北京市高级别
自动驾驶示范区

2022

北京市高级别自动驾驶示范区
数据分类分级白皮书

指导单位：北京市高级别自动驾驶示范区工作办公室
编写单位：北京车网科技发展有限公司
国汽(北京)智能网联汽车研究院有限公司

2022年9月

编写说明

本白皮书重点围绕北京市高级别自动驾驶示范区的建设和运营实际，从保障示范区自动驾驶数据（以下称“示范区数据”）全生命周期安全合规、促进数字经济发展的现实需求出发，提出了一套数据分类分级管理办法，为示范区开展数据安全治理工作奠定基础。

本白皮书的编制工作发起于北京市高级别自动驾驶示范区，旨在发掘共性需求、建立行业共识，为各地智能网联汽车测试示范区（包括智能网联汽车测试与示范运营基地、智慧交通应用示范区、车联网示范区、车联网先导区等）开展数据分类分级和安全管理工作提供参考方案。

本白皮书在编制过程中深入研究了我国数据安全相关法律法规要求，梳理了相关行业的数据分类分级方法，结合智能网联汽车测试示范区数据资产特性，制定了符合示范区业务实际的数据分类维度和分级指标。

本白皮书在编制过程中邀请了智能网联汽车行业专家进行深入交流，并基于专家意见对文中的主要方法、工作流程、发展建议等内容进行完善，获得了行业专家的认可。期望在方案执行过程中能够与各智能网联汽车测试示范区达成共识，并获得行业主管机构认可，为后续开展数据分类分级标准化工作提供参考。

本白皮书的主要观点和内容仅代表编制组现阶段对智能网联汽车测试示范区数据分类分级工作方法的研判和思考，欢迎各方专家学者和企业代表提出宝贵意见，共同推进智能网联汽车测试示范区数据分类分级方法的完善。

本白皮书为《北京市高级别自动驾驶示范区数据安全》系列白皮书的第一部，在此基础上，北京车网科技发展有限公司将会继续联合行业力量围绕智能网联汽车测试示范区数据安全治理工作发布更多成果。

前言

为适应数字经济发展环境、统筹发展与安全、落实国家重大战略部署，我国相继出台《网络安全法》《数据安全法》《个人信息保护法》，对全行业数据安全保障工作提出总体要求，明确由各级政府、社会组织、企业和个人共同维护数据安全。汽车产业主管部门和行业学会、协会密集发布了一系列规范性文件，对智能网联汽车领域的数据安全治理工作提出具体要求，包括推进数据采集处理标准化、实施数据分类分级管理、开展数据资产登记和评估试点、面向社会提供安全可持续的数据服务等。

随着智能网联汽车测试示范区加速建设和运营，数据安全体系建设重要性愈发凸显。在各级政府的支持和指导下，各地测试示范区加速开展基础环境建设，为智能网联汽车多场景应用和推广提供测试验证和示范运营环境，推动车路云一体化智能网联汽车落地应用，赋能自动驾驶发展。在测试示范区运营过程中，智能网联汽车及智慧交通网络持续产生海量数据，但部分涉及国家重要数据和个人隐私数据，对数据安全和合规应用提出更高要求，因此测试示范区的数据安全体系建设逐渐引起行业重点关注。

作为数据安全保障的基础性工作，数据分类分级是智能网联测试示范区全面梳理大规模、多样化且动态流转数据的必要手段，是保障数据安全治理措施高效合理应用的前提条件。为响应国家数据安全法律法规要求，落实智能网联汽车测试示范区的数据安全治理工作，北京车网科技发展有限公司基于北京市高级别自动驾驶示范区数据资产特点及业务实际，启动数据分类分级方法研究工作，旨在明确智能网联测试示范区数据分类维度和分级指标，提供科学合理的数据分类分级方法，为各地智能网联测试示范区开展相关工作提供参考。

目 录

编制背景

近年来，在国家和各级政府的大力支持下，智能网联汽车测试示范区（以下简称示范区）建设取得丰硕成果，为验证智能网联汽车先进技术和应用模式提供了重要环境，同时在示范区运营过程中汇聚了大量的自动驾驶运行数据。本白皮书通过分析示范区数据安全治理形势，开展数据分类分级方法研究，力求为相关政策法规框架内开展的数据安全治理工作提供有效支撑。

（一）数据安全已上升至国家层面

提升智能网联汽车数据安全治理水平已成为公众的主要诉求之一。近年来全球数据安全事件频出，给各国社会环境造成了严重影响。2021年6月，9万名大众和奥迪客户的敏感数据遭到曝光，大众方面称此次数据泄露事件源于一起未经授权的第三方访问，但是调查显示这些被泄露的数据在之前的21个月内都没有得到妥善保护。2022年初，J.D. Power与《环球时报》为了解中国消费者对智能网联汽车数据安全和个人隐私数据的认知态度，发起了“2022中国消费者智能网联汽车数据安全和个人隐私意识与顾虑调查”，结果显示高达77.4%受访者表示非常介意或比较介意个人隐私数据的使用，只有2.5%的受访者完全不介意，与此同时，超过四成的受访者对现阶段相关企业妥善保护智能网联汽车涉及的个人敏感信息缺乏信心。

我国不断完善数据安全监管的顶层设计。近年来为保障数字经济健康发展，我国先后出台并实施的《中华人民共和国网络安全法》（以下简称网安法）、《中华人民共和国数据安全法》（以下简称数安法）、《中华人民共和国个人信息保护法》（以下简称个保法）等法律，明确了数据安全保障范围和管理原则，为配套标准规范制定和安全保障工作开展提供了重要指导。其中，网安法明确要求维护网络数据的完整性、保密性和可用性，保障网络信息依法有序自由流动（第十、十二条）；并要求采取数据分类、重要数据备份和加密等措施，切实履行网络安全保护义务（第二十一条）；同时对个人信息的安全收集和使用做了明确要求（第四十至第四十七条）。数安法则明确了“数据”“数据安全”“数据处理”等重要概念，并在数据安全制度层面明确提出实施数据分类分级保护、制定相关行业、领域重要数据目录，加强对重要数据的保护（第二十一条）。个保法重点关注个人信息数据保护，明确了个人信息及敏感个人信息的定义及处理规则；并提出对个人信息实行分类管理，切实保障个人信息安全（第五十一条）。

我国已初步形成汽车领域数据安全制度框架。国家互联网信息办公室于2021年11月发布《网络数据安全管理条例（征求意见稿）》，强调数据安全防护能力建设，保障数据依法有序自由流动，促进数据依法合理有效利用，分别对个人信息保护、重要数据安全和数据跨境安全管理做了明确要求。其中条例第五条也提出建立数据分类分级保护制度，将数据按照重要程度分为一般数据、重要数据、核心数据，并采取不同的保护措施，对个人信息和重要数据实行重点保护，对核心数据实行严格保护。

图 1 数据安全保障体系

围绕汽车数据安全，2021年9月，国家网信办、发改委、工信部、公安部、交通运输部联合发布了《汽车数据安全管理若干规定（试行）》，明确了“汽车数据”“敏感个人信息”“重要数据”“汽车数据处理”等定义，制定了汽车数据处理安全原则，并进一步规范了个人信息、敏感个人信息和重要数据的处理方法。

同月，工信部发布《关于加强车联网网络安全和数据安全工作的通知》，强调汽车数据有效保护和合法利用，保障车联网安全稳定运行。同时提出按照“谁主管、谁负责，谁运营、谁负责”的原则，实施数据分类分级管理，提升数据安全技术保障能力，规范数据开发利用和共享使用，并强化数据出境管理。

2022年2月，工信部为贯彻落实上位法和国家政策要求，编制并发布了《车联网网络安全和数据安全标准体系建设指南》，用以指导车联网网络安全和数据安全相关标准研制。其中在数据安全部分，指南提出研制通用要求、分类分级、出境安全、个人信息保护、应用数据安全五类标准，明确智能网联汽车、车联网平台、车载应用服务等领域的数据安全和个人信息保护要求。

