

附件：《网络数据安全条例》对比表

《网络数据安全条例（征求意见稿）》	《网络数据安全条例》	主要变化
第一章 总则	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。	第一条 为了规范网络数据处理活动，保障 网络 数据安全， 促进网络数据依法合理有效利用 ，保护个人、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。	调整+新增
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。—	第二条 在中华人民共和国境内开展网络数据处理活动及其安全监督管理，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 自然人 个人信息的活动，符合《中华人民共和国个人信息保护法》第三条第二款规定情形的，也适用本条例。 在中华人民共和国境外开展网络数据处理活动，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。	条文内容调整 +条文顺序调整

《网络数据安全条例（征求意见稿）》	《网络数据安全条例》	主要变化
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。	第三条 网络数据安全管理工作坚持中国共产党的领导，贯彻总体国家安全观，统筹促进网络数据开发利用与保障网络数据安全。	调整
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。	第四条 国家鼓励网络数据在各行业、各领域的创新应用，加强网络数据安全防护能力建设，支持网络数据相关技术、产品、服务创新，开展网络安全宣传教育	调整
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。	第五条 国家根据网络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，对网络数据实行分类分级保护。	重大调整

《网络数据安全条例（征求意见稿）》	《网络数据安全条例》	主要变化
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。	/	删除
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。	/	删除
/	第六条 国家积极参与网络数据安全相关国际规则和标准的制定，促进国际交流与合作。	新增
（请见第五十九条）	第七条 国家支持相关行业组织按照章程，制定网络数据	调整+删除+条

《网络数据安全条例（征求意见稿）》	《网络数据安全条例》	主要变化
	安全行为规范，加强行业自律，指导会员加强网络数据安全保护，提高网络数据安全保护水平，促进行业健康发展。	文顺序变更
第二章 一般规定	第二章 一般规定	
<p>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：—</p> <p>—（一）危害国家安全、荣誉和利益，泄露国家秘密和工作秘密；—</p> <p>—（二）侵害他人名誉权、隐私权、著作权和其他合法权益等；—</p> <p>—（三）通过窃取或者以其他非法方式获取数据；—</p> <p>—（四）非法出售或者非法向他人提供数据；—</p> <p>—（五）制作、发布、复制、传播违法信息；—</p> <p>—（六）法律、行政法规禁止的其他行为。</p> <p>任何个人和组织知道或者应当知道他人从事前款活动</p>	<p>第八条 任何个人、组织不得利用网络数据从事非法活动，不得从事窃取或者以其他非法方式获取网络数据、非法出售或者非法向他人提供网络数据等非法网络数据处理活动。</p> <p>任何个人、组织不得提供专门用于从事前款非法活动的程序、工具；明知他人从事前款非法活动的，不得为其提供互联网接入、服务器托管、网络存储、通讯传输等技术支持，或者提供广告推广、支付结算等帮助。</p>	调整+删除

《网络数据安全条例（征求意见稿）》	《网络数据安全条例》	主要变化
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 。		
<p>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。</p> <p>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。</p> <p>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。</p>	<p>第九条 网络数据处理者应当依照法律、行政法规的规定和国家标准的强制性要求，在网络安全等级保护的基础上，加强网络数据安全防护，建立健全网络数据安全管理制度，采取加密、备份、访问控制、安全认证等技术措施和其他必要措施，保护网络数据免遭篡改、破坏、泄露或者非法获取、非法利用，处置网络数据安全事件，防范针对和利用网络数据实施的违法犯罪活动，并对所处理网络数据的安全承担主体责任。</p>	调整+删除
<p>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</p>	<p>第十条 网络数据处理者提供的网络产品、服务应当符合相关国家标准的强制性要求；发现网络产品、服务存在</p>	调整+新增

《网络数据安全条例（征求意见稿）》	《网络数据安全条例》	主要变化
利益等风险时，应当立即采取补救措施。	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；涉及危害国家安全、公共利益的，网络数据处理者还应当在 24 小时内向有关主管部门报告。	
<p>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。</p> <p>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：</p>	<p>第十一条 网络数据处理者应当建立健全网络数据安全事件应急预案，发生网络数据安全事件时，应当立即启动预案，采取措施防止危害扩大，消除安全隐患，并按照规定向有关主管部门报告。</p> <p>网络数据安全事件对个人、组织合法权益造成危害的，网络数据处理者应当及时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、电子邮件或者公告等方式通知利害关系人；法律、行政法规规定可以不通知的，从其规定。网络数据处理者在处置网络数据安全事件过程中发现涉嫌违法犯罪线索的，应当按照规定向公安机关、国家安全机关报案，并配合开展侦查、调查和处置工作。</p>	调整+删除

