2025.12.19

中国风险消息<2025 No.3>

中国《网络数据安全管理条例》相关解读

【要点】

- 《网络数据安全管理条例》(以下简称《条例》)，由中国国务院于 2024 年 9 月发布，自 2025 年 1 月 1 日起正式施行，标志着中国在网络数据安全管理领域的进一步完善，对在华开展业务的所有企业，包括在华企业，都有着深远的影响。
- 日资企业（特别是有大量网络数据的公司)有必要了解重点内容，并对相关管理制度、合规审查、教育培训等方面采取应对措施。
- 本文中，在介绍《条例》重点内容的基础上，将针对背景意义、与相关法律的比较、对企业影响及应对建议等方面进行整理、说明。

1. 《条例》的背景意义

（1）国际范围

当前，全球范围内网络安全形势日益严峻，美国和欧洲不断出台新的网络安全保护相关法律，建立日趋严格的数据监管体系。

美国方面，近年来先后推出《网络安全信息共享法》《云法案》《数据安全和保护法案》等一系列法律法规。其中，《云法案》要求美国企业及在美运营的外国企业配合提供存储在全球范围内的数据。而《数据安全和保护法案》则对个人数据的收集、使用、存储和传输提出了更严格的要求，强化了企业的数据安全保护责任。

欧洲在网络安全领域的立法更为系统和严格。《通用数据保护条例》（GDPR）自 2018 年实施以来，以规定严苛和处罚力度大（最高可达全球年营业额的 4%或 2000 万欧元）而闻名全球。此后，欧洲又陆续出台《网络安全法》《数字服务法》《数字市场法》等，进一步加强对网络空间的监管，强化平台责任，保障数据安全和用户权益。

在这样的国际背景下，各国对数据跨境流动、数据安全保护的要求不断提高，数据领域的国际规则竞争日趋激烈。中国作为网络数据大国，迫切需要完善相关的安全管理法规体系，以应对国际规则的变化，维护网络数据安全，同时为在华企业提供明确的合规指引，避免因各国法规差异而陷入合规困境。

（2）国内范围

随着中国数字经济的快速发展，网络数据的价值日益凸显，但与此同时，利用网络数据进行犯罪的案例也逐渐增多，给个人、企业和国家的安全带来了严重威胁。

从个人信息泄露来看，一些不法分子通过非法手段获取大量个人信息，用于电信诈骗、精准营销等违法活动。

在企业数据安全方面，商业秘密泄露、核心数据被窃取的案例时有发生。某科技公司的核心技术数据被内部员工与外部人员勾结窃取，并泄露给竞争对手，给该公司造成了巨大的经济损失和市场竞争力下降。此外，一些黑客组织针对企业的网络攻击也日益频繁，通过勒索软件等方式加密企业数据，索取赎金，严重影响企业的正常运营。

（3）重要意义

面对日益严峻的国内网络数据安全形势，此前的《网络安全法》《数据安全法》《个人信息保护法》（以下简称《网安三法》）已对数据安全和个人信息保护制度作出基本规定。但在具体执行层面，仍存在一些需要细化和完善的地方。《条例》的出台，正是为了进一步规范网络数据处理活动，填补法律执行层面的空白，保障网络数据安全，促进数据的依法合理有效利用。

2. 《条例》的适用范围

《条例》适用于在中国境内开展的网络数据处理活动及其安全监管。其中，网络数据是指通过网络收集、存储、传输、处理、使用的各种电子数据。

不仅如此，境外机构、组织、个人在中国境外处理中国境内的个人信息的活动或者开展相关网络数据处理活动，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。这意味着在华企业无论是其在华分支机构的本地数据处理活动，还是与境外总部之间的数据交互，只要涉及在华网络数据，都需遵守该《条例》。

