安全管理机制，依法、文明、规范运营公众账号，以优质信息内容吸引公众关注订阅和互动分享，维护公众账号良好社会形象。

公众账号生产运营者与第三方机构开展公众账号运营、内容供给等合作，应与第三方机构签订书面协议，明确第三方机构信息安全管理义务并督促履行。

第十七条　公众账号生产运营者转载信息内容的，应当遵守著作权保护相关法律法规，依法标注著作权人和可追溯信息来源，尊重和保护著作权人的合法权益。

公众账号生产运营者应当对公众账号留言、跟帖、评论等互动环节进行管理。平台可以根据公众账号的主体性质、信用等级等，合理

设置管理权限，提供相关技术支持。

第十八条　公众账号生产运营者不得有下列违法违规行为：

（一）不以真实身份信息注册，或者注册与自身真实身份信息不相符的公众账号名称、头像、简介等；

（二）恶意假冒、仿冒或者盗用组织机构及他人公众账号生产发布信息内容；

（三）未经许可或者超越许可范围提供互联网新闻信息采编发布等服务；

（四）操纵利用多个平台账号，批量发布雷同低质信息内容，生成虚假流量数据，制造虚假舆论热点；

（五）利用突发事件煽动极端情绪，或者实施网络暴力损害他人和组织机构名誉，干扰组织机构正常运营，影响社会和谐稳定；

（六）编造虚假信息，伪造原创属性，标注不实信息来源，歪曲事实真相，误导社会公众；

（七）以有偿发布、删除信息等手段，实施非法网络监督、营销诈骗、敲诈勒索，谋取非法利益；

（八）违规批量注册、囤积或者非法交易买卖公众账号；

（九）制作、复制、发布违法信息，或者未采取措施防范和抵制制作、复制、发布不良信息；

（十）法律、行政法规禁止的其他行为。

第四章　监督管理

第十九条　公众账号信息服务平台应当加强对本平台公众账号

信息服务活动的监督管理，及时发现和处置违法违规信息或者行为。

公众账号信息服务平台应当对违反本规定及相关法律法规的公众账号，依法依约采取警示提醒、限制账号功能、暂停信息更新、停止广告发布、关闭注销账号、列入黑名单、禁止重新注册等处置措施，保存有关记录，并及时向网信等有关主管部门报告。

第二十条　公众账号信息服务平台和生产运营者应当自觉接受社会监督。

公众账号信息服务平台应当在显著位置设置便捷的投诉举报入口和申诉渠道，公布投诉举报和申诉方式，健全受理、甄别、处置、反馈等机制，明确处理流程和反馈时限，及时处理公众投诉举报和生产运营者申诉。

鼓励互联网行业组织开展公众评议，推动公众账号信息服务平台和生产运营者严格自律，建立多方参与的权威调解机制，公平合理解决行业纠纷，依法维护用户合法权益。

第二十一条　各级网信部门会同有关主管部门建立健全协作监管等工作机制，监督指导公众账号信息服务平台和生产运营者依法依规从事相关信息服务活动。

公众账号信息服务平台和生产运营者应当配合有关主管部门依法实施监督检查，并提供必要的技术支持和协助。

公众账号信息服务平台和生产运营者违反本规定的，由网信部门和有关主管部门在职责范围内依照相关法律法规处理。

第五章　附则

第二十二条　本规定所称互联网用户公众账号，是指互联网用户在互联网站、应用程序等网络平台注册运营，面向社会公众生产发布文字、图片、音视频等信息内容的网络账号。

本规定所称公众账号信息服务平台，是指为互联网用户提供公众账号注册运营、信息内容发布与技术保障服务的网络信息服务提供者。

本规定所称公众账号生产运营者，是指注册运营公众账号从事内容生产发布的自然人、法人或者非法人组织。

第二十三条　本规定自2021年2月22日起施行。本规定施行之前颁布的有关规定与本规定不一致的，按照本规定执行。

涉密信息系统集成资质管理办法

时效性：　　现行有效

发文机关：　国家保密局

文号：　　国家保密局令2020年第1号

发文日期：　2020年12月10日

施行日期：　2021年03月01日

第一章　总　则

第一条　为了加强涉密信息系统集成资质管理，确保国家秘密安全，根据《中华人民共和国保守国家秘密法》、《中华人民共和国行政许可法》、《中华人民共和国行政处罚法》、《中华人民共和国保守国家秘密法实施条例》等有关法律法规，制定本办法。

第二条　本办法所称涉密信息系统集成（以下简称涉密集成），是指涉密信息系统的规划、设计、建设、监理和运行维护等活动。

涉密集成资质是指保密行政管理部门许可企业事业单位从事涉密信息系统集成业务的法定资格。

第三条　涉密集成资质的申请、受理、审查、决定、使用和监督管理，适用本办法。

第四条　从事涉密集成业务的企业事业单位应当依照本办法，取得涉密集成资质。

国家机关和涉及国家秘密的单位（以下简称机关、单位）应当选择具有涉密集成资质的单位（以下简称资质单位）承接涉密集成业务。

第五条　涉密集成资质管理应当遵循依法管理、安全保密、科学

发展、公平公正的原则。

第六条　国家保密行政管理部门主管全国涉密集成资质管理工作，省级保密行政管理部门主管本行政区域内涉密集成资质管理工作。

省级以上保密行政管理部门根据工作需要，可以委托下一级保密行政管理部门开展审查工作，或者组织机构协助开展工作。

第七条　省级以上保密行政管理部门应当指定专门机构承担保密资质管理日常工作。

第八条　省级以上保密行政管理部门建立保密资质审查专家库，组织开展入库审查、培训考核等工作。

第九条　实施涉密集成资质许可不收取任何费用，所需经费纳入同级财政预算。

第二章　等级与条件

第十条　涉密集成资质分为甲级和乙级两个等级。

甲级资质单位可以从事绝密级、机密级和秘密级涉密集成业务；乙级资质单位可以从事机密级、秘密级涉密集成业务。

第十一条　涉密集成资质包括总体集成、系统咨询、软件开发、安防监控、屏蔽室建设、运行维护、数据恢复、工程监理，以及国家保密行政管理部门许可的其他涉密集成业务。取得总体集成业务种类许可的，除从事系统集成业务外，还可从事软件开发、安防监控和所承建系统的运行维护业务。

资质单位应当在保密行政管理部门许可的业务种类范围内承接涉密集成业务。承接涉密系统咨询、工程监理业务的，不得承接所咨

询、监理业务的其他涉密集成业务。

第十二条　申请单位应当具备以下基本条件：

（一）在中华人民共和国境内依法成立三年以上的法人；

（二）无犯罪记录且近三年内未被吊销保密资质（资格），法定代表人、主要负责人、实际控制人未被列入失信人员名单；

（三）法定代表人、主要负责人、实际控制人、董（监）事会人员、高级管理人员以及从事涉密集成业务人员具有中华人民共和国国籍，无境外永久居留权或者长期居留许可，与境外人员无婚姻关系，国家另有规定的除外；

（四）具有从事涉密集成业务的专业能力；

（五）法律、行政法规和国家保密行政管理部门规定的其他条件。

第十三条　申请单位应当具备以下保密条件：

（一）有专门机构或者人员负责保密工作；

（二）保密制度完善；

（三）从事涉密集成业务的人员经过保密教育培训，具备必要的保密知识和技能；

（四）用于涉密集成业务的场所、设施、设备符合国家保密规定和标准；

（五）有专门的保密工作经费；

（六）法律、行政法规和国家保密行政管理部门规定的其他保密条件。

第十四条　申请单位应当无外国投资者直接投资，且通过间接方

式投资的外国投资者在申请单位中的出资比例最终不得超过20%；申请单位及其股东的实际控制人不得为外国投资者，外国投资者在申请单位母公司中的出资比例最终不得超过20%。

在新三板挂牌的企业申请资质以及资质有效期内的，还应当符合以下条件：

（一）参与挂牌交易的股份比例不高于总股本的30%；

（二）实际控制人在申请期间及资质有效期内保持控制地位不变。

第十五条　申请单位应当建立完善的内部管理和信息披露制度，未经国务院有关主管部门或者省级人民政府有关主管部门批准，外国投资者不得接触、知悉国家秘密信息。

第十六条　申请单位申请不同等级和业务种类的涉密集成资质，应当符合涉密集成资质具体条件的要求。

第三章　申请、受理、审查与决定

第十七条　申请甲级资质的，应当向国家保密行政管理部门提出申请；申请乙级资质的，应当向注册地的省级保密行政管理部门提出申请。申请单位应当提交以下材料：

（一）《涉密信息系统集成资质申请书》（以下简称申请书）；

（二）企业营业执照或者事业单位法人证书；

（三）在登记机关备案的章程；

（四）法定代表人、主要负责人、实际控制人、董（监）事会人员、高级管理人员以及从事涉密集成业务的其他人员情况；

（五）资本结构和股权情况；

（六）生产经营和办公场所产权证书或者租赁合同；

（七）近三年集成业务合同清单；

（八）涉密集成业务场所和保密设施、设备情况；

（九）基本管理制度、保密制度以及保密体系运行情况。

申请书及相关材料不得涉及国家秘密，申请单位应当对申请材料的真实性和完整性负责。

第十八条　保密行政管理部门收到申请材料后，应当在五日内完成审查。申请材料齐全且符合法定形式的，应当受理并发出受理通知书；申请材料不齐全或者不符合法定形式的，应当一次告知申请单位十五日内补正材料；逾期未告知申请单位补正的，自收到申请材料之日起即为受理。申请单位十五日内不予补正的，视为放弃本次行政许可申请。

第十九条　资质审查分为书面审查、现场审查。确有需要的，可以组织专家开展评审。

第二十条　对作出受理决定的，保密行政管理部门应当对提交的申请材料进行书面审查。

第二十一条　对书面审查合格的单位，保密行政管理部门应当指派两名以上工作人员，并可以结合工作实际指派一名以上审查专家，依据涉密集成资质审查细则和评分标准，对保密制度、保密工作机构、保密监督管理、涉密人员管理、保密技术防护以及从事涉密集成业务的专业能力等情况进行现场审查。

涉密集成资质审查细则和评分标准由国家保密行政管理部门另行规定。

第二十二条　现场审查应当按照以下程序进行：

（一）提前五日以传真、电子邮件等形式书面通知申请单位现场审查时间；

（二）听取申请单位情况汇报和对有关事项的说明；

（三）审查有关材料；

（四）与主要负责人、保密工作负责人及有关人员谈话了解情况；

（五）组织涉密人员进行保密知识测试；

（六）对涉密场所、涉密设备等进行实地查看；

（七）汇总现场审查情况，形成现场审查报告；

（八）通报审查情况，申请单位法定代表人或者主要负责人在现场审查报告上签字确认。

第二十三条　申请单位具有下列情形之一的，保密行政管理部门应当终止审查：

（一）隐瞒有关情况或者提供虚假材料的；

（二）采取贿赂、请托等不正当手段，影响审查工作公平公正进行的；

（三）无正当理由拒绝按通知时间接受现场审查的；

（四）现场审查中发现不符合评分标准基本项的；

（五）其他违反保密法律法规的行为。

第二十四条　申请单位书面审查、现场审查合格的，保密行政管

理部门应当准予行政许可。

申请单位具有下列情形之一的，保密行政管理部门应当作出不予行政许可的书面决定，说明理由并告知申请单位相关权利：

（一）书面审查不合格的；

（二）现场审查不合格的；

（三）终止审查的；

（四）法律、行政法规规定的不予行政许可的其他情形。

第二十五条　保密行政管理部门应当自受理申请之日起二十日内，对申请单位作出准予行政许可或者不予行政许可的决定。二十日内不能作出决定的，经本行政机关负责人批准，可以延长十日，并应当将延长期限的理由告知申请单位。

保密行政管理部门组织开展专家评审、鉴定所需时间不计入行政许可期限。

第二十六条　保密行政管理部门作出准予行政许可的决定的，自作出决定之日起十日内向申请单位颁发《涉密信息系统集成资质证书》（以下简称《资质证书》）。

第二十七条　《资质证书》有效期为五年，分为正本和副本，正本和副本具有同等法律效力。样式由国家保密行政管理部门统一制作，主要包括以下内容：

（一）单位名称；

（二）法定代表人；

（三）注册地址；

（四）证书编号；

（五）资质等级；

（六）业务种类；

（七）发证机关；

（八）有效期和发证日期。

第二十八条　《资质证书》有效期满，需要继续从事涉密集成业务的，应当在有效期届满三个月前向保密行政管理部门提出延续申请，保密行政管理部门应当按照本办法有关规定开展审查，申请单位未按规定期限提出延续申请的，视为重新申请。

有效期届满且未准予延续前，不得签订新的涉密集成业务合同。对于已经签订合同但未完成的涉密业务，在确保安全保密的条件下可以继续完成。

第二十九条　省级保密行政管理部门应当将许可的乙级资质单位报国家保密行政管理部门备案。

准予行政许可和注销、吊销、撤销以及暂停资质的决定，由作出决定的保密行政管理部门在一定范围内予以发布。

第四章　监督与管理

第三十条　省级以上保密行政管理部门应当加强对下一级保密行政管理部门以及协助开展审查工作的专门机构的监督检查，及时纠正资质管理中的违法违规行为。

第三十一条　保密行政管理部门应当开展“双随机”抽查、飞行检查等形式的保密检查，对资质单位从事涉密集成业务和保密管理情况

进行监督。

第三十二条　机关、单位委托资质单位从事涉密集成业务，应当查验其《资质证书》，签订保密协议，提出保密要求，采取保密措施，加强涉密业务实施现场的监督检查。

第三十三条　资质单位与其他单位合作开展涉密集成业务的，合作单位应当具有相应的涉密集成资质且取得委托方书面同意。

资质单位不得将涉密集成业务分包或者转包给无相应涉密资质的单位。

第三十四条　资质单位承接涉密集成业务的，应当在签订合同后三十日内，向业务所在地省级保密行政管理部门备案，接受保密监督管理。

第三十五条　乙级资质单位拟在注册地的省级行政区域外承接涉密集成业务的，应当向业务所在地的省级保密行政管理部门备案，接受保密监督管理。

第三十六条　资质单位实行年度自检制度，应当于每年3月31日前向作出准予行政许可决定的保密行政管理部门报送上一年度自检报告。

第三十七条　资质单位下列事项发生变更的，应当在变更前向保密行政管理部门书面报告：

（一）注册资本或者股权结构；

（二）控股股东或者实际控制人；

（三）单位性质或者隶属关系；

（四）用于涉密集成业务的场所。

保密行政管理部门应当对资质单位变更事项进行书面审查。通过审查的，资质单位应当按照审定事项实施变更，并在变更完成后十日内提交情况报告。

拟公开上市的，应当资质剥离后重新申请；对影响或者可能影响国家安全的外商投资，应当按照外商投资安全审查制度进行安全审查。

资质单位发生控股股东或者实际控制人、单位性质或者隶属关系、用于涉密集成业务的场所等事项变更的，保密行政管理部门应当组织现场审查。

第三十八条　资质单位下列事项发生变更的，应当在变更后十日内向保密行政管理部门书面报告：

（一）单位名称；

（二）注册地址或者经营地址；

（三）经营范围；

（四）法定代表人、董（监）事会人员或者高级管理人员。

资质单位变更完成需换发《资质证书》的，由保密行政管理部门审核后重新颁发。

第三十九条　保密行政管理部门在现场审查、保密检查过程中，发现申请单位或者资质单位存在涉嫌泄露国家秘密的案件线索，应当根据工作需要，按照泄密案件管辖权限，经保密行政管理部门负责人批准，由具备执法资格的人员对有关设施、设备、载体等采取登记保存措施，依法开展调查工作。

保密行政管理部门调查结束后，认定申请单位或者资质单位存在违反保密法律法规事实的，违法行为发生地的保密行政管理部门应当按照本办法作出处理，并将违法事实、处理结果抄告受理申请或者准予行政许可的保密行政管理部门。

第四十条　有下列情形之一的，作出准予行政许可决定的保密行政管理部门或者其上级保密行政管理部门，依据职权可以撤销行政许可：

（一）保密行政管理部门滥用职权、玩忽职守作出准予行政许可决定的；

（二）超越法定职权作出准予行政许可决定的；

（三）违反法定程序作出准予行政许可决定的；

（四）对不具备申请资格或者不符合法定条件的申请单位准予行政许可的；

（五）依法可以撤销行政许可的其他情形。

资质单位采取欺骗、贿赂等不正当手段取得资质的，保密行政管理部门应当撤销其资质，停止其涉密业务。自撤销之日起，三年内不得再次申请。

第四十一条　资质单位具有下列情形之一的，作出准予行政许可决定的保密行政管理部门应当注销其资质：

（一）《资质证书》有效期届满未延续的；

（二）法人资格依法终止的；

（三）主动申请注销资质的；

（四）行政许可依法被撤销、撤回，或者行政许可证件依法被吊销的；

（五）因不可抗力导致行政许可事项无法实施的；

（六）法律、行政法规规定的应当注销资质的其他情形。

第四十二条　申请单位或者资质单位对保密行政管理部门作出的决定不服的，可以依法申请行政复议或者提起行政诉讼。

第五章　法律责任

第四十三条　资质单位违反本办法的，依照本办法有关规定处理；构成犯罪的，依法追究刑事责任。

第四十四条　资质单位具有下列情形之一的，保密行政管理部门应当责令其在二十日内完成整改，逾期不改或者整改后仍不符合要求的，应当给予六个月以上十二个月以下暂停资质的处罚：

（一）未经委托方书面同意，擅自与其他涉密集成资质单位合作开展涉密集成业务的；

（二）超出行政许可的业务种类范围承接涉密集成业务的；

（三）发生需要报告的事项，未及时报告的；

（四）承接涉密集成业务，未按规定备案的；

（五）未按本办法提交年度自检报告的；

（六）不符合其他保密管理规定，存在泄密隐患的。

第四十五条　资质单位不再符合申请条件，或者具有下列情形之一的，保密行政管理部门应当吊销其资质，停止其涉密业务：

（一）涂改、出卖、出租、出借《资质证书》，或者以其他方式

伪造、非法转让《资质证书》的；

（二）将涉密集成业务分包或者转包给无相应涉密资质单位的；

（三）发现国家秘密已经泄露或者可能泄露，未按法定时限报告的；

（四）拒绝接受保密检查的；

（五）资质暂停期间，承接新的涉密集成业务的；

（六）资质暂停期满，仍不符合保密管理规定的；

（七）发生泄密案件的；

（八）其他违反保密法律法规的行为。

第四十六条　申请单位隐瞒有关情况或者提供虚假材料的，保密行政管理部门应当作出不予受理或者不予行政许可的决定。自不予受理或者不予行政许可之日起，一年内不得再次申请。

第四十七条　未经保密行政管理部门许可的单位从事涉密集成业务的，由保密行政管理部门责令停止违法行为，非法获取、持有的国家秘密载体，应当予以收缴；有违法所得的，由市场监督管理部门没收违法所得；构成犯罪的，依法追究刑事责任。

第四十八条　机关、单位委托未经保密行政管理部门许可的单位从事涉密集成业务的，应当由有关机关、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；构成犯罪的，依法追究刑事责任。

第四十九条　保密行政管理部门及其工作人员未依法履行职责，或者滥用职权、玩忽职守、徇私舞弊的，对直接负责的主管人员和其他直接责任人员依法给予政务处分；构成犯罪的，依法追究刑事责任。

第六章　附　则

第五十条　机关、单位自行开展涉密信息系统集成业务，可以由本机关、单位内部信息化工作机构承担，接受同级保密行政管理部门监督指导。

第五十一条　申请单位资本结构包含香港特别行政区、澳门特别行政区、台湾地区投资者以及定居在国外中国公民投资者的，参照本办法管理。国家另有规定的，从其规定。

第五十二条　本办法规定的实施行政许可的期限以工作日计算，不含法定节假日。

第五十三条　本办法由国家保密局负责解释。

第五十四条　本办法自2021年3月1日起施行。国家保密局发布的《涉密信息系统集成资质管理办法》（国保发〔2013〕7号，国保发〔2019〕13号修订）同时废止。

中国银保监会监管数据安全管理办法（试行）

时效性：　　现行有效

发文机关：　中国银行保险监督管理委员会

发文日期：　2020 年 09 月 23 日

施行日期：　2020 年 09 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建设的，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，必须遵守相关法律和行政法规。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。

第七条　监管数据安全管理实行归口管理，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和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技术防护措施。

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）网络和信息系统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管理措施，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管理评估检查工作。

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责任，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。

中国人民银行金融消费者权益保护实施办法

时效性：　　现行有效

文号：　　中国人民银行令〔2020〕第 5 号

发文机关：　中国人民银行

发文日期：　2020 年 09 月 18 日

施行日期：　2020 年 09 月 18 日

第一章　总　则

第一条 为了保护金融消费者合法权益，规范金融机构提供金融产品和服务的行为，维护公平、公正的市场环境，促进金融市场健康稳定运行，根据《中华人民共和国中国人民银行法》《中华人民共和国商业银行法》《中华人民共和国消费者权益保护法》和《国务院办公厅关于加强金融消费者权益保护工作的指导意见》（国办发〔2015〕81 号）等，制定本办法。

第二条 在中华人民共和国境内依法设立的为金融消费者提供金融产品或者服务的银行业金融机构（以下简称银行），开展与下列业务相关的金融消费者权益保护工作，适用本办法：

（一）与利率管理相关的。

（二）与人民币管理相关的。

（三）与外汇管理相关的。

（四）与黄金市场管理相关的。

（五）与国库管理相关的。

（六）与支付、清算管理相关的。

（七）与反洗钱管理相关的。

（八）与征信管理相关的。

（九）与上述第一项至第八项业务相关的金融营销宣传和消费者金融信息保护。

（十）其他法律、行政法规规定的中国人民银行职责范围内的金融消费者权益保护工作。

在中华人民共和国境内依法设立的非银行支付机构（以下简称支付机构）提供支付服务的，适用本办法。

本办法所称金融消费者是指购买、使用银行、支付机构提供的金融产品或者服务的自然人。

第三条 银行、支付机构向金融消费者提供金融产品或者服务，应当遵循自愿、平等、公平、诚实信用的原则，切实承担金融消费者合法权益保护的主体责任，履行金融消费者权益保护的法定义务。

第四条 金融消费者应当文明、理性进行金融消费，提高自我保护意识，诚实守信，依法维护自身的合法权益。

第五条 中国人民银行及其分支机构坚持公平、公正原则，依法开展职责范围内的金融消费者权益保护工作，依法保护金融消费者合法权益。

中国人民银行及其分支机构会同有关部门推动建立和完善金融机构自治、行业自律、金融监管和社会监督相结合的金融消费者权益保护共同治理体系。

第六条 鼓励金融消费者和银行、支付机构充分运用调解、仲裁等

方式解决金融消费纠纷。

第二章　金融机构行为规范

第七条 银行、支付机构应当将金融消费者权益保护纳入公司治理、企业文化建设和经营发展战略，制定本机构金融消费者权益保护工作的总体规划和具体工作措施。建立金融消费者权益保护专职部门或者指定牵头部门，明确部门及人员职责，确保部门有足够的人力、物力能够独立开展工作，并定期向高级管理层、董（理）事会汇报工作开展情况。

第八条 银行、支付机构应当落实法律法规和相关监管规定关于金融消费者权益保护的相关要求，建立健全金融消费者权益保护的各项内控制度。

（一）金融消费者权益保护工作考核评价制度。

（二）金融消费者风险等级评估制度。

（三）消费者金融信息保护制度。

（四）金融产品和服务信息披露、查询制度。

（五）金融营销宣传管理制度。

（六）金融知识普及和金融消费者教育制度。

（七）金融消费者投诉处理制度。

（八）金融消费者权益保护工作内部监督和责任追究制度。

（九）金融消费者权益保护重大事件应急制度。

（十）中国人民银行明确规定应当建立的其他金融消费者权益保护工作制度。

第九条 银行、支付机构应当建立健全涉及金融消费者权益保护工作的全流程管控机制，确保在金融产品或者服务的设计开发、营销推介及售后管理等各个业务环节有效落实金融消费者权益保护工作的相关规定和要求。全流程管控机制包括但不限于下列内容：

（一）事前审查机制。银行、支付机构应当实行金融消费者权益保护事前审查，及时发现并更正金融产品或者服务中可能损害金融消费者合法权益的问题，有效督办落实金融消费者权益保护审查意。

（二）事中管控机制。银行、支付机构应当履行金融产品或者服务营销宣传中须遵循的基本程序和标准，加强对营销宣传行为的监测与管控。

（三）事后监督机制。银行、支付机构应当做好金融产品和服务的售后管理，及时调整存在问题或者隐患的金融产品和服务规则。

第十条 银行、支付机构应当开展金融消费者权益保护工作人员培训，增强工作人员的金融消费者权益保护意识和能力。

银行、支付机构应当每年至少开展一次金融消费者权益保护专题培训，培训对象应当全面覆盖中高级管理人员、基层业务人员及新入职人员。对金融消费者投诉多发、风险较高的业务岗位，应当适当提高培训的频次。

第十一条 银行、支付机构开展考核评价时，应当将金融消费者权益保护工作作为重要内容，并合理分配相关指标的占比和权重，综合考虑业务合规性、客户满意度、投诉处理及时率与合格率等，不得简单以投诉数量作为考核指标。

第十二条 银行、支付机构应当根据金融产品或者服务的特性评估其对金融消费者的适合度，合理划分金融产品和服务风险等级以及金融消费者风险承受等级，将合适的金融产品或者服务提供给适当的金融消费者。

第十三条 银行、支付机构应当依法保障金融消费者在购买、使用金融产品和服务时的财产安全，不得挪用、非法占用金融消费者资金及其他金融资产。

第十四条 银行、支付机构应当尊重社会公德，尊重金融消费者的人格尊严和民族风俗习惯，不得因金融消费者性别、年龄、种族、民族或者国籍等不同实行歧视性差别对待，不得使用歧视性或者违背公序良俗的表述。

第十五条 银行、支付机构应当尊重金融消费者购买金融产品或者服务的真实意愿，不得擅自代理金融消费者办理业务，不得擅自修改金融消费者的业务指令，不得强制搭售其他产品或者服务。

第十六条 银行、支付机构应当依据金融产品或者服务的特性，及时、真实、准确、全面地向金融消费者披露下列重要内容：

（一）金融消费者对该金融产品或者服务的权利和义务，订立、变更、中止和解除合同的方式及限制。

（二）银行、支付机构对该金融产品或者服务的权利、义务及法律责任。

（三）贷款产品的年化利率。

（四）金融消费者应当负担的费用及违约金，包括金额的确定方

式，交易时间和交易方式。

（五）因金融产品或者服务产生纠纷的处理及投诉途径。

（六）银行、支付机构对该金融产品或者服务所执行的强制性标准、推荐性标准、团体标准或者企业标准的编号和名称。

（七）在金融产品说明书或者服务协议中，实际承担合同义务的经营主体完整的中文名称。

（八）其他可能影响金融消费者决策的信息。

第十七条 银行、支付机构对金融产品和服务进行信息披露时，应当使用有利于金融消费者接收、理解的方式。对利率、费用、收益及风险等与金融消费者切身利益相关的重要信息，应当根据金融产品或者服务的复杂程度及风险等级，对其中关键的专业术语进行解释说明，并以适当方式供金融消费者确认其已接收完整信息。

第十八条 银行、支付机构向金融消费者说明重要内容和披露风险时，应当依照法律法规和监管规定留存相关资料，自业务关系终止之日起留存时间不得少于3年。法律、行政法规另有规定的，从其规定。

留存的资料包括但不限于：

（一）金融消费者确认的金融产品说明书或者服务协议。

（二）金融消费者确认的风险提示书。

（三）记录向金融消费者说明重要内容的录音、录像资料或者系统日志等相关数据电文资料。

第十九条 银行、支付机构不得利用技术手段、优势地位，强制或者变相强制金融消费者接受金融产品或者服务，或者排除、限制金融

消费者接受同业机构提供的金融产品或者服务。

第二十条 银行、支付机构在提供金融产品或者服务的过程中，不得通过附加限制性条件的方式要求金融消费者购买、使用协议中未作明确要求的产品或者服务。

第二十一条 银行、支付机构向金融消费者提供金融产品或者服务时使用格式条款的，应当以足以引起金融消费者注意的字体、字号、颜色、符号、标识等显著方式，提请金融消费者注意金融产品或者服务的数量、利率、费用、履行期限和方式、注意事项、风险提示、纠纷解决等与金融消费者有重大利害关系的内容，并按照金融消费者的要求予以说明。格式条款采用电子形式的，应当可被识别且易于获取。

银行、支付机构不得以通知、声明、告示等格式条款的方式作出含有下列内容的规定：

（一）减轻或者免除银行、支付机构造成金融消费者财产损失的赔偿责任。

（二）规定金融消费者承担超过法定限额的违约金或者损害赔偿金。

（三）排除或者限制金融消费者依法对其金融信息进行查询、删除、修改的权利；

（四）排除或者限制金融消费者选择同业机构提供的金融产品或者服务的权利。

（五）其他对金融消费者不公平、不合理的规定。

银行、支付机构应当对存在侵害金融消费者合法权益问题或者隐

患的格式条款和服务协议文本及时进行修订或者清理。

第二十二条 银行、支付机构应当对营销宣传内容的真实性负责。银行、支付机构实际承担的义务不得低于在营销宣传活动中通过广告、资料或者说明等形式对金融消费者所承诺的标准。

前款“广告、资料或者说明”是指以营销为目的，利用各种传播媒体、宣传工具或者方式，就银行、支付机构的金融产品或者服务进行直接或者间接的宣传、推广等。

第二十三条 银行、支付机构在进行营销宣传活动时，不得有下列行为：

（一）虚假、欺诈、隐瞒或者引人误解的宣传。

（二）引用不真实、不准确的数据和资料或者隐瞒限制条件等，对过往业绩或者产品收益进行夸大表述。

（三）利用金融管理部门对金融产品或者服务的审核或者备案程序，误导金融消费者认为金融管理部门已对该金融产品或者服务提供保证。

（四）明示或者暗示保本、无风险或者保收益等，对非保本投资型金融产品的未来效果、收益或者相关情况作出保证性承诺。

（五）其他违反金融消费者权益保护相关法律法规和监管规定的行为。

第二十四条 银行、支付机构应当切实承担金融知识普及和金融消费者教育的主体责任，提高金融消费者对金融产品和服务的认知能力，提升金融消费者金融素养和诚实守信意识。

银行、支付机构应当制定年度金融知识普及与金融消费者教育工作计划，结合自身特点开展日常性金融知识普及与金融消费者教育活动，积极参与中国人民银行及其分支机构组织的金融知识普及活动。银行、支付机构不得以营销金融产品或者服务替代金融知识普及与金融消费者教育。

第二十五条 银行、支付机构应当重视金融消费者需求的多元性与差异性，积极支持普惠金融重点目标群体获得必要、及时的基本金融产品和服务。

第二十六条 出现侵害金融消费者合法权益重大事件的，银行、支付机构应当根据重大事项报告的相关规定及时向中国人民银行或其分支机构报告。

第二十七条 银行、支付机构应当配合中国人民银行及其分支机构开展金融消费者权益保护领域的相关工作，按照规定报送相关资料。

第三章 消费者金融信息保护

第二十八条 本办法所称消费者金融信息，是指银行、支付机构通过开展业务或者其他合法渠道处理的消费者信息，包括个人身份信息、财产信息、账户信息、信用信息、金融交易信息及其他与特定消费者购买、使用金融产品或者服务相关的信息。

消费者金融信息的处理包括消费者金融信息的收集、存储、使用、加工、传输、提供、公开等。

第二十九条 银行、支付机构处理消费者金融信息，应当遵循合法、正当、必要原则，经金融消费者或者其监护人明示同意，但是法律、

行政法规另有规定的除外。银行、支付机构不得收集与业务无关的消费者金融信息，不得采取不正当方式收集消费者金融信息，不得变相强制收集消费者金融信息。银行、支付机构不得以金融消费者不同意处理其金融信息为由拒绝提供金融产品或者服务，但处理其金融信息属于提供金融产品或者服务所必需的除外。

金融消费者不能或者拒绝提供必要信息，致使银行、支付机构无法履行反洗钱义务的，银行、支付机构可以根据《中华人民共和国反洗钱法》的相关规定对其金融活动采取限制性措施；确有必要时，银行、支付机构可以依法拒绝提供金融产品或者服务。

第三十条 银行、支付机构收集消费者金融信息用于营销、用户体验改进或者市场调查的，应当以适当方式供金融消费者自主选择是否同意银行、支付机构将其金融信息用于上述目的；金融消费者不同意的，银行、支付机构不得因此拒绝提供金融产品或者服务。银行、支付机构向金融消费者发送金融营销信息的，应当向其提供拒绝继续接收金融营销信息的方式。

第三十一条 银行、支付机构应当履行《中华人民共和国消费者权益保护法》第二十九条规定的明示义务，公开收集、使用消费者金融信息的规则，明示收集、使用消费者金融信息的目的、方式和范围，并留存有关证明资料。

银行、支付机构通过格式条款取得消费者金融信息收集、使用同意的，应当在格式条款中明确收集消费者金融信息的目的、方式、内容和使用范围，并在协议中以显著方式尽可能通俗易懂地向金融消费

者提示该同意的可能后果。

第三十二条 银行、支付机构应当按照法律法规的规定和双方约定的用途使用消费者金融信息，不得超出范围使用。

第三十三条 银行、支付机构应当建立以分级授权为核心的消费者金融信息使用管理制度，根据消费者金融信息的重要性、敏感度及业务开展需要，在不影响本机构履行反洗钱等法定义务的前提下，合理确定本机构工作人员调取信息的范围、权限，严格落实信息使用授权审批程序。

第三十四条 银行、支付机构应当按照国家档案管理和电子数据管理等规定，采取技术措施和其他必要措施，妥善保管和存储所收集的消费者金融信息，防止信息遗失、毁损、泄露或者被篡改。

银行、支付机构及其工作人员应当对消费者金融信息严格保密，不得泄露或者非法向他人提供。在确认信息发生泄露、毁损、丢失时，银行、支付机构应当立即采取补救措施；信息泄露、毁损、丢失可能危及金融消费者人身、财产安全的，应当立即向银行、支付机构住所地的中国人民银行分支机构报告并告知金融消费者；信息泄露、毁损、丢失可能对金融消费者产生其他不利影响的，应当及时告知金融消费者，并在72小时以内报告银行、支付机构住所地的中国人民银行分支机构。中国人民银行分支机构接到报告后，视情况按照本办法第五十五条规定处理。

第四章　金融消费争议解决

第三十五条 金融消费者与银行、支付机构发生金融消费争议的，

鼓励金融消费者先向银行、支付机构投诉，鼓励当事人平等协商，自行和解。

金融消费者应当依法通过正当途径客观、理性反映诉求，不扰乱正常的金融秩序和社会公共秩序。

本办法所称金融消费争议，是指金融消费者与银行、支付机构因购买、使用金融产品或者服务所产生的民事争议。

第三十六条 银行、支付机构应当切实履行金融消费投诉处理的主体责任，银行、支付机构的法人机构应当按年度向社会发布金融消费者投诉数据和相关分析报告。

第三十七条 银行、支付机构应当通过金融消费者方便获取的渠道公示本机构的投诉受理方式，包括但不限于营业场所、官方网站首页、移动应用程序的醒目位置及客服电话主要菜单语音提示等。

第三十八条 银行、支付机构应当按照中国人民银行要求，加强对金融消费者投诉处理信息系统的建设与管理，对投诉进行正确分类并按时报送相关信息，不得迟报、漏报、谎报、错报或者瞒报投诉数据。

第三十九条 银行、支付机构收到金融消费者投诉后，依照相关法律法规和合同约定进行处理，并告知投诉人处理情况，但因投诉人原因导致无法告知的除外。

第四十条 中国人民银行分支机构设立投诉转办服务渠道。金融消费者对银行、支付机构作出的投诉处理不接受的，可以通过银行、支付机构住所地、合同签订地或者经营行为发生地中国人民银行分支机构进行投诉。

通过电子商务、网络交易购买、使用金融产品或者服务的，金融消费者通过银行、支付机构住所地的中国人民银行分支机构进行投诉。

第四十一条 金融消费者通过中国人民银行分支机构进行投诉，应当提供以下信息：姓名，有效身份证件信息，联系方式，明确的投诉对象及其住所地，具体的投诉请求、事实和理由。

金融消费者可以本人提出投诉，也可以委托他人代为提出投诉。以来信来访方式进行委托投诉的，应当向中国人民银行分支机构提交前款规定的投诉材料、授权委托书原件、委托人和受托人的身份证明。授权委托书应当载明受托人、委托事项、权限和期限，并由委托人本人签名。

第四十二条 中国人民银行分支机构对下列投诉不予接收：

（一）投诉人投诉的机构、产品或者服务不属于中国人民银行监管范围的。

（二）投诉人未提供真实身份，或者没有明确的被投诉人、没有具体的投诉请求和事实依据的。

（三）投诉人并非金融消费者本人，也未经金融消费者本人委托的。

（四）人民法院、仲裁机构、其他金融管理部门、行政部门或者依法设立的调解组织已经受理、接收或者处理的。

（五）双方达成和解协议并已经执行，没有新情况、新理由的。

（六）被投诉机构已提供公平合理的解决方案，投诉人就同一事项再次向中国人民银行分支机构投诉的。

（七）其他不符合法律、行政法规、规章有关规定的。

第四十三条 中国人民银行分支机构收到金融消费者投诉的，应当自收到投诉之日起7个工作日内作出下列处理：

（一）对投诉人和被投诉机构信息、投诉请求、事实和理由等进行登记。

（二）作出是否接收投诉的决定。决定不予接收的，应当告知投诉人。

（三）决定接收投诉的，应当将投诉转交被投诉机构处理或者转交金融消费纠纷调解组织提供调解服务。

需要投诉人对投诉内容进行补正的，处理时限于补正完成之日起计算。

银行、支付机构应当自收到中国人民银行分支机构转交的投诉之日起15日内答复投诉人。情况复杂的，经本机构投诉处理工作负责人批准，可以延长处理期限，并告知投诉人延长处理期限的理由，但最长处理期限不得超过60日。

第四十四条 银行、支付机构收到中国人民银行分支机构转交的投诉，应当按要求向中国人民银行分支机构反馈投诉处理情况。

反馈的内容包括投诉基本情况、争议焦点、调查结果及证据、处理依据、与金融消费者的沟通情况、延期处理情况及投诉人满意度等。

银行、支付机构应当妥善保存投诉资料，投诉资料留存时间自投诉办结之日起不得少于3年。法律、行政法规另有规定的，从其规定。

第四十五条 银行、支付机构、金融消费者可以向调解组织申请调

解、中立评估。调解组织受理调解、中立评估申请后，可在合理、必要范围内请求当事人协助或者提供相关文件、资料。

本办法所称中立评估，是指调解组织聘请独立专家就争议解决提出参考性建议的行为。

第四十六条 金融消费纠纷调解组织应当依照法律、行政法规、规章及其章程的规定，组织开展金融消费纠纷调解、中立评估等工作，对银行、支付机构和金融消费者进行金融知识普及和教育宣传引导。

第五章 监督与管理机制

第四十七条 中国人民银行综合研究金融消费者保护重大问题，负责拟定发展规划和业务标准，建立健全金融消费者保护基本制度。

第四十八条 中国人民银行及其分支机构与其他金融管理部门、地方政府有关部门建立健全金融消费者权益保护工作协调机制，加强跨市场跨业态跨区域金融消费者权益保护的监管，强化信息共享和部门间沟通协作。

第四十九条 中国人民银行及其分支机构统筹开展金融消费者教育，引导、督促银行、支付机构开展金融知识普及宣传活动，协调推进金融知识纳入国民教育体系，组织开展消费者金融素养调查。

第五十条 中国人民银行及其分支机构会同有关部门构建监管执法合作机制，探索合作开展金融消费者权益保护监督检查、评估等具体工作。

第五十一条 中国人民银行及其分支机构牵头构建非诉第三方解决机制，鼓励、支持金融消费者权益保护社会组织依法履行职责，推

动构建公正、高效、便捷的多元化金融消费纠纷解决体系。

第五十二条 中国人民银行及其分支机构协调推进相关普惠金融工作，建立健全普惠金融工作机制，指导、督促银行、支付机构落实普惠金融发展战略，组织开展职责范围内的普惠金融具体工作。

第五十三条 中国人民银行及其分支机构对金融消费者投诉信息进行汇总和分析，根据汇总和分析结果适时优化金融消费者权益保护监督管理方式、金融机构行为规范等。

第五十四条 中国人民银行及其分支机构可以采取下列措施，依法在职责范围内开展对银行、支付机构金融消费者权益保护工作的监督检查：

（一）进入被监管机构进行检查。

（二）询问被监管机构的工作人员，要求其对有关检查事项作出说明。

（三）查阅、复制被监管机构与检查事项有关的文件、资料，对可能被转移、隐匿或者毁损的文件、资料予以登记保存。

（四）检查被监管机构的计算机网络与信息系统。

进行现场检查时，检查人员不得少于二人，并应当出示合法证件和检查通知书。

银行、支付机构应当积极配合中国人民银行及其分支机构的现场检查和非现场检查，如实提供有关资料，不得拒绝、阻挠、逃避检查，不得谎报、隐匿、销毁相关证据材料。

第五十五条 银行、支付机构有侵害金融消费者合法权益行为的，

中国人民银行及其分支机构可以对其采取下列措施：

（一）要求提交书面说明或者承诺。

（二）约见谈话。

（三）责令限期整改。

（四）视情将相关信息向其上级机构、行业监管部门反馈，在行业范围内发布，或者向社会公布。

（五）建议银行、支付机构对直接负责的董事、高级管理人员和其他直接责任人员给予处分。

（六）依法查处或者建议其他行政管理部门依法查处。

（七）中国人民银行职责范围内依法可以采取的其他措施。

第五十六条 中国人民银行及其分支机构组织开展银行、支付机构履行金融消费者权益保护义务情况的评估工作。

评估工作以银行、支付机构自评估为基础。银行、支付机构应当按年度进行自评估，并于次年1月31日前向中国人民银行或其分支机构报送自评估报告。

中国人民银行及其分支机构根据日常监督管理、投诉管理以及银行、支付机构自评估等情况进行非现场评估，必要时可以进行现场评估。

第五十七条 中国人民银行及其分支机构可以根据具体情况开展金融消费者权益保护环境评估工作。

第五十八条 中国人民银行及其分支机构建立金融消费者权益保护案例库制度，按照预防为先、教育为主的原则向银行、支付机构和

金融消费者进行风险提示。

第五十九条 中国人民银行及其分支机构对于涉及金融消费者权益保护的重大突发事件，应当按照有关规定做好相关应急处置工作。

第六章 法律责任

第六十条 银行、支付机构有下列情形之一，侵害消费者金融信息依法得到保护的权利的，中国人民银行或其分支机构应当在职责范围内依照《中华人民共和国消费者权益保护法》第五十六条的规定予以处罚：

（一）未经金融消费者明示同意，收集、使用其金融信息的。

（二）收集与业务无关的消费者金融信息，或者采取不正当方式收集消费者金融信息的。

（三）未公开收集、使用消费者金融信息的规则，未明示收集、使用消费者金融信息的目的、方式和范围的。

（四）超出法律法规规定和双方约定的用途使用消费者金融信息的。

（五）未建立以分级授权为核心的消费者金融信息使用管理制度，或者未严格落实信息使用授权审批程序的。

（六）未采取技术措施和其他必要措施，导致消费者金融信息遗失、毁损、泄露或者被篡改，或者非法向他人提供的。

第六十一条 银行、支付机构有下列情形之一，对金融产品或者服务作出虚假或者引人误解的宣传的，中国人民银行或其分支机构应当在职责范围内依照《中华人民共和国消费者权益保护法》第五十六条

的规定予以处罚：

（一）实际承担的义务低于在营销宣传活动中通过广告、资料或者说明等形式对金融消费者所承诺的标准的。

（二）引用不真实、不准确的数据和资料或者隐瞒限制条件等，对过往业绩或者产品收益进行夸大表述的。

（三）利用金融管理部门对金融产品或者服务的审核或者备案程序，误导金融消费者认为金融管理部门已对该金融产品或者服务提供保证的。

（四）明示或者暗示保本、无风险或者保收益等，对非保本投资型金融产品的未来效果、收益或者相关情况作出保证性承诺的。

第六十二条 银行、支付机构违反本办法规定，有下列情形之一，有关法律、行政法规有处罚规定的，依照其规定给予处罚；有关法律、行政法规未作处罚规定的，中国人民银行或其分支机构应当根据情形单处或者并处警告、处以五千元以上三万元以下罚款：

（一）未建立金融消费者权益保护专职部门或者指定牵头部门，或者金融消费者权益保护部门没有足够的人力、物力独立开展工作的。

（二）擅自代理金融消费者办理业务，擅自修改金融消费者的业务指令，或者强制搭售其他产品或者服务的。

（三）未按要求向金融消费者披露与金融产品和服务有关的重要内容的。

（四）利用技术手段、优势地位，强制或者变相强制金融消费者接受金融产品或者服务，或者排除、限制金融消费者接受同业机构提

供的金融产品或者服务的。

（五）通过附加限制性条件的方式要求金融消费者购买、使用协议中未作明确要求的产品或者服务的。

（六）未按要求使用格式条款的。

（七）出现侵害金融消费者合法权益重大事件未及时向中国人民银行或其分支机构报告的。

（八）不配合中国人民银行及其分支机构开展金融消费者权益保护领域相关工作，或者未按照规定报送相关资料的。

（九）未按要求对金融消费者投诉进行正确分类，或者迟报、漏报、谎报、错报、瞒报投诉数据的。

（十）收到中国人民银行分支机构转交的投诉后，未在规定期限内答复投诉人，或者未按要求向中国人民银行分支机构反馈投诉处理情况的。

（十一）拒绝、阻挠、逃避检查，或者谎报、隐匿、销毁相关证据材料的。

第六十三条 对银行、支付机构侵害金融消费者权益重大案件负有直接责任的董事、高级管理人员和其他直接责任人员，有关法律、行政法规有处罚规定的，依照其规定给予处罚；有关法律、行政法规未作处罚规定的，中国人民银行或其分支机构应当根据情形单处或者并处警告、处以五千元以上三万元以下罚款。

第六十四条 中国人民银行及其分支机构的工作人员在开展金融消费者权益保护工作过程中有下列情形之一的，依法给予处分；涉嫌

构成犯罪的，移送司法机关依法追究刑事责任：

（一）违反规定对银行、支付机构进行检查的。

（二）泄露知悉的国家秘密或者商业秘密的。

（三）滥用职权、玩忽职守的其他行为。

第七章　附　则

第六十五条 商业银行理财子公司、金融资产管理公司、信托公司、汽车金融公司、消费金融公司以及征信机构、个人本外币兑换特许业务经营机构参照适用本办法。法律、行政法规另有规定的，从其规定。

第六十六条 本办法中除“工作日”以外的“日”为自然日。

第六十七条 本办法由中国人民银行负责解释。

第六十八条 本办法自2020年11月1日起施行。《中国人民银行金融消费权益保护工作管理办法（试行）》（银办发〔2013〕107号文印发）与《中国人民银行金融消费者权益保护实施办法》（银发〔2016〕314号文印发）同时废止。

在线旅游经营服务管理暂行规定

时效性：　　现行有效

发文机关：　文化和旅游部

文号：　　文化和旅游部令第 4 号

发文日期：　2020 年 08 月 20 日

施行日期：　2020 年 10 月 01 日

第一章 总 则

第一条　为保障旅游者合法权益，规范在线旅游市场秩序，促进在线旅游行业可持续发展，依据《中华人民共和国旅游法》《中华人民共和国消费者权益保护法》《中华人民共和国网络安全法》《中华人民共和国电子商务法》《旅行社条例》等相关法律、行政法规，制定本规定。

第二条　在中华人民共和国境内提供在线旅游经营服务，适用本规定。

本规定所称在线旅游经营服务，是指通过互联网等信息网络为旅游者提供包价旅游服务或者交通、住宿、餐饮、游览、娱乐等单项旅游服务的经营活动。

第三条　本规定所称在线旅游经营者，是指从事在线旅游经营服务的自然人、法人和非法人组织，包括在线旅游平台经营者、平台内经营者以及通过自建网站、其他网络服务提供旅游服务的经营者。

本规定所称平台经营者，是指为在线旅游经营服务交易双方或者多方提供网络经营场所、交易撮合、信息发布等服务的法人或者非法

人组织。

本规定所称平台内经营者，是指通过平台经营者提供旅游服务的在线旅游经营者。

第四条　在线旅游经营者提供在线旅游经营服务，应当遵守社会主义核心价值观的要求，坚守人身财产安全、信息内容安全、网络安全等底线，诚信经营、公平竞争，承担产品和服务质量责任，接受政府和社会的监督。

第五条　文化和旅游部按照职责依法负责全国在线旅游经营服务的指导、协调、监管工作。县级以上地方文化和旅游主管部门按照职责分工负责本辖区内在线旅游经营服务的监督管理工作。

第六条　各级文化和旅游主管部门应当积极协调相关部门在财政、税收、金融、保险等方面支持在线旅游行业发展，保障在线旅游经营者公平参与市场竞争，充分发挥在线旅游经营者在旅游目的地推广、旅游公共服务体系建设、旅游大数据应用、景区门票预约和流量控制等方面的积极作用，推动旅游业高质量发展。

第二章 运 营

第七条　在线旅游经营者应当依法建立旅游者安全保护制度，制定应急预案，结合有关政府部门发布的安全风险提示等信息进行风险监测和安全评估，及时排查安全隐患，做好旅游安全宣传与引导、风险提示与防范、应急救助与处置等工作。

第八条　在线旅游经营者发现法律、行政法规禁止发布或者传输的信息，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，保存有关记录并向主管部门报告。

平台经营者应当对上传至平台的文字、图片、音视频等信息内容加强审核，确保平台信息内容安全。

第九条　在线旅游经营者应当按照《中华人民共和国网络安全法》等相关法律规定，贯彻网络安全等级保护制度，落实网络安全管理和技术措施，制定网络安全应急预案，并定期组织开展演练，确保在线旅游经营服务正常开展。

第十条　在线旅游经营者经营旅行社业务的，应当依法取得旅行社业务经营许可。

第十一条　平台经营者应当对平台内经营者的身份、地址、联系方式、行政许可、质量标准等级、信用等级等信息进行真实性核验、登记，建立登记档案，并定期核验更新。

平台经营者应当督促平台内经营者对其旅游辅助服务者的相关信息进行真实性核验、登记。

第十二条　在线旅游经营者应当提供真实、准确的旅游服务信息，不得进行虚假宣传；未取得质量标准、信用等级的，不得使用相关称谓和标识。平台经营者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。

在线旅游经营者为旅游者提供交通、住宿、游览等预订服务的，应当建立公开、透明、可查询的预订渠道，促成相关预订服务依约履行。

第十三条　在线旅游经营者应当保障旅游者的正当评价权，不

得擅自屏蔽、删除旅游者对其产品和服务的评价，不得误导、引诱、替代或者强制旅游者做出评价，对旅游者做出的评价应当保存并向社会公开。在线旅游经营者删除法律、法规禁止发布或者传输的评价信息的，应当在后台记录和保存。

第十四条　在线旅游经营者应当保护旅游者个人信息等数据安全，在收集旅游者信息时事先明示收集旅游者个人信息的目的、方式和范围，并经旅游者同意。

在线旅游经营者在签订包价旅游合同或者出境旅游产品代订合同时，应当提示旅游者提供紧急联络人信息。

第十五条　在线旅游经营者不得滥用大数据分析等技术手段，基于旅游者消费记录、旅游偏好等设置不公平的交易条件，侵犯旅游者合法权益。

第十六条　在线旅游经营者为旅游者提供包价旅游服务的，应当依法与旅游者签订合同，并在全国旅游监管服务平台填报合同有关信息。

第十七条　经营旅行社业务的在线旅游经营者应当投保旅行社责任险。

在线旅游经营者应当提示旅游者投保人身意外伤害保险。销售出境旅游产品时，应当为有购买境外旅游目的地保险需求的旅游者提供必要协助。

第十八条　在线旅游经营者应当协助文化和旅游主管部门对不合理低价游进行管理，不得为其提供交易机会。

第十九条　平台经营者应当对平台内经营者服务情况、旅游合同履行情况以及投诉处理情况等产品和服务信息、交易信息依法进行记录、保存，进行动态管理。

第二十条　社交网络平台、移动应用商店等信息网络提供者知道或者应当知道他人利用其服务从事违法违规在线旅游经营服务，或者侵害旅游者合法权益的，应当采取删除、屏蔽、断开链接等必要措施。

第二十一条　平台经营者应当在首页显著位置公示全国旅游投诉渠道。

平台内经营者与旅游者发生旅游纠纷的，平台经营者应当积极协助旅游者维护合法权益。鼓励平台经营者先行赔付。

第二十二条　平台经营者发现以下情况，应当立即采取必要的救助和处置措施，并依法及时向县级以上文化和旅游主管部门报告：

（一）提供的旅游产品或者服务存在缺陷，危及旅游者人身、财产安全的；

（二）经营服务过程中发生突发事件或者旅游安全事故的；

（三）平台内经营者未经许可经营旅行社业务的；

（四）出现法律、法规禁止交易的产品或者服务的；

（五）其他应当报告的事项。

第三章 监督检查

第二十三条　各级文化和旅游主管部门应当建立日常检查、定期检查以及与相关部门联合检查的监督管理制度，依法对在线旅游经

营服务实施监督检查，查处违法违规行为。

在监督检查过程中，县级以上文化和旅游主管部门要求在线旅游经营者提供相关数据信息的，在线旅游经营者应当予以配合。县级以上文化和旅游主管部门应当采取必要措施保护数据信息的安全。

第二十四条　县级以上文化和旅游主管部门对有不诚信经营、侵害旅游者评价权、滥用技术手段设置不公平交易条件等违法违规经营行为的在线旅游经营者，可以通过约谈等行政指导方式予以提醒、警示、制止，并责令其限期整改。

第二十五条　在线旅游经营服务违法行为由实施违法行为的经营者住所地县级以上文化和旅游主管部门管辖。不能确定经营者住所地的，由经营者注册登记地或者备案地、旅游合同履行地县级以上文化和旅游主管部门管辖。

受理在线旅游经营服务相关投诉，参照前款处理。

第二十六条　县级以上文化和旅游主管部门依法建立在线旅游行业信用档案，将在线旅游经营者市场主体登记、行政许可、抽查检查、列入经营异常名录或者严重违法失信企业名单、行政处罚等信息依法列入信用记录，适时通过全国旅游监管服务平台或者本部门官方网站公示，并与相关部门建立信用档案信息共享机制，依法对严重违法失信者实施联合惩戒措施。

第二十七条　支持在线旅游经营者成立行业组织，并按照本组织章程依法制定行业经营规范和服务标准，加强行业自律，推动行业诚信建设和服务质量评价，监督、引导本行业经营者公平参与市场竞

争。

第四章 法律责任

第二十八条　平台经营者知道或者应当知道平台内经营者不符合保障旅游者人身、财产安全要求或者有其他侵害旅游者合法权益行为，未及时采取必要措施的，依法与该平台内经营者承担连带责任。

平台经营者未对平台内经营者资质进行审核，或者未对旅游者尽到安全提示或保障义务，造成旅游者合法权益损害的，依法承担相应责任。

第二十九条　旅游者有下列情形之一的，依法承担相关责任：

（一）在旅游活动中从事违法违规活动的；

（二）未按要求提供与旅游活动相关的个人健康信息的；

（三）不听从在线旅游经营者的告知、警示，参加不适合自身条件的旅游活动，导致出现人身财产损害的；

（四）对国家应对重大突发事件暂时限制旅游活动的措施、安全防范和应急处置措施不予配合的。

第三十条　因不可抗力或者第三人造成旅游者损害的，在线旅游经营者应当及时进行救助。在线旅游经营者未及时进行救助造成旅游者损害的，依法承担相应责任。旅游者接受救助后，依法支付应当由个人承担的费用。

第三十一条　在线旅游经营者违反本规定第八条第一款规定，由县级以上文化和旅游主管部门依照《中华人民共和国网络安全法》第六十八条有关规定处理。

第三十二条　在线旅游经营者违反本规定第十条规定，未依法取得旅行社业务经营许可开展相关业务的，由县级以上文化和旅游主管部门依照《中华人民共和国旅游法》第九十五条的规定处理。

在线旅游经营者违反本规定第十七条第一款规定，未依法投保旅行社责任保险的，由县级以上文化和旅游主管部门依照《中华人民共和国旅游法》第九十七条有关规定处理。

第三十三条　平台经营者有下列情形之一的，由县级以上文化和旅游主管部门依照《中华人民共和国电子商务法》第八十条的规定处理：

（一）违反本规定第十一条第一款规定，不依法履行核验、登记义务的；

（二）违反本规定第二十二条规定，不依法对违法情形采取必要处置措施或者未报告的；

（三）违反本规定第十九条规定，不依法履行商品和服务信息、交易信息保存义务的。

第三十四条　在线旅游经营者违反本规定第十二条第一款有关规定，未取得质量标准、信用等级使用相关称谓和标识的，由县级以上文化和旅游主管部门责令改正，给予警告，可并处三万元以下罚款。

第三十五条　违反本规定第十六条规定，未在全国旅游监管服务平台填报包价旅游合同有关信息的，由县级以上文化和旅游主管部门责令改正，给予警告；拒不改正的，处一万元以下罚款。

第三十六条　在线旅游经营者违反本规定第十八条规定，为以

不合理低价组织的旅游活动提供交易机会的，由县级以上文化和旅游主管部门责令改正，给予警告，可并处三万元以下罚款。

第三十七条　法律、行政法规对违反本规定行为另有规定的，依照其规定。县级以上地方文化和旅游主管部门在监督检查过程中发现在线旅游经营者有违反《中华人民共和国电子商务法》《中华人民共和国消费者权益保护法》《中华人民共和国网络安全法》等法律、行政法规、部门规章的行为，不属于本部门管辖的，应当及时将相关线索依法移送有关部门。

第五章 附 则

第三十八条　本规定自2020年10月1日起施行。

关于规范互联网保险销售行为可回溯管理的通知

时效性：　　现行有效

发文机关：　中国银行保险监督管理委员会

文号：　　银保监发〔2020〕26号

发文日期：　2020年06月22日

施行日期：　2020年10月01日

各银保监局，各保险集团（控股）公司、保险公司、保险专业中介机构:

为规范和加强互联网保险销售行为可回溯管理，保障消费者知情权、自主选择权和公平交易权等基本权利，促进互联网保险业务健康发展，现将有关事项通知如下：

一、本通知所称互联网保险销售行为可回溯，是指保险机构通过销售页面管理和销售过程记录等方式，对在自营网络平台上销售保险产品的交易行为进行记录和保存，使其可供查验。

本通知所称保险机构包括保险公司和保险中介机构。

二、保险机构在自营网络平台上销售投保人为自然人的商业保险产品时，应当实施互联网保险销售行为可回溯管理。个人税收优惠型健康保险、个人税收递延型养老保险产品除外。

三、销售页面是指保险机构在自营网络平台上设置的投保及承保全流程页面，包含提示进入投保流程、展示说明保险条款、履行提示和明确说明义务、验证投保人身份，及投保人填写投保信息、自主确认阅读有关信息、提交投保申请、缴纳保费等内容的网络页面。

四、保险机构应当在自营网络平台通过设置销售页面实现互联网保险销售，不得在非自营网络平台设置销售页面。保险机构可以在非自营网络平台设置投保申请链接，由投保人点击链接进入自营网络平台的销售页面。非保险机构自营网络平台不得设置保险产品销售页面。

五销售页面管理是指保险机构应当保存销售页面的内容信息及历史修改信息，并建立销售页面版本管理机制。

六、销售页面的首页必须是提示进入投保流程页面，保险机构应当通过设置提示进入投保流程页面，对销售页面和非销售页面进行分隔。非销售页面中不得包含投保人填写投保信息、提交投保申请等内容。

七、 提示进入投保流程页面应当包含提示投保人即将进入投保流程、需仔细阅读保险条款、投保人在销售页面的操作将被记录等内容。

保险中介机构的提示进入投保流程页面，应当增加客户告知书内容并重点披露该保险中介机构和承保保险公司名称。

八、保险机构的销售页面应当展示保险条款或提供保险条款文本链接，说明合同内容，并设置由投保人自主确认已阅读的标识。

九、保险机构应当以足以引起投保人注意的文字、字体、符号或其他明显标志，对保险合同中免除保险公司责任的条款内容进行逐项展示，并以网页、音频或视频等形式予以明确说明。

十、保险机构销售以下保险产品时，应当按照要求展示可能影响保单效力以及可能免除保险公司责任的内容，包括但不限于：

（一）销售人身保险新型产品，应当增加保单利益不确定性风险提示内容；

（二）销售健康保险产品，应当增加保险责任等待期的起算时间、期限及对投保人权益的影响，指定医疗机构，是否保证续保及续保有效时间，是否自动续保，医疗费用补偿原则，费率是否调整等内容；

（三）销售含有犹豫期条款的保险产品，应当增加犹豫期条款内容。

十一、保险机构销售以死亡为给付条件、被保险人与投保人不一致的保险产品时，应当按照要求展示被保险人同意投保并确认保险金额的内容。父母为其未成年子女投保的除外。

十二、保险机构应当对健康告知提示进行展示。投保人健康告知页面应当包含投保人健康告知内容、未尽到如实告知义务后果说明等内容。健康告知提示应当与保险责任直接相关，表述通俗易懂，内容具体且问题边界清晰。

十三、保险机构应当将第七、九、十、十一、十二条的内容设置单独页面展示，并设置由投保人或被保险人自主确认已阅读的标识。

本通知要求由投保人或被保险人自主确认已阅读的销售页面，投保人或被保险人未自主确认的，保险机构不得接收投保人的投保申请、收取保费。

十四、保险机构开展互联网保险销售时，应当根据对个人保险实名制的管理要求，对投保人、被保险人和受益人身份真实性进行验证。

十五、保险机构应当将投保人、被保险人在销售页面上的操作轨

迹予以记录和保存，操作轨迹应当包含投保人进入和离开销售页面的时点、投保人和被保险人填写或点选销售页面中的相关内容及时间等。

十六、保险机构应当记录和保存投保期间通过在线服务体系向投保人解释说明保险条款的有关信息。

十七、保险机构开展互联网保险销售行为可回溯时，收集、使用消费者信息应当遵循合法、正当、必要的原则，不得收集与其销售产品无关的消费者信息。

十八、保险机构负责互联网保险销售行为可回溯资料的归档管理，互联网保险销售行为可回溯资料应当至少包括销售页面，投保人、被保险人在相关销售页面上的操作轨迹和投保期间保险机构通过在线服务体系向投保人解释说明保险条款的有关信息。

十九、互联网保险销售行为可回溯资料保管期限自保险合同终止之日起计算，保险期间在一年以下的不得少于五年，保险期间超过一年的不得少于十年。遇消费者投诉、法律诉讼等纠纷的，应当至少保存至纠纷结束后三年。