《网络数据安全条例（征求意见稿）》	《网络数据安全条例》	主要变化
<p>（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；</p> <p>（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。</p>		
<p>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：—</p> <p>（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；</p> <p>（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</p>	<p>第十二条 网络数据处理者向其他网络数据处理者提供、委托处理个人信息和重要数据的，应当通过合同等与网络数据接收方约定处理目的、方式、范围以及安全保护义务等，并对网络数据接收方履行义务的情况进行监督。向其他网络数据处理者提供、委托处理个人信息和重要数据的处理情况记录，应当至少保存3年。</p> <p>网络数据接收方应当履行网络安全保护义务，并按照约定的目的、方式、范围等处理个人信息和重要数据。</p>	调整+删除+新增

《网络数据安全条例（征求意见稿）》	《网络数据安全条例》	主要变化
<p>进行监督；</p> <p>（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。</p> <p>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。</p>	<p>两个以上的网络数据处理者共同决定个人信息和重要数据的处理目的和处理方式的，应当约定各自的权利和义务。</p>	
<p>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：—</p> <p>—（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；—</p> <p>—（二）处理一百万人以上个人信息的数据处理器赴国外上市的；—</p> <p>—（三）数据处理者赴香港上市，影响或者可能影响国家安全的；—</p> <p>—（四）其他影响或者可能影响国家安全的</p>	<p>第十三条 网络数据处理者开展网络数据处理活动，影响或者可能影响国家安全的，应当按照国家有关规定进行国家安全审查。</p>	删除+新增

《网络数据安全条例（征求意见稿）》	《网络数据安全条例》	主要变化
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。	第十四条 网络数据处理者因合并、分立、解散、破产等原因需要转移网络数据的，网络数据接收方应当继续履行网络数据安全保护义务。	调整+删除
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。	/	删除
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。	/	删除
/	第十五条 国家机关委托他人建设、运行、维护电子政务	新增

《网络数据安全条例（征求意见稿）》	《网络数据安全条例》	主要变化
	系统，存储、加工政务数据，应当按照国家有关规定经过严格的批准程序，明确受托方的网络数据处理权限、保护责任等，监督受托方履行网络数据安全保护义务。	
（请见第五十一条）	第十六条 网络数据处理者为国家机关、关键信息基础设施运营者提供服务，或者参与其他公共基础设施、公共服务系统建设、运行、维护的，应当依照法律、法规的规定和合同约定履行网络数据安全保护义务，提供安全、稳定、持续的服务。 前款规定的网络数据处理者未经委托方同意，不得访问、获取、留存、使用、泄露或者向他人提供网络数据，不得对网络数据进行关联分析。	调整+新增+变更条文顺序
/	第十七条 为国家机关提供服务的信息系统应当参照电子政务系统的管理要求加强网络数据安全保护，保障网络数据安全。	新增
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	第十八条 网络数据处理者使用自动化工具访问、收集网络数据，应当评估对网络服务带来的影响，不得非法侵	调整+删除

《网络数据安全条例（征求意见稿）》	《网络数据安全条例》	主要变化
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。	入他人网络，不得干扰网络服务正常运行。	
/	第十九条 提供生成式人工智能服务的网络数据处理者应当加强对训练数据和训练数据处理活动的安全管理，采取有效措施防范和处置网络数据安全风险。	新增
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。	第二十条 面向社会提供产品、服务的网络数据处理者应当接受社会监督，建立便捷的网络数据安全投诉、举报渠道，公布投诉、举报方式等信息，及时受理并处理网络数据安全投诉、举报。	调整、删除
第三章 个人信息保护	第三章 个人信息保护	不变
第十九条 数据处理者处理个人信息，应当具有明确、合	/	删除

《网络数据安全条例（征求意见稿）》	《网络数据安全条例》	主要变化
<p>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：—</p> <p>—（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；—</p> <p>—（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；—</p> <p>—（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。—</p>		
<p>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。</p> <p>个人信息处理规则应当包括但不限于以下内容：</p> <p>（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</p>	<p>第二十一条 网络数据处理者在处理个人信息前，通过制定个人信息处理规则的方式依法向个人告知的，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、清晰易懂，包括但不限于下列内容：</p> <p>（一）网络数据处理者的名称或者姓名和联系方式；</p> <p>（二）处理个人信息的目的、方式、种类，处理敏感个人信息的必要性以及对个人权益的影响；</p>	调整+删除+新增