3. 《条例》的重点内容

《条例》共有 9 章 64 条，章节明细如下：

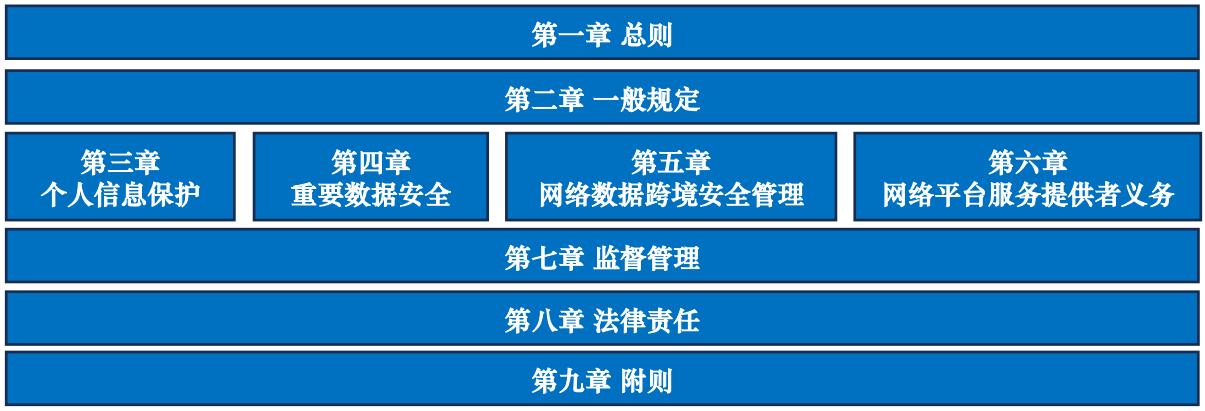

表 1　安全管理条例の各章の役割・位置づけと対象

章节	作用	对象
一、九	搭建条例的基础规则框架，补充辅助性内容。	所有适用《条例》的主体
二	设定数据处理活动的通用基本规则	所有涉及数据处理的主体
三~六	针对“个人信息、重要数据、跨境数据、网络平台服务”四类场景数据，制定专项安全规则	涉及个人信息、重要数据、跨境数据、网络平台服务的主体
七、八	明确监管机制与违规后果，保障条例落地实施	监管机构执行，针对所有数据处理主体

（1）一般规定

禁止非法数据处理活动	✓ **非法行为禁止**：任何组织或个人不得利用网络数据从事非法活动，包括窃取、非法获取、出售或向他人提供网络数据。同时，禁止提供专门用于此类非法活动的程序、工具，或为其提供技术支持（如互联网接入、服务器托管等）。 ✓ **连带责任**：明知他人从事非法数据活动仍提供帮助的，将依法追究法律责任。

数据处理者的主体责任	✓ **基础防护义务**：网络数据处理者需在网络安全等级保护制度[1]基础上，建立健全数据安全管理制度，采取加密、备份、访问控制、安全认证等技术措施，保障数据免遭篡改、破坏、泄露或非法利用。 ✓ **产品与服务合规**：提供的网络产品或服务需符合国家标准；发现安全缺陷或漏洞时，应立即补救并告知用户及主管部门；涉及国家安全或公共利益的，须在 24 小时内报告。 ✓ **应急机制**：必须制定数据安全事件应急预案，事件发生后立即启动预案，防止危害扩大，并向主管部门报告。若事件损害个人或组织权益，需通过电话、短信等方式及时通知利害关系人。
数据合作与转移的规范	✓ **委托处理与数据提供**：向其他处理者提供或委托处理个人信息、重要数据时，需通过合同明确处理目的、范围及安全义务，并对接收方履行义务的情况进行监督。相关记录至少保存 3 年。 ✓ **共同处理与数据转移**：多个处理者共同决定数据处理目的时，需约定各自权责；因合并、解散等原因转移数据的，接收方须继续承担安全保护义务。
技术应用与自动化工具的规范	✓ **自动化数据收集**：使用自动化工具访问、收集数据时，需评估对网络服务的影响，禁止非法侵入或干扰网络正常运行。 ✓ **生成式人工智能服务**：提供此类服务时，需加强训练数据的安全管理，防范数据安全风险。
国家安全审查要求	✓ **审查标准**：网络数据处理活动影响或可能影响国家安全的，必须依规进行国家安全审查，具体参照《网络安全审查办法》（如处理超 100 万人个人信息赴国外上市需申报审查）。

