数据安全管理办法
（征求意见稿）

Measures for Data Security Management
(Draft for Comments)

第一章　总则
Chapter I General Provisions

第一条 为了维护国家安全、社会公共利益，保护公民、法人和其他组织在网络空间的合法权益，保障个人信息和重要数据安全，根据《中华人民共和国网络安全法》等法律法规，制定本办法。

Article 1 These Measures are developed in accordance with the Cybersecurity Law of the People's Republic of China and other laws and regulations for the purposes of safeguarding national security, public interest, protecting the lawful rights and interests of citizens, legal persons and other organizations in cyberspace.

第二条 在中华人民共和国境内利用网络开展数据收集、存储、传输、处理、使用等活动（以下简称数据活动），以及数据安全的保护和监督管理，适用本办法。纯粹家庭和个人事务除外。

法律、行政法规另有规定的，从其规定。

Article 2 This Law shall apply to the collection, storage, transmission, process and use of data (hereinafter referred to as “data activities”) as well as the protection, supervision and administration of cybersecurity within the territory of the People's Republic of China, except for pure domestic and personal matters.

In case of inconformity with the provisions of the laws and regulations, the latter shall prevail.

第三条 国家坚持保障数据安全与发展并重，鼓励研发数据安全保护技术，积极推进数据资源开发利用，保障数据依法有序自由流动。

Article 3 The state shall lay equal stress on data security protection and development, encourage the research and development of data security protection technologies, promote the development and use of data resources, and guarantee the orderly and free flow of data in accordance with the law.

第四条 国家采取措施，监测、防御、处置来源于中华人民共和国境内外的数据安全风险和威胁，保护数据免受泄露、窃取、篡改、毁损、非法使用等，依法惩治危害数据安全的违法犯罪活动。

Article 4 The state shall take measures to monitor, defend against and deal with cybersecurity risks and threats from both inside and outside the territory of the People's Republic of China, protect data from divulged, stolen, falsified or illegal use, punish illegal and criminal activities relating to data security in accordance with the law.

第五条 在中央网络安全和信息化委员会领导下，国家网信部门统筹协调、指导监督个人信息和重要数据安全保护工作。

地（市）及以上网信部门依据职责指导监督本行政区内个人信息和重要数据安全保护工作。

Article 5 Under the leadership of the Central Cyberspace Affairs Commission, the state cyberspace administration organs shall be responsible for the overall planning, coordination, direction and supervision of protecting personal information and important data.

Cyberspace administrations at the municipal level or above shall direct and supervise the protection of personal information and important data within their respective administrative areas.

第六条 网络运营者应当按照有关法律、行政法规的规定，参照国家网络安全标准，履行数据安全保护义务，建立数据安全管理责任和评价考核制度，制定数据安全计划，实施数据安全技术防护，开展数据安全风险评估，制定网络安全事件应急预案，及时处置安全事件，组织数据安全教育、培训。

Article 6 Network operators shall perform data security protection obligations in accordance with relevant laws and administrative regulations and by reference to national cybersecurity standards, establish the accountability of data security management and evaluation systems, formulate data security plans, implement data protection technical measures, carry out data security risk assessments, develop emergency response plans, timely deal with security incidents and organize data security education and training.

第二章　数据收集
Chapter II Data Collection

第七条 网络运营者通过网站、应用程序等产品收集使用个人信息，应当分别制定并公开收集使用规则。收集使用规则可以包含在网站、应用程序等产品的隐私政策中，也可以其他形式提供给用户。

Article 7 Network operators shall, when collecting and using personal information through websites, applications and other products, develop and disclose the rules for collection and use separately. The rules for collection and use may be included in the privacy policy of websites, applications and other products, or may be made available to users in other forms.

