汉坤法律评述
2024 年 3 月 29 日

《自然资源领域数据安全管理办法》解读

作者：段志超 | 汪向阳 | 左今[1]

一、前言

自然资源部于 2024 年 3 月 22 日印发了《自然资源领域数据安全管理办法》（简称为**“《管理办法》”**），标志着自然资源领域数据安全管理尤其是重要数据管理制度逐项落地。《管理办法》进一步细化了自然资源领域的数据安全要求，为相关数据处理活动提供了明确的指导和规范，也将会对包括测绘和地图服务提供商、自动驾驶公司、智能网联汽车企业在内的相关数据处理者产生实质影响。

此外，继《数据安全法》的实施为各行各业的数据安全管理奠定了法律基础之后，包括工业和信息化、银行保险等多个领域均已相继发布了本领域的数据安全管理规定（包括征求意见稿）。在《网络安全法》《数据安全法》《个人信息保护法》等数据相关法规搭建起基本法规体系框架后，数据安全监管的垂直化趋势进一步显现。这和已经体现出行业特色的重要数据监管一起，将成为后续一个阶段里数据处理者需要关注的重心。

二、《自然资源领域数据安全管理办法》概述

《管理办法》全文共七章，与《工业和信息化领域数据安全管理办法（试行）》（简称为**“《工信部管理办法》”**）在结构上高度一致，部分规定内容也有相似之处。总体来说，《管理办法》明确了其适用范围，清晰划分了自然资源领域行业监管部门在数据安全监督方面的责任，同时从数据分类分级管理、数据全生命周期安全管理以及数据安全监测预警与应急管理三个方面对数据处理者提出了具体的合规要求。

- **明确受监管的对象与主体：**《管理办法》旨在监管在中国境内开展的，或在境外履行自然资源部门职责过程中开展的自然资源领域非涉密数据处理活动。值得注意的是，《管理办法》将自然资源领域数据定义为在开展自然资源活动中收集和产生的数据，主要包括基础地理信息、遥感影像等地理信息数据等自然资源管理数据[2]。因此，地图服务提供商、自动驾驶行业企业等如果在业务活动中

[1] 实习生李雅琪对本文的写作亦有贡献。

[2] 《自然资源领域数据安全管理办法》第三条，本办法所称自然资源领域数据，是指在开展自然资源活动中收集和产生的数据，主要包括基础地理信息、遥感影像等地理信息数据，土地、矿产、森林、草原、水、湿地、海域海岛等自然资源调查监测数据，总体规划、详细规划、专项规划等国土空间规划数据，用途管制、资产管理、耕地保护、生态修复、开发利用、不动产登记等自然资源管理数据。
本办法所称自然资源领域数据处理者（以下简称数据处理者），是指开展自然资源领域数据处理活动的自然资源行业各类单位。
本办法所称数据安全，是指通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

处理了《管理办法》中规定的基础地理信息、遥感影像等自然资源管理数据，可能也会受到《管理办法》的监管。

- **多层级且权责一致的监管体系：**《管理办法》明确了行业监管部门对于数据安全的监督责任，沿袭《工信部管理办法》规定，秉承“谁管业务，谁管数据，谁管数据安全”原则，定义了从自然资源部到地方行业监管部门（各省、自治区、直辖市自然资源主管部门、海洋主管部门）以及国家林业和草原局的监管职责。在重要数据与核心数据目录编制和报备、数据安全风险监测机制等具体合规要求上，也明确赋予了各层级监管部门的职责。

- **创新重要数据识别指标并建立数据目录：**为落实《数据安全法》框架下的数据分类分级保护制度，《管理办法》结合自然资源领域数据特点，创新性地提出以参考指标判断重要数据和核心数据的方式。并且在参考指标的选择上，不再局限于影响后果的判定，还增加了覆盖范围、规模、精度等标准，更加审慎合理、易于操作。同时《管理办法》提出建立行业重要数据与核心数据目录（简称为“**数据目录**”），并要求数据处理者报备本单位的重要数据和核心数据目录，进一步推动国家重要数据和核心数据可识别可管控。

