迈林法律评论

2024 年 10 月

MYLINK
迈林律师事务所

公司实务

《网络数据安全管理条例》合规义务解读

Interpretation of Compliance Obligations under the Regulation on Cyber Data Security Management

前言

Preamble

《网络数据安全管理条例》(以下简称《条例》) 于 2024 年 9 月 30 日正式发布，并将于 2025 年 1 月 1 日起正式施行。这一行政法规以《网络安全法》《数据安全法》和《个人信息保护法》作为上位法依据，与之共同构成了我国网络数据安全法律体系的主干。

The Regulation on Cyber Data Security Management (hereinafter referred to as the "Regulation") was officially issued on September 30, 2024 and will come into force on January 1, 2025. This administrative regulation is based on the Cyber Security Law, the Data Security Law and the Personal Information Protection Law, which together constitute the backbone of China's cyber data security legal system.

I. 哪些行为受到《条例》的规制?
Activities subject to the Regulation

(1)在中国境内开展网络数据处理活动及其安全监督管理；

Carrying out cyber data processing activities in China and its safety supervision management;

(2)在境外处理境内自然人个人信息的活动，且符合：以向境内自然人提供产品或者服务为目的，或涉及分析、评估境内自然人的行为的，或法律、行政法规规定的其他情形；

Activities involving processing personal information of natural persons in China from abroad, and meet the following requirements: the purpose is to provide products or services to domestic natural persons, or involve analyzing or evaluating the behavior of domestic natural persons, or other circumstances specified by laws and administrative regulations;

(3)在境外开展网络数据处理活动，且损害中国国家安全、公共利益或者公民、组织合法权益的。
Carrying out cyber data processing activities outside China that damages China's national security, public interests or the legitimate rights and interests of its citizens or organizations.

II. 针对不同的网络数据处理者，《条例》规定了哪些合规义务?
Compliance obligations imposed for different cyber data processors under the Regulation

根据《条例》，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。该定义突出处理者对处理活动的控制权和决定性，有助于厘清参与数据处理活动的不同主体之间的责任义务。
According to the Regulation, a cyber data processor refers to an individual or organization that independently determines the purpose and method of processing in cyber data processing activities. This definition highlights the processor's control and decisiveness over the processing activities, and helps to clarify the responsibilities and obligations between different entities involved in data processing activities.

基于数据分级分类的规则，《条例》除对网络数据处理活动作出【一般规定】外，同时从【个人信息保护】和【重要数据安全】两个方面切入，提出更为特殊的规制要求。此外，《条例》亦对【网络数据跨境安全管理】和【网络平台服务提供者义务】规定了额外的管理要求。
Based on the rules of data classification and grading, in addition to the [General Provisions] on cyber data processing activities, the Regulation also puts forward more special regulatory requirements from the aspects of [Personal Information Protection] and [Important Data Security]. In addition, the Regulation also provides additional regulatory requirements for [cross-border security management of cyber data] and [obligations of cyber platform service providers].

(1)在“个人信息保护”方面，企业应关注的《条例》变化
Changes in the Regulation you should pay attention to regarding "personal information protection"

《条例》第三章重点对《个人信息保护法》的规定进行重申和细化，其中值得关注的变化包括：
Chapter III of the Regulation focuses on reiterating and refining the provisions of the Personal Information Protection Law, with noteworthy changes including:

条文 Provisions	主要变化 Main changes

第二十一条 Article 21	**新增个人信息处理规则（即我们通常所提及的“隐私政策”等文件）中有关保存期限、收集和共享个人信息等要求：** **New requirements on the retention period, collection and sharing of personal information to the personal information processing rules (namely, "privacy policies" or similar documents):** • 保存期限难以确定的，应当明确保存期限的确定方法； If the retention period is difficult to determine, the method for determining the retention period should be clearly stated; • 以清单等形式列明收集和向其他网络数据处理者提供个人信息的相关情况。 Making a checklist outlining the details of personal information collected and provided to other cyber data processors; • 强调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。 It is emphasized that the rules for processing personal information should be displayed publicly, easily accessible and placed in a prominent location.
第二十四条 Article 24	**新增需要删除个人信息或者匿名化处理的场景：** **New scenarios that require deletion of personal information or anonymization:** • 因使用自动化采集技术等（例如应用爬虫技术）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； The use of automated collection technology (such as the use of crawler technology) cannot avoid the collection of unnecessary personal information or personal information for which the individual’s consent has not been obtained in accordance with the law; • 个人注销账号 Personal account cancellation
第二十五条 Article 25	**细化行使“个人信息转移请求权”应满足的条件。** **Clarify the conditions that must be met to exercise the "right to request the transfer of personal information".**
第二十六条 Article 26	**明确境内代表报送信息的渠道：** **Clarify the channels for domestic representatives to submit information:** 落入管辖范围的境外个人信息处理者应当在境内设立专门机构或指定代表，并将有关机构的名称或者代表的姓名、联系方式等报送给所在地设区的市级网信部门。 Foreign personal information processors subject to the Regulation shall establish special institutions or designate representatives in China and report the name of the relevant institution or the name and contact information of the representative to the local municipal cyberspace administration bureau.
第二十七条 Article 27	**强化网络数据处理者定期进行合规审计的要求。** **Strengthen the requirement for cyber data processors to conduct regular compliance audits.**