第八条 收集使用规则应当明确具体、简单通俗、易于访问，突出以下内容：

（一）网络运营者基本信息；

（二）网络运营者主要负责人、数据安全责任人的姓名及联系方式；

（三）收集使用个人信息的目的、种类、数量、频度、方式、范围等；

（四）个人信息保存地点、期限及到期后的处理方式；

（五）向他人提供个人信息的规则，如果向他人提供的；

（六）个人信息安全保护策略等相关信息；

（七）个人信息主体撤销同意，以及查询、更正、删除个人信息的途径和方法；

（八）投诉、举报渠道和方法等；

（九）法律、行政法规规定的其他内容。

Article 8 The rules for collection and use shall be specific, easy to understand and access and shall highlight the following information:

(1) General information about the network operator;

(2) The name and contact information of the network operator's main responsible person as well as the person responsible for the data security;

(3) The purposes, types, volume, frequency, methods, scope of the personal information to be collected and used;

(4) The place of storage, retention period and what the network operator will do with personal data after the retention period expires;

(5) The rules to be followed when providing personal information to others (if the information will be provided to others);

(6) How the network operator protects the security of personal information and other relevant information;

(7) The ways and methods for the data subject to withdraw consent, and to access, correct and delete personal information;

(8) Channels and methods for making complaints and reports;

(9) Other information as prescribed by the laws and regulations.

第九条 如果收集使用规则包含在隐私政策中，应相对集中，明显提示，以方便阅读。另仅当用户知悉收集使用规则并明确同意后，网络运营者方可收集个人信息。

Article 9 The rules for collection and use shall, if included in private policy, be relatively concentrated and presented in an obvious way to facilitate reading. The network operator may collect personal information only after the user has acknowledged the rules for collection and use of personal data and provide express consent.

第十条 网络运营者应当严格遵守收集使用规则，网站、应用程序收集或使用个人信息的功

能设计应同隐私政策保持一致，同步调整。

Article 10 Network operators shall strictly comply with the rules of collection and use. The functionality of the network operator's websites and mobile applications to collect or use personal information shall be designed in accordance with the privacy policy, and it should be adjusted to be consistent with the privacy policy.

第十一条 网络运营者不得以改善服务质量、提升用户体验、定向推送信息、研发新产品等为由，以默认授权、功能捆绑等形式强迫、误导个人信息主体同意其收集个人信息。

个人信息主体同意收集保证网络产品核心业务功能运行的个人信息后，网络运营者应当向个人信息主体提供核心业务功能服务，不得因个人信息主体拒绝或者撤销同意收集上述信息以外的其他信息，而拒绝提供核心业务功能服务。

Article 11 Network operators shall not, through authorization by default, bundling functions or other means, force or mislead data subjects to consent to the collection of personal information on the grounds of improving service quality, user experience, targeted push information or research and development of new products.

After the data subject has provided consent to the collection of personal information that enables the operation of the core functions of network products, network operators shall provide core service functions to the data subject, and shall not cease the provision of such core functions on the ground that the data subject refuses to provide consent or withdraws consent to the collection of personal information.

第十二条 收集 14 周岁以下未成年人个人信息的，应当征得其监护人同意。

Article 12 When collecting personal information of minors under the age of 14 years, consent from the guardians is required.

第十三条 网络运营者不得依据个人信息主体是否授权收集个人信息及授权范围，对个人信息主体采取歧视行为，包括服务质量、价格差异等。

Article 13 Network operators shall not take discriminatory actions, such as implementing different service quality and price, against data subjects based on whether the data subjects have authorized the collection of personal information and the scope of such authorizations.

第十四条 网络运营者从其他途径获得个人信息，与直接收集个人信息负有同等的保护责任和义务。

Article 14 Network operators shall have the same responsibilities and obligations to protect personal information obtained from third party sources.

第十五条 网络运营者以经营为目的收集重要数据或个人敏感信息的，应向所在地网信部门

备案。备案内容包括收集使用规则，收集使用的目的、规模、方式、范围、类型、期限等，不包括数据内容本身。

Article 15 When network operators collect important data or sensitive personal information for the purposes of business operations, such network operators shall make a filing with the local cybersecurity administration. The filing shall include the rules for collection and use of such data, the purpose, volume, method, scope, type, retention period of the data, excluding the content of data itself.

第十六条 网络运营者采取自动化手段访问收集网站数据，不得妨碍网站正常运行；此类行为严重影响网站运行，如自动化访问收集流量超过网站日均流量三分之一，网站要求停止自动化访问收集时，应当停止。

Article 16 Network operators shall not, when using automatic means to access or collect website data, interfere with the normal operation of their websites. If such acts seriously affect the operation of websites (e.g., if the traffic of automatic visits or data collection exceeds one-third of the average traffic of the website) and the website requests the network operator to cease such automatic access and collection, the network operator shall cease such practice.