（2）个人信息保护

《条例》重点细化了个人信息保护相关规定。

透明化要求	✓ **告知形式**：需制定处理规则，集中公开展示于醒目位置，确保内容明确易懂。 ✓ **规则必备内容**：处理者名称/联系方式、处理目的/方式/种类；敏感信息处理的必要性及对个人权益的影响；保存期限及到期处理方式；个人行使权利途径；处理不满 14 周岁未成年人信息需制定专门规则，且需监护人同意。
合规义务	✓ **必要性原则**：仅收集提供服务所必需的信息，禁止超范围收集或通过误导、欺诈、胁迫获取同意。 ✓ **限制性行为**：不得超出同意的目的、方式、种类或保存期限处理信息；不得在用户明确拒绝后频繁征求同意；处理目的/方式/种类变更时需重新取得同意。
保障主体权利	✓ **行权通道**：个人提出查阅、复制、更正、删除、限制处理、撤回同意或注销账号等请求时，处理者需及时受理并提供便捷途径，不得设置不合理条件。 ✓ **可携带权**：个人信息转移需同时满足：身份可验证；转移基于同意或合同收集的信息；技术可行且不损害他人权益。
自动化采集与数据处理	✓ **非必要信息处理**：因自动化技术无法避免采集到非必要或未授权信息的，应删除或匿名化处理；技术难以实现的，需停止除存储和安全保护外的所有处理。 ✓ **账号注销后的义务**：应及时删除或匿名化个人信息。

[1] 等级保护制度（简称等保制度）是中国一项基础性的网络安全管理体系，其核心在于根据网络及信息系统的关键程度进行分级，并针对不同等级规定相应的安全防护措施与评估义务。对于在华日资企业而言，凡在中国境内运营网络及信息系统的，原则上均需遵守该制度，该制度已成为数据安全管理与合规应对的重要基础性制度之一。

跨境与超大规模处理义务	✓ **境外处理者要求：**境外处理境内自然人个人信息的，需按《个保法》在境内设立专门机构或指定代表，并向市级[2]网信部门报送信息。 ✓ **超大规模处理增强义务：**处理 1000 万人以上个人信息的，需设立数据安全管理机构及负责人；因合并、解散等影响数据安全时，需制定处置方案并向省级以上部门报告。
合规审计与监督机制	✓ **定期审计：**需自行或委托专业机构对个人信息处理活动进行合规审计。 ✓ **平台特殊责任：**大型网络平台（用户超 5000 万或月活超 1000 万）需发布个人信息保护社会责任年度报告。

法律责任：对于违反个人信息保护相关规定的，根据情节轻重，可处以警告、罚款等处罚。例如，未按要求履行告知义务或通过不正当方式获取个人同意的，可处 5 万元以上 50 万元以下罚款；情节严重的，处 50 万元以上 200 万元以下罚款，并可以责令暂停相关业务、停业整顿等。

（3）重要数据安全保障

《条例》对重要数据作出明确定义，即特定领域、群体、区域或达到一定精度和规模，一旦遭到篡改、破坏、泄露或非法获取、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。像金融行业的客户交易数据、医疗行业的患者病历数据、能源行业的管网运行数据等都可能被纳入重要数据范畴。

目录管理	✓ **国家统筹：**国家数据安全工作协调机制统筹制定重要数据目录，各地区、各部门据此确定本地区、本行业的具体目录，并动态更新。 ✓ **企业责任：**网络数据处理者需主动识别、申报重要数据，相关地区或部门审核后需及时告知或公开发布。 ✓ **技术辅助：**鼓励使用数据标签标识等技术提升重要数据管理效率。
处理者的组织责任	✓ **机构与人员设置：**必须设立安全管理机构和安全负责人，负责人需具备专业知识和管理经验，且由管理层成员担任；特定行业（如金融、能源）需对安全负责人及关键岗位人员开展安全背景审查，必要时可申请公安或国安机关协助。 ✓ **管理机构职责：**制定安全制度、操作规程及应急预案；定期组织风险监测、应急演练及培训；受理并处理数据安全投诉与举报。
流转风险控制	✓ **事前风险评估：**在提供、委托或共同处理重要数据前（法定职责除外），必须进行风险评估，重点包括：数据接收方的目的合法性、诚信度及合同约束力；数据遭篡改、泄露等风险及对国家安全的影响；防护措施的有效性。 ✓ **特殊场景处置：**因合并、解散、破产等可能影响重要数据安全的，需制定处置方案并向省级以上主管部门报告接收方信息及保障措施。
年度风险评估与报告机制	✓ **报告内容：**处理者基本信息、安全管理机构及负责人联系方式；重要数据的处理目的、种类、数量、存储地点及安全措施（如加密、备份、访问控制）；全年安全风险事件及处置情况；数据出境情况。 ✓ **增强义务：**大型网络平台需额外说明关键业务和供应链数据安全情况。若存在危害国家安全的活动，省级以上主管部门可责令整改或停止处理。
与其他领域的衔接	✓ **金融行业特例：**银行保险机构需将重要数据纳入核心数据层级，实施最高级别保护，事件发生后需 2 小时内报告监管部门。 ✓ **自贸区跨境管理：**自贸区可制定数据出境负面清单，清单外数据跨境可豁免安全评估；清单内重要数据出境需按常规流程申报。