第二十八条 Article 28	**《条例》提高个人信息类重要数据的认定数量门槛：** **The Regulation raise the threshold for identifying important data related to personal information.** 从 100 万提升为 1000 万，并规定处理 1000 万人以上个人信息的网络数据处理者还应遵守对重要数据的处理者作出的规定。 The threshold is raised from 1 million to 10 million, and cyber data processors handling personal information of over 10 million individuals must also comply with regulations for important data processors.

企业应当做什么?
What should you do?

- 核查企业制定的隐私政策等个人信息处理规则是否符合《条例》要求。
  Verify whether the privacy policies and similar rules of your company are consistent with the new requirements of the Regulation.

- 如存在不一致或有遗漏之处，及时比对《条例》中的相关规定（尤其是新增条款）更新文本内容，并以公开、显著的方式进行公开。
  If there are inconsistencies or omissions, promptly refer to the relevant provisions in the Regulation to update its privacy policy.

(2)如涉及“重要数据安全”，企业有哪些合规义务?
Compliance obligations in relation to “critical data security”

根据《条例》规定，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。因此，重要数据处理者受到更严格的监管。
According to the Regulation, critical data refers to data that, due to its specific field, specific group, specific region, or certain level of precision and scale, may directly threaten national security, economic operation, social stability, public health, and safety if altered, destroyed, leaked, illegally accessed, or misused. As a result, processors of critical data are subject to stricter regulation.

重要数据处理者的主要义务包括：
The main obligations of critical data processors include:

条文 **Provisions**	**主要义务内容** **Content of the main obligations**

第三十条 Article 30	应当明确网络数据安全负责人和网络数据安全管理机构。 The person in charge of cyber data security and the cyber data security management agency should be clearly defined. 《条例》同时对上述安全管理机构的责任，以及安全负责人的任职要求作出细化。 The Regulation also details the responsibilities of the above-mentioned security management agency and the job requirements for the person in charge of security.
第三十一条 Article 31	提供、委托处理、共同处理重要数据前，应当进行风险评估（属于履行法定职责或者法定义务的除外）。 Risk assessment should be carried out before providing, entrusting processing, or jointly processing critical data (except for those fulfilling statutory duties or obligations). 《条例》同时规定了上述风险评估的重点评估内容。 The Regulation also sets out the key assessment elements for such risk assessment.
第三十二条 Article 32	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，并向主管机关报送。 Where the security of critical data may be affected due to merger, separation, dissolution, bankruptcy of the company, etc., measures shall be taken to ensure the security of cyber data and reported to the competent authorities.
第三十三条 Article 33	应当每年度对其网络数据处理活动开展风险评估，并向主管机关报送。 Risk assessment of its cyber data processing activities should be conducted annually and reported to the relevant authorities. 《条例》同时规定了上述风险评估报告应包括的内容。 The Regulation also stipulates the contents to be included in such risk assessment report.

(3)《条例》对“数据跨境安全管理”有哪些特殊规定?

Special provisions in the Regulation on “cross-border security management of data”

《条例》第五章规定有关网络数据跨境安全管理的相关要求，其中值得关注的主要规定有：

Chapter V of the Regulation sets out the relevant requirements in relation to cross-border security management of cyber data, of which the main provisions worth noting include:

条文 Provisions	主要内容 Main Content
第三十五条 Article 35	**个人信息出境：** **Cross-border transfer of personal information:**

	明确列举合法出境的八种情形： enumerating eight scenarios for lawful data cross-border transfer, including: ● 通过国家网信部门组织的数据出境安全评估； ● 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； ● 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； ● 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； ● 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； ● 为履行法定职责或者法定义务，确需向境外提供个人信息； ● 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； ● 法律、行政法规或者国家网信部门规定的其他条件。 ● Passing security assessment of data cross-border transfer organized by the national cyberspace administration; ● Obtaining personal information protection certification from professional institution agencies in accordance with the regulations of the national cyberspace administration; ● Following the provisions of the standard contract for personal information cross-border transfer formulated by the national cyberspace administration; ● Providing personal information to overseas parties in order to conclude and perform a contract where the individual is a party; ● Providing employee personal information abroad for cross-border human resources management in accordance with labor regulations and collective contracts; ● Providing personal information abroad in order to perform statutory duties or obligations; ● Providing personal information abroad in order to protect the life, health and property of natural persons in emergency situations; ● Other conditions stipulated by laws, administrative regulations or national cyberspace administration
第三十七、 第三十八条 Article 37 and Article 38	**重要数据出境：** **Cross-border transfer of critical data:** 应通过数据出境安全评估，且通过安全评估的数据出境不得超出原评估时明确范围。 Data export security assessment should be passed, and the exported data which pass through the security assessment should not exceed the scope specified in the original assessment.

