网络数据安全管理条例

（征求意见稿）

第一章 总则

第一条 为了规范网络数据处理活动，保障数据安全，保护个人、组织在网络空间的合法权益，维护国家安全、公共利益，根据《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等法律，制定本条例。

第二条 在中华人民共和国境内利用网络开展数据处理活动，以及网络数据安全的监督管理，适用本条例。

在中华人民共和国境外处理中华人民共和国境内个人和组织数据的活动，有下列情形之一的，适用本条例：

（一）以向境内提供产品或者服务为目的；

（二）分析、评估境内个人、组织的行为；

（三）涉及境内重要数据处理；

（四）法律、行政法规规定的其他情形。

自然人因个人或者家庭事务开展数据处理活动，不适用本条例。

第三条 国家统筹发展和安全，坚持促进数据开发利用与保障数据安全并重，加强数据安全防护能力建设，保障数据依法有序自由流动，促进数据依法合理有效利用。

第四条 国家支持数据开发利用与安全保护相关的技术、产品、服务创新和人才培养。

国家鼓励国家机关、行业组织、企业、教育和科研机构、有关专业机构等开展数据开发利用和安全保护合作，开展数据安全宣传教育和培训。

第五条 国家建立数据分类分级保护制度。按照数据对国家安全、公共利益或者个人、组织合法权益的影响和重要程度，将数据分为一般数据、重要数据、核心数据，不同级别的数据采取不同的保护措施。

国家对个人信息和重要数据进行重点保护，对核心数据实行严格保护。

各地区、各部门应当按照国家数据分类分级要求，对本地区、本部门以及相关行业、领域的数据进行分类分级管理。

第六条 数据处理者对所处理数据的安全负责，履行数据安全保护义务，接受政府和社会监督，承担社会责任。

数据处理者应当按照有关法律、行政法规的规定和国家标准的强制性要求，建立完善数据安全管理制度和技术保护机制。

第七条 国家推动公共数据开放、共享，促进数据开发利用，并依法对公共数据实施监督管理。

国家建立健全数据交易管理制度，明确数据交易机构设立、运行标准，规范数据流通交易行为，确保数据依法有序流通。

第二章 一般规定

第八条 任何个人和组织开展数据处理活动应当遵守法律、行政法规，尊重社会公德和伦理，不得从事以下活动：

（一）危害国家安全、荣誉和利益，泄露国家秘密和工作秘密；

（二）侵害他人名誉权、隐私权、著作权和其他合法权益等；

（三）通过窃取或者以其他非法方式获取数据；

（四）非法出售或者非法向他人提供数据；

（五）制作、发布、复制、传播违法信息；

（六）法律、行政法规禁止的其他行为。

任何个人和组织知道或者应当知道他人从事前款活动的，不得为其提供技术支持、工具、程序和广告推广、支付结算等服务。

第九条 数据处理者应当采取备份、加密、访问控制等必要措施，保障数据免遭泄露、窃取、篡改、毁损、丢失、非法使用，应对数据安全事件，防范针对和利用数据的违法犯罪活动，维护数据的完整性、保密性、可用性。

数据处理者应当按照网络安全等级保护的要求，加强数据处理系统、数据传输网络、数据存储环境等安全防护，处理重要数据的系统原则上应当满足三级以上网络安全等级保护和关键信息基础设施安全保护要求，处理核心数据的系统依照有关规定从严保护。

数据处理者应当使用密码对重要数据和核心数据进行保护。

第十条 数据处理者发现其使用或者提供的网络产品和服务存在安全缺陷、漏洞，或者威胁国家安全、危害公共利益等风险时，应当立即采取补救措施。

第十一条 数据处理者应当建立数据安全应急处置机制，发生数据安全事件时及时启动应急响应机制，采取措施防止危害扩大，消除安全隐患。安全事件对个人、组织造成危害的，数据处理者应当在三个工作日内将安全事件和风险情况、危害后果、已经采取的补救措施等以电话、短信、即时通信工具、电子邮件等方式通知利害关系人，无法通知的可采取公告方式告知，法律、行政法规规定可以不通知的从其规定。安全事件涉嫌犯罪的，数据处理者应当按规定向公安机关报案。