[2] 地级市是中国行政区划中位于省之下的一级地方行政单位，其定位类似于日本以县厅所在地为核心的广域市。通常情况下，针对企业的行政手续办理、监督管理及申报事宜均由地级市级主管部门负责管辖。

法律责任：未按规定识别、申报重要数据，或未开展风险评估的，处 10 万元以上 100 万元以下罚款；情节严重的，处 100 万元以上 1000 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 1 万元以上 10 万元以下罚款。

（4）网络数据跨境安全管理

《条例》在总结相关部门规章制定实施经验基础上，进一步优化数据跨境流动机制。

管理框架	✓ **统筹协调机制：**国家网信部门牵头建立数据出境安全管理专项工作机制，负责制定跨境流动政策、协调重大事项。 ✓ **分类分级监管原则：**仅对重要数据和达到规定规模的个人信息实施出境管控，一般数据可自由跨境流动。 ✓ **自贸试验区创新机制：**允许自贸区制定“数据出境负面清单”，清单外数据免于安全评估、标准合同或认证。
重要数据跨境管理规则	✓ **重要数据定义：**可能危害国家安全、经济运行、社会稳定等的数据。 ✓ **豁免申报：**若未被相关部门或地区告知或公开发布为重要数据，无需申报出境安全评估。 ✓ **出境条件：**经安全评估确认不危害国家安全和社会公共利益的，可出境。 ✓ **风险评估要求：**重要数据出境前需评估接收方目的合法性、合同约束力及防护措施有效性。
跨境传输机制	✓ **合法出境途径：**通过国家网信部门组织的安全评估；经专业机构个人信息保护认证；订立个人信息出境标准合同。 ✓ **特定场景豁免：**履行个人合同（如跨境购物、签证办理）；跨境人力资源管理（依合法制度提供员工信息）；履行法定职业义务；紧急保护生命财产安全；非关键设施运营者年累计出境<10 万非敏感个人信息。 ✓ **规模分级管理：**关键信息基础设施运营者、重要数据出境、年累计出境≥100 万非敏感个人信息[3]或≥1 万敏感个人信息的，必须申报安全评估。
数据处理者的合规义务	✓ **合同监督与记录留存：**需通过合同约束境外接收方的数据使用目的和范围，并监督其履行义务；数据出境审批记录和日志需保存至少 3 年 ✓ **安全保护与事件响应：**采取加密、访问控制等技术措施；发生数据安全事件时需立即补救，并向网信部门报告；损害个人权益的需及时通知利害关系人。 ✓ **禁止行为：**不得超越安全评估或合同中声明的目的、范围、数据类型向境外提供数据。

法律责任：对于违规进行网络数据跨境流动的，处 20 万元以上 200 万元以下罚款；情节严重的，处 200 万元以上 1000 万元以下罚款，并可限制其数据出境，对直接负责的主管人员和其他直接责任人员处 2 万元以上 20 万元以下罚款。

（5）网络平台服务提供者义务

鉴于网络平台服务提供者在数字经济和公共服务中的重要作用，同时针对实践中存在的问题，《条例》对其义务做出专门规定。要求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履行网络数据安全保护义务。

