# 网络数据安全管理条例

(2024年8月30日国务院第40次常务会议通过　2024年9月24日中华人民共和国国务院令第790号公布　自2025年1月1日起施行)

## 第一章　总　　则

**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。

**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。

**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。

**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，开展网络数据安全宣传教育和人才培养，促进网络数据开发利用和产业发展。

**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。

**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。

**第七条** 国家支持相关行业组织按照章程，制定网络数据安全行为规范，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。

## 第二章 一般规定

**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。

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。

**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。

**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。

**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。

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。

**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。

网络数据接收方应当履行网络数据安全保护义务，并按照约定的目的、方式、范围等处理个人信息和重要数据。

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。

**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。

**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。

**第十五条** 国家机关委托他人建设、运行、维护电子政务系统，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。

**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。

**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管理，保障网络数据安全。

**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。

**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。

## 第三章 个人信息保护

**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:

(一) 网络数据处理者的名称或者姓名和联系方式;

(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;

(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;

(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。

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。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。

**第二十二条** 网络数据处理者基于个人同意处理个人信息的，应当遵守下列规定:

(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;

(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;

(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;

(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;

(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;

(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。

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。

**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。

**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。

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。

**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；网信部门应当及时通报同级有关主管部门。

**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。

**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。

## 第四章 重要数据安全

**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。

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，提高重要数据安全管理水平。

**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:

(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;

(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;

(三)受理并处理网络数据安全投诉、举报。

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。

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。

**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。

风险评估应当重点评估下列内容:

(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;

(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;

(三)网络数据接收方的诚信、守法等情况;

(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数据安全的要求能否有效约束网络数据接收方履行网络数据安全保护义务;

(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;

(六)有关主管部门规定的其他评估内容。

**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。

**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情况，不包括网络数据内容本身；

（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；

（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；

（五）提供、委托处理、共同处理重要数据的风险评估情况；

（六）网络数据出境情况；

（七）有关主管部门规定的其他报告内容。

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。

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按照有关要求立即采取措施。

## 第五章　网络数据跨境安全管理

**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。

**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;

(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;

(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;

(八)法律、行政法规或者国家网信部门规定的其他条件。

**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。

**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。

**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。

**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。

## 第六章 网络平台服务提供者义务

**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等明确接入其平台的第三方产品和服务提供者的网络数据安全保护义务，督促第三方产品和服务提供者加强网络数据安全管理。

预装应用程序的智能终端等设备生产者，适用前款规定。

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。

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。

**第四十一条** 提供应用程序分发服务的网络平台服务提供者，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。

**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。

**第四十四条** 大型网络平台服务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。

**第四十五条** 大型网络平台服务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。

**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：

(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;

(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;

(三)对用户实施不合理的差别待遇，损害用户合法权益;

(四)法律、行政法规禁止的其他活动。

## 第七章　监 督 管 理

**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。

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。

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。

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。

**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。

**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络数据安全监督检查予以配合。

**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。

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。

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。

**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。

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。重要数据风险评估和网络安全等级测评的内容重合的，相关结果可以互相采信。

**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。

**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。

## 第八章　法 律 责 任

**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。

**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。

**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。

**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。

**第五十九条** 网络数据处理者存在主动消除或者减轻违法行为危害后果、违法行为轻微并及时改正且没有造成危害后果或者初次违法且危害后果轻微并及时改正等情形的，依照《中华人民共和国行政处罚法》的规定从轻、减轻或者不予行政处罚。

**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。

**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。

## 第九章　附　　则

**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、组织按照约定的目的和方式开展的网络数据处理活动。

(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。

(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。

(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。

**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。

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。

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。

**第六十四条** 本条例自 2025 年 1 月 1 日起施行。