图 2 数据安全标准体系框架

（二）示范区数据安全面临挑战

随着智能网联汽车产业高速发展，相关运行数据爆发式增长，海量结构化和非结构化数据在交通参与者、数据平台运营企业及第三方服务提供商之间常态化流转交互，由此可能产生的数据过度采集、不当存储、越界使用等问题给国家安全、行业利益和个人权益带来了诸多安全隐患。

智能网联汽车数据安全保障在标准规范方面依然有待完善。现行的网络安全标准规范难以覆盖车联网行业的数据安全保障需求，在此背景下国家面向车联网应用场景规划了数据安全标准体系框架，总体明确了数据安全治理目标和研究方向，但现阶段仍缺乏实施层面的标准规范，智能网联汽车数据安全保障在执行阶段缺乏参考方案和技术指导，相关标准的可行性和有效性有待验证，与上位法和顶层规划的协同机制有待检验。

行业内仍然缺乏明确的方法指导自动驾驶数据盘点。由于智能网联汽车相关研发、测试、运营数据量庞大、数据类型复杂，同时涉及车主、驾驶人、乘客、车外人员等的个人信息，并包含高精度地图信息、交通信号、高清晰度的道路环境数据等关系国家安全和社会安定的信息。目前行业内亟需面向真实运营场景全面盘点数据资产、梳理自动驾驶敏感数据和重要数据的可落地方案，从而对相关数据类型实施有效的数据安全治理手段，在保障数据安全的前提下为数据共享提供条件。

智能网联汽车数据安全保障不力阻碍了数据价值发掘。由于智能网联汽车技术研发需要，单一运营主体采集的自动驾驶数据往往难以满足企业的技术研发和优化需求，因此自动驾驶数据的流转通常涉及自动驾驶科技企业、整车企业、车队运营企业、数据平台运营企业、交通监管部门等多个主体。现阶段由于数据归属和数据安全保障责任主体界定不清晰，同时缺乏明确的数据流通规则和访问权限管理办法，导致各主体间的数据流转不通畅，阻碍了数据价值的充分释放。

在示范区运营过程中持续产生与传输海量数据。示范区作为支撑汽车产业朝智能化、网联化方向转型发展的重要基础环境，伴随着智能网联汽车测试和示范运营活动的开展，快速积累了大量数据。其中既包括车辆本身的运行数据，还包括道路环境和交通场景数据，以及用户个人信息数据。并且随着自动驾驶等级的提升和智能化道路覆盖区域的扩大，自动驾驶产生的数据量不断增大，数据类型更加丰富，场景种类持续拓展。

图 3 示范区数据特点

以北京市高级别自动驾驶示范区为例，目前有300多辆各类高级别自动驾驶车辆在60平方公里的区域范围内开展常态化测试和商业服务，累计测试里程已超过700万公里。同时示范区还对超过300个路口进行了智能化改造，可以在车路协同运行过程中通过车端和路侧设备（摄像头、毫米波雷达、激光雷达等）采集大量人员、车辆、道路环境、路侧设施信号状态等真实交通数据，覆盖示范区范围内的多种交通场景，包含交通参与者隐私敏感数据、个人信息数据、地理环境数据等内容，每日采集运营数据超过10TB。此外示范区建设过程中已完成60平方公里地图数据的采集制作，可为示范区云控平台及多家测试企业提供高精度地图服务，通过真实数据还原多时空尺度的区域交通全景。

综上所述，示范区在建设运营过程中汇聚了大量的自动驾驶数据，其数据安全保障工作关乎国家安全、社会安定和公众利益。由于数据量大、类型复杂多样，且涉及多方数据交互等问题，在开展数据安全治理的过程中可能出现对特定数据资产类型或数据流转环节的遗漏。此外考虑到示范区数据价值特性和重要程度不同，在综合考虑治理成本和应用需求的前提下，难以通过单一的治理手段兼顾所有数据的安全保障与价值挖掘。

（三）分类分级是数据安全治理的基础

针对示范区数据特征以及在数据安全治理方面面临的挑战，有必要建立一套符合示范区运营实际的数据分类分级方法，为全面、高效的保障示范区数据安全建立基础。

在数据分类方面，通过梳理示范区数据类型全面盘点数据资产；通过梳理数据应用主体和流转环节明确不同类别的示范区数据产权归属和使用管理权责；通过整理重要和敏感数据为有针对性地实施数据安全治理手段提供依据。

在数据分级方面，通过分析不同类型数据的重要程度，对示范区数据实行分级管理，明确不同等级示范区数据的流通范围、访问权限和使用规则，最大限度平衡数据应用与安全保障需求。

在数据分类分级的基础上，按照数据的种类、安全等级匹配不同的治理措施，制定切实可行的数据安全治理方案，在可控的成本范围内探索示范区数据安全治理主体责任边界、安全保障目标、安全管控范围和方法，并为之配套合理的应急响应预案。从而实现安全治理手段对数据资产的全面覆盖，避免对特定数据对象的重复管理，以及不同数据管理主体之间的责权重叠。同时灵活把控管控强度，在保障数据安全治理方案的可操作性和实施效率的同时，最大限度在应用层面发掘数据价值。

（四）数据分类分级逐步走向标准化

现阶段国家相关主管机构、标准化组织和行业协会围绕数据分类分级出台了一系列政策法规和标准规范。

2020年3月，国家市场监督总局与国家标准化管理委员会发布了国家推荐标准**《GB/T 35273—2020信息安全技术 个人信息安全规范》**，对个人信息控制者在信息处理环节中的相关行为进行了规范，旨在遏制个人信息非法收集、滥用、泄漏等问题，保障个人的合法权益和社会公共利益。该标准将个人信息数据初步划分为个人信息和个人敏感信息两类，并提供了个人信息示例和个人敏感信息的判定标准，从而围绕个人信息这一特定的数据类型提供了分级管理的思路。

2020年8月，工信部发布了**《车联网信息服务 用户个人信息保护要求》**行业标准，明确了车联网信息服务中所涉及的用户个人信息的定义，规定了用户个人信息保护的基本原则，并将用户个人信息划分为用户身份证明类信息、车联网信息服务用户数据和服务内容信息、用户服务相关信息三大类。同时依据信息敏感程度，以及信息滥用或泄露的危害严

重性将用户个人信息的敏感程度划分为个人敏感信息、个人重要信息和个人一般信息三个级别，并分别为不同级别的用户个人信息安全保护提出了具体要求。

同月，工信部发布了**《车联网信息服务 数据安全技术要求》**行业标准，将车联网信息服务数据分为基础属性类数据、车辆工况类数据、环境感知类数据、车控类数据、应用服务类数据、用户个人信息六类数据类型，并依据各数据类型的安全目标、重要性以及安全事件的影响程度，将车联网信息服务数据划分为一般数据、重要数据和敏感数据三个敏感度等级。并根据数据敏感度分级结果，围绕数据生命周期重要环节制定了两级车联网信息服务数据安全保护要求，从而为车联网应用场景下的数据分类分级工作做出了指导。

2021年1月，汽车工程学会发布了**《智能网联汽车数据安全共享模型与规范》**团体标准征求意见稿，该文件提出了针对智能网联汽车的数据安全共享模型与规范。其中在数据分类方面将数据分为车厂数据和第三方数据两大类，并分别依据数据的动/静特性以及第三方数据来源分别做了细分。文件还根据不同类别数据遭篡改、破坏、泄露或非法利用后，可能造成的潜在影响对数据进行分级，最终结合智能网联汽车数据场景，提出了数据安全等级五级分类方法。