对第三方管理的义务	✓ **数据保护：**通过平台规则或合同明确第三方数据安全保护义务，并督促其加强管理；第三方违规对用户造成损害，平台需依法承担相应责任。

[3] 非敏感个人信息是指不属于中国《个人信息保护法》定义的敏感个人信息（种族、宗教、健康信息、生物识别信息、金融账户信息等）的个人信息。根据中国法律，其处理要求相较于敏感个人信息相对宽松，但既然属于个人信息范畴，在收集、使用、跨境提供等环节仍须遵循合法性、正当性、必要性原则，并持续履行安全管理义务。

应用程序分发管理	✓ **核验规则**：建立应用程序核验规则，对不符规定的应用采取警示、不予分发、暂停或终止分发等措施。
自动化决策规范	✓ **信息推送功能**：向个人进行信息推送时，应提供易于操作的个性化推荐关闭选项、拒绝接收推送及删除用户标签的功能。
大型平台特殊义务	✓ **特殊义务**：年度个人信息保护社会责任报告；跨境提供数据需遵守国家安全要求；禁止利用数据、算法等实施误导、欺诈、胁迫、不合理差别待遇等损害用户权益的行为。

法律责任：网络平台服务提供者违反相关义务的，处罚措施也较为严厉，根据违规情节可处 10 万元至 1000 万元不等的罚款，同时可能面临暂停业务、停业整顿等处罚。

4. 《条例》与相关法律的异同

《网安三法》构建起中国网络数据安全领域的基本法律框架，《条例》作为配套行政法规，与这几部法律既有紧密联系，又存在显著差异。

（1）相同点

相同点	
立法目的一致	这几部法律法规的根本目的都是维护国家安全、社会公共利益以及保护个人和组织的合法权益。 ✓ 网络安全法着重保障网络安全，维护网络空间主权，促进经济社会信息化健康发展。 ✓ 数据安全法旨在保障数据安全，促进数据开发利用。 ✓ 个人信息保护法聚焦于保护个人信息权益，规范个人信息处理活动。 ✓ 《条例》同样以规范网络数据处理活动、保障网络数据安全为目标。
遵循共同原则	在数据处理活动中，它们都遵循合法、正当、必要原则。 ✓ 网络安全法强调网络运营者收集、使用个人信息，需要公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。 ✓ 数据安全法要求开展数据处理活动，应当遵守法律法规，遵守商业道德和职业道德，诚实守信，履行数据安全保护义务，承担社会责任。 ✓ 个人信息保护法规定处理个人信息不得通过误导、欺诈、胁迫等方式处理个人信息。 ✓ 《条例》在个人信息保护、重要数据管理等方面，也始终贯穿这些原则。
关注数据安全保护全流程	几部法律均对数据从收集、存储、使用、共享到销毁的全生命周期安全保护提出要求。 ✓ 网络安全法规定网络运营者应当采取技术措施和其他必要措施，保障网络安全、稳定运行，有效应对网络安全事件，保护个人信息安全，防止信息泄露、毁损、丢失。 ✓ 数据安全法明确数据处理者要建立健全全流程数据安全管理制度，组织开展教育培训，采取相应的技术措施和其他必要措施，保障数据安全。 ✓ 个人信息保护法对个人信息处理者在个人信息收集、存储、使用、加工、传输、提供、公开、删除等各环节的安全保护义务作出详细规定。 ✓ 《条例》同样构建了数据识别、处理、防护、评估、检查、整改、应急响应等体系化、闭环式管理机制。