(4)《条例》对网络平台服务提供者提出哪些要求?
Requirements in the Regulation for internet platform service providers

《条例》单设第六章明确网络平台服务提供者义务，并规定了一般网络平台服务提供者、大型网络平台服务提供者的责任和义务。

The Regulation set up a separate Chapter VI to clarify the obligations for internet platform service providers and stipulate the responsibilities and obligations of general internet platform service providers and large-scale internet platform service providers respectively.

条文 Provisions	主要内容 Main Content
第四十条 Article 40	明确网络平台服务提供者，以及预装 app 的智能终端设备生产者，应承担的主体责任 Clarify the subject responsibilities to be borne by internet platform service providers, as well as producers of smart terminal equipment with pre-installed apps
第四十一条 Article 41	明确应用程序分发服务的网络平台服务提供者应承担的合规义务 Clarify the compliance obligations of internet platform service providers engaging in application distribution services
第四十二、四十三条 Article 42 and Article 42	强调网络平台服务提供者的其他合规义务 Emphasize other compliance obligations for internet platform service providers
第四十四至四十六条、第六十二条 Articles 44-46 and Article 62	在对“大型网络平台”作出定义的同时，着重强调大型网络平台应承担的法律合规义务 While defining “large internet platforms”, the legal compliance obligations that large internet platforms should bear are emphasized.

(5)网络数据处理者还应承担的一般性义务
General obligations imposed for cyber data processors

《条例》第二章亦对网络数据处理者作出一般性义务规定，包括：

Chapter II of the Regulation also stipulates general obligations for cyber data processors,

including:

条文 **Provisions**	主要内容 **Main Content**
第八条 Article 8	明确禁止非法网络数据处理活动，并列举具体的非法表现形式 Explicitly prohibit illegal cyber data processing activities and enumerate specific prohibited behaviors
第十条 Article 10	存在安全缺陷、漏洞等风险，且涉及危害国家安全、公共利益，应当在 24 小时内向有关主管部门报告 If there are risks such as security defects and loopholes, which may endanger national security and public interests, they should be reported to the competent authorities within 24 hours.
第十一条 Article 11	建立健全网络数据安全事件应急预案，在发生安全事件时，及时采取措施并报告 Establish and improve emergency response plan for cyber data security incidents, and take timely measures and report in the event when security incidents occur.
第十二条 Article 12	明确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具体法律要求 Clarify the specific law requirements when providing other cyber data processors with or entrusting other cyber data processors to process personal information and critical data
第十三条 Article 13	强调国家安全审查义务 Emphasize the obligations for national security review.
第十四条 Article 14	强调数据转移时网络数据接收方的义务 Emphasize the obligations of cyber data recipients in the event of data transfer
第十五至十七条 Article 15-17	为国家机关、关键信息基础设施运营者提供服务时的具体法律要求 Specific legal requirements when providing services to state agencies and operators of critical information infrastructure

III. 违反《条例》，企业可能面临哪些法律责任?
Legal liabilities in case of violation to the Regulation.

《条例》专章针对企业在个人信息保护和重要数据管理方面设置了明确的责任条款和对应罚则。责任类型包括责令改正，给予警告，没收违法所得，罚款，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以相应罚款等。在严重的特定情形下，企业可能面临 1000 万元以下罚款、其直接负责的主

管人员和其他直接责任人员将面临 100 万元以下罚款。

The Regulation puts a special chapter setting up liability clauses and corresponding penalties for enterprises in terms of personal information protection and critical data management. Possible liability includes ordering rectification, giving warnings, confiscating illegal gains, imposing fines, ordering suspension of related business, suspension of business for rectification, revocation of related business licenses or revocation of business licenses, and imposing corresponding fines against directly responsible persons. In serious specific circumstances, the enterprise may face fines of less than CNY 10,000,000, and the directly responsible person may face fines of less than CNY 1,000,000.

如您对本文有任何问题，请联系：

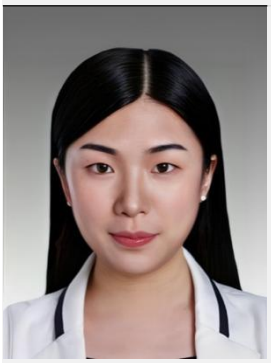
If you have any questions about this article, please contact us via:

陈祥龙，执行合伙人

Erex Chen, Managing Partner

Tel: +86 21 68556511

Email: erexchen@mylinklaw.com



张丽丽，律师

Doris Zhang, Attorney

Tel: +86 21 68556500

Email: doriszhang@mylinklaw.com