2021年7月，中关村车载信息服务产业应用联盟发布**《智能网联汽车数据共享安全要求》**团体标准，该标准整体沿用了《智能网联汽车数据安全共享模型与规范》中的分类分级方法，主要关注车厂数据和第三方平台数据，同时在第三方平台数据大类中加入了路侧监控、车主信息、限行信息等数据子类。同样的，该标准也提出了数据安全等级划分方式，并将不同数据类型与数据安全等级进行了明确对应。

2021年12月，全国信息安全标准化技术委员会发布了**《网络安全标准实践指南-网络数据分类分级指引》**，该文件将任何以电子方式对信息的记录定义为网络数据，并提出了网络数据分类分级的原则、框架、方法，以及实施流程，为开展数据分类分级工作的数据处理者提供了标准化实践指引，也为主管部门进行数据分类分级管理提供了参考。

北京市高级别
自动驾驶示范区

研究内容

本白皮书结合示范区的现实需求，基于对现行数据分类分级标准规范的研究，对数据分类分级工作的实施目标进行了界定，明确了示范区数据分类分级方法在相关标准体系中的定位，确定了本方法秉持的实施原则和重点工作内容。在现有方法的基础上，从示范区的运营实际和数据安全治理需求出发，结合行业内普遍认可的“车、路、云、网、图、第三方”的发展视角，为车路协同技术路线下产生的数据资产制定全方位、可执行、易操作的分类分级方法。

（一）示范区数据分类分级目标

数据分类分级工作需全面盘点示范区数据。按照包含关系梳理出多层级数据类型，并依据数据在经济社会发展中的重要程度，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，对数据实行分级，使数据持有方对数据资产规模及类型有清晰认识，便于形成数据安全保障统筹规划。

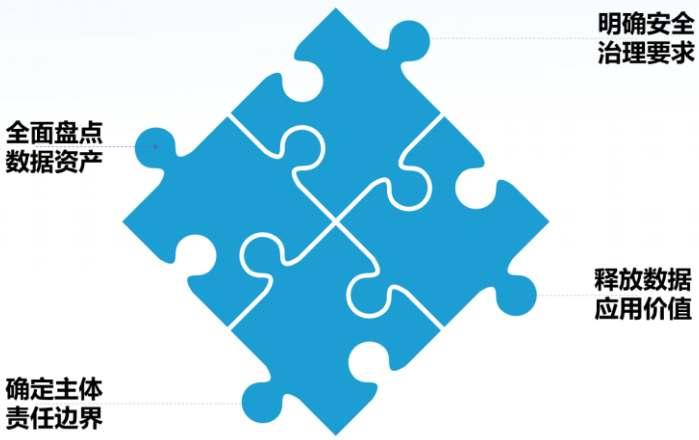

图 4 数据分类分级工作目标

数据分类分级工作需覆盖数据全生命周期。在数据全生命周期中（包括数据采集、传输、存储、使用、分享、销毁等）均需要依据数据分类分级结果制定不同等级的安全管理要求，并实施相应的安全治理策略，保障示范区数据的安全合理应用，同时对关系国家安全、国民经济命脉、重要民生、重大公共利益的重要数据和涉及个人敏感信息的数据等实行更加严格的管理制度。

数据分类分级工作需明确数据安全治理责任边界。示范区数据通常包括来自车辆、路侧设施、云控平台和第三方运营服务机构的数据信息，也包括网络运行数据和地图数据。在数据流转过程中，参与数据采集、存储、传输、使用等活动的相关方都对数据安全保障负有责任。数据分类分级工作可以为确定相关主体的数据使用权限和安全治理义务提供依据。

数据分类分级工作需提升数据业务运行效率。数据分类分级的工作目标不仅在于提升数据安全治理水平，满足数据安全合规要求，也需充分考虑数据业务运行效率。通过明确数据安全治理红线，划分数据流转范围并设置各主体数据使用权限，支持相关机构对于示范区数据的有效访问和安全使用，最大化发挥数据资产价值，提升数据业务运营效率。

（二）示范区数据分类分级原则

示范区数据呈现出应用场景复杂、类型多元、参与者众多的特点，需要在数据流转的各个环节精确发挥安全治理作用。其中在数据采集过程中需要严格遵循“知情同意”、“最小必要”、“目的限定”的个人信息保护原则，同时对于地理环境信息需要依据《中华人民共和国测绘法》及《中华人民共和国保密法》中的相关规定进行重点管理，避免数据过度采集和滥用。在数据传输和存储过程中，需要加强对通信网络和存储环境的安全监控，防止数据篡改和非授权访问。在数据使用过程中，需要明确数据使用方权限，有效控制数据流转范围和使用方式，加强个人信息和重要数据出境管理。

为实现数据安全保障目标，明确相关机构责任划分，同时便于数据安全保障办法的宣贯和实施，依据以下原则进行数据分类分级：

合法合规：数据分类分级方法应遵循有关法律法规要求，对国家和地方主管单位有明确管理要求的数据进行重点识别和管理，并配套相应的数据安全管理办法，满足合法合规要求。

统一维度：数据分类分级方法应明确思路，统一分类视角和颗粒度，确保各部门实施工作的连贯性，并使数据分类分级结果能够直接支持各部门明确数据安全管理责任边界。

科学合理：数据分类分级方法应充分考虑示范区数据特征，合理设定数据类别，确保数据类型覆盖全面，各类别和级别界限明确且具备显著特征，各级类别数据之间客观存在逻辑关联。

客观明确：数据分类分级方法应是客观且可校验的，通过数据自身的属性和定级规则即可判定响应级别，数据定级应明确对应数据本身，确保数据的定级结果是可复核和检查的。

简单实用：数据分类分级方法应尽可能精简且易于理解，避免设置真实运行场景和业务实践中不存在的数据项。数据类型描述简练清晰，符合各部门思维习惯和责任分工模式。

动态调整：数据分类分级方法应进行定期审核和调整，确保充分考虑自动驾驶技术的发展和示范区的运行实际，适应示范区在技术手段、政策标准、业务场景等方面的变化。

优先保障：数据分类分级方法应优先保障较高级别数据安全，对于包含多个级别数据项的数据集，且在数据安全治理过程中不便进行拆解的，应整体按照数据项的最高级别对数据集进行安全治理。

（三）示范区数据分类分级方法

示范区数据分类分级工作的重点内容包括确定数据分类视角与维度，与业务部门联动盘点数据资产，制定数据分级指标，梳理重要数据和个人敏感信息清单，以及制定数据安全治理要求等。其中数据分类维度以及数据分级指标是分类分级方法的核心。

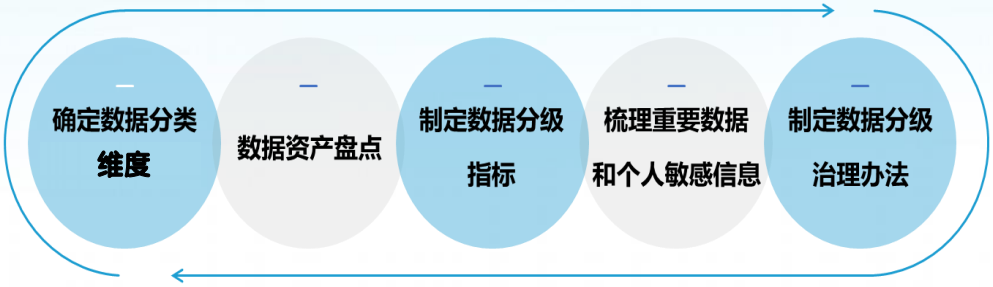

图 5 数据分类分级重点工作

从数据来源的视角对示范区数据进行分类。考虑到示范区数据的复杂性，可能存在多种数据分类维度和颗粒度（如《网络安全标准实践指南—网络数据分类分级指引》中就提到“个人公民维度”“信息传播维度”“行业领域维度”等方式）。为了全面梳理示范区数据类型，采用平行分类法（即面分类法），对拟分类的数据进行集合，从数据来源的视角，分成相互之间没有隶属关系的门类，每个门类包含具备相同来源特征的一组数据类目。同时为了统一颗粒度，参考《GB/T 4754—2017 国民经济行业分类》中采用的等级分类法（即线分类法），把各门类数据逐次再分为大类、中类、小类三个层级，每个层级又分为若干条目，同级类目之间构成并列关系，不同层级类目之间构成隶属关系，尽量保障同层级数据类目互不重复，互不交叉。数据小类作为分级的最细化类目，需要能够清晰描述相关数据的内容、作用或应用场景。