发生重要数据或者十万人以上个人信息泄露、毁损、丢失等数据安全事件时，数据处理者还应当履行以下义务：

（一）在发生安全事件的八小时内向设区的市级网信部门和有关主管部门报告事件基本信息，包括涉及的数据数量、类型、可能的影响、已经或拟采取的处置措施等；

（二）在事件处置完毕后五个工作日内向设区的市级网信部门和有关主管部门报告包括事件原因、危害后果、责任处理、改进措施等情况的调查评估报告。

第十二条 数据处理者向第三方提供个人信息，或者共享、交易、委托处理重要数据的，应当遵守以下规定：

（一）向个人告知提供个人信息的目的、类型、方式、范围、存储期限、存储地点，并取得个人单独同意，符合法律、行政法规规定的不需要取得个人同意的情形或者经过匿名化处理的除外；

（二）与数据接收方约定处理数据的目的、范围、处理方式，数据安全保护措施等，通过合同等形式明确双方的数据安全责任义务，并对数据接收方的数据处理活动进行监督；

（三）留存个人同意记录及提供个人信息的日志记录，共享、交易、委托处理重要数据的审批记录、日志记录至少五年。

数据接收方应当履行约定的义务，不得超出约定的目的、范围、处理方式处理个人信息和重要数据。

第十三条 数据处理者开展以下活动，应当按照国家有关规定，申报网络安全审查：

（一）汇聚掌握大量关系国家安全、经济发展、公共利益的数据资源的互联网平台运营者实施合并、重组、分立，影响或者可能影响国家安全的；

（二）处理一百万人以上个人信息的数据处理者赴国外上市的；

（三）数据处理者赴香港上市，影响或者可能影响国家安全的；

（四）其他影响或者可能影响国家安全的数据处理活动。

大型互联网平台运营者在境外设立总部或者运营中心、研发中心，应当向国家网信部门和主管部门报告。

第十四条 数据处理者发生合并、重组、分立等情况的，数据接收方应当继续履行数据安全保护义务，涉及重要数据和一百万人以上个人信息的，应当向设区的市级主管部门报告；数据处理者发生解散、被宣告破产等情况的，应当向设区的市级主管部门报告，按照相关要求移交或删除数据，主管部门不明确的，应当向设区的市级网信部门报告。

第十五条 数据处理者从其他途径获取的数据，应当按照本条例的规定履行数据安全保护义务。

第十六条 国家机关应当依照法律、行政法规的规定和国家标准的强制性要求，建立健全数据安全管理制度，落实数据安全保护责任，保障政务数据安全。

第十七条 数据处理者在采用自动化工具访问、收集数据时，应当评估对网络服务的性能、功能带来的影响，不得干扰网络服务的正常功能。

自动化工具访问、收集数据违反法律、行政法规或者行业自律公约、影响网络服务正常功能，或者侵犯他人知识产权等合法权益的，数据处理者应当停止访问、收集数据行为并采取相应补救措施。

第十八条 数据处理者应当建立便捷的数据安全投诉举报渠道，及时受理、处置数据安全投诉举报。

数据处理者应当公布接受投诉、举报的联系方式、责任人信息，每年公开披露受理和收到的个人信息安全投诉数量、投诉处理情况、平均处理时间情况，接受社会监督。

第三章 个人信息保护

第十九条 数据处理者处理个人信息，应当具有明确、合理的目的，遵循合法、正当、必要的原则。基于个人同意处理个人信息的，应当满足以下要求：

（一）处理的个人信息是提供服务所必需的，或者是履行法律、行政法规规定的义务所必需的；

（二）限于实现处理目的最短周期、最低频次，采取对个人权益影响最小的方式；

（三）不得因个人拒绝提供服务必需的个人信息以外的信息，拒绝提供服务或者干扰个人正常使用服务。

第二十条 数据处理者处理个人信息，应当制定个人信息处理规则并严格遵守。个人信息处理规则应当集中公开展示、易于访问并置于醒目位置，内容明确具体、简明通俗，系统全面地向个人说明个人信息处理情况。

个人信息处理规则应当包括但不限于以下内容：

（一）依据产品或者服务的功能明确所需的个人信息，以清单形式列明每项功能处理个人信息的目的、用途、方式、种类、频次或者时机、保存地点等，以及拒绝处理个人信息对个人的影响；

（二）个人信息存储期限或者个人信息存储期限的确定方法、到期后的处理方式；

（三）个人查阅、复制、更正、删除、限制处理、转移个人信息，以及注销账号、撤回处理个人信息同意的途径和方法；

（四）以集中展示等便利用户访问的方式说明产品服务中嵌入的所有收集个人信息的第三方代码、插件的名称，以及每个第三方代码、插件收集个人信息的目的、方式、种类、频次或者时机及其个人信息处理规则；