《网络数据安全条例（征求意见稿）》	《网络数据安全条例》	主要变化
<p>理个人信息对个人的影响；</p> <p>（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；</p> <p>（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；</p> <p>（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；</p> <p>（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；</p> <p>（六）个人信息安全风险及保护措施；</p> <p>（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。</p>	<p>（三）个人信息保存期限和到期后的处理方式，保存期限难以确定的，应当明确保存期限的确定方法；</p> <p>（四）个人查阅、复制、转移、更正、补充、删除、限制处理个人信息以及注销账号、撤回同意的方法和途径等。</p> <p>网络数据处理者按照前款规定向个人告知收集和向其他网络数据处理者提供个人信息的目的、方式、种类以及网络数据接收方信息的，应当以清单等形式予以列明。</p> <p>网络数据处理者处理不满十四周岁未成年人个人信息的，还应当制定专门的个人信息处理规则。</p>	
第二十一条 处理个人信息应当取得个人同意的，数据处	第二十二条 网络数据处理者基于个人同意处理个人信息	调整+删除+新

《网络数据安全条例（征求意见稿）》	《网络数据安全条例》	主要变化
<p>理者应当遵守以下规定：</p> <p>（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；</p> <p>（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；</p> <p>（三）处理不满十四周岁未成年人个人信息，应当取得其监护人同意；</p> <p>（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；</p> <p>（五）不得通过误导、欺诈、胁迫等方式获得个人的同意；</p> <p>（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；</p> <p>（七）不得超出个人授权同意的范围处理个人信息；</p> <p>（八）不得在个人明确表示不同意后，频繁征求同意</p>	<p>的，应当遵守下列规定：</p> <p>（一）收集个人信息为提供产品或者服务所必需，不得超范围收集个人信息，不得通过误导、欺诈、胁迫等方式取得个人同意；</p> <p>（二）处理生物识别、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的，应当取得个人的单独同意；</p> <p>（三）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；</p> <p>（四）不得超出个人同意的个人信息处理目的、方式、种类、保存期限处理个人信息；</p> <p>（五）不得在个人明确表示不同意处理其个人信息后，频繁征求同意；</p> <p>（六）个人信息的处理目的、方式、种类发生变更的，应当重新取得个人同意。</p> <p>法律、行政法规规定处理敏感个人信息应当取得书面同</p>	增

《网络数据安全条例（征求意见稿）》	《网络数据安全条例》	主要变化
<p>干扰正常使用服务。</p> <p>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。</p> <p>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。</p>	<p>意的，从其规定。</p>	
<p>第二十三条 有下列情形之一的，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：—</p> <p>—（一）已实现个人信息处理目的或者实现处理目的不再必要；—</p> <p>—（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；—</p> <p>—（三）终止服务或者个人注销账号；—</p> <p>—（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。—</p> <p>删除个人信息从技术上难以实现，或者因业务复杂等原</p>	<p>/</p>	<p>删除</p>

《网络数据安全条例（征求意见稿）》	《网络数据安全条例》	主要变化
<p>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。</p> <p>法律、行政法规另有规定的从其规定。</p>		
<p>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：</p> <p>（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；</p> <p>（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；</p> <p>（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。</p>	<p>第二十三条 个人请求查阅、复制、更正、补充、删除、限制处理其个人信息，或者个人注销账号、撤回同意的，网络数据处理者应当及时受理，并提供便捷的支持个人行使权利的方法和途径，不得设置不合理条件限制个人的合理请求。</p>	调整+删除

《网络数据安全条例（征求意见稿）》	《网络数据安全条例》	主要变化
法律、行政法规另有规定的从其规定。		
/	第二十四条 因使用自动化采集技术等无法避免采集到非必要个人信息或者未依法取得个人同意的个人信息，以及个人注销账号的，网络数据处理者应当删除个人信息或者进行匿名化处理。法律、行政法规规定的保存期限未届满，或者删除、匿名化处理个人信息从技术上难以实现的，网络数据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。	新增
第二十四条 符合下列条件的个人信息转移请求，网络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手同意或者订立、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。	第二十五条 对符合下列条件的个人信息转移请求，网络数据处理者应当为个人指定的其他网络数据处理者访问、获取有关个人信息提供途径： （一）能够验证请求人的真实身份； （二）请求转移的是本人同意提供的或者基于合同收集的个人信息； （三）转移个人信息具备技术可行性； （四）转移个人信息不损害他人合法权益。	调整+删除+新增

《网络数据安全条例（征求意见稿）》	《网络数据安全条例》	主要变化
<p>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。</p> <p>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。</p>	<p>请求转移个人信息次数等明显超出合理范围的，网络数据处理者可以根据转移个人信息的成本收取必要费用。</p>	
<p>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。</p> <p>法律、行政法规另有规定的从其规定。</p>	/	删除
/	<p>第二十六条 中华人民共和国境外网络数据处理者处理境内自然人个人信息，依照《中华人民共和国个人信息保护法》第五十三条规定在境内设立专门机构或者指定代表的，应当将有关机构的名称或者代表的姓名、联系方式等报送所在地设区的市级网信部门；网信部门应当及</p>	新增

