智能网联汽车
数据分类分级白皮书

智马达汽车与安华金和联合发布

STATEMENT 声 明

本白皮书由 smart 与安华金和（以下简称“我们”）联合撰写，旨在提供关于智能网联汽车数据分类分级的综合分析和深入见解。本文档可能包含对其他标准、文献或研究成果的借鉴。请注意，本文档仅供信息参考，不构成任何形式的法律、财务、技术或专业建议。

版权声明：本白皮书的所有原始内容，包括但不限于文本、图表、图像和数据，均为 smart 所有。对于借鉴的内容，我们已尽可能地遵循了适当的引用和版权规定。

借鉴内容：本白皮书在撰写过程中可能参考或借鉴了其他公开的标准、文献、研究成果或公共领域的资料。我们已在可能的情况下注明了这些内容的来源和出处。

信息准确性：尽管我们已尽力确保本白皮书中的信息准确无误，但我们不保证信息的绝对准确性或完整性，也不对因依赖本文档内容而产生的任何后果负责。

免责声明：本白皮书提供的信息仅供参考，不构成任何投资建议或决策依据。我们不对因使用本白皮书内容而导致的任何直接、间接、附带、特殊或后果性损害承担责任。

第三方内容：本白皮书可能包含对第三方产品、服务或组织的引用。这些引用不表示 smart 对这些第三方或其产品、服务的认可或推荐。

学术诚信与引用：本白皮书在撰写过程中严格遵守学术诚信原则，对于所有借鉴的内容均已表明，以尊重原作者的知识产权。

修改与更新：我们保留随时修改或更新本白皮书内容的权利，无需另行通知。建议读者定期查阅最新版本。

适用范围：本免责声明适用于本白皮书的所有版本和修订，以及任何衍生作品或翻译版本。

法律管辖：本免责声明的解释、适用和争议解决应遵循文档发布地的法律。

我们希望通过本白皮书促进对智能网联汽车数据分类分级的理解和讨论，并鼓励读者在遵守上述声明的前提下，自由地分享和讨论相关内容。

ABSTRACT 摘 要

随着信息技术的快速发展和数字化转型的深入推进，“数据”已成为关键的战略资源和重要的生产要素。智能网联汽车作为现代交通技术的重要成果，其核心特征之一是产生了大量的、多样化的数据，这些数据不仅对提升车辆性能和用户体验至关重要，对维护交通安全、推动智能交通系统的发展具有深远影响。在数字经济时代，数据的价值日益凸显，同时数据安全和个人隐私保护问题也日益突出。为了平衡数据的利用与保护，数据分类分级制度成为企业数据治理工具的关键。本白皮书旨在阐述，通过科学合理的分类分级方法，可以为数据的安全保护、合规管理和有效流通提供制度保障，避免敏感数据的防护不足，非敏感数据的过度防护，实现数据安全和开发利用之间的平衡。