（五）向第三方提供个人信息情形及其目的、方式、种类，数据接收方相关信息等；

（六）个人信息安全风险及保护措施；

（七）个人信息安全问题的投诉、举报渠道及解决途径，个人信息保护负责人联系方式。

第二十一条 处理个人信息应当取得个人同意的，数据处理者应当遵守以下规定：

（一）按照服务类型分别向个人申请处理个人信息的同意，不得使用概括性条款取得同意；

（二）处理个人生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等敏感个人信息应当取得个人单独同意；

（三）处理不满十四周岁未成年人的个人信息，应当取得其监护人同意；

（四）不得以改善服务质量、提升用户体验、研发新产品等为由，强迫个人同意处理其个人信息；

（五）不得通过误导、欺诈、胁迫等方式获得个人的同意；

（六）不得通过捆绑不同类型服务、批量申请同意等方式诱导、强迫个人进行批量个人信息同意；

（七）不得超出个人授权同意的范围处理个人信息；

（八）不得在个人明确表示不同意后，频繁征求同意、干扰正常使用服务。

个人信息的处理目的、处理方式和处理的个人信息种类发生变更的，数据处理者应当重新取得个人同意，并同步修改个人信息处理规则。

对个人同意行为有效性存在争议的，数据处理者负有举证责任。

第二十二条 有下列情况之一的，数据处理者应当在十五个工作日内删除个人信息或者进行匿名化处理：

（一）已实现个人信息处理目的或者实现处理目的不再必要；

（二）达到与用户约定或者个人信息处理规则明确的存储期限；

（三）终止服务或者个人注销账号；

（四）因使用自动化采集技术等，无法避免采集到的非必要个人信息或者未经个人同意的个人信息。

删除个人信息从技术上难以实现，或者因业务复杂等原因，在十五个工作日内删除个人信息确有困难的，数据处理者不得开展除存储和采取必要的安全保护措施之外的处理，并应当向个人作出合理解释。

法律、行政法规另有规定的从其规定。

第二十三条 个人提出查阅、复制、更正、补充、限制处理、删除其个人信息的合理请求的，数据处理者应当履行以下义务：

（一）提供便捷的支持个人结构化查询本人被收集的个人信息类型、数量等的方法和途径，不得以时间、位置等因素对个人的合理请求进行限制；

（二）提供便捷的支持个人复制、更正、补充、限制处理、删除其个人信息、撤回授权同意以及注销账号的功能，且不得设置不合理条件；

（三）收到个人复制、更正、补充、限制处理、删除本人个人信息、撤回授权同意或者注销账号申请的，应当在十五个工作日内处理并反馈。

法律、行政法规另有规定的从其规定。

第二十四条 符合下列条件的个人信息转移请求，数据处理者应当为个人指定的其他数据处理者访问、获取其个人信息提供转移服务：

（一）请求转移的个人信息是基于同意或者订立、履行合同所必需而收集的个人信息；

（二）请求转移的个人信息是本人信息或者请求人合法获得且不违背他人意愿的他人信息；

（三）能够验证请求人的合法身份。

数据处理者发现接收个人信息的其他数据处理者有非法处理个人信息风险的，应当对个人信息转移请求做合理的风险提示。

请求转移个人信息次数明显超出合理范围的，数据处理者可以收取合理费用。

第二十五条 数据处理者利用生物特征进行个人身份认证的，应当对必要性、安全性进行风险评估，不得将人脸、步态、指纹、虹膜、声纹等生物特征作为唯一的个人身份认证方式，以强制个人同意收集其个人生物特征信息。

法律、行政法规另有规定的从其规定。

第二十六条 数据处理者处理一百万人以上个人信息的，还应当遵守本条例第四章对重要数据的处理者作出的规定。

第四章 重要数据安全

第二十七条 各地区、各部门按照国家有关要求和标准，组织本地区、本部门以及相关行业、领域的数据处理者识别重要数据和核心数据，组织制定本地区、本部门以及相关行业、领域重要数据和核心数据目录，并报国家网信部门。