第十七条 网络运营者以经营为目的收集重要数据或个人敏感信息的，应当明确数据安全责任人。

数据安全责任人由具有相关管理工作经历和数据安全专业知识的人员担任，参与有关数据活动的重要决策，直接向网络运营者的主要负责人报告工作。

Article 17 Network operators shall, when collecting important data or personal sensitive information for the purpose of business operations, specify the person responsible for data security.

The person responsible for the data security shall be selected from among personnel who have relevant management work experience and professional knowledge on data protection, participate in important decisions of relevant data activities, and report work directly to the main responsible person of the network operators.

第十八条 数据安全责任人履行下列职责：

（一）组织制定数据保护计划并督促落实；

（二）组织开展数据安全风险评估，督促整改安全隐患；

（三）按要求向有关部门和网信部门报告数据安全保护和事件处置情况；

（四）受理并处理用户投诉和举报。

网络运营者应为数据安全责任人提供必要的资源，保障其独立履行职责。

Article 18 The person responsible for data security shall perform the following responsibilities and obligations:

(1) Organize the formulation of data protection plans and manage implementation;

(2) Organize data security risk assessments, and to rectify and eliminate potential risks;

(3) Report to relevant government agencies and cybersecurity administrations the handling of data security protection and incidents;

(4) Accept and handle the complaints and reports of users.

Network operators shall provide necessary recourse to the person responsible for the data security to enable the independent performance of such responsibilities and obligations.

第三章　数据处理使用
Chapter III Process and Use of Data

第十九条 网络运营者应当参照国家有关标准，采用数据分类、备份、加密等措施加强对个人信息和重要数据保护。

Article 19 Network operators shall take measures such as data categorization, data back-up and encryption to strengthen the protection of personal information and important data.

第二十条 网络运营者保存个人信息不应超出收集使用规则中的保存期限，用户注销账号后应当及时删除其个人信息，经过处理无法关联到特定个人且不能复原（以下称匿名化处理）的除外。

Article 20 The retention of personal information by the network operator shall not exceed the retention period provided in the rules for collection and use. Personal data shall be timely deleted after the users close their accounts, unless the personal information has been processed to make it impossible to identify a specific person from the information and such information cannot be processed to re-identify such a person (hereinafter referred to as "anonymization").

第二十一条 网络运营者收到有关个人信息查询、更正、删除以及用户注销账号请求时，应当在合理时间和代价范围内予以查询、更正、删除或注销账号。

Article 21 Network operators shall, upon receipt of requests to access, correct, and delete personal information and close accounts, fulfill such requests within a reasonable time and at reasonable cost.

第二十二条 网络运营者不得违反收集使用规则使用个人信息。因业务需要，确需扩大个人信息使用范围的，应当征得个人信息主体同意。

Article 22 Network operators shall not use personal information in violation of the rules for collection and use. If it is necessary to expand the scope of the use due to business needs, network operators shall obtain consent from personal information subjects.

第二十三条 网络运营者利用用户数据和算法推送新闻信息、商业广告等（以下简称“定向推送”），应当以明显方式标明“定推”字样，为用户提供停止接收定向推送信息的功能；用户选择停止接收定向推送信息时，应当停止推送，并删除已经收集的设备识别码等用户数据和个人信息。

网络运营者开展定向推送活动应遵守法律、行政法规，尊重社会公德、商业道德、公序良俗，诚实守信，严禁歧视、欺诈等行为。

Article 23 Network operators shall, when using user data and algorithms to push news and commercial advertisements, clearly identify the word “targeted push” and provide an option for users to reject the targeted push information. If the user chooses not to receive targeted push information, network operators shall stop the push and erase the device identification code and other collected user data as well as any personal information.

Network operators shall, when conducting targeted push activities, comply with laws and regulations, respect social morality and business ethics, abide by public order and good morals, and be honest and diligent. All discriminatory and fraudulent acts shall be prohibited.

第二十四条 网络运营者利用大数据、人工智能等技术自动合成新闻、博文、帖子、评论等信息，应以明显方式标明“合成”字样；不得以谋取利益或损害他人利益为目的自动合成信息。

Article 24 Network operators shall, when using big data, artificial intelligence or other technologies to automatically synthesize information such as news, blog posts, posts and comments, clearly identify the word “synthesis.” Network operators shall not automatically synthesize information for the purposes of making profits or damaging the interests of any other person.