《网络数据安全条例（征求意见稿）》	《网络数据安全条例》	主要变化
	时通报同级有关主管部门。	
（请见第五十八条）	第二十七条 网络数据处理者应当定期自行或者委托专业机构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。	调整+删除+条文顺序变更
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。	第二十八条 网络数据处理者处理 1000 万人以上个人信息的，还应当遵守本条例第三十条、第三十二条对处理重要数据的网络数据处理者（以下简称重要数据的处理者）作出的规定。	调整
第四章 重要数据安全	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。	第二十九条 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。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，对列入目录的网络数据进行重点保护。 网络数据处理者应当按照国家有关规定识别、申报重要数据。对确认为重要数据的，相关地区、部门应当及时	调整+新增

《网络数据安全条例（征求意见稿）》	《网络数据安全条例》	主要变化
	<p>向网络数据处理者告知或者公开发布。网络数据处理者应当履行网络数据安全保护责任。</p> <p>国家鼓励网络数据处理者使用数据标签标识等技术和产品，提高重要数据安全水平。</p>	
<p>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：</p> <p>（一）研究提出数据安全相关重大决策建议；</p> <p>（二）制定实施数据安全保护计划和数据安全事件应急预案；</p> <p>（三）开展数据安全风险监测，及时处置数据安全风险和事件；</p> <p>（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；</p> <p>（五）受理、处置数据安全投诉、举报；</p> <p>（六）按照要求及时向网信部门和主管、监管部门报告</p>	<p>第三十条 重要数据的处理者应当明确网络数据安全负责人和网络数据安全管理机构。网络数据安全管理机构应当履行下列网络数据安全保护责任：</p> <p>（一）制定实施网络数据安全管理制度、操作规程和网络数据安全事件应急预案；</p> <p>（二）定期组织开展网络数据安全风险监测、风险评估、应急演练、宣传教育培训等活动，及时处置网络数据安全风险和事件；</p> <p>（三）受理并处理网络数据安全投诉、举报。</p> <p>网络数据安全负责人应当具备网络数据安全专业知识和相关管理工作经历，由网络数据处理者管理层成员担任，有权直接向有关主管部门报告网络数据安全情况。</p>	<p>调整+删除+新增</p>

《网络数据安全条例（征求意见稿）》	《网络数据安全条例》	主要变化
<p>数据安全情况。</p> <p>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。</p>	<p>掌握有关主管部门规定的特定种类、规模的重要数据的网络数据处理者，应当对网络数据安全负责人和关键岗位的人员进行安全背景审查，加强相关人员培训。审查时，可以申请公安机关、国家安全机关协助。</p>	
<p>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：—</p> <p>—（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；—</p> <p>—（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；—</p> <p>—（三）国家网信部门和主管、监管部门规定的其他备案内容。</p> <p>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。</p> <p>依据部门职责分工，网信部门与有关部门共享备案信</p>	<p>/</p>	<p>删除</p>

《网络数据安全条例（征求意见稿）》	《网络数据安全条例》	主要变化
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。	/	删除
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。	/	删除
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	第三十三条 重要数据的处理者应当每年度对其网络数据处理活动开展风险评估，并向省级以上有关主管部门报送风险评估报告，有关主管部门应当及时通报同级网信部门、公安机关。 风险评估报告应当包括下列内容： （一）网络数据处理者基本信息、网络数据安全管理机构信息、网络数据安全负责人姓名和联系方式等； （二）处理重要数据的目的、种类、数量、方式、范围、存储期限、存储地点等，开展网络数据处理活动的	拆分+调整+新增

《网络数据安全条例（征求意见稿）》	《网络数据安全条例》	主要变化
<p>有效性；</p> <p>（四）落实国家数据安全法律、行政法规和标准情况；</p> <p>（五）发生的数据安全事件及其处置情况；</p> <p>（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；</p> <p>（七）数据安全相关的投诉及处理情况；</p> <p>（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。</p> <p>数据处理者应当保留风险评估报告至少三年。</p> <p>依据部门职责分工，网信部门与有关部门共享报告信息。</p> <p>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：</p> <p>（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；</p>	<p>情况，不包括网络数据内容本身；</p> <p>（三）网络数据安全管理制度及实施情况，加密、备份、标签标识、访问控制、安全认证等技术措施和其他必要措施及其有效性；</p> <p>（四）发现的网络数据安全风险，发生的网络数据安全事件及处置情况；</p> <p>（五）提供、委托处理、共同处理重要数据的风险评估情况；</p> <p>（六）网络数据出境情况；</p> <p>（七）有关主管部门规定的其他报告内容。</p> <p>处理重要数据的大型网络平台服务提供者报送的风险评估报告，除包括前款规定的内容外，还应当充分说明关键业务和供应链网络数据安全等情况。</p> <p>重要数据的处理者存在可能危害国家安全的重要数据处理活动的，省级以上有关主管部门应当责令其采取整改或者停止处理重要数据等措施。重要数据的处理者应当</p>	