第二十八条 重要数据的处理者，应当明确数据安全负责人，成立数据安全管理机构。数据安全管理机构在数据安全负责人的领导下，履行以下职责：

（一）研究提出数据安全相关重大决策建议；

（二）制定实施数据安全保护计划和数据安全事件应急预案；

（三）开展数据安全风险监测，及时处置数据安全风险和事件；

（四）定期组织开展数据安全宣传教育培训、风险评估、应急演练等活动；

（五）受理、处置数据安全投诉、举报；

（六）按照要求及时向网信部门和主管、监管部门报告数据安全情况。

数据安全负责人应当具备数据安全专业知识和相关管理工作经历，由数据处理者决策层成员承担，有权直接向网信部门和主管、监管部门反映数据安全情况。

第二十九条 重要数据的处理者，应当在识别其重要数据后的十五个工作日内向设区的市级网信部门备案，备案内容包括：

（一）数据处理者基本信息，数据安全管理机构信息、数据安全负责人姓名和联系方式等；

（二）处理数据的目的、规模、方式、范围、类型、存储期限、存储地点等，不包括数据内容本身；

（三）国家网信部门和主管、监管部门规定的其他备案内容。

处理数据的目的、范围、类型及数据安全防护措施等有重大变化的，应当重新备案。

依据部门职责分工，网信部门与有关部门共享备案信息。

第三十条 重要数据的处理者，应当制定数据安全培训计划，每年组织开展全员数据安全教育培训，数据安全相关的技术和管理人员每年教育培训时间不得少于二十小时。

第三十一条 重要数据的处理者，应当优先采购安全可信的网络产品和服务。

第三十二条 处理重要数据或者赴境外上市的数据处理者，应当自行或者委托数据安全服务机构每年开展一次数据安全评估，并在每年 1 月 31 日前将上一年度数据安全评估报告报设区的市级网信部门，年度数据安全评估报告的内容包括：

（一）处理重要数据的情况；

（二）发现的数据安全风险及处置措施；

（三）数据安全管理制度，数据备份、加密、访问控制等安全防护措施，以及管理制度实施情况和防护措施的有效性；

（四）落实国家数据安全法律、行政法规和标准情况；

（五）发生的数据安全事件及其处置情况；

（六）共享、交易、委托处理、向境外提供重要数据的安全评估情况；

（七）数据安全相关的投诉及处理情况；

（八）国家网信部门和主管、监管部门明确的其他数据安全情况。

数据处理者应当保留风险评估报告至少三年。

依据部门职责分工，网信部门与有关部门共享报告信息。

数据处理者开展共享、交易、委托处理、向境外提供重要数据的安全评估，应当重点评估以下内容：

（一）共享、交易、委托处理、向境外提供数据，以及数据接收方处理数据的目的、方式、范围等是否合法、正当、必要；

（二）共享、交易、委托处理、向境外提供数据被泄露、毁损、篡改、滥用的风险，以及对国家安全、经济发展、公共利益带来的风险；

（三）数据接收方的诚信状况、守法情况、境外政府机构合作关系、是否被中国政府制裁等背景情况，承诺承担的责任以及履行责任的能力等是否能够有效保障数据安全；

（四）与数据接收方订立的相关合同中关于数据安全的要求能否有效约束数据接收方履行数据安全保护义务；

（五）在数据处理过程中的管理和技术措施等是否能够防范数据泄露、毁损等风险。

评估认为可能危害国家安全、经济发展和公共利益，数据处理者不得共享、交易、委托处理、向境外提供数据。

第三十三条 数据处理者共享、交易、委托处理重要数据的，应当征得设区的市级及以上主管部门同意，主管部门不明确的，应当征得设区的市级及以上网信部门同意。

第三十四条 国家机关和关键信息基础设施运营者采购的云计算服务，应当通过国家网信部门会同国务院有关部门组织的安全评估。

第五章 数据跨境安全管理

第三十五条 数据处理者因业务等需要，确需向中华人民共和国境外提供数据的，应当具备下列条件之一：

（一）通过国家网信部门组织的数据出境安全评估；

（二）数据处理者和数据接收方均通过国家网信部门认定的专业机构进行的个人信息保护认证；

（三）按照国家网信部门制定的关于标准合同的规定与境外数据接收方订立合同，约定双方权利和义务；

（四）法律、行政法规或者国家网信部门规定的其他条件。

数据处理者为订立、履行个人作为一方当事人的合同所必需向境外提供当事人个人信息的，或者为了保护个人生命健康和财产安全而必须向境外提供个人信息的除外。

第三十六条 数据处理者向中华人民共和国境外提供个人信息的，应当向个人告知境外数据接收方的名称、联系方式、处理目的、处理方式、个人信息的种类以及个人向境外数据接收方行使个人信息权利的方式等事项，并取得个人的单独同意。