第二十五条 网络运营者应采取措施督促提醒用户对自己的网络行为负责、加强自律，对于用户通过社交网络转发他人制作的信息，应自动标注信息制作者在该社交网络上的账户或不可更改的用户标识。

Article 25 Network operators shall take measures to urge and remind users to be responsible for their network behavior and strengthen self-regulation. When users forward information made by any other person, network operators shall automatically suffix the social network account or unchangeable user identification of the information producer.

第二十六条 网络运营者接到相关假冒、仿冒、盗用他人名义发布信息的举报投诉时，应当及时响应，一旦核实立即停止传播并作删除处理。

Article 26 Network operators shall, upon receipt of reports and complaints on faking, counterfeiting or embezzling the release of any information in the name of any other person, shall respond in a timely manner, stop spreading the information, and erase it once verified.

第二十七条 网络运营者向他人提供个人信息前，应当评估可能带来的安全风险，并征得个

人信息主体同意。下列情况除外：

（一）从合法公开渠道收集且不明显违背个人信息主体意愿；

（二）个人信息主体主动公开；

（三）经过匿名化处理；

（四）执法机关依法履行职责所必需；

（五）维护国家安全、社会公共利益、个人信息主体生命安全所必需。

Article 27 Network operators shall, before providing personal information to any other person, assess the security risks and obtain the consent of the data subject, except for the following circumstances:

(1) the personal information is collected from legal public channels and sharing of it is consistent with the understanding of the data subjects;
(2) the personal information was voluntarily disclosed by data subjects;
(3) the personal information has been anonymized;
(4) the sharing is necessary for the performance of responsibilities and functions of law enforcement agencies in accordance with law;
(5) the sharing is necessary for safeguarding national security, social and public interest, or protecting the lives of data subjects.

第二十八条 网络运营者发布、共享、交易或向境外提供重要数据前，应当评估可能带来的安全风险，并报经行业主管监管部门同意；行业主管监管部门不明确的，应经省级网信部门批准。

向境外提供个人信息按有关规定执行。

Article 28 Network operators shall assess potential security risks before publishing, sharing or selling important data or transferring such data across borders, and report to the competent regulatory department for approval. If the identity of the competent regulator is unclear, network operators shall report to the cybersecurity administration at the provincial level for approval.

Overseas provision of personal information shall be implemented according to the relevant provisions.

第二十九条 境内用户访问境内互联网的，其流量不得被路由到境外。

Article 29 When a domestic user is visiting the domestic internet, its flow shall not be routed overseas.

第三十条 网络运营者对接入其平台的第三方应用，应明确数据安全要求和责任，督促监督第三方应用运营者加强数据安全管理。第三方应用发生数据安全事件对用户造成损失的，网络运营者应当承担部分或全部责任，除非网络运营者能够证明无过错。

Article 30 Network operators shall specify data security requirements and responsibilities for third-party apps connected to platforms and supervise third-party app

operators to strengthen data security management. If data security incidents occur due to third-party apps and cause damage to users, network operators shall assume all or part of the liability unless they are able to prove that they are not at fault.

第三十一条 网络运营者兼并、重组、破产的，数据承接方应承接数据安全责任和义务。没有数据承接方的，应当对数据作删除处理。法律、行政法规另有规定的，从其规定。

Article 31 If network operators undergo mergers, acquisitions, reorganizations or bankruptcy, the data recipient shall assume the data security responsibility and obligations of the network operator. If there is no data recipient, network operators shall delete relevant data. In case of inconformity with the provisions of the laws and regulations, the latter shall prevail.

第三十二条 网络运营者分析利用所掌握的数据资源，发布市场预测、统计信息、个人和企业信用等信息，不得影响国家安全、经济运行、社会稳定，不得损害他人合法权益。

Article 32 Network operators shall not, when analyzing and using the data resources in their possession, publish market predictions, statistics, personal and enterprise credit, endanger national security, economic operation, social stability or damage lawful rights and interests of any other person.

第四章　数据安全监督管理
Chapter IV Supervision and Regulation of Data Security

第三十三条 网信部门在履行职责中，发现网络运营者数据安全管理责任落实不到位，应按照规定的权限和程序约谈网络运营者的主要负责人，督促整改。

Article 33 When a cyberspace administration, in the course of performing its functions and duties, finds that a network operator has failed to implement data security management obligations, the cybersecurity administration shall summon the main responsible person of the network operators and urge it to make rectification.