（2）不同点

不同点

法律层级与效力不同	网安三法，是网安领域内的基础性法律，构建了顶层设计框架，而《条例》是其下属的实施细则。 ✓ 网安三法由全国人民代表大会常务委员会制定并通过，属于法律层级，具有较高的法律效力。 ✓ 《条例》由国务院制定颁布，属于行政法规，其效力低于法律，但在行政法规体系内对网络数据安全管理工作具有重要的规范作用。当条例内容与法律规定不一致时，以法律为准；在法律规定的框架内，条例对具体事项进行细化和补充。
规范侧重点不同	网安三法主要侧重于各自的核心领域，而《条例》更关注实施层面的概念和定义。 ✓ 网络安全法更侧重于网络运行安全和网络信息安全两大方面。在网络运行安全上，对关键信息基础设施的运行安全做出专门规定；在网络信息安全方面，主要规范网络运营者对个人信息的收集、使用规则以及信息安全事件的报告等内容。 ✓ 数据安全法以数据为核心，重点规范数据处理活动中的安全保障措施，强调数据分类分级管理，要求建立健全数据安全治理体系。 ✓ 个人信息保护法专门针对个人信息保护进行规范，从个人信息处理规则、个人信息跨境提供规则到个人在个人信息处理活动中的权利等方面做出全面细致的规定。 ✓ 《条例》则聚焦于网络数据处理活动及其安全监管，一方面提炼了"网络数据处理者"这一统筹性概念，另一方面首次在行政法规层面明确了"重要数据"的定义。
宏观与细化的区别	网安三法主要是国家在网络安全方面的总体要求，而《条例》则是落实这些要求的具体细则。 ✓ 网安三法是从宏观层面确立制度和原则。 ✓ 《条例》是对法律的原则进行细化：在个人信息保护方面，法律规定了基本要求，《条例》则明确了更详细的内容，例如明确了"数据可携带权"的行使条件。《条例》还细化了重要数据的全流程安全管理，例如明确安全负责人需为管理层成员，并规定了不同场景下的风险评估要求。

5. 《条例》对企业的要求

企业在日常运营中涉及大量网络数据处理活动，包括员工个人信息管理、客户数据维护、业务数据存储与传输等。《条例》的实施意味着企业需要重新审视和完善自身的数据安全管理体系。

（1）个人信息保护

- **隐私政策需更透明**：不仅要求集中公示、清晰易懂，对于**收集个人信息以及向其他方提供个人信息**，还必须以"**清单**"形式列明目的、方式、种类及接收方信息。
- **支持个人信息转移**：明确了个人行使"**数据可携带权**"的四个具体条件，企业需在技术可行且验证身份后提供转移途径。
- **新增删除或匿名化情形**：因使用自动化采集技术（如爬虫[4]）等无法避免收集到非必要个人信息或未依法取得同意的个人信息时，应当**删除或进行匿名化处理**。
- **强调定期合规审计**：要求企业**定期自行或委托专业机构**对个人信息处理活动进行合规审计。
- **境外处理者信息报送**：在境外处理中国境内自然人个人信息的处理者，若依《个人信息保护法》在境内设立专门机构或指定代表，需将相关信息向**所在地设区的市级网信部门**报送。

（2）重要数据安全保障

- **识别重要数据**：企业需关注并依据国家及行业主管部门制定的**重要数据目录**，判断自身是否处理重要数据。

[4] 爬虫是指利用程序自动巡回收集网站及网络信息的机制（自动获取工具）。虽然存在搜索引擎信息收集等正当用途，但根据设置和使用方式的不同，可能因过度访问或擅自获取数据而引发数据安全及个人信息保护问题。

- **设立管理机构与负责人**：重要数据的处理者需**明确数据安全负责人和管理机构**，并每年通过年度风险报告向主管部门报送。
- **关键操作前进行风险评估**：在**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），且每年通过年度风险报告向主管部门报送。
- **年度风险评估与报送**：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。
- **特殊情形下的数据处置**：因合并、分立、解散、破产等可能影响重要数据安全的，应制定**数据处置方案**并报告主管部门。

（3）网络数据跨境安全管理

- **个人信息出境的八种情形**：除了熟知的通过安全评估、保护认证、标准合同三种路径外，《条例》还补充了其他情形，例如为履行合同、跨境人力资源管理、保护生命健康和财产安全等所必需的情形。
- **重要数据出境需安全评估**：重要数据出境应当通过国家网信部门组织的**数据出境安全评估**。
- **出境活动不得超范围**：通过数据出境安全评估后，向境外提供个人信息和重要数据时，**不得超出评估时明确的目的、方式、范围、种类和规模**。

（4）网络平台服务提供者义务

- 网络平台服务提供者，特别是**大型网络平台**，需承担更严格的责任，包括对平台上的应用进行严格核验、为用户提供个性化推荐关闭选项等，并且大型平台可能需履行**年度审计**等增强性义务。