收集个人信息时已单独就个人信息出境取得个人同意，且按照取得同意的事项出境的，无需再次取得个人单独同意。

第三十七条 数据处理者向境外提供在中华人民共和国境内收集和产生的数据，属于以下情形的，应当通过国家网信部门组织的数据出境安全评估：

（一）出境数据中包含重要数据；

（二）关键信息基础设施运营者和处理一百万人以上个人信息的数据处理者向境外提供个人信息；

（三）国家网信部门规定的其它情形。

法律、行政法规和国家网信部门规定可以不进行安全评估的，从其规定。

第三十八条 中华人民共和国缔结或者参加的国际条约、协定对向中华人民共和国境外提供个人信息的条件等有规定的，可以按照其规定执行。

第三十九条 数据处理者向境外提供数据应当履行以下义务：

（一）不得超出报送网信部门的个人信息保护影响评估报告中明确的目的、范围、方式和数据类型、规模等向境外提供个人信息；

（二）不得超出网信部门安全评估时明确的出境目的、范围、方式和数据类型、规模等向境外提供个人信息和重要数据；

（三）采取合同等有效措施监督数据接收方按照双方约定的目的、范围、方式使用数据，履行数据安全保护义务，保证数据安全；

（四）接受和处理数据出境所涉及的用户投诉；

（五）数据出境对个人、组织合法权益或者公共利益造成损害的，数据处理者应当依法承担责任；

（六）存留相关日志记录和数据出境审批记录三年以上；

（七）国家网信部门会同国务院有关部门核验向境外提供个人信息和重要数据的类型、范围时，数据处理者应当以明文、可读方式予以展示；

（八）国家网信部门认定不得出境的，数据处理者应当停止数据出境，并采取有效措施对已出境数据的安全予以补救；

（九）个人信息出境后确需再转移的，应当事先与个人约定再转移的条件，并明确数据接收方履行的安全保护义务。

非经中华人民共和国主管机关批准，境内的个人、组织不得向外国司法或者执法机构提供存储于中华人民共和国境内的数据。

第四十条 向境外提供个人信息和重要数据的数据处理者，应当在每年 1 月 31 日前编制数据出境安全报告，向设区的市级网信部门报告上一年度以下数据出境情况：

（一）全部数据接收方名称、联系方式；

（二）出境数据的类型、数量及目的；

（三）数据在境外的存放地点、存储期限、使用范围和方式；

（四）涉及向境外提供数据的用户投诉及处理情况；

（五）发生的数据安全事件及其处置情况；

（六）数据出境后再转移的情况；

（七）国家网信部门明确向境外提供数据需要报告的其他事项。

第四十一条 国家建立数据跨境安全网关，对来源于中华人民共和国境外、法律和行政法规禁止发布或者传输的信息予以阻断传播。

任何个人和组织不得提供用于穿透、绕过数据跨境安全网关的程序、工具、线路等，不得为穿透、绕过数据跨境安全网关提供互联网接入、服务器托管、技术支持、传播推广、支付结算、应用下载等服务。

境内用户访问境内网络的，其流量不得被路由至境外。

第四十二条 数据处理者从事跨境数据活动应当按照国家数据跨境安全监管要求，建立健全相关技术和管理措施。

第六章 互联网平台运营者义务

第四十三条 互联网平台运营者应当建立与数据相关的平台规则、隐私政策和算法策略披露制度，及时披露制定程序、裁决程序，保障平台规则、隐私政策、算法公平公正。

平台规则、隐私政策制定或者对用户权益有重大影响的修订，互联网平台运营者应当在其官方网站、个人信息保护相关行业协会互联网平台面向社会公开征求意见，征求意见时长

不得少于三十个工作日，确保用户能够便捷充分表达意见。互联网平台运营者应当充分采纳公众意见，修改完善平台规则、隐私政策，并以易于用户访问的方式公布意见采纳情况，说明未采纳的理由，接受社会监督。

日活用户超过一亿的大型互联网平台运营者平台规则、隐私政策制定或者对用户权益有重大影响的修订的，应当经国家网信部门认定的第三方机构评估，并报省级及以上网信部门和电信主管部门同意。

第四十四条 互联网平台运营者应当对接入其平台的第三方产品和服务承担数据安全管理责任，通过合同等形式明确第三方的数据安全责任义务，并督促第三方加强数据安全管理，采取必要的数据安全保护措施。

第三方产品和服务对用户造成损害的，用户可以要求互联网平台运营者先行赔偿。

移动通信终端预装第三方产品适用本条前两款规定。

第四十五条 国家鼓励提供即时通信服务的互联网平台运营者从功能设计上为用户提供个人通信和非个人通信选择。个人通信的信息按照个人信息保护要求严格保护，非个人通信的信息按照公共信息有关规定进行管理。