- **细化数据全生命周期的安全管理要求：**《管理办法》还为自然资源领域的数据处理者提出了数据处理各环节的合规要求，涵盖了从数据收集到销毁的整个生命周期，并强调了重要数据和核心数据的特殊合规要求。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，具体合规要求请参见本文附件中的合规义务梳理表。

- **重要数据处理者应开展年度风险评估：**数据安全监测预警与应急管理方面，《管理办法》明确要求重要数据处理者每年开展一次风险评估，并建议核心数据处理者优先使用第三方评估机构开展风险评估。该要求与汽车、工信领域的要求一致，对于同时落入多个行业的重要数据范围内的重要数据处理者，可能需要向不同的主管部门报送风险评估报告。此外，《管理办法》也要求数据处理者开展风险监测，建立风险报告机制，制定应急预案并每年向监管部门报告数据安全处置情况。

三、汽车行业测绘地理信息合规新动态

（一）汽车行业测绘地理信息相关规定

如前所述，《管理规定》的监管对象包括基础地理信息、遥感影像等地理信息数据，这些信息通常在测绘活动中产生，并被归类为“测绘地理信息”。由于测绘地理信息在实现高级别自动驾驶功能，以及制作自动驾驶技术所需的高精度地图中发挥着关键作用，因此，我们理解，智能网联汽车企业、自动驾驶相关企业以及地图服务提供商等都可能受到《管理规定》的影响。

在现有的法律框架下，测绘地理信息因其对国家安全的重要性而受到国家的严格监管，尤其体现在对测绘活动的严格资质限制。一方面，根据 2022 年自然资源部发布的《自然资源部关于促进智能网联汽车发展维护测绘地理信息安全的通知》，智能网联汽车通过车辆的传感器处理测绘地理信息的行为被定义为测绘活动。另一方面，根据《测绘法》的要求，国家对从事测绘活动的单位实行测绘资质管理制度，同时根据 2016 年国家测绘地理信息局发布的《关于加强自动驾驶地图生产测试与应用管理的通知》，自动驾驶地图数据的采集、编辑加工和生产制作必须由具备甲级测绘资质的单位执行。因此，自动驾驶相关企业如想使用测绘地理信息，往往需要取得甲级测绘资质或与具备资质的图商进行合作。

此外，根据 2020 年自然资源部与国家保密局发布的《测绘地理信息管理工作国家秘密范围的规定》，部分测绘地理信息，包括一定范围的基础地理信息、遥感影像等属于国家秘密，受到更加严格的保密和

监管要求。

（二）汽车行业测绘地理信息监管形势趋严

随着数据在国家安全领域的影响日益显著，对于测绘地理信息的监管和执法也随之加强。2021 年，测绘单位统一复审换证过程中，31 家持有测绘资质的企业中仅有 19 家通过复审，且几乎没有主机厂，有超过三分之一的企业未能继续持有测绘资质证书。此外，2021 年某公司还因“未取得测绘资质证书，擅自从事测绘活动”和“使用未经依法审核批准的地图提供服务”受到北京市规划和自然资源委员会的行政处罚，没收违法所得高达千万。可见国家对于导航电子地图制作甲级测绘资质的审查趋于严格，对于测绘地理信息的安全保障也更加重视。

本次自然资源部发布的《管理规定》，更加强调和细化了对于测绘地理信息管理的数据分类分级、全生命周期安全管理和安全监测等合规要求。因此，地图服务提供商、自动驾驶行业企业等如果在业务活动中处理了《管理办法》中规定的基础地理信息、遥感影像等数据，需要密切关注《管理规定》的合规要求，确保数据处理活动符合最新的监管要求。

尽管监管政策日益严格，但不可否认测绘地理信息在推动高级别自动驾驶功能测试等高新技术领域扮演着至关重要的角色。我们认为，近年来国家对于测绘地理信息相关要求的加强和细化，目的在于构建一个更加全面和严格的监管框架，并通过法律手段确保测绘地理信息的安全。在企业能够符合法律要求的基础上，仍然可以期待未来对测绘地理信息进行合理开放的使用。