（5）对在华日企的补充提醒

- **跨境数据传输的合规挑战**：在华日企通常需要将数据传回日本或区域总部。《条例》重申了数据出境的多重要求。企业需**谨慎选择并确保其每条跨境传输路径的合规性**，特别是涉及重要数据时必须通过安全评估。
- **应对中日法规差异**：日本也有其数据保护法规（如 APPI）。在华日企需要**同时满足中日两国的合规要求**，注意中国在**重要数据管理、数据本地化及出境评估**等方面可能有**更严格**的规定。
- **供应链数据安全管理**：在华日企多嵌入全球供应链。《条例》要求网络数据处理者向其他处理者提供、委托处理个人信息和重要数据时，应**通过合同约定安全保护义务并进行监督**。这意味着企业需**审视并约束其中国境内的合作伙伴**。
- **"重要数据"的识别压力**：在华日企可能在华经营多年，积累了海量数据。需特别注意，一旦处理 **1000 万人以上个人信息**，将参照重要数据处理者履行部分义务。因此，**准确的数据分类分级**至关重要。

6. 实际案例参考

近年来，已有部分企业因违反数据安全相关法律法规受到处罚。这些案例警示在华日企，必须高度重视数据安全合规工作，严格遵守《条例》及相关法律法规，避免重蹈覆辙。

案例 1：

主题	重庆某科技公司用于汽车租赁服务的“OA 信息系统”数据先后被窃取 159 次
原因	涉事系统 3306 端口开放 MySQL 数据库服务，未设置用户密码，存在弱口令漏洞
违法事项	未依法履行网络安全、数据安全保护义务，未采取技术措施保障数据安全
涉及法律	《网络安全法》《数据安全法》《网络数据安全管理条例》

案例 2：

主题	湖南某科技股份有限公司的内网数据库数据暴露在互联网，存在泄露风险
原因	内网数据库存在未授权访问漏洞和弱口令漏洞；工程师将大量用户数据拷贝至内网数据库，并打开公共互联网访问端口
违法事项	未依法履行网络安全、数据安全保护义务，未建立相关管理制度，未采取技术措施保障数据安全
涉及法律	《网络安全法》《数据安全法》《网络数据安全管理条例》

案例 3：

主题	上海某科技有限公司运营的自动售货机违法收集人脸信息，系统存在安全漏洞
原因	支付环节未经用户同意收集人脸信息，未建立个人信息保护影响评估制度，系统存在 SQL 注入高危漏洞
违法事项	违法违规收集人脸信息，未建立个人信息保护影响评估制度，系统存在高危安全漏洞
涉及法律	《网络安全法》《个人信息保护法》《网络数据安全管理条例》

7. 企业的应对建议

为防止此类事件发生，企业需主动审视自身网络数据处理活动是否符合《条例》的要求，并评估现有措施是否有效运行，据此制定应对方案并推进实施。推进过程中可考虑以下要点：

（1）全面自查与评估

在华企业应组织由法务、IT、业务等部门组成的专业团队，对照《条例》要求，对企业当前的网络数据处理活动进行全面自查。涵盖数据收集的渠道是否合法、存储的安全性、使用的范围是否在授权内、共享的对象是否合规、跨境传输的流程是否符合规定等各个环节。

评估自身在个人信息保护、重要数据管理、数据跨境流动等方面与《条例》的符合程度，详细列出存在的差距和问题，并形成书面报告。例如，检查企业现有的个人信息收集表单是否完整告知了所有必要信息，数据存储系统的安全防护措施是否到位等。

（2）完善管理制度与流程

根据自查结果，完善企业内部的网络数据安全管理制度和操作流程。明确各部门和岗位在数据安全管理中的职责，如 IT 部门负责数据存储安全，业务部门负责数据收集的合规性等。

建立健全数据分类分级制度，按照《条例》对个人信息和重要数据的界定，对企业数据进行分类分级管理。制定风险评估、安全防护、应急处置等制度，如定期开展数据安全风险评估，制定数据泄露应急响应预案等。

例如，制定详细的个人信息处理流程规范，明确从收集、存储、使用到删除的各个环节的操作要求；明确数据访问权限控制机制，确保只有授权人员才能访问敏感数据和重要数据，确保重要数据的安全存储和传输。