CONTENT 目 录

1　智能网联汽车数据分类分级的价值

1.1 保护高价值“数据”资产

在数字化时代，数据被视为一种宝贵的资产，具有极高的经济和战略价值。在现代经济活动中，数据高价值资产的应用已经被广泛认可并得到了大量的实践：

1. 企业决策支持：通过对大数据的分析，企业可以更好地了解市场趋势、客户需求、产品表现等信息，从而制定更明智的决策。

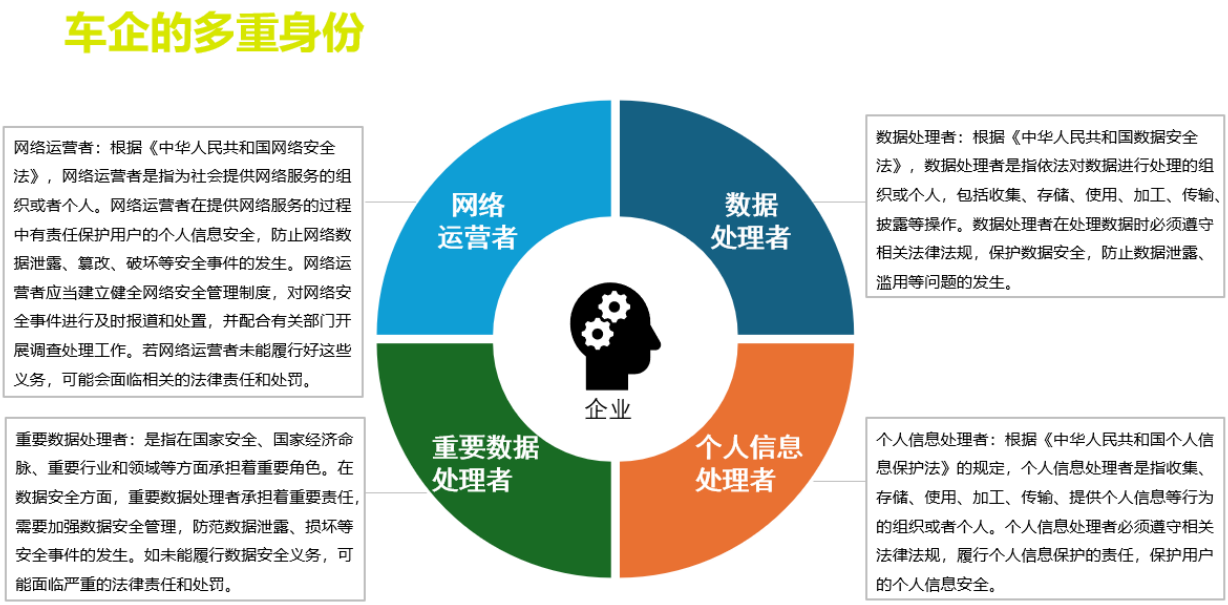
2. 个性化营销：利用数据分析技术，企业可以更好地理解和洞察客户，实现个性化营销，提高市场份额和客户忠诚度。

3. 风险管理：机构利用数据资产进行风险管理，包括信用评分、反欺诈等，确保资产安全并提升盈利能力。

4. 产品创新：通过大数据分析，企业可以更好地了解市场需求，推出更具创新性和竞争力的产品和服务。

5. 效率提升：数据资产还可以帮助企业优化生产过程、供应链管理等，提升生产效率和降低成本。

1.2 识别车企的“多重身份”



网络运营者：根据《中华人民共和国网络安全法》，网络运营者是指为社会提供网络服务的组织或者个人。网络运营者在提供网络服务的过程中有责任保护用户的个人信息安全，防止网络数据泄露、篡改、破坏等安全事件的发生。网络运营者应当建立健全网络安全管理制度，对网络安全事件进行及时报道和处置，并配合有关部门开展调查处理工作。若网络运营者未能履行好这些义务，可能会面临相关的法律责任和处罚。

数据处理者：根据《中华人民共和国数据安全法》，数据处理者是指依法对数据进行处理的组织或个人，包括收集、存储、使用、加工、传输、披露等操作。数据处理者在处理数据时必须遵守相关法律法规，保护数据安全，防止数据泄露、滥用等问题发生。

个人信息处理者：根据《中华人民共和国个人信息保护法》的规定，个人信息处理者是指收集、存储、使用、加工、传输、提供个人信息等行为的组织或者个人。个人信息处理者必须遵守相关法律法规，履行个人信息保护的责任，保护用户的个人信息安全。

重要数据处理者：是指在国家安全、国家经济命脉、重要行业和领域等方面承担着重要角色。在数据安全方面，重要数据处理者承担着重要责任，需要加强数据安全管理，防范数据泄露、损坏等安全事件的发生。如未能履行数据安全义务，可能面临严重的法律责任和处罚。

1.3 剖析智能网联汽车数据

智能网联汽车（Intelligent Connected Vehicles, ICVs）作为汽车产业发展的新焦点，其数据特征具有“多样性”、“实时性”、“交互性”、“规模性”、“高价值性”以及“安全和隐私性”。

1.数据的多样性

智能网联汽车的数据来源于车载传感器、控制器、执行器等装置，以及与外部环境的交互，如车与人、车与车、车与路、车与云端的通信。这些数据包括但不限于车辆状态信息、驾驶行为数据、交通环境信息、位置信息等，形成了一个多源、异构的数据集合。

2.数据的实时性

智能网联汽车在行驶过程中，需要实时收集和处理大量数据，以支持车辆的智能决策和控制。例如，车辆的实时位置、速度、加速度等信息，以及周围环境的实时变化，都需要快速响应和更新。

3.数据的交互性

智能网联汽车的数据不仅在车辆内部流通，还需要与外部系统进行交互。例如，车辆与交通基础设施的通信、车辆与云端服务的交互等，这些交互过程中产生的数据需要有统一的格式和定义，以便于数据的共享和利用。