四、重要数据与核心数据监管动向

（一）重要数据与核心数据的认定

《管理办法》落实了《数据安全法》中国家建立数据分类分级保护制度的总体要求，提出了自然资源领域内的数据分类分级的标准，重要数据、核心数据和一般数据的定义，特别是明确了判断重要数据与核心数据的参考指标。

就数据分类，《管理办法》将自然资源领域的数据分为地理信息数据、自然资源调查监测数据、国土空间规划数据、自然资源管理数据等几类，并且提示分类将可能在后续发布的自然资源领域数据分类分级标准规范中进行细化。

就数据分级，《管理办法》提出了根据“数据重要性、精度、规模、安全风险，以及数据价值、可用性、可共享性、可开放性等，判断数据遭到篡改、破坏、泄露或者非法获取、非法利用后的影响对象、影响程度、影响范围”，从而为数据定级的综合判断标准。《管理办法》延续了《数据安全法》《工信部管理办法》等法律规定的分级思路，将数据分为一般数据、重要数据和核心数据三个级别，同时根据自然资源领域的数据特点，创新性地提出了判断重要数据的参考指标。

数据级别	定义与指标
重要数据	特定领域、特定群体、特定区域或达到一定精度和规模，一旦被泄露或篡改、损毁，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。 结合自然资源领域数据特点，满足以下两项（含）以上参考指标的为重要数据：

数据级别	定义与指标
	（一）支撑党中央和国务院赋予的“两统一[3]”职责产生的具有不可替代性和行业唯一性的，一旦发生数据篡改、泄露或服务中断等安全事故，将影响自然资源部门履行职责，对全国范围内服务对象产生重要影响的数据。 （二）涉及国民经济和重要民生的，为其他行业、领域提供自然资源基础数据支撑的，一旦发生数据安全事故会对其他行业、领域造成重要影响的数据。 （三）覆盖多个省份甚至全国，规模大、精度高，且极具敏感性、重要性的数据。 （四）直接影响国家关键信息基础设施正常运行服务的数据。 （五）危害国家安全、国家经济竞争力、危害公众接受公共服务、危害公民生存条件和安定工作生活环境、危害公民的生命财产安全和其他合法利益、导致社会恐慌等的数据。 （六）我国法律法规及规范性文件规定的其他自然资源重要数据。
核心数据	对领域、群体、区域具有较高覆盖度或达到较高精度、较大规模、一定深度的重要数据，一旦被非法使用或共享，可能直接影响政治安全。核心数据主要包括关系国家安全重点领域的数据，关系国民经济命脉、重要民生和重大公共利益的数据，经国家有关部门评估确定的其他数据。 符合重要数据指标，且关系国家经济命脉、重要民生和重大公共利益、影响政治安全的数据为核心数据。
一般数据	除重要数据、核心数据以外的其他数据。

从重要数据判定的参考指标上来看，《管理办法》对于重要数据的判定仍以国家安全为核心，大部分指标采用了结果导向原则，但同时也结合自然资源领域数据的特点，提出了“覆盖范围广、规模大、精度高”等数据性质方面的衡量指标，便于数据处理者自行判断。这些指标与最近发布的《GBT 43697-2024 数据安全技术 数据分类分级规则》（简称为**“数据分类分级国标”**）中的重要数据识别指南附录相辅相成，后者列出了 17 项考量因素，其中也包括“直接影响领土安全和国家统一，或反映国家自然资源基础情况，如未公开的领陆、领水、领空数据”等自然资源领域重要数据判断的因素，与《管理办法》的理念有一致之处。可以看出，数据分类分级国标提供了全行业的指导性要求，而《管理办法》则针对自然资源领域的重要数据识别提供了更为明确的指导。

预计随着自然资源部发布数据分类分级标准规范，重要数据的识别将被进一步厘清。此外，数据处理者在自行判断并上报重要数据和核心数据后，还需经过国家有关部门的认定，以确保最终形成的数据目录符合国家数据安全管理的要求。

（二）建立双向重要数据与核心数据目录识别与报备机制

为了有效推进国家重要数据与核心数据的识别工作，落实本领域数据分类分级保护制度，《管理办法》提出建立行业重要数据与核心数据目录，并要求数据处理者形成本单位的重要数据和核心数据目录。

