交通运输部关于印发《交通运输数据安全管理办法》的通知

交科技规〔2026〕3号

各省、自治区、直辖市、新疆生产建设兵团及计划单列市交通运输厅（局、委），国家铁路局、中国民用航空局、国家邮政局，中国远洋海运集团有限公司、招商局集团有限公司、中国交通建设集团有限公司，公路水路关键信息基础设施运营者、重要数据处理者，部属各单位、部内各司局：

现将《交通运输数据安全管理办法》印发给你们，请认真贯彻执行。

交通运输部

2026年6月18日

（此件公开发布）

交通运输数据安全管理办法

第一章　总则

第一条 为规范交通运输数据处理活动，保障数据安全，保护个人、组织的合法权益，维护国家安全和公共利益，根据《中华人民共和国数据安全法》《中华人民共和国网络安全法》《中华人民共和国个人信息保护法》《网络数据安全管理条例》等法律法规，制定本办法。

第二条 交通运输数据安全工作坚持“谁管业务，谁管业务数据，谁管数据安全”和“属地管理”原则，实行分级管理和分工负责。

第三条 在国家数据安全工作协调机制统筹协调下，交通运输部负责综合交通运输和公路、水路领域数据安全管理工作，国家铁路局、中国民用航空局、国家邮政局按职责分别负责铁路、民航、邮政领域数据安全管理工作。

交通运输部数据安全主管机构负责综合交通运输和公路、水路领域数据安全监管，组织制定数据安全相关政策制度和标准。

交通运输部业务管理机构按职责负责本业务领域数据安全监管。交通运输部海事局、长江航务管理局、救助打捞局和中国船级社负责本系统数据安全监管。

省级交通运输主管部门负责对本地区交通运输数据处理活动和安全保护进行监管，指导市、县级交通运输主管部门开展数据安全管理工作，配合交通运输部和同级网信、公安、国家安全、数据管理等部门开展相关工作。

第四条 交通运输数据处理者（以下简称数据处理者）承担数据安全主体责任，履行数据安全保护义务，加强数据全生命周期安全保护，建立健全管理制度，采取技术措施和其他必要措施，保护数据免遭篡改、破坏、泄露或者非法获取、非法利用。

第五条 鼓励和支持交通运输数据依法开放共享、授权运营和交易流通，以及相关技术、产品、服务创新，促进数据要素安全合规流通和高效开发利用。

第二章　数据分类分级保护

第六条 交通运输部指导开展综合交通运输和公路、水路领域数据分类分级保护工作，确定行业重要数据目录，提出核心数

据目录建议，加强目录动态管理。

省级交通运输主管部门组织开展本地区数据分类分级保护工作，并向交通运输部报送重要数据识别情况。

数据处理者应当建立数据分类分级保护规程，开展数据分类分级保护工作，定期更新数据目录，按规定识别、申报重要数据。对确认为重要数据的，交通运输主管部门应当及时向数据处理者告知或发布。

第七条 根据数据在经济社会发展和交通运输运行中的重要程度，以及一旦遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者个人、组织合法权益造成的危害程度，将交通运输数据划为核心数据、重要数据、一般数据三个级别。其中，一般数据从高到低分为一般3级数据、一般2级数据和一般1级数据。

第八条 数据内容、规模、时效性、应用场景、加工处理方式等发生变化，或因国家有关要求，导致原定级别不再适用的，数据处理者应当及时变更数据级别。

涉及重要数据和核心数据级别变更的，应当按规定重新开展数据分类分级工作。涉及重要数据和核心数据信息变更的，应当在30日内报告。

第三章　数据全生命周期安全管理

第九条 数据处理者应当建立健全数据全生命周期安全管理制度，明确登记、审批、处理、操作等规程和权限，根据数据级别采取就高从严的安全保护措施。

重要数据、核心数据处理者应当加强数据处理活动全过程监测预警和处置，采取商用密码技术保障数据全生命周期安全。

第十条 数据处理者应当加强对从业人员数据安全知识和技能教育培训，根据需要配备数据安全管理人员。

重要数据处理者应当按规定明确数据安全负责人和数据安全管理机构。数据安全负责人应当由数据处理者管理层成员担任，有权直接向有关交通运输主管部门报告数据安全情况。

核心数据处理者应当对数据安全负责人和关键岗位人员、核心数据信息系统建设和运维单位等进行安全背景审查。

第十一条 数据处理者应当按照合法、正当、必要原则开展数据收集，不得窃取或者以其他非法方式收集数据。涉及收集个人信息的，明确告知收集和使用规则，并取得个人同意。涉及收集敏感个人信息的，还应取得个人单独同意。依照法律法规有关

