Hogan Lovells unofficial translation

Data Security Administrative Measures

June 2019

Hogan Lovells

数据安全管理办法
DATA SECURITY ADMINISTRATIVE MEASURES

（征求意见稿）
(Draft for Comments)

第一章 总则

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。

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。

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。

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。

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

Chapter I General Provisions

Article 1 These Measures are formulated for the purposes of safeguarding national security and the public interest, protecting the legitimate rights and interests of citizens, legal entities and other organizations in cyberspace, and protecting the security of personal information and important data, in accordance with the *People's Republic of China Cybersecurity Law* as well as other laws and regulations.

Article 2 These Measures apply to activities such as the collection, storage, transmission, processing and use of data (hereinafter referred to as "**data activities**"), as well as the protection, regulation and administration of data security, within the People's Republic of China (the "**PRC**"). Pure household and personal affairs are not covered by these Measures.

Where laws or administrative regulations provide otherwise, such provisions shall apply.

Article 3 The State attaches equal importance to data security protection and development, encourages the research and development of data security protection technologies, actively promotes the development and utilization of data resources, and safeguards the orderly and free flow of data in accordance with law.

Article 4 The State adopts measures to monitor, protect against and address data security risks and threats from both within and outside the PRC, so as to protect data from leakage, theft, tampering, damage, illegal use and so forth, and penalize, in accordance with law, illegal and criminal activities which jeopardize data security.

Article 5 Under the leadership of the Central Cyberspace Affairs Commission, the State network information departments shall be responsible for the overall planning, coordination, direction and supervision of the efforts to protect the security of personal information and important data.

The network information departments at and above the local (or municipality) level shall direct and supervise the efforts to protect the security of personal information and

要数据安全保护工作。

important data within their own jurisdictions based on their duties.

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 must perform their obligations to protect data security, establish an accountability and assessment system for data security management, formulate data security plans, implement technical safeguards for data security, conduct data security risk assessments, formulate emergency response plans for cyber security incidents, promptly 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 who collect or use personal information via websites, applications or such other products must formulate and make public separate rules for the collection and use of personal information. Such rules may be included in the privacy policies of the websites, applications or products involved, or otherwise provided to users.

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：

Article 8 The rules for the collection and use of personal information must be clear, specific, written in simple and plain language, easily accessible and emphasize the following:

（一） 网络运营者基本信息；

(1) basic information about the network operator;

（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；

(2) the names and contact details of the principal of the network operator and the person in charge of data security;

（三） 收集使用个人信息的目的、种类、数量、频度、方式、范围等；

(3) the purposes, types, quantity, frequency, methods and scope of the collection and use of personal information;

（四） 个人信息保存地点、期限及到期后的处理方式；

(4) the storage location and retention period of personal information, as well as how personal information will be disposed of upon the expiration of the retention period;

（五） 向他人提供个人信息的规则，如果向他人提供的；

(5) the rules on providing personal information to others (if applicable);

（六） 个人信息安全保护策略等相关信息；

(6) strategies for the protection of personal information security and other relevant information;

（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；

(7) the channels and methods for personal information subjects to revoke consent and access, modify or delete personal information;

（八） 投诉、举报渠道和方法等；

(8) complaint and reporting channels and methods;

（九） 法律、行政法规规定的其他内容。

(9) such other contents as provided by laws or administrative 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 Where the rules for the collection and use of personal information are included in a privacy policy, such rules shall be relatively focused with clear instructions for ease of understanding. In addition, network operators may collect personal information only if the user is aware of and explicitly consents to such rules.

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 must strictly abide by the rules for the collection and use of personal information; the functionality of websites or applications to collect or use personal information shall be designed in line with their privacy policies and adjusted synchronously.

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。

Article 11 Network operators must not coerce or mislead personal information subjects into consenting to the operators' collection of personal information by way of default authorization, function bundling or such other means under the pretext of improving service quality, enhancing user experience, targeted information push, researching and developing new products or such other reasons.

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。

Once a personal information subject consents to the collection of personal information required for ensuring the operation of the core services and functions of the network product, the network operator must provide such core services and functions to the personal information subject, and must not refuse to do so on the grounds that the personal information subject refuses to consent or revokes his/her consent to the collection of information other than that specified above.

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 Where personal information on a minor under the age of 14 is collected, consent must be obtained from of his/her guardian.

