汉坤法律评述

2021 年 10 月 5 日

HAN KUN
汉 坤 律 师 事 务 所
Han Kun Law Offices

北京 | 上海 | 深圳 | 香港

正当其时：工信部强化工业和信息化领域数据安全管理

作者：段志超 | 蔡克蒙 | 王雨婷

2021 年 9 月 30 日，工业和信息化部（“**工信部**”）发布《工业和信息化领域数据安全管理办法（试行）（征求意见稿）》（“**《管理办法》**”），向社会公开征求意见。继《数据安全法》施行以来，《管理办法》系首个由行业、领域主管部门制定发布的数据安全领域规范性文件（征求意见稿），也即将为企业数据合规建设提出一系列新任务、新要求。

《管理办法》的核心内容如下：

- **适用范围。**《管理办法》旨在监管在中国境内开展的工业和电信数据处理活动，各类软件和信息技术服务业企业、电信业务经营许可证持证企业均落入适用范围。若通过 App 提供产品和服务被认定为“软件和信息技术服务业”，各类 App 运营者同样可能落入《管理办法》的适用范围。从数据类型来看，个人信息的处理活动也落入《管理办法》的适用范围。

- **重要数据和核心数据的范围和增强要求。**《管理办法》从潜在危害程度角度重申并细化了重要数据、核心数据的识别原则，但未就具体数据类型进行列举。前述原则将会为《网络安全审查办法（修订草案征求意见稿）》从核心数据、重要数据等考量相关国家安全风险因素提供支撑。此外，《管理办法》就核心数据、重要数据提出了包括工作体系、数据存储、数据传输、和数据跨境等方面的增强要求。特别地，其首次提出了核心数据不得出境的规定。

- **备案和报送义务。**值得注意的是，《管理办法》规定了相关处理者就重要数据和核心数据的处理行为的备案和报送义务。相关备案制度和针对重要数据和核心数据的增强要求（包括数据出境要求）结合，表明了监管要求处理者落实重要数据和核心数据相关监管的态度和路径。

- **明确企业数据安全责任人并落实数据全生命周期安全保护义务。**企业应明确数据安全管理的主要负责人和责任部门，处理重要数据或核心数据的，还应设置专门的数据安全管理责任部门，并将责任人上升到党委（党组）或领导班子水平。同时企业应根据《管理办法》逐一落实数据全生命周期各处理环节的合规义务。

- **开展安全评估并配合数据安全审查。**企业应针对各级别数据制定并开展相应的数据安全评估及整改工作，对一般数据开展自评估，对重要数据和核心数据开展年度安全评估并履行报告义务。企业处理重要数据、核心数据影响或可能影响国家安全的，可能被要求通过数据安全审查，同时，也不排除相关处理活动被纳入网络安全审查范围的可能性。

我们将在下文梳理和总结《管理办法》中关于工业和电信数据安全管理的关键要求，并同时提出我们的解读。

一、广泛的适用范围：个人信息的多维监管和特殊行业例外

《管理办法》从数据类型和适用主体两个维度设置了广泛的适用范围，互联网、车联网、自动驾驶、人工智能、云计算等行业企业都可能落入其适用范围。医疗、金融、酒店住宿等领域企业若持有电信业务经营许可证，也可能适用《管理办法》。此外，若“软件和信息技术服务行业”被解释为各类以 App 为形式提供的产品和服务，则各 App 运营者无论其行业领域均可能落入《管理办法》的适用范围。

具体而言，《管理办法》第 2 条规定本办法的适用范围为：中华人民共和国境内开展的工业和电信数据处理活动及其安全监管。第 3 条明确，**电信数据**是指在电信业务经营活动中收集和产生的数据。**工业数据**是指“原材料工业、装备工业、消费品工业、电子信息制造业、软件和信息技术服务业、民爆”等行业领域在“研发设计、生产制造、经营管理、运维服务、平台运营、应用服务”等业务过程中收集和产生的数据。**工业和电信数据处理者**的范围则涵盖了对工业、电信数据进行各项数据处理活动的工业企业、软件和信息技术服务企业、取得电信业务经营许可证的电信业务经营者等各类主体。

值得注意的是，和《数据安全法》以及《个人信息保护法》不同，《管理办法》并不具有域外效力，且，《管理办法》第八章进一步将涉及国家秘密信息、密码使用、军事数据、政务数据、国防科工领域、烟草领域的数据处理活动排除出其适用范围之外。

《管理办法》的广泛适用性也体现在数据类型上。《管理办法》秉承《数据安全法》将个人信息纳入重要数据目录和核心数据目录进行重点保护的工作理念，将个人信息纳入数据全生命周期安全管理[1]。因此，个人信息既要遵守个人信息保护相关法律法规的规定，也要遵守《管理办法》项下关于数据安全管理的规定。