《网络数据安全条例（征求意见稿）》	《网络数据安全条例》	主要变化
<p>（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；</p> <p>（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；</p> <p>（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；</p> <p>（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。</p> <p>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。</p>	<p>按照有关要求立即采取措施。</p> <p>第三十一条 重要数据的处理者提供、委托处理、共同处理重要数据前，应当进行风险评估，但是属于履行法定职责或者法定义务的除外。</p> <p>风险评估应当重点评估下列内容：</p> <p>（一）提供、委托处理、共同处理网络数据，以及网络数据接收方处理网络数据的目的、方式、范围等是否合法、正当、必要；</p> <p>（二）提供、委托处理、共同处理的网络数据遭到篡改、破坏、泄露或者非法获取、非法利用的风险，以及对国家安全、公共利益或者个人、组织合法权益带来的风险；</p> <p>（三）网络数据接收方的诚信、守法等情况；</p> <p>（四）与网络数据接收方订立或者拟订立的相关合同中关于网络安全的要求能否有效约束网络数据接收方履行网络安全保护义务；</p>	

《网络数据安全条例（征求意见稿）》	《网络数据安全条例》	主要变化
	<p>（五）采取或者拟采取的技术和管理措施等能否有效防范网络数据遭到篡改、破坏、泄露或者非法获取、非法利用等风险；</p> <p>（六）有关主管部门规定的其他评估内容。</p>	
/	<p>第三十二条 重要数据的处理者因合并、分立、解散、破产等可能影响重要数据安全的，应当采取措施保障网络数据安全，并向省级以上有关主管部门报告重要数据处置方案、接收方的名称或者姓名和联系方式等；主管部门不明确的，应当向省级以上数据安全工作协调机制报告。</p>	新增
<p>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。</p>	/	删除
<p>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</p>	/	删除

《网络数据安全条例（征求意见稿）》	《网络数据安全条例》	主要变化
门组织的安全评估。		
第五章 数据跨境安全管理	第五章 网络 数据跨境安全管理	调整
/	第三十四条 国家网信部门统筹协调有关部门建立国家数据出境安全管理专项工作机制，研究制定国家网络数据出境安全管理相关政策，协调处理网络数据出境安全重大事项。	新增
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	第三十五条 符合下列条件之一的，网络数据处理者可以向境外提供个人信息： （一）通过国家网信部门组织的数据出境安全评估； （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） 符合 国家网信部门制定的关于 个人信息 出境标准合同的规定； （四）为订立、履行个人作为一方当事人的合同， 确需 向境外提供个人信息； （五）按照依法制定的劳动规章制度和依法签订的集体	调整+新增

《网络数据安全条例（征求意见稿）》	《网络数据安全条例》	主要变化
<p>必需向境外提供当事人个人信息的，或者为子保护全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。</p>	<p>合同实施跨境人力资源管理，确需向境外提供员工个人信息；</p> <p>（六）为履行法定职责或者法定义务，确需向境外提供个人信息；</p> <p>（七）紧急情况下为保护自然人的生命健康和财产安全，确需向境外提供个人信息；</p> <p>（八）法律、行政法规或者国家网信部门规定的其他条件。</p>	
<p>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。</p> <p>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。</p>	/	删除

《网络数据安全条例（征求意见稿）》	《网络数据安全条例》	主要变化
<p>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：—</p> <p>—（一）出境数据中包含重要数据；—</p> <p>—（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；—</p> <p>—（三）国家网信部门规定的其它情形。—</p> <p>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。—</p>	<p>第三十七条 网络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确需向境外提供的，应当通过国家网信部门组织的数据出境安全评估。网络数据处理者按照国家有关规定识别、申报重要数据，但未被相关地区、部门告知或者公开发布为重要数据的，不需要将其作为重要数据申报数据出境安全评估。</p>	调整
<p>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。</p>	<p>第三十六条 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。</p>	条文顺序调整
<p>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：—</p> <p>—（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</p>	<p>第三十八条 通过数据出境安全评估后，网络数据处理者向境外提供个人信息和重要数据的，不得超出评估时明确的数据出境目的、方式、范围和种类、规模等。</p>	调整+删除

《网络数据安全条例（征求意见稿）》	《网络数据安全条例》	主要变化
<p>境外提供个人信息；—</p> <p>—（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；—</p> <p>—（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；—</p> <p>—（四）接受和处理数据出境所涉及的用户投诉；—</p> <p>—（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；—</p> <p>—（六）存留相关日志记录和数据出境审批记录三年以上；—</p> <p>—（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；—</p> <p>—（八）国家网信部门认定不得出境的，数据处理者应当</p>		