使用定性指标判定示范区数据的重要性等级。在数据分级指标方面，为便于在业务部门中宣贯和实施，在完成数据盘点工作后，需要根据各类型数据属性特征，综合考虑数据安全事件影响对象和影响程度两方面因素制定数据分级指标，并将各示范区数据小类与特定数据等级明确对应。在完成数据分级工作后，从中梳理出重要数据和个人敏感信息数据，形成清单，便于后续实施重点合规治理。针对不同数据等级，以及重要数据、个人敏感信息数据将分别制定相对应的数据安全治理要求，为后续实施不同强度的安全治理手段提供依据。

工作实践

本白皮书从示范区业务实际出发，围绕示范区运营平台企业的典型架构和工作模式，梳理了数据分类分级工作的实施流程，结合示范区数据特征确定了分类维度和分级指标，并本着安全应用的原则对不同类型和级别的数据提出了安全管理要求。

（一）示范区数据分类分级总体流程

综合示范区数据分类分级工作目标以及示范区的运营模式，制定数据分类分级整体流程如图6所示。

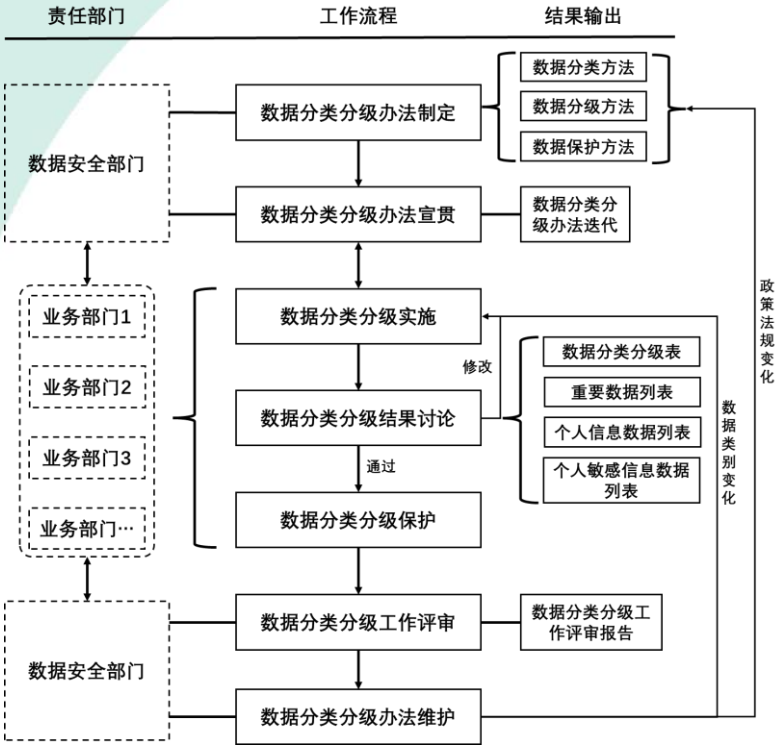

图 6 数据分类分级工作目标

数据分类分级方法评审。数据安全管理者在开展数据分类分级工作之前需要充分调研数据安全相关政策法规，学习各行业现行的数据分类分级方法，保障自身制定的数据分类分级方法与相关标准法规和行业规范的整体要求一致，并通过内部评审确认示范区数据分类分级方法满足行业需求。

数据分类分级办法宣贯。在数据分类分级办法制定完成并通过数据安全主管机构（如本单位数据安全管理委员会）评审后，需要面向该办法约束范围所涉及的业务部门进行宣贯，向各部门数据安全员详细解读数据分类分级思路及操作方法，听取业务部门意见，解答业务部门疑问，并对办法中普遍存在异议的内容进行适当调整。

数据分类分级办法实施。完成数据分类分级办法的宣贯工作后，各业务部门数据安全员将负责协调开展本部门的数据资产盘点工作，依据办法要求对部门管理范围内的数据进行分类分级，并依据办法中的定义，识别出重要数据、个人信息和个人敏感信息数据。

各业务部门完成数据分类分级工作后，将数据分类分级结果以表格形式反馈给数据安全主管机构，经讨论确认后，由数据安全机构汇总形成本单位数据分类分级表、重要数据列表、个人信息数据列表和个人敏感信息数据列表，并存档。

数据分类分级工作审计。各业务部门后续需要依据数据分类分级结果和数据安全管理办法，对本部门各级数据实施相应等级的安全治理，保障数据的安全合理应用。数据安全主管机构定期对各业务部门的数据安全管理结果进行审计，出具审计报告，并组织业务部门针对审计过程中发现的问题进行整改。

数据分类分级方法维护。数据安全主管机构将实时关注示范区运营状况，以确保当政策环境或示范区的运营范围、业务场景、道路参与者类型等发生变化，并导致现行数据分类分级办法不能有效覆盖新增数据种类，或数据等级发生变化时，及时对办法进行调整，并将调整结果同步给相关业务部门。

（二）示范区数据分类

1、数据资产盘点

示范区运营企业各业务部门在开展数据分类工作之前，需要对各自管理范围内的数据资产进行盘点，梳理数据基本信息、数据应用场景和数据存储状态，如图7所示，并形成数据资产识别清单。主要目的是为数据分类分级提供数据资产全景，防止遗漏，同时使数据安全主管机构成员对于本单位的数据资产有总体了解，便于确定数据分类分级方法。

图 7 数据资产盘点工作内容

在进行数据盘点的过程中，还需要根据数据的实际应用场景，明确数据资产在单位内部各部门，以及单位外部企业单位（包括交管部门、自动驾驶技术企业、保险公司、第三方服务平台等）之间的流转过程，如图8所示。以便于控制数据流转范围，并针对各个数据使用节点制定安全管控原则，保障数据资产的合理应用，同时明确各部门对特定数据资产安全治理的权责边界，支撑数据安全治理工作的顺利开展。

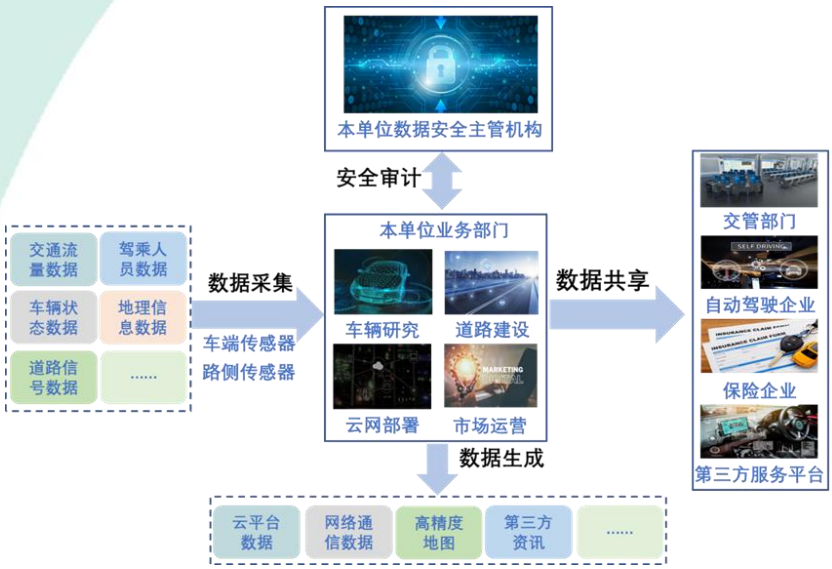

图 8 自动驾驶示范区数据流转

2、数据分类实践

本文中的数据分类方法结合示范区的建设和运营实际，从“车、路、云、网、图、第三方”六个门类对示范区数据进行梳理，从车路协同系统的业务逻辑出发，以数据出口作为数据分类边界，将整体的数据分类架构分为门类、大类、中类、小类四个层级，同时对各数据小类包含的信息内容做出示例。