二十、互联网保险销售行为可回溯资料应当可以还原为可供查验的有效文件，销售页面应当可以还原为可供查验的有效图片或视频。

二十一、保险机构开展互联网保险销售行为可回溯相关工作时，应当严格依照有关法律法规，采取切实可行的管理措施和技术措施，保护投保人、被保险人和受益人的个人信息安全。

二十二、保险机构应当对互联网保险销售行为可回溯管理建立全面、系统、规范的内部控制体系，加强内控制度建设和内控流程设计，

实现对销售行为可回溯管理所有流程和操作环节的有效监控。

二十三、保险机构开展互联网保险销售时，涉及非互联网保险销售方式的，一并适用本通知和中国银保监会关于可回溯管理的其他监管要求。

二十四、保险机构通过固定场所设置的自助终端销售保险产品的，适用本通知。本通知实施前关于自助终端销售行为可回溯管理的相关监管要求与本通知不一致的，以本通知为准。

二十五、 保险机构未按照本通知要求对互联网保险销售行为进行可回溯管理的，由中国银保监会及其派出机构依照有关法律规定予以处罚或采取监管措施。

二十六、本通知自 2020 年 10 月 1 日起实施。本通知实施后仍不能符合要求的保险机构，应当立即停止开展相关互联网保险销售业务。

网络安全审查办法

时效性：　　现行有效

发文机关：　国家互联网信息办公室、国家发展和改革委员会、工业和信息化部、公安部、国家安全部、财政部、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

文号：　　国家互联网信息办公室、国家发展和改革委员会、工业和信息化部、公安部、国家安全部、财政部、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、国家密码管理局令第 8 号

发文日期：　2021 年 12 月 28 日

施行日期：　2022 年 02 月 15 日

第一条　为了确保关键信息基础设施供应链安全，保障网络安全和数据安全，维护国家安全，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》、《中华人民共和国数据安全法》、《关键信息基础设施安全保护条例》，制定本办法。

第二条　关键信息基础设施运营者采购网络产品和服务，网络平台运营者开展数据处理活动，影响或者可能影响国家安全的，应当按照本办法进行网络安全审查。

前款规定的关键信息基础设施运营者、网络平台运营者统称为当事人。

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，从产品和服务以及数据处理活动安全性、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　关键信息基础设施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。

关键信息基础设施安全保护工作部门可以制定本行业、本领域预判指南。

第六条　对于申报网络安全审查的采购活动，关键信息基础设施运营者应当通过采购文件、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者必要的技术支持服务等。

第七条　掌握超过100万用户个人信息的网络平台运营者赴国外上市，必须向网络安全审查办公室申报网络安全审查。

第八条　当事人申报网络安全审查，应当提交以下材料：

（一）申报书；

（二）关于影响或者可能影响国家安全的分析报告；

（三）采购文件、协议、拟签订的合同或者拟提交的首次公开募股（IPO）等上市申请文件；

（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符合本办法第八条规定的审查申报材料起10个工作日内，确定是否需要审查并书面通知当事人。

第十条　网络安全审查重点评估相关对象或者情形的以下国家安全风险因素：

（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、遭受干扰或者破坏的风险；

（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、重要数据或者大量个人信息被窃取、泄露、毁损以及非法利用、非法出境的风险；

（六）上市存在关键信息基础设施、核心数据、重要数据或者大量个人信息被外国政府影响、控制、恶意利用的风险，以及网络信息安全风险；

（七）其他可能危害关键信息基础设施安全、网络安全和数据安全的因素。

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，应当自向当事人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和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当事人；意见不一致的，按照特别审查程序处理，并通知当事人。

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单位和部门意见，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部门意见，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当事人。

第十四条　特别审查程序一般应当在90个工作日内完成，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，当事人、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者可能影响国家安全的网络产品和服务以及数据处理活动，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。

为了防范风险，当事人应当在审查期间按照网络安全审查要求采取预防和消减风险的措施。

第十七条　参与网络安全审查的相关机构和人员应当严格保护知识产权，对在审查工作中知悉的商业秘密、个人信息，当事人、产品和服务提供者提交的未公开材料，以及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者用于审查以外的目的。

第十八条　当事人或者网络产品和服务提供者认为审查人员有失客观公正，或者未能对审查工作中知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　当事人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　当事人违反本办法规定的，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、网络安全和数据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。

国家对数据安全审查、外商投资安全审查另有规定的，应当同时符合其规定。

第二十三条　本办法自2022年2月15日起施行。2020年4月13日公布的《网络安全审查办法》（国家互联网信息办公室、国家发展和改革委员会、工业和信息化部、公安部、国家安全部、财政部、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、国家保密局、国家密码管理局令第6号）同时废止。

关于构建更加完善的要素市场化配置体制机制的意见

时效性：　　现行有效

发布机关：　中共中央、国务院

发布日期：　2020 年 3 月 30 日

完善要素市场化配置是建设统一开放、竞争有序市场体系的内在要求，是坚持和完善社会主义基本经济制度、加快完善社会主义市场经济体制的重要内容。为深化要素市场化配置改革，促进要素自主有序流动，提高要素配置效率，进一步激发全社会创造力和市场活力，推动经济发展质量变革、效率变革、动力变革，现就构建更加完善的要素市场化配置体制机制提出如下意见。

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，全面贯彻党的十九大和十九届二中、三中、四中全会精神，坚持稳中求进工作总基调，坚持以供给侧结构性改革为主线，坚持新发展理念，坚持深化市场化改革、扩大高水平开放，破除阻碍要素自由流动的体制机制障碍，扩大要素市场化配置范围，健全要素市场体系，推进要素市场制度建设，实现要素价格市场决定、流动自主有序、配置高效公平，为建设高标准市场体系、推动高质量发展、建设现代化经济体系打下坚实制度基础。

（二）基本原则。一是市场决定，有序流动。充分发挥市场配置资源的决定性作用，畅通要素流动渠道，保障不同市场主体平等获取生产要素，推动要素配置依据市场规则、市场价格、市场竞争实现效

益最大化和效率最优化。二是健全制度，创新监管。更好发挥政府作用，健全要素市场运行机制，完善政府调节与监管，做到放活与管好有机结合，提升监管和服务能力，引导各类要素协同向先进生产力集聚。三是问题导向，分类施策。针对市场决定要素配置范围有限、要素流动存在体制机制障碍等问题，根据不同要素属性、市场化程度差异和经济社会发展需要，分类完善要素市场化配置体制机制。四是稳中求进，循序渐进。坚持安全可控，从实际出发，尊重客观规律，培育发展新型要素形态，逐步提高要素质量，因地制宜稳步推进要素市场化配置改革。

二、推进土地要素市场化配置

（三）建立健全城乡统一的建设用地市场。加快修改完善土地管理法实施条例，完善相关配套制度，制定出台农村集体经营性建设用地入市指导意见。全面推开农村土地征收制度改革，扩大国有土地有偿使用范围。建立公平合理的集体经营性建设用地入市增值收益分配制度。建立公共利益征地的相关制度规定。

（四）深化产业用地市场化配置改革。健全长期租赁、先租后让、弹性年期供应、作价出资（入股）等工业用地市场供应体系。在符合国土空间规划和用途管制要求前提下，调整完善产业用地政策，创新使用方式，推动不同产业用地类型合理转换，探索增加混合产业用地供给。

（五）鼓励盘活存量建设用地。充分运用市场机制盘活存量土地和低效用地，研究完善促进盘活存量建设用地的税费制度。以多种方

式推进国有企业存量用地盘活利用。深化农村宅基地制度改革试点，深入推进建设用地整理，完善城乡建设用地增减挂钩政策，为乡村振兴和城乡融合发展提供土地要素保障。

（六）完善土地管理体制。完善土地利用计划管理，实施年度建设用地总量调控制度，增强土地管理灵活性，推动土地计划指标更加合理化，城乡建设用地指标使用应更多由省级政府负责。在国土空间规划编制、农村房地一体不动产登记基本完成的前提下，建立健全城乡建设用地供应三年滚动计划。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。加强土地供应利用统计监测。实施城乡土地统一调查、统一规划、统一整治、统一登记。推动制定不动产登记法。

三、引导劳动力要素合理畅通有序流动

（七）深化户籍制度改革。推动超大、特大城市调整完善积分落户政策，探索推动在长三角、珠三角等城市群率先实现户籍准入年限同城化累计互认。放开放宽除个别超大城市外的城市落户限制，试行以经常居住地登记户口制度。建立城镇教育、就业创业、医疗卫生等基本公共服务与常住人口挂钩机制，推动公共资源按常住人口规模配置。

（八）畅通劳动力和人才社会性流动渠道。健全统一规范的人力资源市场体系，加快建立协调衔接的劳动力、人才流动政策体系和交流合作机制。营造公平就业环境，依法纠正身份、性别等就业歧视现象，保障城乡劳动者享有平等就业权利。进一步畅通企业、社会组织人员进入党政机关、国有企事业单位渠道。优化国有企事业单位面向

社会选人用人机制，深入推行国有企业分级分类公开招聘。加强就业援助，实施优先扶持和重点帮助。完善人事档案管理服务，加快提升人事档案信息化水平。

（九）完善技术技能评价制度。创新评价标准，以职业能力为核心制定职业标准，进一步打破户籍、地域、身份、档案、人事关系等制约，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渠道。加快建立劳动者终身职业技能培训制度。推进社会化职称评审。完善技术工人评价选拔制度。探索实现职业技能等级证书和学历证书互通衔接。加强公共卫生队伍建设，健全执业人员培养、准入、使用、待遇保障、考核评价和激励机制。

（十）加大人才引进力度。畅通海外科学家来华工作通道。在职业资格认定认可、子女教育、商业医疗保险以及在中国境内停留、居留等方面，为外籍高层次人才来华创新创业提供便利。

四、推进资本要素市场化配置

（十一）完善股票市场基础制度。制定出台完善股票市场基础制度的意见。坚持市场化、法治化改革方向，改革完善股票市场发行、交易、退市等制度。鼓励和引导上市公司现金分红。完善投资者保护制度，推动完善具有中国特色的证券民事诉讼制度。完善主板、科创板、中小企业板、创业板和全国中小企业股份转让系统（新三板）市场建设。

（十二）加快发展债券市场。稳步扩大债券市场规模，丰富债券市场品种，推进债券市场互联互通。统一公司信用类债券信息披露标

准，完善债券违约处置机制。探索对公司信用类债券实行发行注册管理制。加强债券市场评级机构统一准入管理，规范信用评级行业发展。

（十三）增加有效金融服务供给。健全多层次资本市场体系。构建多层次、广覆盖、有差异、大中小合理分工的银行机构体系，优化金融资源配置，放宽金融服务业市场准入，推动信用信息深度开发利用，增加服务小微企业和民营企业的金融服务供给。建立县域银行业金融机构服务“三农”的激励约束机制。推进绿色金融创新。完善金融机构市场化法治化退出机制。

（十四）主动有序扩大金融业对外开放。稳步推进人民币国际化和人民币资本项目可兑换。逐步推进证券、基金行业对内对外双向开放，有序推进期货市场对外开放。逐步放宽外资金融机构准入条件，推进境内金融机构参与国际金融市场交易。

五、加快发展技术要素市场

（十五）健全职务科技成果产权制度。深化科技成果使用权、处置权和收益权改革，开展赋予科研人员职务科技成果所有权或长期使用权试点。强化知识产权保护和运用，支持重大技术装备、重点新材料等领域的自主知识产权市场化运营。

（十六）完善科技创新资源配置方式。改革科研项目立项和组织实施方式，坚持目标引领，强化成果导向，建立健全多元化支持机制。完善专业机构管理项目机制。加强科技成果转化中试基地建设。支持有条件的企业承担国家重大科技项目。建立市场化社会化的科研成果评价制度，修订技术合同认定规则及科技成果登记管理办法。建立健

全科技成果常态化路演和科技创新咨询制度。

（十七）培育发展技术转移机构和技术经理人。加强国家技术转移区域中心建设。支持科技企业与高校、科研机构合作建立技术研发中心、产业研究院、中试基地等新型研发机构。积极推进科研院所分类改革，加快推进应用技术类科研院所市场化、企业化发展。支持高校、科研机构和科技企业设立技术转移部门。建立国家技术转移人才培养体系，提高技术转移专业服务能力。

（十八）促进技术要素与资本要素融合发展。积极探索通过天使投资、创业投资、知识产权证券化、科技保险等方式推动科技成果资本化。鼓励商业银行采用知识产权质押、预期收益质押等融资方式，为促进技术转移转化提供更多金融产品服务。

（十九）支持国际科技创新合作。深化基础研究国际合作，组织实施国际科技创新合作重点专项，探索国际科技创新合作新模式，扩大科技领域对外开放。加大抗病毒药物及疫苗研发国际合作力度。开展创新要素跨境便利流动试点，发展离岸创新创业，探索推动外籍科学家领衔承担政府支持科技项目。发展技术贸易，促进技术进口来源多元化，扩大技术出口。

六、加快培育数据要素市场

（二十）推进政府数据开放共享。优化经济治理基础数据库，加快推动各地区各部门间数据共享交换，制定出台新一批数据共享责任清单。研究建立促进企业登记、交通运输、气象等公共数据开放和数据资源有效流动的制度规范。

（二十一）提升社会数据资源价值。培育数字经济新产业、新业态和新模式，支持构建农业、工业、交通、教育、安防、城市管理、公共资源交易等领域规范化数据开发利用的场景。发挥行业协会商会作用，推动人工智能、可穿戴设备、车联网、物联网等领域数据采集标准化。

（二十二）加强数据资源整合和安全保护。探索建立统一规范的数据管理制度，提高数据质量和规范性，丰富数据产品。研究根据数据性质完善产权性质。制定数据隐私保护制度和安全审查制度。推动完善适用于大数据环境下的数据分类分级安全保护制度，加强对政务数据、企业商业秘密和个人数据的保护。

七、加快要素价格市场化改革

（二十三）完善主要由市场决定要素价格机制。完善城乡基准地价、标定地价的制定与发布制度，逐步形成与市场价格挂钩动态调整机制。健全最低工资标准调整、工资集体协商和企业薪酬调查制度。深化国有企业工资决定机制改革，完善事业单位岗位绩效工资制度。建立公务员和企业相当人员工资水平调查比较制度，落实并完善工资正常调整机制。稳妥推进存贷款基准利率与市场利率并轨，提高债券市场定价效率，健全反映市场供求关系的国债收益率曲线，更好发挥国债收益率曲线定价基准作用。增强人民币汇率弹性，保持人民币汇率在合理均衡水平上的基本稳定。

（二十四）加强要素价格管理和监督。引导市场主体依法合理行使要素定价自主权，推动政府定价机制由制定具体价格水平向制定定

价规则转变。构建要素价格公示和动态监测预警体系，逐步建立要素价格调查和信息发布制度。完善要素市场价格异常波动调节机制。加强要素领域价格反垄断工作，维护要素市场价格秩序。

（二十五）健全生产要素由市场评价贡献、按贡献决定报酬的机制。着重保护劳动所得，增加劳动者特别是一线劳动者劳动报酬，提高劳动报酬在初次分配中的比重。全面贯彻落实以增加知识价值为导向的收入分配政策，充分尊重科研、技术、管理人才，充分体现技术、知识、管理、数据等要素的价值。

八、健全要素市场运行机制

（二十六）健全要素市场化交易平台。拓展公共资源交易平台功能。健全科技成果交易平台，完善技术成果转化公开交易与监管体系。引导培育大数据交易市场，依法合规开展数据交易。支持各类所有制企业参与要素交易平台建设，规范要素交易平台治理，健全要素交易信息披露制度。

（二十七）完善要素交易规则和服务。研究制定土地、技术市场交易管理制度。建立健全数据产权交易和行业自律机制。推进全流程电子化交易。推进实物资产证券化。鼓励要素交易平台与各类金融机构、中介机构合作，形成涵盖产权界定、价格评估、流转交易、担保、保险等业务的综合服务体系。

（二十八）提升要素交易监管水平。打破地方保护，加强反垄断和反不正当竞争执法，规范交易行为，健全投诉举报查处机制，防止发生损害国家安全及公共利益的行为。加强信用体系建设，完善失信

行为认定、失信联合惩戒、信用修复等机制。健全交易风险防范处置机制。

（二十九）增强要素应急配置能力。把要素的应急管理和配置作为国家应急管理体系建设的重要内容，适应应急物资生产调配和应急管理需要，建立对相关生产要素的紧急调拨、采购等制度，提高应急状态下的要素高效协同配置能力。鼓励运用大数据、人工智能、云计算等数字技术，在应急管理、疫情防控、资源调配、社会管理等方面更好发挥作用。

九、组织保障

（三十）加强组织领导。各地区各部门要充分认识完善要素市场化配置的重要性，切实把思想和行动统一到党中央、国务院决策部署上来，明确职责分工，完善工作机制，落实工作责任，研究制定出台配套政策措施，确保本意见确定的各项重点任务落到实处。

（三十一）营造良好改革环境。深化“放管服”改革，强化竞争政策基础地位，打破行政性垄断、防止市场垄断，清理废除妨碍统一市场和公平竞争的各种规定和做法，进一步减少政府对要素的直接配置。深化国有企业和国有金融机构改革，完善法人治理结构，确保各类所有制企业平等获取要素。

（三十二）推动改革稳步实施。在维护全国统一大市场的前提下，开展要素市场化配置改革试点示范。及时总结经验，认真研究改革中出现的新情况新问题，对不符合要素市场化配置改革的相关法律法规，要按程序抓紧推动调整完善。

网络信息内容生态治理规定

时效性：　　现行有效

发文机关：　国家互联网信息办公室

文号：　　国家互联网信息办公室令第 5 号

发文日期：　2019 年 12 月 15 日

施行日期：　2020 年 03 月 01 日

第一章　总则

第一条　为了营造良好网络生态，保障公民、法人和其他组织的合法权益，维护国家安全和公共利益，根据《中华人民共和国国家安全法》《中华人民共和国网络安全法》《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　中华人民共和国境内的网络信息内容生态治理活动，适用本规定。

本规定所称网络信息内容生态治理，是指政府、企业、社会、网民等主体，以培育和践行社会主义核心价值观为根本，以网络信息内容为主要治理对象，以建立健全网络综合治理体系、营造清朗的网络空间、建设良好的网络生态为目标，开展的弘扬正能量、处置违法和不良信息等相关活动。

第三条　国家网信部门负责统筹协调全国网络信息内容生态治理和相关监督管理工作，各有关主管部门依据各自职责做好网络信息内容生态治理工作。

地方网信部门负责统筹协调本行政区域内网络信息内容生态治

理和相关监督管理工作，地方各有关主管部门依据各自职责做好本行政区域内网络信息内容生态治理工作。

第二章　网络信息内容生产者

第四条　网络信息内容生产者应当遵守法律法规，遵循公序良俗，不得损害国家利益、公共利益和他人合法权益。

第五条　鼓励网络信息内容生产者制作、复制、发布含有下列内容的信息：

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

(二)宣传党的理论路线方针政策和中央重大决策部署的；

(三)展示经济社会发展亮点，反映人民群众伟大奋斗和火热生活的；

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

(五)有效回应社会关切，解疑释惑，析事明理，有助于引导群众形成共识的；

(六)有助于提高中华文化国际影响力，向世界展现真实立体全面的中国的；

(七)其他讲品味讲格调讲责任、讴歌真善美、促进团结稳定等的内容。

第六条　网络信息内容生产者不得制作、复制、发布含有下列内容的违法信息：

(一)反对宪法所确定的基本原则的;

(二)危害国家安全,泄露国家秘密,颠覆国家政权,破坏国家统一的;

(三)损害国家荣誉和利益的;

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

(五)宣扬恐怖主义、极端主义或者煽动实施恐怖活动、极端主义活动的;

(六)煽动民族仇恨、民族歧视,破坏民族团结的;

(七)破坏国家宗教政策,宣扬邪教和封建迷信的;

(八)散布谣言,扰乱经济秩序和社会秩序的;

(九)散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的;

(十)侮辱或者诽谤他人,侵害他人名誉、隐私和其他合法权益的;

(十一)法律、行政法规禁止的其他内容。

第七条　网络信息内容生产者应当采取措施,防范和抵制制作、复制、发布含有下列内容的不良信息:

(一)使用夸张标题,内容与标题严重不符的;

(二)炒作绯闻、丑闻、劣迹等的;

(三)不当评述自然灾害、重大事故等灾难的;

(四)带有性暗示、性挑逗等易使人产生性联想的;

(五)展现血腥、惊悚、残忍等致人身心不适的;

(六)煽动人群歧视、地域歧视等的;

(七)宣扬低俗、庸俗、媚俗内容的;

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

(九)其他对网络生态造成不良影响的内容。

第三章　网络信息内容服务平台

第八条　网络信息内容服务平台应当履行信息内容管理主体责任，加强本平台网络信息内容生态治理，培育积极健康、向上向善的网络文化。

第九条　网络信息内容服务平台应当建立网络信息内容生态治理机制，制定本平台网络信息内容生态治理细则，健全用户注册、账号管理、信息发布审核、跟帖评论审核、版面页面生态管理、实时巡查、应急处置和网络谣言、黑色产业链信息处置等制度。

网络信息内容服务平台应当设立网络信息内容生态治理负责人，配备与业务范围和服务规模相适应的专业人员，加强培训考核，提升从业人员素质。

第十条　网络信息内容服务平台不得传播本规定第六条规定的信息，应当防范和抵制传播本规定第七条规定的信息。

网络信息内容服务平台应当加强信息内容的管理，发现本规定第六条、第七条规定的信息的，应当依法立即采取处置措施，保存有关记录，并向有关主管部门报告。

第十一条　鼓励网络信息内容服务平台坚持主流价值导向，优化信息推荐机制，加强版面页面生态管理，在下列重点环节(包括服务类

型、位置版块等)积极呈现本规定第五条规定的信息:

(一)互联网新闻信息服务首页首屏、弹窗和重要新闻信息内容页面等;

(二)互联网用户公众账号信息服务精选、热搜等;

(三)博客、微博客信息服务热门推荐、榜单类、弹窗及基于地理位置的信息服务版块等;

(四)互联网信息搜索服务热搜词、热搜图及默认搜索等;

(五)互联网论坛社区服务首页首屏、榜单类、弹窗等;

(六)互联网音视频服务首页首屏、发现、精选、榜单类、弹窗等;

(七)互联网网址导航服务、浏览器服务、输入法服务首页首屏、榜单类、皮肤、联想词、弹窗等;

(八)数字阅读、网络游戏、网络动漫服务首页首屏、精选、榜单类、弹窗等;

(九)生活服务、知识服务平台首页首屏、热门推荐、弹窗等;

(十)电子商务平台首页首屏、推荐区等;

(十一)移动应用商店、移动智能终端预置应用软件和内置信息内容服务首屏、推荐区等;

(十二)专门以未成年人为服务对象的网络信息内容专栏、专区和产品等;

(十三)其他处于产品或者服务醒目位置、易引起网络信息内容服务使用者关注的重点环节。

网络信息内容服务平台不得在以上重点环节呈现本规定第七条

规定的信息。

第十二条　网络信息内容服务平台采用个性化算法推荐技术推送信息的，应当设置符合本规定第十条、第十一条规定要求的推荐模型，建立健全人工干预和用户自主选择机制。

第十三条　鼓励网络信息内容服务平台开发适合未成年人使用的模式，提供适合未成年人使用的网络产品和服务，便利未成年人获取有益身心健康的信息。

第十四条　网络信息内容服务平台应当加强对本平台设置的广告位和在本平台展示的广告内容的审核巡查，对发布违法广告的，应当依法予以处理。

第十五条　网络信息内容服务平台应当制定并公开管理规则和平台公约，完善用户协议，明确用户相关权利义务，并依法依约履行相应管理职责。

网络信息内容服务平台应当建立用户账号信用管理制度，根据用户账号的信用情况提供相应服务。

第十六条　网络信息内容服务平台应当在显著位置设置便捷的投诉举报入口，公布投诉举报方式，及时受理处置公众投诉举报并反馈处理结果。

第十七条　网络信息内容服务平台应当编制网络信息内容生态治理工作年度报告，年度报告应当包括网络信息内容生态治理工作情况、网络信息内容生态治理负责人履职情况、社会评价情况等内容。

第四章　网络信息内容服务使用者

第十八条　网络信息内容服务使用者应当文明健康使用网络，按照法律法规的要求和用户协议约定，切实履行相应义务，在以发帖、回复、留言、弹幕等形式参与网络活动时，文明互动，理性表达，不得发布本规定第六条规定的信息，防范和抵制本规定第七条规定的信息。

第十九条　网络群组、论坛社区版块建立者和管理者应当履行群组、版块管理责任，依据法律法规、用户协议和平台公约等，规范群组、版块内信息发布等行为。

第二十条　鼓励网络信息内容服务使用者积极参与网络信息内容生态治理，通过投诉、举报等方式对网上违法和不良信息进行监督，共同维护良好网络生态。

第二十一条　网络信息内容服务使用者和网络信息内容生产者、网络信息内容服务平台不得利用网络和相关信息技术实施侮辱、诽谤、威胁、散布谣言以及侵犯他人隐私等违法行为，损害他人合法权益。

第二十二条　网络信息内容服务使用者和网络信息内容生产者、网络信息内容服务平台不得通过发布、删除信息以及其他干预信息呈现的手段侵害他人合法权益或者谋取非法利益。

第二十三条　网络信息内容服务使用者和网络信息内容生产者、网络信息内容服务平台不得利用深度学习、虚拟现实等新技术新应用从事法律、行政法规禁止的活动。

第二十四条　网络信息内容服务使用者和网络信息内容生产者、网络信息内容服务平台不得通过人工方式或者技术手段实施流量造

假、流量劫持以及虚假注册账号、非法交易账号、操纵用户账号等行为，破坏网络生态秩序。

第二十五条　网络信息内容服务使用者和网络信息内容生产者、网络信息内容服务平台不得利用党旗、党徽、国旗、国徽、国歌等代表党和国家形象的标识及内容，或者借国家重大活动、重大纪念日和国家机关及其工作人员名义等，违法违规开展网络商业营销活动。

第五章　网络行业组织

第二十六条　鼓励行业组织发挥服务指导和桥梁纽带作用，引导会员单位增强社会责任感，唱响主旋律，弘扬正能量，反对违法信息，防范和抵制不良信息。

第二十七条　鼓励行业组织建立完善行业自律机制，制定网络信息内容生态治理行业规范和自律公约，建立内容审核标准细则，指导会员单位建立健全服务规范、依法提供网络信息内容服务、接受社会监督。

第二十八条　鼓励行业组织开展网络信息内容生态治理教育培训和宣传引导工作，提升会员单位、从业人员治理能力，增强全社会共同参与网络信息内容生态治理意识。

第二十九条　鼓励行业组织推动行业信用评价体系建设，依据章程建立行业评议等评价奖惩机制，加大对会员单位的激励和惩戒力度，强化会员单位的守信意识。

第六章　监督管理

第三十条　各级网信部门会同有关主管部门，建立健全信息共

享、会商通报、联合执法、案件督办、信息公开等工作机制，协同开展网络信息内容生态治理工作。

第三十一条　各级网信部门对网络信息内容服务平台履行信息内容管理主体责任情况开展监督检查，对存在问题的平台开展专项督查。

网络信息内容服务平台对网信部门和有关主管部门依法实施的监督检查，应当予以配合。

第三十二条　各级网信部门建立网络信息内容服务平台违法违规行为台账管理制度，并依法依规进行相应处理。

第三十三条　各级网信部门建立政府、企业、社会、网民等主体共同参与的监督评价机制，定期对本行政区域内网络信息内容服务平台生态治理情况进行评估。

第七章　法律责任

第三十四条　网络信息内容生产者违反本规定第六条规定的，网络信息内容服务平台应当依法依约采取警示整改、限制功能、暂停更新、关闭账号等处置措施，及时消除违法信息内容，保存记录并向有关主管部门报告。

第三十五条　网络信息内容服务平台违反本规定第十条、第三十一条第二款规定的，由网信等有关主管部门依据职责，按照《中华人民共和国网络安全法》《互联网信息服务管理办法》等法律、行政法规的规定予以处理。

第三十六条　网络信息内容服务平台违反本规定第十一条第二

款规定的，由设区的市级以上网信部门依据职责进行约谈，给予警告，责令限期改正；拒不改正或者情节严重的，责令暂停信息更新，按照有关法律、行政法规的规定予以处理。

第三十七条　网络信息内容服务平台违反本规定第九条、第十二条、第十五条、第十六条、第十七条规定的，由设区的市级以上网信部门依据职责进行约谈，给予警告，责令限期改正；拒不改正或者情节严重的，责令暂停信息更新，按照有关法律、行政法规的规定予以处理。

第三十八条　违反本规定第十四条、第十八条、第十九条、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，由网信等有关主管部门依据职责，按照有关法律、行政法规的规定予以处理。

第三十九条　网信部门根据法律、行政法规和国家有关规定，会同有关主管部门建立健全网络信息内容服务严重失信联合惩戒机制，对严重违反本规定的网络信息内容服务平台、网络信息内容生产者和网络信息内容使用者依法依规实施限制从事网络信息服务、网上行为限制、行业禁入等惩戒措施。

第四十条　违反本规定，给他人造成损害的，依法承担民事责任；构成犯罪的，依法追究刑事责任；尚不构成犯罪的，由有关主管部门依照有关法律、行政法规的规定予以处罚。

第八章　附则

第四十一条　本规定所称网络信息内容生产者，是指制作、复制、

发布网络信息内容的组织或者个人。

本规定所称网络信息内容服务平台，是指提供网络信息内容传播服务的网络信息服务提供者。

本规定所称网络信息内容服务使用者，是指使用网络信息内容服务的组织或者个人。

第四十二条　本规定自2020年3月1日起施行。

App 违法违规收集使用个人信息行为认定方法

时效性：　　现行有效

发文机关：　国家互联网信息办公室秘书局,工业和信息化部办公厅,公安部办公厅,国家市场监督管理总局

文号：　　国信办秘字〔2019〕191 号

发文日期：　2019 年 11 月 28 日

施行日期：　2019 年 11 月 28 日

一、以下行为可被认定为“未公开收集使用规则”

1.在 App 中没有隐私政策，或者隐私政策中没有收集使用个人信息规则；

2.在 App 首次运行时未通过弹窗等明显方式提示用户阅读隐私政策等收集使用规则；

3.隐私政策等收集使用规则难以访问，如进入 App 主界面后，需多于 4 次点击等操作才能访问到；

4.隐私政策等收集使用规则难以阅读，如文字过小过密、颜色过淡、模糊不清，或未提供简体中文版等。

二、以下行为可被认定为“未明示收集使用个人信息的目的、方式和范围”

1.未逐一列出 App(包括委托的第三方或嵌入的第三方代码、插件)收集使用个人信息的目的、方式、范围等；

2.收集使用个人信息的目的、方式、范围发生变化时，未以适当方式通知用户，适当方式包括更新隐私政策等收集使用规则并提醒用

户阅读等；

3.在申请打开可收集个人信息的权限，或申请收集用户身份证号、银行账号、行踪轨迹等个人敏感信息时，未同步告知用户其目的，或者目的不明确、难以理解；

4.有关收集使用规则的内容晦涩难懂、冗长繁琐，用户难以理解，如使用大量专业术语等。

三、以下行为可被认定为“未经用户同意收集使用个人信息”

1.征得用户同意前就开始收集个人信息或打开可收集个人信息的权限；

2.用户明确表示不同意后，仍收集个人信息或打开可收集个人信息的权限，或频繁征求用户同意、干扰用户正常使用；

3.实际收集的个人信息或打开的可收集个人信息权限超出用户授权范围；

4.以默认选择同意隐私政策等非明示方式征求用户同意；

5.未经用户同意更改其设置的可收集个人信息权限状态，如 App 更新时自动将用户设置的权限恢复到默认状态；

6.利用用户个人信息和算法定向推送信息，未提供非定向推送信息的选项；

7.以欺诈、诱骗等不正当方式误导用户同意收集个人信息或打开可收集个人信息的权限，如故意欺瞒、掩饰收集使用个人信息的真实目的；

8.未向用户提供撤回同意收集个人信息的途径、方式；

9.违反其所声明的收集使用规则，收集使用个人信息。

四、以下行为可被认定为“违反必要原则，收集与其提供的服务无关的个人信息”

1.收集的个人信息类型或打开的可收集个人信息权限与现有业务功能无关；

2.因用户不同意收集非必要个人信息或打开非必要权限，拒绝提供业务功能；

3.App 新增业务功能申请收集的个人信息超出用户原有同意范围，若用户不同意，则拒绝提供原有业务功能，新增业务功能取代原有业务功能的除外；

4.收集个人信息的频度等超出业务功能实际需要；

5.仅以改善服务质量、提升用户体验、定向推送信息、研发新产品等为由，强制要求用户同意收集个人信息；

6.要求用户一次性同意打开多个可收集个人信息的权限，用户不同意则无法使用。

五、以下行为可被认定为“未经同意向他人提供个人信息”

1.既未经用户同意，也未做匿名化处理，App 客户端直接向第三方提供个人信息，包括通过客户端嵌入的第三方代码、插件等方式向第三方提供个人信息；

2.既未经用户同意，也未做匿名化处理，数据传输至 App 后台服务器后，向第三方提供其收集的个人信息；

3.App 接入第三方应用，未经用户同意，向第三方应用提供个人

信息。

六、以下行为可被认定为“未按法律规定提供删除或更正个人信息功能”或“未公布投诉、举报方式等信息”

1.未提供有效的更正、删除个人信息及注销用户账号功能；

2.为更正、删除个人信息或注销用户账号设置不必要或不合理条件；

3.虽提供了更正、删除个人信息及注销用户账号功能，但未及时响应用户相应操作，需人工处理的，未在承诺时限内（承诺时限不得超过15个工作日，无承诺时限的，以15个工作日为限）完成核查和处理；

4.更正、删除个人信息或注销用户账号等用户操作已执行完毕，但App后台并未完成的；

5.未建立并公布个人信息安全投诉、举报渠道，或未在承诺时限内（承诺时限不得超过15个工作日，无承诺时限的，以15个工作日为限）受理并处理的。

儿童个人信息网络保护规定

时效性：　　现行有效

发文机关：　国家互联网信息办公室

文号：　　国家互联网信息办公室令第 4 号

发文日期：　2019 年 08 月 22 日

施行日期：　2019 年 10 月 01 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。

互联网个人信息安全保护指南

时效性：　　现行有效

发布机关：　公安部网络安全保卫局、北京网络行业协会、公安部第三研究所联合发布

发布日期：　2019 年 4 月 10 日

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。

[GB/T 35273-2017，定义 3.3]

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。

[GB/T 35273-2017，定义 3.5]

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。

[GB/T 35273-2017，定义 3.9]

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，以及个人信息的范围、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用户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。

App 违法违规收集使用个人信息自评估指南

时效性：　　现行有效

发布机关：　App 专项治理工作组

发布日期：　2019 年 3 月

本指南主要用于 App 运营者对其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、即时通讯、社区社交、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 运营者基本情况进行描述，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。

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 应通过弹窗提示等显著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	当使用 Cookie 等同类技术（包括脚本、Clickstream、Web 信标、Flash Cookie、内

其同类技术收集个人信 息，是否向用户明示	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	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。

受的情形	

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。
27. 是否收集	App 不应收集与业务功能无任何关系的

与业务功能无关的个人信息	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 运营者对用户权利的保障

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运营者应妥善受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。

具有舆论属性或社会动员能力的互联网信息服务安全评估规定

时效性：　　现行有效

发布机关：　公安部

发文日期：　2018 年 11 月 15 日

施行日期：　2018 年 11 月 30 日

第一条　为加强对具有舆论属性或社会动员能力的互联网信息服务和相关新技术新应用的安全管理，规范互联网信息服务活动，维护国家安全、社会秩序和公共利益，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》《计算机信息网络国际联网安全保护管理办法》，制订本规定。

第二条　本规定所称具有舆论属性或社会动员能力的互联网信息服务，包括下列情形：

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

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

第三条　互联网信息服务提供者具有下列情形之一的，应当依照本规定自行开展安全评估，并对评估结果负责：

（一）具有舆论属性或社会动员能力的信息服务上线，或者信息服务增设相关功能的；

（二）使用新技术新应用，使信息服务的功能属性、技术实现方式、基础资源配置等发生重大变更，导致舆论属性或者社会动员能力

发生重大变化的；

（三）用户规模显著增加，导致信息服务的舆论属性或者社会动员能力发生重大变化的；

（四）发生违法有害信息传播扩散，表明已有安全措施难以有效防控网络安全风险的；

（五）地市级以上网信部门或者公安机关书面通知需要进行安全评估的其他情形。

第四条　互联网信息服务提供者可以自行实施安全评估，也可以委托第三方安全评估机构实施。

第五条　互联网信息服务提供者开展安全评估，应当对信息服务和新技术新应用的合法性，落实法律、行政法规、部门规章和标准规定的安全措施的有效性，防控安全风险的有效性等情况进行全面评估，并重点评估下列内容：

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

（二）用户真实身份核验以及注册信息留存措施；

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

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

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

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

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

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

第六条　互联网信息服务提供者在安全评估中发现存在安全隐患的，应当及时整改，直至消除相关安全隐患。

经过安全评估，符合法律、行政法规、部门规章和标准的，应当形成安全评估报告。安全评估报告应当包括下列内容：

（一）互联网信息服务的功能、服务范围、软硬件设施、部署位置等基本情况和相关证照获取情况；

（二）安全管理制度和技术措施落实情况及风险防控效果；

（三）安全评估结论；

（四）其他应当说明的相关情况。

第七条　互联网信息服务提供者应当将安全评估报告通过全国互联网安全管理服务平台提交所在地地市级以上网信部门和公安机关。

具有本规定第三条第一项、第二项情形的，互联网信息服务提供者应当在信息服务、新技术新应用上线或者功能增设前提交安全评估

报告；具有本规定第三条第三、四、五项情形的，应当自相关情形发生之日起30个工作日内提交安全评估报告。

第八条　地市级以上网信部门和公安机关应当依据各自职责对安全评估报告进行书面审查。

发现安全评估报告内容、项目缺失，或者安全评估方法明显不当的，应当责令互联网信息服务提供者限期重新评估。

发现安全评估报告内容不清的，可以责令互联网信息服务提供者补充说明。

第九条　网信部门和公安机关根据对安全评估报告的书面审查情况，认为有必要的，应当依据各自职责对互联网信息服务提供者开展现场检查。

网信部门和公安机关开展现场检查原则上应当联合实施，不得干扰互联网信息服务提供者正常的业务活动。

第十条　对存在较大安全风险、可能影响国家安全、社会秩序和公共利益的互联网信息服务，省级以上网信部门和公安机关应当组织专家进行评审，必要时可以会同属地相关部门开展现场检查。

第十一条　网信部门和公安机关开展现场检查，应当依照有关法律、行政法规、部门规章的规定进行。

第十二条　网信部门和公安机关应当建立监测管理制度，加强网络安全风险管理，督促互联网信息服务提供者依法履行网络安全义务。

发现具有舆论属性或社会动员能力的互联网信息服务提供者未

按本规定开展安全评估的，网信部门和公安机关应当通知其按本规定开展安全评估。

第十三条　网信部门和公安机关发现具有舆论属性或社会动员能力的互联网信息服务提供者拒不按照本规定开展安全评估的，应当通过全国互联网安全管理服务平台向公众提示该互联网信息服务存在安全风险，并依照各自职责对该互联网信息服务实施监督检查，发现存在违法行为的，应当依法处理。

第十四条　网信部门统筹协调具有舆论属性或社会动员能力的互联网信息服务安全评估工作,公安机关的安全评估工作情况定期通报网信部门。

第十五条　网信部门、公安机关及其工作人员对在履行职责中知悉的国家秘密、商业秘密和个人信息应当严格保密，不得泄露、出售或者非法向他人提供。

第十六条　对于互联网新闻信息服务新技术新应用的安全评估，依照《互联网新闻信息服务新技术新应用安全评估管理规定》执行。

第十七条　本规定自2018年11月30日起施行。

检察机关办理侵犯公民个人信息案件指引

时效性：　　现行有效

发文机关：　最高人民检察院

文号：　　高检发侦监字〔2018〕13号

发文日期：　2018年11月09日

施行日期：　2018年11月09日

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和对比资料等。

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，重点注意以下问题：

（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、免予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。

公安机关互联网安全监督检查规定

时效性：　　现行有效

发文机关：　公安部

文号：　　中华人民共和国公安部令第151号

发文日期：　2018年09月15日

施行日期：　2018年11月01日

第一章　总则

第一条　为规范公安机关互联网安全监督检查工作，预防网络违法犯罪，维护网络安全，保护公民、法人和其他组织合法权益，根据《中华人民共和国人民警察法》《中华人民共和国网络安全法》等有关法律、行政法规，制定本规定。

第二条　本规定适用于公安机关依法对互联网服务提供者和联网使用单位履行法律、行政法规规定的网络安全义务情况进行的安全监督检查。

第三条　互联网安全监督检查工作由县级以上地方人民政府公安机关网络安全保卫部门组织实施。

上级公安机关应当对下级公安机关开展互联网安全监督检查工作情况进行指导和监督。

第四条　公安机关开展互联网安全监督检查，应当遵循依法科学管理、保障和促进发展的方针，严格遵守法定权限和程序，不断改进执法方式，全面落实执法责任。

第五条　公安机关及其工作人员对履行互联网安全监督检查职

责中知悉的个人信息、隐私、商业秘密和国家秘密，应当严格保密，不得泄露、出售或者非法向他人提供。

公安机关及其工作人员在履行互联网安全监督检查职责中获取的信息，只能用于维护网络安全的需要，不得用于其他用途。

第六条　公安机关对互联网安全监督检查工作中发现的可能危害国家安全、公共安全、社会秩序的网络安全风险，应当及时通报有关主管部门和单位。

第七条　公安机关应当建立并落实互联网安全监督检查工作制度，自觉接受检查对象和人民群众的监督。

第二章　监督检查对象和内容

第八条　互联网安全监督检查由互联网服务提供者的网络服务运营机构和联网使用单位的网络管理机构所在地公安机关实施。互联网服务提供者为个人的，可以由其经常居住地公安机关实施。

第九条　公安机关应当根据网络安全防范需要和网络安全风险隐患的具体情况，对下列互联网服务提供者和联网使用单位开展监督检查：

（一）提供互联网接入、互联网数据中心、内容分发、域名服务的；

（二）提供互联网信息服务的；

（三）提供公共上网服务的；

（四）提供其他互联网服务的；

对开展前款规定的服务未满一年的，两年内曾发生过网络安全事

件、违法犯罪案件的，或者因未履行法定网络安全义务被公安机关予以行政处罚的，应当开展重点监督检查。

第十条　公安机关应当根据互联网服务提供者和联网使用单位履行法定网络安全义务的实际情况，依照国家有关规定和标准，对下列内容进行监督检查：

（一）是否办理联网单位备案手续，并报送接入单位和用户基本信息及其变更情况；

（二）是否制定并落实网络安全管理制度和操作规程，确定网络安全负责人；

（三）是否依法采取记录并留存用户注册信息和上网日志信息的技术措施；

（四）是否采取防范计算机病毒和网络攻击、网络侵入等技术措施；

（五）是否在公共信息服务中对法律、行政法规禁止发布或者传输的信息依法采取相关防范措施；

（六）是否按照法律规定的要求为公安机关依法维护国家安全、防范调查恐怖活动、侦查犯罪提供技术支持和协助；

（七）是否履行法律、行政法规规定的网络安全等级保护等义务。

第十一条　除本规定第十条所列内容外，公安机关还应当根据提供互联网服务的类型，对下列内容进行监督检查：

（一）对提供互联网接入服务的，监督检查是否记录并留存网络地址及分配使用情况；

（二）对提供互联网数据中心服务的，监督检查是否记录所提供的主机托管、主机租用和虚拟空间租用的用户信息；

（三）对提供互联网域名服务的，监督检查是否记录网络域名申请、变动信息，是否对违法域名依法采取处置措施；

（四）对提供互联网信息服务的，监督检查是否依法采取用户发布信息管理措施，是否对已发布或者传输的法律、行政法规禁止发布或者传输的信息依法采取处置措施，并保存相关记录；

（五）对提供互联网内容分发服务的，监督检查是否记录内容分发网络与内容源网络链接对应情况；

（六）对提供互联网公共上网服务的，监督检查是否采取符合国家标准的网络与信息安全保护技术措施。

第十二条　在国家重大网络安全保卫任务期间，对与国家重大网络安全保卫任务相关的互联网服务提供者和联网使用单位，公安机关可以对下列内容开展专项安全监督检查：

（一）是否制定重大网络安全保卫任务所要求的工作方案、明确网络安全责任分工并确定网络安全管理人员；

（二）是否组织开展网络安全风险评估，并采取相应风险管控措施堵塞网络安全漏洞隐患；

（三）是否制定网络安全应急处置预案并组织开展应急演练，应急处置相关设施是否完备有效；

（四）是否依法采取重大网络安全保卫任务所需要的其他网络安全防范措施；

（五）是否按照要求向公安机关报告网络安全防范措施及落实情况。

对防范恐怖袭击的重点目标的互联网安全监督检查，按照前款规定的内容执行。

第三章　监督检查程序

第十三条　公安机关开展互联网安全监督检查，可以采取现场监督检查或者远程检测的方式进行。

第十四条　公安机关开展互联网安全现场监督检查时，人民警察不得少于二人，并应当出示人民警察证和县级以上地方人民政府公安机关出具的监督检查通知书。

第十五条　公安机关开展互联网安全现场监督检查可以根据需要采取以下措施：

（一）进入营业场所、机房、工作场所；

（二）要求监督检查对象的负责人或者网络安全管理人员对监督检查事项作出说明；

（三）查阅、复制与互联网安全监督检查事项相关的信息；

（四）查看网络与信息安全保护技术措施运行情况。

第十六条　公安机关对互联网服务提供者和联网使用单位是否存在网络安全漏洞，可以开展远程检测。

公安机关开展远程检测，应当事先告知监督检查对象检查时间、检查范围等事项或者公开相关检查事项，不得干扰、破坏监督检查对象网络的正常运行。

第十七条　公安机关开展现场监督检查或者远程检测，可以委托具有相应技术能力的网络安全服务机构提供技术支持。

网络安全服务机构及其工作人员对工作中知悉的个人信息、隐私、商业秘密和国家秘密，应当严格保密，不得泄露、出售或者非法向他人提供。公安机关应当严格监督网络安全服务机构落实网络安全管理与保密责任。

第十八条　公安机关开展现场监督检查，应当制作监督检查记录，并由开展监督检查的人民警察和监督检查对象的负责人或者网络安全管理人员签名。监督检查对象负责人或者网络安全管理人员对监督检查记录有异议的，应当允许其作出说明；拒绝签名的，人民警察应当在监督检查记录中注明。

公安机关开展远程检测，应当制作监督检查记录，并由二名以上开展监督检查的人民警察在监督检查记录上签名。

委托网络安全服务机构提供技术支持的，技术支持人员应当一并在监督检查记录上签名。

第十九条　公安机关在互联网安全监督检查中，发现互联网服务提供者和联网使用单位存在网络安全风险隐患，应当督促指导其采取措施消除风险隐患，并在监督检查记录上注明；发现有违法行为，但情节轻微或者未造成后果的，应当责令其限期整改。

监督检查对象在整改期限届满前认为已经整改完毕的，可以向公安机关书面提出提前复查申请。

公安机关应当自整改期限届满或者收到监督检查对象提前复查

申请之日起三个工作日内，对整改情况进行复查，并在复查结束后三个工作日内反馈复查结果。

第二十条　监督检查过程中收集的资料、制作的各类文书等材料，应当按照规定立卷存档。

第四章　法律责任

第二十一条　公安机关在互联网安全监督检查中，发现互联网服务提供者和联网使用单位有下列违法行为的，依法予以行政处罚：

（一）未制定并落实网络安全管理制度和操作规程，未确定网络安全负责人的，依照《中华人民共和国网络安全法》第

五十九条第一款的规定予以处罚；

（二）未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的，依照《中华人民共和国网络安全法》第

五十九条第一款的规定予以处罚；

（三）未采取记录并留存用户注册信息和上网日志信息措施的，依照《中华人民共和国网络安全法》第五十九条第一款的规定予以处罚；

（四）在提供互联网信息发布、即时通讯等服务中，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，依照《中华人民共和国网络安全法》第六十一条的规定予以处罚；

（五）在公共信息服务中对法律、行政法规禁止发布或者传输的信息未依法或者不按照公安机关的要求采取停止传输、消除等处置措施、保存有关记录的，依照《中华人民共和国网络安全法》第六十八

条或者第六十九条第一项的规定予以处罚；

（六）拒不为公安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的，依照《中华人民共和国网络安全法》第六十九条第三项的规定予以处罚。有前款第四至六项行为违反《中华人民共和国反恐怖主义法》规定的，依照《中华人民共和国反恐怖主义法》第八十四条或者第八十六条第一款的规定予以处罚。

第二十二条　公安机关在互联网安全监督检查中，发现互联网服务提供者和联网使用单位，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，依照《中华人民共和国网络安全法》第六十四条第二款的规定予以处罚。

第二十三条　公安机关在互联网安全监督检查中，发现互联网服务提供者和联网使用单位在提供的互联网服务中设置恶意程序的，依照《中华人民共和国网络安全法》第六十条第一项的规定予以处罚。

第二十四条　互联网服务提供者和联网使用单位拒绝、阻碍公安机关实施互联网安全监督检查的，依照《中华人民共和国网络安全法》第六十九条第二项的规定予以处罚；拒不配合反恐怖主义工作的，依照《中华人民共和国反恐怖主义法》第九十一条或者第九十二条的规定予以处罚。

第二十五条　受公安机关委托提供技术支持的网络安全服务机构及其工作人员，从事非法侵入监督检查对象网络、干扰监督检查对象网络正常功能、窃取网络数据等危害网络安全的活动的，依照《中华人民共和国网络安全法》第六十三条的规定予以处罚；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在工作中获悉的个人信息的，依照《中华人民共和国网络安全法》第六十四条第二款的规定予以处罚，构成犯罪的，依法追究刑事责任。

前款规定的机构及人员侵犯监督检查对象的商业秘密，构成犯罪的，依法追究刑事责任。

第二十六条　公安机关及其工作人员在互联网安全监督检查工作中，玩忽职守、滥用职权、徇私舞弊的，对直接负责的主管人员和其他直接责任人员依法予以处分；构成犯罪的，依法追究刑事责任。

第二十七条　互联网服务提供者和联网使用单位违反本规定，构成违反治安管理行为的，依法予以治安管理处罚；构成犯罪的，依法追究刑事责任。

第五章　附则

第二十八条　对互联网上网服务营业场所的监督检查，按照《互联网上网服务营业场所管理条例》的有关规定执行。

第二十九条　本规定自2018年11月1日起施行。

银行业金融机构数据治理指引

时效性：　　现行有效

发文机关：　中国银行保险监督管理委员会

文号：　　银保监发〔2018〕22号

发文日期：　2018年05月21日

施行日期：　2018年05月21日

第一章　总则

第一条　为指导银行业金融机构加强数据治理，提高数据质量，发挥数据价值，提升经营管理能力，根据《中华人民共和国银行业监督管理法》等法律法规，制定本指引。

第二条　本指引适用于中华人民共和国境内经银行业监督管理机构批准设立的银行业金融机构。

本指引所称银行业金融机构，是指在中华人民共和国境内设立的商业银行、农村信用合作社等吸收公众存款的金融机构、政策性银行以及国家开发银行。

第三条　数据治理是指银行业金融机构通过建立组织架构，明确董事会、监事会、高级管理层及内设部门等职责要求，制定和实施系统化的制度、流程和方法，确保数据统一管理、高效运行，并在经营管理中充分发挥价值的动态过程。

第四条　银行业金融机构应当将数据治理纳入公司治理范畴，建立自上而下、协调一致的数据治理体系。

第五条　银行业金融机构数据治理应当遵循以下基本原则：

（一）全覆盖原则。数据治理应当覆盖数据的全生命周期，覆盖业务经营、风险管理和内部控制流程中的全部数据，覆盖内部数据和外部数据，覆盖监管数据，覆盖所有分支机构和附属机构。

（二）匹配性原则。数据治理应当与管理模式、业务规模、风险状况等相适应，并根据情况变化进行调整。

（三）持续性原则。数据治理应当持续开展，建立长效机制。

（四）有效性原则。数据治理应当推动数据真实准确客观反映银行业金融机构实际情况，并有效应用于经营管理。

第六条　银行业金融机构应当将监管数据纳入数据治理，建立工作机制和流程，确保监管数据报送工作有效组织开展，监管数据质量持续提升。

法定代表人或主要负责人对监管数据质量承担最终责任。

第七条　银行业监督管理机构依据本指引对银行业金融机构数据治理情况实施监管。

第二章　数据治理架构

第八条　银行业金融机构应当建立组织架构健全、职责边界清晰的数据治理架构，明确董事会、监事会、高级管理层和相关部门的职责分工，建立多层次、相互衔接的运行机制。

第九条　银行业金融机构董事会应当制定数据战略，审批或授权审批与数据治理相关的重大事项，督促高级管理层提升数据治理有效性，对数据治理承担最终责任。

第十条　银行业金融机构监事会负责对董事会和高级管理层在

数据治理方面的履职尽责情况进行监督评价。

第十一条　银行业金融机构高级管理层负责建立数据治理体系，确保数据治理资源配置，制定和实施问责和激励机制，建立数据质量控制机制，组织评估数据治理的有效性和执行情况，并定期向董事会报告。

银行业金融机构可根据实际情况设立首席数据官。首席数据官是否纳入高级管理人员由银行业金融机构根据经营状况确定；纳入高级管理人员管理的，应当符合相关行政许可事项的要求。

第十二条　银行业金融机构应当确定并授权归口管理部门牵头负责实施数据治理体系建设，协调落实数据管理运行机制，组织推动数据在经营管理流程中发挥作用，负责监管数据相关工作，设置监管数据相关工作专职岗位。

第十三条　业务部门应当负责本业务领域的数据治理，管理业务条线数据源，确保准确记录和及时维护，落实数据质量控制机制，执行监管数据相关工作要求，加强数据应用，实现数据价值。

第十四条　银行业金融机构应当在数据治理归口管理部门设立满足工作需要的专职岗位，在其他相关业务部门设置专职或兼职岗位。

第十五条　银行业金融机构应当建立一支满足数据治理工作需要的专业队伍，至少按年度对人员进行系统培训，科学规划职业成长通道，确定合理薪酬水平。

第十六条　银行业金融机构应当建立良好的数据文化，树立数据是重要资产和数据应真实客观的理念与准则，强化用数意识，遵循依

规用数、科学用数的职业操守。

第三章　数据管理

第十七条　银行业金融机构应当结合自身发展战略、监管要求等，制定数据战略并确保有效执行和修订。

第十八条　银行业金融机构应当制定全面科学有效的数据管理制度，包括但不限于组织管理、部门职责、协调机制、安全管控、系统保障、监督检查和数据质量控制等方面。

银行业金融机构应当根据监管要求和实际需要，持续评价更新数据管理制度。

第十九条　银行业金融机构应当制定与监管数据相关的监管统计管理制度和业务制度，及时发布并定期评价和更新，报银行业监督管理机构备案。制度出现重大变化的，应当及时向银行业监督管理机构报告。

第二十条　银行业金融机构应当建立覆盖全部数据的标准化规划，遵循统一的业务规范和技术标准。数据标准应当符合国家标准化政策及监管规定，并确保被有效执行。

第二十一条　银行业金融机构应当持续完善信息系统，覆盖各项业务和管理数据。信息系统应当有完备的数据字典和维护流程，并具有可拓展性。

第二十二条　银行业金融机构应当建立适应监管数据报送工作需要的信息系统，实现流程控制的程序化，提高监管数据加工的自动化程度。

第二十三条　银行业金融机构应当加强数据采集的统一管理，明确系统间数据交换流程和标准，实现各类数据有效共享。

第二十四条　银行业金融机构应当建立数据安全策略与标准，依法合规采集、应用数据，依法保护客户隐私，划分数据安全等级，明确访问和拷贝等权限，监控访问和拷贝等行为，完善数据安全技术，定期审计数据安全。

银行业金融机构采集、应用数据涉及到个人信息的，应遵循国家个人信息保护法律法规要求，符合与个人信息安全相关的国家标准。

第二十五条　银行业金融机构应当加强数据资料统一管理，建立全面严密的管理流程、归档制度，明确存档交接、口径梳理等要求，保证数据可比性。

第二十六条　银行业金融机构应当建立数据应急预案，根据业务影响分析，组织开展应急演练，完善处置流程，保证在系统服务异常以及危机等情景下数据的完整、准确和连续。

第二十七条　银行业金融机构应当建立数据治理自我评估机制，明确评估周期、流程、结果应用、组织保障等要素的相关要求。

评估内容应覆盖数据治理架构、数据管理、数据安全、数据质量和数据价值实现等方面，并按年度向银行业监督管理机构报送。

第二十八条　银行业金融机构应当建立问责机制，定期排查数据管理、数据质量控制、数据价值实现等方面问题，依据有关规定对高级管理层和相关部门及责任人进行问责。

银行业金融机构应结合实际情况，建立激励机制，保障数据治理

工作有效推进。

第四章　数据质量控制

第二十九条　银行业金融机构应当确立数据质量管理目标，建立控制机制，确保数据的真实性、准确性、连续性、完整性和及时性。

第三十条　银行业金融机构各项业务制度应当充分考虑数据质量管理需要，涉及指标含义清晰明确，取数规则统一，并根据业务变化及时更新。

第三十一条　银行业金融机构应当加强数据源头管理，确保将业务信息全面准确及时录入信息系统。信息系统应当能自动提示异常变动及错误情况。

第三十二条　银行业金融机构应当建立数据质量监控体系，覆盖数据全生命周期，对数据质量持续监测、分析、反馈和纠正。

第三十三条　银行业金融机构应当建立数据质量现场检查制度，定期组织实施，原则上不低于每年一次，对重大问题要按照既定的报告路径提交，并按流程实施整改。

第三十四条　银行业金融机构应当建立数据质量考核评价体系，考核结果纳入本机构绩效考核体系，实现数据质量持续提升。

第三十五条　银行业金融机构应当建立数据质量整改机制，对日常监控、检查和考核评价过程中发现的问题，及时组织整改，并对整改情况跟踪评价，确保整改落实到位。

第三十六条　银行业金融机构应当按照监管要求报送法人和集团的相关数据，保证同一监管指标在监管报送与对外披露之间的一致

性。如有重大差异，应当及时向银行业监督管理机构解释说明。

第三十七条　银行业金融机构应当建立监管数据质量管控制度，包括但不限于：关键监管指标数据质量承诺、数据异常变动分析和报告、重大差错通报以及问责等。

第五章　数据价值实现

第三十八条　银行业金融机构应当在风险管理、业务经营与内部控制中加强数据应用，实现数据驱动，提高管理精细化程度，发挥数据价值。

第三十九条　银行业金融机构应当充分运用数据分析，合理制定风险管理策略、风险偏好、风险限额以及风险管理政策和程序，监控执行情况并适时优化调整，提升风险管理体系的有效性。

全球系统重要性银行应遵循更高的标准，对照有效风险数据加总与风险报告评估要点的相关要求，强化风险管理。

第四十条　银行业金融机构应当加强数据应用，持续改善风险管理方法，有效识别、计量、评估、监测、报告和控制各类风险。

第四十一条　银行业金融机构应当提高数据加总能力，明确数据加总范围、方法、流程和加总结果要求等，满足在正常经营、压力情景以及危机状况下风险管理的数据需要。

加总内容包括但不限于交易对手、产品、地域、行业、客户以及其他相关的分类。加总技术应当主要采取自动化方式。

第四十二条　银行业金融机构应当加强数据分析应用能力，提高风险报告质量，明确风险报告数据准确性保障措施，覆盖重要风险领

域和新风险，提供风险处置的决策与建议以及未来风险发展趋势。

第四十三条　银行业金融机构应当加强数据积累，优化风险计量，持续完善风险定价模型，优化风险定价体系。

第四十四条　银行业金融机构应当充分评估兼并收购、资产剥离等业务对自身数据治理能力的影响。有重大影响的，应当明确整改计划和时间表，满足银行集团风险管理要求。

第四十五条　银行业金融机构应当明确新产品新服务的数据管理相关要求，确保清晰评估成本、风险和收益，并作为准入标准。

第四十六条　银行业金融机构应当通过数据分析挖掘，准确理解客户需求，提供精准产品服务，提升客户服务质量和服务水平。

第四十七条　银行业金融机构应当通过量化分析业务流程，减少管理冗余，提高经营效率，降低经营成本。

第四十八条　银行业金融机构应当充分运用大数据技术，实现业务创新、产品创新和服务创新。

第四十九条　银行业金融机构应当按照可量化导向，完善内部控制评价制度和内部控制评价质量控制机制，前瞻性识别内部控制流程的缺陷，评估影响程度并及时处理，持续提升内部控制的有效性。

第六章　监督管理

第五十条　银行业监督管理机构应当通过非现场监管和现场检查对银行业金融机构数据治理情况进行持续监管。

第五十一条　银行业监督管理机构可根据需要，要求银行业金融机构通过内部审计机构或委托外部审计机构对其数据治理情况进行审

计，并及时报送审计报告。

第五十二条　对数据治理不满足《中华人民共和国银行业监督管理法》等法律法规及国务院银行业监督管理机构审慎经营规则要求的银行业金融机构，银行业监督管理机构可采取相应措施：

（一）要求其制定整改方案，责令限期改正；

（二）与公司治理评价结果或监管评级挂钩；

（三）依法采取监管措施及实施行政处罚。

第七章　附则

第五十三条　外国银行分行以及银行业监督管理机构负责监管的其他金融机构参照执行本指引。

第五十四条　本指引由国务院银行业监督管理机构负责解释。

第五十五条　本指引自印发之日起施行。《银行监管统计数据质量管理良好标准（试行）》（银监发〔2011〕63号）同时废止。

科学数据管理办法

时效性：　　现行有效

发文机关：　国务院办公厅

文号：　　国办发〔2018〕17号

发文日期：　2018年03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：

（一）组织研究制定国家科学数据管理政策和标准规范；

（二）协调推动科学数据规范管理、开放共享及评价考核工作；

（三）统筹推进国家科学数据中心建设和发展；

（四）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：

（一）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；

（二）指导所属法人单位加强和规范科学数据管理；

（三）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；

（四）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；

（五）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：

（一）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；

（二）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；

（三）按照有关规定做好科学数据保密和安全管理工作；

（四）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；

（五）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：

（一）承担相关领域科学数据的整合汇交工作；

（二）负责科学数据的分级分类、加工整理和分析挖掘；

（三）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、国家安全和社会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；加强数据下载的认证、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。

促进和规范健康医疗大数据应用发展的指导意见

时效性：　　现行有效

发文机关：　国务院办公厅

文号：　　国办发〔2016〕47号

发文日期：　2016年06月21日

施行日期：　2016年06月21日

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，建立数据安全管理责任制度，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。