《网络数据安全条例（征求意见稿）》	《网络数据安全条例》	主要变化
<p>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；—</p> <p>（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。—</p> <p>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。—</p>		
<p>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：—</p> <p>（一）全部数据接收方名称、联系方式；—</p> <p>（二）出境数据的类型、数量及目的；—</p> <p>（三）数据在境外的存放地点、存储期限、使用范围和方式；—</p> <p>（四）涉及向境外提供数据的用户投诉及处理情况；—</p>	/	删除

《网络数据安全条例（征求意见稿）》	《网络数据安全条例》	主要变化
（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。	第三十九条 国家采取措施，防范、处置网络数据跨境安全风险和威胁。任何个人、组织不得提供专门用于破坏、避开技术措施的程序、工具等；明知他人从事破坏、避开技术措施等活动的，不得为其提供技术支持或者帮助。	调整+删除
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。	/	删除
第六章 互联网平台运营者 义务	第六章 网络平台服务提供者 义务	调整

《网络数据安全条例（征求意见稿）》	《网络数据安全条例》	主要变化
<p>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。</p> <p>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。</p> <p>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。</p>	/	删除

《网络数据安全管理条例（征求意见稿）》	《网络数据安全管理条例》	主要变化
<p>第四十四 互联网平台运营者应当对接入其平台的第三方产品和服务承担数据安全责任，通过合同等形式明确第三方的数据安全责任义务，并督促第三方加强数据安全保护，采取必要的数据安全保护措施。</p> <p>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。</p> <p>移动通信终端预装第三方产品适用本条前两款规定。</p>	<p>第四十条 网络平台服务提供者应当通过平台规则或者合同明确接入其平台的第三方产品和服务提供者的网络安全保护义务，督促第三方产品和服务提供者加强网络数据安全管理。</p> <p>预装应用程序的智能终端等设备生产者，适用前款规定。</p> <p>第三方产品和服务提供者违反法律、行政法规的规定或者平台规则、合同约定开展网络数据处理活动，对用户造成损害的，网络平台服务提供者、第三方产品和服务提供者、预装应用程序的智能终端等设备生产者应当依法承担相应责任。</p> <p>国家鼓励保险公司开发网络数据损害赔偿责任险种，鼓励网络平台服务提供者、预装应用程序的智能终端等设备生产者投保。</p>	调整+新增
<p>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</p>	/	删除

《网络数据安全条例（征求意见稿）》	《网络数据安全条例》	主要变化
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。		
<p>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：</p> <p>（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权益的行为；</p> <p>（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；</p> <p>（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；</p> <p>（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。</p>	<p>第四十六条 大型网络平台服务提供者不得利用网络数据、算法以及平台规则等从事下列活动：</p> <p>（一）通过误导、欺诈、胁迫等方式处理用户在平台上产生的网络数据；</p> <p>（二）无正当理由限制用户访问、使用其在平台上产生的网络数据；</p> <p>（三）对用户实施不合理的差别待遇，损害用户合法权益；</p> <p>（四）法律、行政法规禁止的其他活动。</p>	调整+删除
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	第四十一条 提供应用程序分发服务的网络服务平台服务提供者，应当建立应用程序核验规则并开展网络数据安全相	调整

《网络数据安全条例（征求意见稿）》	《网络数据安全条例》	主要变化
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 的应用程序 ，应当采取 拒绝上架、督促整改、下架处置 等措施。	关核验。发现待分发或者已分发的应用程序不符合法律、行政法规的规定或者国家标准的强制性要求的，应当采取警示、不予分发、暂停分发或者终止分发等措施。	
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。	/	删除
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	第四十二条 网络平台服务提供者通过自动化决策方式向个人进行信息推送的，应当设置易于理解、便于访问和操作的个性化推荐关闭选项，为用户 提供 拒绝接收推送信息、 删除 针对其个人特征的用户标签等功能。	调整+删除

《网络数据安全条例（征求意见稿）》	《网络数据安全条例》	主要变化
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。	第四十三条 国家推进网络身份认证公共服务建设，按照政府引导、用户自愿原则进行推广应用。 鼓励网络平台服务提供者支持用户使用国家网络身份认证公共服务登记、核验真实身份信息。	
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。	（请见第十六条）	调整+新增+变更条文顺序
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	/	删除

《网络数据安全条例（征求意见稿）》	《网络数据安全条例》	主要变化
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。	第四十四条 大型网络服务平台提供者应当每年度发布个人信息保护社会责任报告，报告内容包括但不限于个人信息保护措施和成效、个人行使权利的申请受理情况、主要由外部成员组成的个人信息保护监督机构履行职责情况等。	
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。	/	删除
/	第四十五条 大型网络服务平台提供者跨境提供网络数据，应当遵守国家数据跨境安全管理要求，健全相关技术和管理措施，防范网络数据跨境安全风险。	新增