其中车端数据包括车辆基本信息、感知数据、决策数据、运行数据、个人信息五个大类；路侧数据包括路侧设施基本信息、感知数据、融合计算数据、应用服务数据、运行状态数据五个大类；云端数据包括云平台基本信息、控制数据两个大类；网络数据包括网络基本信息和网络监测数据两大类数据；地图数据包括高精度地图数据和交通大数据两大类；第三方数据包括生活服务数据和车辆服务数据两大类（示范区数据分类实践结果见附件）。

本数据分类方法充分考虑了北京市高级别自动驾驶示范区的建设实际，并尽量响应各示范区数据分类的共性需求，但是由于在技术路线选择和实际运营过程的差异性，本文中对于数据大类的划分方式无法完全适应所有示范区的工作实际。如本方法将云端数据分为区域云和边缘云两大类，但部分示范区可能因为自身规模较大，选择部署多个区域云，并建设中心云对区域云进行智能控制。各示范区可依据自身实际对本白皮书中的数据分类方法进行灵活扩展和剪裁。

（三）示范区数据分级

1、数据安全影响

数据分级管理是建立数据生命周期安全保护框架的基础性工作，为实施有针对性的数据安全管控措施提供支撑。本办法将不同类型的示范区数据在遭泄露、破坏或非法利用后带来的负面影响作为判断依据，**从影响对象和影响程度两个方面考虑，确定示范区数据的重要性等级。**

图 9 数据等级的判断因素

在影响对象层面，示范区数据安全风险可能影响到国家安全、公众利益、个人权益和企业合法权益。

（1）可能对**国家安全**产生影响的示范区数据主要包括高精度地理信息、军事设施位置信息、宏观经济数据，以及核安全、生物安全、生态安全、能源安全、通信安全等相关的关键基础设施信息、重要机构及骨干企业信息、重要自然资源信息等。此类数据在出现安全问题后可能使国家重大利益遭受损害或威胁。

（2）可能对公众利益产生影响的示范区数据主要包括自动驾驶控制信息、道路信号

控制信息、重要物流信息等。此类数据在出现安全问题后可能会在一个或多个省市的大部分地区引起社会安全事件，或干扰社会经济建设。

（3）可能对**个人权益**产生影响的示范区数据包括行动轨迹、身份信息、账户信息等个人敏感信息。此类数据在出现安全问题后可能导致个人的人格尊严受到侵害，或者人身、财产安全受到危害，使自然人的健康受到损害，财产蒙受损失，或对其生活、工作和其他经济社会活动造成不利影响。

（4）可能对**企业合法权益**产生影响的示范区数据包括企业重要专利信息、核心技术方案、重要产品参数、市场规划方案等。此类数据在出现安全问题后可能导致相关企业的业务无法正常开展，或蒙受经济、技术及声誉损失，给企业生存造成困难，或对企业发展和参与市场竞争造成不利影响。

在影响程度层面，根据数据安全事件造成后果的严重程度，分为以下四个级别。

（1）**无损害**是指对国家安全、公众利益、个人权益和企业合法权益均不存在负面影响。

（2）**一般损害**是指不影响国家安全，但对公众利益、个人权益和企业合法权益存在一定的负面影响，造成一般性损害。

在公众利益方面，一般损害是指在较小的区域范围内对社会秩序造成一定影响，给部分公众造成经济损失或影响到区域内人员工作生活的正常开展，在短时间内引起了公众担忧。但整体损失较小，社会正常秩序在短时间内可恢复，影响范围不会向区域外扩散。

在个人权益方面，一般损害是指侵害数据主体对于个人数据使用的知情权，并在较小的程度上使数据主体的人身安全受到威胁，个人经济利益受到损失，个人声誉受到损害，从而使数据主体的正常生活和社会活动受到干扰。

在企业合法权益方面，一般损害是指在较小的程度上给特定企业造成经济、声誉或竞争力损失，或使企业面临业务和产权纠纷，或受到监管部门警告，干扰到企业的正常经营活动，或对企业的发展前景造成不利影响。

（3）**严重损害**是指不影响国家安全，但对公众利益、个人权益和企业合法权益存在较大负面影响，造成较大损害。

在公众利益方面，严重损害是指在较大的区域范围内对社会秩序造成严重影响，给大量公众人员造成经济损失或严重干扰区域内的正常工作生活，引起了公众的普遍恐慌。整体损失较大，社会正常秩序在短时间内难以恢复，影响范围开始向区域外扩散，或有向区域外扩散的风险。

在个人权益方面，严重损害是指违背数据主体对于个人数据的使用意愿，并在较大的程度上使数据主体的人身安全遭受损害，个人经济利益遭受损失，个人声誉受到损害，从而使数据主体的正常生活和社会活动受到严重干扰，并可能在短期内难以消除对数据主体造成的负面影响。

在企业合法权益方面，严重损害是指在较大的程度上给企业造成经济、声誉或竞争力损失，或使企业面临严重的业务和产权纠纷，或受到监管部门处罚，长时间干扰到企业的正常经营活动，使企业的生存和发展遭受严重威胁，且在短期内难以找到有效措施消除不利影响。

（4）**特别严重损害**是指对国家安全造成威胁或产生不利影响，或对公众利益、个人权益和企业合法权益造成极大负面影响和损害。

在国家安全层面，特别严重损害是指对国土安全、军事安全、科技安全、生态安全、资源安全、核安全、文化安全等造成危害或威胁。可能导致我国的安定环境遭到破坏，国际地位受到影响，人民福祉遭到损害，国土面积、自然环境及资源遭到破坏，时代主题和文化环境遭到恶意渗透等。

在公众利益方面，特别严重损害是指在全国范围内对社会秩序造成严重影响，给大量公众人员造成巨大经济损失或严重破坏社会秩序，使公众正常的社会活动无法正常开展，严重打击公众情绪，引起公众的强烈恐慌和担忧，恶劣影响在短期内无法消除，影响范围波及全国，且在短期内难以有效限制影响范围。

在个人权益方面，特别严重损害是指严重违背或强迫改变数据主体对于个人数据的使用意愿，使数据主体的人身安全遭受直接威胁或严重损害，个人经济利益遭受巨大损失，个人声誉受到严重损害，从而使数据主体的正常生活和社会活动无法正常开展，并长期对数据主体造成负面影响。

在企业合法权益方面，特别严重损害是指给企业造成巨大的经济、声誉或竞争力损失，导致企业损失部分业务或产权，或遭受监管部门严厉处罚，企业长时间无法正常开展经营活动，企业生存和发展面临严重危机，难以通过有效手段消除影响或恢复企业的市场地位。

2、数据分级实践

根据上述内容，通过判断数据一旦遭到破坏、泄露、损毁等，对国家安全、公众利益、个人权益和企业合法权益的危害程度与影响，将数据等级分为如下5级：

DL1级：数据被泄露、破坏或非法利用后，对国家安全、公众利益、个人权益和企业合法权益均无危害。

DL2级：数据被泄露、破坏或非法利用后，对个人权益和企业合法权益造成一般损害，不影响国家安全和公众利益

DL3级：数据被泄露、破坏或非法利用后，对个人权益和企业合法权益造成严重损害，可能对公众利益造成一般损害，不影响国家安全。

DL4级：数据被泄露、破坏或非法利用后，对个人权益和企业合法权益造成特别严重损害，可能对公众利益造成严重损害，不影响国家安全。

DL5级：数据被泄露、破坏或非法利用后，对公众利益造成特别严重损害，可能对国家安全造成损害。

数据分级方法如表1所示。

表 1 数据等级

影响程度 影响对象	特别严重损害	严重损害	一般损害	无损害
国家安全	DL5	——	——	——
公众利益	DL5	DL4	DL3	DL1
个人和企业利益	DL4	DL3	DL2	DL1