促进大数据发展行动纲要

时效性：　　现行有效

发文机关：　国务院

文号：　　国发〔2015〕50号

发文日期：　2015年08月31日

施行日期：　2015年08月31日

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、万众创新的创新驱动新格局。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。

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。

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。

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事业单位将市场监管、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、交通旅游、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服务大数据应用体系。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关键技术攻关、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。

贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见

时效性：　　现行有效

发文机关：　国务院

文号：　　国发〔2015〕50号

发文日期：　2015年08月31日

施行日期：　2015年08月31日

一、　指导思想、基本原则和工作目标

（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，按照党中央、国务院决策部署，以总体国家安全观为统领，认真贯彻实施网络强国战略，全面加强网络安全工作统筹规划，以贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度为基础，以保护关键信息基础设施、重要网络和数据安全为重点，全面加强网络安全防范管理、监测预警、应急处置、侦查打击、情报信息等各项工作，及时监测、处置网络安全风险、威胁和网络安全突发事件，保护关键信息基础设施、重要网络和数据免受攻击、侵入、干扰和破坏，依法惩治网络违法犯罪活动，切实提高网络安全保护能力，积极构建国家网络安全综合防控体系，切实维护国家网络空间主权、国家安全和社会公共利益，保护人民群众的合法权益，保障和促进经济社会信息化健康发展。

（二）基本原则

坚持分等级保护、突出重点。根据网络（包含网络设施、信息系

统、数据资源等）在国家安全、经济建设、社会生活中的重要程度，以及其遭到破坏后的危害程度等因素，科学确定网络的安全保护等级，实施分等级保护、分等级监管，重点保障关键信息基础设施和第三级（含第三级、下同）以上网络的安全。

坚持积极防御、综合防护。按照法律法规和有关国家标准规范，充分利用人工智能、大数据分析等技术，积极落实网络安全管理和技术防范措施，强化网络安全监测、态势感知、通报预警和应急处置等重点工作，综合采取网络安全保护、保卫、保障措施，防范和遏制重大网络安全风险、事件发生，保护云计算、物联网、新型互联网、大数据、智能制造等新技术应用和新业态安全。

坚持依法保护、形成合力。依据《网络安全法》等法律法规规定，公安机关依法履行网络安全保卫和监督管理职责，网络安全行业主管部门（含监管部门，下同）依法履行网络安全主管、监管责任，强化和落实网络运营者主体防护责任，充分发挥和调动社会各方力量，协调配合、群策群力，形成网络安全保护工作合力。

（三）工作目标

网络安全等级保护制度深入贯彻实施。网络安全等级保护定级备案、等级测评、安全建设和检查等基础工作深入推进。网络安全保护“实战化、体系化、常态化”和“动态防御、主动防御、纵深防御、精准防护、整体防控、联防联控”的“三化六防”措施得到有效落实，网络安全保护良好生态基本建立，国家网络安全综合防护能力和水平显著提升。

关键信息基础设施安全保护制度建立实施。关键信息基础设施底

数清晰，安全保护机构健全、职责明确、保障有力。在贯彻落实网络安全等级保护制度的基础上，关键信息基础设施涉及的关键岗位人员管理、供应链安全、数据安全、应急处置等重点安全保护措施得到有效落实，关键信息基础设施安全防护能力明显增强。

网络安全监测预警和应急处置能力显著提升。跨行业、跨部门、跨地区的立体化网络安全监测体系和网络安全保护平台基本建成，网络安全态势感知、通报预警和事件发现处置能力明显提高。网络安全预案科学齐备，应急处置机制完善，应急演练常态化开展，网络安全重大事件得到有效防范、遏制和处置。

网络安全综合防控体系基本形成。网络安全保护工作机制健全完善，党委统筹领导、各部门分工负责、社会力量多方参与的网络安全工作格局进一步完善。网络安全责任制得到有效落实，网络安全管理防范、监督指导和侦查打击等能力显著提升，“打防管控”一体化的网络安全综合防控体系基本形成。

二、 深入贯彻实施国家网络安全等级保护制度

按照国家网络安全等级保护制度要求，各单位、各部门在公安机关指导监督下，认真组织、深入开展网络安全等级保护工作，建立良好的网络安全保护生态，切实履行主体责任，全面提升网络安全保护能力。

（一）深化网络定级备案工作。网络运营者应全面梳理本单位各类网络，特别是云计算、物联网、新型互联网、大数据、智能制造等新技术应用的基本情况，并根据网络的功能、服务范围、服务对象和

处理数据等情况，科学确定网络的安全保护等级，对第二级以上网络依法向公安机关备案，并向行业主管部门报备。对新建网络，应在规划设计阶段确定安全保护等级。公安机关对网络运营者提交的备案材料和网络的安全保护等级进行审核，对定级结果合理、备案材料符合要求的，及时出具网络安全等级保护备案证明。行业主管部门可以依据《网络安全等级保护定级指南》国家标准，结合行业特点制定行业网络安全等级保护定级指导意见。

（二）定期开展网络安全等级测评。网络运营者应依据有关标准规范，对已定级备案网络的安全性进行检测评估，查找可能存在的网络安全问题和隐患。第三级以上网络运营者应委托符合国家有关规定的等级测评机构，每年开展一次网络安全等级测评，并及时将等级测评报告提交受理备案的公安机关和行业主管部门。新建第三级以上网络应在通过等级测评后投入运行。网络运营者在开展测评服务过程中要与测评机构签署安全保密协议，并对测评过程进行监督管理。公安机关要加强对本地等级测评机构的监督管理，建立测评人员背景审查和人员审核制度，确保等级测评过程客观、公正、安全。

（三）科学开展安全建设整改。网络运营者应在网络建设和运营过程中，同步规划、同步建设、同步使用有关网络安全保护措施。应依据《网络安全等级保护基本要求》《网络安全等级保护安全设计技术要求》等国家标准，在现有安全保护措施的基础上，全面梳理分析安全保护需求，并结合等级测评过程中发现的问题隐患，按照“一个中心（安全管理中心）、三重防护（安全通信网络、安全区域边界、安

全计算环境）”的要求，认真开展网络安全建设和整改加固，全面落实安全保护技术措施。网络运营者可将网络迁移上云，或将网络安全服务外包，充分利用云服务商和网络安全服务商提升网络安全保护能力和水平。应全面加强网络安全管理，建立完善人员管理、教育培训、系统安全建设和运维等管理制度，加强机房、设备和介质安全管理，强化重要数据和个人信息保护，制定操作规范和工作流程，加强日常监督和考核，确保各项管理措施有效落实。

（四）强化安全责任落实。行业主管部门、网络运营者应依据《网络安全法》等法律法规和有关政策要求，按照“谁主管谁负责、谁运营谁负责”的原则，厘清网络安全保护边界，明确安全保护工作责任，建立网络安全等级保护工作责任制，落实责任追究制度，作到“守土有责、守土尽责”。网络运营者要定期组织专门力量开展网络安全自查和检测评估，行业主管部门要组织风险评估，及时发现网络安全隐患和薄弱环节并予以整改，不断提高网络安全保护能力和水平。

（五）加强供应链安全管理。网络运营者应加强网络关键人员的安全管理，第三级以上网络运营者应对为其提供设计、建设、运维、技术服务的机构和人员加强管理，评估服务过程中可能存在的安全风险，并采取相应的管控措施。网络运营者应加强网络运维管理，因业务需要确需通过互联网远程运维的，应进行评估论证，并采取相应的管控措施。网络运营者应采购、使用符合国家法律法规和有关标准规范要求的网络产品及服务，第三级以上网络运营者应积极应用安全可信的网络产品及服务。

（六）落实密码安全防护要求。网络运营者应贯彻落实《密码法》等有关法律法规规定和密码应用相关标准规范。第三级以上网络应正确、有效采用密码技术进行保护，并使用符合相关要求的密码产品和服务。第三级以上网络运营者应在网络规划、建设和运行阶段，按照密码应用安全性评估管理办法和相关标准，在网络安全等级测评中同步开展密码应用安全性评估。

三、　建立并实施关键信息基础设施安全保护制度

公安机关指导监督关键信息基础设施安全保护工作。各单位、各部门应加强关键信息基础设施安全的法律体系、政策体系、标准体系、保护体系、保卫体系和保障体系建设，建立并实施关键信息基础设施安全保护制度，在落实网络安全等级保护制度基础上，突出保护重点，强化保护措施，切实维护关键信息基础设施安全。

（一）组织认定关键信息基础设施。根据党中央和公安部有关规定，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主管、监管部门（以下统称保护工作部门）应制定本行业、本领域关键信息基础设施认定规则并报公安部备案。保护工作部门根据认定规则负责组织认定本行业、本领域关键信息基础设施，及时将认定结果通知相关设施运营者并报公安部。应将符合认定条件的基础网络、大型专网、核心业务系统、云平台、大数据平台、物联网、工业控制系统、智能制造系统、新型互联网、新兴通讯设施等重点保护对象纳入关键信息基础设施。关键信息基础设施清单实行动态调整机制，有关网络设施、信息系统发生

较大变化，可能影响其认定结果的，运营者应及时将相关情况报告保护工作部门，保护工作部门应组织重新认定，将认定结果通知运营者，并报公安部。

（二）明确关键信息基础设施安全保护工作职能分工。公安部负责关键信息基础设施安全保护工作的顶层设计和规划部署，会同相关部门健全完善关键信息基础设施安全保护制度体系。保护工作部门负责对本行业、本领域关键信息基础设施安全保护工作的组织领导，根据国家网络安全法律法规和有关标准规范要求，制定并实施本行业、本领域关键信息基础设施安全总体规划和安全防护策略，落实本行业、本领域网络安全指导监督责任。关键信息基础设施运营者负责设置专门安全管理机构，组织开展关键信息基础设施安全保护工作，主要负责人对本单位关键信息基础设施安全保护负总责。

（三）落实关键信息基础设施重点防护措施。关键信息基础设施运营者应依据网络安全等级保护标准开展安全建设并进行等级测评，发现问题和风险隐患要及时整改；依据关键信息基础设施安全保护标准，加强安全保护和保障，并进行安全检测评估。要梳理网络资产，建立资产档案，强化核心岗位人员管理、整体防护、监测预警、应急处置、数据保护等重点保护措施，合理分区分域，收敛互联网暴露面，加强网络攻击威胁管控，强化纵深防御，积极利用新技术开展网络安全保护，构建以密码技术、可信计算、人工智能、大数据分析等为核心的网络安全保护体系，不断提升关键信息基础设施内生安全、主动免疫和主动防御能力。有条件的运营者应组建自己的安全服务机构，

承担关键信息基础设施安全保护任务，也可通过迁移上云或购买安全服务等方式，提高网络安全专业化、集约化保障能力。

（四）加强重要数据和个人信息保护。运营者应建立并落实重要数据和个人信息安全保护制度，对关键信息基础设施中的重要网络和数据库进行容灾备份，采取身份鉴别、访问控制、密码保护、安全审计、安全隔离、可信验证等关键技术措施，切实保护重要数据全生命周期安全。运营者在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，应当遵守有关规定并进行安全评估。

（五）强化核心岗位人员和产品服务的安全管理。要对专门安全管理机构的负责人和关键岗位人员进行安全背景审查，加强管理。要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，采购安全可信的网络产品和服务，确保供应链安全。当采购产品和服务可能影响国家安全的，应按照国家有关规定通过安全审查。公安机关加强对关键信息基础设施安全服务机构的安全管理，为运营者开展安全保护工作提供支持。

四、　加强网络安全保护工作协作配合

行业主管部门、网络运营者与公安机关要密切协同，大力开展安全监测、通报预警、应急处置、威胁情报等工作，落实常态化措施，提升应对、处置网络安全突发事件和重大风险防控能力。

（一）加强网络安全立体化监测体系建设。各单位、各部门要全面加强网络安全监测，对关键信息基础设施、重要网络等开展实时监

测，发现网络攻击和安全威胁，立即报告公安机关和有关部门并采取有效措施处置。要加强网络新技术研究和应用，研究绘制网络空间地理信息图谱（网络地图），实现挂图作战。行业主管部门、网络运营要建设本行业、本单位的网络安全保护业务平台，建设平台智慧大脑，依托平台和大数据开展实时监测、通报预警、应急处置、安全防护、指挥调度等工作，并与公安机关有关安全保卫平台对接，形成条块结合、纵横联通、协同联动的综合防控大格局。重点行业、网络运营者和公安机关要建设网络安全监控指挥中心，落实 7×24 小时值班值守制度，建立常态化、实战化的网络安全工作机制。

（二）加强网络安全信息共享和通报预警。行业主管部门、网络运营者要依托国家网络与信息安全信息通报机制，加强本行业、本领域网络安全信息通报预警力量建设，及时收集、汇总、分析各方网络安全信息，加强威胁情报工作，组织开展网络安全威胁分析和态势研判，及时通报预警和处置。第三级以上网络运营者和关键信息基础设施运营者要开展网络安全监测预警和信息通报工作，及时接收、处置来自国家、行业和地方网络安全预警通报信息，按规定向行业主管部门、备案公安机关报送网络安全监测预警信息和网络安全事件。公安机关要加强网络与信息安全信息通报预警机制建设和力量建设，不断提高网络安全通报预警能力。

（三）加强网络安全应急处置机制建设。行业主管部门、网络运营者要按照国家有关要求制定网络安全应急预案，加强网络安全应急力量建设和应急资源储备，与公安机关密切配合，建立网络安全事件

报告制度和应急处置机制。关键信息基础设施运营者和第三级以上网络运营者应定期开展应急演练，有效处置网络安全事件，并针对应急演练中发现的突出问题和漏洞隐患，及时整改加固，完善保护措施。行业主管部门、网络运营者应配合公安机关每年组织开展的网络安全监督检查、比武演习等工作，不断提升安全保护能力和对抗能力。

（四）加强网络安全事件处置和案件侦办。关键信息基础设施、第三级以上网络发生重大网络安全威胁和事件时，行业主管部门、网络运营者和公安机关应联合开展处置。电信业务经营者、网络服务提供者应提供支持及协助。网络运营者应配合公安机关打击网络违法犯罪行为；发现违法犯罪线索、重大网络安全威胁和事件时，应及时报告公安机关和有关部门并提供必要协助。

（五）加强网络安全问题隐患整改督办。公安机关建立挂牌督办制度，针对网络运营者网络安全工作不力、重大安全问题隐患久拖不改，或存在较大网络安全风险、发生重大网络安全案事件的，按照规定的权限和程序，会同行业主管部门对相关负责人进行约谈，挂牌督办，并加大监督检查和行政执法力度，依法依规进行行政处罚。网络运营者应按照有关要求采取措施，及时进行整改，消除重大风险隐患。发生重大网络安全案事件的，行业主管部门应组织全行业开展整改整顿。

五、 加强网络安全工作各项保障

（一）加强组织领导。各单位、各部门要高度重视网络安全等级保护和关键信息基础设施安全保护工作，将其列入重要议事日程，加

强统筹领导和规划设计，认真研究解决网络安全机构设置、人员配备、经费投入、安全保护措施建设等重大问题。行业主管部门和网络运营者要明确本单位主要负责人是网络安全的第一责任人，并确定一名领导班子成员分管网络安全工作，成立网络安全专门机构，明确任务分工，一级抓一级，层层抓落实。

（二）加强经费政策保障。各单位、各部门要通过现有经费渠道，保障关键信息基础设施、第三级以上网络等开展等级测评、风险评估、密码应用安全性检测、演练竞赛、安全建设整改、安全保护平台建设、密码保障系统建设、运行维护、监督检查、教育培训等经费投入。关键信息基础设施运营者应保障足额的网络安全投入，作出网络安全和信息化有关决策时应有网络安全管理机构人员参与。有关部门要扶持重点网络安全技术产业和项目，支持网络安全技术研究开发和创新应用，推动网络安全产业健康发展。公安机关要会同相关部门组织实施“一带一路”网络安全战略，支持网络安全企业“走出去”，与有关国家共享中国网络安全保护经验。

（三）加强考核评价。各单位、各部门要进一步健全完善网络安全考核评价制度，明确考核指标，组织开展考核。公安机关将网络安全工作纳入社会治安综合治理考核评价体系，每年组织对各地区网络安全工作进行考核评价，每年评选网络安全等级保护、关键信息基础设施安全保护工作先进单位，并将结果报告党委政府，通报网信部门。

（四）加强技术攻关。各单位、各部门要充分调动网络安全企业、科研机构、专家等社会力量积极参与网络安全核心技术攻关，加强网

络安全协同协作、互动互补、共治共享和群防群治。公安机关要会同有关部门加强网络安全等级保护和关键信息基础设施安全保护标准制定工作，出台标准应用指南，加强标准宣贯和应用实施，建设试点示范基地，促进我国网络安全产业和企业的健康发展。

（五）加强人才培养。各单位、各部门要加强网络安全等级保护和关键信息基础设施安全保护业务交流，通过组织开展比武竞赛等形式，发现选拔高精尖技术人才，建设人才库，建立健全人才发现、培养、选拔和使用机制，为做好网络安全工作提供人才保障。

电信和互联网用户个人信息保护规定

时效性：　　现行有效

发文机关：　工业和信息化部

文号：　　工业和信息化部令第24号

发文日期：　2013年07月16日

施行日期：　2013年09月01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　工业和信息化部和各省、自治区、直辖市通信管理局（以下统称电信管理机构）依法对电信和互联网用户个人信息保护工作实施监督管理。

第四条　本规定所称用户个人信息，是指电信业务经营者和互联网信息服务提供者在提供服务的过程中收集的用户姓名、出生日期、身份证件号码、住址、电话号码、账号和密码等能够单独或者与其他信息结合识别用户的信息以及用户使用服务的时间、地点等信息。

第五条　电信业务经营者、互联网信息服务提供者在提供服务的过程中收集、使用用户个人信息，应当遵循合法、正当、必要的原则。

第六条　电信业务经营者、互联网信息服务提供者对其在提供服务过程中收集、使用的用户个人信息的安全负责。

第七条　国家鼓励电信和互联网行业开展用户个人信息保护自律工作。

第二章　信息收集和使用规范

第八条　电信业务经营者、互联网信息服务提供者应当制定用户个人信息收集、使用规则，并在其经营或者服务场所、网站等予以公布。

第九条　未经用户同意，电信业务经营者、互联网信息服务提供者不得收集、使用用户个人信息。

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。

四、司法解释

最高人民法院关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定

时效性：　现行有效

发文机关：　最高人民法院

文号：　法释〔2021〕15号

发文日期：　2021年07月27日

施行日期：　2021年08月01日

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，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，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。

最高人民法院关于审理侵犯商业秘密民事案件适用法律若干问题的规定

时效性：　　现行有效

发文机关：　最高人民法院

文号：　　法释〔2020〕7号

发文日期：　2020年09月10日

施行日期：　2020年09月12日

为正确审理侵犯商业秘密民事案件，根据《中华人民共和国反不正当竞争法》《中华人民共和国民事诉讼法》等有关法律规定，结合审判实际，制定本规定。

第一条　与技术有关的结构、原料、组分、配方、材料、样品、样式、植物新品种繁殖材料、工艺、方法或其步骤、算法、数据、计算机程序及其有关文档等信息，人民法院可以认定构成反不正当竞争法第九条第四款所称的技术信息。

与经营活动有关的创意、管理、销售、财务、计划、样本、招投标材料、客户信息、数据等信息，人民法院可以认定构成反不正当竞争法第九条第四款所称的经营信息。

前款所称的客户信息，包括客户的名称、地址、联系方式以及交易习惯、意向、内容等信息。

第二条　当事人仅以与特定客户保持长期稳定交易关系为由，主张该特定客户属于商业秘密的，人民法院不予支持。

客户基于对员工个人的信赖而与该员工所在单位进行交易，该员

工离职后，能够证明客户自愿选择与该员工或者该员工所在的新单位进行交易的，人民法院应当认定该员工没有采用不正当手段获取权利人的商业秘密。

第三条　　权利人请求保护的信息在被诉侵权行为发生时不为所属领域的相关人员普遍知悉和容易获得的，人民法院应当认定为反不正当竞争法第九条第四款所称的不为公众所知悉。

第四条　　具有下列情形之一的，人民法院可以认定有关信息为公众所知悉：

（一）该信息在所属领域属于一般常识或者行业惯例的；

（二）该信息仅涉及产品的尺寸、结构、材料、部件的简单组合等内容，所属领域的相关人员通过观察上市产品即可直接获得的；

（三）该信息已经在公开出版物或者其他媒体上公开披露的；

（四）该信息已通过公开的报告会、展览等方式公开的；

（五）所属领域的相关人员从其他公开渠道可以获得该信息的。

将为公众所知悉的信息进行整理、改进、加工后形成的新信息，符合本规定第三条规定的，应当认定该新信息不为公众所知悉。

第五条　　权利人为防止商业秘密泄露，在被诉侵权行为发生以前所采取的合理保密措施，人民法院应当认定为反不正当竞争法第九条第四款所称的相应保密措施。

人民法院应当根据商业秘密及其载体的性质、商业秘密的商业价值、保密措施的可识别程度、保密措施与商业秘密的对应程度以及权利人的保密意愿等因素，认定权利人是否采取了相应保密措施。

第六条　具有下列情形之一，在正常情况下足以防止商业秘密泄露的，人民法院应当认定权利人采取了相应保密措施：

（一）签订保密协议或者在合同中约定保密义务的；

（二）通过章程、培训、规章制度、书面告知等方式，对能够接触、获取商业秘密的员工、前员工、供应商、客户、来访者等提出保密要求的；

（三）对涉密的厂房、车间等生产经营场所限制来访者或者进行区分管理的;

（四）以标记、分类、隔离、加密、封存、限制能够接触或者获取的人员范围等方式，对商业秘密及其载体进行区分和管理的；

（五）对能够接触、获取商业秘密的计算机设备、电子设备、网络设备、存储设备、软件等，采取禁止或者限制使用、访问、存储、复制等措施的；

（六）要求离职员工登记、返还、清除、销毁其接触或者获取的商业秘密及其载体，继续承担保密义务的；

（七）采取其他合理保密措施的。

第七条　权利人请求保护的信息因不为公众所知悉而具有现实的或者潜在的商业价值的，人民法院经审查可以认定为反不正当竞争法第九条第四款所称的具有商业价值。

生产经营活动中形成的阶段性成果符合前款规定的，人民法院经审查可以认定该成果具有商业价值。

第八条　被诉侵权人以违反法律规定或者公认的商业道德的

方式获取权利人的商业秘密的，人民法院应当认定属于反不正当竞争法第九条第一款所称的以其他不正当手段获取权利人的商业秘密。

第九条　被诉侵权人在生产经营活动中直接使用商业秘密，或者对商业秘密进行修改、改进后使用，或者根据商业秘密调整、优化、改进有关生产经营活动的，人民法院应当认定属于反不正当竞争法第九条所称的使用商业秘密。

第十条　当事人根据法律规定或者合同约定所承担的保密义务，人民法院应当认定属于反不正当竞争法第九条第一款所称的保密义务。

当事人未在合同中约定保密义务，但根据诚信原则以及合同的性质、目的、缔约过程、交易习惯等，被诉侵权人知道或者应当知道其获取的信息属于权利人的商业秘密的，人民法院应当认定被诉侵权人对其获取的商业秘密承担保密义务。

第十一条　法人、非法人组织的经营、管理人员以及具有劳动关系的其他人员，人民法院可以认定为反不正当竞争法第九条第三款所称的员工、前员工。

第十二条　人民法院认定员工、前员工是否有渠道或者机会获取权利人的商业秘密，可以考虑与其有关的下列因素：

（一）职务、职责、权限；

（二）承担的本职工作或者单位分配的任务；

（三）参与和商业秘密有关的生产经营活动的具体情形；

（四）是否保管、使用、存储、复制、控制或者以其他方式接触、

获取商业秘密及其载体；

（五）需要考虑的其他因素。

第十三条　被诉侵权信息与商业秘密不存在实质性区别的，人民法院可以认定被诉侵权信息与商业秘密构成反不正当竞争法第三十二条第二款所称的实质上相同。

人民法院认定是否构成前款所称的实质上相同，可以考虑下列因素：

（一）被诉侵权信息与商业秘密的异同程度；

（二）所属领域的相关人员在被诉侵权行为发生时是否容易想到被诉侵权信息与商业秘密的区别；

（三）被诉侵权信息与商业秘密的用途、使用方式、目的、效果等是否具有实质性差异；

（四）公有领域中与商业秘密相关信息的情况；

（五）需要考虑的其他因素。

第十四条　通过自行开发研制或者反向工程获得被诉侵权信息的，人民法院应当认定不属于反不正当竞争法第九条规定的侵犯商业秘密行为。

前款所称的反向工程，是指通过技术手段对从公开渠道取得的产品进行拆卸、测绘、分析等而获得该产品的有关技术信息。

被诉侵权人以不正当手段获取权利人的商业秘密后，又以反向工程为由主张未侵犯商业秘密的，人民法院不予支持。

第十五条　被申请人试图或者已经以不正当手段获取、披露、

使用或者允许他人使用权利人所主张的商业秘密，不采取行为保全措施会使判决难以执行或者造成当事人其他损害，或者将会使权利人的合法权益受到难以弥补的损害的，人民法院可以依法裁定采取行为保全措施。

前款规定的情形属于民事诉讼法第一百条、第一百零一条所称情况紧急的，人民法院应当在四十八小时内作出裁定。

第十六条　经营者以外的其他自然人、法人和非法人组织侵犯商业秘密，权利人依据反不正当竞争法第十七条的规定主张侵权人应当承担的民事责任的，人民法院应予支持。

第十七条　人民法院对于侵犯商业秘密行为判决停止侵害的民事责任时，停止侵害的时间一般应当持续到该商业秘密已为公众所知悉时为止。

依照前款规定判决停止侵害的时间明显不合理的，人民法院可以在依法保护权利人的商业秘密竞争优势的情况下，判决侵权人在一定期限或者范围内停止使用该商业秘密。

第十八条　权利人请求判决侵权人返还或者销毁商业秘密载体，清除其控制的商业秘密信息的，人民法院一般应予支持。

第十九条　因侵权行为导致商业秘密为公众所知悉的，人民法院依法确定赔偿数额时，可以考虑商业秘密的商业价值。

人民法院认定前款所称的商业价值，应当考虑研究开发成本、实施该项商业秘密的收益、可得利益、可保持竞争优势的时间等因素。

第二十条　权利人请求参照商业秘密许可使用费确定因被侵

权所受到的实际损失的，人民法院可以根据许可的性质、内容、实际履行情况以及侵权行为的性质、情节、后果等因素确定。

人民法院依照反不正当竞争法第十七条第四款确定赔偿数额的，可以考虑商业秘密的性质、商业价值、研究开发成本、创新程度、能带来的竞争优势以及侵权人的主观过错、侵权行为的性质、情节、后果等因素。

第二十一条　对于涉及当事人或者案外人的商业秘密的证据、材料，当事人或者案外人书面申请人民法院采取保密措施的，人民法院应当在保全、证据交换、质证、委托鉴定、询问、庭审等诉讼活动中采取必要的保密措施。

违反前款所称的保密措施的要求，擅自披露商业秘密或者在诉讼活动之外使用或者允许他人使用在诉讼中接触、获取的商业秘密的，应当依法承担民事责任。构成民事诉讼法第一百一十一条规定情形的，人民法院可以依法采取强制措施。构成犯罪的，依法追究刑事责任。

第二十二条　人民法院审理侵犯商业秘密民事案件时，对在侵犯商业秘密犯罪刑事诉讼程序中形成的证据，应当按照法定程序，全面、客观地审查。

由公安机关、检察机关或者人民法院保存的与被诉侵权行为具有关联性的证据，侵犯商业秘密民事案件的当事人及其诉讼代理人因客观原因不能自行收集，申请调查收集的，人民法院应当准许，但可能影响正在进行的刑事诉讼程序的除外。

第二十三条　当事人主张依据生效刑事裁判认定的实际损失

或者违法所得确定涉及同一侵犯商业秘密行为的民事案件赔偿数额的，人民法院应予支持。

第二十四条　权利人已经提供侵权人因侵权所获得的利益的初步证据，但与侵犯商业秘密行为相关的账簿、资料由侵权人掌握的，人民法院可以根据权利人的申请，责令侵权人提供该账簿、资料。侵权人无正当理由拒不提供或者不如实提供的，人民法院可以根据权利人的主张和提供的证据认定侵权人因侵权所获得的利益。

第二十五条　当事人以涉及同一被诉侵犯商业秘密行为的刑事案件尚未审结为由，请求中止审理侵犯商业秘密民事案件，人民法院在听取当事人意见后认为必须以该刑事案件的审理结果为依据的，应予支持。

第二十六条　对于侵犯商业秘密行为，商业秘密独占使用许可合同的被许可人提起诉讼的，人民法院应当依法受理。

排他使用许可合同的被许可人和权利人共同提起诉讼，或者在权利人不起诉的情况下自行提起诉讼的，人民法院应当依法受理。

普通使用许可合同的被许可人和权利人共同提起诉讼，或者经权利人书面授权单独提起诉讼的，人民法院应当依法受理。

第二十七条　权利人应当在一审法庭辩论结束前明确所主张的商业秘密具体内容。仅能明确部分的，人民法院对该明确的部分进行审理。

权利人在第二审程序中另行主张其在一审中未明确的商业秘密具体内容的，第二审人民法院可以根据当事人自愿的原则就与该商业

秘密具体内容有关的诉讼请求进行调解；调解不成的，告知当事人另行起诉。双方当事人均同意由第二审人民法院一并审理的，第二审人民法院可以一并裁判。

第二十八条　人民法院审理侵犯商业秘密民事案件，适用被诉侵权行为发生时的法律。被诉侵权行为在法律修改之前已经发生且持续到法律修改之后的，适用修改后的法律。

第二十九条　本规定自2020年9月12日起施行。最高人民法院以前发布的相关司法解释与本规定不一致的，以本规定为准。

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；施行前已经作出生效裁判的案件，不适用本规定再审。

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

时效性：　　现行有效

发文机关：　最高人民法院

文号：　　法释〔2020〕17号

发文日期：　2020年12月29日

施行日期：　2021年01月01日

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：

（一）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；

（二）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；

（三）该网络信息侵害人身权益的类型及明显程度；

（四）该网络信息的社会影响程度或者一定时间内的浏览量；

（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；

（六）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；

（七）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：

（一）转载主体所承担的与其性质、影响范围相适应的注意义务；

（二）所转载信息侵害他人人身权益的明显程度；

（三）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，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：

（一）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；

（二）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；

（三）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；

（四）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。

最高人民法院关于审理侵害信息网络传播权民事纠纷案件适用法律若干问题的规定

时效性：　　现行有效

发文机关：　最高人民法院

文号：　　法释〔2020〕19号

发文日期：　2020年12月29日

施行日期：　2021年01月01日

第一条　人民法院审理侵害信息网络传播权民事纠纷案件，在依法行使裁量权时，应当兼顾权利人、网络服务提供者和社会公众的利益。

第二条　本规定所称信息网络，包括以计算机、电视机、固定电话机、移动电话机等电子设备为终端的计算机互联网、广播电视网、固定通信网、移动通信网等信息网络，以及向公众开放的局域网络。

第三条　网络用户、网络服务提供者未经许可，通过信息网络提供权利人享有信息网络传播权的作品、表演、录音录像制品，除法律、行政法规另有规定外，人民法院应当认定其构成侵害信息网络传播权行为。

通过上传到网络服务器、设置共享文件或者利用文件分享软件等方式，将作品、表演、录音录像制品置于信息网络中，使公众能够在个人选定的时间和地点以下载、浏览或者其他方式获得的，人民法院应当认定其实施了前款规定的提供行为。

第四条　有证据证明网络服务提供者与他人以分工合作等方式

共同提供作品、表演、录音录像制品，构成共同侵权行为的，人民法院应当判令其承担连带责任。网络服务提供者能够证明其仅提供自动接入、自动传输、信息存储空间、搜索、链接、文件分享技术等网络服务，主张其不构成共同侵权行为的，人民法院应予支持。

第五条　网络服务提供者以提供网页快照、缩略图等方式实质替代其他网络服务提供者向公众提供相关作品的，人民法院应当认定其构成提供行为。

前款规定的提供行为不影响相关作品的正常使用，且未不合理损害权利人对该作品的合法权益，网络服务提供者主张其未侵害信息网络传播权的，人民法院应予支持。

第六条　原告有初步证据证明网络服务提供者提供了相关作品、表演、录音录像制品，但网络服务提供者能够证明其仅提供网络服务，且无过错的，人民法院不应认定为构成侵权。

第七条　网络服务提供者在提供网络服务时教唆或者帮助网络用户实施侵害信息网络传播权行为的，人民法院应当判令其承担侵权责任。

网络服务提供者以言语、推介技术支持、奖励积分等方式诱导、鼓励网络用户实施侵害信息网络传播权行为的，人民法院应当认定其构成教唆侵权行为。

网络服务提供者明知或者应知网络用户利用网络服务侵害信息网络传播权，未采取删除、屏蔽、断开链接等必要措施，或者提供技术支持等帮助行为的，人民法院应当认定其构成帮助侵权行为。

第八条　人民法院应当根据网络服务提供者的过错，确定其是否承担教唆、帮助侵权责任。网络服务提供者的过错包括对于网络用户侵害信息网络传播权行为的明知或者应知。

网络服务提供者未对网络用户侵害信息网络传播权的行为主动进行审查的，人民法院不应据此认定其具有过错。

网络服务提供者能够证明已采取合理、有效的技术措施，仍难以发现网络用户侵害信息网络传播权行为的，人民法院应当认定其不具有过错。

第九条　人民法院应当根据网络用户侵害信息网络传播权的具体事实是否明显，综合考虑以下因素，认定网络服务提供者是否构成应知：

（一）基于网络服务提供者提供服务的性质、方式及其引发侵权的可能性大小，应当具备的管理信息的能力；

（二）传播的作品、表演、录音录像制品的类型、知名度及侵权信息的明显程度；

（三）网络服务提供者是否主动对作品、表演、录音录像制品进行了选择、编辑、修改、推荐等；

（四）网络服务提供者是否积极采取了预防侵权的合理措施；

（五）网络服务提供者是否设置便捷程序接收侵权通知并及时对侵权通知作出合理的反应；

（六）网络服务提供者是否针对同一网络用户的重复侵权行为采取了相应的合理措施；

（七）其他相关因素。

第十条　网络服务提供者在提供网络服务时，对热播影视作品等以设置榜单、目录、索引、描述性段落、内容简介等方式进行推荐，且公众可以在其网页上直接以下载、浏览或者其他方式获得的，人民法院可以认定其应知网络用户侵害信息网络传播权。

第十一条　网络服务提供者从网络用户提供的作品、表演、录音录像制品中直接获得经济利益的，人民法院应当认定其对该网络用户侵害信息网络传播权的行为负有较高的注意义务。

网络服务提供者针对特定作品、表演、录音录像制品投放广告获取收益，或者获取与其传播的作品、表演、录音录像制品存在其他特定联系的经济利益，应当认定为前款规定的直接获得经济利益。网络服务提供者因提供网络服务而收取一般性广告费、服务费等，不属于本款规定的情形。

第十二条　有下列情形之一的，人民法院可以根据案件具体情况，认定提供信息存储空间服务的网络服务提供者应知网络用户侵害信息网络传播权：

（一）将热播影视作品等置于首页或者其他主要页面等能够为网络服务提供者明显感知的位置的；

（二）对热播影视作品等的主题、内容主动进行选择、编辑、整理、推荐，或者为其设立专门的排行榜的；

（三）其他可以明显感知相关作品、表演、录音录像制品为未经许可提供，仍未采取合理措施的情形。

第十三条　网络服务提供者接到权利人以书信、传真、电子邮件等方式提交的通知及构成侵权的初步证据，未及时根据初步证据和服务类型采取必要措施的，人民法院应当认定其明知相关侵害信息网络传播权行为。

第十四条　人民法院认定网络服务提供者转送通知、采取必要措施是否及时，应当根据权利人提交通知的形式，通知的准确程度，采取措施的难易程度，网络服务的性质，所涉作品、表演、录音录像制品的类型、知名度、数量等因素综合判断。

第十五条　侵害信息网络传播权民事纠纷案件由侵权行为地或者被告住所地人民法院管辖。侵权行为地包括实施被诉侵权行为的网络服务器、计算机终端等设备所在地。侵权行为地和被告住所地均难以确定或者在境外的，原告发现侵权内容的计算机终端等设备所在地可以视为侵权行为地。

第十六条　本规定施行之日起，《最高人民法院关于审理涉及计算机网络著作权纠纷案件适用法律若干问题的解释》（法释〔2006〕11号）同时废止。

本规定施行之后尚未终审的侵害信息网络传播权民事纠纷案件，适用本规定。本规定施行前已经终审，当事人申请再审或者按照审判监督程序决定再审的，不适用本规定。

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

时效性：　　现行有效

发文机关：　最高人民法院,最高人民检察院

文号：　　法释〔2019〕15号

发文日期：　2019年10月21日

施行日期：　2019年11月01日

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，并对单位判处罚金。

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，可以不起诉或者免予刑事处罚；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。

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

时效性：　　现行有效

发文机关：　最高人民法院,最高人民检察院

文号：　　法释〔2017〕10号

发文日期：　2017年05月08日

施行日期：　2017年06月01日

第一条　刑法第二百五十三条之一规定的“公民个人信息”，是指以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息，包括姓名、身份证件号码、通信通讯联系方式、住址、账号密码、财产状况、行踪轨迹等。

第二条　违反法律、行政法规、部门规章有关公民个人信息保护的规定的，应当认定为刑法第二百五十三条之一规定的“违反国家有关规定”。

第三条　向特定人提供公民个人信息，以及通过信息网络或者其他途径发布公民个人信息的，应当认定为刑法第二百五十三条之一规定的“提供公民个人信息”。

未经被收集者同意，将合法收集的公民个人信息向他人提供的，属于刑法第二百五十三条之一规定的“提供公民个人信息”，但是经过处理无法识别特定个人且不能复原的除外。

第四条　违反国家有关规定，通过购买、收受、交换等方式获取

公民个人信息，或者在履行职责、提供服务过程中收集公民个人信息的，属于刑法第二百五十三条之一第三款规定的“以其他方法非法获取公民个人信息”。

第五条　非法获取、出售或者提供公民个人信息，具有下列情形之一的，应当认定为刑法第二百五十三条之一规定的“情节严重”：

（一）出售或者提供行踪轨迹信息，被他人用于犯罪的；

（二）知道或者应当知道他人利用公民个人信息实施犯罪，向其出售或者提供的；

（三）非法获取、出售或者提供行踪轨迹信息、通信内容、征信信息、财产信息五十条以上的；

（四）非法获取、出售或者提供住宿信息、通信记录、健康生理信息、交易信息等其他可能影响人身、财产安全的公民个人信息五百条以上的；

（五）非法获取、出售或者提供第三项、第四项规定以外的公民个人信息五千条以上的；

（六）数量未达到第三项至第五项规定标准，但是按相应比例合计达到有关数量标准的；

（七）违法所得五千元以上的；

（八）将在履行职责或者提供服务过程中获得的公民个人信息出售或者提供给他人，数量或者数额达到第三项至第七项规定标准一半以上的；

（九）曾因侵犯公民个人信息受过刑事处罚或者二年内受过行政

处罚，又非法获取、出售或者提供公民个人信息的；

（十）其他情节严重的情形。

实施前款规定的行为，具有下列情形之一的，应当认定为刑法第二百五十三条之一第一款规定的“情节特别严重”：

（一）造成被害人死亡、重伤、精神失常或者被绑架等严重后果的；

（二）造成重大经济损失或者恶劣社会影响的；

（三）数量或者数额达到前款第三项至第八项规定标准十倍以上的；

（四）其他情节特别严重的情形。

第六条　为合法经营活动而非法购买、收受本解释第五条第一款第三项、第四项规定以外的公民个人信息，具有下列情形之一的，应当认定为刑法第二百五十三条之一规定的“情节严重”：

（一）利用非法购买、收受的公民个人信息获利五万元以上的；

（二）曾因侵犯公民个人信息受过刑事处罚或者二年内受过行政处罚，又非法购买、收受公民个人信息的；

（三）其他情节严重的情形。

实施前款规定的行为，将购买、收受的公民个人信息非法出售或者提供的，定罪量刑标准适用本解释第五条的规定。

第七条　单位犯刑法第二百五十三条之一规定之罪的，依照本解释规定的相应自然人犯罪的定罪量刑标准，对直接负责的主管人员和其他直接责任人员定罪处罚，并对单位判处罚金。

第八条　设立用于实施非法获取、出售或者提供公民个人信息违法犯罪活动的网站、通讯群组，情节严重的，应当依照刑法第二百八十七条之一的规定，以非法利用信息网络罪定罪处罚；同时构成侵犯公民个人信息罪的，依照侵犯公民个人信息罪定罪处罚。

第九条　网络服务提供者拒不履行法律、行政法规规定的信息网络安全管理义务，经监管部门责令采取改正措施而拒不改正，致使用户的公民个人信息泄露，造成严重后果的，应当依照刑法第二百八十六条之一的规定，以拒不履行信息网络安全管理义务罪定罪处罚。

第十条　实施侵犯公民个人信息犯罪，不属于“情节特别严重”，行为人系初犯，全部退赃，并确有悔罪表现的，可以认定为情节轻微，不起诉或者免予刑事处罚；确有必要判处刑罚的，应当从宽处罚。

第十一条　非法获取公民个人信息后又出售或者提供的，公民个人信息的条数不重复计算。

向不同单位或者个人分别出售、提供同一公民个人信息的，公民个人信息的条数累计计算。

对批量公民个人信息的条数，根据查获的数量直接认定，但是有证据证明信息不真实或者重复的除外。

第十二条　对于侵犯公民个人信息犯罪，应当综合考虑犯罪的危害程度、犯罪的违法所得数额以及被告人的前科情况、认罪悔罪态度等，依法判处罚金。罚金数额一般在违法所得的一倍以上五倍以下。

第十三条　本解释自2017年6月1日起施行。

最高人民法院、最高人民检察院、公安部关于办理刑事案件收集提取和审查判断电子数据若干问题的规定

时效性：　　现行有效

发文机关：　最高人民检察院、最高人民法院、公安部

文号：　　法发〔2016〕22号

发文日期：　2016年09月09日

施行日期：　2016年10月01日

一、一般规定

第一条　电子数据是案件发生过程中形成的，以数字化形式存储、处理、传输的，能够证明案件事实的数据。

电子数据包括但不限于下列信息、电子文件：

（一）网页、博客、微博客、朋友圈、贴吧、网盘等网络平台发布的信息；

（二）手机短信、电子邮件、即时通信、通讯群组等网络应用服务的通信信息；

（三）用户注册信息、身份认证信息、电子交易记录、通信记录、登录日志等信息；

（四）文档、图片、音视频、数字证书、计算机程序等电子文件。

以数字化形式记载的证人证言、被害人陈述以及犯罪嫌疑人、被告人供述和辩解等证据，不属于电子数据。确有必要的，对相关证据的收集、提取、移送、审查，可以参照适用本规定。

第二条　侦查机关应当遵守法定程序，遵循有关技术标准，全面、

客观、及时地收集、提取电子数据；人民检察院、人民法院应当围绕真实性、合法性、关联性审查判断电子数据。

第三条　人民法院、人民检察院和公安机关有权依法向有关单位和个人收集、调取电子数据。有关单位和个人应当如实提供。

第四条　电子数据涉及国家秘密、商业秘密、个人隐私的，应当保密。

第五条　对作为证据使用的电子数据，应当采取以下一种或者几种方法保护电子数据的完整性：

（一）扣押、封存电子数据原始存储介质；

（二）计算电子数据完整性校验值；

（三）制作、封存电子数据备份；

（四）冻结电子数据；

（五）对收集、提取电子数据的相关活动进行录像；

（六）其他保护电子数据完整性的方法。

第六条　初查过程中收集、提取的电子数据，以及通过网络在线提取的电子数据，可以作为证据使用。

二、电子数据的收集与提取

第七条　收集、提取电子数据，应当由二名以上侦查人员进行。取证方法应当符合相关技术标准。

第八条　收集、提取电子数据，能够扣押电子数据原始存储介质的，应当扣押、封存原始存储介质，并制作笔录，记录原始存储介质的封存状态。

封存电子数据原始存储介质，应当保证在不解除封存状态的情况下，无法增加、删除、修改电子数据。封存前后应当拍摄被封存原始存储介质的照片，清晰反映封口或者张贴封条处的状况。

封存手机等具有无线通信功能的存储介质，应当采取信号屏蔽、信号阻断或者切断电源等措施。

第九条　具有下列情形之一，无法扣押原始存储介质的，可以提取电子数据，但应当在笔录中注明不能扣押原始存储介质的原因、原始存储介质的存放地点或者电子数据的来源等情况，并计算电子数据的完整性校验值：

（一）原始存储介质不便封存的；

（二）提取计算机内存数据、网络传输数据等不是存储在存储介质上的电子数据的；

（三）原始存储介质位于境外的；

（四）其他无法扣押原始存储介质的情形。

对于原始存储介质位于境外或者远程计算机信息系统上的电子数据，可以通过网络在线提取。

为进一步查明有关情况，必要时，可以对远程计算机信息系统进行网络远程勘验。进行网络远程勘验，需要采取技术侦查措施的，应当依法经过严格的批准手续。

第十条　由于客观原因无法或者不宜依据第八条、第九条的规定收集、提取电子数据的，可以采取打印、拍照或者录像等方式固定相关证据，并在笔录中说明原因。

第十一条　具有下列情形之一的，经县级以上公安机关负责人或者检察长批准，可以对电子数据进行冻结：

（一）数据量大，无法或者不便提取的；

（二）提取时间长，可能造成电子数据被篡改或者灭失的；

（三）通过网络应用可以更为直观地展示电子数据的；

（四）其他需要冻结的情形。

第十二条　冻结电子数据，应当制作协助冻结通知书，注明冻结电子数据的网络应用账号等信息，送交电子数据持有人、网络服务提供者或者有关部门协助办理。解除冻结的，应当在三日内制作协助解除冻结通知书，送交电子数据持有人、网络服务提供者或者有关部门协助办理。

冻结电子数据，应当采取以下一种或者几种方法：

（一）计算电子数据的完整性校验值；

（二）锁定网络应用账号；

（三）其他防止增加、删除、修改电子数据的措施。

第十三条　调取电子数据，应当制作调取证据通知书，注明需要调取电子数据的相关信息，通知电子数据持有人、网络服务提供者或者有关部门执行。

第十四条　收集、提取电子数据，应当制作笔录，记录案由、对象、内容、收集、提取电子数据的时间、地点、方法、过程，并附电子数据清单，注明类别、文件格式、完整性校验值等，由侦查人员、电子数据持有人（提供人）签名或者盖章；电子数据持有人（提供人）

无法签名或者拒绝签名的，应当在笔录中注明，由见证人签名或者盖章。有条件的，应当对相关活动进行录像。

第十五条　收集、提取电子数据，应当根据 刑事诉讼法的规定，由符合条件的人员担任见证人。由于客观原因无法由符合条件的人员担任见证人的，应当在笔录中注明情况，并对相关活动进行录像。

针对同一现场多个计算机信息系统收集、提取电子数据的，可以由一名见证人见证。

第十六条　对扣押的原始存储介质或者提取的电子数据，可以通过恢复、破解、统计、关联、比对等方式进行检查。必要时，可以进行侦查实验。

电子数据检查，应当对电子数据存储介质拆封过程进行录像，并将电子数据存储介质通过写保护设备接入到检查设备进行检查；有条件的，应当制作电子数据备份，对备份进行检查；无法使用写保护设备且无法制作备份的，应当注明原因，并对相关活动进行录像。

电子数据检查应当制作笔录，注明检查方法、过程和结果，由有关人员签名或者盖章。进行侦查实验的，应当制作侦查实验笔录，注明侦查实验的条件、经过和结果，由参加实验的人员签名或者盖章。

第十七条　对电子数据涉及的专门性问题难以确定的，由司法鉴定机构出具鉴定意见，或者由公安部指定的机构出具报告。对于人民检察院直接受理的案件，也可以由最高人民检察院指定的机构出具报告。

具体办法由公安部、最高人民检察院分别制定。

三、电子数据的移送与展示

第十八条　收集、提取的原始存储介质或者电子数据，应当以封存状态随案移送，并制作电子数据的备份一并移送。

对网页、文档、图片等可以直接展示的电子数据，可以不随案移送打印件；人民法院、人民检察院因设备等条件限制无法直接展示电子数据的，侦查机关应当随案移送打印件，或者附展示工具和展示方法说明。

对冻结的电子数据，应当移送被冻结电子数据的清单，注明类别、文件格式、冻结主体、证据要点、相关网络应用账号，并附查看工具和方法的说明。

第十九条　对侵入、非法控制计算机信息系统的程序、工具以及计算机病毒等无法直接展示的电子数据，应当附电子数据属性、功能等情况的说明。

对数据统计量、数据同一性等问题，侦查机关应当出具说明。

第二十条　公安机关报请人民检察院审查批准逮捕犯罪嫌疑人，或者对侦查终结的案件移送人民检察院审查起诉的，应当将电子数据等证据一并移送人民检察院。人民检察院在审查批准逮捕和审查起诉过程中发现应当移送的电子数据没有移送或者移送的电子数据不符合相关要求的，应当通知公安机关补充移送或者进行补正。

对于提起公诉的案件，人民法院发现应当移送的电子数据没有移送或者移送的电子数据不符合相关要求的，应当通知人民检察院。

公安机关、人民检察院应当自收到通知后三日内移送电子数据或

者补充有关材料。

第二十一条　控辩双方向法庭提交的电子数据需要展示的，可以根据电子数据的具体类型，借助多媒体设备出示、播放或者演示。必要时，可以聘请具有专门知识的人进行操作，并就相关技术问题作出说明。

四、电子数据的审查与判断

第二十二条　对电子数据是否真实，应当着重审查以下内容：

（一）是否移送原始存储介质；在原始存储介质无法封存、不便移动时，有无说明原因，并注明收集、提取过程及原始存储介质的存放地点或者电子数据的来源等情况；

（二）电子数据是否具有数字签名、数字证书等特殊标识；

（三）电子数据的收集、提取过程是否可以重现；

（四）电子数据如有增加、删除、修改等情形的，是否附有说明；

（五）电子数据的完整性是否可以保证。

第二十三条　对电子数据是否完整，应当根据保护电子数据完整性的相应方法进行验证：

（一）审查原始存储介质的扣押、封存状态；

（二）审查电子数据的收集、提取过程，查看录像；

（三）比对电子数据完整性校验值；

（四）与备份的电子数据进行比较；

（五）审查冻结后的访问操作日志；

（六）其他方法。

第二十四条　对收集、提取电子数据是否合法，应当着重审查以下内容：

（一）收集、提取电子数据是否由二名以上侦查人员进行，取证方法是否符合相关技术标准；

（二）收集、提取电子数据，是否附有笔录、清单，并经侦查人员、电子数据持有人（提供人）、见证人签名或者盖章；没有持有人（提供人）签名或者盖章的，是否注明原因；对电子数据的类别、文件格式等是否注明清楚；

（三）是否依照有关规定由符合条件的人员担任见证人，是否对相关活动进行录像；

（四）电子数据检查是否将电子数据存储介质通过写保护设备接入到检查设备；有条件的，是否制作电子数据备份，并对备份进行检查；无法制作备份且无法使用写保护设备的，是否附有录像。

第二十五条　认定犯罪嫌疑人、被告人的网络身份与现实身份的同一性，可以通过核查相关 IP 地址、网络活动记录、上网终端归属、相关证人证言以及犯罪嫌疑人、被告人供述和辩解等进行综合判断。

认定犯罪嫌疑人、被告人与存储介质的关联性，可以通过核查相关证人证言以及犯罪嫌疑人、被告人供述和辩解等进行综合判断。

第二十六条　公诉人、当事人或者辩护人、诉讼代理人对电子数据鉴定意见有异议，可以申请人民法院通知鉴定人出庭作证。人民法院认为鉴定人有必要出庭的，鉴定人应当出庭作证。

经人民法院通知，鉴定人拒不出庭作证的，鉴定意见不得作为定

案的根据。对没有正当理由拒不出庭作证的鉴定人，人民法院应当通报司法行政机关或者有关部门。

公诉人、当事人或者辩护人、诉讼代理人可以申请法庭通知有专门知识的人出庭，就鉴定意见提出意见。

对电子数据涉及的专门性问题的报告，参照适用前三款规定。

第二十七条　电子数据的收集、提取程序有下列瑕疵，经补正或者作出合理解释的，可以采用；不能补正或者作出合理解释的，不得作为定案的根据：

（一）未以封存状态移送的；

（二）笔录或者清单上没有侦查人员、电子数据持有人（提供人）、见证人签名或者盖章的；

（三）对电子数据的名称、类别、格式等注明不清的；

（四）有其他瑕疵的。

第二十八条　电子数据具有下列情形之一的，不得作为定案的根据：

（一）电子数据系篡改、伪造或者无法确定真伪的；

（二）电子数据有增加、删除、修改等情形，影响电子数据真实性的；

（三）其他无法保证电子数据真实性的情形。

五、附则

第二十九条　本规定中下列用语的含义：

（一）存储介质，是指具备数据信息存储功能的电子设备、硬盘、

光盘、优盘、记忆棒、存储卡、存储芯片等载体。

（二）完整性校验值，是指为防止电子数据被篡改或者破坏，使用散列算法等特定算法对电子数据进行计算，得出的用于校验数据完整性的数据值。

（三）网络远程勘验，是指通过网络对远程计算机信息系统实施勘验，发现、提取与犯罪有关的电子数据，记录计算机信息系统状态，判断案件性质，分析犯罪过程，确定侦查方向和范围，为侦查破案、刑事诉讼提供线索和证据的侦查活动。

（四）数字签名，是指利用特定算法对电子数据进行计算，得出的用于验证电子数据来源和完整性的数据值。

（五）数字证书，是指包含数字签名并对电子数据来源、完整性进行认证的电子文件。

（六）访问操作日志，是指为审查电子数据是否被增加、删除或者修改，由计算机信息系统自动生成的对电子数据访问、操作情况的详细记录。

第三十条　本规定自2016年10月1日起施行。之前发布的规范性文件与本规定不一致的，以本规定为准。

最高人民法院、最高人民检察院关于办理利用信息网络实施诽谤等刑事案件适用法律若干问题的解释

时效性：　　现行有效

发文机关：　最高人民法院、最高人民检察院

文号：　　法释〔2013〕21号

发文日期：　2013年09月06日

施行日期：　2013年09月10日

第一条　具有下列情形之一的，应当认定为刑法第二百四十六条第一款规定的“捏造事实诽谤他人”：

（一）捏造损害他人名誉的事实，在信息网络上散布，或者组织、指使人员在信息网络上散布的；

（二）将信息网络上涉及他人的原始信息内容篡改为损害他人名誉的事实，在信息网络上散布，或者组织、指使人员在信息网络上散布的；

明知是捏造的损害他人名誉的事实，在信息网络上散布，情节恶劣的，以“捏造事实诽谤他人”论。

第二条　利用信息网络诽谤他人，具有下列情形之一的，应当认定为刑法第二百四十六条第一款规定的“情节严重”：

（一）同一诽谤信息实际被点击、浏览次数达到五千次以上，或者被转发次数达到五百次以上的；

（二）造成被害人或者其近亲属精神失常、自残、自杀等严重后果的；

（三）二年内曾因诽谤受过行政处罚，又诽谤他人的；

（四）其他情节严重的情形。

第三条　利用信息网络诽谤他人，具有下列情形之一的，应当认定为刑法第二百四十六条第二款规定的“严重危害社会秩序和国家利益”：

（一）引发群体性事件的；

（二）引发公共秩序混乱的；

（三）引发民族、宗教冲突的；

（四）诽谤多人，造成恶劣社会影响的；

（五）损害国家形象，严重危害国家利益的；

（六）造成恶劣国际影响的；

（七）其他严重危害社会秩序和国家利益的情形。

第四条　一年内多次实施利用信息网络诽谤他人行为未经处理，诽谤信息实际被点击、浏览、转发次数累计计算构成犯罪的，应当依法定罪处罚。

第五条　利用信息网络辱骂、恐吓他人，情节恶劣，破坏社会秩序的，依照刑法第二百九十三条第一款第（二）项的规定，以寻衅滋事罪定罪处罚。

编造虚假信息，或者明知是编造的虚假信息，在信息网络上散布，或者组织、指使人员在信息网络上散布，起哄闹事，造成公共秩序严重混乱的，依照刑法第二百九十三条第一款第（四）项的规定，以寻衅滋事罪定罪处罚。

第六条　以在信息网络上发布、删除等方式处理网络信息为由，威胁、要挟他人，索取公私财物，数额较大，或者多次实施上述行为的，依照刑法第二百七十四条的规定，以敲诈勒索罪定罪处罚。

第七条　违反国家规定，以营利为目的，通过信息网络有偿提供删除信息服务，或者明知是虚假信息，通过信息网络有偿提供发布信息等服务，扰乱市场秩序，具有下列情形之一的，属于非法经营行为“情节严重”，依照刑法第二百二十五条第（四）项的规定，以非法经营罪定罪处罚：

（一）个人非法经营数额在五万元以上，或者违法所得数额在二万元以上的；

（二）单位非法经营数额在十五万元以上，或者违法所得数额在五万元以上的。

实施前款规定的行为，数额达到前款规定的数额五倍以上的，应当认定为刑法第二百二十五条规定的“情节特别严重”。

第八条　明知他人利用信息网络实施诽谤、寻衅滋事、敲诈勒索、非法经营等犯罪，为其提供资金、场所、技术支持等帮助的，以共同犯罪论处。

第九条　利用信息网络实施诽谤、寻衅滋事、敲诈勒索、非法经营犯罪，同时又构成刑法第二百二十一条规定的损害商业信誉、商品声誉罪，第二百七十八条规定的煽动暴力抗拒法律实施罪，第二百九十一条之一规定的编造、故意传播虚假恐怖信息罪等犯罪的，依照处罚较重的规定定罪处罚。

第十条　本解释所称信息网络，包括以计算机、电视机、固定电话机、移动电话机等电子设备为终端的计算机互联网、广播电视网、固定通信网、移动通信网等信息网络，以及向公众开放的局域网络。

最高人民法院、最高人民检察院关于办理危害计算机信息系统安全刑事案件应用法律若干问题的解释

时效性：　　现行有效

发文机关：　最高人民法院、最高人民检察院

文号：　　法释〔2011〕19号

发文日期：　2011年08月01日

施行日期：　2011年09月01日

第一条　非法获取计算机信息系统数据或者非法控制计算机信息系统，具有下列情形之一的，应当认定为刑法第二百八十五条第二款规定的“情节严重”：

（一）获取支付结算、证券交易、期货交易等网络金融服务的身份认证信息十组以上的；

（二）获取第（一）项以外的身份认证信息五百组以上的；

（三）非法控制计算机信息系统二十台以上的；

（四）违法所得五千元以上或者造成经济损失一万元以上的；

（五）其他情节严重的情形。

实施前款规定行为，具有下列情形之一的，应当认定为刑法第二百八十五条第二款规定的“情节特别严重”：

（一）数量或者数额达到前款第（一）项至第（四）项规定标准五倍以上的；

（二）其他情节特别严重的情形。

明知是他人非法控制的计算机信息系统，而对该计算机信息系统

的控制权加以利用的，依照前两款的规定定罪处罚。

第二条　具有下列情形之一的程序、工具，应当认定为刑法第二百八十五条第三款规定的“专门用于侵入、非法控制计算机信息系统的程序、工具”：

（一）具有避开或者突破计算机信息系统安全保护措施，未经授权或者超越授权获取计算机信息系统数据的功能的；

（二）具有避开或者突破计算机信息系统安全保护措施，未经授权或者超越授权对计算机信息系统实施控制的功能的；

（三）其他专门设计用于侵入、非法控制计算机信息系统、非法获取计算机信息系统数据的程序、工具。

第三条　提供侵入、非法控制计算机信息系统的程序、工具，具有下列情形之一的，应当认定为刑法第二百八十五条第三款规定的“情节严重”：

（一）提供能够用于非法获取支付结算、证券交易、期货交易等网络金融服务身份认证信息的专门性程序、工具五人次以上的；

（二）提供第（一）项以外的专门用于侵入、非法控制计算机信息系统的程序、工具二十人次以上的；

（三）明知他人实施非法获取支付结算、证券交易、期货交易等网络金融服务身份认证信息的违法犯罪行为而为其提供程序、工具五人次以上的；

（四）明知他人实施第（三）项以外的侵入、非法控制计算机信息系统的违法犯罪行为而为其提供程序、工具二十人次以上的；

（五）违法所得五千元以上或者造成经济损失一万元以上的；

（六）其他情节严重的情形。

实施前款规定行为，具有下列情形之一的，应当认定为提供侵入、非法控制计算机信息系统的程序、工具“情节特别严重”：

（一）数量或者数额达到前款第（一）项至第（五）项规定标准五倍以上的；

（二）其他情节特别严重的情形。

第四条　破坏计算机信息系统功能、数据或者应用程序，具有下列情形之一的，应当认定为刑法第二百八十六条第一款和第二款规定的“后果严重”：

（一）造成十台以上计算机信息系统的主要软件或者硬件不能正常运行的；

（二）对二十台以上计算机信息系统中存储、处理或者传输的数据进行删除、修改、增加操作的；

（三）违法所得五千元以上或者造成经济损失一万元以上的；

（四）造成为一百台以上计算机信息系统提供域名解析、身份认证、计费等基础服务或者为一万以上用户提供服务的计算机信息系统不能正常运行累计一小时以上的；

（五）造成其他严重后果的。

实施前款规定行为，具有下列情形之一的，应当认定为破坏计算机信息系统“后果特别严重”：

（一）数量或者数额达到前款第（一）项至第（三）项规定标准

五倍以上的；

（二）造成为五百台以上计算机信息系统提供域名解析、身份认证、计费等基础服务或者为五万以上用户提供服务的计算机信息系统不能正常运行累计一小时以上的；

（三）破坏国家机关或者金融、电信、交通、教育、医疗、能源等领域提供公共服务的计算机信息系统的功能、数据或者应用程序，致使生产、生活受到严重影响或者造成恶劣社会影响的；

（四）造成其他特别严重后果的。

第五条　具有下列情形之一的程序，应当认定为刑法第二百八十六条第三款规定的“计算机病毒等破坏性程序”：

（一）能够通过网络、存储介质、文件等媒介，将自身的部分、全部或者变种进行复制、传播，并破坏计算机系统功能、数据或者应用程序的；

（二）能够在预先设定条件下自动触发，并破坏计算机系统功能、数据或者应用程序的；

（三）其他专门设计用于破坏计算机系统功能、数据或者应用程序的程序。

第六条　故意制作、传播计算机病毒等破坏性程序，影响计算机系统正常运行，具有下列情形之一的，应当认定为刑法第二百八十六条第三款规定的“后果严重”：

（一）制作、提供、传输第五条第（一）项规定的程序，导致该程序通过网络、存储介质、文件等媒介传播的；

（二）造成二十台以上计算机系统被植入第五条第（二）、（三）项规定的程序的；

（三）提供计算机病毒等破坏性程序十人次以上的；

（四）违法所得五千元以上或者造成经济损失一万元以上的；

（五）造成其他严重后果的。

实施前款规定行为，具有下列情形之一的，应当认定为破坏计算机信息系统“后果特别严重”：

（一）制作、提供、传输第五条第（一）项规定的程序，导致该程序通过网络、存储介质、文件等媒介传播，致使生产、生活受到严重影响或者造成恶劣社会影响的；

（二）数量或者数额达到前款第（二）项至第（四）项规定标准五倍以上的；

（三）造成其他特别严重后果的。

第七条　明知是非法获取计算机信息系统数据犯罪所获取的数据、非法控制计算机信息系统犯罪所获取的计算机信息系统控制权，而予以转移、收购、代为销售或者以其他方法掩饰、隐瞒，违法所得五千元以上的，应当依照刑法第三百一十二条第一款的规定，以掩饰、隐瞒犯罪所得罪定罪处罚。