第四十六条 互联网平台运营者不得利用数据以及平台规则等从事以下活动：

（一）利用平台收集掌握的用户数据，无正当理由对交易条件相同的用户实施产品和服务差异化定价等损害用户合法利益的行为；

（二）利用平台收集掌握的经营者数据，在产品推广中实行最低价销售等损害公平竞争的行为；

（三）利用数据误导、欺诈、胁迫用户，损害用户对其数据被处理的决定权，违背用户意愿处理用户数据；

（四）在平台规则、算法、技术、流量分配等方面设置不合理的限制和障碍，限制平台上的中小企业公平获取平台产生的行业、市场数据等，阻碍市场创新。

第四十七条 提供应用程序分发服务的互联网平台运营者，应当按照有关法律、行政法规和国家网信部门的规定，建立、披露应用程序审核规则，并对应用程序进行安全审核。对不符合法律、行政法规的规定和国家标准的强制性要求的应用程序，应当采取拒绝上架、督促整改、下架处置等措施。

第四十八条 互联网平台运营者面向公众提供即时通信服务的，应当按照国务院电信主管部门的规定，为其他互联网平台运营者的即时通信服务提供数据接口，支持不同即时通信服务之间用户数据互通，无正当理由不得限制用户访问其他互联网平台以及向其他互联网平台传输文件。

第四十九条 互联网平台运营者利用个人信息和个性化推送算法向用户提供信息的，应当对推送信息的真实性、准确性以及来源合法性负责，并符合以下要求：

（一）收集个人信息用于个性化推荐时，应当取得个人单独同意；

（二）设置易于理解、便于访问和操作的一键关闭个性化推荐选项，允许用户拒绝接受定向推送信息，允许用户重置、修改、调整针对其个人特征的定向推送参数；

（三）允许个人删除定向推送信息服务收集产生的个人信息，法律、行政法规另有规定或者与用户另有约定的除外。

第五十条 国家建设网络身份认证公共服务基础设施，按照政府引导、网民自愿原则，提供个人身份认证公共服务。

互联网平台运营者应当支持并优先使用国家网络身份认证公共服务基础设施提供的个人身份认证服务。

第五十一条 互联网平台运营者在为国家机关提供服务，参与公共基础设施、公共服务系统建设运维管理，利用公共资源提供服务过程中收集、产生的数据不得用于其他用途。

第五十二条 国务院有关部门履行法定职责需要调取或者访问互联网平台运营者掌握的公共数据、公共信息，应当明确调取或者访问的范围、类型、用途、依据，严格限定在履行法定职责范围内，不得将调取或者访问的公共数据、公共信息用于履行法定职责之外的目的。

互联网平台运营者应当对有关部门调取或者访问公共数据、公共信息予以配合。

第五十三条 大型互联网平台运营者应当通过委托第三方审计方式，每年对平台数据安全情况、平台规则和自身承诺的执行情况、个人信息保护情况、数据开发利用情况等进行年度审计，并披露审计结果。

第五十四条 互联网平台运营者利用人工智能、虚拟现实、深度合成等新技术开展数据处理活动的，应当按照国家有关规定进行安全评估。

第七章 监督管理

第五十五条 国家网信部门负责统筹协调数据安全和相关监督管理工作。

公安机关、国家安全机关等在各自职责范围内承担数据安全监管职责。

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

主管部门应当明确本行业、本领域数据安全保护工作机构和人员，编制并组织实施本行业、本领域的数据安全规划和数据安全事件应急预案。

主管部门应当定期组织开展本行业、本领域的数据安全风险评估，对数据处理者履行数据安全保护义务情况进行监督检查，指导督促数据处理者及时对存在的风险隐患进行整改。

第五十六条 国家建立健全数据安全应急处置机制，完善网络安全事件应急预案和网络安全信息共享平台，将数据安全事件纳入国家网络安全事件应急响应机制，加强数据安全信息共享、数据安全风险和威胁监测预警以及数据安全事件应急处置工作。