本文将依据上述分类分级方法，从示范区数据中筛选出重要数据清单，并予以重点治理。此外本文还将指导形成自动驾驶个人数据和个人敏感数据列表。并对数据主体主观上不愿为他人知晓（指数据主体有数据不为他人所知的主观意愿，或对数据受保护已经形成了预期，并且这种主观心态或期待是合理的，符合社会一般观念，能得到社会普遍接受或认可）或客观上具有私密性（是指数据处于隐秘状态的客观事实，此种隐秘状态与他人利益和社会公共利益无关，不会给他人或社会公共利益带来不可容忍的减损）的数据进行重点治理，保障个人数据的私密性。

（四）示范区数据安全管理

本文将依据示范区数据分类分级结果，针对数据全生命周期的各重要环节制定安全分级管理方法。同时落实数据安全管理主体责任，定期对数据分类分级和安全管理方法进行复查。

1、数据安全管理总体要求

数据安全管理总体要求包括常规管理要求、安全审计与报告、风险评估与监控以及安全事件管理等内容。

数据安全常规管理要求。包括成立专门的数据安全主管部门，制定数据分类分级管理制度和数据安全防护要求，并向业务部门进行宣贯。业务部门在数据全生命周期内，按数据分类分级结果及数据安全等级保障要求，实施适当的安全管理与技术控制，提供与数据安全保障级别相匹配的保护手段。处理重要数据时，应由数据安全主管部门按照行业监管部门或示范区主管部门的要求开展风险评估，并提交风险评估报告。当业务部门委托第三方处理数据时，应与第三方签订数据安全保障承诺函并报数据安全主管部门审批备案。

数据安全审计与报告。数据安全主管部门应根据数据资产变化情况，制定并定期更新数据安全审计计划，并根据计划实施审计。对于重要数据资产。数据安全主管部门应根据需要制定专项审计计划（如重要数据处理审查、合作第三方数据处理审查等），并根据计划实施审计，向主管领导报告审计结果。数据安全主管部门应定期组织各业务部门对自己所管理的业务数据进行盘点，并将盘点结果提交数据安全主管部门汇总，由数据安全主管部门管理与维护数据资产台账与重要数据清单。

风险评估与监控及安全事件管理。数据安全主管部门应周期性组织各业务部门进行数据合规风险评估，识别数据处理活动中出现的缺陷、漏洞等风险，要求相关业务部门采取缓解或补救措施，跟踪措施落地并执行有效性评价。除此之外还应在数据安全相关的国家与行业法规、政策和标准、单位的业务范围、相关业务平台（如云控平台）的运营情况，以及处理数据的目的和手段发生变更，或业务运营数据流发生变化时实施专项合规审查。当数据安全事件发生时，涉及的业务部门数据安全员应立即上报数据安全主管部门负责人，并按既定数据安全应急管理制度要求进行处置。

2、数据安全等级保障要求

数据安全等级保障是以最大限度消除数据安全问题可能产生的危害为目的，依据数据等级（DL），制定不同强度的数据安全保障等级（DSAL），并对不同等级和类型的数据分别使用DSAL所对应的保障手段，维护示范区数据安全，并使数据资产价值在合规的基础上得到最大释放。

总体而言，各业务部门在确定DL后，需按表2所示DSAL，对应采取适宜的数据安全保护措施。

表2 数据安全保障等级

数据等级	DL5	DL4	DL3	DL2	DL1
安全保障等级	DSAL3	DSAL3	DSAL2	DSAL 1	QM

DSAL1安全要求

在**数据采集**方面，应遵循最小化采集原则，仅采集业务必须的最少数据。对数据源进行身份鉴别，防止数据源假冒或伪造。对采集的数据进行唯一标识，方便对数据进行查询、修改、跟踪、删除等管理操作。涉及个人信息的采集，应具有合理、必要、明确的采集目的，只采集为满足使用目的所需的最少数据类型和数量，并征得个人信息主体同意。难以实现事先征求同意的应当对个人信息进行匿名化处理。

在**数据存储**方面，对个人信息和重要数据存储应采取最小保存期限原则，并根据所提供的功能服务分类设定数据保留期限。建议采用数据加密存储，并在数据传输过程中通过安全传输通道传输示范区数据。

在**数据使用**方面，应满足目的明确原则和最少够用原则，为各数据使用者分配执行其岗位职责所需的最小权限，并基于权限进行数据访问和使用。通过外部网络远程访问数据时应使用公司要求的加密通道。禁止数据使用者批量导出个人数据，避免访问到与个人直接关联的信息。对终端设备采取权限管控，当设备访问个人信息时，保障只有经过允许的进程可以对相关数据进行访问。

在**数据分享**方面，所有示范区数据应经数据安全主管部门审批同意后方可对外分享，涉及个人信息的数据需要经数据主体授权同意后方可对外分享。主管部门应对分享的数据进行标识和备案，并保障数据的传输满足数据安全传输要求，数据的接口调用建议采用认证技术。

在**数据销毁**方面，示范区数据在其使用目的完成后，或超过存储期限，经业务部门负责人同意，提交数据安全主管部门批准，并经数据安全主管部门备案后，可实施销毁。涉及个人信息时，若数据主体要求删除，则应实施销毁。如有必要，还应对数据存储介质进行低级格式化或填充，使数据无法恢复，实现数据的安全销毁。

在**数据出境**方面，示范区数据原则上不出境。若因特殊情况需要出境，应由数据安全管理部门审核并批准后，申请启动数据出境流程，由数据安全管理部门组织进行出境数据的风险评估。出境数据通过内部风险评估后，再由数据安全主管部门向地方网信部门相关机构提交数据出境申请，获得网信部门的出境许可后方可传输出境。为便于内外部监管部门对数据出境情况进行抽查，应使用专用平台或系统传输数据，并提供出境数据监控功能，可方便读取出境数据清单，并以清晰明了的方式展示。

DSAL2安全要求

在**数据采集、数据销毁**和**数据出境**方面与DSAL1安全要求相同。在**数据存储**方面，除满足DSAL1安全要求外，还需在云端和终端设备上对数据进行加密，如数据存储方案不支持针对特定字段的加密，则需对整表进行加密，并提供数据安全备份与恢复机制。建议对数据进行签名和验签。

在**数据传输**方面，除满足DSAL1安全要求外，还应在云端和终端设备(路侧设备/车载设备等)进行数据交互之前加密。加密后通过安全传输协议传输，且在数据传输前实施双向身份认证。

在**数据使用**方面，除满足DSAL1安全要求外，还需对数据使用者进行身份认证和访问权限控制。严格限制数据使用者的人数，实现日志记录功能，记录数据使用者对数据的操作行为。对涉及个人信息的数据做匿名化处理。若提供基于个人画像的个性化推荐服务，应具备让数据主体自行控制是否开启该服务的功能。

在**数据分享**方面，除满足DSAL1安全要求外，还需采取有效措施监督接收者按照双方约定的目的、范围、方式使用数据。涉及个人信息时需要经数据主体授权同意后方可对外分享，且需要对数据进行脱敏处理。建议使用隐私计算技术实现数据 “可用不可见”。