实施前款规定行为，违法所得五万元以上的，应当认定为刑法第三百一十二条第一款规定的“情节严重”。

单位实施第一款规定行为的，定罪量刑标准依照第一款、第二款的规定执行。

第八条　以单位名义或者单位形式实施危害计算机信息系统安全犯罪，达到本解释规定的定罪量刑标准的，应当依照刑法第二百八十五条、第二百八十六条的规定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。

第九条　明知他人实施刑法第二百八十五条、第二百八十六条规定的行为，具有下列情形之一的，应当认定为共同犯罪，依照刑法第二百八十五条、第二百八十六条的规定处罚：

（一）为其提供用于破坏计算机信息系统功能、数据或者应用程序的程序、工具，违法所得五千元以上或者提供十人次以上的;

（二）为其提供互联网接入、服务器托管、网络存储空间、通讯传输通道、费用结算、交易服务、广告服务、技术培训、技术支持等帮助，违法所得五千元以上的;

（三）通过委托推广软件、投放广告等方式向其提供资金五千元以上的。

实施前款规定行为，数量或者数额达到前款规定标准五倍以上的，应当认定为刑法第二百八十五条、第二百八十六条规定的“情节特别严重”或者“后果特别严重”。

第十条　对于是否属于刑法第二百八十五条、第二百八十六条规定的“国家事务、国防建设、尖端科学技术领域的计算机信息系统”、“专门用于侵入、非法控制计算机信息系统的程序、工具”、“计算机病毒等破坏性程序”难以确定的，应当委托省级以上负责计算机信息系统安全保护管理工作的部门检验。司法机关根据检验结论，并结合案件具

体情况认定。

第十一条　本解释所称“计算机信息系统”和“计算机系统”，是指具备自动处理数据功能的系统，包括计算机、网络设备、通信设备、自动化控制设备等。

本解释所称“身份认证信息”，是指用于确认用户在计算机信息系统上操作权限的数据，包括账号、口令、密码、数字证书等。

本解释所称“经济损失”，包括危害计算机信息系统犯罪行为给用户直接造成的经济损失，以及用户为恢复数据、功能而支出的必要费用。

五、国家及行业标准

JR/T 0218-2021 金融业数据能力建设指引

时效性：　　现行有效

发布机关：　中国人民银行

类别：　　金融行业标准

发布日期：　2021 年 02 月 09 日

实施日期：　2021 年 02 月 09 日

1 范围

本文件规定了数据战略、数据治理、数据架构、数据规范、数据保护、数据质量、数据应用、数据生存周期管理能力域划分，明确了相关能力项，提出了每个能力项的建设目标和思路。

本文件适用于指导金融机构开展金融数据能力建设。

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。

JR/T 0149—2016 中国金融移动支付标记化技术规范

JR/T 0171—2020 个人金融信息保护技术规范

JR/T 0196—2020 多方安全计算金融应用技术规范

JR/T 0197—2020 金融数据安全数据安全分级指南

3 术语和定义

下列术语和定义适用于本文件。

3.1 能力域 capability area

数据管理相关活动、过程等以及一组相关数据能力子域的集合。

3.2 数据战略 data strategy

组织开展数据工作的愿景、目的、目标和原则。

3.3 数据治理 data governance

对数据进行处置、格式化和规范化的过程[1]。

2.数据治理涉及数据全生存周期管理，无论数据是处于静态、动态、未完成状态还是交易状态。

3.4 数据质量 data quality

在特定条件下使用时,数据特性满足明确要求及隐含要求的程度。

3.5 数据生存周期 data lifecycle

将原始数据转化为可用于行动的知识的一组过程。

3.6 主数据 master data

企业中需要跨系统、跨部门进行共享的核心业务实体数据。

3.7 参考数据 reference data

对其他数据进行分类和规范的数据。

4 缩略语

下列缩略语适用于本文件。

PEST：宏观环境分析模型(Politics Economy Society Technology)

SWOT：企业战略分析法(Strengths Weaknesses Opportunities

[1] 注：数据治理是数据和数据系统管理的基本要素。

Threats)

TCO：总拥有成本(Total Cost of Ownership)

5 能力域与能力项

金融数据管理能力划分为 8 个能力域和 29 个能力项(见下表)。

能力域及能力项表

6 基本原则

金融业数据能力建设遵循以下基本原则：

用户授权。明确告知用户数据采集和使用的目的、方式以及范围，确保用户充分知情，获取用户自愿授权后方可采集使用，严格保障用户知情权和自主选择权。

安全合规。遵循国家法律法规、管理制度，符合国家及金融行业标准规范，建立健全数据安全管理长效机制和防护措施，通过技术手段将原始信息脱敏，并与关联性较高的敏感信息进行安全隔离、分散存储，严控访问权限，严防数据泄露、篡改、损毁与不当使用，依法依规保护数据主体隐私权在数据管理与应用过程中不受侵害。

分类施策。综合考量国家安全、公众权益、个人隐私和企业合法利益等因素，根据数据的保密性、完整性、可用性等属性受到破坏后的影响对象和影响程度，对数据进行分级分类管理。对不同级别数据进行分类施策，采取差异化控制措施，实现数据精细化管理。

最小够用。规范数据使用行为，严控数据获取和应用范围，确保数据专事专用、最小够用，杜绝过度采集、误用、滥用数据，切实保障数据主体的数据所有权和使用权。

可用不可见。建立数据规范共享机制，在保障原始数据可用不可见的前提下规范开展数据共享与融合应用，保证跨行业、跨机构的数据使用合规、范围可控，有效保护数据隐私安全，确保数据所有权不因共享应用而发生让渡。

7 数据战略

7.1 数据战略规划

7.1.1 概述

数据战略规划是基于金融机构对数据的需求，经相关方充分协商达成一致后拆解出可评估、可衡量、可操作的目标，最终形成数据战略内容的过程。数据战略具有一定前瞻性和统领性，内容覆盖数据管理工作愿景、目标、原则、任务、路径等要素，做到内容全面、目标合理、范围明确、路径清晰，可操作性强，能够指导未来一段时间有效开展数据管理工作。

7.1.2 工作措施

数据战略规划采取的工作措施包括但不限于：

a）开展数据战略需求评估，全面考量法律法规、行业监管要求、金融机构业务发展规划、金融科技发展趋势等对数据的需求，并将数据战略列入金融科技发展故略中，

b）对当前和未来面临内外部形势开展分析评估和研判。

c）识别数据战略的相关方，包括行业主管部门、股东、职员、客户、业务合作伙伴等。数据战略为相关方充分协商并达成一致的结果。

d）由董事会负责制定数据战略。

e）至少考量以下数据战略内容：

1）愿景陈述，包括数据管理的原则、目的和目标。

2）规划范围，包括重要业务领域、数据范围。

3）现状分析，包括企业当前数据管理现状及与目标存在的差距。

4）主要工作任务和优先级。

5）所选择数据管理模型和建设方法。

6）战略相关方名单。

7）管理层和相关职能部门具体责任和工作任务分工。

8）相关保障措施。

9）量化考核机制。

10）持续优化路线图。

f）将数据战略形成文档，并经审批后以正式文件发布。

g）根据法律法规、监管政策、业务战略、金融科技发展等方面的要求，持续优化改进数据战略。

h）运用 PEST、SWOT 等方法对宏观环境进行全面分析。

i）以股东大会表决等形式审批数据战略，确保获得企业内广泛认可。

J）通过数据战略的发布，带动形成良好的数据文化。

7.2 数据战略实施

7.2.1 概述

数据战略实施是按照既定目标和路线持续执行数据战略工作任务的过程，做好工作任务责任分解和措施保障，强化过程监督管理，确

保达成预期目标。

7.2.2 工作措施

数据战略实施采取的工作措施包括但不限于：

a）落实数据战略实施过程中的组织、资金、制度、人才等保障措施。

b）做好数据战略实施过程中的工作计划和中长期规划，有序开展数据战略实施。在实施过程中定期总结，及时对照修正偏差。

c）明确实施过程中的领导机构和牵头部门以及具体负责部门的职责分工，做好工作任务分解落实。

d）由监事会对数据战略的实施过程进行有效监督，强化目标管理与工作考核。

e）强化数据战略实施组织保障.如设立专职负责数据管理的部门和岗位等。

7.3 数据战略评估

7.3.1 概述

数据战略评估是在数据战略实施期间和实施后，对照目标和实施情况全面综合评价数据战略实施的效果，并进行闭环反馈。

7.3.2 工作措施

数据战略评估采取的工作措施包括但不限于：

a）针对数据战略实施建立系统完整的评估准则，明确评估方法。

b）定期对数据战略实施情况进行评估。

c）根据评估结果对数据战略进行持续优化，指导数据管理工作的

有效开展。

d）采取量化分析方法或统计方法，从成本、效益、时间、风险等角度对企业整体的数据战略实施情况开展成本效益评估。

e）构建专门的数据管理 TCO 方法，衡量评估数据管理工作的切入点和实施基础的变化，并调整资金预算。

f）编制并发布数据管理资金预算报告。

g）定期对数据能力建设情况进行评估。

8 数据治理

8.1 组织建设

8.1.1 概述

组织建设包括组织架构、岗位设置、团队建设、数据责任等内容，是各项数据职能工作开展的基础。其目标是对数据管理和应用进行职责规划与控制，指导各项数据职能的执行，以确保有效落实数据战略目标。

8.1.2 工作措施

数据治理组织建设采取的工作措施包括但不限于：

a）管理层负责数据治理工作相关决策，参与数据治理相关工作。

b）明确统一的数据治理归口部门，负责组织协调各项数据职能工作。

c）明确数据工作人员的岗位职责。

d）制定数据治理工作的评价标准，建立人员奖惩制度。

e）建立健全覆盖管理、业务和技术等方面人员的数据责任体系，

明确各方在数据管理过程中的职责。

f）定期进行培训和经验分享，不断提高数据治理能力。

g）建立覆盖管理、技术、运营等的复合型数据团队。

h）建立适用于数据工作相关岗位人员的量化绩效评估指标，评估相关岗位人员绩效，并发布考核结果。

8.2 制度建设

8.2.1 概述

制度建设是数据管理和数据应用各项工作有序开展的基础，是数据治理的依据。制度建设分层次设计，遵循严格的发布流程，并定期检查和更新。

8.2.2 工作措施

数据治理制度建设采取的工作措施包括但不限于：

a）建立科学的数据制度框架。

b）建立全面、有效的数据管理和数据应用机制。

c）建立完备的数据制度体系，保障数据治理工作的规范性和严肃性。

d）根据实施情况对数据制度进行持续修订，保障制度有效性。

e）定期开展数据制度相关培训和宣传。

f）业务人员积极参与数据制度的制定。

g）数据制度的制定符合监管、合规要求。

h）量化评估数据制度的执行情况。

8.3 流程规范

数据治理流程规范采取的工作措施包括但不限于：

a）建立规范的数据治理流程，规定具体的工作步骤以及各环节主要活动。

b）明确数据治理流程中各参与人员工作任务，并有效执行。

c）建立完善的数据治理流程管理机制，用以指导数据治理流程的修订，保障流程有效性。

d）业务人员积极参与数据治理流程的制定，并有效推动业务工作的开展。

e）数据治理流程的制定参考行业先进案例，体现未来业务发展的需要。

8.4 技术支撑

8.4.1 概述

技术支撑是指为开展数据治理工作而建设的相关系统或平台。

8.4.2 工作措施

数据治理技术支撑采取的工作措施包括但不限于：

a）对数据治理系统或平台进行整体建设规划。

b）将数据治理相关组织、制度、流程落实到系统或平台当中，以规范数据治理工作流程，提高数据治理工作效率。

c）业务人员充分运用系统或平台开展数据治理各领域工作。

d）明确数据治理系统或平台的规划、建设和运维责任部门。

e）数据治理系统或平台建设参考行业先进案例，充分满足数据治理各领域工作开展的需要。

f）针对数据治理系统或平台建立科学的效能评价体系，对系统或平台使用效能进行量化评估，不断完善其功能。

9 数据架构

9.1 元数据管理

9.1.1 概述

元数据管理是关于元数据的创建、存储、整合、控制等一整套流程的集合。

9.1.2 工作措施

元数据管理采取的工作措施包括但不限于：

a）根据业务、管理、应用等方面的需求,对元数据进行分类，建立元数据标准，保障元数据的互操作性。

b）建立集中的元数据存储库，统一管理多个业务领域及应用系统的元数据。

c）制定和执行贯穿数据生存周期的元数据集成和变更流程，实现元数据采集和变更规范化管理。

d）制定和执行统一的元数据应用需求管理流程，实现元数据应用需求的规范化管理。

e）通过服务、接口等方式实现各类元数据内容在应用系统之间共享使用。

f）定义并应用量化指标，衡量元数据管理工作的有效性。

g）建立元数据间的关联关系，并通过可视化形式展现。

h）在满足用户授权、安全合规、最小够用等前提下，实现跨机构、

跨行业的元数据共享、交换和应用。

9.2 数据模型

9.2.1 概述

数据模型使用结构化的语言将收集到的业务经营、管理和决策中使用的数据需求进行综合分析，并按照模型设计规范将数据需求重新组织。数据模型分为企业级数据模型和系统应用级数据模型。企业级数据模型包括主题域模型、概念模型和逻辑模型，系统应用级数据模型包括逻辑模型和物理模型。

9.2.2 工作措施

数据模型采取的工作措施包括但不限于：

a）对应用系统的数据现状进行全面梳理，了解当前存在的问题并提出解决办法。

b）分析相关方的数据需求，至少包括系统的分析应用需求、内部组织战略和合规需求、行业监管需求、跨机构互联互通需求。

c）制定企业级数据模型开发规范，指导企业级数据模型的开发和管理.

d）建立覆盖业务经营、管理和决策数据需求的企业级数据模型。

e）使用企业级数据模型指导系统应用级数据模型的设计，并设置相应的角色进行管理。

f）建立企业级数据模型和系统应用级数据模型的映射关系，并根据系统的建设定期更新企业级数据模型。

g）基于数据模型建立统一的数据资源目录，实现数据资源的统一

管理。

h）根据数据变化情况持续维护、发布数据资源目录。

i）使用企业级数据模型，指导和规划整个企业应用系统的投资、建设和维护。

j）建立企业级数据模型和系统应用级数据模型的同步更新机制，确保一致性。

k）及时跟踪、研判内外部数据需求变化趋势，持续优化企业级数据模型。

9.3 数据分布

数据分布采取的工作措施包括但不限于：

a）在企业层面制定数据分布关系管理规范，统一数据分布关系的表现形式和管理流程。

b）梳理数据与业务流程、组织机构、系统之间的分布关系，形成数据分布关系库。

c)梳理数据的权威数据源,对每类数据明确合理的唯一管理主体、信息采集和存储系统，减少重复采集，降低数据冗余。

d）根据数据分布关系对数据相关工作进行规范。

e）根据业务流程和系统建设情况，定期维护和更新数据分布关系库。

f)通过数据分布关系的梳理,員化分析数据相关工作的业务价值。

g）通过数据分布关系的梳理，优化数据的存储和集成关系。

h）实现数据分布关系管理流程的自动优化，提升管理效率。

9.4 数据集成

数据集成采取的工作措施包括但不限于：

a）建立数据集成规范管理制度，明确数据集成管理的原则、方式和方法。

b）形成数据集成管理标准，实现内部数据规范整合与有序流转。

c)建设数据集成管理平台或工具,实现数据统一采集与集中管理。

d）对新建系统的数据集成方式进行检查，确保统一性和规范性.

e）具备持续优化和提升数据集成管理的能力。

10 数据规范

10.1 数据元

10.1.1 概述

数据元是由一组属性规定其定义、标识、表示和允许值的数据单元。通过制定核心数据元的统一规范，提升数据相关方对数据理解的一致性。

10.1.2 工作措施

数据元管理采取的工作措施包括但不限于：

a）建立内部数据元管理规范，明确数据元的管理流程。

b）基于国家和金融行业相关制度、规范，建立健全内部数据元规范体系。

c）制定完整的规范落地方案，并发布数据元的统一目录，提供统一的查询方法。

d）定期开展数据元规范落地执行情况分析，形成分析报告，并对

相关问题进行处理和跟踪。

e）定期组织开展数据元应用相关培训。

f）发布数据元管理报告，汇总数据元管理工作的进展。

g）对数据元管理过程进行监控分析，支持数据元信息定期更新，实现数据元高效有序管理。

h）制定各部门数据元管理工作的考核体系，生成数据元管理考核报告。

10.2 参考数据和主数据

10.2.1 概述

参考数据是一组增强数据可读性、可维护性、可理解性的数据集合。借助参考数据可实现对其他数据的合理分类。

主数据是企业中需要跨系统、跨部门共享的核心业务实体数据。主数据管理是对主数据规范和内容进行管理，实现主数据跨系统、跨部门的一致、共享使用。

10.2.2 工作措施

参考数据和主数据管理采取的工作措施包括但不限于：

a）制定参考数据和主数据的管理流程，规范参考数据和主数据的应用。

b）实现企业级参考数据和主数据的统一管理、展现和使用。

e）制定企业内部各参考数据和主数据的数据规范，并在企业内部发布。

d）制定编码规则和数据模型，定义参考数据和主数据唯一标识的

生成规则、组成部分及其含义。

e）识别参考数据值域和取值范围。

f）明确参考数据和主数据管理部门和可信数据源，保障参考数据和主数据的数据质量和使用效果。

g）保持各应用系统中的参考数据和主数据与企业级的参考数据和主数据一致。

h）新建项目的过程中，统一分析项目与企业内部已有的参考数据和主数据的数据集成问题。

i）建立参考数据和主数据相关的质量规则，分析、跟踪并推动解决各应用系统中参考数据和主数据的数据质量问题。

j）建立参考数据和主数据管理的资源库。

k）优化参考数据和主数据的管理规范和管理流程，并支持参考数据和主数据信息定期更新，实现参考数据和主数据高效有序管理。

l）制定各部门参考数据和主数据管理工作的考核评价体系。

m）定期生成、发布参考数据和主数据管理工作的考核报告。

10.3 明细数据

10.3.1 概述

明细数据是日常生产经营等活动中直接产生或获取的未经任何加工的初始数据。

10.3.2 工作措施

明细数据管理采取的工作措施包括但不限于：

a）制定统一的明细数据管理规范、细则等制度文件，规范企业层

面的明细数据管理流程，明确明细数据管理要求，包括质量要求、安全要求等。

b）根据企业业务管理需求，制定企业内明细数据主题域分类。

c）根据企业业务战略需求、行业监管要求建立统一的明细数据资源目录。

d）遵循统一的业务规则、技术规范，建立企业层面的明细数据规范。

e）明确各类明细数据的管理部门，进行明细数据的管理。

f）对明细数据相关问题进行处理和跟踪。

g）定期分析明细数据规范执行情况，形成分析报告，不断完善明细数据规范。

h）结合企业业务情况，根据国家和金融行业相关制度规范，优化完善明细数据规范。

i）定期发布明细数据及其规范管理报告，阶段汇总明细数据管理工作的进展。

j）制定明细数据及其规范的考核体系。

k）通过量化分析的方式对明细数据及其规范的管理过程进行考核。

l）定期发布明细数据及其规范管理工作考核报告。

10.4 指标数据

10.4.1 概述

指标数据是在经营分析过程中衡量某一个目标或事物的数据，由

明细数据按照统计需求和分析规则加工生成，一般由管理属性、业务属性、技术属性等组

10.4.2 工作措施

指标数据管理采取的工作措施包括但不限于：

a）制定统一的指标数据管理规范、细则等制度文件，规范企业层面的指标数据管理流程，明确指标数据的管理要求，包括质量要求、安全要求等。

b）根据企业业务管理需求制定企业内指标数据分类管理框架，保证指标分类框架的全面性和各分类之间的独立性。

c）根据指标数据的数据、接门规范等，由相关部门或应用系统定期进行数据的采集、生成。

d）对指标数据进行授权访问，并根据用户需求进行数据展示。

e）对指标数据采集、生成过程进行监控，保证指标数据的准确性。

f）对各部门的指标数据进行统一汇总和梳理，形成企业层面的指标数据字典并发布。

g）根据企业的业务战略需求、行业监管要求建立统一的指标数据资源目录。

h）遵循统一的业务规则、技术规范，在企业层面建立指标数据规范。

i）明确各类指标数据的归口管理部门，负责相应指标数据的管理。

j）对指标数据相关问题进行处理和跟踪。

k）定期分析指标数据规范执行情况，形成分析报告，不断完善指

标数据规范。

l）建立指标数据价值评价体系，包括质量、标准、应用频次、依赖車要性等。

m）结合企业业务情况，根据国家和金融行业相关制度规范，优化完善指标数据规范。

n）定期发布指标数据及其规范管理报告，阶段汇总指标数据管理工作的进展。

o）制定各部门指标数据及其规范的考核体系。

p）通过量化分析的方式对指标数据及其规范的管理过程进行考核。

q）定期发布指标数据及其规范管理工作考核报告。

11 数据保护

11.1 数据保护策略

11.1.1 概述

数据保护策略是数据保护的核心内容，在制定的过程中结合企业管理需求、行业监管要求以及相关制度规范等统一制定。

企业在制定数据保护策略的过程中需要了解、掌握行业监管要求，并根据企业对数据保护的业务需要，定义企业数据保护管理的目标、原则、制度、管理组织、管理流程等，制定适合的数据保护标准，确定数据保护等级及覆盖范围等，建立数据保护管理策略，指导数据保护管理及相关工作，为企业的数据保护管理提供保障。

11.1.2 工作措施

数据保护策略采取的工作措施包括但不限于：

a）制定数据保护规范与策略相关的管理流程，并以此指导数据保护规范和策略的制定。

b）依据法律法规、行业规章制度以及相关规范的基本要求，建立统一的数据保护规范以及策略并正式发布。

c）识别数据保护相关方，并明确数据保护相关方在数据保护管理过程中的职责。

d)在数据保护规范与策略制定过程中能够识别企业内外部的数据保护需求，包括法律法规、行业监管的要求。

e）建立针对数据收集、传输、存储、使用、删除、销毁等全生命周期的安全保护策略。

f）依据法律法规、行业规章制度以及相关规范的基本要求，建立个人金融信息保护策略。

g）针对数据保护，建立相应的风险监测机制、风险评估机制、应急处置机制、风险事件通报机制。

h）根据 JR/T0197-2020 相关要求，依据合法合规、可执行性、时效性、自主性、差异性、客观性等原则，建立统一的数据分级分类管理制度。

i）采用或提供云服务时制定相应的数据保护策略。

j）定期开展数据保护规范和策略相关教育培训和宣传工作。

k）梳理和明确有关法律法规'行业规章制度以及相关规范等关于数据保护方面的要求列表,并与企业的数据保护规范和策略进行关联。

l）根据内外部环境的变化定期优化完善数据保护规范与策略。

11.2 数据保护管理

11.2.1 概述

数据保护管理是通过开展数据保护等级划分、数据访问权限控制、用户身份认证和访问行为监控、数据安全风险防护、数据隐私保护等管理工作，满足数据保护的业务需求和监管要求，实现对数据生存周期的安全管理。

11.2.2 工作措施

数据保护管理采取的工作措施包括但不限于：

a）依据保护策略对数据进行全面的等级划分，清晰定义每级数据的保护需求，明确保护需求的责任部门。

b）根据行业监管对数据保护的要求明确定义数据范围。

c）围绕数据生存周期，了解相关方的数据保护需求，并对数据进行严格的使用授权和保护。

d）能对数据生存周期进行风险监控，及时了解可能存在的风险隐患。

e）通过数据脱敏、加密、过滤等手段，保证数据安全和数据隐私。

f）定期开展数据安全风险分析活动，明确分析要点，制定风险预案并监督实施.

g）定期汇总、分析企业内部的数据风险问题，并形成数据保护知识库。

h）定期开展数据保护相关培训和宣传，提升人员数据保护意识。

i）数据保护管理工作符合相关法律法规、规章制度以及金融行业规范等。

j）依据保护策略提供数据收集、传输、存储、使用、删除、销毁等全生命周期的保护。

k）采用或提供云服务时依据数据保护策略提供数据保护。

l）依据个人金融信息保护策略开展数据隐私保护。

m）建立涵盖密钥生成、存储、备份、恢复、更新、有效期变更、停止使用、撤销、销毁等全生命周期的密钥管理制度，保障数据安全。

n）定义数据保护管理的考核指标和考核办法，并定期考核。

o）定期总结数据保护管理工作，在企业层面发布数据保护管理工作报告。

p）对重点数据的风险控制可落实到字段级，明确核心字段的保护等级和管控措施。

q）能主动防范数据风险，并对已发生的数据风险问题进行溯源和分析。

r）建设自动化工具或平台，实现对数据保护管理工作的自动化支持能力。

11.3 数据保护审计

11.3.1 概述

数据保护审计是一项控制活动，负责定期分析、验证、讨论、改进数据保护管理相关的策略、规范和活动。审计工作可由企业内部或外部审计人员执行，并且审计人员独立于审计所涉及的数据和流程。

11.3.2 工作措施

数据保护审计采取的工作措施包括但不限于：

a）评审数据保护规范与策略是否满足国家法律法规、金融行业规章制度要求，检查数据保护管理规范与策略是否能满足业务需要，以及数据保护管理的措施是否能按照数据保护管理规范与策略的要求进行。

b）在企业层面规范、统一数据保护审计的流程、相关文档模板和规范，并征求相关方意见。

c）制定数据保护审计计划，评审企业数据保护等级的划分情况，评审数据保护管理岗位、职责、流程的设置和保护审计计划的执行情况，定期发布数据保护审计报告。

d）针对合规性审计、日志审计、网络行为审计、主机审计、应用系统审计、集中操作运维审计分别提出要求，并开展审计工作。数据保护审计覆盖全部重要节点、环节、用户，审计内容包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的相关事件。

e）审计记录至少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。对审计数据、分析结果、审计结果（报告）进行保护，定期备份，避免受到意外删除、修改或覆盖等，留存时间符合法律法规等要求。

f）具备审计工具，对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行审计操作，并对这些操作进行审计。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。

g)对云服务提供者和云服务使用者在远程管理时执行的特权命令进行审计，至少包括虚拟机删除、虚拟机重启、管理员用户行为。

h）根据云服务提供者和云服务使用者的职责划分，实现各自控制部分的审计。

i）建立数据保护审计平台，在发现已定义的潜在风险时可实现自动报警或处置。

j）建立数据保护审计报告管理机制，并跟踪数据保护审计工作开展情况。

k）根据数据保护审计结果对数据保护的管理流程、制度进行优化提升，实现数据保护管理的闭环。

l）数据保护审计成为企业审计工作的重要组成部分，能有效推动数据保护规范和策略的优化及实施。

12 数据质量

12.1 数据质量需求

12.1.1 概述

数据质量需求是根据业务、数据需要制定的一种衡量数据质量的规则，是度量和管理数据质量的依据，包括技术指标、业务指标以及相应的校验方法。数据质量需求符合相关规范，依据数据管理目标、业务管理需求和行业监管要求统一制定和管理。

12.1.2 工作措施

数据质量需求采取的工作措施包括但不限于：

a）深入分析数据质量管理目标、范围、规则等，明确数据质量需求。

b）数据质量需求符合内部管理、行业监管、国家及金融行业标准规范等的相关要求。

c）制定数据质量需求统一模板，明确相关管理规范。

d）建立机制明确各类数据管理人员及相关职责，制定各类数据的优先级和质量管理需求。

e）设计统一的数据质量评价指标体系以及相应的规则库，数据质量评价指标体系的制定符合国家标准、金融行业相关规范。

f）将数据质量需求融入数据生命周期管理的各个阶段.能满足业务发展的需要。

g）定义并应用量化指标，衡量数据质量规则库运行的有效性，持续优化数据质量规则库。

12.2 数据质量检查

12.2.1 概述

数据质量检查是根据数据质量规则中的技术指标、业务指标、校验方法等对数据质量进行有效监控、发现问题并及时反馈的一种方法。

12.2.2 工作措施

数据质量检查采取的工作措施包括但不限于：

a）基于出现的数据问题，开展数据质量检查工作。

b）制定统一的数据质量检查管理制度、流程和工具，明确数据质

量检查的主要内容和方式，定义相关人员的职责。

c）明确各个阶段数据质量的检查点、检查模板，强化数据质量检查管理。

d）制定企业级的数据质量检查计划。

e）在企业层面统一开展数据质量的校验，帮助数据管理人员及时发现数据质量问题。

f）在企业层面建立数据质量问题发现、告警机制，明确数据质量责任人员。

g）采用技术手段开展数据核验，保障共享数据、监管报送数据等的一致性、完整性、真实性。

h）建立数据质量相关考核制度，明确数据质量考核的目标、范围和方法。

i）定义并应用量化指标对数据质量检查和问题处理过程进行有效分析，及时对相关制度和流程进行优化。

j）将数据质量管理纳入业务人员日常管理工作中，主动发现并解决相关问题。

12.3 数据质量分析

12.3.1 概述

数据质量分析作为数据质量提升的参考依据，通过对检查过程中发现的数据质量问题及相关信息进行分析，找出影响数据质量的原因，并定义数据质量问题的优先级。

12.3.2 工作措施

数据质量分析采取的工作措施包括但不限于：

a）基于出现的数据质量问题开展数据质量分析，明确数据质量问题原因和影响。

b）数据质量分析满足内部管理、行业监管等要求。

c）建立企业级的数据质量问题评估分析方法，制定统一的数据质量报告模板，明确数据质量问题分析的要求。

d）制定数据质量问题分析计划，定期进行数据质量问题分析。

e）对数据质量关键问题的根本原因、影响范围进行分析。

f）定期组织编制数据质量报告并发送至相关方。

g）建立数据质量分析案例库、知识库，提升人员对数据质最的关注度和理解度。

h）建立数据质量问题的效益评估模型，分析数据质量问题对机构效益的影响。

i）通过数据质量分析及时发现潜在的数据质量风险，预防数据质量问题的发生.

j）持续优化数据质量知识库。

k）通过数据质量分析提升人员的数据质量意识。

12.4 数据质量提升

12.4.1 概述

数据质量提升针对数据质量分析结果，制定实施数据质量改进和数据问题预防方案，确保数据质量改进工作有效落实。具体包括错误数据更正、业务流程优化、应用系统问题修复等。

12.4.2 工作措施

数据质量提升采取的工作措施包括但不限于：

a）建立数据质量整改机制。

b）建立企业层面的数据质量提升管理制度，明确数据质量提升方案的构成要素，指导数据质量提升工作。

c）明确数据质量提升的相关方及其职责，明确数据质量问题责任人，及时处理出现的问题，并提出相关建议。

d）结合相关方的诉求制定数据质量提升工作计划，并监督执行。

e）跟踪内部管理、行业监管等要求的变化，及时更新数据质量提升管理制度。

f）定期开展数据质量提升工作，对重点问题进行汇总分析，制定数据质量提升方案，避免相关问题的发生，形成良性循环。

g）对数据质量问题进行校正，建立数据质量跟踪记录。

h）根据数据质量分析，制定并实施数据质量问题预防方案。

i）持续开展培训和宣传，建立企业数据质量文化氛围。

j）企业中的管理人员、技术人员、业务人员能协同推动数据质量提升工作。

k）通过量化分析的方式对数据质量提升过程进行评估，并对管理过程和方法进行优化。

13 数据应用

13.1 数据分析

13.1.1 概述

数据分析是对企业各项经营管理活动提供数据决策支持而进行的数据挖掘、建模、成果交付推广等的活动，有助于促进业务发展。

13.1.2 工作措施

数据分析采取的工作措施包括但不限于：

a）具有专门的数据分析团队，统筹各部门数据分析需求。

b）在企业内部建立统一的数据分析与应用的管理办法，指导各部门数据分析工作。

c）形成统一的数据分析管理平台，数据分析结果能在各个部门之间复用，分析口径定义明确，可实现数据统一管理、按需调用。

d）建设企业统一报表平台，支持部门间及部门内部的常规报表分析和数据接口开发。

0）在风险管理、业务经营与内部控制中加强数据分析结果应用，实现数据驱动.

f）根据 JR/T 0171-2020 相关要求，建立个人金融信息滥用及泄露防范机制，对个人金融信息滥用行为与泄漏风险进行有效的识别、监控和预警。

g）建立分析结果评价方法，量化评价数据分析效果。

h）建立数据分析模型库，支持业务人员进行数据分析处理，并主动开展数据分析方法或模型等方面的自主创新，

i）运用数据仓库、数据挖掘、机器学习、数据可视化等技术方法，深入开展数据分析。

13.2 数据交换

13.2.1 概述

数据交换是指数据在企业内外部的流转交互，包括按一定策略引入外部数据供内部应用以及有选择地对外提供企业内部数据等。数据交换的主要目的是通过及时高效获取外部数据和安全合规分享内部数据，从而更好地发挥数据价值。开展数据交换需建立明确的交换曰录和策略，并做好交换合作方的管理。

13.2.2 工作措施

数据交换采取的工作措施包括但不限于：

a）数据交换满足数据保护等相关要求。

b）对数据交换实行统一管理，规范数据交换工作。

c）在企业层面制定统一的数据交换策略，指导数据交换实践.

d）在企业层面制定数据交换目录，便于内外部用户浏览、查询可供交换的数据。

e）根据需求更新完善数据交换目录。

f）加强对外部合作机构的管理，确认外部数据的合规性、完整性、真实性。

g）按照安全合规、专事专用、最小够用要求开展数据交换，对交换获得的数据未经许可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。

h）定期开展内部评估和外部意见收集，及时改进数据交换流程和策略，消除相关风险。

i）按照 JR/T0196-2020、JR/T0149-2016 等，积极运用多方安全计

算、标记化等技术，提升数据交换安全性。

13.3 数据服务

13.3.1 概述

数据服务是通过对企业内外部数据的统一加工和分析，结合公众、行业和企业的需要，以数据分析结果的形式提供服务。数据服务一般需经过需求分析、服务开发、服务部署、服务监控、用户管理等过程。

13.3.2 工作措施

数据服务采取的工作措施包括但不限于：

a）建立企业层面统一的数据服务申请、审核和监控制度。

b)制定数据服务管理相关的流程和策略，实现数据服务规范管理。

c）根据业务需求，设计对外提供的数据服务产品。

d）编制并发布统一的数据服务目录。

e）定期评估数据使用情况，并向相关方提供数据应用情况报告。

f）对数据服务进行状态监控、统计分析、服务管理、用户意见处理等。

g）对数据服务价值进行量化评估，持续提升数据服务质量。

14 数据生存周期管理

14.1 数据需求管理

14.1.1 概述

数据需求是指企业在业务运营、经营分析和战略决策过程中产生和使用数据的分类、含义、分布和流转相关要求的描述。

14.1.2 工作措施

数据需求管理采取的工作措施包括但不限于：

a）建记和执行规范化的数据需求收集、验证和汇总流程。

b）数据需求管理流程与信息化项目管理流程协调一致。

c）建立统一的数据需求管理模板，明确数据需求描述有关内容，

d）统筹各部门的数据需求，根据业务、管理等方面的要求制定数据需求的优先级。

e）开展数据需求评审，与相关方就数据优先级、应用范围、权责等内容达成共识。

f）记录、管理和维护业务流程与数据需求的匹配关系。

g）基于数据需求对数据规范和数据架构进行完善，增强三者之间的一致性。

h）建立数据需求变更管理流程，并对需求变更进行管理。

i）采取有效措施持续改善数据需求管理流程。

j）定义并应用量化指标，衡量数据需求管理的有效性。

14.2 数据开发管理

14.2.1 概述

数据开发是指设计实施数据解决方案、提供数据服务并持续满足企业数据需求的过程。数据解决方案包括数据结构设计、采集存储、整合交换、挖掘探索、可视化（报表、用户视图）等内容。

14.2.2 工作措施

数据开发管理采取的工作措施包括但不限于：

a）建立并执行规范化的数据开发流程。

b）建立数据开发规范、设计模板，指导数据开发。

c）建立并执行数据开发的质量规范、保护规范。

d）数据开发过程中参考权威数据源的设计，优化数据集成关系并进行评审。

e）明确数据供需双方职责，统一开展数据准备工作。

f）在数据解决方案中制定并执行数据权限管控，确保数据所有权、数据保护等得到有效保障。

g）数据开发能支撑数据战略的落地，有效促进数据的应用。

h）采取有效措施持续改善数据开发流程。

i）定义并应用量化指标，衡量数据开发流程的有效性。

14.3 数据维护管理

14.3.1 概述

数据维护是指数据服务上线投入运营后，对数据采集、数据处理、数据存储等日常的运行维护，保证数据正常服务的过程。

14.3.2 工作措施

数据维护管理工作措施包括但不限于：

a）建立并执行数据维护规范化管理方案和流程。

b）在数据采集环节，建立并执行规范化管理流程和规则，强化数据源管理。

c）在数据访问环节，制定并严格执行数据访问策略、涉密数据策略等，并对数据访问行为进行合规检测。

d）在数据处理环节，确保数据平台及相关数据服务安全高效运转，

能够及时响应各类数据提取、分析等需求。

e）在数据存储环节，按照授权方式存储数据并在数据保存期限内做好数据保护，禁止擅自留存未经授权的数据。

f）定期生成并发布数据维护管理工作报告。

g）采取有效措施持续改善数据维护管理方案和流程。

h）定义并应用量化指标，衡量数据维护管理工作的有效性。

14.4 历史数据管理

14.4.1 概述

历史数据管理是指根据法律法规、行业监管要求，以及业务、技术等方面的需求对历史数据进行归档、迁移、销毁等。

14.4.2 工作措施

历史数据管理采取的工作措施包括但不限于：

a）满足内部管理、行业监管等对历史数据的管理要求。

b）制定统一的历史数据定义规范和处置规范，对历史数据进行准确定位，合法合规确定处置方式。

c）结合业务需求对不同历史数据建立并执行符合处置规范的管理策略，提升数据访问性能，降低数据存储成本，保证数据的安全。

d）历史数据的处置需科学、合理，无纰漏、无隐患。

e）实施数据处理方案过程中，进行全流程记录和重要节点监督，对数据销毁等处置落实到多人并相互监督。

f）对于保留的历史数据，定期开展数据可用性和可恢复性验证。

g）建立历史数据恢复请求审批机制，规范历史数据的恢复管理。

h）采取有效措施持续改善历史数据管理策略。

i）定义并应用量化指标，衡量历史数据管理的有效性。

GB/T39335-2020 信息安全技术 个人信息安全影响评估指南

时效性：　　现行有效

发布机关：　国家市场监督管理总局、国家标准化管理委员会

类别：　　中华人民共和国国家标准

实施日期：　2021 年 6 月 1 日

1 范围

本标准给出了个人信息安全影响评估的基本原理、实施流程。

本标准适用于各类组织自行开展个人信息安全影响评估工作，同时可为主管监管部门、第三方测评机构等组织开展个人信息安全监督、检查、评估等工作提供参考。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB／T 20984 信息安全技术 信息安全风险评估规范

GB／T 25069-2010 信息安全技术 术语

GB／T 35273-2020 信息安全技术 个人信息安全规范

3 术语和定义

GB／T 25069-2010、GB／T35273-2020 界定的以及下列术语和定义适用于本文件。

3.1

个人信息 personal information

以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息。

［GB / T 35273-2020，定义 3.1］

3.2

个人敏感信息 personal sensitive information

一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息。

［GB / T 35273-2020，定义 3.2］

3.3

个人信息主体 personal information subject

个人信息所标识或者关联的自然人。

［GB / T 35273-2020，定义 3.3］

3.4

个人信息安全影响评估 personal information security impact assessment

针对个人信息处理活动，检验其合法合规程度，判断其对个人信息主体合法权益造成损害的各种风险，以及评估用于保护个人信息主体的各项措施有效性的过程。

4 评估原理

4.1 概述

个人信息安全影响评估旨在发现、处置和持续监控个人信息处理过程中对个人信息主体合法权益造成不利影响的风险。

4.2 开展评估的价值

实施个人信息安全影响评估，能够有效加强对个人信息主体权益的保护，有利于组织对外展示其保护个人信息安全的努力，提升透明度，增进个人信息主体对其的信任。包括：

a)在开展个人信息处理前，组织可通过影响评估，识别可能导致个人信息主体权益遭受损害的风险，并据此采用适当的个人信息安全控制措施。

b)对于正在开展的个人信息处理，组织可通过影响评估，综合考虑内外部因素的变化情况，持续修正已采取的个人信息安全控制措施，确保对个人合法权益不利影响的风险处于总体可控的状态。

c)个人信息安全影响评估及其形成的记录文档，可帮助组织在政府、相关机构或商业伙伴的调查、执法、合规性审计等中，证明其遵守了个人信息保护与数据安全等方面的法律、法规和标准的要求。

d)在发生个人信息安全事件时，个人信息安全影响评估及其形成的记录文档，可用于证明组织已经主动评估风险并采取一定的安全保护措施，有助于减轻、甚至免除组织相关责任和名誉损失。

e)组织可通过个人信息安全影响评估，加强对员工的个人信息安全教育。参与评估之中，员工能熟悉各种个人信息安全风险，增强处置风险的能力。

f)对合作伙伴，组织通过评估的实际行动表明其严肃对待个人信息安全保护，并引导其能够采取适当的安全控制措施，以达到同等或类似的安全保护水平。

4.3 评估报告的用途

个人信息安全影响评估报告的内容主要包括：评估所覆盖的业务场景、业务场景所涉及的具体的个人信息处理活动、负责及参与的部门和人员、已识别的风险、已采用及拟采用的安全控制措施清单、剩余风险等。

因此，个人信息安全影响评估报告的用途包括但不限于：

a）对于个人信息主体，评估报告可确保个人信息主体了解其个人信息被如何处理、如何保护，并使个人信息主体能够判断是否有剩余风险尚未得到处置。

b）对于开展影响评估的组织，评估报告的用途可能包括：

1)在产品、服务或项目的规划阶段，用于确保在产品或服务的设计中充分考虑并实现个人信息的保护要求（例如，安全机制的可实现性、可行性、可追踪性等）；

2)在产品、服务或项目的运营过程中，用于判断运营的内外部因素（例如运营团队的变动、互联网安全环境、信息共享的第三方安全控制能力等）、法律法规是否发生实质变更，是否需要对影响评估结果进行审核和修正；

3)用于建立责任制度，监督发现存在安全风险的个人信息处理活动是否已采取安全保护措施，改善或消除已识别的风险；

4)用于提升内部员工的个人信息安全意识。

c)对于主管监管部门，要求组织提供个人信息安全影响评估报告，可督促组织开展评估并采取有效的安全控制措施。在处理个人信息安

全相关投诉、调查个人信息安全事件等时，主管监管部门可通过影响评估报告了解相关情况，或将报告作为相关证据。

d)对于开展影响评估的组织的合作伙伴，用于整体了解其在业务场景中的角色和作用,以及其应具体承担的个人信息保护工作和责任。

4.4 评估责任主体

组织指定个人信息安全影响评估的责任部门或责任人员，由其负责个人信息安全影响评估工作流程的制定、实施、改进，并对个人信息安全影响评估工作结果的质量负责。该责任部门或人员具有独立性，不受到被评估方的影响。通常，组织内部牵头执行个人信息安全影响评估工作的部门为法务部门、合规部门或信息安全部门。

组织内的责任部门可根据部门的具体能力配备情况，选择自行开展个人信息安全影响评估工作，或聘请外部独立第三方来承担具体的个人信息安全影响评估工作。

对于具体的产品、服务或项目，由相应的产品、服务或项目负责人确保个人信息安全影响评估活动的开展和顺利进行，并给予相应支持。

当由组织自行进行个人信息安全影响评估时，主管监管部门和客户可要求独立审计来核证影响评估活动的合理性和完备性。同时，该组织允许主管监管部门对影响评估流程以及相关信息系统或程序进行取证。

4.5 评估基本原理

个人信息安全影响评估的基本原理如图 1

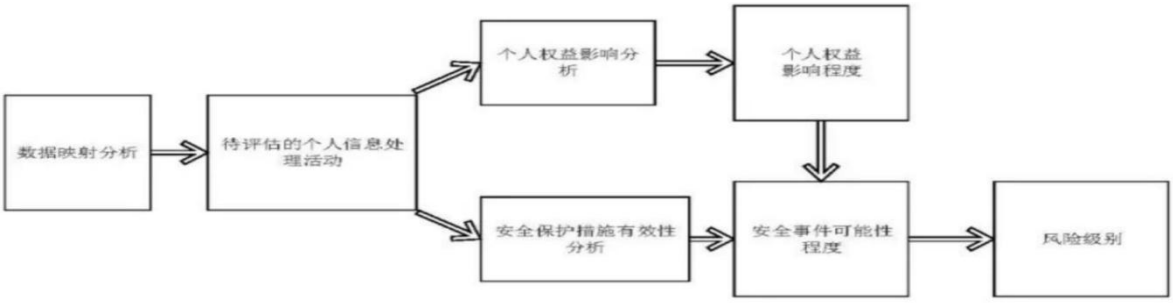


图 1 评估原理示意图

开展评估前，需对待评估的对象（可为某项产品、某类业务、某项具体合作等）进行全面的调研，形成清晰的数据清单及数据映射图表（data flow charts），并梳理出待评估的具体的个人信息处理活动。开展评估时，通过分析个人信息处理活动对个人信息主体的权益可能造成的影响及其程度，以及分析安全措施是否有效、是否会导致安全事件发生及其可能性，综合两方面结果得出个人信息处理活动的安全风险及风险等级，并提出相应的改进建议，形成评估报告。

4.6 评估实施考虑的要素

4.6.1 评估规模

个人信息安全影响评估的规模往往取决于受到影响的个人信息主体范围、数量和受影响的程度。通常，组织在实施该类个人信息安全影响评估时，个人信息的类型、敏感程度、数量，涉及个人信息主体的范围和数量，以及能访问个人信息的人员范围等，都会成为影响评估规模的重要因素。

4.6.2 评估方法

评估实施过程中采用的基本评估方法，包括但不限于以下三种：

a）访谈：指评估人员对相关人员进行谈话，以对信息系统中个人信息的处理、保护措施设计和实施情况进行了解、分析和取证的过程。访谈的对象包括产品经理、研发工程师、个人信息保护负责人、法务负责人员、系统架构师、安全管理员、运维人员、人力资源人员和系统用户等。

b) 检查：指评估人员通过对管理制度、安全策略和机制、合同协议、安全配置和设计文档、运行记录等进行观察、查验、分析，以便理解、分析或取得证据的过程。检查的对象为规范、机制和活动，如个人信息保护策略规划和程序、系统的设计文档和接口规范、应急规划演练结果、事件响应活动、技术手册和用户／管理员指南、信息系统的硬件／软件中信息技术机制的运行等。

c) 测试：指评估人员通过人工或自动化安全测试工具进行技术测试，获得相关信息，并进行分析以便获取证据的过程。测试的对象为安全控制机制，如访问控制、身份识别和验证、安全审计机制、传输链路和保存加密机制、对重要事件进行持续监控、测试事件响应能力、以及应急规划演练能力等。

4.6.3 评估工作形式

从实施主体来区分，个人信息安全影响评估分为自评估和检查评估两种形式。

自评估是指组织自行发起对其个人信息处理行为的评估，自评估可以由本组织指定专门负责评估、审计的岗位或角色开展，也可以委托外部专业组织开展评估工作。

检查评估是指组织的上级组织发起的个人信息安全影响评估工作。上级组织是对组织有直接领导关系或负有监督管理责任的组织。检查评估也可以委托外部专业组织开展评估。

在确定评估规模，选定评估方法、评估工作形式后，评估实施的具体流程可参照第 5 章内容。

5 评估实施流程

5.1 评估必要性分析

5.1.1 概述

个人信息安全影响评估可用于合规差距分析，也可以用于合规之上、进一步提升自身安全风险管理能力和安全水平的目的。因此启动个人信息安全影响评估的必要性，取决于组织的个人信息安全目标，组织可根据实际的需求选取需要启动评估的业务场景。

5.1.2 合规差距评估

5.1.2.1 概述

当组织定义的个人信息安全目标为符合相关法律、法规或标准的基线要求时，则个人信息安全影响评估主要目的在于识别待评估的具体个人信息处理活动已采取的安全控制措施，与相关法律、法规或标准的具体要求之间的差距。例如在某业务场景中与第三方共享个人信息，是否取得了个人信息主体的明示同意。

5.1.2.2 整体合规分析

组织可根据所适用的个人信息保护相关法律、法规、政策及标准，分析特定产品或服务所涉及的全部个人信息处理活动与所适用规则的

差距。该评估方式的应用场景包括但不限于以下情形：

a）产品或服务的年度整体评估；

b）新产品或新服务（不限技术平台）设计阶段评估；

c）新产品或新服务（不限技术平台）上线初次评估；

d）法律法规、政策、标准等出现重大变化时重新评估；

e）业务模式、互联网安全环境、外部环境等发生重大变化的重新评估；

f）发生重大个人信息安全事件后重新评估；

g）发生收购、兼并、重组等情形开展评估。

5.1.2.3 局部合规分析

组织可根据所适用的个人信息保护相关法律、法规、政策及标准，对特定产品或服务所涉及的部分个人信息处理活动与所适用规则的差距进行分析。该评估方式的应用场景包括但不限于以下情形：

a）新增功能需要收集新的个人信息类型时的评估；

b）法律、法规、政策、标准出现部分变化时的评估；

c）业务模式、信息系统、运行环境等发生变化时评估。

5.1.2.4 评估性合规要求分析

部分个人信息保护相关的法律、法规、标准的规定提出了评估性合规要求。这类规定并没有针对特定的个人信息处理活动提出明确、具体的安全控制措施，而是要求组织对特定个人信息处理活动，专门开展风险评估，并采取与风险程度相适应的安全控制措施，将对个人信息主体合法权益不利影响的风险降低到可接受的程度，才符合其规

定。

评估性合规要求往往针对的是对个人权益有重大影响的个人信息处理活动，例如处理个人敏感信息、使用自动化决策方式处理个人信息、委托处理个人信息、向第三方转让或共享个人信息、公开披露个人信息、向境外转移个人信息等。

针对此类规定，组织可使用本指南提供的个人信息安全影响评估方法进行评估，保证个人信息处理活动的安全风险可控，以符合相应的法律、法规、标准的要求[1]。

5.1.3 尽责性风险评估

出于审慎经营、声誉维护、品牌建立等目的，组织往往选取可能对个人合法权益产生高风险的个人信息处理活动，开展尽责性风险评估。此种风险评估的目标，是在符合相关法律、法规和标准的基线要求之上，尽可能降低对个人信息主体合法权益的不利影响[2]。

组织可使用本指南提供的个人信息安全影响评估方法，对高风险个人信息处理活动进行评估，进一步降低个人信息处理活动的安全风险。

5.2 评估准备工作

5.2.1 组建评估团队

组织确认并任命负责进行个人信息安全影响评估的人员（评估人）。此外，组织还要指定人员负责签署评估报告。

---

[1] 注：评估性合规要求分析示例及具体评估要点可参考附录 A。

[2] 注：高风险个人信息处理活动示例可参考附录 B。

评估人明确规定个人信息安全影响评估报告的提交对象、个人信息安全影响评估的时间段、是否会公布评估报告或其摘要。

如有必要评估人需申请团队支持，例如由技术部门、相关业务部门及法律部门的代表构成的团队。组织内部个人信息安全影响评估需要组织管理层给予长期支持。

管理层需为个人信息安全影响评估团队配置必要资源。

5.2.2 制定评估计划

计划需清楚规定完成个人信息安全影响评估报告所进行的工作、评估任务分工、评估计划表。此外，计划还需考虑到待评估场景中止或撤销的情况。具体操作时考虑以下方面：

a）人员、技能、经验及能力；

b）执行各项任务所需时间；

c）进行评估每一步骤所需资源，如自动化的评估工具等[1]。

如涉及相关方咨询，计划需说明在何种情况下需要咨询相关方、将咨询哪些人员、以及具体的咨询方式（例如通过公众意见调查、研讨会、焦点小组、公众听证会、线上体验等等）。

5.2.3 确定评估对象和范围

从以下三个方面描述评估的对象和范围：

a）描述系统基本信息，包括但不限于：

1）处理个人信息的目的和类型；

[1] 注：涉及的场景复杂、耗用资源多时，建议对原有方案进行更新迭代，针对常规评估活动或涉及待评估场景复杂度低等情形时，可沿用原有计划或简化该步骤。

2）对支撑当前或未来业务流程的信息系统的描述；

3）履行信息系统管理职责的部门或相关人员，以及其职责或履行水平；

4）关于个人信息处理方式、处理范围的说明、有权访问个人信息的角色等；

5）如预计委托第三方处理，或与第三方共享、转让信息系统的个人信息，说明上述第三方身份、第三方接入信息系统的情况等。

b）描述系统设计信息，包括但不限于：

1）功能（或逻辑）结构概览；

2）物理结构概览；

3）包含个人信息的信息系统数据库、表格和字段的清单和结构；

4）按组件和接口划分的数据流示意图；

5）个人信息生命周期的数据流示意图，例如个人信息的收集、存储、使用和共享等；

6）描述通知个人信息主体的时间节点、以及取得个人信息主体同意的时间节点和工作流程图；

7）可对外传输个人信息的接口清单；

8）个人信息处理过程中的安全措施。

c）描述处理流程和程序信息，包括但不限于：

1）信息系统的身份与用户管理概念；

2）操作概念，包括信息系统或其中部分结构采用现场运行、外部托管、或云外包的方式；

3）支持概念，包括列示可访问个人信息的第三方范围、其所拥有的个人信息访问权限、其可访问个人信息的位置等；

4）记录概念，包括已登入信息的保存计划；

5）备份与恢复计划；

6）元数据的保护与管理；

7）数据保存与删除计划及存储介质的处置。

5.2.4 制定相关方咨询计划

相关方包括但不限于：

员工，例如人力资源、法律、信息安全、财务、业务运营职能、通信与内部审计（尤其是在监管环境下）相关人员；

个人信息主体和消费者代表；

分包商和业务合作伙伴；

系统开发和运维人员；

对于评估有相应担忧的其他组织人员。

为保证评估流程的透明，实现降低安全风险的目标，评估人需详细确认进入评估程序的内部或外部相关方。相关方与待评估的个人信息处理活动具有直接的利益关系，相关方可以是拥有或可能获取个人信息访问权限的组织或个人。

评估人需确认相关方的分类，然后具体确认各类相关方中的特定组织或个人。如果相关方为个人，则该个人宜尽可能具有代表性。

个人信息的范围与规模，以及业务重要性、成本收益等因素，对于确定恰当的相关方非常重要。如对大型个人信息处理活动进行评估，

则可能存在较多相关方。在这种情况下，社会团体（如消费者权保护组织）可能被确认为相关方。相反，一些小型评估，可能不需要确认宽泛的相关方清单。

制定咨询计划需明确不同的相关方所受的影响、后果(如果已知)、以及所采取的用于降低不利影响的安全控制措施等相关问题。计划中还包含咨询范围及计划表。

咨询计划的目标包括但不限于：

a）确定相关方的数量与范围；

b）相关方参与识别并评估个人权益影响及安全风险的具体方式[1]；

c）就评估报告咨询相关方意见以确认报告是否充分反映他们对有关问题的关注。

组织在开展个人信息安全影响评估时,可以督促适当的相关方(主要包括分包商和业务合作伙伴）开展个人信息安全影响评估。适当的相关方有义务开展个人信息安全影响评估，或者配合组织开展个人信息安全影响评估，组织可以引用相关方的个人信息安全影响评估报告作为咨询结果。

5.3 数据映射分析

组织在针对个人信息处理过程进行全面的调研后，形成清晰的数据清单及数据映射图表。

数据映射分析阶段需结合个人信息处理的具体场景。调研内容包

[1] 注：相关方的反馈意见所提出的问题可能与主观风险认识有关、而非客观实际风险，但不能忽略这些意见，组织可将这些意见放在更广泛的相关方管理问题中进行处理，为交流活动提供帮助。

括个人信息收集、存储、使用、转让、共享、删除等环节涉及的个人信息类型、处理目的、具体实现方式等，以及个人信息处理过程涉及的资源（如内部信息系统）和相关方（如个人信息处理者、平台经营者、外部服务供应商、云服务商等第三方）。调研过程中尽可能考虑已下线系统、系统数据合并、企业收购、并购及全球化扩张等情况。

梳理数据映射分析的结果时，根据个人信息的类型、敏感程度、收集场景、处理方式、涉及相关方等要素，对个人信息处理活动进行分类，并描述每类个人信息处理活动的具体情形，便于后续分类进行影响分析和风险评价。

注：开展数据映射分析，可参考附录C中表C．1和表C．2。

5.4 风险源识别

风险源识别是为了分析个人信息处理活动面临哪些威胁源，是否缺乏足够的安全措施，导致存在脆弱性而引发安全事件。决定个人信息安全事件发生的要素很多，就威胁源而言，有内部威胁源，也有外部威胁源，有恶意人员导致的数据被窃取等事件，也有非恶意人员无意中导致的数据泄露等事件；就脆弱性而言，有物理环境影响导致的数据毁损，有技术因素导致的数据泄露、篡改、丢失等事件，也有管理不当引起的滥用等事件。

GB／T 20984 中所描述的威胁识别和脆弱性识别方法均可用于对个人信息安全事件的分析过程。为进一步简化个人信息安全事件可能性的分析过程，将与个人信息安全事件可能性相关的要素归纳为以下四个方面：

a）网络环境和技术措施。评估时关注的要素包括但不限于：

1) 处理个人信息的信息系统所处网络环境为内部网络还是互联网，不同的网络环境其面临的威胁源不同，连接互联网的信息系统面临的风险更高；

2) 处理个人信息的信息系统与其他系统的交互方式，比如是否采用网络接口进行数据交互,是否嵌入可收集个人信息的第三方代码、插件等，通常情况下数据交互越多，需采取更加全面的安全措施防止信息泄露、窃取等风险；

3) 个人信息处理过程中是否实施严格的身份鉴别、访问控制等措施；

4) 是否在网络边界部署了边界防护设备，配置了严格的边界防护策略，实施了数据防泄露技术措施；

5) 是否监测和记录网络运行状态，是否标记、分析个人信息在内部或与第三方交互时的状态，及时发现异常流量和违规使用情况；

6) 是否采取了防范病毒和木马后门攻击、端口扫描、拒绝服务攻击等网络入侵行为的技术措施；

7) 是否采用加密传输、加密存储等措施对个人敏感信息进行额外保护；

8) 是否对个人信息收集、保存、传输、使用、共享等各阶段的个人信息处理活动进行审计，并对异常操作行为进行报警；

9) 是否建立了完备的网络安全事件预警、应急处置、报告机制；

10）是否对信息系统进行定期安全检查、评估、渗透测试，并及

时进行补丁更新和安全加固；

11）是否对数据存储介质加强安全管理，是否具备对数据进行备份和恢复的能力。

12）其他必要的网络安全技术保障措施[1]。

b) 个人信息处理流程。评估时关注的要素包括但不限于：

1）个人敏感信息的判定是否准确；

2）收集个人信息的目的是否正当、合法；

3）从第三方获得的数据是否得到正式的处理授权；

4）告知方式和告知的内容是否友好可达，是否所有的处理活动都征得了用户同意；

5)是否定义了个人信息最小元素集,是否超范围收集了个人信息；

6) 变更个人信息使用目的是否对个人信息主体产生影响；

7）是否提供便捷有效的个体参与的机制，包括查询、更正、删除、撤回同意、注销账号等；

8) 接收个人信息的第三方是否会变更目的使用个人信息；

9) 个人信息的保存时间是否最小化，超出期限的删除等机制是否合理；

10）是否对用户画像机制进行限制，避免精确定位到特定个人；

11）是否为个性化展示提供用户可控制、可退出或关闭的机制；

12）匿名化机制是否有效，去标识化后的个人信息是否能够被关

[1] 注：如果组织参照其他网络安全、数据安全相关国家标准建立成熟的安全防护体系，可基于其已有基础进行分析评估。

联分析等，导致可重新识别个人信息主体身份；

13）是否提供及时有效的安全事件通知机制和应急处置机制；

14）是否提供有效的投诉和维权渠道等；

15）是否未经用户同意向第三方共享、转让个人信息：

16）是否散播不准确的数据或不完整的误导性数据；

17）是否诱导或强迫个人提供过多个人信息；

18）是否过多地追踪或监视个人行为；

19）是否无根据地制个人控制其个人信息的行为等；

20）其他个人信息处理流程的规范性[1]。

c）参与人员与第三方。评估时关注的要素包括但不限于：

1）是否任命个人信息保护负责人或个人信息保护工作机构，个人信息保护负责人是否由具有相关管理工作经历和个人信息保护专业知识的人员担任；

2）是否依据业务安全需求，制定并执行个人信息安全管理的方针和策略；

3) 是否制定涉及个人信息处理各环节的安全管理制度，并提出具体的安全管理要求；

4) 是否与从事个人信息处理岗位上的相关人员签署保密协议，并对大量接触个人敏感信息的人员进行背景审查；

5) 是否明确内部涉及个人信息处理不同岗位的安全职责，并建立发生安全事件的处罚、问责机制；

[1] 注：对个人信息处理流程规范性的分析可参照 GB / T 35273-2020 相应内容。

6) 是否对个人信息处理岗位上的相关人员开展个人信息安全专业化培训和考核，并确保相关人员熟练掌握隐私政策和相关规程；

7) 是否明确可能访问个人信息的外部服务人员需遵守的个人信息安全要求，并进行监督；

8) 是否与第三方签署有约束力的合同等文件，约定个人信息传输至第三方后的处理目的、方式、数据留存期限、超出期限后的处理方式；

9）是否对第三方处理个人信息的行为进行定期检查、审计，确保其严格执行合同等约定；

10）其他方面的必要措施[1]。

d) 业务特点和规模及安全态势。评估时关注的要素包括但不限于：

1）业务对个人信息处理的依赖性；

2）业务处理或可能处理个人信息的数量、频率、用户规模、用户峰值等；

3）是否曾经发生过个人信息泄露、篡改、毁损、丢失等事件；

4）个人信息保护相关执法监管动态；

5）近期内遭受网络攻击或发生安全事件的情况；

6）近期收到过或公开发布的安全相关的警示信息。

组织在对以上维度的相应内容进行充分了解后，通过调研访谈、

[1] 注：如果组织参照其他网络安全、数据安全相关国家标准建立成熟的安全管理体系，可基于其已有基础进行分析评估。

查阅支撑性文档、功能检查、技术测试等方式，识别已采取的措施与当前的状态。针对 5.5 中对个人权益影响分析的不同维度，从以上四方面对安全事件发生的可能性等级进行综合评价[1]。