与《工信部管理办法》类似，《管理办法》提出了一种双向识别与完善重要数据和核心数据目录的

[3] “两统一”指统一行使全民所有自然资源资产所有者职责、统一行使所有国土空间用途管制和生态保护修复职责。

机制，这一机制包括“自上而下”的编制与审核数据目录和“自下而上”的定期更新与报备数据目录。

具体而言，就行业数据目录，《管理办法》规定自然资源部负责制定自然资源领域的数据分类分级标准、重要数据与核心数据的识别认定以及数据安全保护的相关规范。地方行业监管部门负责组织并实施数据分类分级管理工作，进行重要数据与核心数据的识别和审核。自然资源领域数据处理者则负责定期填写并上报重要数据和核心数据目录。

此外，针对数据处理者自身的数据目录，《管理办法》规定了分层级报备制度，要求自然资源部所属的数据处理者应当将本单位的重要数据和核心数据目录向自然资源部报备，其他数据处理者应当将本单位数据目录向本地区行业监管部门报备。报备后，数据目录都将最终经过国家有关部门的认定并反馈给数据处理者。

这一机制有利于推动重要数据和核心数据目录的建立，并确保数据目录的时效性。对于数据处理者来说，应当密切关注自然资源部发布的标准规范，这将直接影响数据处理者如何识别并上报重要数据与核心数据。

五、结语

总体来说，《管理办法》响应了《数据安全法》中的国家数据安全工作协调机制，为自然资源领域的数据安全管理提供了指引，特别是进一步推动了该领域国家重要数据和核心数据的识别、分类分级保护以及数据安全风险信息的监测、分析、研判和预警等机制的落地。相关数据处理者后续应保持对数据目录和重要数据监管具体要求的关注，及时调整自身数据处理行为以及采取相关合规措施，避免由《管理办法》落实带来的合规风险。

附件：

《自然资源领域数据安全管理办法》数据处理者合规义务总结

义务类型	数据处理者一般义务	重要数据与核心数据处理者的特殊义务
数据梳理、报备义务（第 8–11 条）	■ 可在自然资源领域数据分类分级标准规范的基础上，细分数据的类别和一般数据级别	■ 定期按照自然资源领域数据分类分级标准规范梳理填报重要数据和核心数据目录 ■ 向所属行业监管部门[4]报备[5]本单位重要数据和核心数据目录 ■ 在报备内容发生重大变化[6]的三个月内履行变更手续
数据分级防护义务（第 12 条）	■ **分级保护**：不同级别数据同时被处理且难以分别采取保护措施的，按照其中级别最高的要求保护 ■ **制度建设**：建立数据安全管理制度，制定数据全生命周期各环节的具体分级防护要求和操作规程 ■ **人员管理**：配备数据安全管理人员；定期对从业人员开展数据安全知识和技能相关教育培训 ■ **制度落实**：落实网络安全等级保护、关键信息基础设施安全保护、密码保护和保密等制度要求 ■ **保护措施**：采取相应技术措施和其他必要措施保障数据安全；落实法律法规等规定的其他措施 ■ **权限控制**：合理确定数据处理活动的操作权限，严格实施人员权限管理 ■ **应急管理**：制定数据安全事件应急预案，开展应急演练	■ **组织架构**：建立覆盖本单位相关部门的数据安全工作体系，明确数据安全负责人[7]和管理机构，建立常态化沟通与协作机制 ■ **人员管理**： - 明确数据处理关键岗位和岗位职责，并要求关键岗位人员签署数据安全责任书[8] - 涉及核心数据的相关关键岗位人员、信息系统建设和运维单位等，提交公安机关、国家安全机关进行国家安全背景审查 ■ **权限控制**：按照业务工作需要和最小授权原则，依据岗位职责设定数据处理权限，根据人员变动及时调整 ■ **日志记录**：建立内部登记、审批机制，对重要数据和核心数据的处理活动进行严格管理并留存记录不少于六个月

[4] 自然资源部所属的数据处理者应当将本单位重要数据和核心数据目录向自然资源部报备，国家林业和草原局所属的数据处理者应当将本单位重要数据和核心数据目录向国家林业和草原局报备，其他数据处理者应当将本单位重要数据和核心数据目录向本地区行业监管部门报备。