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 must not engage in discriminatory treatment (including disparities in service quality, pricing and so forth) against personal information subjects based on whether the personal information subjects authorize the collection of personal information and the scope of such authorization.

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 who obtain personal information through other channels are subject to the same responsibilities and obligations to protect such personal information as those in the case of direct collection.

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

Article 15 Network operators who collect important data or sensitive personal information for business purposes must carry out record-filling procedures with the local network information department. Materials to be filed for record include the rules for the collection and

用的目的、规模、方式、范围、类型、期限等，不包括数据内容本身。

use of such information, as well as the purposes, scale, methods, scope, types, periods and other aspects of such collection and use, but do not include the 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 When accessing and collecting website data by automated means, network operators must not interfere with the normal operation of the website; where such activities severely affect the operation of the website (e.g. the traffic generated by accessing and collecting data through automated means exceeds one third of the average daily traffic of the website), and the website requires a cease of such activities, the network operator concerned must act accordingly.

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。

Article 17 Network operators who collect important data or sensitive personal information for business purposes must designate a person in charge of data security.

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。

The person in charge of data security must have relevant management experience and data security expertise, participate in important decision-making process with respect to data activities and report directly to the principal of the network operator.

第十八条 数据安全责任人履行下列职责：

Article 18 Persons in charge of data security are to perform the following duties:

（一）组织制定数据保护计划并督促落实；

(1) to be responsible for the development, and to procure and supervise the implementation, of data protection plans;

（二）组织开展数据安全风险评估，督促整改安全隐患；

(2) to be responsible for data security risk assessments, to procure and supervise the rectification of latent security hazards;

（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；

(3) to report to the competent authorities and network information departments on data security protection and the handling of related incidents;

（四）受理并处理用户投诉和举报。

(4) to accept and handle user complaints and reports.

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。

Network operators must provide the persons in charge of data security with the necessary resources to ensure their independence in performing their duties.

第三章 数据处理使用

Chapter III Data Processing and Use

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 must adopt data classification, backup, encryption and such other measures with reference to relevant national standards 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 Network operators must not retain personal information beyond the retention period specified in their rules for the collection and use of personal information, and must delete the personal information belonging to a user promptly after such user cancels his/her account, except information which has been processed such that it can neither be linked to the specific individual nor restored (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 Upon receipt of a request for accessing, correcting or deleting personal information or for cancelling an account from a user, network operators must permit such access, effect such correction or deletion or cancel the account within a reasonable period for reasonable consideration.

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 must not use personal information in violation of the rules for the collection and use of the same. Where it is necessary to expand the scope of use of personal information for business needs, consent must be obtained from the personal information subject.

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。

Article 23 Where a network operator uses user data and algorithms to push news, information, commercial advertisements and so forth (hereinafter referred to as "**targeted push**"), the legend "Targeted Push" must be shown in a conspicuous manner, and users must be provided with a function to stop receiving targeted pushes. Where a user opts to stop receiving targeted pushes, the network operator must stop sending such pushes and delete the user data and personal information (such as device identifier) which have already been collected.

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。

Network operators sending targeted pushes must abide by laws and administrative regulations, respect social mores, business ethics, public order and good customs, and act with integrity, and must not engage in discrimination, fraud or other such conduct.

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 Where a network operator uses big data, artificial intelligence or other such technologies to automatically synthesize news, blog articles, posts, comments or such other information, the legend "Synthetic" must be shown in a conspicuous manner. Network operators must not automatically synthesize any information for the purposes of gaining benefits or harming the interests of others.

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 must adopt measures to urge and remind users to take responsibility for their own cyber behaviour, to strengthen self-discipline, and to take the initiative to indicate the information originator's account on the social network or the unchangeable user ID where the user forwards information generated by others.

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 Upon receipt of any report or complaint that certain information has been posted under a fake, fraudulent or misappropriated name, network operators must respond in a timely manner and immediately stop disseminating and delete such information once the complaint or report is 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：

Article 27 Prior to providing personal information to others, network operators must assess the potential security risks and obtain the consent of the personal information subject except where:

（一） 从合法公开渠道收集且不明显违背个人信息主体意愿；

(1) the personal information was collected from legitimate and public channels in a manner that is not evidently against the will of the personal information subject;

（二） 个人信息主体主动公开；

(2) the personal information has been made public by the personal information subject voluntarily;

（三） 经过匿名化处理；

(3) the personal information has undergone anonymization;

（四） 执法机关依法履行职责所必需；

(4) the provision is necessary for law enforcement agencies to perform their duties in accordance with law;

（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。

(5) the provision is necessary for the purposes of safeguarding national security, social and public interests, or the life and safety of the personal information subject.