5.5 个人权益影响分析

5.5.1 个人权益维度

个人权益影响分析指分析特定的个人信息处理活动是否会对个人信息主体合法权益产生影响，以及可能产生何种影响。个人权益影响概括可分为“限制个人自主决定权”“引发差别性待遇”“个人名誉受损或遭受精神压力”“人身财产受损”四个维度：

a）限制个人自主决定权。例如被强迫执行不愿执行的操作、缺乏相关知识或缺少相关渠道更正个人信息、无法选择拒绝个性化广告的推送、被蓄意推送影响个人价值观判断的资讯等；

b) 引发差别性待遇。例如因疾病、婚史、学籍等信息泄露造成的针对个人权利的歧视；因个人消费习惯等信息的滥用而对个人公平交易权造成损害等；

c) 个人名誉受损或遭受精神压力。例如被他人冒用身份、公开不愿为人知的习惯、经历等，被频繁骚扰、监视追踪等；

d) 人身财产受损。例如引发人身伤害、资金账户被盗、遭受诈骗、勒索等。

5.5.2 个人权益影响分析过程

组织可根据数据映射分析结果及确定需要评估的个人信息处理活

[1] 注：安全事件可能性等级评估可参考附录 D 中 D．1。

动，结合相关法律、法规、标准的要求或组织自定义的个人信息安全目标，分析个人信息处理活动全生命周期或特定处理行为对个人权

益可能产生的影响，以及个人信息泄露、毁损、丢失、滥用等对个人权益可能产生的影响，以审视是否存在侵害个人信息主体权益的风险。

个人权益影响分析过程一般包含对个人信息敏感程度分析、个人信息处理活动特点分析、个人信息处理活动问题分析以及影响程度分析四个阶段：

a）在个人信息敏感程度分析阶段，组织可参照国家有关法律、法规、标准，依据数据映射分析结果，分析个人信息的敏感程度对个人权益可能产生的影响。例如健康生理信息的泄露、滥用等可能会对个人生理、心理生较严重的影响；

b) 在个人信息处理活动特点分析阶段，组织可参照与国家有关法律、法规、标准，依据数据映射分析结果，分析个人信息处理活动是否涉及限制个人自主决定权、引发差别性待遇、个人名誉受损或遭受精神压力、人身财产受损等。例如公开披露个人经历的行为可能会对个人声誉产生影响；

c) 在个人信息处理活动问题分析阶段，组织可参照与国家有关法律、法规、标准，依据数据映射分析结果，分析个人信息处理活动可能存在的弱点、差距和问题，其中 5.4b）中的对个人信息流程规范性的分析结果可以支撑该阶段的分析过程，对问题严重程度的分析有助于分析个人权益的影响程度；

d) 在个人权益影响程度分析阶段，组织可结合前几个阶段的分析结果，综合分析个人信息处理活动对个人权益可能造成的影响，及其严重程度[1]。

5.6 安全风险综合分析

进行安全风险综合分析时，可参照 4.5 中的基本原理，采取以下步骤：

a）参照 5.4，分析已实施的安全措施、相关方、处理规模等要素，评价安事件发生的可能性等级；

b) 参照 5.5，分析可能发生的安全事件会对个人权益产生何种影响，并评价对个人权益影响的度等级；

c）综合考虑安全事件可能性和个人权益影响程度两个要素，综合分析得出个人信息处理活动的安全风险等级[2]。

在完成针对特定个人信息处理活动影响评估之后，组织可综合针对所有相关个人信息处理活动的评估结果，形成对整个评估对象（如业务部门、具体项目、具体合作等）的风险等级。

5.7 评估报告

评估报告的内容通常包括：个人信息保护专员的审批页面、评估报告适用范围、实施评估及撰写报告的人员信息、参考的法律、法规和标准、个人信息影响评估对象（明确涉及的个人敏感信息）、评估

[1] 注：个人权益影响程度评估可参考附录 D 中 D．2。

[2] 注：安全风险分析的具体过程和风险等级的判定可参考附录 D 中 D．3，安全风险分析的具体过程可参考使用附录 C 中表 C．3、表 C．4 和表 C．5。

内容、涉及的相关方等，以及个人权益影响分析结果，安全保护措施分析结果、安全事件发生的可能性分析结果、风险判定的准则、合规性分析结果、风险分析过程及结果、风险处置建议等。

5.8 风险处置和持续改进

根据评估结果，组织可选取并实施相应的安全控制措施进行风险处置。通常情况下，可根据风险的等级，采取立即处置、限期处置、权衡影响和成本后处置，接受风险等处置方式。

组织需持续跟踪风险处置的落实情况，评估剩余风险，将风险控制在可接受的范围内。此外，还可将评估结果用于下一次个人信息安全影响评估工作。

5.9 制定报告发布策略

为促进自身持续提升个人信息保护水平、配合监管活动、增加客户信任，组织可制定个人信息安全影响评估报告发布策略。选择公开发布的个人信息安全影响评估报告可以在已有评估报告基础上予以简化，但其内容通常不少于以下方面：

a）收集和处理个人信息的类型和必要性；

b）收集和处理的个人信息类型（个人敏感信息需单独强调）；

c）个人信息处理的例外情况（法律法规规定等）；

d）合规性分析的概况；

e）评估过程和结果概况；

f）已实施和将要实施的风险处置措施概况；

g）对个人信息主体的建议；

h）实施评估责任部门和人员的联系方式和解答疑问的渠道等。

附录 A

（资料性附录）

评估性合规的示例及评估要点

A．1 概述

常见的个人信息相关法律、法规、标准中评估性合规要求，包括处理个人敏感信息、使用自动化决策方式处理个人信息、委托处理个人信息、向第三方转让或共享个人信息、公开披露个人信息、向境外转移个人信息、个人信息处理目的变更评估、个人信息匿名化和去标识化效果评估，以及确定个人信息安全事件处置方案的评估等，其中部分评估要点示例如下。

A．2 个人信息出境安全评估

个人信息出境场景的评估可参照有关国家标准执行。

A．3 个人信息处理目的变更前的影响评估

分析个人信息处理活动的影响时，需要考虑多种因素，以评估“与收集个人信息时所声称的目的具有直接或合理关联的范围”的影响为例，如果新设目的与原目的有直接或合理的关联，且不会为个人权益带来额外影响，无需再次告知个人信息主体并征得其明示同意。判断时是否有直接或合理的关联，至少需要考虑如下因素：

个人信息主体对原先目的、组织处理个人信息方式和方法的合理性的理解程度；

个人信息收集时的场景，包括个人信息主体和组织之间的关系、产品或服务的范围及使用的商标和名称、个人信息主体使用产品或服

务的方式、产品或服务为个人信息主体提供的便利等；

特定场景中可合理预期的个人信息处理方式，如常规商业运营中，可预见到的将被使用的个人信息的类型，与个人信息主体之间直接互动的范围、频率、性质、历史，以及为提供产品或服务，或改进或推广产品或服务，可预见到的将被使用的个人信息的类型。

如将所收集的个人信息用于学术研究或得出对自然、科学、社会、经济等现象总体状态的描述，属于与收集目的具有合理关联的范围之内。但对外提供学术研究或描述的结果时，需对结果中所包含的个人信息进行去标识化处理，否则在对目的变更后的影响评估中可能会得出存在高风险的判断。

A．4 个人信息匿名化和去标识化效果评估

匿名化和去标识化对个人信息进行了技术处理，使其在不借助额外信息的情况下，无法识别个人信息主体。但数据接收方可能会借助于额外的信息以及技术手段，进行重标识攻击，从而将去标识化的数据集归因到原始个人信息主体或一组个人信息主体。

常见的用于重标识的方法如下：

筛选：基于是否能唯一确定一个个人信息主体，将属于一个个人信息主体的记录筛选出来；

关联：将不同数据集中关于相同个人信息主体的信息关联；

推断：通过其它属性的值以一定概率推断出一个属性的值。

评估个人信息匿名化和去标识化效果时，可充分考虑以下要素：

个人信息匿名化和去标识化过程的规范性，所采用技术的通用性；

匿名化后的个人信息是否为统计型结果；

去标识化后的个人信息是否能够达到使用目的；

匿名化和去标识化后的个人信息使用场景；

如委托第三方进行去标识化或匿名化时，需评估其采用的方案及数据安全保障能力；

能否在公开渠道或数据交易组织获得类似的个人信息；

未经去标识化或匿名化处理保留的个人信息类型和内容的特殊性。

A．5 个人信息委托处理、转让、共享或公开披露前的影响评估

在对个人信息进行委托处理、转让、共享和公开披露前，开展个人信息安全影响评估，评估的内容包括但不限于以下方面：

个人信息的类型、数量、敏感程度等；

是否向个人信息主体告知了转让、共享、公开披露的基本情况，并征得个人信息主体的明示授权同意；

数据发送方的安全管理保障和安全技术保障能力；

数据接收方的安全管理保障和安全技术保障能力（不包括公开披露）；

数据接收方可能会开展的个人信息处理活动，或公开披露的个人信息可能会被使用的个人信息处理场景；

个人信息是否进行过去标识化处理；

发生个人信息安全事件后的补救措施；

数据接收方所能响应个人信息主体的请求的范围，如：访问、更

正、删除等。

A．6 确定个人信息安全事件处置方案的评估

发生个人信息安全事件后,组织需及时评估事件可能造成的影响,并采取必要措施控制事态，消除隐患。评估影响时，可充分考虑以下因素：

个人信息的类型、数量、敏感程度、涉及的个人信息主体数量等；

发生事件的信息统状况，对其他互联系统的影响；

已采取或将要采取的处置措施及措施的有效性；

对个人信息主体权益造成的直接影响和长期影响；

向个人信息主体告知事件的方式和内容；

是否达到《国家网络安全事件应急预案》等有关规定的上报要求。

A．7 使用自动化决策方式处理个人信息的评估

组织在设计、采用自动化决策方式处理个人信息时，如自动决定个人征信及贷款额度，或用于面试人员的自动化筛选等，需充分考虑对个人权益产生的不利影响，并在在规划设计阶段或首次使用前开展个人信息安全影响评估，评估考虑的要素包括：

是否向用户说明了自动化决策的基本原理或运行机制；

是否定期对自动化决策的效果进行评价；

是否对自动化决策使用的数据源、算法等持续优化；

是否向用户提供针对自动化决策结果的投诉渠道；

是否支持对自动化决策结果的人工复核。

附录 B

（资料性附录）

高风险的个人信息处理活动示例

个人信息处理活动自身可能涉及对个人信息主体权益影响及相应风险较高的情况下，需开展个人信息安全影响评估，可能产生高风险的个人信息处理活动及场景示例见表 A．1。

表 B．1 高风险的个人信息处理活动及场景示例

个人信息处理活动	场景示例
a）数据处理涉及对个人信息主体的评价或评分，特别是对个人信息主体的工作表现、经济状况、健康状况、偏好或兴趣的评估或预测；	示例 1：对个人信息主体使用社交网络和其他应用程序的行为进行分析，以便向其发送商业信息或垃圾邮件。示例 2：银行或其他金融组织在提供贷款前使用人工智能算法对个人信息主体进行信用评估，数据处理可能涉及与信用评估没有直接关联的个人信息。示例 3：保险公司通过分析香烟、酒精、极限运动、驾驶等偏好数据，评估个人信息主体的生活方式、健康状况等，据此作出保费设置的决策。
b）使用个人信息进行自动分析给出司法裁定或其他对个人有重大影响的决定；	示例 1：在设置有分段测速或电子收费的道路，建设有用于流量、道路违规等行为的检测系统，特别是能够自动识别车辆的系统，对驾驶员及其驾驶行为进行详细的记录和监督，并给出是否违法的判断。示例 2：电商平台监控

	用户购物行为，进行用户画像，分析用户的购买偏好和购买能力，设置针对用户特定偏好的营销计划。
c）系统性的监控分析个人或个人信息，如在公共区域监控、采集个人信息等，但仅在涉及违规事件分析时才使用的视频监测系统除外：	示例 1：大规模公共空间监测系统，用于人员追踪，并且能够收集超出提供服务范围的个人信息。示例 2：设置在工作场所的 IT 监测系统，监控员工的电子邮件、所使用的应用程序等，用于分析员工工作时间及使用工具（如电子邮件、互联网）的情况。
d）收集的个人敏感信息数量、比重较多，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；	示例 1：通过智能手表、手环、制服、头盔或其它移动设备持续收集或监控个人信息主体的活动、健康相关数据。示例 2：通过健身手环或智能手机中的传感器持续收集或监控用户运动、健康相关数据，通过数据分析和处理提供定制化的健身建议或改善训练流程的服务。
e）数据处理的规模较大，如涉及 100 万人以上、持续时间久、在某个特定群体的占比超过 50%、涵盖的地理区	示例 1：社交网络、在线浏览器、有线电视订阅服务大规模收集用户浏览网站、购买记录、观看记录、收听记录等数据。示例 2：百货商店、购物中心或其他类似营业场所中，通过收集路人和顾客的 GPS、蓝牙或移动通信信

域广泛或较集中等：	号，对客流情况进行监测，跟踪顾客的购物路线和购物习惯。

表 B. 1（续）

个人信息处理活动	场景示例
f）对不同处理活动的数据集进行匹配和合并，并应用于业务：	示例 1：基于防欺诈或风险管控目的，电商平台合并处理不同来源的数据集，以便根据分析或测试结果显示的风险值采取相应管控措施。示例 2：电商平台、零售商店通过分析顾客的购物、优惠券使用等行为数据，结合顾客的信数据、第三方和社交网络数据等，获得提高销售额的营销策略。
g）数据处理涉及弱势群体的，如未成年人、病人、老年人、低收入人群等；	示例 1：能够连接网络的智能玩具收集儿童玩要的音频、视频数据，或收集儿童的年龄、性别、位置等信息。 示例 2：在远程医疗场景中，医生通过网站或应用程序与患者进行视频通话，通过各类传感器收集分析患者的血糖、血氧等健康数据。

h）创新型技术或解决方案的应用，如生物特征识别、物联网、人工智能等：	示例 1：通过人工智能提供客户服务或支持，呼叫中心利用人工智能技术处理呼叫者的音频数据，自动评估呼叫者的心情，并根据评估结果确定与呼叫者的沟通方式或向呼叫者提供的建议。示例 2：健身俱乐部、酒店等入口控制系统，指纹支付或刷脸支付等支付程序，通过收集和处理个人信息主体的个人生物识别信息，判断是否拥有进入某些区域、使用某些功能的权限。
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。	示例 1：提供贷款、信贷、分期付款销售的实体通过收集、处理包含有债务人或类似个人信息主体的数据库信息，针对潜在客户制定信贷决策。

判断个人信息处理活动是否与上述场景相关，需考虑贯穿数据映射分析、合规差距分析等过程，一旦涉及上述情形，可针对以上场景评估影响和风险，同时重视个人信息主体代表等相关方的咨询意见，保障评估的准确性。

附录 C

（资料性附录）

个人信息安全影响评估常用工具表

以下工具表（表 C．1-表 C．5）均为资料性工具，供组织进行评估时选取参考。工具表以个人信息处理活动／场景／特性或组件为维度，各表可基于此项进行整合或分开处理。建议组织采取 IT 化／自动化处理方式进行影响评估。

表 C．1 基于处理活动／场景／特性或组件的个人信息映射表

个人信息处理活动／场景／特性或组件	个人信息类型	个人信息主体	个人信息收集、处理的目的	个人信息处理的合法事由	个人信息控制者	个人信息处理者	是否涉及跨境转移	是否涉及第三方共享
处理活动 A								
处理活动 B								
处理活动 C								

表 C．2 个人信息生命周期安全管理

个人信息处理活动／场景／特性或组件	相关个人信息项	收集来源	收集方式	存储方式／加密措施	传输方式／加密措施	存储期限	删除／匿名化方式
处理活动 A							
处理活动 B							
处理活动 C							

具体字段请详细列举。

涉及联合控制者的，请详细列举并说明。

涉及多个处理者的，清详细列举并说明。

4 如涉及，请填写表 C．3 相关内容。

如涉及，请填写表 C．3 相关内容。

此处可分为多行填写（每一行对应一项个人信息字段），也可合并处理。

表 C．3 安全事件可能性分析表

个人信息处理活动／场景／特性或组件	风险源维度	产生风险的原因／存在的问题	相关证据	安全事件发生可能性
处理活动 A	网络环境和技术措施			
	个人信息处理流程			
	参与人员与第三方			
	业务特点和规模及安全态势			
处理活动 B				

个人信息处理活动/场景/特性或组件	风险源维度	产生风险的原因/存在的问题	安全事件发生可能性等级	对个人权益产生的影响维度	影响程度	风险描述及等级	相关责任方与风险处置建议	整改效果验证及归档情况
处理活动A	网络环境和技术措施			限制个人自主决定权				
				引发差别性待遇				
				个人名誉受损或遭受精神压力				
				人身财产受损				
	个人信息处理流程							
	参与人员与第三方							
	业务特点和规模及安全							

	态势							
处理活动B								

表 C．4 安全风险评估及整改措施表[1]

[1] 评估过程中仅需体现识别出的风险源维度及对个人权益产生的影响维度，可不体现本标准所列举所有维度。组织针对特定个人信息处理活动开展具体的风险分析时，可参考表 C．5 简化评估过程，首先，从识别的风险源维度出发，分析可能发生的安全事件及其可能性，同时，按照影响程度类型，分析对个人信息主体权益的影响程度，如果两者存在交叉，则可参考表 D．5 得出风险等级，并简要说明存在风险的原因。

表 C．5 特定个人信息处理活动的安全风险评估表

影响方面	限制个人自主决定权		引发差别性待遇		名誉受损或精神压力		人身财产受损	
	风险等级	原因说明	风险等级	原因说明	风险等级	原因说明	风险等级	原因说明
网络环境和技术措施								
个人信息处理流程								
参与人员与第三方								
业务特点和规模及安全态势								

附录 D

（资料性附录）

个人信息安全影响评估参考方法

D．1 评估安全事件发生的可能性

安全事件可能性等级评价可采用定性、半定量和定量的方式。安全事件可能性等级判定准则见表 D.1。

表 D．1 安全事件可能性等级判定准则

可能性描述	可能性等级
采取的措施严重不足，个人信息处理行为极不规范，安全事件的发生几乎不可避免。	很高
采取的措施存在不足，个人信息处理行为不规范，安全事件曾经发生过或已经在类似场景下被证实发生过。	高
采取了一定的措施，个人信息处理行为遵循了基本的规范性原则，安全事件在同行业、领域被证实发生过。	中
采取了较有效的措施，个人信息处理行为遵循了规范性最佳实践，安全事件还未被证实发生过。	低

以定性方式为例，可从“网络环境和技术措施”、“处理流程规范性”、“参与人员与第三方”、“安全态势及业务特点”等方面，依据本标准表 D．1 的判定准则，对安全事件可能性等级进行评价。可能性等级分为“很高”、“高”、“中”、“低”四个等级，安全事件可能性判定可参考表 D．2。

表 D．2 可能性判定表

可能性描述	可能性等级
网络环境与互联网及大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，管理制度无落实的记录，未对第三方处理个人信息的范围提出相关要求。	
威胁引发的相关安全事件曾经在组织内部发生过，或已在合作方中发生，或收到过权威组织发出的相关风险预警信息，或处理个人信息的规模超过 1000 万人。	

表 D．2（续）

可能性描述	可能性等级
网络环境与互联网及其他信息系统有交互现象，采取了一定的安全措施。	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。	
有相关的管理制度，对人员提出了管理要求，对第三方处理个人信息的范围提出限制条件，但相应的管理和监督效果不明。	
威胁引发的相关安全事件已经被同领域其他组织发现，或在专业组织相关报告中被证实已出现，或处理个人信息的规模超过 100 万人。	
网络环境比较独立，交互少，或采取了有效的措施保护个人信息安全。	低
该个人信息处理行为非常态业务行为，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。	
有完善的管理机制，对人员的管理和审核比较严格，与第三方合作时提出有效的约束条件并进行监督。	
威胁引发的安全事件仅被专业组织所预测。	

评估过程中，可根据事件自身的性质估计和经验数据评估其可能性，再根据组织所实施的针对性安全控制措施、相关事件处置经验对可能性进行修正。比如，个人信息处理的规模超过 1000 万人，但有完备的、针对性的个人信息保护措施和应急机制，或者已具备类似事件处置的经验，并得到了个人信息主体的认同，则安全可能性等级可降

低一个级别。在进行修正时需要具体说明修正的理由，必要时可咨询外部专业组织保证修正过程的合理性。

D．2 评估个人信息主体权益影响程度

个人权益影响程度评价可采用定性、半定量和定量的方式。个人权益影响程度判定准则见表D．3。

表D．3个人权益影响程度判定准则

影响描述	影响程度
个人信息主体可能会遭受重大的、不可消除的、可能无法克服的影响。如遭受无法承担的债务、失去工作能力、导致长期的心理或生理疾病、导致死亡等。	严重
个人信息主体可能遭受重大影响，个人信息主体克服难度高，消除影响代价大。如遭受诈骗、资金被盗用、被银行列入黑名单、信用评分受损、名誉受损、造成歧视、被解雇、被法院传唤、健康状况恶化等。	高
个人信息主体可能会遭受较严重的困扰，且克服困扰存在一定的难度。如付出额外成本、无法使用所提供的服务、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“限制个人自主决定权”、“引发差别性待遇”、“个人名誉受损和遭受精神压力”、“人身财产受损”四个

维度，依据表D．3的判定准则，对个人信息主体的权益进行影响程度评价。影响程度分为“严重”、“高”、“中”、“低”四个等级，影响度判定可参考表D．4。

表D．4 影响程度判定表

影响类别	影响描述	影响程度
限制个人自主决定权	例如个人人身自由受限。	严重
	例如被强迫执行违反个人意愿的操作、被蓄意推送消息影响个人价值观判断、可能引发个人人身自由受限。	高
	例如缺乏相关知识或缺少相关渠道更正个人信息、为使用应提供的产品或服务而付出额外的成本等。	中
	例如被占用额外的时间。	低
引发差别性待遇	例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
	例如造成对个人合法权利的歧视性待遇、造成对个人公平交易权的损害（无法全部或部分使用所提供的产品或服务）。	高
	例如造成误解、为使用所提供的产品或服务而需付出额外的成本（包含资金成本、	中

	时间成本等）。	
	例如耗费额外的时间获取公平的服务或取得相应的资格等。	低
个人名誉受损和遭受精神压力	例如名誉受损以致长期无法获得财务收入、导致长期的心理或生理疾病以至于失去工作能力、导致死亡等。	严重
	例如名誉受损以致被用人单位解除劳动关系、导致心理或生理疾病以致健康遭受不可逆的损害等。	高
	例如造成误解、名誉受损（通过澄清可全部或部分恢复）、产生害怕和紧张的情绪、导致心理或生理疾病（通过治疗或纠正措施，短期可痊愈）等。	中
	例如被频繁打扰、产生厌烦和恼怒情绪等。	低
人身财产受损	例如造成重伤、遭受无法承担的债务等。	严重
	例如造成轻伤、遭受金融诈骗、资金被盗用、征信信息受损等。	高
	例如造成轻微伤、社会信用受损，为获取金融产品或服务，或挽回损失需付出额外的成本等。	中
	例如因个人信息更正而需执行额外的流程（或提供额外的证明性材料）等。	低

评估过程中，可先分析个人信息处理活动对某一个个人信息主体造成的影响程度，再根据处理活动的规模、特点、外部环境、个人信息去标识化、群体性特征等要素修正影响等级。比如，个人信息处理活动涉及典型的个人敏感信息，如健康状况等，且达到一定的数量（如50万人），则影响程度可上升一个级别；如果受影响个人信息主体群体抗财务风险能力差、心理承受能力差等情形。如未成年人、学生、老年人等，则影响程度可上升一个级别；如果个人信息经去标识化后已确认降低敏感程度的，影响程度可降低一个级别。在进行修正时需要具体说明修正的理由，必要时可咨询外部专业组织保证修正过程的合理性。

此外，从组织实践角度出发，可以进一步将个人信息主体权益的影响映射到对组织的影响，以促进组织进一步认识到其中的风险。比如，可根据个人权益受损对组织付出的成本进行评价。成本一般包括：违规成本（如监管处罚、诉讼费用、整改费用等）、直接的业务损失（如流失客户减少了业务收入等）、名誉损失（如品牌形象受损、客户信任受损等）、内部企业文化损失（如企业执行力受损、价值观冲突引起员工积极性下降等）等，以上方面还可以进行初步的半定量或定量分析（比如处罚的案例与罚金等），以促进组织充分重视个人信息保护工作，积极改进，降低个人信息处理过程对个人权益的影响。

D．3 个人信息安全风险综合评估

综合分析个人权益影响程度和安全事件可能性两个要素，得出风险等级，并给出相应的改进建议，最终形成评估报告。风险等级可分

为：严重、高、中、低四个等级。以定性分析为例，可参考表D．5。组织可以根据自身业务特点和内部风险管理策略，设计科学、合理的风险等级判定表，并设定何种等级风险为不可接受的风险，但注意保证风险等级判定表不得随意变更或修订，必要时可咨询外部专业组织保证风险等级判定表的合理性。

<table>
<tr><td colspan="2" rowspan="2">风险等级</td><td colspan="4">可能性级别</td></tr>
<tr><td>低</td><td>中</td><td>高</td><td>很高</td></tr>
<tr><td rowspan="4">影响级别</td><td>严重</td><td>中</td><td>高</td><td rowspan="2">严重</td><td>严重</td></tr>
<tr><td>高</td><td>中</td><td>中</td><td>高</td><td></td></tr>
<tr><td>中</td><td>低</td><td>中</td><td>中</td><td>高</td></tr>
<tr><td>低</td><td>低</td><td>低</td><td>中</td><td>中</td></tr>
</table>

表D．5 风险等级判定表

TC260-PG-20203A 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

时效性：　现行有效

发布机关：　全国信息安全标准化技术委员会秘书处

发布日期：　2020 年 09 月 18 日

1 范围

本实践指南给出了当前 App1 个人信息保护十大常见问题及典型问题情形，同时给出了问题相应的处置建议。

本实践指南适用于 App 提供者防范和处置个人信息保护常见问题，也可为 App 开发者、移动互联网应用分发平台运营者和移动智能终端厂商提供参考。

2App 个人信息保护十大常见问题及处置指南

2.1 未说明收集使用的个人信息目的、类型、方式

2.1.1 问题描述

App 未说明收集使用的个人信息目的、类型、方式，是指未逐一列出 App（包括委托的第三方或嵌入的第三方代码、插件）收集使用个人信息的目的、方式和范围等，其典型问题情形包括但不限于：

情形一：使用概括性描述或不完整列举收集个人信息的业务功能及收集个人信息的目的、类型、方式。例如使用“等、例如”等方式不完整列举个人信息收集类型。

情形二：未列出嵌入的第三方代码、插件收集使用个人信息的目

的、类型、方式。App[1]嵌入了收集用户个人信息的第三方代码或插件（如第三方 SDK），但未通过隐私政策或其他显著方式（如第三方代码或插件隐私政策链接）向用户明示第三方代码或插件的个人信息收集使用行为。

情形三：未列出委托的第三方收集使用个人信息的目的、类型、

方式。App 委托第三方进行个人信息处理，未通过隐私政策或其他方式向用户明示委托第三方的个人信息收集使用行为。

情形四：收集使用个人信息的目的、方式、范围发生变化时，未以适当方式通知用户。例如未及时更新隐私政策，或未提醒用户阅读等。

2.1.2 处置指南

该问题的处置建议，包括但不限于：

a)完整、清晰、区分说明各业务功能所收集的个人信息。宜根据用户使用习惯逐项说明各业务功能收集个人信息的目的、类型、方式，避免使用“等、例如”等方式不完整列举。

b)使用 Cookie 等同类技术（包括脚本、Clickstream、Web 信标、Flash Cookie、内嵌 Web 链接等）收集个人信息时，简要说明相关机制，以及收集个人信息的目的、类型。

c)如嵌入的第三方代码、插件（如 SDK）收集个人信息，说明第三方代码、插件的类型或名称，及收集个人信息的目的、类型、方式。

[1] 注：本实践指南中的 App 是指通过预装、下载等方式获取并运行在移动智能终端上、向用户提供信息服务的应用软件。

d)如存在委托第三方处理个人信息，说明委托第三方的类型或身份、涉及的个人信息类型、委托处理目的等。

e)收集使用个人信息的目的、方式、范围发生变化时，更新隐私政策等收集使用规则，并以推送消息、邮件、弹窗、红点提示等方式提醒用户阅读发生变化的条款。

2.2 隐私政策未征得用户明示同意

2.2.1 问题描述

App 隐私政策未征得用户明示同意，是指 App 采用默认选择同意等非明示方式征得用户同意，其典型问题情形包括但不限于：

情形一：未提示用户阅读隐私政策。未在用户首次使用或用户注册时主动提示用户阅读隐私政策，或以缩小字号、减淡颜色、遮挡等方式诱导用户略过隐私政策链接。

情形二：默认勾选同意。例如，App 在注册/登录界面下方“我已阅读并同意服务许可协议及隐私政策”前的勾选框中提前替用户打钩；注册/登录界面下方只给出隐私政策链接，并未说明注册/登录后是否视为同意隐私政策。

2.2.2 处置指南

该问题的处置建议，包括但不限于：

a)为用户提供主动选择同意、或显著提醒用户阅读后同意隐私政策的选项，对于通过勾选框形式征得同意的，不默认勾选同意。

b)在首次运行 App 或用户注册时，主动提示用户阅读隐私政策。如通过弹窗等形式主动展示隐私政策的主要或核心内容，帮助用户理

解收集个人信息的范围和规则进而做出决定。

2.3 超范围收集

2.3.1 问题描述

App 超范围收集，是指违反必要原则，收集与业务功能无关的个人信息，或收集个人信息的范围、频度等超出实现 App 业务功能实际需要，其典型问题情形包括但不限于：

情形一：收集无关个人信息。收集的个人信息类型与 App 提供的业务功能无关，例如未提供短信功能的 App 读取短信数据。

情形二：强制收集非必要个人信息。因用户不同意收集非必要个人信息，App 拒绝提供业务功能。例如：因用户拒绝提供某服务类型最小必要个人信息 2 以外的信息，App 拒绝提供该类型服务基本业务功能；仅以改善服务质量、提升用户体验、定向推送信息、研发新产品等为由，强制要求用户同意收集个人信息；在非必需的服务场景，诱导或强制采集个人生物识别信息、手持身份证照片等个人敏感信息，如可以通过密码方式验证而确保安全性的，却诱导用户使用指纹识别或人脸识别的方式验证。

情形三：过度索权。App 超范围索取权限 3，例如：申请打开与 App 所提供业务功能无关的权限；App 安装和运行时，向用户申请当前服务类型非必要权限，用户拒绝授权申请后，App 退出、关闭或拒绝提供该类型服务基本业务功能；App 在用户未使用相关功能或服务时，提前申请开启通讯录、位置、短信、麦克风、相机等权限[1]。

[1] 注：服务类型的必要系统权限，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》的常

情形四：收集时机和频度不合理。例如：收集个人信息的频度超出 App 业务功能实际需要，特别是在静默状态或在后台运行时，收集个人信息的频度和数量超出业务需要，如预订车票功能场景下每 1 秒上传一次用户精确定位信息；用户关闭 App 后，App 未经用户同意通过自启动、关联启动方式收集个人信息[1]。

2.3.2 处置指南

该问题的处置建议，包括但不限于：

a)结合实际的业务功能和场景所需，App 收集的个人信息类型应与业务功能有直接关联，不收集与所提供业务功能无关的个人信息。

b)遵循最小必要原则，仅申请 App 业务功能所必需的权限，不申请与 App 业务功能无关的权限（即使用户可选择拒绝）。

c)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》，明确 App 所提供的服务类型和最小必要个人信息范围，且不因用户拒绝提供最小必要个人信息以外的信息，拒绝提供该类型服务的基本业务功能[2]。

d)如用户拒绝或撤回授予某服务类型非必要系统权限，App 不应

见服务类型最小必要个人信息进行判断。

[1] 最小必要个人信息，是指保障某一服务类型正常运行最少够用的个人信息，一旦缺少将导致该服务类型基本业务功能无法实现或无法正常运行；本实践指南中的“权限”指“可收集个人信息权限”。

[2] 《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》，给出了常见服务类型的最小必要个人信息；《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》，给出了权限相关的业务功能示例，及与常见服务类型相关程度较低，不建议申请的安卓系统权限。

强制退出或关闭，且不影响与此权限无关的业务功能使用。

e)App 所需的权限应在对应业务功能执行时动态申请，在用户未触发相关业务功能时，不提前申请与当前业务功能无关的权限。

f)权限申请获得授权后，自动采集个人信息的频率应在实现 App 业务功能所必需的最低合理频率范围内，且仅访问满足业务功能需要的最少个人信息。

g)除为满足法律法规规定、保护公共利益和个人重要人身财产权利之外，App 开展业务活动时不应限定使用个人生物识别信息作为唯一实现业务目标的方式。

2.4 强制捆绑授权

2.4.1 问题描述

App 强制捆绑授权，是指以捆绑、频繁打扰等不合理方式征得用户同意收集个人信息或申请系统权限，其典型问题情形包括但不限于：

情形一：要求用户一次性同意打开多个可收集个人信息权限，用户不同意则无法安装或使用。例如，用户安装 App 时，以捆绑打包形式申请其向操作系统声明的所有权限，用户不同意则无法安装或使用，安装完成后申请的所有权限默认打开（如 Android 版 App 设置 targetSdkVersion 小于 23 所致）。

情形二：频繁索权。App 在用户明确拒绝权限申请后，频繁申请开启通讯录、位置、短信、麦克风、相机等与当前业务功能无关的权限骚扰用户。又如，对于用户可选提供的权限，在用户明确拒绝后，

每当其重新打开 App 或进入相应界面，都会再次向用户索要或以

弹窗等形式提示用户缺少相关权限，干扰用户正常使用。

情形三：以捆绑方式征得新增类型个人信息收集的同意。App 新增业务功能申请收集的个人信息超出用户原有同意范围，若用户不同意，则拒绝提供原有业务功能（新增业务功能取代原有业务功能的除外）。

2.4.2 处置指南

该问题的处置建议，包括但不限于：

a)安卓 App 的目标 API 等级应不低于 23（targetSdkVersion>=23），目标 API 等级宜及时更新适配安卓新版本[1]。

b)App 宜区分基本业务功能和附加业务功能，不通过捆绑服务类型、捆绑基本业务功能和附加业务功能等方式，强制要求用户一次性授权同意个人信息收集请求。

c)对于仅为实现附加功能、个性化服务、提升用户体验，同时又并非 App 实现基本业务功能所必要的个人信息,可单独征得用户同意，并保障用户可拒绝个人信息收集的权利，且用户拒绝此类信息后不影响其正常使用 App 基本业务功能。

d)如用户明确拒绝 App 业务功能所需权限，App 不应频繁申请系统权限干扰用户正常使用，除非由用户主动触发功能，且没有该权限参与此业务功能无法实现。“频繁”的形式包括但不限于：

1)单个场景在用户拒绝权限后，48 小时内弹窗提示用户打开系统权限的次数超过 1 次；

[1] 注：截至本实践指南发布时，推荐设置目标 API 等级不低于 28。

2)每次重新打开 App 或使用某一业务功能时，都会向用户索要或提示用户缺少相关系统权限。

2.5 未经用户同意收集个人信息

2.5.1 问题描述

App 未经用户同意收集个人信息，是指实际收集使用个人信息的行为未经用户同意或违背用户意愿，其典型问题情形包括但不限于：

情形一：征得同意前开始收集个人信息。例如 App 首次运行时，

用户点击同意隐私政策前已产生个人信息收集行为。

情形二：拒绝或撤回同意后仍收集个人信息。用户撤回权限授权后，仍收集相关个人信息。例如用户拒绝电话权限后，仍存在收集 IMEI 行为。

情形三：私自截留用户向第三方提供的个人信息。未经用户同意，收集用户向第三方（包括接入的第三方应用）提供的个人信息。

情形四：未征得用户同意读取剪切板或公共存储区的个人信息。如银行类 App 未在隐私政策中说明会读取剪切板内容，当用户打开

银行类 App，提示用户是否向剪切板中的账号转账的情形。

情形五：私自调用权限隐蔽上传个人信息。例如，使用相机、麦克风、位置等敏感权限获取个人敏感信息时，在用户不知情情况下隐蔽读取并上传个人信息。

2.5.2 处置指南

该问题的处置建议，包括但不限于：

a)用户点击同意隐私政策前，不产生任何个人信息收集行为。

b)将权限申请的触发时间点置于用户点击同意隐私政策后。

c)如 App 不存在下载、读取外部存储文件的实际业务功能，可直接在 App 自有的目录下进行保存，不建议申请外部存储权限。

d)以下操作应由用户主动触发，并在用户知情情况下执行：

1)执行拨打电话、发送短信等操作；

2)打开或关闭 Wi-Fi、蓝牙、GPS 等；

3)拍摄、录音、截屏、录屏等；

4)读写用户短信、联系人等个人信息。

e)不应隐蔽收集个人信息，当录音、拍摄、录屏、定位等敏感功能在后台执行时，应采用显著方式（如图标闪烁、状态栏提示、自定义提示条等）提示用户。

f)不应在用户不知情或未授权的情况下，通过隐蔽方式读取并上传剪切板中包含的个人信息和公共存储区中的个人信息。

g)对于用户直接向第三方提供个人信息的情形，不私自收集用户直接向第三方提供的个人信息。

2.6 申请权限或收集个人敏感信息未同步告知目的

2.6.1 问题描述

App 申请权限或收集个人敏感信息未同步告知目的，是指 App 申请权限或收集个人敏感信息时，未同步告知收集目的，或目的描述不明确，其典型问题情形包括但不限于：

情形一：未同步告知个人敏感信息收集目的。收集身份证件号码、银行账户、个人生物识别信息等个人敏感信息时，未同步告知用户其

目的。例如 App 收集面部识别特征前未展示单独协议或进行显著特殊说明，在用户点击“继续”后，App 在无任何提示的情况下便开始采集用户的面部识别特征。

情形二：未告知权限申请目的。App 申请权限时未同步告知权限的申请目的，例如仅通过操作系统弹窗向用户申请权限，且未告知权限申请目的。

情形三：目的告知不明确。目的描述不明确、难以理解，例如将目的描述为“为保证某某权限相关功能的正常使用”、“为了保证 App 正常运行”、“为了提高用户体验”等，未具体明确地说明权限的使用目的。

2.6.2 处置指南

该问题的处置建议，包括但不限于：

a)收集个人生物识别信息前，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)收集身份证号、银行账户、行踪轨迹等个人敏感信息时，同步告知用户收集使用目的，目的应明确且易于理解。

c)申请权限时应同步告知权限申请目的，目的明确且易于理解，不包含任何欺诈、诱骗、误导用户授权的描述。

d)对于权限申请系统弹窗中可编辑目的的操作系统，App 可在操作系统提供的权限申请弹窗中编辑具体明确的申请目的；权限申请系统弹窗中无法编辑目的的，建议通过 App 弹窗提示等方式，向用户告

知权限的申请目的。

2.7 实际收集使用个人信息行为与声明不一致

2.7.1 问题描述

App 实际收集使用个人信息行为与声明不一致，是指 App 实际收集使用的个人信息超出用户授权范围，或实际行为与其所声明的隐私政策等收集使用规则存在偏差、不一致，其典型问题情形包括但不限于：

情形一：实际收集使用个人信息的范围与隐私政策所述不一致。

例如，实际收集使用个人信息范围超出隐私政策所述，即实际收集的个人信息未在隐私政策中或以其他形式说明；实际收集使用个人信息的范围少于隐私政策所述，即声明了实际并未收集的个人信息、权限或并未提供的业务功能。

情形二：故意欺瞒、掩饰收集使用个人信息的真实目的，诱骗用户同意收集个人信息或申请打开权限。例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，并将该类信息用于发送商业广告或其它目的；又如通过积分、奖励、优惠等方式欺骗误导用户提供身份证号码以及个人生物特征信息。

情形三：隐私政策所述存在明显偏差、错误。即隐私政策所述与实际情况存在明显偏差、错误，甚至出现大篇幅抄袭导致隐私政策内容不实等。

2.7.2 处置指南

该问题的处置建议，包括但不限于：

a)实际收集的个人信息类型、申请打开可收集使用个人信息的权限、提供的业务功能等，与隐私政策等收集使用规则中相关内容一致，不超出隐私政策等收集使用规则所述范围。

b)严格遵守隐私政策等收集使用规则，App 收集或使用个人信息的功能设计同隐私政策保持一致、同步调整。

c)明示收集使用个人信息的目的需真实、准确，不故意欺瞒、掩饰收集使用个人信息的真实目的，不诱骗用户同意收集个人信息或打开可收集个人信息权限。

2.8 未经同意向第三方提供个人信息

2.8.1 问题描述

App 未经同意向第三方提供个人信息，是指 App 未经用户同意，也未做匿名化处理，私自将其他第三方应用或服务器发送、共享个人信息，其典型问题情形包括但不限于：

情形一：App 未经同意直接向第三方提供个人信息。例如存在

App 客户端直接向第三方服务器传输个人信息(如设备识别信息、商品浏览记录、搜索使用习惯、常用软件应用列表等)，或者数据传输至 App 后台服务器后，向第三方提供其收集的个人信息等行为，但未在隐私政策中说明或以其他显著方式明示用户，或未经用户授权同意，也未做匿名化处理。

情形二：内嵌 SDK 未经同意向第三方提供个人信息。例如存在嵌入的第三方代码、插件将个人信息传输至第三方服务器的行为，但未在隐私政策中说明或以其他显著方式明示用户，或未经用户授权同意，

也未做匿名化处理。

2.8.2 处置指南

该问题的处置建议，包括但不限于：

a)如存在从客户端直接向第三方发送个人信息的情形，包括通过客户端嵌入第三方代码、插件（如 SDK）等方式向第三方发送个人信息的情形，需事先征得用户同意，经匿名化处理的除外。

b)如个人信息传输至服务器后，App 运营者向第三方提供其收集的个人信息，需事先征得用户同意，经匿名化处理的除外。

c)如向第三方传输的个人信息类型、接收数据的第三方身份等发生变更的，需以适当方式通知用户，并征得用户同意。

d)如 App 接入第三方应用，当用户使用第三方应用时，需在征得用户同意后，再向第三方应用提供个人信息。当用户获知应用为第三方提供后，自行以主动填写等方式向第三方直接授权的除外。

e)App 提供者宜对于接入的第三方应用收集个人信息的合法、正当、必要性等方面进行审核，并明确标识相关业务功能为第三方提供。

f)用户跳转至第三方应用时，宜提醒用户关注第三方应用的收集使用规则。

g)App 宜对第三方代码（如 SDK）使用的权限进行审核，要求引入第三方代码所需使用的权限最小化。

h)App 宜采取技术检测、安全审计等手段，确保第三方代码或插件收集、使用行为符合约定要求。

2.9 未提供删除、更正或投诉举报的功能或渠道

2.9.1 问题描述

App 未提供删除、更正或投诉举报的功能或渠道，是指 App 未提供有效且能及时响应的删除、更正或投诉举报的功能或渠道，或设置不合理条件，其典型问题情形包括但不限于：

情形一：无法删除个人信息或设置不合理条件。例如，App 未提供有效的个人信息删除功能或渠道；为删除个人信息设置不合理条件；未按相关要求或约定时限响应用户删除个人信息请求等。

情形二：无法更正个人信息或设置不合理条件。例如，App 未提供有效的个人信息更正功能或渠道；为更正个人信息设置不合理条件；未按相关要求或约定时限响应用户更正个人信息请求；用户已完成更正个人信息操作，但 App 后台并未完成的等。

情形三：未提供个人信息申诉渠道或用户申诉机制无效。例如，

未建立并公布个人信息安全投诉、举报渠道，或未在承诺时限内（承诺时限不得超过 15 个工作日，无承诺时限的，以 15 个工作日为限）受理并处理的。

2.9.2 处置指南

该问题的处置建议，包括但不限于：

a)提供有效的更正、删除个人信息的途径。

b)宜提供在线操作方式及时响应个人信息更正、删除请求，需人工处理的，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)更正和删除个人信息的功能应简单易操作，不设置不必要或不

合理的条件。

d)用户更正、删除个人信息等操作完成时，App 后台及时执行完成相关操作，因法律法规规定需要留存个人信息的，不再将其用于日常业务中。

e)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。

f)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。

2.10 未提供有效的注销用户账号途径

2.10.1 问题描述

App 未提供有效的注销用户账号途径，是指 App 未提供有效的注销用户账号功能或渠道，或为注销用户账号设置不必要或不合理条件，其典型问题情形包括但不限于：

情形一：无法注销或未按要求注销。例如：App 未提供注销用户账号的功能或渠道；通过 App 界面、邮件、客服电话等渠道提交注销申请后，未按相关要求或约定完成注销；受理注销账户请求后，未在承诺时限内（不超过 15 个工作日）完成核查和处理；注销成功后，未按相关要求或约定对用户个人信息进行删除或匿名化处理（法律法规另有规定的除外）；用户难以找到注销入口，或注销操作流程非常复杂不易操作等。

情形二：设置不合理的注销账号条件。例如：注销过程进行身份

核验时，要求用户提交超过 App 注册、使用时收集的个人信息类型（如注册使用时未提供身份信息，但是注销时要求提供手持身份证照片、绑定银行卡等）；对于采用同一账号注册登录多个 App 的情形，注销或退出单个 App 将导致其他无必要业务关联的 App 不能使用；要求用户填写精确的历史操作记录作为注销的必要条件等。

2.10.2 处置指南

该问题的处置建议，包括但不限于：

a)提供简便易操作的注销功能或渠道，若有可能宜在应用或网站上设置便捷的交互页面提供在线注销功能，且注销入口易于访问，注销状态易于查询。

b)不设置不合理的注销条件，不响应账号注销请求的情形不超过 GB/T 35273-2020《信息安全技术 个人信息安全规范》8.7 e）给出的情形[1]。

c)注销过程如需进行身份核验，不要求用户提供超出注册、使用等服务环节收集的个人信息类型，特别是注销时要求额外提供手持身份证照片、银行卡绑定、人脸识别等。

d)制定并公开账号注销条款，明示账号注销的条件、后果、方法、流程等信息[2]。

e)及时响应用户注销请求，需要人工处理的，在承诺时限内（不超过 15 个工作日）完成核查和处理。

---

[1] 注：如用户自愿选择放弃账号下相应权益（如 XX 币、XX 积分），若有可能宜允许用户注销账号。

[2] 注：注销条款可作为个人信息保护政策的章节，也可制定单独的注销协议。

f)用户注销后的数据处理，建议：

1)注销后停止对用户个人信息的收集和使用，并按照相关要求和约定删除其个人信息或匿名化处理；

2)因法律法规规定需要留存个人信息的，将其隔离存储，不再将其用于日常业务活动中；

3)注销时因验证用户身份所收集的个人敏感信息，完成用户身份验证后立即删除或匿名化处理。

g)多个 App 共用一个账号体系时，单个 App 注销建议：

1)用户可退出或注销单个 App，且不影响无必要业务关联 App 的正常使用；

2)提供解除单个 App 用户账号使用关系等措施实现注销，并对该 App 账号以外其他个人信息进行删除；

3)如多个 App 之间存在必要业务关联而无法拆分账号，需在注销前向用户详细说明账号关联的应用、注销条件、注销后果等信息[1]。

[1] 注：存在必要业务关联，是指如一旦注销某个 App 的账号，将会导致其他 App 的必要业务功能无法实现或者服务质量明显下降的。

JR/T 金融数据安全 数据安全分级指南

时效性：　　现行有效

发布机关：　中国人民银行

类别：　　金融行业标准

发布日期：　2020 年 09 月 23 日

本标准给出了金融数据安全分级的目标、原则和范围，以及数据安全定级的要素、规则和定级过程。本标准适用于金融业机构开展电子数据安全分级工作，并为第三方评估机构等单位开展数据安全检查与评估工作提供参考。

2 规范性引用文件

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。

信息 information

关于客体（如事实、事件、事物、过程或思想，包括概念）的知识，在一定的场合中具有特定的意思[1]

数据 data

信息的可再解释的形式化表示，以适用于通信、解释或处理[2]。

隐私 privacy

个人所具有的控制或影响与之相关信息的权限，涉及由谁收集和

[1] 注：改^GB/T 5271.1—2000,定义 2.01.01.01.

[2] 注:可以通过人工或自动手段处理.[GB/T 5271. 1—2000,定义 2.01. 01.021

存储、由谁披露。

[GB/T 25069—2010,定义 2.1.63]

信息处理 information processing

对信息操作的系统执行，包括数据处理，也可包括诸如数据通信和办公自动化之类的操作[1]。

数据处理 data processing

数据操作的系统执行。

示例：数据的数学运算或逻辑运算，数据的归并或分类，程序的汇编或编洋，或文本的操作，诸如編辑、分类、归并、存储、检索、显示或打印[2]。

保密性 confidentiality

使信息不泄露给未授权的个人、实体、进程，或不被其利用的特性。

[GB/T 25069—2010,定义 2.1.1]

完整性 integrity

保卫资产准确和完整的特性[3]。

可用性 avaiIabiIity

已授权实体一旦需要就可访问和使用的数据和资源的特性。

[GB/T 25069—2010,定义 2.1. 20]

---

[1] 注：术语"信息处理"不能用为“数据处理"的同义词。[GB/T 5271. 1—2000,定义 2. 01.01. 05]

[2] 注：木谱“数据处理"不能用为"信息处理"的同义词；改写 GB/T 5271.1—2000.定义 2.01.01.06

[3] 注：改 SGB/T 25069—2010,定义 2.1.42。

安全级别 security level

有关敏感信息访问的级别划分，以此级别加之安全范畴能更精细地控制对数据的访问。

[GB/T 25069—2010,定义 2.2.1. 6]

0

金融数据 financial data

金融业机构开展金融业务、提供金融服务以及日常经营管理所需或产生的各类数据[1]。

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[2]。

2

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[3]。

影响 impact

事件的后果。在信息安全中，一般指不测事件的后果。

[GB/T 25069—2010,定义 2. 3.105]

4 目标原则和范围

4.1 数据安全定级目标

---

[1] 注：该类数据可用传统数据处理技术或大数据处理技术进行组织、存储、计算、分析利管理。

[2] 注 1：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；改写 GB/T 35273—2020,定义 3.1。

[3] 注：改写 GB/T 35273-2020,定义 3. 3。

数据安全定级旨在对数据资产进行全面梳理并确立适当的数据安全分级，是金融业机构实施有效数据分级管理的必要前提和基础。数据分级管理是建立统一、完善的数据生命周期安全保护框架的基础工作，能够为金融业机构制定有针对性的数据安全管控措施提供支撑。金融业包括货币金融服务、资本市场服务、保险业等，参见 GB/T 4754-2017。本标准所述“金融业机构"是指从事上述金融业的相关机构。

4.2 数据安全定级原则

数据安全定级遵循以下原则：

a） 合法合规性原则：满足国家法律法规及行业主管部门有关规定。

b） 可执行性原则：数据定级规则避免过于复杂，以确保数据定级工作的可行性。

c） 时效性原则：数据安全级别具有一定的有效期限，金融业机构宜按照级别变更策略对数据级别进行及时调整。

d） 自主性原则：结合金融业机构自身数据管理需要（如战略需要、业务需要、风险接受程度等），在本标准的框架下自主确定数据安全级别.

e） 差异性原则：根据本机构数据的类型、敏感程度等差异，划分不同的数据安全层级，并将数据分散至不同的级别中，不宜将所有数据集中划分到其中若干个级别中。

f） 客观性原则：数据定级规则是客观且可校验的，即通过数据

自身的属性和定级规则即可判定其级别，并且数据的定级是可复核和检查的.

4.3 数据安全定级范围

金融数据安全定级过程中，未经电子化的金融数据，依据档案文件等有关管理规范执行；涉及国家秘密的金融数据，依据国家有关法律法规执行，不在本标准规定的范围之内。证券行业数据安全分级工作可参照 JR/T 0158—2018 执行。其中，安全定级工作所涉及的金融数据包括但不限于：

提供金融产品或服务过程中直接（或间接）采集的数据，包括通过柜面以纸质协议签署或收集，并经信息处理后在计算机系统中流转或保存的数据，以及通过信息系统签约或收集的电子信息。

金融业机构信息系统内生成和存储的数据，包括业务数据、经营管理数据等，其中：

业务数据指金融业机构在提供金融产品或服务过程中产生的数据，如交易信息、统计数据等

经营管理数据指金融业机构在履行职能与经营管理过程中采集、产生的数据，如营销服务数据、运营数据、风险管理数据、技术管理数据（如程序代码、系统以及网络等）、统计分析数据、综合管理数据等。

金融业机构内部办公网络与办公设备（终端）中产生、交换、归档的电子数据，如机构内部日常事务处理信息、政策法规与部门规章、业务终端临时存储的业务或经营管理数据、电子邮件信息等。

金融业机构原纸质文件经过扫描或其他电子化手段形成的电子数据。

其他宜进行分级的金融数据。

5 数据安全定级

5. 1 定级要素

5 1.1 概述

安全性（保密性、完整性、可用性）是信息安全风险评估中的重要参考属性。数据安全性遭到破坏后可能造成的影响（如可能造成的危害、损失或潜在风险等），是确定数据安全级别的重要判断依据，主要考虑影响对象与影响程度两个要素,

5.1.2 影响对象

影响对象指金融业机构数据安全性遭受破坏后受到影响的对象，包括国家安全、公众权益、个人隐私、企业合法权益等。影响对象的确定主要考虑以下内容：

影响对象为国家安全的情况，一般指数据的安全性遭到破坏后，可能对国家政权稳固、领土主权、民族团结、社会和金融市场稳定等造成影响。

影响对象为公众权益的情况，一般指数据的安全性遭到破坏后，可能对生产经营、教学科研、医疗卫生、公共交通等社会秩序和公众的政治权利、人身自由、经济权益等造成影响.

影响对象为个人隐私的情况，一般指数据的安全性遭到破坏后，可能对个人金融信息主体的个人信息、私人活动和私有领域等造成影

响。

影响对象为企业合法权益的情况，一般指数据的安全性遭到破坏后，可能对某企业或其他组织（可能是金融业机构，也可能是其他行业机构）的生产运营、声誉形象、公信力等造成影响。

5.1.3 影响程度

影响程度指金融业机构数据安全性遭到破坏后所产生影响的大小，从高到低划分为严重损害、一般损害、轻微损害和无损害，相关说明如表 1 所示，可作为影响程度判定的参考。影响程度的确定宜综合考虑数据类型、数据特征与数据规模等因素，并结合金融业务属性确定数据安全性遭到破坏后的影响程度，例如：数据安全性遭到破坏后，客户的个人自然信息产生的影响程度通常要高于单位基本信息。数据安全性遭到破坏后，身份鉴别信息产生的影响程度通常要高于个人基本概况信息。交易信息中对实时性要求较高的数据，其安全性遭到破坏产生的影响程度通常要高于实时性要求较低的数据等。

5.2 要素识别

5. 2.1 安全影响评估

安全影响评估宜综合考虑数据类型、数据内容、数据规模、数据来源、机构职能和业务特点等因素，对数据安全性（保密性、完整性、可用性）遭受破坏后所造成的影响进行评估。评估过程中，根据实际情况识别各项安全性在影响评定中的优先级，分别进行保密性、完整性及可用性评估，并综合考虑保密性、完整性及可用性的评估结果，形成最终安全影响评估。保密性评估：通过评价数据遭受未经授权的

披露所造成的影响，以及机构继续使用这些数据可能产生的影响，进行数据保密性评估。评估的内容包括但不限于：

数据未经授权的披露，可能对国家安全、公众权益、个人隐私及企业合法权益造成的损害，以及损害的严重程度。

数据被非授权对象获取或利用，可能对国家安全、公众权益、个人隐私及企业合法权益造成的损害，以及损害的严重程度°

数据被非授权对象利用进行窃密、篡改、销毁或拒绝服务等攻击，可能对国家安全、公众权益、个人隐私及企业合法权益等造成的损害，以及损害的严重程度。

数据的未经授权披露或传播是否违反国家法律法规、行业主管部门有关规定或机构内部管理规定。完整性评估：通过评价数据遭受未经授权的修改或损毁所造成的影响，以及机构继续使用这些数据可能产生的影响，进行数据完整性评估。评估的内容包括但不限于：

数据未经授权修改或损毁，可能对国家安全、公众权益、个人隐私及企业合法权益造成的损害，以及损害的严重程度。

数据未经授权修改或损毁，可能对其他组织或个人造成的损害，以及损害的严重程度。

数据未经授权修改或损毁，可能对机构职能、公信力造成的损害，以及损害的严重程度。

数据未经授权修改或损毁是否违反国家法律法规、行业主管部门有关规定或机构内部管理规定。可用性评估：通过评价数据及其经组合/融合后形成的各类数据出现访问或使用中断所造成的影响，以及机

构无法正常使用这些数据可能产生的影响，进行数据可用性评估。评估的内容包括但不限于：

数据的访问或使用中断，可能对国家安全、公众权益、个人隐私及企业合法权益造成的损害，以及损害的严重程度。

数据的访问或使用中断，可能对机构职能、公信力造成的损害，以及损害的严重程度。

数据的访问或使用中断，可能对其他组织或个人造成的损害，以及损害的严重程度.

数据的访问或使用中断是否违反国家法律法规、行业主管部门有关规定或机构内部管理规定。

5.2.2 定级要素识别

通过综合考虑保密性、完整性和可用性的影响评估结果，识别数据安全定级关键要素，即作为最终数据安全级别评定时所使用的主要影响对象及影响程度，并根据 5. 3 定级规则进行数据安全级别的评定。定级要素识别宜至少满足：因不同数据在安全性（保密性、完整性、可用性）方面有不同侧重，以所侧重的安全性评估结果，作为相应数据安全定级的主要依据。数据的保密性、完整性和可用性要求基本一致的，则重点以保密性评估所确定的定级要素为主要定级依据。

5.3 定级规则

5.3.1 安全级别概述

本标准根据金融业机构数据安全性遭受破坏后的影响对象和所造成的影响程度，将数据安全级别从高到低划分为 5 级、4 级、3 级、2

级、1 级，一般具有如下特征：

5 级数据特征如下：

重要数据，通常主要用于金融业大型或特大型机构、金融交易过程中重要核心节点类机构的关键业务使用，一般针对特定人员公开，且仅为必须知悉的对象访问或使用。

数据安全性遭到破坏后，对国家安全造成影响，或对公众权益造成严重影响[1]。

4 级数据特征如下：

数据通常主要用于金融业大型或特大型机构、金融交易过程中重要核心节点类机构的重要业务使用，一般针对特定人员公开，且仅为必须知悉的对象访同或使用。

个人金融信息中的 C3 类信息.

数据安全性遭到破坏后，对公众权益造成一般影响，或对个人隐私或企业合法权益造成严重影响，但不影响国家安全。

3 级数据特征如下：

数据用于金融业机构关键或重要业务使用，一般针对特定人员公开，且仅为必须知悉的对象访问或使用。

个人金融信息中的 C2 类信息。

数据的安全性遭到破坏后，对公众权益造成轻微影响，或对个人隐私或企业合法权益造成

[1] 注：“必须知悉"是指对数据确定知悉范围，只有对数据知悉有明确的必要性时,该对象才能对数据知悉，一般情 况下遵循工作 55 要原则和最小化原则，前者指因工作必须才可知悉，后者指知悉的范围满足最小够用即可。

一般影响，但不影响国家安全。

2 级数据特征如下：

数据用于金融业机构一般业务使用，一般针对受限对象公开，通常为内部管理且不宜广泛公开的数据。

个人金融信息中的 C1 类信息。

数据的安全性遭到破坏后，对个人隐私或企业合法权益造成轻微影响,但不影响国家安全、公众权益。

1 级数据特征如下：

数据一般可被公开或可被公众获知、使用。

个人金融信息主体主动公开的信息.

数据的安全性遭到破坏后，可能对个人隐私或企业合法权益不造成影响，或仅造成微弱影响但不影响国家安全、公众权益。

5. 3.2 定级通用规则

金融数据安全级别划分的通用规则包括但不限于，

“重要数据”的安全等级不可低于本标准所述 5 级。

个人金融信息相关数据参照 JR/T 0171-2020 进行定级，并在数据安全定级过程中从高考虑。

对于数据体量大，涉及的客户（包含个人客户和单位客户）多、涉及客户（包含个人客户和单位客户）资金量大、涉及多行业及多机构客户的情况，影响程度宜从高确定。

综上所述，数据安全级别划定规则如表 2 所示。根据本标准所述定级规则，本标准给出了金融业典型数据类型及其建议划分的最低安

全级别，参见附录 A,供各金融业机构在数据资产梳理及定级过程中参考。

5.4.1 组织保障

确定数据安全管理最高决策组织，设立并明确相关部门（或组织）及其职责，包括但不限于：本机构数据分级工作的领导组织及其负责人，主要负责统筹、规划数据安全分级工作。本机构数据分级工作的管理部门（或组织）及其负责人，主要负责数据分级相关工作的组织、协调、管理、审核、评审等工作。

本机构信息科技部门及其负责人在数据安全分级工作中的角色，主要负责落实数据安全分级有关要求，并主导数据安全分级实施工作.

本机构业务部门（和/或数据属主部门）及其负责人在数据安全分级工作中的角色，主要负责落实数据安全分级有关要求，并协同开展数据安全分级实施工作。

本机构其他相关部门在数据安全分级工作中的角色、职责及负责人。

建立数据分级工作的相关制度，明确并落实相关工作要求，包括但不限于：

数据分级的目标和原则。

数据分级工作涉及的角色、部门及相关职责。

数据分级的方法和具体要求。

数据分级的日常管理流程和操作规程，以及分级结果的确定、评审、批准、发布和变更机制.

数据分级管理相关绩效考核和评价机制。

数据分级结果的发布、备案和管理的相关规定。

数据分级清单审核与修订的原则和周期。

5.4.3 定级流程

金融数据安全定级过程包括数据资产梳理、数据安全定级准备、数据安全级别判定、数据安全级别审核及数据安全级别批准。

数据定级流程基本步骤如下：

数据资产梳理：

第一步：对数据进行盘点、梳理与分类，形成统一的数据资产清单，并进行数据安全定级合规性相关准备工作。

数据安全定级准备：

第二步：明确数据定级的颗粒度〈如库文件、表、字段等）O

第三步：识别数据安全定级关键要素.