DSAL3安全要求

在**数据采集、数据销毁**和**数据出境**方面与DSAL1、DSAL2安全要求相同。在**数据存储**方面，除满足DSAL1、DSAL2安全要求外，还需采用漏洞扫描系统对数据存储系统进行定期扫描，以保证符合安全基线要求。采用逻辑存储隔离，实时监控不同隔离区域之间的数据传递。对存储介质采用专人看守，任何存储媒介入库或出库需经过授权，并保留相应记录。在终端设备上配备硬件实现的安全区域或安全模块，实现数据安全存储与隔离。采用漏洞扫描工具对路侧和车载设备进行定期测试，检查是否存在安全漏洞。终端设备不应存在未经声明的外围介质接口。对终端设备数据进行定期备份，备份介质采用的数据安全治理手段不应低于原有强度。

在**数据传输**方面，除满足DSAL1、DSAL2安全要求外，还需在涉及个人信息数据传输时，对数据进行脱敏处理后再进行传输。

在**数据使用**方面，除满足DSAL1、DSAL2安全要求外，还需要求内部人员在使用数据时由本部门负责人审批确认，由数据安全主管部门对数据使用者的权限进行审批，并对数据使用进行登记和记录。外部人员应在接触数据之前接受背调和评估，并签署数据安全保障承诺书，严格控制在必须的工作范围内使用数据。定期开展数据安全审计和异常行为分析，发现可能造成安全风险的数据使用行为应及时告警。在人员调岗或离职时，及时收回其使用、保管的本公司数据资产。终端设备面向普通用户只提供数据服务，不提供原始数据，确需提供原始数据的，应严格限定数据查询频率，并记录日志。在终端设备采用可信执行环境，对关键应用提供安全执行空间，控制对数据的访问，保护数据的保密性和完整性。

在**数据共享**方面，DSAL3数据原则上不允许分享，如确需分享，除满足DSAL1、DSAL2安全要求外，还需须上报数据安全主管部门评审确认，若数据安全主管部门评审通过，方可在境内脱敏分享。

发展建议

智能网联汽车测试示范区数据安全合规工作仍存诸多挑战，需坚持顶层设计引领，自上而下构建科学高效的管理制度，真正平衡数据安全与创新发展。聚焦组织、流程、技术、人员等方面，以数据分类分级为基础，提升数据合规治理能力。

（一）强化顶层设计，落实数据安全管理体系

以网安法、数安法、个保法为指引，加强网信办、发改委、工信部等有关部门协同，形成工作合力。进一步推动数据监管体系建设，指导相关企业细化数据安全管理制度，统筹安全和发展，切实促进智能网联汽车行业健康有序发展。

发挥智能网联汽车测试示范区牵引带动作用，在示范区内部重点宣贯数据分类分级及安全治理规范，自上而下落实责任义务，将数据安全规划纳入企业顶层管理规范，推动跨部门落地实施数据分类分级及安全管理方案。鼓励建设数据安全监测平台，建立统一的数据安全工作协调统筹机制，提供示范区数据分类分级和安全治理工作专项支持，推进第三方评估机构和人员资质认证等配套管理制度建设。

（二）完善标准体系，提升数据分类分级工作效力

以《车联网网络安全和数据安全标准体系建设指南》为基础，组织行业共同完善数据安全标准体系建设及关键标准研制，以示范区探索实践为标准制订及验证提供实证参考，面向全行业提供示范区数据分类分级标准化方案。

依据示范区运营实际对数据分类分级方法进行定期复核，使之适应示范区数据规模、涵盖信息、应用场景、处理手段等方面的变化，持续保障数据分类分级结果的合理性。同时构建自动化数据发现和分级分类的解决方案，借助数据标签、知识图谱等智能化工具实现数据资产的自动化盘点和监控，提升数据分类分级与安全治理工作效率。

（三）平衡安全与发展，释放数据资产价值

充分响应“数据安全与发展”目标，探索有效措施最大限度消除数据安全治理工作与数据开发利用效率之间的矛盾，构建自动化数据发现和分级分类的解决方案，并在数据应用的关键环节提供数据安全技术支撑，以快捷、轻量、制度化的安全治理方案支持数据安全治理工作，有效降低数据安全治理工作实施成本。

结合智能网联汽车测试示范区的数据资产特性，探索数据应用业务新模式，发掘数据开发利用内在驱动力，依托隐私计算、区块链等数据安全保障技术，促进数据资产在安全合规前提下的有序利用和流动，推动数字产业和数据产品创新，支撑数字经济发展。

（四）协调行业力量，引导数据分类分级跨区应用

充分发挥智能网联汽车测试示范区的平台示范作用，强化地方主管部门、标准化组织、行业协会和专业机构统筹协调，分阶段有序建立产业协同机制，共同发掘智能网联汽车数据资产价值，支撑数据应用技术创新和产业发展。

以智能网联汽车测试示范区数据分类分级方法为核心内容，积极深化数据安全工作的跨部门跨企业渗透，总结和分享优秀成果与经验，为智能网联汽车测试示范区数据分类分级及安全治理工作的全行业推广应用提供有力支撑。

（五）加强地方政府引导，保障示范区数据安全

加强政府部门协同、明确安全管理职责，建立统一的示范区数据安全工作协调统筹机制，完善政府部门系统性访问示范区运营企业数据的法律依据，确保政府部门自觉遵守数据安全管理规则，将系统性访问示范区数据的过程中可能产生的数据安全风险降到最低。

建议政府主管部门向示范区提供数据分类分级和安全治理工作专项支持，鼓励相关技术研发和人才培养，实现对示范区范围内的海量、多元和非结构化数据的统筹管理，逐步使安全关口前移，及早发现安全风险，并进行快速反应和优先处置。

附件 数据分类分级列表

大类	中类	子类	示例	建议等级
车	基本数据	车辆标识数据	车牌号、车辆识别号VIN、注册号、车辆厂商、商标、品牌、车辆产品型号等	DL1/DL2
		车辆属性数据	车辆类型数据（车型、用途、动力类型等）	DL1
			车辆配置数据（外观、长宽高、轴距、百公里续航等参数配置信息）	DL1
			自动驾驶系统配置	DL1
		零部件数据	零部件标识数据（发动机号、电机号、动力电池编号、Tbox编号等部件编号）	DL2
			零部件属性数据（动力电池容量、发动机扭矩、排量、电动机扭矩等零部件参数）	DL2
		车辆保险数据	车辆保险信息（机动车商业保险、强制险等保险信息）	DL2
		鉴别数据	CA证书数据	DL3
			密钥	DL3
	感知数据	激光雷达数据	点云数据信息	DL3
		毫米波雷达数据	点云数据或目标物信息	DL3
		超声波雷达数据	障碍物信息	DL3
		摄像头数据	视频、图片信息	DL4
		IMU数据	角速度和加速度信息	DL3
		时空定位信息	GNSS速度、时间戳、载波、伪距等	DL3
			经纬度信息	DL4
		融合后的自车位置数据	绝对位置信息	DL4
			相对位置信息	DL3
		目标物识别数据	目标物属性	DL3
		V2X数据	车辆基本安全消息（BSM）	DL3
	决策数据	人类驾驶员操作数据	人类驾驶档位信息	DL3
			人类驾驶加速踏板开度	DL3
			人类驾驶刹车踏板开度	DL3
			人类驾驶方向盘转向角	DL3
		自动驾驶系统决策数据	自动驾驶请求档位信息	DL3
			自动驾驶请求横纵向加速度	DL3
			自动驾驶请求转向角	DL3
			自动驾驶请求转向力矩	DL3
			自动驾驶请求灯光、雨刮状态	DL3
		预测规划数据	感知目标物轨迹预测数据	DL4
			车辆路径规划数据	DL4
	运行数据	运行统计信息	行程统计信息	DL2
			功耗续航统计	DL2
		车辆状态数据	电动车电池SOC	DL2
			燃油车剩余油量	DL2
			自动驾驶与人工切换信息	DL2
		车辆运行数据	挡位信息	DL2
			车速	DL2