一直以来工信部门和网信部门同时针对 App 处理个人信息开展频繁的执法监管活动，企业处理个人信息面对不同部门的多头监管。此次《管理办法》将《网络安全法》、《数据安全法》作为上位法基础，但并未提及《个人信息保护法》，这在一定程度上可以被解读为未来工信部的监管执法将侧重于工业与电信行业领域的数据安全，而并非是广泛适用的各类个人信息处理活动。

二、重要数据和核心数据：行业列举和危害程度标准

《管理办法》再次重申了《数据安全法》确立的数据分类分级管理方法，提出企业应当坚持先分类后分级的工作方法，将工业与电信数据分为**研发数据、生产运行数据、管理数据、运维数据、业务服务数据、个人信息**等类别（第 7 条）；并参考第 8 条至第 10 条的标准，将工业与电信数据分为一**般数据、重要数据和核心数据**三级。

危害程度符合下列条件之一的数据为**重要数据**：

- 对政治、国土、军事、经济、文化、社会、科技、网络、生态、资源、核安全等构成威胁，影响海外利益、生物、太空、极地、深海、人工智能等重点领域国家安全相关数据的安全；

[1] 参见《工业和信息化领域数据安全管理办法（试行）（征求意见稿）》起草说明，访问地址：https://www.miit.gov.cn/cms_files/filemanager/1226211233/attach/20219/1d1668e46e644b42b04a95db43854607.pdf。

- 对工业、电信行业发展、生产、运行和经济利益等造成影响；
- 造成重大数据安全事件或生产安全事故，对公共利益或者个人、组织合法权益造成严重影响，社会负面影响大；
- 引发的级联效应明显，影响范围涉及多个行业、区域或者行业内多个企业，或者影响持续时间长，对行业发展、技术进步和产业生态等造成严重影响；
- 恢复数据或消除负面影响所需付出的代价大。

危害程度符合下列条件之一的数据为**核心数据**：

- 对政治、国土、军事、经济、文化、社会、科技、网络、生态、资源、核安全等构成严重威胁，严重影响海外利益、生物、太空、极地、深海、人工智能等重点领域国家安全相关数据的安全；
- 对工业、电信行业及其重要骨干企业、关键信息基础设施、重要资源等造成严重影响；
- 对工业生产运营、电信和互联网运行和服务等造成重大损害，导致大范围停工停产、大面积网络与服务瘫痪、大量业务处理能力丧失等。

从定义来看，可能对国家安全造成影响的工业和电信数据可能被认定为重要数据、甚至核心数据。因此，聚焦国家安全的《网络安全审查办法（修订草案征求意见稿）》将“核心数据、重要数据或大量个人信息被窃取、泄露、毁损以及非法利用或出境的风险”纳入审查因素。

但企业如何在实践中落实工业与电信数据的分级工作仍有待主管部门提供更明确的指引，原因在于《管理办法》提及的“严重威胁”、“严重影响”、“重大损害”等判断因素缺乏量化标准。此外，各地区行业的重要数据、核心数据目录将由地方工信主管部门、通信管理局制定并上报工信部，因此，哪些数据会落入重要数据、核心数据的范畴，很大程度上有待《管理办法》落地后工信部的进一步明确。

三、报送及备案：增强的数据处理透明性

《管理办法》第 11 条指出，要构建工业和信息化领域“工信部—地方主管部门—数据处理者”三级联动的数据分类分级机制。在此基础上，未来将构筑起包括数据分类分级防护、重要数据与核心数据目录报送、重要数据与核心数据备案管理等一系列工作机制。相对应地，企业主要有如下三方面合规义务：

- **一是形成数据分类清单，并在此基础上划定重要数据和核心数据。**有关分类分级情况应定期梳理，实行动态管理。
- **二是分类分级后的分级防护义务。**对重要数据进行重点保护，对核心数据在重要数据保护基础上实施更严格的管理和保护。不同级别数据同时被处理且难以分别采取保护措施的，应当按照其中级别最高的要求实施保护。
- **三是分类分级后对重要数据和核心数据的报送义务、备案义务。**将重要数据和核心数据目录报送地方工业和信息化主管部门或通信管理局，并按照有关要求对重要数据和核心数据进行备案。备案内容[2]发生变化的，应在三个月内报备变更情况，同时对整体备案情况进行更新。

[2] 备案内容包括数据的数量、类别、处理目的和方式、使用范围、主体责任、安全保护措施等基本情况，数据提供、公开、出境、承接，以及数据安全风险、事件处置等情况。参见《管理办法》第 12 条。

针对列入重要数据和核心数据报送目录中的数据，企业应注意在数据处理的各个环节落实《管理办法》关于重要数据和核心数据的增强要求。

四、数据安全组织架构：职责细化和领导负责

企业依照《管理办法》落实数据安全管理义务的第一步将是建立健全数据安全组织架构。《管理办法》细化了部门与人员要求，指出企业要明确数据安全管理的责任部门和主要负责人、明确数据处理的关键岗位及人员。