（3）加强员工培训与教育

组织全体员工参与网络数据安全培训，特别是涉及数据处理的关键岗位人员，如人力资源部门员工（处理员工个人信息）、市场部门员工（处理客户数据）等。

培训内容应涵盖《条例》的主要内容、企业内部数据安全管理制度和流程、数据安全风险防范意识等。可以通过案例分析、模拟演练等方式提高培训效果，让员工深刻理解违规处理数据的严重后果，提高员工对网络数据安全的重视程度和合规操作能力。

（4）建立合规审查机制

设立专门的合规审查岗位或团队，由具备法律和数据安全知识的专业人员组成。对企业新的业务模式、数据处理活动、数据合作项目等进行事前合规审查，确保其符合《条例》及相关法律法规的要求。

例如，在开展新的市场调研项目需要收集大量用户数据时，合规审查团队需提前审查数据收集方案是否合规；在与其他企业进行数据共享合作时，审查合作协议中关于数据使用的条款是否符合规定，避免因违规操作而面临法律风险和声誉损失。

（5）寻求专业支持

如果企业自身在数据安全和合规方面的专业能力不足，可以寻求专业的咨询机构或律师事务所的帮助。这些专业机构能够为企业提供《条例》的深度解读、合规方案设计、风险评估等服务，帮助企业更高效地达到《条例》的要求。

我方也推出专业评估服务（名称：网安三法对应评估服务），依据网安三法及相关 GB 标准，为企业排查合规风险、保护数据资产与信誉，规避罚款等处罚。实施方法包括访谈、现场检查、工具测试等，主要评估网络环境、等保及数据安全、系统脆弱性等 7 项内容。

图 1 网安三法对应评估服务的实施方法和评价项目

图 2 网安三法对应评估服务的成果物举例

服务周期约 1 个月，提交中日文的评估报告。最终梳理高、中、低风险项，提供分级分类、安全防护等整改建议，让企业管理层完整了解既存风险以及下一步的改善方向，完善企业网络安全能力。

8.总结

在本文中，根据《网络数据安全管理条例》，围绕日资企业的网络数据管理希望特别注意的要点进行了解说。

《网络数据安全管理条例》的实施为在华企业的网络数据安全管理提出了新的要求和挑战。在华企业应积极应对，加强合规管理，提升网络数据安全保护水平，以确保企业在华业务的稳健发展。

执笔：瑛得管理咨询（上海）有限公司 高级经理 张若亭

参考资料:

- 《网络数据安全管理条例》
  https://www.gov.cn/zhengce/zhengceku/202409/content_6977767.htm
- 国家网信办发布近期网络安全、数据安全、个人信息保护相关执法典型案例
  https://www.cac.gov.cn/2025-09/16/c_1759741437315419.htm
- 健全数据安全法律制度 筑牢网络数据安全防线
  https://www.moj.gov.cn/pub/sfbgw/zcjd/202409/t20240930_507078.html
- 宽严相济，张弛有道:《网络数据安全管理条例》主要亮点与合规参考
  https://www.zhonglun.com/research/articles/53628.html

MS&AD InterRisk综研隶属于MS&AD保险集团控股株式会社，是一家专门从事风险管理有关的调查研究以及咨询相关的专业公司。
面向有意向中国进军的企业有关咨询・研讨会方面的洽谈可以联系我公司下述联络方式或是联系三井住友海上、爱和谊日生同和各营业担当。

联系方式 MS&AD InterRisk综研 风险咨询本部 国际业务组
TEL.03-5296-8920 http://www.irric.co.jp/

瑛得管理咨询（上海）有限公司是在中国上海设立的隶属于ＭＳ＆ＡＤ保险集团的风险管理公司，主要提供诸如工厂/仓库的风险查勘、BCP 计划的制定等各种风险相关的咨询服务。如欲联系或申请等请联系下述地址。
联系方式 瑛得管理咨询（上海）有限公司 （日语：インターリスク上海）
上海市浦东新区世纪大道 100 号 环球金融中心 34 层 T10 室-2
TEL:+86-(0)21-6841-0611（代表）

本刊是基于媒体报道的公开信息制作完成。
本刊目的为读者以及读者所属的组织在实施风险管理活动中提供一些参考价值。并无意图针对某一事件本身提出批评或意见。

严禁复制 / Copyright 株式会社 MS&AD InterRisk 综研 2025