第五十七条 有关主管、监管部门可以采取以下措施对数据安全进行监督检查：

（一）要求数据处理者相关人员就监督检查事项作出说明；

（二）查阅、调取与数据安全有关的文档、记录；

（三）按照规定程序，利用检测工具或者委托专业机构对数据安全措施运行情况进行技术检测；

（四）核验数据出境类型、范围等；

（五）法律、行政法规、规章规定的其他必要方式。

有关主管、监管部门开展数据安全监督检查，应当客观公正，不得向被检查单位收取费用。在数据安全监督检查中获取的信息只能用于维护数据安全的需要，不得用于其他用途。

数据处理者应当对有关主管、监管部门的数据安全监督检查予以配合，包括对组织运作、技术系统、算法原理、数据处理程序等进行解释说明，开放安全相关数据访问、提供必要技术支持等。

第五十八条 国家建立数据安全审计制度。数据处理者应当委托数据安全审计专业机构定期对其处理个人信息遵守法律、行政法规的情况进行合规审计。

主管、监管部门组织开展对重要数据处理活动的审计，重点审计数据处理者履行法律、行政法规规定的义务等情况。

第五十九条 国家支持相关行业组织按照章程，制定数据安全行为规范，加强行业自律，指导会员加强数据安全保护，提高数据安全保护水平，促进行业健康发展。

国家支持成立个人信息保护行业组织，开展以下活动：

（一）接受个人信息保护投诉举报并进行调查、调解；

（二）向个人提供信息和咨询服务，支持个人依法对损害个人信息权益的行为提起诉讼；

（三）曝光损害个人信息权益的行为，对个人信息保护开展社会监督；

（四）向有关部门反映个人信息保护情况、提供咨询、建议；

（五）违法处理个人信息、侵害众多个人的权益的行为，依法向人民法院提起诉讼。

第八章 法律责任

第六十条 数据处理者不履行第九条、第十条、第十一条、第十二条、第十三条、第十四条、第十五条、第十八条的规定，由有关主管部门责令改正，给予警告，可以并处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员可以处一万元以上十万元以下罚款；拒不改正或者导致危害数据安全等严重后果的，处五十万元以上二百万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处五万元以上二十万元以下罚款。

第六十一条 数据处理者不履行第十九条、第二十条、第二十一条、第二十二条、第二十三条、第二十四条、第二十五条规定的数据安全保护义务的，由有关部门责令改正，给予警告，没收违法所得，对违法处理个人信息的应用程序，责令暂停或者终止提供服务；拒不改正的，并处一百万元以下罚款；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

有前款规定的违法行为，情节严重的，由有关部门责令改正，没收违法所得，并处五千万元以下或者上一年度营业额百分之五以下罚款，并可以责令暂停相关业务或者停业整顿、通报有关主管部门吊销相关业务许可证或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款，并可以决定禁止其在一定期限内担任相关企业的董事、监事、高级管理人员和个人信息保护负责人。

第六十二条 数据处理者不履行第二十八条、第二十九条、第三十条、第三十一条、第三十二条、第三十三条规定的数据安全保护义务的，由有关部门责令改正，给予警告，对违法处理重要数据的系统及应用，责令暂停或者终止提供服务；拒不改正的，并处二百万元以下罚款，对直接负责的主管人员和其他直接责任人员处五万元以上二十万元以下罚款。

有前款规定的违法行为，情节严重的，由有关部门责令改正，没收违法所得，并处二百万元以上五百万元以下罚款，并可以责令暂停相关业务或者停业整顿、通报有关主管部门吊销相关业务许可证或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处二十万元以上一百万元以下罚款。

第六十三条 关键信息基础设施运营者违反第三十四条的规定，由有关部门责令改正，依照有关法律、行政法规的规定予以处罚。

第六十四条 数据处理者违反第三十五条、第三十六条、第三十七条、第三十九条第一款、第四十条、第四十二条的规定，由有关部门责令改正，给予警告，暂停数据出境，可以并处十万元以上一百万元以下罚款，对直接负责的主管人员和其他直接责任人员可以处一万元以上十万元以下罚款；情节严重的，处一百万元以上一千万元以下罚款，并可以责令暂停

相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款。

第六十五条 违反本条例第三十九条第二款的规定，未经主管机关批准向外国司法或者执法机构提供数据的，由有关主管部门给予警告，可以并处十万元以上一百万元以下罚款，对直接负责的主管人员和其他直接责任人员可以处一万元以上十万元以下罚款；造成严重后果的，处一百万元以上五百万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处五万元以上五十万元以下罚款。

第六十六条 个人和组织违反第四十一条的规定，由有关主管部门责令改正，给予警告、没收违法所得；拒不改正的，处违法所得一倍以上十倍以下的罚款，没有违法所得的，对直接负责的主管人员和其他直接负责人员，处五万元以上五十万元以下罚款；情节严重的，由有关主管部门依照相关法律、行政法规的规定，责令其暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照；构成犯罪的，依照相关法律、行政法规的规定处罚。