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。

Article 28 Prior to distributing, sharing or trading any important data or providing any important data abroad, network operators must assess the potential security risks and obtain the approval of the competent industry regulatory authority; where the competent industry regulatory authority is in doubt, the approval of the provincial network information department must be obtained.

向境外提供个人信息按有关规定执行。

The provision of personal information abroad shall be subject to the relevant regulations.

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 Where a domestic user surfs the Internet domestically, the traffic must not be routed abroad.

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 must specify the data security requirements and responsibilities for third party applications connected to the operators' platform, urge the third party application operators to strengthen their data security management, and exercise oversight over such management. Where a data security incident occurs to any such third party application, thereby causing any loss to any user, the network operator must bear the liability partially or fully, unless the network operator is able to prove that it is 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 Where a network operator undergoes a merger, restructuring or bankruptcy, the party taking over the data must also take over the data security responsibilities and obligations. Where no one is to take over the data, the data must be deleted. Where laws or administrative regulations provide otherwise, such provisions shall apply.

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 When analysing or using available data resources to publish market forecasts, statistical information, personal and corporate credit information or such other information, network operators must not compromise national security, the operation of the economy or social stability, and must not harm others' legitimate rights and interests.

第四章 数据安全监督管理

Chapter IV Data Security Regulation and Administration

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 If a network information department, in performing its duties, discovers any failure on the part of a network operator to adequately perform its responsibilities with respect to data security management, the network information department shall, in accordance with its authority and the prescribed procedures, interview the principal of the network operator and urge the network operator to make rectifications.

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。

Article 34 The State encourages network operators to voluntarily obtain data security management certification and application security certification, and encourages search engines, application stores or such other operators to clearly identify and recommend certified applications.

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。

The State network information departments, together with the market supervision and administration departments under the State Council, shall provide guidance to the State network security audit and certification agencies on work relating to data security management certification and application security certification.

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 the event of a data security incident (such as the leakage, damage or loss of personal information), or in the event of a significantly increased risk of data security incidents, network operators must immediately adopt remedial measures, promptly inform the personal information subjects concerned by telephone, text message, email, mail or otherwise, and report such incident or risk to the competent industry regulatory authority and network information departments as required.

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

Article 36 Where a competent department under the State Council requires a network operator to provide relevant data in its possession pursuant to laws or

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。

administrative regulations for the purposes of safeguarding national security, administering social affairs, implementing economic regulatory measures, and discharging such other duties, the network operator must comply.

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。

The competent department under the State Council shall be responsible for protecting the security of the data provided by the network operator, and shall not use the same for any purpose unrelated to the performance of the department's duties.

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 Any network operator found to have violated the provisions of these Measures shall be subject to penalties by the competent authority pursuant to applicable laws or administrative regulations; such penalties range from having its violation publicly exposed, having its illegal gains confiscated, being ordered to suspend operations, close down its business pending rectification or shut down its website(s), to having its business permit(s) or business licence revoked, depending on the severity of the violation; where the violation constitutes a criminal offence, the network operator shall be pursued for criminal liability in accordance with 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：

Article 38 In these Measures, the following terms and expressions shall have the meanings ascribed to them below:

（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。

(1) "Network operator" means an owner or manager of any cyber network, and a network service provider.

（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。

(2) "Network data" means all types of electronic data collected, stored, transmitted, processed and generated via a network.

（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。

(3) "Personal information " means any information, recorded electronically or otherwise, which can be used on its own or in combination with other information to identify a natural person, including but not limited to his/her name, date of birth, identification card number, personal biometric information, address, telephone number and so forth.

（四） 个人信息主体，是指个人信息所标识或关联到的自然人。

(4) "Personal information subject" means the natural person who is identified by or linked to personal information.

（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

(5) "Important data" means data whose leakage may directly impact national security, economic security, social stability, or public health and

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。	security, such as non-public government information, and information on large area population, genetic health, geography and mineral resources. In general, important data does not include information and personal information related to the production, operations and internal management of an enterprise.
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 passwords shall be subject to the relevant regulations of the State.
第四十条 本办法自 年 月 日起施行。	**Article 40** These measures shall come into force on _____.