数据安全级别判定：

第四步：按照 5.3 所述数据定级规则，结合国家及行业有关法律法规、部门规章，对数据安全等级进行初步判定。

第五步：综合考虑数据规模、数据时效性、数据形态（如是否经汇总、加工、统计、脱敏或匿名化处理等）等因素，对数据安全级别进行复核，调整形成数据安全级别评定结果及定级清单。

数据安全级别审核：

第六步：审核数据安全级别评定过程和结果，必要时重复第三步及其后工作，直至安全级别的划定与本机构数据安全保护目标一致.

数据安全级别批准：

第七步：最终由数据安全管理最高决策组织对数据安全分级结果进行审议批准。

5.5 级别变更

数据安全定级完成后，出现下列情形之一时，金融业机构宜对相关数据的安全级别进行变更（相关示例参见附录 B）,并按照 5. 4. 3 数据定级流程实施。

数据内容发生变化，导致原有数据的安全级别不适用变化后的数据。

数据内容未发生变化，但因数据时效性、数据规模、数据使用场景、数据加工处理方式等发生变化，导致原定的数据安全级别不再适用。

因数据汇聚融合，导致原有数据安全级别不再适用汇聚融合后的数据。

因国家或行业主管部门要求，导致原定的数据安全级别不再适用.

需要对数据安全级别进行变更的其他情形。

6 重要数据识别

金融业机构所承载重要数据的识别和认定工作宜遵照国家及行业主管部门有关规定执行。重要数据的性质和内容相关描述参见附录 C,仅供金融业机构开展数据安全分级工作时参考使用。重要数据的安全级别不宜低于本标准中确定的 5 级。

最高人民法院、最高人民检察院关于办理药品、医疗器械注册申请材料造假刑事案件适用法律若干问题的解释

时效性：　现行有效

发文机关：　最高人民法院、最高人民检察院

文号：　法释〔2017〕15号

发文日期：　2017年08月14日

施行日期：　2017年09月01日

第一条 药物非临床研究机构、药物临床试验机构、合同研究组织的工作人员，故意提供虚假的药物非临床研究报告、药物临床试验报告及相关材料的，应当认定为刑法第二百二十九条规定的“故意提供虚假证明文件”。

实施前款规定的行为，具有下列情形之一的，应当认定为刑法第二百二十九条规定的“情节严重”，以提供虚假证明文件罪处五年以下有期徒刑或者拘役，并处罚金：

（一）在药物非临床研究或者药物临床试验过程中故意使用虚假试验用药品的；

（二）瞒报与药物临床试验用药品相关的严重不良事件的；

（三）故意损毁原始药物非临床研究数据或者药物临床试验数据的；

（四）编造受试动物信息、受试者信息、主要试验过程记录、研究数据、检测数据等药物非临床研究数据或者药物临床试验数据，影响药品安全性、有效性评价结果的；

（五）曾因在申请药品、医疗器械注册过程中提供虚假证明材料受过刑事处罚或者二年内受过行政处罚，又提供虚假证明材料的；

（六）其他情节严重的情形。

第二条 实施本解释第一条规定的行为，索取或者非法收受他人财物的，应当依照刑法第二百二十九条第二款规定，以提供虚假证明文件罪处五年以上十年以下有期徒刑，并处罚金；同时构成提供虚假证明文件罪和受贿罪、非国家工作人员受贿罪的，依照处罚较重的规定定罪处罚。

第三条 药品注册申请单位的工作人员，故意使用符合本解释第一条第二款规定的虚假药物非临床研究报告、药物临床试验报告及相关材料，骗取药品批准证明文件生产、销售药品的，应当依照刑法第一百四十一条规定，以生产、销售假药罪定罪处罚。

第四条 药品注册申请单位的工作人员指使药物非临床研究机构、药物临床试验机构、合同研究组织的工作人员提供本解释第一条第二款规定的虚假药物非临床研究报告、药物临床试验报告及相关材料的，以提供虚假证明文件罪的共同犯罪论处。

具有下列情形之一的，可以认定为前款规定的“指使”，但有相反证据的除外：

(一)明知有关机构、组织不具备相应条件或者能力，仍委托其进行药物非临床研究、药物临床试验的；

(二)支付的价款明显异于正常费用的。

药品注册申请单位的工作人员和药物非临床研究机构、药物临床

试验机构、合同研究组织的工作人员共同实施第一款规定的行为，骗取药品批准证明文件生产、销售药品，同时构成提供虚假证明文件罪和生产、销售假药罪的，依照处罚较重的规定定罪处罚。

第五条 在医疗器械注册申请中，故意提供、使用虚假的医疗器械临床试验报告及相关材料的，参照适用本解释第一条至第四条规定。

第六条 单位犯本解释第一条至第五条规定之罪的，对单位判处罚金，并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。

第七条 对药品、医疗器械注册申请负有核查职责的国家机关工作人员，滥用职权或者玩忽职守，导致使用虚假证明材料的药品、医疗器械获得注册，致使公共财产、国家和人民利益遭受重大损失的，应当依照刑法第三百九十七条规定，以滥用职权罪或者玩忽职守罪追究刑事责任。

第八条 对是否属于虚假的药物非临床研究报告、药物或者医疗器械临床试验报告及相关材料，是否影响药品或者医疗器械安全性、有效性评价结果，以及是否属于严重不良事件等专门性问题难以确定的，可以根据国家药品监督管理部门设置或者指定的药品、医疗器械审评等机构出具的意见，结合其他证据作出认定。

第九条 本解释所称“合同研究组织”，是指受药品或者医疗器械注册申请单位、药物非临床研究机构、药物或者医疗器械临床试验机构的委托，从事试验方案设计、数据统计、分析测试、监查稽查等与非临床研究或者临床试验相关活动的单位。

第十条 本解释自2017年9月1日起施行。

TC260-PG-20202A 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

时效性：　　现行有效

发布机关：　全国信息安全标准化技术委员会秘书处

发布日期：　2020 年 07 月

评估点一：是否公开收集使用个人信息的规则

1.1 是否公开隐私政策等收集使用规则

a)隐私政策通过弹窗、文本链接、附件、常见问题（FAQs）等界面或形式展示。

b)隐私政策中包含收集使用个人信息规则的相关内容。

c)隐私政策文本链接有效，文本可正常显示。

d)如存在涉及收集使用儿童个人信息相关业务功能的，需制定针对儿童的个人信息保护规则[1]。

1.2 是否提示用户阅读隐私政策等收集使用规则

a)在 App 首次运行或用户注册时主动提示用户阅读隐私政策[2]。

b)避免使用不明显的方式展示隐私政策链接，导致用户不易发现隐私政策[3]。

1.3 隐私政策等收集使用规则是否易于访问

---

[1] 注 1：详见 2019 年国家互联网信息办公室令（第 4 号）《儿童个人信息网络保护规定》；例如收集不满十四周岁的未成年人个人信息的教育类 App，需制定针对儿童的个人信息保护规则。

[2] 注：例如可采用通过弹窗、突出链接等主动方式提示用户阅读隐私政策。

[3] 注：例如采用与背景颜色相近的字体、刻意缩小字号、弹出键盘遮挡、置于边缘等为不明显方式展示隐私政策链接。

a)用户进入主功能界面后，通过4次（含）以内的点击等操作，能够访问到隐私政策。

b)尽可能在界面的固定路径展示隐私政策（或其链接），以便用户随时访问和获取，避免仅在注册/登录界面展示隐私政策链接，或只能以咨询客服等方式查找隐私政策等情形[1]。

c)隐私政策以单独成文的形式发布，而不是作为用户协议、用户须知等文件中的一部分存在[2]。

信息收集使用规则，则尽可能显著标识并以连续篇幅呈现。

1.4 隐私政策等收集使用规则是否易于阅读

a)隐私政策文本文字显示方式不会造成阅读困难[3]。

b)提供简体中文版隐私政策。

c)隐私政策内容使用标准化的数字、图示，采用通用的语言习惯，避免误用概念、术语或存在有歧义的语句等。

1.5 公开的收集使用规则是否完整

a)对App运营者基本情况进行描述，至少包括组织名称、注册地址或常用办公地址、个人信息保护工作机构或相关负责人联系方式。

b)说明隐私政策的发布、生效或更新日期。

---

[1] 注：例如通过“我--设置--关于”或者“我的--设置--隐私”等用户熟悉路径展示隐私政策，不频繁变更展示隐私政策的路径；在首次展示隐私政策时，宜说明查找隐私政策的方法、路径。

[2] 注：如果因展示条件等特殊原因使用用户协议、用户须知等文件描述个人

[3] 注：例如可采取与App其他界面等同的样式；例如文本字号过小、颜色与背景色相近、行间距过密、字迹模糊、列宽大于手机屏幕等易造成阅读困难。

c)说明收集使用个人信息的目的、方式、范围[1]。

d)对个人信息存放地域（境内、境外哪个国家或地区）、存储期限（法律规定范围内最短期限或明确的期限）、超期处理方式进行说明。

e)如果将个人信息用于用户画像、个性化展示等，说明其应用场景和可能对用户权益产生的影响[2]。

f)如果存在个人信息出境情形，说明出境个人信息类型并显著标识[3]。

g)对个人信息保护方面采取的措施和具备的能力进行说明。

h)如果存在个人信息对外共享、转让、公开披露的情况，说明以下内容：①对外共享、转让、公开披露个人信息的目的；②涉及的个人信息类型；③接收方类型或身份。

i)对以下用户权利和相关操作方法进行说明：①个人信息查询；②个人信息更正；③个人信息删除；④用户账号注销；⑤撤回已同意的授权。

j)至少说明以下一种投诉、举报渠道：①电子邮件；②电话；③在线客服；④在线表单；⑤即时通信账号[4]。

评估点二：是否明示收集使用个人信息的目的、方式和范围

---

[1] 注：详见本《实践指南》2.1 节。

[2] 注：如部分业务功能不涉及用户画像、个性化展示，可在规则中明确说明。

[3] 注：例如可采用字体加粗、标星号、下划线、斜体、不同颜色等显著标识方式。

[4] 注：本节相关定义和内容可参考 GB/T 35273-2020《信息安全技术 个人信息安全规范》5.5 节。

2.1 是否逐一列出收集使用个人信息的目的、方式、范围等

a)完整、清晰、区分说明各业务功能所收集的个人信息。宜根据用户使用习惯逐项说明各业务功能收集个人信息的目的、类型、方式，避免使用“等、例如”等方式不完整列举[1]。

b)使用 Cookie 等同类技术（包括脚本、Clickstream、Web 信标、Flash Cookie、内嵌 Web 链接等）收集个人信息时，简要说明相关机制，以及收集个人信息的目的、类型。

c)如嵌入的第三方代码、插件（如 SDK）收集个人信息，说明第三方代码、插件的类型或名称，及收集个人信息的目的、类型、方式[2]。

2.2 收集使用个人信息的目的、方式、范围发生变化时是否通知用户

a)收集使用个人信息的目的、方式和范围发生变化时，以适当方式通知用户[3]。

2.3 是否同步告知申请打开权限和要求提供个人敏感信息的目的

a)在申请打开可收集个人信息权限时，通过显著方式同步告知用

---

[1] 注：业务功能通常是指 App 为面向用户的具体使用需求所提供的一类完整的服务类型，如地图导航、网络约车、即时通信、网络支付、新闻资讯、网上购物、短视频、快递物流、餐饮外卖、交通票务、婚恋相亲、房屋租 售、求职招聘、网络借贷等。

[2] 注：例如可采用隐私政策、弹窗提示、文字备注、文本链接等方式说明。

[3] 注：例如可采用更新隐私政策等收集使用规则并以推送消息、邮件、弹窗、红点提示等方式提醒用户阅读发生变化的条款。

户其目的，对目的的描述明确、易懂[1]。

b)在要求用户提供个人敏感信息时，通过显著方式同步告知用户其目的，对目的的描述明确、易懂[2]。

2.4 收集使用规则是否易于理解

a)有关收集使用规则的内容需简练、结构清晰、重点突出。注：例如使用晦涩难懂的词语、冗长繁琐的篇幅、大量专业术语、逻辑结构混乱等易造成用户难以理解。

评估点三：是否征得用户同意后才收集使用个人信息

3.1 收集个人信息或打开可收集个人信息权限前是否征得用户同意

a)收集个人信息前提供可由用户自主作出同意或不同意的选项[3]

b)未征得用户同意前，不收集个人信息或打开可收集个人信息权限[4]。

---

[1] 注：常见可收集个人信息权限类型有：iOS 系统:定位、通讯录、日历、提醒事项、照片、麦克风、相机、健康等；Android 系统:日历、通话记录、相机、通讯录、位置、麦克风、电话、传感器、短信、存储等；例如可采用弹窗提示、用途描述等显著方式告知。

[2] 注：个人敏感信息定义见 GB/T 35273-2020《信息安全技术 个人信息安全规范》3.2 节；例如可采用弹窗提示、用途描述等显著方式告知。

[3] 注：例如提供“退出”“上一步”“关闭”“取消”的按钮等方式供用户作出不同意的选项。

[4] 注：例如用户首次使用 App 时，在未得知收集个人信息的目的并作出同意前，App 就开始收集个人信息的行为属于未征得用户同意收集个人信息；相关定义和内容可参考 GB/T 35273-2020《信息安全技术 个人信息安全规范》5.4 节。

c)未征得用户同意前，不利用 Cookie 等同类技术或通过调用可收集用户个人信息的权限、接口等方式收集个人信息。

3.2 用户明确表示不同意收集后是否仍收集个人信息

a)用户通过拒绝提供个人信息、不同意收集使用规则、拒绝提供或关闭权限等操作，明确表示不同意收集某类个人信息后，不以任何形式收集该类个人信息或打开该类可收集个人信息权限。

3.3 用户明确表示不同意收集后是否频繁征求用户同意、干扰用户正常使用

a)用户明确表示不同意收集后，不在每次重新打开 App、或使用某一业务功能时，向用户频繁询问（如 48 小时内询问超过一次）是否同意收集该类个人信息。

b)用户明确表示不同意打开某类可收集个人信息权限后，不在每次重新打开 App、或使用某一业务功能时，向用户频繁询问（如 48 小时内询问超过一次）是否同意打开该类可收集个人信息权限[1]。

3.4 实际收集的个人信息是否超出用户授权范围

a)收集使用个人信息的过程需与其所声明的隐私政策等收集使用规则保持一致。实际收集的个人信息类型、申请打开可收集使用个人信息的权限等与隐私政策等收集使用规则中相关内容一致，不超出隐私政策等收集使用规则所述范围。

---

[1] 注：为支持 App 正常运行，或用户主动选择使用的某一具体功能触发征得同意的动作，不属于频繁干扰情形。例如用户拒绝授权“相机”权限后的 48 小时内，主动选择使用拍摄、扫码等功能时，App 再次申请打开该权限的情形不属于频繁干扰。

3.5 是否以默认选择同意隐私政策等非明示方式征求用户同意

a)在首次运行、用户注册等时，可通过弹窗、突出链接等明示方式提醒用户阅读隐私政策后征求用户同意，不采用默认勾选隐私政策等非明示方式。

b)通过设置“下一步”“注册”“登录即代表同意”等方式征求用户同意的情形，除以显著方式展示隐私政策等收集使用规则外，还需明确执行上述动作与同意隐私政策之间的逻辑关系，以达到主动提醒用户主动阅读隐私政策后征求用户同意的效果。

3.6 是否未经用户同意更改其设置的可收集个人信息权限状态

a)未经用户同意，不私自更改用户设置的可收集个人信息权限和收集使用个人信息相关功能的状态[1]。

3.7 存在定向推送信息情形的是否提供非定向推送信息的选项

a)存在利用用户个人信息和算法定向推送信息情形时（包括利用个人信息和个性化推荐算法等推送新闻和信息、展示商品、推送广告等），需为用户提供拒绝接收定向推送信息，或停止、退出、关闭相应功能的机制，或不基于个人信息和个性化推荐算法等推送的模式、选项[2]。

3.8 是否以不正当方式误导用户同意收集个人信息

a)明示收集使用个人信息的目的需真实、准确。不故意欺瞒、掩

[1] 注：例如未经用户同意，在更新升级后，将用户设置的可收集个人信息权限恢复到默认状态，或将用户已关闭的使用通讯录匹配好友等功能重新打开。

[2] 注：相关定义和内容可参考 GB/T 35273-2020《信息安全技术 个人信息安全规范》7.5 节。

饰收集使用个人信息的真实目的，不诱骗用户同意收集个人信息或打开可收集个人信息权限[1]。

3.9 是否向用户提供撤回同意收集个人信息的途径、方式

a)向用户提供撤回同意收集个人信息的途径、方式，并在隐私政策等收集使用规则中予以明确。

b)如用户拒绝或撤回特定业务功能收集个人信息的同意时，除非用户拒绝或撤回的个人信息是其他业务功能所必需，否则不暂停其他业务功能，或降低其他业务功能的服务质量。

c)如用户拒绝或关闭可收集个人信息权限时，不影响用户正常使用与该权限无关的业务功能，除非该权限是保证 App 正常运行所必需[2]。

3.10 是否违反其所声明的收集使用规则

a)开展个人信息处理活动需严格遵循所公开的隐私政策等收集使用规则，并遵守与用户的约定；如个人信息使用目的、方式、范围等发生变化的，需再次征得用户同意。

评估点四：是否遵循必要原则，仅收集与其提供的服务相关的个人信息

4.1 是否收集与业务功能无关的个人信息

---

[1] 注：例如 App 提示用户打开通讯录权限以参与红包、金币、抽奖等活动。事实上，通讯录权限与上述活动之间毫无关联，App 诱骗用户打开通讯录权限后，立即上传用户通讯录信息，并将该类信息用于发送商业广告或其它目的。

[2] 注 1：相关定义和内容可参考 GB/T 35273-2020《信息安全技术个人信息安全规范》8.4 节;如用户需要撤回对同意 App 收集使用其所有个人信息的授权，可采取注销账号等方式执行。

a)不收集与业务功能无关的个人信息。

b)不申请打开与业务功能无关的可收集个人信息权限。

4.2 用户是否可拒绝收集非必要信息或打开非必要权限

a)收集与业务功能相关但非必要的个人信息或申请打开相关但非必要的可收集个人信息权限时，需由用户自主选择同意，如用户不同意，不影响其使用现有业务功能或相关服务。

b)不将同意收集其他业务功能所需的个人信息或同意打开其他业务功能所需的可收集个人信息权限，作为用户使用当前业务功能的前提条件。

c)如提供无需注册即可使用的服务模式（如仅浏览、游客模式），当用户拒绝同意该类服务模式以外的个人信息收集行为时，不影响其使用仅浏览等功能[1]。

4.3 是否以非正当方式强迫收集用户个人信息

a)根据用户主动填写、点击、勾选等自主行为，作为各个业务功能收集使用个人信息的前提条件。

b)新增业务功能申请收集的个人信息超出用户原有同意范围时，不因用户拒绝新增业务功能收集个人信息的请求，拒绝提供原有业务功能，新增业务功能取代原有业务功能的除外。

---

[1] 注 1：必要信息指与业务功能直接相关的个人信息，缺少该个人信息则无法提供最基本的服务。必要信息范围可参考《信息安全技术 移动互联网应用程序（App）收集个人信息基本规范》，如果服务类型不在该标准内，则可根据其业务特点，参考该标准相关定义和理念自行分析;相关内容和实践案例可参考 GB/T 35273-2020《信息安全技术 个人信息安全规范》5.3 节及其附录 C。

c)不仅以改善服务质量、提升使用体验、研发新产品、定向推送信息、增强安全性等为由，强制要求个人信息主体同意收集个人信息。

d)不以捆绑方式强制要求用户一次性同意打开多个可收集个人信息权限[1]。

4.4 收集个人信息的频度是否超出业务功能实际需要

a)收集个人信息的频度不超出业务功能实际需要，在用户使用某业务功能过程中，仅收集与当前业务功能相关的个人信息。

b)在 App 未打开或处于后台运行状态时，不收集用户个人信息，除非业务功能需要后台运行时继续提供服务，如导航功能等[2]。

c)接入第三方应用时，不私自截留第三方应用收集的个人信息[3]。

评估点五：是否经用户同意后才向他人提供个人信息

5.1 向他人提供个人信息前是否征得用户同意

a)如存在从客户端直接向第三方发送个人信息的情形，包括通过客户端嵌入第三方代码、插件（如 SDK）等方式向第三方发送个人信息的情形，需事先征得用户同意，经匿名化处理的除外。

b)如个人信息传输至服务器后，App 运营者向第三方提供其收集的个人信息，需事先征得用户同意，经匿名化处理的除外。

---

[1] 注：例如将安卓版 App 的 targetSdkVersion 值设置低于 23，通过声明机制，在安装 App 时要求用户一次性同意打开多个可收集个人信息权限属于捆绑方式。

[2] 注：在用户主动关闭 App 后，未经用户同意不采用自启动、关联启动方式收集个人信息。

[3] 注：例如信息查询类 App，在用户向第三方应用提交相关个人信息时，截留用户个人信息并上传至其后端服务器的行为属于私自截留个人信息。

c)如向第三方传输的个人信息类型、接收数据的第三方身份等发生变更的，需以适当方式通知用户，并征得用户同意[1]。

5.2 向接入的第三方应用提供个人信息前是否经用户同意

a)如 App 接入第三方应用，当用户使用第三方应用时，需在征得用户同意后，再向第三方应用提供个人信息；当用户获知应用为第三方提供后，自行以主动填写等方式向第三方直接授权的除外。

b)App 运营者宜对于接入的第三方应用收集个人信息的合法、正当、必要性等方面进行审核，明确标识相关业务功能为第三方提供，并提醒用户关注第三方应用收集使用个人信息的规则[2]。

评估点六：是否提供删除或更正个人信息功能，或公布投诉、举报方式等信息

6.1 是否提供有效的注销用户账号功能

a)提供有效的注销账号途径，并在用户注销账号后，及时删除其个人信息或进行匿名化处理[3]。

b)受理注销账号请求后，在承诺时限内（承诺时限不得超过 15 个工作日，无承诺时限的，以 15 个工作日为限）完成核查和处理。

c)注销账号的过程简单易操作，不设置不必要或不合理的注销条件[4]。

---

[1] 注：“匿名化”的定义可参考 GB/T 35273-2020《信息安全技术 个人信息安全规范》3.14 节。

[2] 注：第三方接入管理相关内容可参考 GB/T 35273-2020《信息安全技术个人信息安全规范》9.7 节。

[3] 注：例如可提供在线操作、客服电话、电子邮件等注销账号的途径。

[4] 注：不必要或不合理的注销条件相关内容可参考 GB/T 35273-2020《信息安全技术 个人信息安全规范》8.5 节。

6.2 是否提供有效的更正或删除个人信息途径

a)提供有效的查询、更正、删除个人信息的途径[1]。

b)无法通过在线操作方式及时响应个人信息查询、更正、删除请求的，在承诺时限内（承诺时限不超过 15 个工作日，无承诺时限的，以 15 个工作日为限）完成核查和处理。

c)查询、更正和删除个人信息的过程简单易操作，不设置不必要或不合理的条件。

d)用户更正、删除个人信息等操作完成时，后台需及时执行完成相关操作。

6.3 是否建立并公布个人信息安全投诉、举报渠道

a)建立并公布可受理个人信息安全问题相关的投诉、举报渠道。

注：例如可采取电子邮件、电话、在线客服、在线表单、即时通讯账号等受理方式。

妥善受理用户关于个人信息相关的投诉、举报，并在承诺时限内（承诺时限不超过 15 个工作日，无承诺时限的，以 15 个工作日为限）受理并处理。

[1] 注：隐私政策中注明的，经证实无法完成相关操作的，视为无效途径。

GB/T35273-2020 信息安全技术 个人信息安全规范

时效性：　　现行有效

发布机关：　国家市场监督管理总局、国家标准化管理委员会

类别：　　中华人民共和国国家标准

发布日期：　2020 年 03 月 06 日

实施日期：　2020 年 10 月 01 日

1　范围

本标准规定了开展收集、存储、使用、共享、转让、公开披露、删除等个人信息处理活动应遵循的原则和安全要求。

本标准适用于规范各类组织的个人信息处理活动，也适用于主管监管部门、第三方评估机构等组织对个人信息处理活动进行监督、管理和评估。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 25069—2010 信息安全技术术语

3　术语和定义

GB/T 25069—2010 界定的以及下列术语和定义适用于本文件。

3.1

个人信息 personal information

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[1]。

3.2

个人敏感信息 personal sensitive information

一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息[2]。

3.3

个人信息主体 personal information subject

个人信息所标识或者关联的自然人。

3.4

个人信息控制者 personal information controller

有能力决定个人信息处理目的、方式等的组织或个人。

3.5

收集 collect

---

[1] 注：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;关于个人信息的判定方法和类型参见附录 A;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。

[2] 注 1：个人敏感信息包括身份证件号码、个人生物识别信息、银行账户、通信记录和内容、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息、14 岁以下（含）儿童的个人信息等; 2：关于个人敏感信息的判定方法和类型参见附录 B;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。

获得个人信息的控制权的行为[1]。

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[2]。

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[3]。

3.8 用户画像 user profiling

通过收集、汇聚、分析个人信息，对某特定自然人个人特征，如职业、经济、健康、教育、个人喜好、信用、行为等方面作出分析或预测，形成其个人特征模型的过程[4]。

---

[1] 注：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;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。

[2] 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] 注：包括通过积极的行为作出授权（即明示同意），或者通过消极的不作为而作出授权（如信息采集区域内的个人信息主体在被告知信息收集行为后没有离开该区域）。

[4] 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[1]。

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[2]。

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[3]。

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，

[1] 注：个人信息经匿名化处理后所得的信息不属于个人信息。

[2] 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] 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。

对其个人信息处理活动对个人信息主体合法权益造成的损害承担责任；

b)目的明确：具有明确、清晰、具体的个人信息处理目的；

c)选择同意：向个人信息主体明示个人信息处理目的、方式、范围等规则，征求其授权同意；

d)最小必要：只处理满足个人信息主体授权同意的目的所需的最少个人信息类型和数量。目的达成后，应及时删除个人信息；

e)公开透明：以明确、易懂和合理的方式公开处理个人信息的范围、目的、规则等，并接受外部监督；

f)确保安全：具备与所面临的安全风险相匹配的安全能力，并采取足够的管理措施和技术手段，保护个人信息的保密性、完整性、可用性；

g)主体参与：向个人信息主体提供能够查询、更正、删除其个人信息，以及撤回授权同意、注销账户、投诉等方法。

5 个人信息的收集

5.1 收集个人信息的合法性

对个人信息控制者的要求包括：

a)不应以欺诈、诱骗、误导的方式收集个人信息；

b)不应隐瞒产品或服务所具有的收集个人信息的功能；

c)不应从非法渠道获取个人信息。

5.2 收集个人信息的最小必要

对个人信息控制者的要求包括：

a)收集的个人信息的类型应与实现产品或服务的业务功能有直接关联；直接关联是指没有上述个人信息的参与，产品或服务的功能无法实现；

b)自动采集个人信息的频率应是实现产品或服务的业务功能所必需的最低频率；

c)间接获取个人信息的数量应是实现产品或服务的业务功能所必需的最少数量。

5.3 多项业务功能的自主选择

当产品或服务提供多项需收集个人信息的业务功能时，个人信息控制者不应违背个人信息主体的自主意愿，强迫个人信息主体接受产品或服务所提供的业务功能及相应的个人信息收集请求。对个人信息控制者的要求包括：

a)不应通过捆绑产品或服务各项业务功能的方式，要求个人信息主体一次性接受并授权同意其未申请或使用的业务功能收集个人信息的请求；

b)应把个人信息主体自主作出的肯定性动作，如主动点击、勾选、填写等，作为产品或服务的特定业务功能的开启条件。个人信息控制者应仅在个人信息主体开启该业务功能后，开始收集个人信息；

c)关闭或退出业务功能的途径或方式应与个人信息主体选择使用业务功能的途径或方式同样方便。个人信息主体选择关闭或退出特定业务功能后，个人信息控制者应停止该业务功能的个人信息收集活动；

d)个人信息主体不授权同意使用、关闭或退出特定业务功能的，

不应频繁征求个人信息主体的授权同意；

e)个人信息主体不授权同意使用、关闭或退出特定业务功能的，不应暂停个人信息主体自主选择使用的其他业务功能，或降低其他业务功能的服务质量；

f)不得仅以改善服务质量、提升使用体验、研发新产品、增强安全性等为由，强制要求个人信息主体同意收集个人信息。

5.4 收集个人信息时的授权同意

对个人信息控制者的要求包括：

a)收集个人信息，应向个人信息主体告知收集、使用个人信息的目的、方式和范围等规则，并获得个人信息主体的授权同意[1]；

b)收集个人敏感信息前，应征得个人信息主体的明示同意，并应确保个人信息主体的明示同意是其在完全知情的基础上自主给出的、具体的、清晰明确的意愿表示；

c)收集个人生物识别信息前，应单独向个人信息主体告知收集、使用个人生物识别信息的目的、方式和范围，以及存储时间等规则，并征得个人信息主体的明示同意[2]；

d)收集年满 14 周岁未成年人的个人信息前，应征得未成年人或其

---

[1] 注 1：如产品或服务仅提供一项收集、使用个人信息的业务功能时，个人信息控制者可通过个人信息保护政策的形式，实现向个人信息主体的告知；产品或服务提供多项收集、使用个人信息的业务功能的，除个人信息保护政策外，个人信息控制者宜在实际开始收集特定个人信息时，向个人信息主体提供收集、使用该个人信息的目的、方式和范围，以便个人信息主体在作出具体的授权同意前，能充分考虑对其的具体影响;符合 5.3 和 a）要求的实现方法，可参考附录 C。

[2] 注：个人生物识别信息包括个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部识别特征等。

监护人的明示同意；不满 14 周岁的，应征得其监护人的明示同意；

e)间接获取个人信息时：

1)应要求个人信息提供方说明个人信息来源，并对其个人信息来源的合法性进行确认；

2)应了解个人信息提供方已获得的个人信息处理的授权同意范围，包括使用目的，个人信息主体是否授权同意转让、共享、公开披露、删除等；

3)如开展业务所需进行的个人信息处理活动超出已获得的授权同意范围的，应在获取个人信息后的合理期限内或处理个人信息前，征得个人信息主体的明示同意，或通过个人信息提供方征得个人信息主体的明示同意。

5.5 个人信息保护政策

对个人信息控制者的要求包括：

a)应制定个人信息保护政策，内容应包括但不限于：

1)个人信息控制者的基本情况，包括主体身份、联系方式；

2)收集、使用个人信息的业务功能，以及各业务功能分别收集的个人信息类型。涉及个人敏感信息的，需明确标识或突出显示；

3)个人信息收集方式、存储期限、涉及数据出境情况等个人信息处理规则；

4)对外共享、转让、公开披露个人信息的目的、涉及的个人信息类型、接收个人信息的第三方类型，以及各自的安全和法律责任；

5)个人信息主体的权利和实现机制，如查询方法、更正方法、删

除方法、注销账户的方法、撤回授权同意的方法、获取个人信息副本的方法、对信息系统自动决策结果进行投诉的方法等；

6)提供个人信息后可能存在的安全风险，及不提供个人信息可能产生的影响；

7)遵循的个人信息安全基本原则，具备的数据安全能力，以及采取的个人信息安全保护措施，必要时可公开数据安全和个人信息保护相关的合规证明；

8)处理个人信息主体询问、投诉的渠道和机制，以及外部纠纷解决机构及联络方式。

b)个人信息保护政策所告知的信息应真实、准确、完整；

c)个人信息保护政策的内容应清晰易懂，符合通用的语言习惯，使用标准化的数字、图示等，避免使用有歧义的语言；

d)个人信息保护政策应公开发布且易于访问，例如，在网站主页、移动互联网应用程序安装页、附录 C 中的交互界面或设计等显著位置设置链接；

e)个人信息保护政策应逐一送达个人信息主体。当成本过高或有显著困难时，可以公告的形式发布；

f)在 a）所载事项发生变化时，应及时更新个人信息保护政策并重新告知个人信息主体[1]。

---

[1] 注：组织会习惯性将个人信息保护政策命名为“隐私政策”或其他名称，其内容宜与个人信息保护政策内容保持一致;个人信息保护政策的内容可参考附录 D;在个人信息主体首次打开产品或服务、注册账户等情形时，宜通过弹窗等形式主动向其展示个人信息保护政策的主要或核心内容，帮助个人信息主体理解该产品或服务的个人信息处理范围和规则，并决定

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[1]；

h)从合法公开披露的信息中收集个人信息的，如合法的新闻报道、政府信息公开等渠道；

i)维护所提供产品或服务的安全稳定运行所必需的，如发现、处置产品或服务的故障；

j)个人信息控制者为新闻单位，且其开展合法的新闻报道所必需的；

k)个人信息控制者为学术研究机构，出于公共利益开展统计或学术研究所必要，且其对外提供学术研究或描述的结果时，对结果中所包含的个人信息进行去标识化处理的。

是否继续使用该产品或服务。

[1] 注：个人信息保护政策的主要功能为公开个人信息控制者收集、使用个人信息范围和规则，不宜将其视为合同。

6 个人信息的存储

6.1 个人信息存储时间最小化

对个人信息控制者的要求包括：

a)个人信息存储期限应为实现个人信息主体授权使用的目的所必需的最短时间，法律法规另有规定或者个人信息主体另行授权同意的除外；

b)超出上述个人信息存储期限后，应对个人信息进行删除或匿名化处理。

6.2 去标识化处理

收集个人信息后，个人信息控制者宜立即进行去标识化处理，并采取技术和管理方面的措施，将可用于恢复识别个人的信息与去标识化后的信息分开存储并加强访问和使用的权限管理。

6.3 个人敏感信息的传输和存储

对个人信息控制者的要求包括：

a)传输和存储个人敏感信息时，应采用加密等安全措施[1]；

b)个人生物识别信息应与个人身份信息分开存储；

c)原则上不应存储原始个人生物识别信息（如样本、图像等），可采取的措施包括但不限于：

1)仅存储个人生物识别信息的摘要信息；

2)在采集终端中直接使用个人生物识别信息实现身份识别、认证等功能；

[1] 注：采用密码技术时宜遵循密码管理相关国家标准。

3)在使用面部识别特征、指纹、掌纹、虹膜等实现识别身份、认证等功能后删除可提取个人生物识别信息的原始图像[1]。

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

[1] 注：摘要信息通常具有不可逆特点，无法回溯到原始信息;个人信息控制者履行法律法规规定的义务相关的情形除外。

[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；

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[2]。

---

[1] 注：个人信息保护责任人或个人信息保护工作机构的确定见 11.1。

[2] 注：将所收集的个人信息用于学术研究或得出对自然、科学、社会、经济等现象总体状态的描述，属于与收集目的具有合理关联的范围之内。但对外提供学术研究或描述的结果时，需对结果中所包含的个人信息进行去标识化处理;加工处理而产生的个人信息属于个人敏感信息的，对其处理需符合对个人敏感信息的要求。

7.4 用户画像的使用限制

对个人信息控制者的要求包括：

a)用户画像中对个人信息主体的特征描述，不应：

1)包含淫秽、色情、赌博、迷信、恐怖、暴力的内容；

2)表达对民族、种族、宗教、残疾、疾病歧视的内容。

b)在业务运营或对外业务合作中使用用户画像的，不应：

1)侵害公民、法人和其他组织的合法权益；

2)危害国家安全、荣誉和利益，煽动颠覆国家政权、推翻社会主义制度，煽动分裂国家、破坏国家统一，宣扬恐怖主义、极端主义，宣扬民族仇恨、民族歧视，传播暴力、淫秽色情信息，编造、传播虚假信息扰乱经济秩序和社会秩序。

c)除为实现个人信息主体授权同意的使用目的所必需外，使用个人信息时应消除明确身份指向性，避免精确定位到特定个人。例如，为准确评价个人信用状况，可使用直接用户画像，而用于推送商业广告目的时，则宜使用间接用户画像。

7.5 个性化展示的使用

对个人信息控制者的要求包括：

a)在向个人信息主体提供业务功能的过程中使用个性化展示的，应显著区分个性化展示的内容和非个性化展示的内容[1]；

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

[1] 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。

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[1]；

c)在向个人信息主体推送新闻信息服务的过程中使用个性化展示的，应：

1)为个人信息主体提供简单直观的退出或关闭个性化展示模式的选项；

2)当个人信息主体选择退出或关闭个性化展示模式时，向个人信息主体提供删除或匿名化定向推送活动所基于的个人信息的选项。

d)在向个人信息主体提供业务功能的过程中使用个性化展示的，宜建立个人信息主体对个性化展示所依赖的个人信息（如标签、画像维度等）的自主控制机制，保障个人信息主体调控个性化展示相关性程度的能力。

7.6 基于不同业务目的所收集个人信息的汇聚融合

对个人信息控制者的要求包括：

a)应遵守 7.3 的要求；

b)应根据汇聚融合后个人信息所用于的目的，开展个人信息安全影响评估，采取有效的个人信息保护措施。

7.7 信息系统自动决策机制的使用

个人信息控制者业务运营所使用的信息系统，具备自动决策机制且能对个人信息主体权益造成显著影响的（例如，自动决定个人征信及贷款额度，或用于面试人员的自动化筛选等），应：

---

[1] 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。

a)在规划设计阶段或首次使用前开展个人信息安全影响评估，并依评估结果采取有效的保护个人信息主体的措施；

b)在使用过程中定期（至少每年一次）开展个人信息安全影响评估，并依评估结果改进保护个人信息主体的措施；

c)向个人信息主体提供针对自动决策结果的投诉渠道，并支持对自动决策结果的人工复核。

8 个人信息主体的权利

8.1 个人信息查询

个人信息控制者应向个人信息主体提供查询下列信息的方法：

a)其所持有的关于该主体的个人信息或个人信息的类型；

b)上述个人信息的来源、所用于的目的；

c)已经获得上述个人信息的第三方身份或类型[1]。

8.2 个人信息更正

个人信息主体发现个人信息控制者所持有的该主体的个人信息有错误或不完整的，个人信息控制者应为其提供请求更正或补充信息的方法。

8.3 个人信息删除

对个人信息控制者的要求包括：

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] 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。

1)个人信息控制者违反法律法规规定，收集、使用个人信息的；

2)个人信息控制者违反与个人信息主体的约定，收集、使用个人信息的。

b)个人信息控制者违反法律法规规定或违反与个人信息主体的约定向第三方共享、转让个人信息，且个人信息主体要求删除的，个人信息控制者应立即停止共享、转让的行为，并通知第三方及时删除；

c)个人信息控制者违反法律法规规定或违反与个人信息主体的约定，公开披露个人信息，且个人信息主体要求删除的，个人信息控制者应立即停止公开披露的行为，并发布通知要求相关接收方删除相应的信息。

8.4 个人信息主体撤回授权同意

对个人信息控制者的要求包括：

a)应向个人信息主体提供撤回收集、使用其个人信息的授权同意的方法。撤回授权同意后，个人信息控制者后续不应再处理相应的个人信息；

b)应保障个人信息主体拒绝接收基于其个人信息推送商业广告的权利。对外共享、转让、公开披露个人信息，应向个人信息主体提供撤回授权同意的方法[1]。

8.5 个人信息主体注销账户

对个人信息控制者的要求包括：

a)通过注册账户提供产品或服务的个人信息控制者，应向个人信

[1] 注：撤回授权同意不影响撤回前基于授权同意的个人信息处理。

息主体提供注销账户的方法，且方法简便易操作；

b)受理注销账户请求后，需要人工处理的，应在承诺时限内（不超过 15 个工作日）完成核查和处理；

c)注销过程如需进行身份核验，要求个人信息主体再次提供的个人信息类型不应多于注册、使用等服务环节收集的个人信息类型；

d)注销过程不应设置不合理的条件或提出额外要求增加个人信息主体义务，如注销单个账户视同注销多个产品或服务，要求个人信息主体填写精确的历史操作记录作为注销的必要条件等[1]；

e)注销账户的过程需收集个人敏感信息核验身份时，应明确对收集个人敏感信息后的处理措施，如达成目的后立即删除或匿名化处理等；

f)个人信息主体注销账户后，应及时删除其个人信息或匿名化处理。因法律规规定需要留存个人信息的，不能再次将其用于日常业务活动中。

8.6 个人信息主体获取个人信息副本

根据个人信息主体的请求，个人信息控制者宜为个人信息主体提供获取以下类型个人信息副本的方法，或在技术可行的前提下直接将以下类型个人信息的副本传输给个人信息主体指定的第三方：

a)本人的基本资料、身份信息；

[1] 注：多个产品或服务之间存在必要业务关联关系的，例如，一旦注销某个产品或服务的账户，将会导致其他产品或服务的必要业务功能无法实现或者服务质量明显下降的，需向个人信息主体进行详细说明;产品或服务没有独立的账户体系的，可采取对该产品或服务账号以外其他个人信息进行删除，并切断账户体系与产品或服务的关联等措施实现注销。

b)本人的健康生理信息、教育工作信息。

8.7 响应个人信息主体的请求

对个人信息控制者的要求包括：

a)在验证个人信息主体身份后，应及时响应个人信息主体基于8.1~8.6提出的请求，应在三十天内或法律法规规定的期限内作出答复及合理解释，并告知个人信息主体外部纠纷解决途径；

b)采用交互式页面（如网站、移动互联网应用程序、客户端软件等）提供产品或服务的，宜直接设置便捷的交互式页面提供功能或选项，便于个人信息主体在线行使其访问、更正、删除、撤回授权同意、注销账户等权利；

c)对合理的请求原则上不收取费用，但对一定时期内多次重复的请求，可视情收取一定成本费用；

d)直接实现个人信息主体的请求需要付出高额成本或存在其他显著困难的，个人信息控制者应向个人信息主体提供替代方法，以保障个人信息主体的合法权益；

e)以下情行可不响应个人信息主体基于8.1~8.6提出的请求，包括：

1)与个人信息控制者履行法律法规规定的义务相关的；

2)与国家安全、国防安全直接相关的；

3)与公共安全、公共卫生、重大公共利益直接相关的；

4)与刑事侦查、起诉、审判和执行判决等直接相关的；

5)个人信息控制者有充分证据表明个人信息主体存在主观恶意或滥用权利的；

6)出于维护个人信息主体或其他个人的生命、财产等重大合法权益但又很难得到本人授权同意的；

7)响应个人信息主体的请求将导致个人信息主体或其他个人、组织的合法权益受到严重损害的；

8)涉及商业秘密的。

f)如决定不响应个人信息主体的请求，应向个人信息主体告知该决定的理由，并向个人信息主体提供投诉的途径。

8.8 投诉管理

个人信息控制者应建立投诉管理机制和投诉跟踪流程，并在合理的时间内对投诉进行响应。

9 个人信息的委托处理、共享、转让、公开披露

9.1 委托处理

个人信息控制者委托第三方处理个人信息时，应符合以下要求：

a)个人信息控制者作出委托行为，不应超出已征得个人信息主体授权同意的范围或应遵守 5.6 所列情形；

b)个人信息控制者应对委托行为进行个人信息安全影响评估，确保受委托者达到 11.5 的数据安全能力要求；

c)受委托者应：

1)严格按照个人信息控制者的要求处理个人信息。受委托者因特殊原因未按照个人信息控制者的要求处理个人信息的，应及时向个人信息控制者反馈；

2)受委托者确需再次委托时，应事先征得个人信息控制者的授权；

3)协助个人信息控制者响应个人信息主体基于 8.1~8.6 提出的请求；

4)受委托者在处理个人信息过程中无法提供足够的安全保护水平或发生了安全事件的，应及时向个人信息控制者反馈；

5)在委托关系解除时不再存储相关个人信息。

d)个人信息控制者应对受委托者进行监督，方式包括但不限于：

1)通过合同等方式规定受委托者的责任和义务；

2)对受委托者进行审计。

e)个人信息控制者应准确记录和存储委托处理个人信息的情况；

f)个人信息控制者得知或者发现受委托者未按照委托要求处理个人信息，或未能有效履行个人信息安全保护责任的，应立即要求受托者停止相关行为，且采取或要求受委托者采取有效补救措施（如更改口令、回收权限、断开网络连接等）控制或消除个人信息面临的安全风险。必要时个人信息控制者应终止与受委托者的业务关系，并要求受委托者及时删除从个人信息控制者获得的个人信息。

9.2 个人信息共享、转让

个人信息控制者共享、转让个人信息时，应充分重视风险。共享、转让个人信息，非因收购、兼并、重组、破产原因的，应符合以下要求：

a)事先开展个人信息安全影响评估，并依评估结果采取有效的保护个人信息主体的措施；

b)向个人信息主体告知共享、转让个人信息的目的、数据接收方

的类型以及可能产生的后果，并事先征得个人信息主体的授权同意。共享、转让经去标识化处理的个人信息，且确保数据接收方无法重新识别或者关联个人信息主体的除外；

c)共享、转让个人敏感信息前，除 b）中告知的内容外，还应向个人信息主体告知涉及的个人敏感信息类型、数据接收方的身份和数据安全能力，并事先征得个人信息主体的明示同意；

d)通过合同等方式规定数据接收方的责任和义务；

e)准确记录和存储个人信息的共享、转让情况，包括共享、转让的日期、规模、目的，以及数据接收方基本情况等；

f)个人信息控制者发现数据接收方违反法律法规要求或双方约定处理个人信息的，应立即要求数据接收方停止相关行为，且采取或要求数据接收方采取有效补救措施（如更改口令、回收权限、断开网络连接等）控制或消除个人信息面临的安全风险；必要时个人信息控制者应解除与数据接收方的业务关系，并要求数据接收方及时删除从个人信息控制者获得的个人信息；

g)因共享、转让个人信息发生安全事件而对个人信息主体合法权益造成损害的，个人信息控制者应承担相应的责任；

h)帮助个人信息主体了解数据接收方对个人信息的存储、使用等情况，以及个人信息主体的权利，例如，访问、更正、删除、注销账户等；

i)个人生物识别信息原则上不应共享、转让。因业务需要，确需共享、转让的，应单独向个人信息主体告知目的、涉及的个人生物识

别信息类型、数据接收方的具体身份和数据安全能力等，并征得个人信息主体的明示同意。

9.3 收购、兼并、重组、破产时的个人信息转让

当个人信息控制者发生收购、兼并、重组、破产等变更时，对个人信息控制者的要求包括：

a)向个人信息主体告知有关情况；

b)变更后的个人信息控制者应继续履行原个人信息控制者的责任和义务，如变更个人信息使用目的时，应重新取得个人信息主体的明示同意；

c)如破产且无承接方的，对数据做删除处理。

9.4 个人信息公开披露

个人信息原则上不应公开披露。个人信息控制者经法律授权或具备合理事由确需公开披露时，应符合以下要求：

a)事先开展个人信息安全影响评估，并依评估结果采取有效的保护个人信息主体的措施；

b)向个人信息主体告知公开披露个人信息的目的、类型，并事先征得个人信息主体明示同意；

c)公开披露个人敏感信息前，除 b）中告知的内容外，还应向个人信息主体告知涉及的个人敏感信息的内容；

d)准确记录和存储个人信息的公开披露的情况，包括公开披露的日期、规模、目的、公开范围等；

e)承担因公开披露个人信息对个人信息主体合法权益造成损害的

相应责任；

f)不应公开披露个人生物识别信息；

g)不应公开披露我国公民的种族、民族、政治观点、宗教信仰等个人敏感数据的分析结果。

9.5 共享、转让、公开披露个人信息时事先征得授权同意的例外

以下情形中，个人信息控制者共享、转让、公开披露个人信息不必事先征得个人信息主体的授权同意：

a)与个人信息控制者履行法律法规规定的义务相关的；

b)与国家安全、国防安全直接相关的；

c)与公共安全、公共卫生、重大公共利益直接相关的；

d)与刑事侦查、起诉、审判和判决执行等直接相关的；

e)出于维护个人信息主体或其他个人的生命、财产等重大合法权益但又很难得到本人授权同意的；

f)个人信息主体自行向社会公众公开的个人信息；

g)从合法公开披露的信息中收集个人信息的，如合法的新闻报道、政府信息公开等渠道。

9.6 共同个人信息控制者

对个人信息控制者的要求包括：

a)当个人信息控制者与第三方为共同个人信息控制者时，个人信息控制者应通过合同等形式与第三方共同确定应满足的个人信息安全要求，以及在个人信息安全方面自身和第三方应分别承担的责任和义务，并向个人信息主体明确告知；

b)如未向个人信息主体明确告知第三方身份，以及在个人信息安全方面自身和第三方应分别承担的责任和义务，个人信息控制者应承担因第三方引起的个人信息安全责任[1]。

9.7 第三方接入管理

当个人信息控制者在其产品或服务中接入具备收集个人信息功能的第三方产品或服务且不适用 9.1 和 9.6 时，对个人信息控制者的要求包括：

a)建立第三方产品或服务接入管理机制和工作流程，必要时应建立安全评估等机制设置接入条件；

b)应与第三方产品或服务提供者通过合同等形式明确双方的安全责任及应实施的个人信息安全措施；

c)应向个人信息主体明确标识产品或服务由第三方提供；

d)应妥善留存平台第三方接入有关合同和管理记录，确保可供相关方查阅；

e)应要求第三方根据本标准相关要求向个人信息主体征得收集个人信息的授权同意，必要时核验其实现的方式；

f)应要求第三方产品或服务建立响应个人信息主体请求和投诉等的机制，以供个人信息主体查询、使用；

g)应监督第三方产品或服务提供者加强个人信息安全管理，发现

[1] 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。

第三方产品或服务没有落实安全管理要求和责任的，应及时督促整改，必要时停止接入；

h)产品或服务嵌入或接入第三方自动化工具（如代码、脚本、接口、算法模型、软件开发工具包、小程序等）的，宜采取以下措施：

1)开展技术检测确保其个人信息收集、使用行为符合约定要求；

2)对第三方嵌入或接入的自动化工具收集个人信息的行为进行审计，发现超出约定的行为，及时切断接入。

9.8 个人信息跨境传输

在中华人民共和国境内运营中收集和产生的个人信息向境外提供的，个人信息控制者应遵循国家相关规定和相关标准的要求。

10 个人信息安全事件处置

10.1 个人信息安全事件应急处置和报告

对个人信息控制者的要求包括：

a)应制定个人信息安全事件应急预案；

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

c)发生个人信息安全事件后，个人信息控制者应根据应急响应预案进行以下处置：

1)记录事件内容，包括但不限于：发现事件的人员、时间、地点，涉及的个人信息及人数，发生事件的系统名称，对其他互联系统的影响，是否已联系执法机关或有关部门；

2)评估事件可能造成的影响，并采取必要措施控制事态，消除隐

患；

3)按照《国家网络安全事件应急预案》等有关规定及时上报，报告内容包括但不限于：涉及个人信息主体的类型、数量、内容、性质等总体情况，事件可能造成的影响，已采取或将要采取的处置措施，事件处置相关人员的联系方式；

4)个人信息泄露事件可能会给个人信息主体的合法权益造成严重危害的，如个人敏感信息的泄露，按照 10.2 的要求实施安全事件的告知。

d)根据相关法律法规变化情况，以及事件处置情况，及时更新应急预案。

10.2 安全事件告知

对个人信息控制者的要求包括：

a)应及时将事件相关情况以邮件、信函、电话、推送通知等方式告知受影响的个人信息主体。难以逐一告知个人信息主体时，应采取合理、有效的方式发布与公众有关的警示信息；

b)告知内容应包括但不限于：

1)安全事件的内容和影响；

2)已采取或将要采取的处置措施；

3)个人信息主体自主防范和降低风险的建议；

4)针对个人信息主体提供的补救措施；

5)个人信息保护负责人和个人信息保护工作机构的联系方式。

11 组织的个人信息安全管理要求

11.1 明确责任部门与人员

对个人信息控制者的要求包括：

a)应明确其法定代表人或主要负责人对个人信息安全负全面领导责任，包括为个人信息安全工作提供人力、财力、物力保障等；

b)应任命个人信息保护负责人和个人信息保护工作机构，个人信息保护负责人应由具有相关管理工作经历和个人信息保护专业知识的人员担任，参与有关个人信息处理活动的重要决策直接向组织主要负责人报告工作；

c)满足以下条件之一的组织，应设立专职的个人信息保护负责人和个人信息保护工作机构，负责个人信息安全工作：

1)主要业务涉及个人信息处理，且从业人员规模大于200人；

2)处理超过100万人的个人信息,或预计在12个月内处理超过100万人的个人信息；

3)处理超过10万人的个人敏感信息的。

d)个人信息保护负责人和个人信息保护工作机构的职责应包括但不限于：

1)全面统筹实施组织内部的个人信息安全工作，对个人信息安全负直接责任；

2)组织制定个人信息保护工作计划并督促落实；

3)制定、签发、实施、定期更新个人信息保护政策和相关规程；

4)建立、维护和更新组织所持有的个人信息清单（包括个人信息的类型、数量、来源、接收方等）和授权访问策略；

5)开展个人信息安全影响评估，提出个人信息保护的对策建议，督促整改安全隐患；

6)组织开展个人信息安全培训；

7)在产品或服务上线发布前进行检测，避免未知的个人信息收集、使用、共享等处理行为；

8)公布投诉、举报方式等信息并及时受理投诉举报；

9)进行安全审计；

10)与监督、管理部门保持沟通，通报或报告个人信息保护和事件处置等情况。

e)应为个人信息保护负责人和个人信息保护工作机构提供必要的资源，保障其独立履行职责。

11.2 个人信息安全工程

开发具有处理个人信息功能的产品或服务时，个人信息控制者宜根据国家有关标准在需求、设计、开发、测试、发布等系统工程阶段考虑个人信息保护要求，保证在系统建设时对个人信息保护措施同步规划、同步建设和同步使用。

11.3 个人信息处理活动记录

个人信息控制者宜建立、维护和更新所收集、使用的个人信息处理活动记录，记录的内容可包括：

a）所涉及个人信息的类型、数量、来源（如从个人信息主体直接收集或通过间接获取方式获得）；

b）根据业务功能和授权情况区分个人信息的处理目的、使用场景，

以及委托处理、共享、转让、公开披露、是否涉及出境等情况；

c）与个人信息处理活动各环节相关的信息系统、组织或人员。

11.4 开展个人信息安全影响评估

对个人信息控制者的要求包括：

a)应建立个人信息安全影响评估制度，评估并处置个人信息处理活动存在的安全风险；

b)个人信息安全影响评估应主要评估处理活动遵循个人信息安全基本原则的情况，以及个人信息处理活动对个人信息主体合法权益的影响，内容包括但不限于：

1)个人信息收集环节是否遵循目的明确、选择同意、最小必要等原则；

2)个人信息处理是否可能对个人信息主体合法权益造成不利影响，包括是否会危害人身和财产安全、损害个人名誉和身心健康、导致差别性待遇等；

3)个人信息安全措施的有效性；

4)匿名化或去标识化处理后的数据集重新识别出个人信息主体或与其他数据集汇聚后重新识别出个人信息主体的风险；

5)共享、转让、公开披露个人信息对个人信息主体合法权益可能产生的不利影响；

6)发生安全事件时，对个人信息主体合法权益可能产生的不利影响。

c)在产品或服务发布前，或业务功能发生重大变化时，应进行个

人信息安全影响评估；

d)在法律法规有新的要求时，或在业务模式、信息系统、运行环境发生重大变更时，或发生重大个人信息安全事件时，应进行个人信息安全影响评估；

e)形成个人信息安全影响评估报告，并以此采取保护个人信息主体的措施，使风险降低到可接受的水平；

f)妥善留存个人信息安全影响评估报告，确保可供相关方查阅，并以适宜的形式对外公开。

11.5 数据安全能力

个人信息控制者应根据有关国家标准的要求，建立适当的数据安全能力，落实必要的管理和技术措施，防止个人信息的泄漏、损毁、丢失、篡改。

11.6 人员管理与培训

对个人信息控制者的要求包括：

a)应与从事个人信息处理岗位上的相关人员签署保密协议，对大量接触个人敏感信息的人员进行背景审查，以了解其犯罪记录、诚信状况等；

b)应明确内部涉及个人信息处理不同岗位的安全职责，建立发生安全事件的处罚机制；

c)应要求个人信息处理岗位上的相关人员在调离岗位或终止劳动合同时，继续履行保密义务；

d)应明确可能访问个人信息的外部服务人员应遵守的个人信息安

全要求，与其签署保密协议，并进行监督；

e)应建立相应的内部制度和政策对员工提出个人信息保护的指引和要求；

f)应定期（至少每年一次）或在个人信息保护政策发生重大变化时，对个人信息处理岗位上的相关人员开展个人信息安全专业化培训和考核，确保相关人员熟练掌握个人信息保护政策和相关规程。

11.7 安全审计

对个人信息控制者的要求包括：

a)应对个人信息保护政策、相关规程和安全措施的有效性进行审计；

b)应建立自动化审计系统，监测记录个人信息处理活动；

c)审计过程形成的记录应能对安全事件的处置、应急响应和事后调查提供支撑；

d)应防止非授权访问、篡改或删除审计记录；

e)应及时处理审计过程中发现的个人信息违规使用、滥用等情况；

f)审计记录和留存时间应符合法律法规的要求。

附 录 A

（资料性附录）

个人信息示例

个人信息是指以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息，如姓名、出生日期、身份证件号码、个人生物识别信息、住址、通信通讯联系方式、通信记录和内容、账号密码、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息等。

判定某项信息是否属于个人信息，应考虑以下两条路径：一是识别，即从信息到个人，由信息本身的特殊性识别出特定自然人，个人信息应有助于识别出特定个人。二是关联，即从个人到信息，如已知特定自然人，由该特定自然人在其活动中产生的信息（如个人位置信息、个人通话记录、个人浏览记录等）即为个人信息。符合上述两种情形之一的信息，均应判定为个人信息。表A.1给出了个人信息举例。

表A.1 个人信息举例

个人基本资料	个人姓名、生日、性别、民族、国籍、家庭关系、住址、个人电话号码、电子邮件地址等
个人身份信息	身份证、军官证、护照、驾驶证、工作证、出入证、社保卡、居住证等
个人生物识别信息	个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部识别特征等
网络身份标识信息	个人信息主体账号、IP地址、个人数字证书等

个人健康生理信息	个人因生病医治等产生的相关记录，如病症、住院志、医嘱单、检验报告、手术及麻醉记录、护理记录、用药记录、药物食物过敏信息、生育信息、以往病史、诊治情况、家族病史、现病史、传染病史等，以及与个人身体健康状况相关的信息，如体重、身高、肺活量等
个人教育工作信息	个人职业、职位、工作单位、学历、学位、教育经历、工作经历、培训记录、成绩单等
个人财产信息	银行账户、鉴别信息(口令)、存款信息（包括资金数量、支付收款记录等）、房产信息、信贷记录、征信信息、交易和消费记录、流水记录等，以及虚拟货币、虚拟交易、游戏类兑换码等虚拟财产信息
个人通信信息	通信记录和内容、短信、彩信、电子邮件，以及描述个人通信的数据（通常称为元数据）等
联系人信息	通讯录、好友列表、群列表、电子邮件地址列表等
个人上网记录	指通过日志储存的个人信息主体操作记录，包括网站浏览记录、软件使用记录、点击记录、收藏列表等
个人常用设备信息	指包括硬件序列号、设备MAC地址、软件列表、唯一设备识别码(如IMEI/Android ID/IDFA/OpenUDID/GUID/SIM卡 IMSI信息等）等在内的描述个人常用设备基本情况的信息
个人位置信息	包括行踪轨迹、精准定位信息、住宿信息、经纬度等
其他信息	婚史、宗教信仰、性取向、未公开的违法犯罪记录等

附 录 B

（资料性附录）

个人敏感信息判定

个人敏感信息是指一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息。通常情况下，14岁以下（含）儿童的个人信息和涉及自然人隐私的信息属于个人敏感信息。可从以下角度判定是否属于个人敏感信息：

泄露：个人信息一旦泄露，将导致个人信息主体及收集、使用个人信息的组织和机构丧失对个人信息的控制能力，造成个人信息扩散范围和用途的不可控。某些个人信息在泄漏后，被以违背个人信息主体意愿的方式直接使用或与其他信息进行关联分析，可能对个人信息主体权益带来重大风险，应判定为个人敏感信息。例如，个人信息主体的身份证复印件被他人用于手机号卡实名登记、银行账户开户办卡等。

非法提供：某些个人信息仅因在个人信息主体授权同意范围外扩散，即可对个人信息主体权益带来重大风险，应判定为个人敏感信息。例如，性取向、存款信息、传染病史等。

滥用：某些个人信息在被超出授权合理界限时使用（如变更处理目的、扩大处理范围等），可能对个人信息主体权益带来重大风险，应判定为个人敏感信息。例如，在未取得个人信息主体授权时，将健康信息用于保险公司营销和确定个体保费高低。表B.1给出了个人敏感信息举例。

表B.1 个人敏感信息举例

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

附 录 C

（资料性附录）

实现个人信息主体自主意愿的方法

概述

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，尤其是移动互联网应用程序运营者，可通过以下方式实现。

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[1]；

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；

[1] 注：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;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。个人信息控制者仍可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宜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，个人信息控制者宜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。

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。

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：

d)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[1]；扩展业务功能的告知和明示同意的实现方法如下：

e)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；

f)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的，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48h内向个人信息主体征求同意的次数

[1] 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，宜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，并即时完成告知要求,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的，个人信息控制者可拒绝向个人信息主体提供该业务功能；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;上述要求的实现方式可参考C.5。