对涉及重要数据和核心数据的企业，《管理办法》进一步明确了企业党委（党组）或领导班子对数据安全负主体责任、主要负责人是数据安全第一责任人、分管数据安全的负责人是数据安全直接责任人。同时，企业应该设置专门的责任部门。因此，对于可能处理重要数据、核心数据的企业，未来可能需要重新审视并调整其组织架构，目前常见的一部门或一岗位多职责的设置可能无法满足《管理办法》对于重要数据、核心数据的增强要求。

五、全生命周期安全管理：国家安全和公共利益体现

相较于《数据安全法》、《网络安全法》的笼统规定，《管理办法》借鉴了《数据安全管理办ｚ法（征求意见稿）》的管理思路，针对数据全命周期的不同环节，分别提出了适用各级别数据的通用要求、以及处理重要数据与核心数据应遵守的额外要求。《管理办法》提出的合规要求较为具体，例如签署数据安全协议、承诺函、留存处理记录等，为企业落实数据安全管理义务提供了指引。在贯穿数据全生命周期的各项合规义务中，如下合规要求值得企业关注：

- 未经个人、单位等同意，不得针对特定主体进行精准画像、数据复原等加工处理活动。
- 基于保护国家安全、社会公共利益目的，且有第三方机构提供证明请求销毁的，企业应销毁工业和电信数据。
- 企业针对一般数据的传输、重要数据的提供、以及重要数据与核心数据的使用加工建立登记、审批机制，这对企业内部流程和数据处理记录提出了较高的要求。
- 核心数据的传输和提供应通过国家审批。
- 重要数据应在境内存储，确需向境外提供的应当依法依规进行数据出境安全评估。核心数据不得出境。

结合《数据安全法》[3]、《网络安全法》[4]的规定，重要数据出境的规则将由网信部门会同国务院有关部门制定。《管理办法》尚未针对一般数据出境提出针对性的要求，一般数据是否需在境内存储、出境是否受到限制，取决于该等数据是否受到特殊监管。典型如个人信息，其出境规则应遵守《个人信息保护法》的规定。

[3] 《数据安全法》第 31 条：关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的重要数据的出境安全管理，适用《中华人民共和国网络安全法》的规定；其他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的出境安全管理办法，由国家网信部门会同国务院有关部门制定。

[4] 《网络安全法》第 37 条：关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。

六、安全评估、监督检查、数据安全审查：制度构建下的不确定性

根据《管理办法》第五章、第六章，国家通过数据安全检测、评估、认证，以及监督检查、安全审查，落实数据安全监督管理。

（一）开展安全评估

《管理办法》第 33 条规定：对一般数据，企业可开展安全自评估；对重要数据和核心数据，企业应尽到一年一次的安全评估与向地方主管部门**报告**的义务。值得注意的是，《管理办法》第 33 条允许企业自主选择自行评估或委托第三方进行评估。

（二）协助监督检查

《管理办法》第 34 条规定，企业有配合行业监管部门开展监督检查、并预留检查接口的义务。对于企业而言，主管部门可通过检查接口访问并审查的数据范围、接口的技术标准与调用条件，可能是企业最为关心的事项，很遗憾的是《管理办法》尚未作出明确规定。实践中如何落实预留检查接口的要求，有待主管部门进一步明晰。

（三）通过数据安全审查

承接《数据安全法》第 24 条[5]的规定，《管理办法》第 35 条规定，工业和信息化部在国家数据安全工作协调机制指导下，对影响或可能影响国家安全的工业和电信数据处理活动开展数据安全审查。但《管理办法》尚未明确数据安全审查的启动条件与具体流程。另一方面，2021 年 7 月 10 日发布的《网络安全审查办法（修订草案征求意见稿）》将数据处理活动纳入审查范围，审查因素新增“核心数据、重要数据或大量个人信息被窃取、泄露、毁损以及非法利用或出境的风险”。因此，工业与电信数据处理者未来可能需要同时面对基于工信部《管理办法》与网信办《网络安全审查办法》的双重审查。

七、结语

工信部在整个数据安全监管体系内具有不可替代的重要作用。工信部主管的装备与消费品工业、通信业、电子信息制造业、软件业、互联网行业是影响数字经济发展的基础行业、重点行业。工业领域、电信领域数据也是《数据安全法》提及的数据安全行业领域之首，是当前强化数据安全管理的重要领域。此次《管理办法》首先在工业与信息化领域明确了重要数据、核心数据的判断标准，并针对重要数据、核心数据提出了实操层面的增强合规要求，工业与电信行业企业应予以高度重视。

[5] 《数据安全法》第 24 条：国家建立数据安全审查制度，对影响或者可能影响国家安全的数据处理活动进行国家安全审查。

特别声明

汉坤律师事务所编写《汉坤法律评述》的目的仅为帮助客户及时了解中国或其他相关司法管辖区法律及实务的最新动态和发展，仅供参考，不应被视为任何意义上的法律意见或法律依据。

如您对本期《汉坤法律评述》内容有任何问题或建议，请与汉坤律师事务所以下人员联系：

段志超

电话： +86 10 8516 4123
Email： kevin.duan@hankunlaw.com