[5] 报备内容包括但不限于数据类别、级别、规模、精度、来源、载体、使用范围、对外共享、跨境传输、安全情况及责任单位情况等，不包括数据内容本身。

[6] 重大变化是指数据内容发生变化导致原有级别不再适用的，或某类重要数据和核心数据规模变化 30%以上的，等等。

[7] 本单位法定代表人或主要负责人是数据安全第一责任人，领导班子中分管数据安全的班子成员是直接责任人，其他成员对职责范围内的数据安全工作负领导责任，履行数据安全保护义务，接受监督。

[8] 责任书内容包括但不限于数据安全岗位职责、义务、处罚措施、注意事项等内容。

义务类型	数据处理者一般义务	重要数据与核心数据处理者的特殊义务
		■ **安全保护**：综合运用加密、鉴权、认证、脱敏、校验、审计等技术手段进行数据全生命周期安全保护，并依法使用商用密码进行保护 ■ **涉重要数据信息系统建设、运维：** - 未经委托方批准不得转包、分包 - 建设运维人员未经委托方明确授权，不得处理委托方的重要数据 - 系统建设、运维过程中收集、产生的数据，不得用于其他用途 - 服务完成后按照与委托方约定处理或及时删除 ■ **加强人员、经费保障**
数据收集环节义务（第 13 条）	■ 遵循合法、正当原则，在法律法规规定的目的、范围内收集数据 ■ 根据数据安全级别采取相应的安全措施	■ **直接收集**：加强重要数据和核心数据收集生产人员、设备的管理 ■ **间接收集**：与数据提供方通过签署相关协议、承诺书等方式，明确双方法律责任
数据存储环节义务（第 14 条、第 20 条）	■ 依据法律法规规定的方式和期限存储数据 ■ 可以从物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全等方面，加强数据存储安全管控	■ 存储重要数据的，应当落实第三级及以上网络安全等级保护要求 ■ 存储核心数据的，应当落实关键信息基础设施安全保护要求或第四级网络安全等级保护要求 ■ 在中华人民共和国境内收集和产生的重要数据，应当在境内存储
数据加工使用处理环节义务（第 15 条）	■ 采取访问控制、数据防泄露、操作审计等管控措施，确保过程安全、合规、可控、可溯源 ■ 防范数据关联挖掘、分析过程中有价值信息和个人隐私泄露的安全风险 ■ 明确数据使用加工过程中的相关责任 ■ 按照数据级别采取相应的措施保护数据的安全性 ■ 使用真实可靠的数据，审查、核实数据来源、收集过程	■ 实施严格的访问控制 ■ 建立数据可信可控、日志留存审计、风险监测评估、实时监控、应急处置、数据溯源等相关技术和管理机制

义务类型	数据处理者一般义务	重要数据与核心数据处理者的特殊义务
	■ 涉及利用数据进行自动化决策的，应当保证决策的透明度和结果公平合理	
数据传输环节义务（第 16 条）	■ 根据传输的数据类型、级别和应用场景，制定安全策略并采取保护措施	■ 采取校验技术、密码技术、安全传输通道或者安全传输协议等措施
数据提供环节义务（第 17 条、第 20 条）	■ 依法依规提供数据，明确提供的范围、类别、条件、程序等 ■ 提供的数据应当限于实现数据接收方处理目的的最小范围 ■ 告知数据接收方按照对应级别进行分类分级保护，采取必要的安全保护措施	■ 涉及重要数据的，应当： - 与数据接收方签订数据安全协议 - 采取技术措施定期监测数据共享、调用的情况 - 配备风险隔离、认证鉴权、威胁告警等安全保护措施 - 在中华人民共和国境内收集和产生的重要数据，确需向境外提供的应当开展数据出境安全评估 ■ 涉及核心数据的，应当： - 采取必要的安全保护措施，并上报自然资源部 - 自本年度 1 月 1 日起可能累计达到总量 30%及以上的，应当经自然资源部报国家数据安全工作协调机制组织风险评估[9]
数据公开环节义务（第 18 条）	■ 在数据公开前分析研判可能对国家安全、公共利益产生的影响，存在显著负面影响或风险的，不得公开	/
数据销毁环节义务（第 19 条）	■ 建立数据销毁制度，明确销毁对象、规则、流程和技术等要求 ■ 对销毁活动进行记录和留存 ■ 依据法律法规规定、合同约定等请求销毁的，应当销毁相应数据	■ 采取必要的安全保护措施 ■ 事前向行业监管部门报告数据销毁方案 ■ 引起重要数据和核心数据目录变化的，应当及时向行业监管部门报备，不得恢复销毁数据
数据转移环节义务（第 21 条）	■ 因重组等原因需要转移数据的，应当明确数据转移方案	■ 涉及重要数据的，应当采取必要的安全保护措施，事前向行业监管部门报告数据转移方案 ■ 引起重要数据目录发生变化的，应当及时向行业监管部门报备