不应超过一次；

g)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的，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；

h)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[1]。

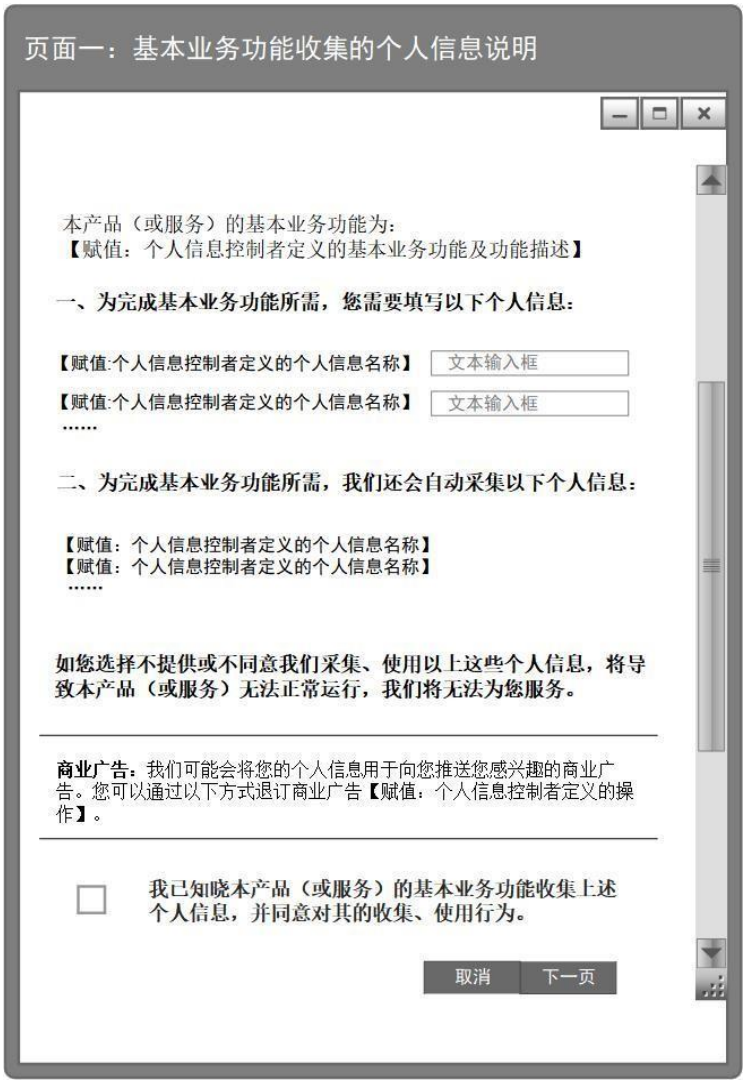
交互式功能界面设计

个人信息控制者可参考表C.1所示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。

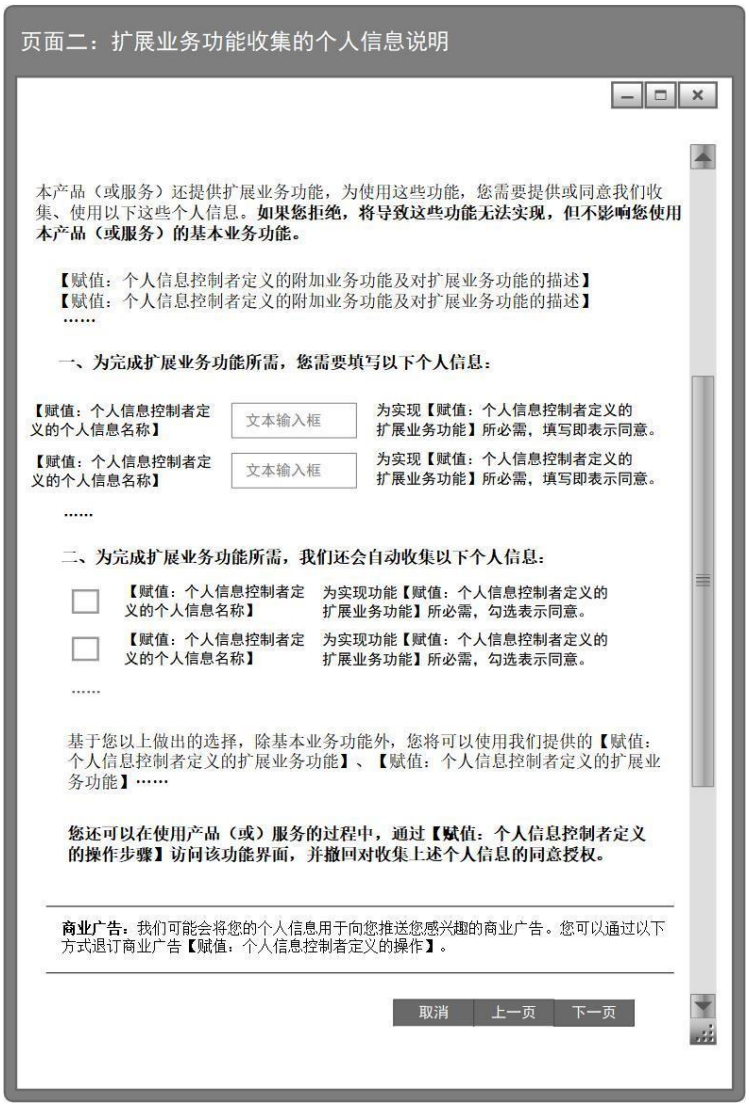
该功能界面应在个人信息控制者开始收集个人信息前，如产品安装过程中，或个人信息主体首次使用产品或服务时，或个人信息主体注册账号时，由个人信息控制者主动向个人信息主体提供。如以填写纸质材料收集个人信息的，个人信息控制者可以参考以下模板内容设计表格，以保障个人信息主体能行使选择同意的权利。

[1] 注：上述要求的实现方式可参考C.5。

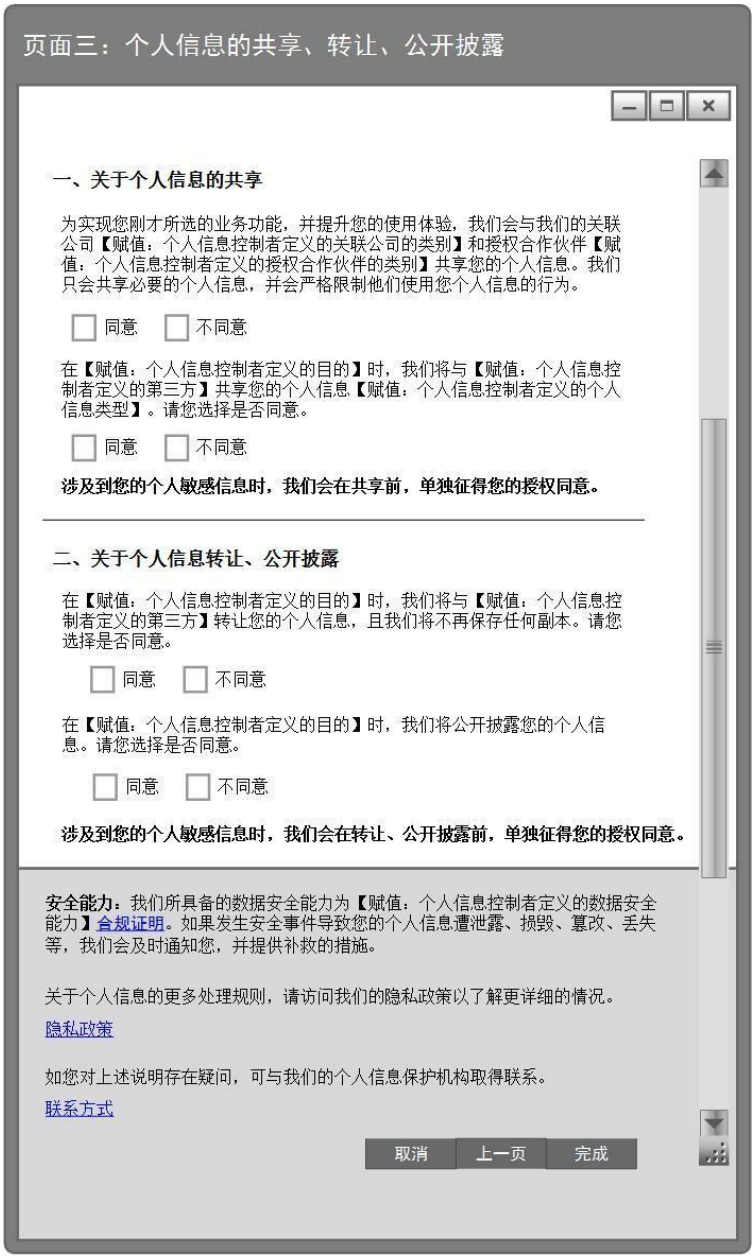
表C.1 交互式功能界面模板

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。

表C.1 （续）

功能界面模板	说明
	6、扩展业务功能是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，强制收集个人信息。 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。

表C.1 （续）

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、应明示个人信息保护政策的链接，以便个人信息主体查阅。

附 录 D

（资料性附录）

个人信息保护政策模板

发布个人信息保护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。个人信息保护政策应清晰、准确、完整地描述个人信息控制者的个人信息处理行为。个人信息保护政策模板示例见表D.1。

表D.1 个人信息保护政策模板

个人信息保护政策模版	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。包含个人信息保护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	该部分为个人信息保护政策的重点说明，是个人信息保护政策的一个要点摘录。目的是使个人信息主体快速了解个人信息保护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。

本政策如何更新 如何联系我们 XXXX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，XXXX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《个人信息保护政策》。	

表D.1续

个人信息保护政策模版	编写要求
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。 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	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、驾驶证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

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、本个人信息保护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】	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、接收方使用个人信息的目的、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

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】 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，但以下情形除外： 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、组织继续受此个人信息保护政策的约束，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 我们仅会在以下情形下，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。	信息安全审计、保护个人信息主体避免遭受欺诈和严重人身伤害等。

表D.1 （续）个人信息保护政策模版	编写要求
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，XXX （二）我们已经取得了以下认证：XXX （三）我们的数据安全能力：XXX （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。 （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和可能的影响、我们已采取或将要采取的处置措施、您可自主防范	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

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。	事件后，将及时告知个人信息主体。

表D.1 （续）

个人信息保护政策模版	编写要求
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，您可以随时使用我们的Web表单联系，或发送电子邮件至XXX 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，只要我们不需要过多投入，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XXX （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XXX 我们将在30天内回复您的更正请求。	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授权同意和注销账户的渠道、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、撤回授权同意等目的，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。

（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收集和使用，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	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、撤回授权同意等的要求，需明确说明拒绝的原因和依据。

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：……	

表D.1 （续）

个人信息保护政策模版	编写要求
（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，如数据接口已匹配，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作出决定。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：…… 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；涉及商业秘密的。	

表D.1 （续）

个人信息保护政策模版	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。	
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器提供产品或服务，这意味着，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	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）。

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。	

表D.1 （续）

个人信息保护政策模版	编写要求
本政策如何更新 我们的个人信息保护政策可能变更。 未经您明确同意，我们不会削减您按照本个人信息保护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，说明个人信息保护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。	个人信息控制者在个人信息保护政策发生重大变化时，需及时更新个人信息保护政策，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。

我们还会将本政策的旧版本存档，供您查阅。	
如何联系我们 如果您对本个人信息保护政策有任何疑问、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、电子邮件地址、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个人信息保护政策的独立机构、行业自律协会或政府相关管理机构等。

GB/T38652-2020 电子商务业务术语

时效性：　　现行有效

发布机关：　国家市场监督管理总局、国家标准化管理委员会

类别：　　中华人民共和国国家标准

发布日期：　2020 年 03 月 31 日

实施日期：　2020 年 10 月 01 日

1 范围

本标准界定了电子商务交易业务相关的术语和定义。本标准适用于电子商务交易业务及相关应用领域。

2 基础术语

2.1 电子商务 e-commerce 电商

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。

2.2 电子商务平台 e-commerce platform

为交易的双方或多方提供信息发布、信息递送、数据处理等一项或多项服务，实现交易撮合目的的信息网络系统[1]。

2.3 电子商务经营者 e-commerce operator

通过石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白然人、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。

2.3.1 电子商务平台经营者 ecommerce platform operator

[1] 注:改写 GB/T 35408—2017，定义 2.1.2。

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

2.3.2 平台内经营者 operator on e-commerce platform

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。

3 电子商务模式

3.1B2B 电子商务 business-to-business e-commerce 企业卖家对企业买家的电子商务模式。

3.2B2C 电子商务 business-to-customer e-commerce 企业卖家对个人买家的电子商务模式。

3.3C2B 电子商务 customer-to-business e-commerce

基于个人买家的需求，企业卖家设计生产产品或服务的电子商务模式。

3.4C2C 电子商务 customer-to-customer e-commerce 个人卖家对个人买家的电子商务模式。

3.5O2O 电子商务 online-to-offline e-commerce

通过线上营销和线上购买的方式带动线下经营和线下消费的电子商务模式。

3.6 跨境电子商务 cross-border e-commerce

分属不同关境的交易主体，通过互联网达成交易、进行支付结算，并通过跨境物流送达商品、完成交易的经营活动。

3.7 移动电子商务 mobile e-commerce

通过无线终端进行的电子商务模式[1]。

3.8 社交电子商务 social e-commerce

基于人际关系网络，利用互联网社交工具，从事商品或服务销售的电子商务模式。

3.9 团购 group buying

由电子商务经营者发起的，多个买家联合起来加大与商家的谈判能力，以求得优惠价格的购物方式。

4 电子商务交易过程相关方

4.1 会员 registered member

在电子商务平台登记注册的组织或个人。

4.2 访客 visitor

未以会员身份登录电子商务平台的访问者。

4.3 用户 user

电子商务平台各项服务的使用者，包括会员和访客。

4.4 买家 buyer 顾客 customer

在电子商务平台上购买商品或接受服务的用户。

GB/T 38652—2020

4.5 卖家 seller

通过电子商务平台、自建网站、其他网络服务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。4.6

4.6 商家 merchant

[1] 注:无线终端有多种形式，如手机、掌上电脑等。【GB/T 35408—2017，定义 2.1.47

通过电子商务平台、自建网站、其他网络服务等信息网络从事销售商品或者提供服务的经营活动的企业类型的卖家。4.7

4.7 物流服务提供者 logistics service provider

为电子商务平台经营者、卖家和买家提供配送服务的组织或个人。

4.8 电子支付服务提供者 electronic payment service provider

为电子商务交易相关方提供支付服务的组织或个人。

4.9 广告服务提供者 advertising service provider

为电子商务交易过程或活动提供广告服务的组织或个人。

4.10 第三方软件提供者 the third party software provider

以第三方身份提供软件或软件服务的组织或个人。

4.11 代运营服务提供者 agent operation service provider

受卖家委托，以卖家名义进行店铺运营管理等工作的组织或个人。

4.12 品牌权利人 brand holder

拥有品牌商标等的所有权或使用权的组织或个人。

4.13 知识产权权利人入 intellectual property right holder

对作品、商标、专利等智力劳动成果享有所有权的主体。

5 交易前过程

5.1 注册 register

访客按电子商务平台经营者的要求，提供相关信息，获取平台会员账号的过程。

5.2 入驻 entry

卖家按电子商务平台经营者的招商要求，提交开店申请，经电子商务平台经营者审核并允许卖家开展经营活动的过程。

5.3 店铺 shop

卖家通过电子商务平台销售商品或提供服务的网络经营场所。

GB/'T 38652—2020

5.4 店铺域名 domain name

店铺在电子商务平台上的网络地址。

5.5 实名验证 identity verification

电子商务平台经营者验证会员身份真实性的过程。

5.6 实人验证 biometric verification

电子商务平台经营者验证会员的身份与本人的对应性，确保身份真实性的过程。

5.7 实地验证 field verification

电子商务经营者对会员或相关的企业通过现场检验、实地考察等方式，确保相关信息真实性的过程。

5.8 类目 category

按商品的属性进行分类的结构化目录。

5.9 类目属性 category attribute

指定类目下的商品和服务所具有的共同特征。

5.10 类目授权 category authorization

电子商务平台经营者授予卖家在某些类目下发布并经营商品的行为。

5.11 品牌授权 brand authorization

品牌权利人或有权使用者出具品牌授权书，将其所拥有或代理的商标或品牌授予被授权者使用。

【GB/T 35408—2017，定义 3.2.6】

5.11.1 一级授权 first-level authorization

品牌权利人直接向商家进行品牌授权[1]。

【GB/T 35409—2017，定义 3.4】

5.11.2 多级授权 multi-level authorization

商家通过一个及以上转授权间接获得品牌权利人的品牌授权。

【GB/T 35409—2017，定义 3.5】

5.12 近似品牌 confusingly similar brand

商标、名称、用语、符号、形象、标识、包装、装潢、设计或其组合，与其他品牌存在近似，容易使消费者在电子商务平台购物时产生混淆或误认的品牌。

5.13 禁售商品 gods on ban

依照相关法律法规、部门规章、规范性文件、行政指令等禁止交易的特定商品或服务，或者电子商务平台经营者通过协议、规则、用户通知明确告知的不适宜在该平台交易的特定商品或服务[2]。

5.14 限售商品 restricted goods

平台内经营者依法应当取得行政许可方可经营的特定商品或服务，或者电子商务平台经营者通过协议、规则等明确设立的需要经营

[1] 注:品牌权利人的分公司、全资子公司、国内唯一总代理（仅适用于国外品牌权利人）等的授权可视为品牌权利人的授权。

[2] 注:相关禁止性要求包括对该特定商品或服务的经营行为及相关信息的发布行为。

者取得一定资质方可经营的特定商品或服务[1]。

6 交易中过程

6.1 下单 make order

买家在电子商务平台上点击确认购买商品或服务的行为。

6.2 订单 order

买家向卖家同一时间拍下单款或多款商品或服务的合约。

6.3 订单确认 order confirmation

买家对交易订单的商品或服务、价格、配送方式、物流信息等内容进行核实确认的过程。

6.4 在线客服 online customer service

客服人员通过互联网在线与客户进行沟通、处理、反馈、维护客户关系的服务方式。

6.5 电话客服 phone customer service

客服人员通过电话与客户进行沟通、处理、反馈、维护客户关系的服务方式。

6.6 电子优惠券 electronic coupon

由电子商务平台经营者或卖家设立，用于买家抵扣商品价格的一种交易抵价券。

6.7 购物车 shopping cart

在电子商务交易过程中装载待支付商品或服务的虚拟容器。

6.8 在线支付 online payment

[1] 注:相关限制性要求包括对该特定商品或服务的经营行为及相关信息的发布行为。

交易双方通过网络进行的支付行为。

6.9 货到付款 cash on delivery

买家收货确认后再付款的支付方式。

6.10 包邮 free shipping

卖家对所售商品承担承诺条件下的发货运费的服务。

6.11 运费险 freight policy

保险公司为投保该险种的电子商务平台买家支付绑定商品退货运费的保险服务。

6.12 发货 delivery

卖家按照订单发出商品的过程。

7 交易后过程

7.1 签收 sign for goods

买家收到商品后签字确认的过程。

7.2 拒收 ref use to sign

买家在收到商品后拒绝签收的行为。

7.3 代收 agent collection

买家委托第三方代为签收商品的行为。

7.4 确认收货 receipt confirmation

买家在电子商务平台确认签收的过程。

7.5 延长收货 prolong the receipt of goods

买家通过电子商务平台的订单页面提交延后接收商品信息的过程。

7.6 破损补寄 compensatory mailing for breakage

买卖双方约定，买家签收商品后在约定时间内发现商品破损，由卖家提供补寄服务的过程。

7.7 交易评价 transaction comment

完成交易后，由买家对购买的商品或服务;在满足其要求和期望的程度等方面进行的衡量、评定、评估以及反馈的过程[1]。

7.8 虚假评价 fake comment

评价人为达到某种目的，不以客观事实为依据，给予与事实不符的评价[2]。

7.9 店铺评分 store grade

电子商务平台经营者根据交易评价规则对店铺进行的评价活动。

7.10 申诉 appeal

会员提供相应的客观证据证明自身不存在违规行为的过程。

7.11 交易纠纷处理 transaction disagreement resolution

电子商务平台经营者根据买方或卖方的申请，针对交易纠纷判定责任归属，并对所涉及的商品、资金、赔偿等做出处理的过程。

7.12 大众评审 public review

由一定数量符合评定条件的评判人员，以主动申领、投票表决的方式完成判定任务的评价方法。

7.13 客户满意度 satisfaction of customer service

---

[1] 注:从交易全过程而言，这些评价可包含咨询、购买、支付、配送、售后服务、纠纷处理等某个过程或全过程;改写 GB/T35408—2017，定义 4.4。

[2] 注:改写 GB/T 35408—2017，定义 4.7。

客户感知的服务效果与客户期望值相比较后得出的结果，体现客户期望值与客户体验的匹配程度。

8 交易管理

8.1 交易规则 transaction rules

电子商务平台经营者对商户、顾客开展交易活动的方式、履行的义务和限制基本权利等要求的规定。

8.2 商品下架 commodity removal

根据电子商务平台管理需要或卖家经营需要，将商品从在线状态转为下线状态，且不可被买家购买。

8.3 商品删除 commodity deletion

根据平台管理需要或卖家经营需要，删除产品对应链接的行为。

8.4 商品屏蔽 commodity shielding

电子商务经营者采取的让商品的信息在搜索结果中不展现的措施。

8.5 店铺屏蔽 shop shielding

电子商务平台经营者采取的让会员店铺在平台内搜索结果页面无法展示，或停止为店铺提供信息递送服务的措施。

8.6 店铺关闭 shop closure

电子商务平台经营者采取的断开店铺以及店铺内所有商品和服务网址链接;或停止为店铺以及店铺所有商品和服务信息提供递送服务的措施[1]。

---

[1] 注：改写 GB/T35408—2017，定义 3.2.9。

8.7 限制发布商品 restrict commodity releasing

在特定时段、特定区域，制约卖家对特定商品与服务的信息进行发布的措施。

8.8 限制营销活动 restrict marketing activity

对违反交易规则的卖家实施限制参加电子商务平台上的营销活动的措施。

8.9 限制买家行为 restrict buying

禁止买家在电子商务平台购买商品。

8.10 限制网站登录 restrict logging in to the website

禁止会员登录电子商务平台网页及相关客户端。

8.11 滥发信息 abuse of information releasing

用户未按法律法规、电子商务平台相关规则及发布要求发布商品或服务信息;妨害相关方权益的行为，包括但不限于：

a）广告信息;

b）与实际不符的信息;

c） 重复信息;

d）商品要素不一致的信息;

e） 价格作弊信息;

f） 其他行业特殊要求的信息。

8.12 发布未经准入商品 release commodity without admittance

卖家未经电子商务平台经营者备案或审查，发布需要准入类目所属的商品或信息。

8.13 描述不符 inconsistent description

卖家实际销售的商品或提供的服务，与在电子商务平台展示的商品或服务信息不一致的情况。

8.14 违背承诺 disobey commitment

卖家未按照约定向买家提供承诺的服务的行为。

8.15 延迟发货 delay delivery

除特殊商品外，卖家在买家付款后实际未在平台规定时间内发货，或定制、预售及其他特殊情形等另行约定发货时间的商品，卖家实际未在约定时间内发货的行为。

8.16 神秘抽检 mystery sampling inspection

为监管平台商品的质量;由相关人员以普通消费者身份在卖家店铺中下单购买样品，交由具备相关资质的机构进行检验检测并做合格判定的行为。

8.17 滥用会员权利 membership rights abuse

会员不以消费为目的，不合理利用会员权利损害他人合法权益、妨害平台运营秩序的行为。

8.18 虚假交易 fake transaction

通过不正当方式获得商品销量、店铺评分、信用积分等不当利益的行为。

8.19 保证金 deposit

卖家根据平台协议约定的条款和条件及其他公示规则的规定缴存并止付锁定于卖家的第三方交易账户的资金。

9 消费者服务

9.1 基础保障服务 basic guarantee service

电子商务经营者在相关法律法规规定的范围内，提供的退货、配送等保障消费者基础权益的服务。

9.2 交易约定服务 promissory service in transaction

电子商务经营者在提供基础保障服务之外提供的旨在提升消费者体验的服务。

10 交易数据分析

10.1 客单价 unit price by customer

平均成交金额，反映一个时间段内用户购买的能力。

10.2 浏览时长 browse duration

统计周期内，用户浏览商品页面的平均时长。

10.3 活跃会员数 number of active members

统计周期内，在商品页面开展电子商务活动行为的会员数。

10.4 转化率 transfer rate

统计周期内;完成转化目标行动的总次数占总访问次数的比例。

10.5 商品动销率 commodity sales rate

统计周期内，商品累计销售数量占商品期末库存数量的比例。

10.6 库存周转率 inventory carry rate

统计周期内，年度销售商品成本占当年平均库存价值总额的比例。

10.7 售罄率 complete sales rate

统计周期内，实际销售货品零售价占总进货零售价的比例。

10.8 快递投诉率 express complaint rate

统计周期内，有客户投诉的快递占发出快递的比例。

10.9 包裹破损率 parcel breakage rate 统计周期内，破损包裹占发

出包裹的比例。

10.10 包裹遗失率 parcel loss rate

统计周期内，丢失包裹占发出包裹的比例。

10.11 退款率 refund rate

统计周期内，当期退款笔数占当期支付成交笔数的比例。

10.12 退款纠纷率 refund dispute rate

统计周期内，申请电子商务平台经营者介入或由电子商务平台经营者主动介入的退款笔数占退款总笔数的比例。

10.13 退款自主完结率 refund automatic completion rate

统计周期内，卖家自主完结退款笔数占全部退款完结笔数的比例[1]。

10.14 责任纠纷率 liability dispute rate

统计周期内，电子商务平台经营者最终判定为卖家责任的纠纷数占消费者申请电子商务平台经营者介入的纠纷数的比例。

10.15 登录转化率 login transfer rate

统计周期内，网站登录会员数占网站登录用户数的比例。

10.16 成交转化率 deal transfer rate

统计周期内，下单购买的用户数占网页浏览的用户数的比例。

10.17 熟客率 regular customer rate

统计周期内，成功购买三次以上的独立访客数量占所有购买商品的独立访客数量的比例。

[1] 注：退款包括售中和售后的仅退款和退货退款。

10.18 店铺动销率 dynamic sales rate

统计周期内，有成交的商品数占在线商品数的比例。

JR/T0171-2020 个人金融信息保护技术规范

时效性：　　现行有效

发布机关：　中国人民银行

类别：　　金融行业标准

发布日期：　2020 年 02 月 13 日

实施日期：　2020 年 02 月 13 日

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

Hi T 0071 金融行业信息系统信息安全等级保护实施指引

IK I 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

Hi 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[1]。

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[2]。

3.4

---

[1] 注：本标准中的个人金融信息包括账户信息、签别信息、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；改写 GB/T 35273—2017.定义 3. h

[2] 注：支付敏感信息包括但不限于银行卡破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鳖权的个人金融信息。

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[1]。

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[2]。

3.6

收集 co11ect

获得个人金融信息的控制权的行为[3]。

3. 7

公开披露 public disclosure

向社会或不特定群体发布信息的行为。[GB/T 35273—2017,定义 3.10]

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

---

[1] 注：改写 GB/T 35273—2017,定义 3. 3.

[2] 注：改写 GB/T 35273—2017,定义 3. 4.

[3] 注：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、搜栗公开信息等同接获取个人金融信息等行为；如金做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伯息进行访同的，则不届 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税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；改写 CB/T 35273—2017,定义 3.5.

[1]。

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[2]。

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]。

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[4]。

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。[JR/T 0149—2016,定义 3. 2]

3. 13

---

[1] 注：改写 GB/T 35273—2017,定义 3.11.

[2] 注：改写 GB/T 35273—2017.定义 3.12.

[3] 注：改写 GB/T 35273—2017,定义 3.8.

[4] 注：改写 JR/T 0149—2016,定义 3.1.

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[1]。

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。

[JR/T 0061—2011,定义 8. 7]

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。[JR/T 0061—2011,定义 8.8]

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。[GM/Z 0001—2013,定义 2.15]

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。[JR/T 0088. 1—2012,定义 2.44]

客户法定名称 customer's legal

[1] 注：磁道数据可以在物理卡的磁条上，也可以被包含在集成电路或者其他媒介上。[JR/T 0061—2011,定义 3.20]

在法律上认可的客户名称[1]。

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[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[3]。

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[4]。

---

[1] 注：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；改 GB/T 31186.2—2014,定义 3.2.

[2] 注：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；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。

[3] 注：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;非法查看是对未经授权的查看的一种不严谨但在特定的谱境下并无二义性的提法。

[4] 注：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（BPHM 除原有的内容）三种情况，也可能是三种情况的组合；未经授权的变更可能是善意的，也可能是悲意的：往往表现为伯息篡改事件、信息假冒事件、信息丢失事件等；非法变更是对未经授权的变更的一种不严谨但在特定

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[1]。

3.23

匿名化 anony mization

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[2]

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[3]。

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

的语境下并无二义性的提法。

[1] 注：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；改写 GB/T 35273—2017,定义 3.6.

[2] 注：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；改写 GB/T 35273—2017,定义 3.13。

[3] 注：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曾代对 个人金融信息的标识；改写 GB/T 35273—2017,定义 3.14.

其保持不可被检索、访问的状态[1]。

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

[1] 注：改写 GB/T 35273—2017,定义 3.9。

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；用于用户樂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：

b） 应建立相应的个人金融信息传输安全策略和规程，采用满足个人金融信息传输安全策略的安全控制措施，如安全通道、数据加密等技术措施。

b） 传输个人金融信息前，通信双方应通过有效技术手段进行身份鉴别和认证。

c） 通过公共网络传输时，C2、C3 类别信息应使用加密通道或数据加密的方式进行传输，保障个人金融信息传输过程的安全；对于 C3 类别中的支付敏感信息，其安全传输技术控制措施应符合有关行业技术标准与行业主管部门有关规定要求。

d） 应根据个人金融信息的不同类别，采用技术手段保证个人金融信息的安全传输：低敏感程度类别的个人金融信息因参与身份鉴别等关键活动导致敏感程度上升的（如，经组合后构成交易授权完整要素的情况），应提升相应的安全传输保障手段。

e） 个人金融信息传输的接收方应对接收的信息进行完整性校验。

f） 应建立有效机制对个人金融信息传输安全策略进行审核、监控和优化，包括对通道安全配置、密码算法配置、密钥管理等保护措施的管理和监控，

g） 应采取有效措施（如个人金融信息传输链路冗余）保证数据传输可靠性和网络传输服务可用性。

6.1.3 存储

个人金融信息存储的具体技术要求如下：

a） 不应留存非本机构的银行卡磁道数据（或芯片等效信息）、银行卡有效期、卡片验证码（CVN 和 CVN2）、银行卡密码、网络支付密码等 C3 类别信息。若确有必要留存的，应取得个人金融信息主体及账户管理机构的授权。

b） 应根据个人金融信息的不同类别，采用技术手段保证个人金融信息的存储安全；低敏感程度类别的个人金融信息因参与身份鉴别等关键活动导致敏感程度上升的（如，经组合后构成交易授权完整要素的情况），应提升相应的安全存储保障手段。

c） C3 类别个人金融信息应采用加密措施确保数据存储的保密性。

d） 受理终端、个人终端及客户端应用软件均不应存储银行卡磁道数据（或芯片等效信息）、银行卡有效期、卡片验证码（CVN 和 CVN2）、银行卡密码、网络支付密码等支付敏感信息及个人生物识别信息的样本数据、模板，仅可保存完成当前交易所必需的基本信息要素，并在完成交易后及时予以清除。

e） 采取必要的技术和管控措施保证个人金融信息存储转移过程中的安全性。

f） 应将去标识化、匿名化后的数据与可用于恢复识别个人的信息采取逻辑隔离的方式进行存储，确保去标识化、匿名化后的信息与

个人金融信息不被混用。

g） 在停止运营时，应依据国家法律法规与行业主管部门有关规定要求，对所存储的个人金融信息进行妥善处置，或移交国家与行业主管部门指定的机构继续保存。

6.1.4 使用

6.1.4. 1 信息展示

提供业务办理与查询等功能的应用软件，对个人金融信息展示具体技术要求如下：

a） 依据国家法律法规与行业主管部门有关规定要求，对通过计算机屏幕、客户端应用软件、银行卡受理设备、自助终端设备、纸面（如受理终端打印出的交易凭条等交易凭证）等界面展示的个人金融信息应采取信息屏蔽（或截词）等处理措施，降低个人金融信息在展示环节的泄露风险[1]。

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。

[1] 注:关于信息屏蔽（或截词）的使用方式，参见附录A；金融业机构柜面打印的凭证依据有关规范执行.

涉及其他个人金融信息主体的信息时，除以下情况外，宜进行屏蔽展示：

其他方主动发起的活动包含的信息，此种情况需展示必要的信息以供活动接收方对活动内容进行确认，例如：其他方发起的交易、其他方发起的收付款、保险保费代收。

与其他方已建立信任关系（间接授权），此时需活动发起方确认发起活动的必要信息

的正确性（或活动发起方需接收活动结果信息，并确认活动已正确完成），例如：向其他方收款，其他方已付款；向其他方申请代付，其他方同意付款或者其他方在自己业务应用范围内的联系人。

其他法律法规要求的情况。

应用软件的后台管理与业务支撑系统，对个人金融信息展示具体技术要求如下：

a） 除银行卡有效期外，C3 类别信息不应明文展示。

b） 应采取技术措施防范个人金融信息在展示过程中泄露或被未经授权的拷贝。

c） 后台系统对支付账号、客户法定名称、支付预留手机号码、证件类或其他类识别标识信息等展示宜进行屏蔽处理，如需完整展示，应做好此类信息管理，采取有效措施防范未经授权的拷贝。

d） 后台系统不应具备开放式查询能力，应严格限制批量查询。

e） 对于确有明文查看需要的业务场景可以保留明文查看权限，后台系统应对所有查询操作进行细粒度的授权与行为审计。

应防止通过散列碰撞等方法推导出完整的数据，若使用"截词”的

方式进行部分字段的屏蔽处理，不应用散列代替字段被截词的部分。

6. 1.4.2 共享和转让

个人金融信息在共享和转让的过程中，应充分重视信息转移或交换过程中的安全风险，具体技术要求如下：

a） 在共享和转让前，应开展个人金融信息安全影响评估，并依据评估结果采取有效措施保护个人金融信息主体权益。

b） 在共享和转让前，应开展个人金融信息接收方信息安全保障能力评估，并与其签署数据保护责任承诺

c） 支付账号及其等效信息在共享和转让时，除法律法规和行业主管部门另有规定外，应使用支付标记化（按照 JR/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，并应确保对共享和转让的信息及其过程可被追溯。

j） 应采取有效技术防护措施，防范信息转移过程中被除信息发送方与接收方之外的其他个人、组织和机构截获和利用。

6.1.4. 3 公开披露

个人金融信息原则上不得公开披露。金融业机构经法律授权或具备合理事由确需公开披露时，具体技术要求如下：

a） 应事先开展个人金融信息安全影响评估，并依据评估结果采收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 F：

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。

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 I 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（成公告）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）管理规范和制度，应明确不同敏感级别个人金融信息脱敏规则、脱敏方法和脱敏数据的使用限制

f） 依据国家与行业有关标准，建立个人金融信息安全影响评估制度，应定期（至少每年一次）开展个人金融信息安全影响评估。

g） 建立外包服务机构与外部合作机构管理制度，包括但不限于：

应对个人金融信息生命周期过程中相关的外包服务机构与外部合作机构进行审查与评估，评估其个人金融信息的保护能力是否达到国家、行业主管部门与金融业机构的要求；应通过协议或合同的方式，约束外包服务机构与外部合作机构不应留存 C2、C3 类别信息：对于 C2 类别信息中的支付账号等信息，若因清分清算、差错处理等业务需要确需留存，金融业机构应明确其保密义务与保密责任，并应根据安全要求落实安全控制措施，并将有关资料留档备查；对可能访问个人金融信息的外包服务机构、外部合作机构及其人员，金融业机构应要求外包服务机构与外部合作机构向有关人员传达个人金融信息保护安全要求，与其签署保密协议，并对协议履行情况进行监督。

不应将存储个人金融信息的数据库交由外部合作机构运维。

应定期对外包服务机构与外部合作机构的个人金融信息保护措施落实情况进行确认，确认的方式包括但不限于外部信息安全评估、现场检查等。

国家法律法规与行业主管部门另有规定的，按照相关要求执行。

h） 建立个人金融信息安全检查及监督机制.应建立个人金融信息安全日常检查机制和工作流程、定期评估个人金融信息管理方面存

在的不足，及时调整检查机制和工作流程。

i） 应将个人金融信息泄露等相关事件处理纳入机构信息安全事件应急处置工作机制，制定专门的流程和预案。定期评估应急处理流程制预案，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。

i）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度；制定、实施、定期更新隐私政策和相关规程；监督本机构内部，以及本机构与外部合作方个人金融信息安全管理；开展信息安全管理内部审计、分析处理信息安全相关事件。组织开展个人金融信息安全影响评估，提出个人金融信息保护的对策建议：组织在金融产品或服务上线发布前进行技术检测，避免未知〈与金融产品或服务功能及隐私政策不符）的个人金融信息收集、使用、共享等处理行为；

公布投诉与申诉方式等信息并及时受理个人金融信息有关的投诉、申诉。

c)应明确在提供金融产品和服务的过程中知悉个人金融信息的岗位,并针对相关岗位明确其个人金融信息安全管理责任与保密责任，如不得未经授权的复制、存储、使用个人金融信息，不得向他人出售或者以其他形式未经授权的共享、转让、披露个人金融信息等。

7.2.3 人员管理

对涉及个人金融信息相关人员的安全管理，具体要求如 E

a） 录用员工前，应进行必要的背景调查，并与所有可访问个人金融信息的员工签署保密协议，或在劳动合同中设置保密条款。

b） 应定期开展内外部个人金融信息保护培训与意识教育活动，并保留相关记录。

c） 在发生人员调离岗位时，应立即调整和完成相关人员的个人金融信息访问、使用等权限的配置，并明确有关人员后续的个人金融信息保护管理权限和保密责任;若有关人员调整后的岗位不涉及个人金融信息的访问与处理的，应明确其继续履行有关信息的保密义务要求，

d） 与员工终止劳动合同时，应立即终止并收回其对个人金融信息的访问权限，并明确其继续履行有关信息的保密义务要求。

e） 系统开发人员、系统测试人员与运维人员之间不应相互兼岗.

f） 应定期（至少每年一次）或在隐私政策发生重大变化时，对个人金融信息处理岗位上的相关人员开展个人金融信息安全专业化培训和考核，确保相关人员熟练掌握隐私政策和相关规程。

7.3 访问控制

加强个人金融信息访问控制管理，具体要求如卜'：

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） 对于可访同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通程访问设备上留存.

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。

e）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[1]。

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

[1] 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）。

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
个人身份信息	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位十**+后2位。如：90****85台湾：显示前2位十****+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
	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***@11.Com如果少于三位,则全部显示，@前加***，例如tt@111.com则

		显示为tt***e111.com

TC260-PG-20191A 网络安全实践指南—移动互联网应用基本业务功能必要信息规范

时效性：　现行有效

发布机关：　全国信息安全标准化技术委员会

发布日期：　2019 年 06 月 01 日

一、适用范围

本规范给出了移动互联网应用收集个人信息的原则，以及地图导航、网络约车、即时通讯社交、社区社交、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、求职、招聘、金融借贷、房产交易、汽车交易 16 类基本业务功能正常运行所需的个人信息。

本规范适用于移动互联网应用提供者规范个人信息收集行为，也适用于主管监管部门、第三方评估机构等对个人信息收集行为进行监督、管理和评估，还可为移动互联网应用开发者、移动互联网应用分发平台运营者和移动智能终端厂商提供参考。

二、术语定义

1、移动互联网应用

安装、运行在移动智能终端上的应用程序。

2、业务功能

满足个人信息主体的具体使用需求的业务或功能。如地图导航、网络约车、即时通讯社交、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。

3、基本业务功能

满足个人信息主体选择使用移动互联网应用的最主要需求和根本期待的业务或功能。

4、非基本业务功能

移动互联网应用所提供的基本业务功能之外的其他业务或功能。

5、必要信息

保障移动互联网应用基本业务功能正常运行所需的个人信息。关于个人信息的范围和类型参见GB/T35273《信息安全技术 个人信息安全规范》附录A。

6、移动互联网应用提供者提供移动互联网应用的组织或个人。

7、移动互联网应用开发者设计开发移动互联网应用程序的组织或个人，包括移动互联网应用程序的开发者，以及移动互联网应用集成的第三方代码开发者和提供者。

8、移动互联网应用分发平台运营者面向公众提供移动互联网应用分发服务的组织，负责管理移动互联网应用分发平台，对移动互联网应用开发者上传的应用软件进行内容审核、版权保护、发布和管理，同时向移动互联网应用消费者提供应用软件搜索、浏览、下载的梁道。

9、移动智能终端厂商生产移动智能终端的组织。移动智能终端，是指能够接入移动通信网，具备能够提供应用程序开发接口的开放操作系统，并能够安装和运行应用软件的移动终端。

三、个人信息收集原则

移动互联网应用个人信息收集活动，主要依据GB/T35273《信息

安全技术 个人信息安全规范》的"4 个人信息安全基本原则"，遵循以下基本原则：

1）权责一致原则——个人信息收集应遵循法律法规要求，不采用非法的方式和渠道收集个人信息，不收集法律法规禁止的个人信息，不违反与用户的约定收集使用个人信息，并对因个人信息处理活动对个人信息主体合法权益造成的损害承担责任。

2）目的明确原则——向用户明示收集使用个人信息的目的、方式和范围，收集的个人信息及申请的权限应具有合法、正当、必要、明确的收集使用目的和业务功能。

3）最少够用原则——不收集与其提供的服务无关的个人信息，不申请打开可收集无关个人信息的权限。只收集满足业务功能所必需的最少类型和数量的个人信息，自动收集个人信息的频率不超过业务功能实际所需的频率。

4）选择同意原则——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。不以改善服务质量、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。不因个人信息主体拒绝或者撤销同意收集必要信息以外的其他信息，而拒绝提供基本业务功能服务或频繁征求用户同意。

5）公开透明原则——以明确具体、简单通俗、易于访问的方式公开收集、使用个人信息的规则，并接受外部监督。

6）确保安全原则——采用足够的安全技术和管理措施，保障个

人信息收集安全，防范数据窃取、违规爬取、采集传输泄密等安全风险。

四、基本业务功能相关必要信息

依据个人信息收集最少够用的原则，本规范针对地图导航、网络约车、网上购物等16类基本业务功能，给出了每类业务功能相关的必要信息范围。必要信息主要包括基本业务功能相关必要信息和通用功能相关必要信息：基本业务功能相关必要信息，是与基本业务功能直接关联，一旦缺少会导致基本业务功能无法实现或无法正常运行的

个人信息;通用功能相关必要信息，是相关法律法规要求、保障移动互联网应用安全风险管控所必需的个人信息。

（一）地图导航

地图导航是指基于用户地理位置，为用户提供互联网地图和导航服务的业务功能，包括基于用户地理位置定位提供地图搜索和展示服务，及根据用户指令提供由起点到终点的路线规划、导航服务。地图导航基本业务功能收集的必要信息如表1所示。

表1 地图导航基本业务功能必要信息

业务功能	收集信息	使用要求
地图导航	位置信息 1.精准定位信息 2.行踪轨迹	精准定位信息仅用于确定用户位置，进行地图搜索展示和导航服务。行踪轨迹仅用于在导航服务中判断实时路况及重新规划导航路线。

（二）网络约车

网络约车是指为用户提供网络预约汽车服务（不包含汽车租赁服务）的业务功能，涉及网络预约快车、专车、豪华车、出租车、顺风

车等。网络约车基本业务功能收集的必要信息如表 2 所示。

表 2 网络约车基本业务功能必要信息

业务功能	收集信息	使用要求
地图导航	1.手机号码	仅用于满足注册用户实名认证要求,及司机与乘客联系。
	2. 账号信息 账号 口令	仅用于标识网络约车用户和保障账号信息安全。
	3. 位置信息 精准定位信息 行踪轨迹	精准定位信息仅用于确定用户当前位置,推荐周围上车点,搜索显示附近车辆信息。行踪轨迹仅用于保障行程安全及处理用户纠纷,满足网络预约出租汽车经营服务管理暂行办法要求。
	4. 交易信息 订单出发地 订单到达地 订单金额 下单实践	仅用于处理用户纠纷,满足网络预约出租汽车经营服务管理暂行办法要求。
	5. 第三方支付信息 支付方式 支付状态	仅用于用户使用第三方支付方式对叫车订单付款。

表 2 所列个人信息主要是收集的网约车乘客用户的个人信息，不包含网约车车主用户的个人信息。

（三）即时通讯社交

即时通讯社交是指为用户提供即时通讯和社交服务，例如采用文字、图片、语音、视频等形式聊天，进行语音通话、视频通话，建立和反映用户关系，提供社交互动和社交空间晨示等功能。即时通讯社交基本业务功能收集的必要信息如表 3 所示。

表 3 即时通讯社交基本业务功能必要信息

业务功能	收集信息	使用要求
即时通讯社交	1.手机号码	仅用于用户注册，满足注册用户实名认证要求。
	2.账号信息 账号 口令	仅用于标识即时通讯用户、保障账号信息安全和用户聊天交流。

	昵称 头像	
	3.好友列表	仅用于建立和管理用户在即时通讯社交应用的联系人关系。应允许用户在即时通讯社交应用中手动添加好友，而不应强制读取用户的通讯录。
	4. 好友信息 好友账号 好友昵称 好友头像	仅用于向用户展示好友基本信息，或经本人同意后授权第三方平台登录使用。
	5.群列表	仅用于实现群组聊天功能。

（四）社区社交

社区社交是指为具有相同兴趣和共性特征的用户提供社区和社交服务，包括话题讨论、信息分享和关注互动等功能。社区社交基本业务功能收集的必要信息如表4所示。

表4 社区社交基本业务功能必要信息

业务功能	收集信息	使用要求
社区社交	1.手机号码	仅用于用户注册，满足注册用户实名认证要求。
	2.账号信息 账号 口令 昵称 头像	仅用于标识社区社交用户、保障账号信息安全和用户这区互动交流。
	3.好友关注的内容	仅用于建立和管理用户和社区内容（如关注的栏目、关注的话题、关注的吧等）的关注关系，以及向用户展示和推送关注的内容。
	4.关注用户列表	仅用于建立和管理社区用户间的关注关系，以及向用户展示和推送关注的用户发布的图文资讯、音视频、链接等。 应允许用户在社区社交应用中手动设置关注用户，而不应强制读取用户的通讯录。
	5. 公众账号用户信息（仅对公众账号用户收集） 姓名 证件类型	仅用于满足互联网用户公众账号相关管理规定要求，对公众账号用户进行真实身份信息的实名强认证。

	证件号码	

（五）网络支付

网络支付是指为用户提供在收付款人之间转移货币资金的服务的业务功能，包括充值与提现、转账、交易、账单等功能，用户通常远程发起支付指令，且付款客户电子设备不与收款客户特定专属设备交互。网络支付基本业务功能收集的必要信息如表 5 所示。

表 5 网络支付基本业务功能必要信息

业务功能	收集信息	使用要求
网络支付	1.手机号码	仅用于用户注册，满足注册用户实名认证要求。
	2.账号信息 账号 口令	仅用于标识网络支付用户和保障账号信息安全。
	3. 身份信息 姓名 身份证件种类 身份证件号码 身份证件有效期限 身份证件复印件或影印件	仅用于对支付客户进行实名制管理，满足非银支付相关规范性文件要求。
	4. 银行账户信息 开户行名称 银行卡卡号 银行卡有效期限 银行预留手机号码	仅用于实现银行卡和支付账号绑卡、银行卡身份认证、充值、提现、转账功能。
	5. 交易信息 支付指令 交易金额 交易对象 交易商品 交易事件 交易渠道 交易类型 交易币种	仅用于实现收款、转账等支付功能，满足相关法律法规要求。
	6. 交易身份验证信息（用户支付事件可任选一种） 静态密码 数字证书 电子签名	仅用于对用户真实身份进行验证，以确保用户账户与资金安全。

	动态密码	

此外，支付机构通常还会提供基于生物特征的身份验证方式，回涉及个人生物特征信息，但由于生物特征信息比较敏感，应再次告知用户并获得用户明示同意，并应优先采取本地终端认证机制。

（六）新闻资讯

新闻资讯是指为用户提供浏览、搜索和发布图文、音视频等新闻资讯信息服务的业务功能，包括实时新闻、热门资讯等功能。新闻资讯业务基本功能收集的必要信息如表 6 所示。

表 6 新闻资讯基本业务功能必要信息

业务功能	收集信息	使用要求
新闻咨询	1.关注的账号	仅用于向用户展示和推送关注的账号所发布的新闻资讯。
	2. 自媒体用户信息（仅对自媒体用户收集） 姓名 证件类型 证件号码	仅用于满足相关法律法规的实名认证要求，对自媒体用户进行真实身份信息的实名强认证。

新闻资讯业务功能应以提供新闻资讯浏览为主要目的，传统新闻类应用在用户浏览时通常不收集个人信息，但随着新闻资讯应用的发展，也存在以个性化推荐资讯内容为核心业务模式的聚合类新闻应用，该定制化新闻资讯推送功能通常会收集用户的浏览操作记录，用于挖掘用户可能感兴趣的内容及最有价值的新闻进行推送，该业务功能需要告知用户并征得其同意，如果用户拒绝可退出定向推送模式。

（七）短视频

短视频是指为用户提供浏览、搜索、制作、上传、发布短视频等服务的业务功能。短视频基本业务功能收集的必要信息如表 7 所示。

表 7 短视频基本业务功能必要信息

业务功能	收集信息	使用要求
短视频	1.关注的账号	仅用于向用户展示所发布的短视频。
	2.自媒体用户信息（仅对自媒体用户收集） 姓名 证件类型 证件号码	仅用于满足相关法律法规的实名认证要求，对自媒体用户进行真实身份信息的实名强认证。

（八）网上购物

网上购物是通过网络销售商品或服务的业务功能，包括商品展示、搜索、咨询、议价、下单、信用评价、收货等功能。此处的商品或服务不包含金融类产品和服务，和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。网上购物基本业务功能收集的必要信息如表 8 所示。

表 8 网上购物基本业务功能必要信息

业务功能	收集信息	使用要求
网上购物	1. 手机号码	仅用于用户注册，满足注册用户实名认证要求。
	2. 账号信息 账号 口令	仅用于标识网上购物用户和保障账号信息安全。
	3. 收货人信息 姓名 地址 手机号码	仅用于网上购物收货时识别收货人、送达货物和联系收货人。
	4. 交易信息 订单价格 订单商品 下单事件 订单商户 订单编号 订单状态	仅用于实现网上购物的订单交易和处理用户纠纷，满足电子商务法相关要求。

	5. 第三方支付信息 支付账号或交易流水号 支付状态	仅用于实现网上购物的订单支付功能，通常由网上购物业务功能调用第三方支付服务间接获取。

表 8 所列个人信息主要针对大众用户购物的普通场景，不包括为跨境电商通关、购买手机号等实名购买情景下需提供的用户身份信息，实名购物场景下通常需要收集用户的证件号码。在一些 O2O 线上到线下的购物场景中，由于需要判断用户所在的商场、所属的商圈范围等，可能还会收集用户的位置信息，应告知用户并获得用户授权同意。

（九）快递配送

快递配送是指为用户提供信件、包裹、印刷品等物品的寄递的业务功能，包括寄件、查件、收件等功能。快递配送基本业务功能收集的必要信息如表 9 所示。

表 9 快递配送基本业务功能必要信息

业务功能	收集信息	使用要求
快递配送	1. 寄件人基本信息 姓名 地址 联系电话（固定电话或手机号码）	仅用于实现快递寄件和收件功能。
	2. 收件人基本信息 姓名 地址 联系电话	
	3. 快递运单号码	仅用于实现快递查件功能和标识快递件。

表 9 所列个人信息主要针对国内快递配送场景，不包括国际快递场景下需提供的收方身份证信息和清关信息，以及快递增值业务如代收货款等场景下需提供的支付信息。此外，依据快递暂行条例要求，

经营快递业务的企业收寄快件，要对寄件人身份进行查验并登记身份信息，但具有快递配送业务功能的移动互联网应用一般不直接收集相关身份信息。

（十）餐饮外卖

餐饮外卖是指为个人用户提供餐饮等外卖信息和外卖服务的业务功能，包括餐饮配送、到店自取等功能。餐饮外卖基本业务功能收集的必要信息如表 10 所示。

表 10 餐饮外卖基本业务功能必要信息

业务功能	收集信息	使用要求
餐饮外卖	1.手机号码	仅用于用户注册，满足注册用户实名认证要求。
	2.账号信息 账号 口令	仅用于标识餐饮外卖用户和保障账号信息安全。
	3.位置信息	仅用于向用户展示所在位置周边的外卖店铺信息，及便于用户选择外卖收货地址。
	4.联系人信息 姓名 手机号码 地址	仅用于商家和配送员与用户取得联系和配送员送餐，姓名可无需真实。
	5.交易信息 订单商品 订单金额 订单时间 订单商户 订单编号 订单状态	仅用于餐饮外卖订单交易和处理用户纠纷，满足电子商务法相关要求。
	6. 第三方支付信息 支付方式 支付状态	仅用于实现餐饮外卖订单支付。

（十一）交通票务

交通票务是指为用户提供交通相关的票务和运输服务的业务功能，包含票务查询、购买、改签、退票、值机等功能。交通票务基本业务功能收集的必要信息如表 11 所示。

表 11 交通票务基本业务功能必要信息

业务功能	收集信息	使用要求
交通票务	1. 账号信息 账号 口令	仅用于标识交通票务用户和保障账号信息安全。
	2. 旅客和联系人基本信息 姓名（联系人、旅客） 联系人手机号码 旅客类型	仅用于实现用户交通票务和运输服务，包括购票、改签、退票、乘机功能。
	3. 行程信息 出发地 目的地 出发时间 车次/航班号 席别/航位等级 座位号	
	4. 旅客身份信息 旅客证件类型 旅客证件号码	仅用于实现旅客购买车票的实名强认证要求。
	5. 交易信息 订单时间 订单金额 订单编号 订单状态	仅用于实现用户订单查询和处理用户纠纷。

（十二）婚恋相亲

婚恋相亲是指为用户提供征婚服务的业务功能，包括异性推荐、相亲牵线等功能。婚恋相亲基本业务功能收集的必要信息如表 12 所示。

表 12 婚恋相亲基本业务功能必要信息

业务功能	收集信息	使用要求

婚恋相亲	1.手机号码	仅用于用户注册,满足注册用户实名认证要求
	2.账号信息 账号 口令 昵称 本人照片	仅用户标识婚恋相亲用户、保障账号信息安全和展示用户形象。
	3. 个人基本资料 性别 出生日期 所在城市 身高 学历 收入状况 婚姻状况	仅用于一行推荐、相亲牵线等婚恋相亲服务。

（十三）求职招聘

求职招聘是指为用户提供网上招聘和求职服务，包括职位发布、职位展示、职位搜索、投递简历等功能。求职招聘基本业务功能收集的必要信息如表13所示。

表13 求职招聘基本业务功能必要信息

业务功能	收集信息	使用要求
求职招聘	1.手机号码	仅用于用户注册,满足注册用户实名认证要求
	2.账号信息 账号 口令	仅用于标识求职和招聘的用户,保障账号信息安全。
	3.求职者基本信息 姓名 年龄 性别 健康状况 联系邮箱 求职意向	仅用于招聘单位识别求职者、岗位需求匹配、招聘单位与求职者联系使用。 求职者民族、视力应为求职者自愿提供,特殊岗位除外。 求职者健康状况不应出现单项健康信息,如是否为乙肝病毒携带者等。
	4. 求职者教育信息 学校 学历 专业	仅用于求职者简历编辑投递,和招聘单位匹配是否符合岗位需求。

	毕业时间 受教育类型	
	5. 求职者工作经历信息 公司名称 职位职务 在职时间	
	6.招聘者身份证件号码（仅对招聘者用户收集）	仅用于对招聘者身份进行认证。

（十四）金融借贷

金融借贷是指为个人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，这里的金融机构通常是指有放贷资质的银行、消费金融公司、小贷公司等

在网络上提供借贷服务的机构，金融借贷基本业务功能收集的必要信如表 14 所示。

表 14 金融借贷基本业务功能必要信息

业务功能	收集信息	使用要求
金融借贷	1.手机号码	仅用于用户注册，满足注册用户实名认证要求
	2. 账号信息 账号 口令	仅用于对借贷用户进行身份识别和认证，满足相关法律法规要求。
	3.身份信息 姓名 身份证件种类 身份证件号码 身份证件有效期限 身份证件复印件或影印件	仅用于对借贷用户进行身份识别和认证，满足相关法律法规要求。
	4.银行账户信息 开户行名称 银行卡卡号 银行卡有效期限 银行预留手机号码	仅用于实现银行卡和借贷账号绑卡、银行卡身份认证、借款、还款功能。

	5.个人征信信息 中国人民银行个人信用报告 第三方个人信用评分	仅用于对借贷用户的个人信用进行评估，确定授信额度。 个人征信信息须经用户授权查询。
	6. 紧急联系人信息 两位常用联系人的联系方式	仅用于金融机构在借贷个人逾期不还款时进行催款。 应允许用户在金融借贷应用中手动输入紧急联系人信息，而不应强制读取用户的通讯录。
	7. 借贷交易记录 订单号 还款方式 还款期数 还款金额 还款日期 借款本金 利息 订单状态	仅用于实现用户借贷历史查询和处理用户纠纷。

（十五）房产交易

房产交易是指通过网络提供房源信息、房屋出租和买卖服务，包括房源展示、房源搜索、联系预约、房屋出租等功能。房产交易基本业务功能手机的必要信息如表15所示。

表15 房产交易基本业务功能必要信息

业务功能	收集信息	使用要求
房产交易	1.手机号码	仅用于房产交易的用户注册和沟通联系，满足注册用户实名认证要求，用户仅浏览房源信息不需注册。
	2.租户身份信息 身份证件复印件或影印件	仅用于用户线上租房时进行身份验证。
	3.租户身份信息 身份证件复印件或影印件	仅用于用户线上租房时进行身份验证。
	4.交易信息 交易合同信息 交易进度信息	仅用于用户房产交易和处理用户纠纷。

	5. 业主身份信息 身份证件复印件或影印件	仅用于房屋权利人线上发布房源信息、房产交易时对身份进行验证。
	6. 个人房产信息 房屋地址 面积 户型 期望售价或租金	仅用于房源信息发布、房源信息搜索和房产交易。
	7. 第三方支付信息 支付账号或交易流水号 支付状态	仅用于线上租房交易时完成房屋租金支付。

表 15 仅列出通过房产交易类移动互联网应用线上收集的个人信息。目前房产交易服务通常采用线上和线下结合的方式，房源信息和租房大多实现线上服务，而房屋买卖交易仍以线下方式为为主，具体收集信息可依据相关政策文件要求。

（十六）汽车交易

汽车交易是指通过网络为用户提供汽车资讯、新车及二手车交易的服务，包括车源信息搜索和展示、车辆审核、新车和二手车买卖等功能，汽车交易基本业务功能收集的必要信息如表 16 所示。

表 16 汽车交易基本业务功能必要信息

业务功能	收集信息	使用要求
汽车交易	1. 手机号码	仅用于汽车交易的用户注册和沟通联系，满足注册用户实名认证要求，用户仅浏览车源信息不需注册。
	2. 账号信息 账号 口令	仅用于标识汽车交易用户和保障账号信息安全。
	3. 车辆审核地址	仅用于网络发布车源前进行现场审核车源时使用，便于审核员到车辆所在地址进行审核。

	4.购买方信息 姓名 住址 身份证件号码 银行卡号码	仅用于新车和二手车购买方的实名制登记买车、身份验证和完成车辆商户登记、电子签约合同签订等购车流程。 银行卡号码仅用于退还保证金。
	5.出售方信息 姓名 身份证件号码 驾驶证号 车辆行驶证编号	仅用于二手车出售方的实名制登记卖车、身份验证和完成车辆上户登记、电子合同签订、车辆过户等交易流程。
	6.交易信息 订单状态 电子签约合同	仅用于记录汽车交易状态和处理用户纠纷。
	7.第三方支付信息 支付方式 支付状态	仅用于汽车交易居间方服务费支付。

表16仅列出通过汽车交易类移动互联网应用线上收集的个人信息。目前汽车交易服务通常采用线上和线下结合的方式，新车、二手车交易大多已实现电子合同在线签约，车辆审核、车辆上户登记、车辆过户、买卖费用支付等部分环节仍需结合线下进行，比如二手车车辆审核过程中还会收集一些个人车辆信息，具体可参考二手车流通管理办法等相关政策规章要求。

五、通用功能相关必要信息

移动互联网应用因通用性业务功能需求或法律法规要求，收集的必要信息如表17所示。

表17 通用功能相关必要信息

通用功能需求	收集信息	适用的业务功能	使用要求
网络访问	网络访问日志信息： IP地址。 用户登录时间。 用户退出时间。	各类业务功能	仅用于满足相关法律法规要求和网络安全保障需要。

安全风控	设备信息：唯一设备识别码、硬件序列号	具有安全风控需求的业务功能	仅用于保障移动互联网应用业务安全风控，应对反作弊、反欺诈、违法不良信息管控等安全风险。
客户服务	客服场景下的通话记录和内容：电话号码（仅电话客服）通话内容录音（仅电话客服）。聊天信息（在线客服）。	具有客服场景的业务功能	仅用于客服处理用户纠纷，具体包括电话客服和在线客服。

移动互联网应用通常还会因为保障网络安全和处理用户纠纷，实现个性化推荐、提高用户体验和改善服务质量等目的收集个人上网记录，收集个人上网记录需考虑以下几点：

a）收藏、评论、转发、点赞、发布、举报等用户主动操作的日志记录，判断其收集信息必要性需结合这些用户操作的必要性进行判断.

b）浏览、搜索、点击等操作记录通常是非必要信息，收集时告知用户并征得其同意。

c）保存和使用个人上网记录时，对个人信息进行去标识化处理。

d）使用个人上网记录用于分析用户画像进行个性化展示和推荐时，告知用户使用目的，并提供用户退出定向推送模式选项。

此外，移动互联网应用因法律法规等规范性文件要求收集的其他必要信息，仅用于法律法规所描述的用途。

GB/T22239-2019A 信息安全技术网络安全等级保护基本要求

时效性：　　现行有效

发布机关：　国家市场监督管理总局、中国国家标准化管理委员会

类别：　　中华人民共和国国家标准

发布日期：　2019 年 05 月 10 日

1 范围

本标准规定了网络安全等级保护的第一级到第四级等级保护对象的安全通用要求和安全扩展要求。

本标准适用于指导分等级的非涉密对象的安全建设和监督管理。

注：第五级等级保护对象是非常重要的监督管理对象，对其有特殊的管理模式和安全要求，所以不在本标准中进行描述。

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 17859 计算机信息系统安全保护等级划分准则

GB/T 22240 信息安全技术信息系统安全等级保护定级指南

GB/T 25069 信息安全技术术语

GB/T 31167-2014 信息安全技术云计算服务安全指南

GB/T 31168-2014 信息安全技术云计算服务安全能力要求

GB/T 32919-2016 信息安全技术工业控制系统安全控制应用指南。

3 术语和定义

GB 17859、GB/T 22240、GB/T 25069、GB/T 31167-2014、GB/T 31168-2014 和 GB/T 32919—2016 界定的以及下列术语和定义适用于本文件。为了便于使用，以下重复列出了 GB/T 31167—2014、GB/T 31168—2014 和 GB/T 32919—2016 中的一些术语和定义。

3.1 网络安全 cyber security

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。

3.2 安全保护能力 security protection ability

能够抵御威胁、发现安全事件以及在遭到损害后能够恢复先前状态等的程度。

3.3 云计算 cloud computing

通过网络访问可扩展的、灵活的物理或虚拟共享资源池，并按需自助获取和管理资源的模式[1]。

3.4 云服务商 cloud service provider

云计算服务的供应方[2]。

3.5 云服务客户 cloud service customer

为使用云计算服务同云服务商建立业务关系的参与方。

[GB/T 31168—2014，定义 3.4]

---

[1] 注：资源实例包括服务器、操作系统、网络、软件、应用和存储设备等。[GB/T 31167—2014，定义 3.1]

[2] 注：云服务商管理、运营、支撑云计算的计算基础设施及软件，通过网络交付云计算的资源。[GB/T 31167—2014，定义 3.3]