附件 数据分类分级列表

大类	中类	子类	示例	建议等级
			车辆航向角	DL2
			车辆侧倾角速度	DL2
			横摆角速度	DL2
			横纵向加速度	DL2
		零部件状态数据	车灯喇叭状态	DL2
			制动标志	DL2
			雨刮状态	DL2
			GNSS运行状态	DL2
			IMU运行状态	DL2
			TBox运行状态	DL2
			OBU运行状态	DL2
			其他设备运行状态	DL2
		零部件运行数据	驱动电机转速	DL2
			驱动电机扭矩	DL2
			发动机转速	DL2
			发动机扭矩	DL2
			制动主缸压力	DL2
			制动分泵压力	DL2
			油门踏板开度	DL2
			制动踏板开度	DL2
			方向盘转角	DL2
			方向盘转向扭矩	DL2
		车辆故障信息	ECU故障	DL2
			系统故障	DL2
	个人信息	驾驶员/安全员个人直接标识	姓名	DL2
			驾驶证信息	DL3
			身份证信息	DL3
		驾驶员/安全员生物特征	安全员人脸	DL4
			安全员声纹	DL4
		乘客个人资料	姓名	DL2
			手机号	DL3
			位置行程	DL4
		乘客生物特征	乘客人脸	DL4
			乘客声纹	DL4
		用户状态检测	驾驶员状态监测	DL2
			乘客状态监测	DL2
			驾驶行为习惯	DL2
			应用使用习惯	DL2
		人机交互操作记录	多媒体大屏操作记录	DL2
			方控/中控操作记录	DL2
路	基本信息	路侧编号信息	摄像头、雷达、RSU、MEC等设备编号	DL1/DL2
			道路编号信息	DL1/DL2

附件 数据分类分级列表

大类	中类	子类	示例	建议等级
		路侧设备属性数据	设备类型	DL1
			使用性质	DL1
			性能参数	DL1
			设备通信模式	DL1
		安装位置	安装位置行政区划	DL2
			安装位置经纬度	DL3
			安装高度、角度	DL3
		OTA数据	版本信息	DL2
			升级中心信息下发	DL3
			升级状态和日志	DL3
	感知数据	摄像头视频	视频图像数据	DL4
		毫米波雷达数据	毫米波雷达结构化数据	DL3
		激光雷达数据	激光雷达原始点云数据	DL3
		雷视一体机数据	感知结构化数据	DL3
		交通控制信号	信号灯数据	DL3
	融合计算数据	融合计算感知目标物数据	目标物结构化数据	DL3
		融合计算交通流数据	交通流量（自然数）	DL3
			交通流量（当量数）	DL3
			路口车辆平均通行时间	DL3
			绿灯启亮时刻排队车辆数（自然数）	DL3
			绿灯启亮时刻排队车辆数（当量数）	DL3
			绿灯启亮时刻排队长度	DL3
			排队长度	DL3
			红灯启亮时刻未通过车辆数（自然数）	DL3
			红灯启亮时刻未通过车辆数（当量数）	DL3
			绿灯启亮类排队车辆数（自然数）	DL3
			绿灯启亮类排队车辆数（当量数）	DL3
			停车次数（感知）	DL3
			车头时距	DL3
			浪费时间	DL3
			绿灯时间	DL3
			溢流次数	DL3
			溢流时间	DL3
			溢流系数	DL3
			定时长ROI范围车辆自然数	DL3
			定时长ROI范围车辆当量数	DL3
	应用服务数据	协同决策数据	信号灯消息（SPAT）	DL3
			地图消息（MAP）	DL4
			交通事件信息以及交通标志信息（RSI）	DL3
			路侧安全消息（RSM）	DL3
		信息服务	充电桩状态	DL3
			高速电子收费	DL4

附件 数据分类分级列表

大类	中类	子类	示例	建议等级
	运行状态数据	系统运行状态	远程访问下发	DL3
			远程访问上报	DL3
		部件运行状态	设备行为状态	DL3
		日志记录	设备故障历史	DL3
			设备异常日志	DL3
			设备状态日志	DL3
云	基本信息	云控平台建设基本信息	平台编号	DL2
			平台类别（中心云、区域云）	DL1
			行政区划代码	DL1
			路口路段列表	DL1
			设备列表	DL1
			车辆列表	DL1
		展示信息	实时视频数据	DL1
			历史视频数据	DL1
			道路状态统计数据	DL1
			路侧设备故障统计数据	DL1
			车辆驾驶统计数据	DL1
			车辆系统故障统计数据	DL1
	控制数据	协同控制数据	匝道汇入协同	DL4
			绿波车速引导	DL4
			网联式超级巡航	DL4
		信号配时方案	周期	DL4
			绿信比	DL4
			相位差	DL4
网	基本信息	网络类别	C-V2X 、EUHT	DL1
		网络性能指标	通信性能数据（丢包率、端到端时延、验签时延等）	DL2
			信道忙率CBR	DL2
			信道质量指示CQI	DL2
	网络监测数据	网络状态监测数据	网络状态监测数据	DL2
		流量监测数据	流量监测数据	DL2
		网络异常和安全事件监测	网络异常事件、网络安全事件监测信息	DL2
图	高精地图数据	静态高精地图数据	道路线	DL4
			道路边界	DL4
			道路拓扑	DL4
			路口	DL4
			车道中心线	DL4
			车道标线	DL4
			车道拓扑	DL4
			停止线	DL4
			人行横道	DL4
			箭头	DL4

附件 数据分类分级列表

大类	中类	子类	示例	建议等级
			导流带	DL4
			地面文字	DL4
			地面符号	DL4
			禁止停车区	DL4
			紧急停车区	DL4
			紧急避险区	DL4
			交通信号灯	DL4
			安全岛	DL4
			自行车道	DL4
			公交车站	DL4
			建筑物	DL4
			减速线	DL4
			路牙	DL4
			护栏	DL4
			路口内导向线	DL4
			警告区	DL4
			填充区	DL4
			停车场	DL4
			停车位	DL4
			龙门架	DL4
			收费站	DL4
			服务区	DL4
			杆/柱子	DL4
			其他道路设施	DL4
			重要属性（纵坡、横坡、航向、曲率、高程、物理限制）	DL5
		准静态高精地图数据	交通标牌	DL2
			可变标志牌	DL2
			限速信息	DL2
		准动态高精地图数据	施工信息	DL2
			天气信息	DL2
			事故事件信息（交通事故、交通管制）	DL2
			生活服务类信息	DL2
		动态高精地图数据	实时路况（交通状态等级）	DL2
			交通信号灯信息（灯色、剩余时长、信号控制方案等）	DL2
			交通参与者（车辆、行人、三轮车、电瓶车等）	DL2
			交通运行数据（如停车场的空闲车位数、充电桩的可用性）	DL2
	交通大数据	交通流量	交通流量	DL2
		平均行程速度	平均行程速度	DL2
		平均行程时间	平均行程时间	DL2

附件 数据分类分级列表

大类	中类	子类	示例	建议等级
		车均延误	车均延误	DL2
		停车次数	由多个路口组成的路段，平均停车次数	DL2
		交通拥堵指数	统计交通拥堵指数	DL2
第三方	生活服务	日常生活服务	美食、影视、酒店、外卖服务	DL1
		电商	电商服务	DL1
		IOT	手机、智能家居控制	DL2
	车辆服务	维保预约	维修保养服务（4S店地址、行政区划）	DL1
		预约加油	加油服务（加油站地址、联系方式、油价）	DL1
		违章查询	违章信息	DL2
		天气预报	天气服务（行政区划、当地天气）	DL1
		商业保险	保险服务	DL1

北京市高级别
自动驾驶示范区

联系方式：

北京市高级别自动驾驶示范区工作办公室
邮箱：bjhad@bda.gov.cn

北京车网科技发展有限公司
邮箱：cooperation@bcavt.com