第三十四条 国家鼓励网络运营者自愿通过数据安全管理认证和应用程序安全认证，鼓励搜索引擎、应用商店等明确标识并优先推荐通过认证的应用程序。

国家网信部门会同国务院市场监督管理部门，指导国家网络安全审查与认证机构，组织数据安全管理认证和应用程序安全认证工作。

Article 34 The state shall encourage network operators to voluntarily pass data security management authentication and application security authentication for their applications, and shall encourage search engines, application stores and others to clearly identify and give priority to applications that have passed the authentication.

The national cyberspace administration shall direct national cybersecurity review and

authentication institutions, organize data security management authentications and application security authentications in conjunction with the market regulatory department of the State Council.

第三十五条 发生个人信息泄露、毁损、丢失等数据安全事件，或者发生数据安全事件风险明显加大时，网络运营者应当立即采取补救措施，及时以电话、短信、邮件或信函等方式告知个人信息主体，并按要求向行业主管监管部门和网信部门报告。

Article 35 In security incidents where personal information has been divulged, damaged or lost, or the risk of data security incidents has increased significantly, network operators shall immediately take remedial measures to inform users in a timely manner through phone calls, messages, emails, letters or other means, and report it to the competent supervising department and cyberspace administration according to relevant requirements.

第三十六条 国务院有关主管部门为履行维护国家安全、社会管理、经济调控等职责需要，依照法律、行政法规的规定，要求网络运营者提供掌握的相关数据的，网络运营者应当予以提供。

国务院有关主管部门对网络运营者提供的数据负有安全保护责任，不得用于与履行职责无关的用途。

Article 36 In order to perform national security, social management, economic control and other functions and duties, when the relevant competent departments of the State Council require network operators to provide relevant data in its possession in accordance with relevant laws and administrative regulations, the network operators shall provide such data.

The relevant competent departments of the State Council shall assume the responsibility of security protection of the data provided by network operators, and shall not use the data for purposes unrelated to the performance of its functions.

第三十七条 网络运营者违反本办法规定的，由有关部门依照相关法律、行政法规的规定，根据情节给予公开曝光、没收违法所得、暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或吊销营业执照等处罚；构成犯罪的，依法追究刑事责任。

Article 37 Where a network operator violates the provision of this measure, the competent department shall, in accordance with relevant laws and administrative regulations, take disciplinary actions such as confiscating the violator's illegal income therefrom, suspending relevant business operation, ceasing business operation for rectification, shutting down the website, revoking the relevant business permit or business license or other punishments as the case may be. If the violation constitutes a crime, the violator will be subject to criminal liability in accordance with the law.

第五章　附则
Chapter V Supplemental Provisions

第三十八条 本办法下列用语的含义：

（一）网络运营者，是指网络的所有者、管理者和网络服务提供者。

（二）网络数据，是指通过网络收集、存储、传输、处理和产生的各种电子数据。

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

（四）个人信息主体，是指个人信息所标识或关联到的自然人。

（五）重要数据，是指一旦泄露可能直接影响国家安全、经济安全、社会稳定、公共健康和安全的数据，如未公开的政府信息，大面积人口、基因健康、地理、矿产资源等。重要数据一般不包括企业生产经营和内部管理信息、个人信息等。

Article 38 In this Measures, the following terms shall have the meanings as follows:

(1) “Network operator” means the owners and administrators of the network as well as network service providers.

(2) “Network data” means all kinds of electronic data collected, stored, transmitted, processed and generated through the network.

(3) “Personal information” means all kinds of information recorded in electronic or other forms, which can be used, independently or in combination with other information, to identify a natural person's personal identity, including but not limited to the natural person's name, date of birth, identity certificate number, biometric information, address and telephone number.

(4) “Personal information subject” means the natural person identified or connected by the personal information.

(5) “Important data” means the kind of data, if divulged, may directly affect national security, economic security, social stability, public health and security, such as undisclosed government information, large-scale population, genetic health, geographic, mineral resources. Important data usually doesn’t include information related to the production and operation of enterprises, internal management information or personal information.

第三十九条 涉及国家秘密信息、密码使用的数据活动，按照国家有关规定执行。

Article 39 Data activities involving state secrets or the use of encryption shall comply with the relevant provisions of the state.

第四十条 本办法自 年 月 日起施行。

Article 40 This Measures shall take effect on _____.