3.6 云计算平台/系统 cloud computing platform/system

云服务商提供的云计算基础设施及其上的服务软件的集合。

3.7 虚拟机监视器 hypervisor

运行在基础物理服务器和操作系统之间的中间软件层，可允许多个操作系统和应用共享硬件。

3.8 宿主机 host machine

运行虚拟机监视器的物理服务器。

3.9 移动互联 mobile communication

采用无线通信技术将移动终端接入有线网络的过程。

3.10 移动终端 mobile device

在移动业务中使用的终端设备，包括智能手机、平板电脑、个人电脑等通用终端和专用终端设备。

3.11 无线接入设备 wireless access device

采用无线通信技术将移动终端接入有线网络的通信设备。

3.12 无线接入网关 wireless access gateway

部署在无线网络与有线网络之间，对有线网络进行安全防护的设备。

3.13 移动应用软件 mobile application

针对移动终端开发的应用软件。

3.14 移动终端管理系统 mobile device management system

用于进行移动终端设备管理、应用管理和内容管理的专用软件，包括客户端软件和服务端软件。

3.15 物联网 internet of things

将感知节点设备通过互联网等网络连接起来构成的系统。

3.16 感知节点设备 sensor node

对物或环境进行信息采集和/或执行操作，并能联网进行通信的装置。

3.17 感知网关节点设备 sensor layer gateway

将感知节点所采集的数据进行汇总、适当处理或数据融合，并进行转发的装置。

3.18 工业控制系统 industrial control system

工业控制系统（ICS）是一个通用术语，它包括多种工业生产中使用的控制系统，包括监控和数据采集系统（SCADA）、分布式控制系统（DCS）和其他较小的控制系统，如可编程逻辑控制器（PLC），现已广泛应用在工业部门和关键基础设施中。

[GB/T 32919—2016，定义 3.1]

4 缩略语

下列缩略语适用于本文件。

AP：无线访问接入点（Wireless Access Point）

DCS：集散控制系统（Distributed Control System）

DDoS：拒绝服务（Distributed Denial of Service）

ERP：企业资源计划（Enterprise Resource Planning）

FTP：文件传输协议（File Transfer Protocol）

HMI：人机界面（Human Machine Interface）

IaaS：基础设施即服务（Infrastructure-as-a-Service）

ICS：工业控制系统（Industrial Control System）

IoT：物联网（Internet of Things）

IP：互联网协议（Internet Protocol）

IT：信息技术（Information Technology）

MES：制造执行系统（Manufacturing Execution System）

PaaS：平台即服务（Platform-as-a-Service）

PLC：可编程逻辑控制器（Programmable Logic Controller）

RFID：射频识别（Radio Frequency Identification）

SaaS：软件即服务（Software-as-a-Service）

SCADA：数据采集与监视控制系统（Supervisory Control and Data Acquisition System）

SSID：服务集标识（Service Set Identifier）

TCB：可信计算基（Trusted Computing Base）

USB：通用串行总线（Universal Serial Bus）

WEP：有线等效加密（Wired Equivalent Privacy）

WPS:WiFi 保护设置（WiFi Protected Setup）

5 网络安全等级保护概述

5.1 等级保护对象

等级保护对象是指网络安全等级保护工作中的对象，通常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，主要包括基础信息

网络、云计算平台/系统、大数据应用/平台/资源、物联网（IoT）、工业控制系统和采用移动互联技术的系统等。等级保护对象根据其在国家安全、经济建设、社会生活中的重要程度，遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等，由低到高被划分为五个安全保护等级。

保护对象的安全保护等级确定方法见GB/T 22240。

5.2 不同级别的安全保护能力

不同级别的等级保护对象应具备的基本安全保护能力如下：

第一级安全保护能力：应能够防护免受来自个人的、拥有很少资源的威胁源发起的恶意攻击、一般的自然灾难，以及其他相当危害程度的威胁所造成的关键资源损害，在自身遭到损害后，能够恢复部分功能。

第二级安全保护能力：应能够防护免受来自外部小型组织的、拥有少量资源的威胁源发起的恶意攻击、一般的自然灾难，以及其他相当危害程度的威胁所造成的重要资源损害，能够发现重要的安全漏洞和处置安全事件，在自身遭到损害后，能够在一段时间内恢复部分功能。

第三级安全保护能力：应能够在统一安全策略下防护免受来自外部有组织的团体、拥有较为丰富资源的威胁源发起的恶意攻击、较为严重的自然灾难，以及其他相当危害程度的威胁所造成的主要资源损害，能够及时发现、监测攻击行为和处置安全事件，在自身遭到损害后，能够较快恢复绝大部分功能。

第四级安全保护能力：应能够在统一安全策略下防护免受来自国家级别的、敌对组织的、拥有丰富资源的威胁源发起的恶意攻击、严重的自然灾难，以及其他相当危害程度的威胁所造成的资源损害，能够及时发现、监测发现攻击行为和安全事件，在自身遭到损害后，能够迅速恢复所有功能。

第五级安全保护能力：略。

5.3 安全通用要求和安全扩展要求

由于业务目标的不同、使用技术的不同、应用场景的不同等因素，不同的等级保护对象会以不同的形态出现，表现形式可能称之为基础信息网络、信息系统（包含采用移动互联等技术的系统）、云计算平台/系统、大数据平台/系统、物联网、工业控制系统等。形态不同的等级保护对象面临的威胁有所不同，安全保护需求也会有所差异。为了便于实现对不同级别的和不同形态的等级保护对象的共性化和个性化保护，等级保护要求分为安全通用要求和安全扩展要求。

安全通用要求针对共性化保护需求提出，等级保护对象无论以何种形式出现，应根据安全保护等级实现相应级别的安全通用要求；安全扩展要求针对个性化保护需求提出，需要根据安全保护等级和使用的特定技术或特定的应用场景选择性实现安全扩展要求。安全通用要求和安全扩展要求共同构成了对等级保护对象的安全要求。安全要求的选择见附录A，整体安全保护能力的要求见附录B和附录C。本标准针对云计算、移动互联、物联网、工业控制系统提出了安全扩展要求。云计算应用场景参见附录D，移动互联应用场景参见附录E，物

联网应用场景参见附录F，工业控制系统应用场景参见附录G，大数据应用场景参见附录H。对于采用其他特殊技术或处于特殊应用场景的等级保护对象，应在安全风险评估的基础上，针对安全风险采取特殊的安全措施作为补充。

6 第一级安全要求

6.1 安全通用要求

6.1.1 安全物理环境

6.1.1.1 物理访问控制

机房出入口应安排专人值守或配置电子门禁系统，控制、鉴别和记录进入的人员。

6.1.1.2 防盗窃和防破坏

应将设备或主要部件进行固定，并设置明显的不易除去的标识。

6.1.1.3 防雷击

应将各类机柜、设施和设备等通过接地系统安全接地。

6.1.1.4 防火

机房应设置灭火设备。

6.1.1.5 防水和防潮

应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透。

6.1.1.6 温湿度控制

应设置必要的温湿度调节设施，使机房温湿度的变化在设备运行所允许的范围之内。

6.1.1.7 电力供应

应在机房供电线路上配置稳压器和过电压防护设备。

6.1.2 安全通信网络

6.1.2.1 通信传输

应采用校验技术保证通信过程中数据的完整性。

6.1.2.2 可信验证

可基于可信根对通信设备的系统引导程序、系统程序等进行可信验证，并在检测到其可信性受到破坏后进行报警。

6.1.3 安全区域边界

6.1.3.1 边界防护

应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。

6.1.3.2 访问控制

本项要求包括：

a）应在网络边界根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；

b）应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；

c）应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出。

6.1.3.3 可信验证

可基于可信根对边界设备的系统引导程序、系统程序等进行可信验证，并在检测到其可信性受到破坏后进行报警。

6.1.4 安全计算环境

6.1.4.1 身份鉴别

本项要求包括：

a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；

b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施。

6.1.4.2 访问控制

本项要求包括：

a）应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。

6.1.4.3 入侵防范

本项要求包括：

a）应遵循最小安装的原则，仅安装需要的组件和应用程序；b）应关闭不需要的系统服务、默认共享和高危端口。

6.1.4.4 恶意代码防范

应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。

6.1.4.5 可信验证

可基于可信根对计算设备的系统引导程序、系统程序等进行可信验证，并在检测到其可信性受到破坏后进行报警。

6.1.4.6 数据完整性

应采用校验技术保证重要数据在传输过程中的完整性。

6.1.4.7 数据备份恢复

应提供重要数据的本地数据备份与恢复功能。

6.1.5 安全管理制度

6.1.5.1 管理制度

应建立日常管理活动中常用的安全管理制度。

6.1.6 安全管理机构

6.1.6.1 岗位设置

应设立系统管理员等岗位，并定义各个工作岗位的职责。

6.1.6.2 人员配备

应配备一定数量的系统管理员。

6.1.6.3 授权和审批

应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等。

6.1.7 安全管理人员

6.1.7.1 人员录用

应指定或授权专门的部门或人员负责人员录用。

6.1.7.2 人员离岗

应及时终止离岗人员的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备。

6.1.7.3 安全意识教育和培训

应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施。

6.1.7.4 外部人员访问管理

应保证在外部人员访问受控区域前得到授权或审批。

6.1.8 安全建设管理

6.1.8.1 定级和备案

应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由。

6.1.8.2 安全方案设计

应根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施。

6.1.8.3 产品采购和使用

应确保网络安全产品采购和使用符合国家的有关规定。

6.1.8.4 工程实施

应指定或授权专门的部门或人员负责工程实施过程的管理。

6.1.8.5 测试验收应进行安全性测试验收。

6.1.8.6 系统交付

本项要求包括：

a）应制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点；

b）应对负责运行维护的技术人员进行相应的技能培训。

6.1.8.7 服务供应商选择

本项要求包括：

a）应确保服务供应商的选择符合国家的有关规定；

b）应与选定的服务供应商签订与安全相关的协议，明确约定相关责任。

6.1.9 安全运维管理

6.1.9.1 环境管理

本项要求包括：

a)应指定专门的部门或人员负责机房安全，对机房出入进行管理，定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理；

b）应对机房的安全管理做出规定，包括物理访问、物品进出和环境安全等方面。

6.1.9.2 介质管理

应将介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点。

6.1.9.3 设备维护管理

应对各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理。

6.1.9.4 漏洞和风险管理

应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补。

6.1.9.5 网络和系统安全管理

本项要求包括：

a）应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限；

b）应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制。

6.1.9.6 恶意代码防范管理

本项要求包括：

a）应提高所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等；b）应对恶意代码防范要求做出规定，包括防恶意代码软件的授权使用、恶意代码库升级、恶意代码的定期查杀等。

6.1.9.7 备份与恢复管理

本项要求包括：

a）应识别需要定期备份的重要业务信息、系统数据及软件系统等；

b）应规定备份信息的备份方式、备份频度、存储介质、保存期等。

6.1.9.8 安全事件处置

本项要求包括：

a）应及时向安全管理部门报告所发现的安全弱点和可疑事件；

b）应明确安全事件的报告和处置流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责。

6.2 云计算安全扩展要求

6.2.1 安全物理环境

6.2.1.1 基础设施位置

应保证云计算基础设施位于中国境内。

6.2.2 安全通信网络

6.2.2.1 网络架构

本项要求包括：

a）应保证云计算平台不承载高于其安全保护等级的业务应用系统；

b）应实现不同云服务客户虚拟网络之间的隔离。

6.2.3 安全区域边界

6.2.3.1 访问控制

应在虚拟化网络边界部署访问控制机制，并设置访问控制规则。

6.2.4 安全计算环境

6.2.4.1 访问控制

本项要求包括：

a）应保证当虚拟机迁移时，访问控制策略随其迁移；

b）应允许云服务客户设置不同虚拟机之间的访问控制策略。

6.2.4.2 数据完整性和保密性

应确保云服务客户数据、用户个人信息等存储于中国境内，如需出境应遵循国家相关规定。

6.2.5 安全建设管理

6.2.5.1 云服务商选择

本项要求包括：

a）应选择安全合规的云服务商，其所提供的云计算平台应为其所

承载的业务应用系统提供相应等级的安全保护能力；

b)应在服务水平协议中规定云服务的各项服务内容和具体技术指标；

c）应在服务水平协议中规定云服务商的权限与责任，包括管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任等。

6.2.5.2 供应链管理

应确保供应商的选择符合国家有关规定。

6.3 移动互联安全扩展要求

6.3.1 安全物理环境

6.3.1.1 无线接入点的物理位置

应为无线接入设备的安装选择合理位置，避免过度覆盖和电磁干扰。

6.3.2 安全区域边界 6.3.2.1 边界防护

应保证有线网络与无线网络边界之间的访问和数据流通过无线接入安全网关设备。

6.3.2.2 访问控制

无线接入设备应开启接入认证功能，并且禁止使用 WEP 方式进行认证，如使用口令，长度不小于 8 位字符。

6.3.3 安全计算环境

6.3.3.1 移动应用管控

应具有选择应用软件安装、运行的功能。

6.3.4 安全建设管理

6.3.4.1 移动应用软件采购

应保证移动终端安装、运行的应用软件来自可靠分发渠道或使用可靠证书签名。

6.4 物联网安全扩展要求

6.4.1 安全物理环境

6.4.1.1 感知节点设备物理防护

本项要求包括：

a）感知节点设备所处的物理环境应不对感知节点设备造成物理破坏，如挤压、强振动；b）感知节点设备在工作状态所处物理环境应能正确反映环境状态（如温湿度传感器不能安装在阳光直射区域）。

6.4.2 安全区域边界 6.4.2.1 接入控制

应保证只有授权的感知节点可以接入。

6.4.3 安全运维管理

6.4.3.1 感知节点管理

应指定人员定期巡视感知节点设备、网关节点设备的部署环境，对可能影响感知节点设备、网关节点设备正常工作的环境异常进行记录和维护。

6.5 工业控制系统安全扩展要求

6.5.1 安全物理环境

6.5.1.1 室外控制设备物理防护

本项要求包括：

a）室外控制设备应放置于采用铁板或其他防火材料制作的箱体或

装置中并紧固；箱体或装置具有透风、散热、防盗、防雨和防火能力等；b）室外控制设备放置应远离强电磁干扰、强热源等环境，如无法避免应及时做好应急处置及检修，保证设备正常运行。

6.5.2 安全通信网络 6.5.2.1 网络架构

本项要求包括：

a）工业控制系统与企业其他系统之间应划分为两个区域，区域间应采用技术隔离手段；b）工业控制系统内部应根据业务特点划分为不同的安全域，安全域之间应采用技术隔离手段。

6.5.3 安全区域边界 6.5.3.1 访问控制

应在工业控制系统与企业其他系统之间部署访问控制设备，配置访问控制策略，禁止任何穿越区域边界的 E-Mail、Web、Telnet、Rlogin、FTP 等通用网络服务。

6.5.3.2 无线使用控制

本项要求包括：

a）应对所有参与无线通信的用户（人员、软件进程或者设备）提供唯一性标识和鉴别；b）应对无线连接的授权、监视以及执行使用进行限制。

6.5.4 安全计算环境

6.5.4.1 控制设备安全

本项要求包括：

a）控制设备自身应实现相应级别安全通用要求提出的身份鉴别、访问控制和安全审计等安全要求，如受条件限制控制设备无法实现上

述要求，应由其上位控制或管理设备实现同等功能或通过管理手段控制；b）应在经过充分测试评估后，在不影响系统安全稳定运行的情况下对控制设备进行补丁更新、固件更新等工作。

7 第二级安全要求

7.1 安全通用要求

7.1.1 安全物理环境

7.1.1.1 物理位置选择

本项要求包括：

a）机房场地应选择在具有防震、防风和防雨等能力的建筑内；

b）机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施。

7.1.1.2 物理访问控制

机房出入口应安排专人值守或配置电子门禁系统，控制、鉴别和记录进入的人员。

7.1.1.3 防盗窃和防破坏

本项要求包括：

a)应将设备或主要部件进行固定,并设置明显的不易除去的标识；

b）应将通信线缆铺设在隐蔽安全处。

7.1.1.4 防雷击

应将各类机柜、设施和设备等通过接地系统安全接地。

7.1.1.5 防火

本项要求包括：

a）机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火；

b）机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料。

7.1.1.6 防水和防潮

本项要求包括：

a）应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；b）应采取措施防止机房内水蒸气结露和地下积水的转移与渗透。

7.1.1.7 防静电

应采用防静电地板或地面并采用必要的接地防静电措施。

7.1.1.8 温湿度控制

应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内。

7.1.1.9 电力供应

本项要求包括：

a）应在机房供电线路上配置稳压器和过电压防护设备；

b）应提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求。

7.1.1.10 电磁防护

电源线和通信线缆应隔离铺设，避免互相干扰。

7.1.2 安全通信网络

7.1.2.1 网络架构

本项要求包括：

a）应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）应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段。

7.1.2.2 通信传输

应采用校验技术保证通信过程中数据的完整性。

7.1.2.3 可信验证

可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

7.1.3 安全区域边界

7.1.3.1 边界防护

应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。

7.1.3.2 访问控制

本项要求包括：

a）应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；

b）应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；

c）应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；

d）应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力。

7.1.3.3 入侵防范

应在关键网络节点处监视网络攻击行为。

7.1.3.4 恶意代码防范

应在关键网络节点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。

7.1.3.5 安全审计

本项要求包括：

a）应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；

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，避免受到未预期的删除、修改或覆盖等。

7.1.3.6 可信验证

可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

7.1.4 安全计算环境

7.1.4.1 身份鉴别

本项要求包括：

a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；

b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；

c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。

7.1.4.2 访问控制

本项要求包括：

a）应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）应授予管理用户所需的最小权限，实现管理用户的权限分离。

7.1.4.3 安全审计

本项要求包括：

a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；

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，避免受到未预期的删除、修改或覆盖等。

7.1.4.4 入侵防范

本项要求包括：

a）应遵循最小安装的原则，仅安装需要的组件和应用程序；

b）应关闭不需要的系统服务、默认共享和高危端口；

c）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）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；

e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。

7.1.4.5 恶意代码防范

应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。

7.1.4.6 可信验证

可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

7.1.4.7 数据完整性

应采用校验技术保证重要数据在传输过程中的完整性。

7.1.4.8 数据备份恢复

本项要求包括：

a）应提供重要数据的本地数据备份与恢复功能；

b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。

7.1.4.9 剩余信息保护

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。

7.1.4.10 个人信息保护

本项要求包括：

a）应仅采集和保存业务必需的用户个人信息；

b）应禁止未授权访问和非法使用用户个人信息。

7.1.5 安全管理中心

7.1.5.1 系统管理

本项要求包括：

a）应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计；

b)应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。

7.1.5.2 审计管理

本项要求包括：

a）应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计；

b）应通过审计管理员对审计记录进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。

7.1.6 安全管理制度

7.1.6.1 安全策略

应制定网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全框架等。

7.1.6.2 管理制度

本项要求包括：

a）应对安全管理活动中的主要管理内容建立安全管理制度；

b）应对管理人员或操作人员执行的日常管理操作建立操作规程。

7.1.6.3 制定和发布

本项要求包括：

a）应指定或授权专门的部门或人员负责安全管理制度的制定；

b）安全管理制度应通过正式、有效的方式发布，并进行版本控制。

7.1.6.4 评审和修订

应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。

7.1.7 安全管理机构

7.1.7.1 岗位设置

本项要求包括：

a）应设立网络安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责；

b）应设立系统管理员、审计管理员和安全管理员等岗位，并定义部门及各个工作岗位的职责。

7.1.7.2 人员配备

应配备一定数量的系统管理员、审计管理员和安全管理员等。

7.1.7.3 授权和审批

本项要求包括：

a）应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等；

b）应针对系统变更、重要操作、物理访问和系统接入等事项执行审批过程。

7.1.7.4 沟通和合作

本项要求包括：

a）应加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通，定期召开协调会议，共同协作处理网络安全问题；

b）应加强与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通；

c）应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。

7.1.7.5 审核和检查

应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况。

7.1.8 安全管理人员

7.1.8.1 人员录用

本项要求包括：

a）应指定或授权专门的部门或人员负责人员录用；

b）应对被录用人员的身份、安全背景、专业资格或资质等进行审查。

7.1.8.2 人员离岗

应及时终止离岗人员的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备。

7.1.8.3 安全意识教育和培训

应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施。

7.1.8.4 外部人员访问管理

本项要求包括：

a）应在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案；

b）应在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并登记备案；

c）外部人员离场后应及时清除其所有的访问权限。

7.1.9 安全建设管理

7.1.9.1 定级和备案

本项要求包括：

a)应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由；

b)应组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定；

c）应保证定级结果经过相关部门的批准；

d）应将备案材料报主管部门和相应公安机关备案。

7.1.9.2 安全方案设计

本项要求包括：

a）应根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施；

b）应根据保护对象的安全保护等级进行安全方案设计；

c）应组织相关部门和有关安全专家对安全方案的合理性和正确性进行论证和审定，经过批准后才能正式实施。

7.1.9.3 产品采购和使用

本项要求包括：

a）应确保网络安全产 品采购和使用符合国家的有关规定；

b）应确保密码产品与服务的采购和使用符合国家密码管理主管部门的要求。

7.1.9.4 自行软件开发

本项要求包括：

a）应将开发环境与实际运行环境物理分开，测试数据和测试结果受到控制；

b）应在软件开发过程中对安全性进行测试，在软件安装前对可能存在的恶意代码进行检测。

7.1.9.5 外包软件开发

本项要求包括：

a）应在软件交付前检测其中可能存在的恶意代码；

b）应保证开发单位提供软件设计文档和使用指南。

7.1.9.6 工程实施

本项要求包括：

a）应指定或授权专门的部门或人员负责工程实施过程的管理；

b）应制定安全工程实施方案控制工程实施过程。

7.1.9.7 测试验收

本项要求包括：

a）应制订测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告；

b）应进行上线前的安全性测试，并出具安全测试报告。

7.1.9.8 系统交付

本项要求包括：

a）应制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点；

b）应对负责运行维护的技术人员进行相应的技能培训；

c）应提供建设过程文档和运行维护文档。

7.1.9.9 等级测评

本项要求包括：

a）应定期进行等级测评，发现不符合相应等级保护标准要求的及时整改；

b）应在发生重大变更或级别发生变化时进行等级测评；

c）应确保测评机构的选择符合 国家有关规定。

7.1.9.10 服务供应商选择

本项要求包括：

a）应确保服务 供应商的选择符合国家的有关规定；

b）应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务。

7.1.10 安全运维管理

7.1.10.1 环境管理

本项要求包括：

a)应指定专门的部门或人员负责机房安全,对机房出入进行管理,定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理；

b）应对机房的安全管理做出规定，包括物理访问、物品进出和环境安全等；

c）应不在重要区域接待来访人员，不随意放置含有敏感信息的纸档文件和移动介质等。

7.1.10.2 资产管理

应编制并保存与保护对象相关的资产清单，包括资产责任部门.重要程度和所处位置等内容。

7.1.10.3 介质管理

本项要求包括：

a）应将介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点；

b）应对介质在物理传输过程中的人员选择、打包.交付等情况进行控制，并对介质的归档和查询等进行登记记录。

7.1.10.4 设备维护管理

本项要求包括：

a）应对各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理；

b）应对配套设施、软硬件维护管理做出规定，包括明确维护人员的责任、维修和服务的审批、维修过程的监督控制等。

7.1.10.5 漏洞和风险管理

应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补。

7.1.10.6 网络和系统安全管理

本项要求包括：

a）应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限；

b）应指定专门的部门或人员进行账户管理，对申请账户、建立账户.删除账户等进行控制；

c）应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定；

d）应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等；

e）应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容。

7.1.10.7 恶意代码防范管理

本项要求包括：

a）应提高所有用户 的防恶意代码意识，对外来计算机或存储设备接人系统前进行恶意代码检查等；

b）应对恶意代码防范要求做出规定，包括防恶意代码软件的授权使用、恶意代码库升级、恶意代码的定期查杀等；

c）应定期检查恶意代码库的升级情况，对截获的恶意代码进行及时分析处理。

7.1.10.8 配置管理

应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等。

7.1.10.9 密码管理

本项要求包括：

a）应遵循密码相关国家标准和行业标准；

b）应使用国家密码管理主管部门认证核准的密码技术和产品。

7.1.10.10 变更管理

应明确变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施。

7.1.10.11 备份与恢复管理

本项要求包括：

a)应识别需要定期备份的重要业务信息、系统数据及软件系统等；

b）应规定备份信息的备份方式、备份频度、存储介质、保存期等；

c）应根据数据的重 要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序等。

7.1.10.12 安全事件处置

本项要求包括：

a）应及时向安全管理部门报告所发现的安全弱点和可疑事件；

b）应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等；

c）应在安全事件报告和响应 处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训。

7.1.10.13 应急预案管理

本项要求包括：

a）应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容；

b）应定期对系统相关的人员进行应急预案培训，并进行应急预案的演练。

7.1.10.14 外包运维管理

本项要求包括：

a）应确保外包运维服务商的选择符合国家的有关规定；

b）应与选定的外包运维服务商签订相关的协议。明确约定外包运维的范围、工作内容。

7.2 云计算安全扩展要求

7.2.1 安全物理环境

7.2.1.1 基础设施位置

应保证云计算基础设施位于中国境内。

7.2.2 安全通信网络

7.2.2.1 网络架构

本项要求包括：

a）应保证云计算平台不承载高于其安全保护等级的业务应用系统；

b）应实现不同云服务客户虚拟网络之间的隔离；

c）应具有根据云服务客户业务需求提供通信传输、边界防护、入侵防范等安全机制的能力。

7.2.3 安全区域边界

7.2.3.1 访问控制

本项要求包括：

a)应在虚拟化网络边界部署访问控制机制,并设置访问控制规则；

b）应在不同等级的网络区域边界部署访问控制机制，设置访问控制规则。

7.2.3.2 入侵防范

本项要求包括：

a）应能检测到云服务客户发起的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等；

b）应能检测到对虚拟网络节点的网络攻击行为.并能记录攻击类型、攻击时间、攻击流量等；

c)应能检测到虚拟机与宿主机、虚拟机与虚拟机之间的异常流量。

7.2.3.3 安全审计

本项要求包括：

a)应对云服务商和云服务客户在远程管理时执行的特权命令进行审计，至少包括虚拟机删除、虚拟机重启；

b)应保证云服务商对云服务客户系统和数据的操作可被云服务客户审计。

7.2.4 安全计算环境.

7.2.4.1 访问控制

本项要求包括：

a）应保证当虚拟机迁移时，访问控制策略随其迁移；

b）应允许云服务客户设置不同虚拟机之间的访问控制策略。

7.2.4.2 镜像和快照保护

本项要求包括：

a)应针对重要业务系统提供加固的操作系统镜像或操作系统安全加固服务；

b）应提供虚拟机镜像、快照完整性校验功能，防止虚拟机镜像被恶意篡改。

7.2.4.3 数 据完整性和保密性

本项要求包括：

a）应确保云服务客户数据、用户个人信息等存储于中国境内，如需出境应遵循国家相关规定；

b）应确保只有在云服务客户授权下，云服务商或第三方才具有云服务客户数据的管理权限；

c）应确保虚拟机迁移过程中重要数据的完整性，并在检测到完整性受到破坏时采取必要的恢复措施。

7.2.4.4 数据备份恢复

本项要求包括：

a）云服务客户应在本地保存其业务数据的备份；

b）应提供查询云服务客户数据及备份存储位置的能力。

7.2.4.5 剩余信息保护

本项要求包括：

a）应保证虚拟机所使用的内存和存储空间回收时得到完全清除；

b）云服务客户删除业务应用数据时，云计算平台应将云存储中所有副本删除。

7.2.5 安全建设管理

7.2.5.1 云服务商选择

本项要求包括：

a）应选择安全合规的云服务商，其所提供的云计算平台应为其所承载的业务应用系统提供相应等级的安全保护能力；

b)应在服务水平协议中规定云服务的各项服务内容和具体技术指标；

c）应在服务水平协议中规定云服务商的权限与责任，包括管理范围.职责划分、访问授权、隐私保护、行为准则、违约责任等；

d）应在服务水平协议中规定服务合约到期时，完整提供云服务客户数据，并承诺相关数据在云计算平台.上清除。

7.2.5.2 供应链管理

本项要求包括：

a）应确保供应商的选择符合国家有关规定；

b)应将供应链安全事件信息或安全威胁信息及时传达到云服务客户。

7.2.6 安全运维管理

7.2.6.1 云计算环境管理

云计算平台的运维地点应位于中国境内，境外对境内云计算平台实施运维操作应遵循国家相关规定。

7.3 移动互联安全扩展要求

7.3.1 安全物理环境

7.3.1.1 无线接入点的物理位置

应为无线接人设备的安装选择合理位置，避免过度覆盖和电磁干扰。

7.3.2 安全区域边界

7.3.2.1 边界防护

应保证有线网络与无线网络边界之间的访问和数据流通过无线接入网关设备。

7.3.2.2 访问控制

无线接人设备应开启接入认证功能，并且禁止使用 WEP 方式进行认证，如使用口令，长度不小于 8 位字符。

7.3.2.3 入侵防范

本项要求包括：

a）应能够检测到非授权无线接入设备和非授权移动终端的接入行为；

b）应能够检测到针对无线接入设备的网络扫描.DDoS 攻击、密钥破解、中间人攻击和欺骗攻击等行为；

c）应能够检测到无线接入设备的 SSID 广播、WPS 等高风险功能的开启状态；

d）应禁用无线接入设备和无线接入网关存在风险的功能.如：SSID 广播、WEP 认证等；

e）应禁止多个 AP 使用同一个认证密钥。

7.3.3 安全计算环境

7.3.3.1 移动应用管控

本项要求包括：

a）应具有选择应用软件安装、运行的功能；

b）应只允许可靠证书签名的应用软件安装和运行。

7.3.4 安全建设管理

7.3.4.1 移动应用软件采购

本项要求包括：

a）应保证移动终端安装、运行的应用软件来自可靠分发渠道或使用可靠证书签名；

b）应保证移动终端安装、运行的应用软件由可靠的开发者开发。

7.3.4.2 移动应用软件开发

本项要求包括：

a）应对移动业务应用 软件开发者进行资格审查；

b）应保证开发移动业务应用软件的签名证书合法性。

7.4 物联网安全扩展要求

7.4.1 安全物理环境

7.4.1.1 感知节点设备物理防护

本项要求包括：

a）感知节点设备所处的物理环境应不对感知节点设备造成物理破坏，如挤压、强振动；

b）感知节点设备在工作状态所处物理环境应能正确反映环境状态（如温湿度传感器不能安装在阳光直射区域）。

7.4.2 安全区域边界

7.4.2.1 接入控制

应保证只有授权的感知节点可以接人。

7.4.2.2 入侵防范

本项要求包括：

a）应能够限制与感知节点通信的目标地址，以避免对陌生地址的攻击行为；

b）应能够限制与网关节点通信的目标地址，以避免对陌生地址的攻击行为。

7.4.3 安全运维管理

7.4.3.1 感知节点管理

本项要求包括：

a)应指定人员定期巡视感知节点设备、网关节点设备的部署环境，对可能影响感知节点设备、网关节点设备正常工作的环境异常进行记录和维护；

b）应对感知节点设备、网关节点设备入库、存储、部署、携带、维修、丢失和报废等过程作出明确规定，并进行全程管理，

7.5 工业控制系统安全扩展要求

7.5.1 安全物理环境

7.5.1.1 室外控制设备物理防护

本项要求包括：

a)室外控制设备应放置于采用铁板或其他防火材料制作的箱体或装置中并紧固；箱体或装置具有透风、散热、防盗、防雨和防火能力等；

b）室外控制设备放置应远离强电磁干扰、强热源等环境，如无法避免应及时做好应急处置及检修，保证设备正常运行。

7.5.2 安全通信网络

7.5.2.1 网络架构

本项要求包括：

a）工业控制系统与企业其他系统之间应划分为两个区域，区域间应采用技术隔离手段；

b）工业控制系统内部应根据业务特点划分为不同的安全域，安全域之间应采用技术隔离手段；.

c）涉及实时控制和数据传输的工业控制系统，应使用独立的网络设备组网，在物理层面上实现与其他数据网及外部公共信息网的安全隔离。

7.5.2.2 通信传输

在工业控制系统内使用广域网进行控制指令或相关数据交换的应采用加密认证技术手段实现身份认证、访问控制和数据加密传输。

7.5.3 安全区域边界

7.5.3.1 访问控制

本项要求包括：

a）应在工业控制系统与企业其他系统之间部署访问控制设备.配置访问控制策略.禁止任何穿越区域边界的 E-Mail、Web.Telnet、Rlogin.FTP 等通用网络服务；

b)应在工业控制系统内安全域和安全域之间的边界防护机制失效时，及时进行报警。

7.5.3.2 拨号使用控制.

工业控制系统确需使用拨号访问服务的，应限制具有拨号访问权

限的用户数量，并采取用户身份鉴别和访问控制等措施。

7.5.3.3 无线使用控制

本项要求包括：

a）应对所有参与无线通信的用户（人员、软件进程或者设备）提供唯一性标识和鉴别；

b）应对所有参与无线通信的用户（人员、软件进程或者设备）进行授权以及执行使用进行限制。

7.5.4 安全计算环境

7.5.4.1 控制设备安全

本项要求包括：

a）控制设备自身应实现相应级别安全通用要求提出的身份鉴别、访问控制和安全审计等安全要求，如受条件限制控制设备无法实现上述要求，应由其上位控制或管理设备实现同等功能或通过管理手段控制；

b）应在经过充分测试评估后，在不影响系统安全稳定运行的情况下对控制设备进行补丁更新、固件更新等工作。

7.5.5 安全建设管理

7.5.5.1 产品采购和使用

工业控制系统重要设备应通过专业机构的安全性检测后方可采购使用。

7.5.5.2 外包软件开发

应在外包开发合同中规定针对开发单位、供应商的约束条款，包

括设备及系统在生命周期内有关保密、禁止关键技术扩散和设备行业专用等方面的内容。

8 第三级安全要求

8.1 安全通用要求

8.1.1 安全物理环境

8.1.1.1 物理位置选择

本项要求包括：

a）机房场地应选择在具有防震、防风和防雨等能力的建筑内；

b）机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施。

8.1.1.2 物理访问控制

机房出入口应配置电子门禁系统，控制、鉴别和记录进入的人员。

8.1.1.3 防盗窃和防破坏

本项要求包括：

a)应将设备或主要部件进行固定,并设置明显的不易除去的标识；

b）应将通信线缆铺设在隐蔽安全处；

c）应设置机房防盗报警系统或设置有专人值守的视频监控系统。

8.1.1.4 防雷击

本项要求包括：

a）应将各类机柜、设施和设备等通过接地系统安全接地；

b）应采取措施防止感应雷，例如设置防雷保安器或过压保护装置等。

8.1.1.5 防火

本项要求包括：

a）机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火；

b）机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料；

c）应对机房划分区域进行管理，区域和区域之 间设置隔离防火措施。

8.1.1.6 防水和防潮

本项要求包括：

a）应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；

b）应采取措施防止机房内水蒸气结露和地下积水的转移与渗透；

c）应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警。

8.1.1.7 防静电

本项要求包括：

a）应采用防静电地板或地面并采用必要的接地防静电措施；

b）应采取措施防止静电的产生.例如采用静电消除器、佩戴防静电手环等。

8.1.1.8 温湿度控制

应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内。

8.1.1.9 电力供应

本项要求包括：

a）应在机房供电线路上配置稳压器和过电压防护设备；

b）应提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求；

c）应设置冗余或并行的电力电缆线路为计算机系统供电。

8.1.1.10 电磁防护

本项要求包括：

a）电源线和通信线缆应隔离铺设，避免互相干扰；

b）应对关键设备实施电磁屏蔽。

8.1.2 安全通信网络

8.1.2.1 网络架构

本项要求包括：

a）应保证网络设备的业务处理能力满足业务高峰期需要；

b）应保证网络各个部分的带宽满足业务高峰期需要；

c）应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；

d）应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段；

e）应提供通信线路、关键网络设备和关键计算设备的硬件冗余，保证系统的可用性。

8.1.2.2 通信传输

本项要求包括：

a）应采用校验技术或密码技术保证通信过程中数据的完整性；

b）应采用密码技术保证通信过程中数据的保密性。

8.1.2.3 可信验证

可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心

8.1.3 安全区域边界

8.1.3.1 边界防护

本项要求包括：

a)应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信；

b）应能够对非授权设备私自联到内部网络的行为进行检查或限制；

c）应能够对内部用户非授权联到外部网络的行为进行检查或限制；

d)应限制无线网络的使用，保证无线网络通过受控的边界设备接入内部网络，

8.1.3.2 访问控制

本项要求包括：

a）应在网络边界或区域之间根据访问控制策略设置访问控制规

则，默认情况下除允许通信外受控接口拒绝所有通信；

b）应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；

c）应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；

d）应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力；

e）应对进出网络的数据流实现基于应用协议和应用内容的访问控制。

8.1.3.3 入侵防范

本项要求包括：

a）应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为；

b）应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为；

c）应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析；

d）当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目标、攻击时间，在发生严重入侵事件时应提供报警。

8.1.3.4 恶意代码和垃圾邮件防范

本项要求包括：

a）应在关键网络节点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；

b）应在关键网络节点处对垃圾邮件进行检测和防护，并维护垃圾邮件防护机制的升级和更新。

8.1.3.5 安全审计

本项要求包括：

a）应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；

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，避免受到未预期的删除、修改或覆盖等；

d）应能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。

8.1.3.6 可信验证

可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

8.1.4 安全计算环境

8.1.4.1 身份鉴别

本项要求包括：

a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，

身份鉴别信息具有复杂度要求并定期更换；

b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；

c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听；

d）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。

8.1.4.2 访问控制

本项要求包括：

a）应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）应授予管理用户所需的最小权限，实现管理用户的权限分离；

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或进程级，客体为文件、数据库表级；

g）应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。

8.1.4.3 安全审计

本项要求包括：

a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；

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，避免受到未预期的删除、修改或覆盖等；

d）应对审计进程进行保护，防止未经授权的中断。

8.1.4.4 入侵防范

本项要求包括：

a）应遵循最小安装的原则，仅安装需要的组件和应用程序；

b）应关闭不需要的系统服务、默认共享和高危端口；

c）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）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；

e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞；

f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。

8.1.4.5 恶意代码防范

应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断

8.1.4.6 可信验证

可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

8.1.4.7 数据完整性

本项要求包括：

a）应采用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、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等；

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、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。

8.1.4.8 数据保密性

本项要求包括：

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、重要业务数据和重要个人信息等

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、重要业务数据和重要个人信息等

8.1.4.9 数据备份恢复

本项要求包括：

a）应提供重要数据的本地数据备份与恢复功能；

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。

8.1.4.10 剩余信息保护

本项要求包括：

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）应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除。

8.1.4.11 个人信息保护

本项要求包括：

a）应仅采集和保存业务必需的用户个人信息；

b）应禁止未授权访问和非法使用用户个人信息。

8.1.5 安全管理中心

8.1.5.1 系统管理

本项要求包括：

a）应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计；

b）应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。

8.1.5.2 审计管理

本项要求包括：

a）应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计；

b）应通过审计管理员对审计记录应进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。

8.1.5.3 安全管理

本项要求包括：

a）应对安全管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全管理操作，并对这些操作进行审计；

b）应通过安全管理员对系统中的安全策略进行配置，包括安全参数的设置，主体、客体进行统一安全标记，对主体进行授权，配置可信验证策略等。

8.1.5.4 集中管控

本项要求包括：

a）应划分出特定的管理区域，对分布在网络中的安全设备或安全组件进行管控；

b）应能够建立一条安全的信息传输路径，对网络中的安全设备或安全组件进行管理；

c）应对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测；

d）应对分散在各个设备上的审计数据进行收集汇总和集中分析，并保证审计记录的留存时间符合法律法规要求；

e）应对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理；

f）应能对网络中发生的各类安全事件进行识别、报警和分析。

8.1.6 安全管理制度

8.1.6.1 安全策略

应制定网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全框架等。

8.1.6.2 管理制度

本项要求包括：

a）应对安全管理活动中的各类管理内容建立安全管理制度；

b）应对管理人员或操作人员执行的日常管理操作建立操作规程；

c）应形成由安全策略、管理制度、操作规程、记录表单等构成的全面的安全管理制度体系。

8.1.6.3 制定和发布

本项要求包括：

a）应指定或授权专门的部门或人员负责安全管理制度的制定；

b）安全管理制度应通过正式、有效的方式发布，并进行版本控制。

8.1.6.4 评审和修订

应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。

8.1.7 安全管理机构

8.1.7.1 岗位设置

本项要求包括

a）应成立指导和管理网络安全工作的委员会或领导小组，其最高领导由单位主管领导担任或授权；

b）应设立网络安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责；

c）应设立系统管理员、审计管理员和安全管理员等岗位，并定义部门及各个工作岗位的职责。

8.1.7.2 人员配备

本项要求包括：

a）应配备一定数量的系统管理员、审计管理员和安全管理员等；

b）应配备专职安全管理员，不可兼任

8.1.7.3 授权和审批

本项要求包括：

a）应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等；

b）应针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序，按照审批程序执行审批过程，对重要活动建立逐级审批制度；

c）应定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息。

8.1.7.4 沟通和合作

本项要求包括：

a）应加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通，定期召开协调会议，共同协作处理网络安全问题；

b）应加强与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通；

c）应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。

8.1.7.5 审核和检查

本项要求包括：

a）应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况；

b）应定期进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等；

c）应制定安全检查表格实施安全检查，汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报

8.1.8 安全管理人员

8.1.8.1 人员录用

本项要求包括：

a）应指定或授权专门的部门或人员负责人员录用；

b）应对被录用人员的身份、安全背景、专业资格或资质等进行审查，对其所具有的技术技能进行考核

c）应与被录用人员签署保密协议，与关键岗位人员签署岗位责任协议。

8.1.8.2 人员离岗

本项要求包括

a）应及时终止离岗人员的所有访问权限，取回各种身份证件、钥匙、微章等以及机构提供的软硬件设备；

b)应办理严格的调离手续,并承诺调离后的保密义务后方可离开。

8.1.8.3 安全意识教育和培训

本项要求包括：

a）应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施；

b）应针对不同岗位制定不同的培训计划，对安全基础知识、岗位操作规程等进行培训；c）应定期对不同岗位的人员进行技能考核。

8.1.8.4 外部人员访问管理

本项要求包括：

a）应在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案；

b）应在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并登记备案；

c）外部人员离场后应及时清除其所有的访问权限；

d）获得系统访问授权的外部人员应签署保密协议，不得进行非授权操作，不得复制和泄露任何敏感信息。

8.1.9 安全建设管理

8.1.9.1 定级和备案

本项要求包括：

a）应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由；

b）应组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定；

c）应保证定级结果经过相关部门的批准；

d）应将备案材料报主管部门和相应公安机关备案。

8.1.9.2 安全方案设计

本项要求包括：

a）应根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施；

b）应根据保护对象的安全保护等级及与其他级别保护对象的关系进行安全整体规划和安全方案设计，设计内容应包含密码技术相关内容，并形成配套文件；

c）应组织相关部门和有关安全专家对安全整体规划及其配套文件的合理性和正确性进行论证和审定，经过批准后才能正式实施。

8.1.9.3 产品采购和使用

本项要求包括：

a）应确保网络安全产品采购和使用符合国家的有关规定；

b）应确保密码产品与服务的采购和使用符合国家密码管理主管部门的要求；

c）应预先对产品进行选型测试，确定产品的候选范围，并定期审

定和更新候选产品名单。

8.1.9.4 自行软件开发

本项要求包括：

a）应将开发环境与实际运行环境物理分开，测试数据和测试结果受到控制；

b）应制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则；

c）应制定代码编写安全规范，要求开发人员参照规范编写代码；

d）应具备软件设计的相关文档和使用指南，并对文档使用进行控制；

e）应保证在软件开发过程中对安全性进行测试，在软件安装前对可能存在的恶意代码进行检测；

f）应对程序资源库的修改、更新、发布进行授权和批准，并严格进行版本控制；

g）应保证开发人员为专职人员，开发人员的开发活动受到控制、监视和审查。

8.1.9.5 外包软件开发

本项要求包括：

a）应在软件交付前检测其中可能存在的恶意代码；

b）应保证开发单位提供软件设计文档和使用指南；

c）应保证开发单位提供软件源代码，并审查软件中可能存在的后门和隐蔽信道

8.1.9.6 工程实施

本项要求包括：

a）应指定或授权专门的部门或人员负责工程实施过程的管理；

b）应制定安全工程实施方案控制工程实施过程；

c）应通过第三方工程监理控制项目的实施过程。

8.1.9.7 测试验收

本项要求包括：

a）应制订测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告；

b）应进行上线前的安全性测试，并出具安全测试报告，安全测试报告应包含密码应用安全性测试相关内容。

8.1.9.8 系统交付

本项要求包括

a）应制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点；

b）应对负责运行维护的技术人员进行相应的技能培训；

c）应提供建设过程文档和运行维护文档。

8.1.9.9 等级测评

本项要求包括：

a）应定期进行等级测评，发现不符合相应等级保护标准要求的及时整改；

b）应在发生重大变更或级别发生变化时进行等级测评；

c）应确保测评机构的选择符合国家有关规定。

8.1.9.10 服务供应商选择

本项要求包括：

a）应确保服务供应商的选择符合国家的有关规定；

b）应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务；

c）应定期监督、评审和审核服务供应商提供的服务，并对其变更服务内容加以控制。

8.1.10 安全运维管理

8.1.10.1 环境管理

本项要求包括：

a)应指定专门的部门或人员负责机房安全,对机房出入进行管理,定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理

b）应建立机房安全管理制度，对有关物理访问、物品带进出和环境安全等方面的管理作出规定；

c）应不在重要区域接待来访人员，不随意放置含有敏感信息的纸档文件和移动介质等

8.1.10.2 资产管理

本项要求包括：

a)应编制并保存与保护对象相关的资产清单,包括资产责任部门、重要程度和所处位置等内容；

b）应根据资产的重要程度对资产进行标识管理，根据资产的价值

选择相应的管理措施；

c）应对信息分类与标识方法作出规定，并对信息的使用、传输和存储等进行规范化管理。

8.1.10.3 介质管理

本项要求包括：

a）应将介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点；

b）应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质的归档和查询等进行登记记录。

8.1.10.4 设备维护管理

本项要求包括：

a）应对各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理；

b）应建立配套设施、软硬件维护方面的管理制度，对其维护进行有效的管理，包括明确维护人员的责任、维修和服务的审批、维修过程的监督控制等；

c）信息处理设备应经过审批才能带离机房或办公地点，含有存储介质的设备带出工作环境时其中重要数据应加密；

d）含有存储介质的设备在报废或重用前，应进行完全清除或被安全覆盖，保证该设备上的敏感数据和授权软件无法被恢复重用。

8.1.10.5 漏洞和风险管理

本项要求包括：

a）应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补；

b）应定期开展安全测评，形成安全测评报告，采取措施应对发现的安全问题。

8.1.10.6 网络和系统安全管理

本项要求包括：

a）应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限；

b）应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制；

c）应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定；

d）应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等；

e）应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容；

f）应指定专门的部门或人员对日志、监测和报警数据等进行分析、统计，及时发现可疑行为；

g）应严格控制变更性运维，经过审批后才可改变连接、安装系统组件或调整配置参数，操作过程中应保留不可更改的审计日志，操作结束后应同步更新配置信息库；

h）应严格控制运维工具的使用，经过审批后才可接入进行操作，操作过程中应保留不可更改的审计日志，操作结束后应删除工具中的敏感数据；

i）应严格控制远程运维的开通，经过审批后才可开通远程运维接口或通道，操作过程中应保留不可更改的审计日志，操作结束后立即关闭接口或通道；

j）应保证所有与外部的连接均得到授权和批准，应定期检查违反规定无线上网及其他违反网络安全策略的行为。

8.1.10.7 恶意代码防范管理

本项要求包括：

a）应提高所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等；

b）应定期验证防范恶意代码攻击的技术措施的有效性

8.1.10.8 配置管理

本项要求包括：

a）应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等；

b）应将基本配置信息改变纳入变更范畴，实施对配置信息改变的控制，并及时更新基本配置信息库。

8.1.10.9 密码管理

本项要求包括：

a）应遵循密码相关国家标准和行业标准；

b）应使用国家密码管理主管部门认证核准的密码技术和产品。

8.1.10.10 变更管理

本项要求包括：

a）应明确变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施；

b)应建立变更的申报和审批控制程序,依据程序控制所有的变更,记录变更实施过程；

c）应建立中止变更并从失败变更中恢复的程序，明确过程控制方法和人员职责，必要时对恢复过程进行演练。

8.1.10.11 备份与恢复管理

本项要求包括：

a)应识别需要定期备份的重要业务信息、系统数据及软件系统等；

b）应规定备份信息的备份方式、备份频度、存储介质、保存期等；

c）应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序等

8.1.10.12 安全事件处置

本项要求包括：

a）应及时向安全管理部门报告所发现的安全弱点和可疑事件；

b）应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等；

c）应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训；

d）对造成系统中断和造成信息泄漏的重大安全事件应采用不同的处理程序和报告程序。

8.1.10.13 应急预案管理

本项要求包括：

a）应规定统一的应急预案框架，包括启动预案的条件、应急组织构成、应急资源保障、事后教育和培训等内容；

b）应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容；

c）应定期对系统相关的人员进行应急预案培训，并进行应急预案的演练；

d）应定期对原有的应急预案重新评估，修订完善。

8.1.10.14 外包运维管理

本项要求包括：

a）应确保外包运维服务商的选择符合国家的有关规定；

b）应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容；

c）应保证选择的外包运维服务商在技术和管理方面均应具有按照等级保护要求开展安全运维工作的能力，并将能力要求在签订的协议中明确；

d）应在与外包运维服务商签订的协议中明确所有相关的安全要

求，如可能涉及对敏感信息的访问、处理、存储要求，对 IT 基础设施中断服务的应急保障要求等。

8.2 云计算安全扩展要求

8.2.1 安全物理环境

8.2.1.1 基础设施位置

应保证云计算基础设施位于中国境内。

8.2.2 安全通信网络

8.2.2.1 网络架构

本项要求包括：

a）应保证云计算平台不承载高于其安全保护等级的业务应用系统；

b）应实现不同云服务客户虚拟网络之间的隔离；

c）应具有根据云服务客户业务需求提供通信传输、边界防护、入侵防范等安全机制的能力；

d）应具有根据云服务客户业务需求自主设置安全策略的能力，包括定义访问路径、选择安全组件、配置安全策略；

e）应提供开放接口或开放性安全服务，允许云服务客户接入第三方安全产品或在云计算平台选择第三方安全服务。

8.2.3 安全区域边界

8.2.3.1 访问控制

本项要求包括：

a)应在虚拟化网络边界部署访问控制机制,并设置访问控制规则;

b）应在不同等级的网络区域边界部署访问控制机制，设置访问控制规则。

8.2.3.2 入侵防范

本项要求包括：

a）应能检测到云服务客户发起的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等；

b）应能检测到对虚拟网络节点的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等；

c）应能检测到虚拟机与宿主机、虚拟机与虚拟机之间的异常流量；

d）应在检测到网络攻击行为、异常流量情况时进行告警。

8.2.3.3 安全审计

本项要求包括：

a）应对云服务商和云服务客户在远程管理时执行的特权命令进行审计，至少包括虚拟机删除、虚拟机重启；

b）应保证云服务商对云服务客户系统和数据的操作可被云服务客户审计。

8.2.4 安全计算环境

8.2.4.1 身份鉴别

当远程管理云计算平台中设备时，管理终端和云计算平台之间应建立双向身份验证机制。

8.2.4.2 访问控制

本项要求包括：

a）应保证当虚拟机迁移时，访问控制策略随其迁移；

b）应允许云服务客户设置不同虚拟机之间的访问控制策略。

8.2.4.3 入侵防范

本项要求包括：

a）应能检测虚拟机之间的资源隔离失效，并进行告警；

b)应能检测非授权新建虚拟机或者重新启用虚拟机,并进行告警；

c）应能够检测恶意代码感染及在虚拟机间蔓延的情况，并进行告警。

8.2.4.4 镜像和快照保护

本项要求包括：

a)应针对重要业务系统提供加固的操作系统镜像或操作系统安全加固服务；

b）应提供虚拟机镜像、快照完整性校验功能，防止虚拟机镜像被恶意篡改；

c）应采取密码技术或其他技术手段防止虚拟机镜像、快照中可能存在的敏感资源被非法访问。

8.2.4.5 数据完整性和保密性

本项要求包括

a）应确保云服务客户数据、用户个人信息等存储于中国境内，如需出境应遵循国家相关规定；

b）应确保只有在云服务客户授权下，云服务商或第三方才具有云服务客户数据的管理权限；

c）应使用校验码或密码技术确保虚拟机迁移过程中重要数据的完整性，并在检测到完整性受到破坏时采取必要的恢复措施；

d）应支持云服务客户部署密钥管理解决方案，保证云服务客户自行实现数据的加解密过程。

8.2.4.6 数据备份恢复

本项要求包括：

a）云服务客户应在本地保存其业务数据的备份；

b）应提供查询云服务客户数据及备份存储位置的能力；

c）云服务商的云存储服务应保证云服务客户数据存在若干个可用的副本，各副本之间的内容应保持一致；

d）应为云服务客户将业务系统及数据迁移到其他云计算平台和本地系统提供技术手段，并协助完成迁移过程。

8.2.4.7 剩余信息保护

本项要求包括：

a）应保证虚拟机所使用的内存和存储空间同收时得到完全清除；

b）云服务客户删除业务应用数据时，云计算平台应将云存储中所有副本删除。

8.2.5 安全管理中心

8.2.5.1 集中管控

本项要求包括：

a）应能对物理资源和虚拟资源按照策略做统一管理调度与分配；

b）应保证云计算平台管理流量与云服务客户业务流量分离；

c）应根据云服务商和云服务客户的职责划分，收集各自控制部分的审计数据并实现各自的集中审计；

d）应根据云服务商和云服务客户的职责划分，实现各自控制部分，包括虚拟化网络、虚拟机、虚拟化安全设备等的运行状况的集中监测。

8.2.6 安全建设管理

8.2.6.1 云服务商选择

本项要求包括：

a）应选择安全合规的云服务商，其所提供的云计算平台应为其所承载的业务应用系统提供相应等级的安全保护能力；

b）应在服务水平协议中规定云服务的各项服务内容和具体技术指标；

c）应在服务水平协议中规定云服务商的权限与责任，包括管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任等；

d）应在服务水平协议中规定服务合约到期时，完整提供云服务客户数据，并承诺相关数据在云计算平台上清除；

e）应与选定的云服务商签署保密协议，要求其不得泄露云服务客户数据

8.2.6.2 供应链管理

本项要求包括：

a）应确保供应商的选择符合国家有关规定；

b）应将供应链安全事件信息或安全威胁信息及时传达到云服务客户；

c）应将供应商的重要变更及时传达到云服务客户，并评估变更带来的安全风险，采取措施对风险进行控制。

8.2.7 安全运维管理

8.2.7.1 云计算环境管理

云计算平台的运维地点应位于中国境内，境外对境内云计算平台实施运维操作应遵循国家相关规定。

8.3 移动互联安全扩展要求

8.3.1 安全物理环境

8.3.1.1 无线接入点的物理位置

应为无线接入设备的安装选择合理位置，避免过度覆盖和电磁干扰。

8.3.2 安全区域边界

8.3.2.1 边界防护

应保证有线网络与无线网络边界之间的访问和数据流通过无线接入网关设备。

8.3.2.2 访问控制

无线接入设备应开启接入认证功能，并支持采用认证服务器认证或国家密码管理机构批准的密码模块进行认证

8.3.2.3 入侵防范

本项要求包括：

a）应能够检测到非授权无线接入设备和非授权移动终端的接入行为；

b）应能够检测到针对无线接入设备的网络扫描、DDos 攻击、密钥破解、中间人攻击和欺骗攻击等行为;

c）应能够检测到无线接入设备的 SSID 广播、WPS 等高风险功能的开启状态;

d）应禁用无线接入设备和无线接入网关存在风险的功能，如：SSID 广播、WEP 认证等;

e）应禁止多个 AP 使用同一个认证密钥；f）应能够阻断非授权无线接入设备或非授权移动终端。

8.3.3 安全计算环境

8.3.3.1 移动终端管控

本项要求包括：

a）应保证移动终端安装、注册并运行终端管理客户端软件;

b）移动终端应接受移动终端管理服务端的设备生命周期管理、设备远程控制，如：远程锁定、远程擦除等。

8.3.3.2 移动应用管控

本项要求包括：

a）应具有选择应用软件安装、运行的功能;

b）应只允许指定证书签名的应用软件安装和运行;

c）应具有软件白名单功能，应能根据白名单控制应用软件安装、运行。

8.3.4 安全建设管理

8.3.4.1 移动应用软件采购

本项要求包括：

a）应保证移动终端安装、运行的应用软件来自可靠分发渠道或使用可靠证书签名；

b）应保证移动终端安装、运行的应用软件由指定的开发者开发。

8.3.4.2 移动应用软件开发

本项要求包括

a）应对移动业务应用软件开发者进行资格审查；

b）应保证开发移动业务应用软件的签名证书合法性。

8.3.5 安全运维管理

8.3.5.1 配置管理

应建立合法无线接入设备和合法移动终端配置库，用于对非法无线接入设备和非法移动终端的识别。

8.4 物联网安全扩展要求

8.4.1 安全物理环境

8.4.1.1 感知节点设备物理防护

本项要求包括：

a)感知节点设备所处的物理环境应不对感知节点设备造成物理破坏，如挤压、强振动；

b)感知节点设备在工作状态所处物理环境应能正确反映环境状态（如温湿度传感器不能安装在阳光直射区域）；

c)感知节点设备在工作状态所处物理环境应不对感知节点设备的正常工作造成影响，如强干扰、阻挡屏蔽等；

d）关键感知节点设备应具有可供长时间工作的电力供应（关键网关节点设备应具有持久稳定的电力供应能力）。

8.4.2 安全区域边界

8.4.2.1 接入控制

应保证只有授权的感知节点可以接入。

8.4.2.2 入侵防范

本项要求包括：

a）应能够限制与感知节点通信的目标地址，以避免对陌生地址的攻击行为；

b）应能够限制与网关节点通信的目标地址，以避免对陌生地址的攻击行为。

8.4.3 安全计算环境

8.4.3.1 感知节点设备安全

本项要求包括：

a）应保证只有授权的用户可以对感知节点设备上的软件应用进行配置或变更；

b）应具有对其连接的网关节点设备（包括读卡器）进行身份标识和鉴别的能力；

c）应具有对其连接的其他感知节点设备（包括路由节点）进行身份标识和鉴别的能力。

8.4.3.2 网关节点设备安全

本项要求包括：

a）应具备对合法连接设备（包括终端节点、路由节点、数据处理中心）进行标识和鉴别的能力；

b）应具备过滤非法节点和伪造节点所发送的数据的能力；

c）授权用户应能够在设备使用过程中对关键密钥进行在线更新；

d)授权用户应能够在设备使用过程中对关键配置参数进行在线更新。

8.4.3.3 抗数据重放

本项要求包括

a）应能够鉴别数据的新鲜性，避免历史数据的重放攻击；

b）应能够鉴别历史数据的非法修改，避免数据的修改重放攻击。

8.4.3.4 数据融合处理

应对来自传感网的数据进行数据融合处理，使不同种类的数据可以在同一个平台被使用。

8.4.4 安全运维管理

8.4.4.1 感知节点管理

本项要求包括：

a)应指定人员定期巡视感知节点设备、网关节点设备的部署环境，对可能影响感知节点设备、网关节点设备正常工作的环境异常进行记录和维护；

b）应对感知节点设备、网关节点设备入库、存储、部署、携带、维修、丢失和报废等过程作出明确规定，并进行全程管理；

c)应加强对感知节点设备、网关节点设备部署环境的保密性管理，

包括负责检查和维护的人员调离工作岗位应立即交还相关检查工具和检查维护记录等。

8.5 工业控制系统安全扩展要求

8.5.1 安全物理环境

8.5.1.1 室外控制设备物理防护

本项要求包括：

a）室外控制设备应放置于采用铁板或其他防火材料制作的箱体或装置中并紧固；箱休或装置具有透风、散热、防盗、防雨和防火能力等；

b）室外控制设备放置应远离强电磁干扰、强热源等环境，如无法避免应及时做好应急处置及检修，保证设备正常运行。

8.5.2 安全通信网络

8.5.2.1 网络架构

本项要求包括：

a）工业控制系统与企业其他系统之间应划分为两个区域，区域间应采用单向的技术隔离手段；

b）工业控制系统内部应根据业务特点划分为不同的安全域，安全域之间应采用技术隔离手段；

c）涉及实时控制和数据传输的工业控制系统，应使用独立的网络设备组网，在物理层面上实现与其他数据网及外部公共信息网的安全隔离。

8.5.2.2 通信传输

在工业控制系统内使用广域网进行控制指令或相关数据交换的应采用加密认证技术手段实现身份认证、访问控制和数据加密传输。

8.5.3 安全区域边界

8.5.3.1 访问控制

本项要求包括：

a）应在工业控制系统与企业其他系统之间部署访问控制设备，配置访问控制策略，禁止任何穿越区域边界的 E-Mail，web，Telnet，Rlogin，FTP 等通用网络服务；

b）应在工业控制系统内安全域和安全域之间的边界防护机制失效时，及时进行报警。

8.5.3.2 拨号使用控制

本项要求包括：

a）工业控制系统确需使用拨号访问服务的，应限制具有拨号访问权限的用户数量，并采取用户身分鉴别和访问控制等措施；

b）拨号服务器和客户端均应使用经安全加固的操作系统，并采取数字证书认证、传输加密和访问控制等措施

8.5.3.3 无线使用控制

本项要求包括：

a）应对所有参与无线通信的用户（人员、软件进程或者设备）提供唯一性标识和鉴别；

b）应对所有参与无线通信的用户（人员、软件进程或者设备）进行授权以及执行使用进行限制；

c）应对无线通信采取传输加密的安全措施，实现传输报文的机密性保护；

d）对采用无线通信技术进行控制的工业控制系统，应能识别其物理环境中发射的未经授权的无线设备，报告未经授权试图接入或干扰控制系统的行为。

8.5.4 安全计算环境

8.5.4.1 控制设备安全

本项要求包括：

a）控制设备自身应实现相应级别安全通用要求提出的身份鉴别、访问控制和安全审计等安全要求，如受条件限制控制设备无法实现上述要求，应由其上位控制或管理设备实现同等功能或通过管理手段控制；

b）应在经过充分测试评估后，在不影响系统安全稳定运行的情况下对控制设备进行补丁更新、固件更新等工作；

c）应关闭或拆除控制设备的软盘驱动、光盘驱动、USB 接口、串行口或多余网口等，确需保留的应通过相关的技术措施实施严格的监控管理；

d）应使用专用设备和专用软件对控制设备进行更新；

e）应保证控制设备在上线前经过安全性检测，避免控制设备固件中存在恶意代码程序。

8.5.5 安全建设管理

8.5.5.1 产品采购和使用

工业控制系统重要设备应通过专业机构的安全性检测后方可采购使用。

8.5.5.2 外包软件开发

应在外包开发合同中规定针对开发单位、供应商的约束条款，包括设备及系统在生命周期内有关保密、禁止关键技术扩散和设备行业专用等方面的内容。