[9] 涉及国家机关依法履职或单位内部流动的除外。

义务类型	数据处理者一般义务	重要数据与核心数据处理者的特殊义务
数据委托处理环节义务（第22条）	■ 通过签订合同协议等方式，明确委托方与受托方的数据安全责任和义务 ■ 除法律法规等另有规定外，未经委托方同意，受托方不得将数据提供给第三方	■ 涉及重要数据的，委托方应当： - 评估或核实受托方的数据安全保护能力、资质 - 严格审批程序 - 明确受托方的数据处理权限和保护责任 - 监督受托方履行数据安全保护义务
日志记录留存义务（第23条）	■ 在数据全生命周期记录数据处理、权限管理、人员操作等日志 ■ 采用商用密码技术保护日志的完整性 ■ 一般数据的日志留存时间不少于六个月	■ 涉及重要数据安全事件处置、溯源的，日志留存时间不少于一年 ■ 涉及向他人提供、委托处理、共同处理重要数据的，日志留存时间不少于三年 ■ 涉及核心数据安全事件处置、溯源的，日志留存时间不少于三年
数据安全监测义务（第24条）	■ 开展数据安全风险监测，及时排查安全隐患，采取必要的措施防范数据安全风险	/
安全风险评估义务（第25条）	■ 保留风险评估报告至少三年	■ 重要数据处理者应当自行或委托第三方评估机构，每年对其数据处理活动至少开展一次风险评估，及时整改风险问题，并向行业监管部门报送风险评估报告[10] ■ 核心数据处理者优先使用第三方评估机构开展风险评估 ■ 组织重要数据安全风险评估时，应当对其数据查询、下载、修改、删除等重点操作的日志开展审计分析，发现违规或异常行为应及时采取相应处置措施
安全事件风险报告义务（第26条）	■ 及时将可能造成较大及以上安全事件的风险向行业监管部门报告	/

[10] 风险评估报告应当包括处理的重要数据的类别、数量，开展数据处理活动的情况，面临的数据安全风险、应对措施及其有效程度等。

义务类型	数据处理者一般义务	重要数据与核心数据处理者的特殊义务
安全事件应急处置义务（第 27 条）	■ 在数据安全事件发生后，按照应急预案及时开展应急处置 ■ 每年向行业监管部门报告数据安全事件处置情况 ■ 对发生的可能损害用户合法权益的数据安全事件，应当及时告知用户，并提供减轻危害措施	■ 涉及重要数据和核心数据的安全事件，第一时间向行业监管部门、属地公安部门报告，事件处置完成后在一周以内形成总结报告
监督检查配合义务（第 28 条）	■ 应当对行业监管部门监督检查予以配合	/
保密义务（第 29 条）	■ 数据处理者及其委托的数据安全风险评估机构工作人员对在履行职责中知悉的个人信息、商业秘密等，应当严格保密	/
其他义务（第 33–35 条）	■ 开展涉及个人信息的数据处理活动，应当遵守有关法律法规的规定 ■ 涉及国家秘密信息或自然资源领域数据汇聚关联后属于国家秘密事项的数据处理活动，应当符合国家及部门相关保密规定 ■ 法律法规规定开展数据处理活动应当取得行政许可的，应当依法取得许可	/

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