第六十七条 互联网平台运营者违反第四十三条、第四十四条、第四十五条、第四十七条、第五十三条的规定，由有关部门责令改正，予以警告；拒不改正，处五十万元以上五百万元以下罚款，对直接负责的主管人员和其他直接负责人员，处五万元以上五十万元以下罚款；情节严重的，可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照。

第六十八条 互联网平台运营者违反第四十六条、第四十八条、第五十一条的规定，由有关主管部门责令改正，给予警告；拒不改正的，处上一年度销售额百分之一以上百分之五以下的罚款；情节严重的，由有关主管部门依照相关法律、行政法规的规定，责令其暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照；构成犯罪的，依照相关法律、行政法规的规定处罚。

第六十九条 互联网平台运营者违反第四十九条、第五十四条的规定，由有关主管部门责令改正，予以警告；拒不改正，处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款；情节严重的，可由有关主管部门责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照。

第七十条 数据处理者违反本条例规定，给他人造成损害的，依法承担民事责任；构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

第七十一条 国家机关不履行本法规定的数据安全保护义务的，由其上级机关或者履行数据安全管理职责的部门责令改正；对直接负责的主管人员和其他直接责任人员依法给予处分。

第七十二条 在中华人民共和国境外开展数据处理活动，损害中华人民共和国国家安全、公共利益或者公民、组织合法权益的，依法追究法律责任。

第九章 附则

第七十三条 本条例下列用语的含义：

（一）网络数据（简称数据）是指任何以电子方式对信息的记录。

（二）数据处理活动是指数据收集、存储、使用、加工、传输、提供、公开、删除等活动。

（三）重要数据是指一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能危害国家安全、公共利益的数据。包括以下数据：

1.未公开的政务数据、工作秘密、情报数据和执法司法数据；

2.出口管制数据，出口管制物项涉及的核心技术、设计方案、生产工艺等相关的数据，密码、生物、电子信息、人工智能等领域对国家安全、经济竞争实力有直接影响的科学技术成果数据；

3.国家法律、行政法规、部门规章明确规定需要保护或者控制传播的国家经济运行数据、重要行业业务数据、统计数据等；

4.工业、电信、能源、交通、水利、金融、国防科技工业、海关、税务等重点行业和领域安全生产、运行的数据，关键系统组件、设备供应链数据；

5.达到国家有关部门规定的规模或者精度的基因、地理、矿产、气象等人口与健康、自然资源与环境国家基础数据；

6.国家基础设施、关键信息基础设施建设运行及其安全数据，国防设施、军事管理区、国防科研生产单位等重要敏感区域的地理位置、安保情况等数据；

7.其他可能影响国家政治、国土、军事、经济、文化、社会、科技、生态、资源、核设施、海外利益、生物、太空、极地、深海等安全的数据。

（四）核心数据是指关系国家安全、国民经济命脉、重要民生和重大公共利益等的数据。

（五）数据处理者是指在数据处理活动中自主决定处理目的和处理方式的个人和组织。

（六）公共数据是指国家机关和法律、行政法规授权的具有管理公共事务职能的组织履行公共管理职责或者提供公共服务过程中收集、产生的各类数据，以及其他组织在提供公共服务中收集、产生的涉及公共利益的各类数据。

（七）委托处理是指数据处理者委托第三方按照约定的目的和方式开展的数据处理活动。

（八）单独同意是指数据处理者在开展具体数据处理活动时，对每项个人信息取得个人同意，不包括一次性针对多项个人信息、多种处理活动的同意。

（九）互联网平台运营者是指为用户提供信息发布、社交、交易、支付、视听等互联网平台服务的数据处理者。

（十）大型互联网平台运营者是指用户超过五千万、处理大量个人信息和重要数据、具有强大社会动员能力和市场支配地位的互联网平台运营者。

（十一）数据跨境安全网关是指阻断访问境外反动网站和有害信息、防止来自境外的网络攻击、管控跨境网络数据传输、防范侦查打击跨境网络犯罪的重要安全基础设施。

（十二）公共信息是指数据处理者在提供公共服务过程中收集、产生的具有公共传播特性的信息。包括公开发布信息、可转发信息、无明确接收人信息等。

第七十四条 涉及国家秘密信息、核心数据、密码使用的数据处理活动，按照国家有关规定执行。

第七十五条 本条例自 年 月 日起施行。