《网络数据安全条例（征求意见稿）》	《网络数据安全条例》	主要变化
第七章 监督管理	第七章 监督管理	不变
<p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p>	<p>第四十七条 国家网信部门负责统筹协调网络数据安全和相关监督管理工作。</p> <p>公安机关、国家安全机关依照有关法律、行政法规和本条例的规定，在各自职责范围内承担网络数据安全监督管理职责，依法防范和打击危害网络数据安全的违法犯罪活动。</p> <p>国家数据管理部门在具体承担数据管理工作中履行相应的网络数据安全职责。</p> <p>各地区、各部门对本地区、本部门工作中收集和产生的网络数据及网络数据安全负责。</p> <p>第四十八条 各有关主管部门承担本行业、本领域网络数据安全监督管理职责，应当明确本行业、本领域网络数据安全保护工作机构，统筹制定并组织实施本行业、本领域网络数据安全事件应急预案，定期组织开展本行业、本领域网络数据安全风险评估，对网络数据处理者</p>	调整+拆分+新增

《网络数据安全条例（征求意见稿）》	《网络数据安全条例》	主要变化
	履行网络数据安全保护义务情况进行监督检查，指导督促网络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。	第四十九条 国家网信部门统筹协调有关主管部门及时汇总、研判、共享、发布网络数据安全风险相关信息，加强网络数据安全信息共享、网络数据安全风险和威胁监测预警以及网络数据安全事件应急处置工作。	调整
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。	第五十条 有关主管部门可以采取下列措施对网络数据安全进行监督检查： （一）要求网络数据处理者及其相关人员就监督检查事项作出说明； （二）查阅、复制与网络数据安全有关的文件、记录； （三）检查网络数据安全措施运行情况； （四）检查与网络数据处理活动有关的设备、物品； （五）法律、行政法规规定的其他必要措施。 网络数据处理者应当对有关主管部门依法开展的网路数	调整+拆分+新增+删除

《网络数据安全条例（征求意见稿）》	《网络数据安全条例》	主要变化
<p>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。</p> <p>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。</p>	<p>据安全监督检查予以配合。</p> <p>第五十一条 有关主管部门开展网络数据安全监督检查，应当客观公正，不得向被检查单位收取费用。</p> <p>有关主管部门在网络数据安全监督检查中不得访问、收集与网络数据安全无关的业务信息，获取的信息只能用于维护网络数据安全的需要，不得用于其他用途。</p> <p>有关主管部门发现网络数据处理者的网络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要求网络数据处理者暂停相关服务、修改平台规则、完善技术措施等，消除网络数据安全隐患。</p>	
/	<p>第五十二条 有关主管部门在开展网络数据安全监督检查时，应当加强协同配合、信息沟通，合理确定检查频次和检查方式，避免不必要的检查和交叉重复检查。</p> <p>个人信息保护合规审计、重要数据风险评估、重要数据出境安全评估等应当加强衔接，避免重复评估、审计。</p> <p>重要数据风险评估和网络安全等级测评的内容重合的，</p>	

《网络数据安全条例（征求意见稿）》	《网络数据安全条例》	主要变化
	相关结果可以互相采信。	
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。	（请见第二十七条）	调整+删除+条文顺序变更
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；	（请见第九条）	调整+删除+条文顺序变更

《网络数据安全条例（征求意见稿）》	《网络数据安全条例》	主要变化
（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。		
/	第五十三条 有关主管部门及其工作人员对在履行职责中知悉的个人隐私、个人信息、商业秘密、保密商务信息等网络数据应当依法予以保密，不得泄露或者非法向他人提供。	新增
/	第五十四条 境外的组织、个人从事危害中华人民共和国国家安全、公共利益，或者侵害中华人民共和国公民的个人信息权益的网络数据处理活动的，国家网信部门会同有关主管部门可以依法采取相应的必要措施。	新增
第八章 法律责任	第八章 法律责任	不变
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	第五十五条 违反本条例第十二条、第十六条至第二十条、第二十二条、第四十条第一款和第二款、第四十一条、第四十二条规定的，由网信、电信、公安等主管部	调整