规定可以不向个人告知、不需取得个人同意的除外。

通过间接途径收集数据的，应当确保数据来源合法、真实可信，保证数据的完整性和可用性。使用自动化工具访问、收集数据的，应当确保不造成网络服务影响。

第十二条 数据处理者应当根据业务需求和数据级别确定数据存储方式、保存期限以及保护措施。交通运输主管部门处理的个人信息，关键信息基础设施运营者在我国境内运营中收集、产生以及有关法律法规明确要求的个人信息和重要数据，应当在境内存储。

信息系统存储重要数据的应当至少满足网络安全等级保护第三级要求，存储核心数据的应当至少满足第四级要求或者关键信息基础设施安全保护要求，并优先使用安全可信的产品和服务。涉及使用云计算服务存储重要数据的，应当选择通过安全评估的云计算服务。

数据处理者应当加强数据存储、备份介质管理，定期进行数据备份。重要数据和核心数据应当实施容灾备份，定期开展数据恢复测试和灾难恢复演练。

第十三条 数据处理者应当按照数据级别采取访问控制、数据脱敏加密、操作审计等保护措施，确保数据使用和加工过程安

全、合规、可控、可溯源。

使用和加工重要数据和核心数据的，应当实施严格的访问控制，建立健全数据可信可控、日志留存审计、风险监测评估、数据溯源等技术体系。

第十四条 数据处理者应当根据数据类型、数据级别和应用场景等制定数据传输安全策略并采取必要的保护措施。

传输一般3级数据、重要数据和核心数据的，应当采取校验技术、密码技术、安全传输通道或者安全传输协议等保护措施。

第十五条 数据处理者在交换共享、授权运营等数据提供过程中，应当按照最小必要原则向数据接收方提供所需数据。提供数据涉及敏感信息的，应当进行必要的脱敏处理。

提供个人信息、重要数据和核心数据的，应当核验数据接收方的数据安全保护能力，通过签订合同或协议等方式，约定数据处理的目的、方式、范围等，明确数据接收方的保护义务和措施，强化履约监督，发现不按约定履行的立即停止数据提供。

第十六条 交通运输主管部门按规定及时、准确地公开政务数据。依法不予公开的除外。

数据处理者应当加强开源数据安全管理，规范公路、水路视频图像和科学数据公开管理。

数据处理者不得公开其处理的个人信息，取得个人单独同意的除外。

第十七条 数据处理者应当建立数据删除制度，对删除活动进行记录和留存，采用信息清除技术确保数据删除后不可恢复。数据删除从技术上难以实现的，应当停止除存储和采取必要的安全保护措施之外的处理。

法律法规规定应主动删除、个人请求删除的个人信息，以及合同或协议约定删除的数据，数据处理者应当依法删除。

删除重要数据和核心数据应当在操作前制定数据删除方案，评估可能存在的风险，并提前报告。

第十八条 数据处理者因合并、分立、解散、破产等原因需要转移数据的，应当明确数据转移方案，通过协议、承诺等方式约定数据接收方全面承接对应数据的安全保护义务。涉及个人信息的，应当向个人告知数据接收方名称或者姓名和联系方式。

涉及重要数据、核心数据和 1000 万人以上个人信息的，应当提前报告数据转移方案、接收方名称或者姓名和联系方式等。数据转移应当采用安全可控方式，确保过程可追溯。

第十九条 数据处理者委托他人处理、与他人共同处理数据的，数据安全责任不因委托而改变，应当通过签订合同或协议等

方式，明确双方数据安全责任和义务。未经委托方同意，数据接收方不得向他人提供数据，不得加工、训练、挪用数据，不得开展数据关联分析。

委托处理重要数据和核心数据的，还应当核实或评估数据接收方的数据安全保护能力和资质。

第二十条 数据处理者向境外提供数据，应当遵守国家数据跨境安全管理有关规定，履行数据安全保护义务，并采取技术措施和其他必要措施，保障数据跨境安全。不得采取数据拆分等手段规避相关义务。向境外提供个人信息的，应当按规定履行告知、取得个人单独同意、进行个人信息保护影响评估等义务。

第二十一条 利用人工智能技术开展数据处理活动，数据处理者应当在模型算法投入使用前，评估语料库、训练数据及算法的合理性、正当性、可解释性，以及数据利用对相关主体合法权益的影响、伦理风险和防控措施有效性。

强化人工智能生成数据及人工智能产品的安全管理，按照生成数据及数据处理结果对应的分类分级，严格落实相应的数据安全管理要求。

提供生成式人工智能服务的，应当加强训练数据和训练数据处理活动的安全管理，强化数据标注质量评估。

第二十二条 数据处理者应当留存数据全生命周期的数据处理、权限管理、人员操作等网络日志，并开展分类分级管理，满足风险溯源和事件处置需要。

网络日志留存时间不少于6个月。政务应用系统访问、数据库操作以及重要数据安全事件相关日志留存时间不少于1年。核心数据安全事件相关日志，向其他数据处理者提供、委托处理、共同处理个人信息和重要数据的处理情况记录，留存时间不少于3年。

第四章　数据安全风险评估

第二十三条 重要数据、核心数据处理者和1000万人以上个人信息处理者，应当每年开展数据安全风险评估（以下简称风险评估），并报送风险评估报告。

鼓励一般数据处理者至少每3年开展1次风险评估。

大型网络平台运营者按照有关规定开展风险评估。

第二十四条 存在下列情形之一的，数据处理者应开展风险评估：

（一）发生重大数据安全事件或被通报存在重大数据安全风

险。

（二）提供、委托处理、共同处理重要数据，履行法定职责或者义务的除外。

（三）重要数据处理者出现合并、分立、解散等重大变化，承载重要数据的信息系统发生重大变更。

（四）向境外提供数据等高风险数据处理活动。

（五）其他可能危害国家安全、公共利益或严重危害个人、组织合法权益的情形。

第二十五条 数据处理者可自行或委托第三方开展风险评估，第三方应当为国家有关部门认定的专业检测评估机构，或符合国家有关规定的其他机构。

第二十六条 风险评估报告应当符合有关规定，至少保存 3 年，可作为交通运输主管部门数据安全监督检查依据。

第二十七条 数据处理者应当及时整改风险评估发现的问题，消除风险隐患。

风险评估中发现重大数据安全风险、事件或特殊紧急情况的，重要数据和核心数据处理者应当及时报告。

第二十八条 交通运输个人信息处理者应当按规定定期自行或者委托专业机构开展个人信息保护合规审计。

第五章　数据安全监测预警与应急处置

第二十九条 交通运输部统筹建立行业网络和数据安全风险监测预警与信息通报工作机制，省级交通运输主管部门建立本地区工作机制，加强与网信、公安、国家安全、数据管理等部门的信息共享。

数据处理者应当建立数据安全风险监测机制，及时发现、处置、报告安全风险和事件。

根据对国家安全、社会秩序、经济建设、公众利益等造成的影响范围和危害程度，将交通运输数据安全事件分为特别重大、重大、较大和一般4个等级。

第三十条 交通运输主管部门、数据处理者应当制定数据安全事件应急预案，加强预警响应和应急联动，定期组织开展应急演练。重要数据和核心数据处理者应当每年开展应急演练。

第三十一条 对个人、组织合法权益造成危害的数据安全事件，数据处理者应当及时通知利害关系人，发现涉嫌违法犯罪线索的，应当按规定向公安机关、国家安全机关报案，并配合开展侦查、调查和处置工作。

第三十二条 数据处理者应当在数据安全事件处置结束后，完成事件的调查评估，提出改进措施并落实。

第六章　监督检查与责任追究

第三十三条 交通运输主管部门定期组织开展风险评估，依法开展数据安全检查，指导监督数据处理者履行数据安全保护义务。数据处理者应当予以配合，及时整改风险隐患。

第三十四条 交通运输主管部门开展数据安全监督检查，应当客观公正，不得向被检查单位收取费用，不得访问、收集与数据安全无关的业务信息，获取的信息应当依法予以保密，只能用于维护数据安全的需要，不得用于其他用途。

发现数据处理活动存在较大安全风险的，可以按规定的权限和程序，要求数据处理者暂停相关服务、完善技术措施等，消除数据安全隐患。

第三十五条 交通运输主管部门在开展数据安全监督检查时，应当加强协同配合、信息沟通，合理确定检查频次和检查方式，避免不必要的检查和交叉重复检查。

第三十六条 风险评估、网络安全等级测评、关键信息基础

设施安全检查、商用密码应用安全性评估中涉及数据安全内容重合的，结果可互相采信。

第三十七条 违反本办法规定的，由交通运输主管部门责令改正，对直接负责的主管人员和其他直接责任人员依法给予处分或处罚。涉嫌违法犯罪的，按规定向有关部门报告。

第七章　附则

第三十八条 本办法第八条、第十七条、第十八条、第二十三条、第二十七条涉及的报告、报送情形，应当由省级交通运输主管部门审核后，报至交通运输部。部属单位、中央交通运输企业可直接报至交通运输部。

第三十九条 开展核心数据以及涉及国家秘密、工作秘密的数据处理活动，按照国家有关规定执行。

第四十条 本办法由交通运输部负责解释。

第四十一条 本办法自 2026 年 7 月 1 日起实施。