《网络数据安全条例（征求意见稿）》	《网络数据安全条例》	主要变化
<p>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。</p> <p>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、第二十三条、第二十四条、第二十五条规定的网络安全保护义务的，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。</p> <p>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</p>	<p>门依据各自职责责令改正，给予警告，没收违法所得；拒不改正或者情节严重的，处 100 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可以处 1 万元以上 10 万元以下罚款。</p> <p>第五十六条 违反本条例第十三条规定的，由网信、电信、公安、国家安全等主管部门依据各自职责责令改正，给予警告，可以并处 10 万元以上 100 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 1 万元以上 10 万元以下罚款；拒不改正或者情节严重的，处 100 万元以上 1000 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 10 万元以上 100 万元以下罚款。</p> <p>第五十七条 违反本条例第二十九条第二款、第三十条第二款和第三款、第三十一条、第三十二条规定的，由网</p>	

《网络数据安全条例（征求意见稿）》	《网络数据安全条例》	主要变化
<p>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。</p> <p>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。</p> <p>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</p>	<p>信、电信、公安等主管部门依据各自职责责令改正，给予警告，可以并处 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可以处 1 万元以上 10 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 50 万元以上 200 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 5 万元以上 20 万元以下罚款。</p>	

《网络数据安全条例（征求意见稿）》	《网络数据安全条例》	主要变化
<p>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。</p> <p>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。</p> <p>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</p>		

《网络数据安全条例（征求意见稿）》	《网络数据安全条例》	主要变化
<p>照；构成犯罪的，依照相关法律、行政法规的规定处罚。</p> <p>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。</p>		
<p>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。</p> <p>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</p>	<p>第五十八条 违反本条例其他有关规定的，由有关主管部门依照《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》等法律的有关规定追究法律责任。</p>	删除+新增

《网络数据安全条例（征求意见稿）》	《网络数据安全条例》	主要变化
<p>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。</p>		
<p>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。</p>		
<p>第六十六条 个人和组织违反第四十一条的规定，由有关</p>		

《网络数据安全条例（征求意见稿）》	《网络数据安全条例》	主要变化
<p>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。</p>		
<p>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。</p>	<p>第六十一条 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。</p>	<p>调整+条文顺序调整</p>
<p>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。</p>	<p>第六十条 国家机关不履行本条例规定的网络数据安全保护义务的，由其上级机关或者有关主管部门责令改正；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。</p>	<p>调整+条文顺序调整</p>

《网络数据安全条例（征求意见稿）》	《网络数据安全条例》	主要变化
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。	（请见第二条）	调整+条文顺序调整
第九章 附则	第九章 附则	不变
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	第六十二条 本条例下列用语的含义： （一）网络数据，是指通过网络处理和产生的各种电子数据。 （二）网络数据处理活动，是指网络数据的收集、存储、使用、加工、传输、提供、公开、删除等活动。 （三）网络数据处理者，是指在网络数据处理活动中自主决定处理目的和处理方式的个人、组织。 （四）重要数据，是指特定领域、特定群体、特定区域或者达到一定精度和规模，一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能直接危害国家安全、经济运行、社会稳定、公共健康和安全的数据。 （五）委托处理，是指网络数据处理者委托个人、组织	调整+删除

《网络数据安全条例（征求意见稿）》	《网络数据安全条例》	主要变化
<p>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；—</p> <p>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；—</p> <p>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；—</p> <p>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；—</p> <p>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；—</p> <p>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、</p>	<p>按照约定的目的和方式开展的网络数据处理活动。</p> <p>（六）共同处理，是指两个以上的网络数据处理者共同决定网络数据的处理目的和处理方式的网络数据处理活动。</p> <p>（七）单独同意，是指个人针对其个人信息进行特定处理而专门作出具体、明确的同意。</p> <p>（八）大型网络平台，是指注册用户 5000 万以上或者月活跃用户 1000 万以上，业务类型复杂，网络数据处理活动对国家安全、经济运行、国计民生等具有重要影响的网络平台。</p>	

《网络数据安全条例（征求意见稿）》	《网络数据安全条例》	主要变化
<p>太空、极地、深海等安全的数据。</p> <p>（四）核心数据是指关系国家安全、国民经济命脉、重要民生和重大公共利益等的的数据。</p> <p>（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。</p> <p>（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。</p> <p>（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。</p> <p>（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。</p> <p>（九）互联网平台运营者是指为用户提供信息发布、社</p>		

《网络数据安全条例（征求意见稿）》	《网络数据安全条例》	主要变化
<p>交、交易、支付、视听等互联网平台服务的数据处理者。</p> <p>（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。</p> <p>（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。</p> <p>（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。</p>		
<p>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。</p>	<p>第六十三条 开展核心数据的网络数据处理活动，按照国家有关规定执行。</p> <p>自然人因个人或者家庭事务处理个人信息的，不适用本条例。</p>	调整+新增

《网络数据安全条例（征求意见稿）》	《网络数据安全条例》	主要变化
	开展涉及国家秘密、工作秘密的网络数据处理活动，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。	
第七十五条 本条例自 年 月 日起施行。	第六十四条 本条例自 2025 年 1 月 1 日起施行。	/