4.数据的规模性

智能网联汽车产生的数据量巨大，随着车辆数量的增加和网联化程度的提高，数据规模将持续增长。这对数据存储、处理和分析提出了更高的要求，需要强大的数据处理能力和高效的数据管理策略。

5.数据的高价值性

智能网联汽车的数据不仅对车辆的运行和维护具有重要意义，而且对于提升交通安全、优化交通管理、推动智能交通系统建设等方面都具有极高的价值。通过对数据的分析和挖掘，可以发现新的商业模式和服务模式，促进产业创新和高质量发展。

6.数据的安全和隐私性

智能网联汽车的数据涉及用户的个人信息和车辆的运行状态，因此数据的安全性和隐私保护尤为重要。数据的采集、存储、传输和使用都需要符合相关的法律法规和标准要求，确保数据不被非法获取、滥用或泄露。

2　数据分类分级制度保障

我国在数据安全方面的制度保障采用了全面而系统的体系，在规范数据处理活动，保障数据安全，促进数据开发利用，保护个人、组织的合法权益，同时维护国家主权、安全和发展利益等各方面均制定了相应的要求。以下是我国数据分类分级相关法律法规政策要求及标准。

2.1 数据分类分级相关法律法规政策要求

中华人民共和国网络安全法			
发布单位	全国人民代表大会常务委员会	实施时间	2017 年 6 月 1 日
条文号	内容		
第三章第一节 第二十一条	国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改： （一）制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任； （二）采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施； （三）采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月； （四）采取数据分类、重要数据备份和加密等措施； （五）法律、行政法规规定的其他义务。		
第四章 第四十条	网络运营者应当对其收集的用户信息严格保密，并建立健全用户信息保护制度。		

【解读】我国于 2016 年颁布并于 2017 年施行的《中华人民共和国网络安全法》是我国网络安全管理方面的第一部基础性立法，旨在应对我国网络安全领域的严峻形势，以制度建设加强网络空间治理。《中华人民共和国网络安全法》全面地规定网络与信息安全治理的基本规则，以网络播秩序，惩治网络违法犯罪。运营者及关键信息基础设施运

营者为主要规制对象，明确网络运行安全、网络信息安全、监测预警与应急处置等方面的义务。

《中华人民共和国网络安全法》第二十一条规定了网络安全等级保护制度，在保障网络系统安全的组织架构及管理体系上，要求网络运营者需按照该制度要求制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任。在保障网络系统安全的技术体系上，要求网络运营者采取包括：防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施，保护网络系统和数据的安全；采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月;采取数据分类、重要数据备份和加密等措施。第四十条强调用户信息保密责任，建立健全用户信息保护制度等。

中华人民共和国数据安全法			
发布单位	全国人民代表大会常务委员会	实施时间	2021 年 9 月 1 日
条文号	内容		
第三章 第二十一条	国家建立数据分类分级保护制度，根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，对数据实行分类分级保护。国家数据安全工作协调机制统筹协调有关部门制定重要数据目录，加强对重要数据的保护。 关系国家安全、国民经济命脉、重要民生、重大公共利益等数据属于国家核心数据，实行更加严格的管理制度。 各地区、各部门应当按照数据分类分级保护制度，确定本地区、本部门以及相关行业、领域的重要数据具体目录，对列入目录的数据进行重点保护。		

第四章 第二十七条	开展数据处理活动应当依照法律、法规的规定，建立健全全流程数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，保障数据安全。利用互联网等信息网络开展数据处理活动，应当在网络安全等级保护制度的基础上，履行上述数据安全保护义务。 重要数据的处理者应当明确数据安全负责人和管理机构，落实数据安全保护责任。

【解读】由于不同维度的数据的价值不一，而且对于国家利益、社会利益、个人利益有着不同程度的影响,数据安全治理首先需要实施数据的分类分级保护，避免因重要数据泄露、损毁带来影响国家安全、社会安全的严重后果。

鉴于此，《中华人民共和国数据安全法》第二十一条明确国家建立数据分类分级保护制度，具体内容包括：数据分类分级，对数据实行分类分级保护；制定重要数据目录，加强对重要数据的保护。对核心数据实行更加严格的管理制度等。同时，第二十七条明确要求开展数据处理活动应当依照法律、法规的规定，建立健全全流程数据安全管理制度。这意味着数据处理者在数据的收集、存储、使用、加工、传输、提供、公开等各个环节，都需要有相应的安全管理制度来规范和保障数据的安全，确保数据处理活动合法合规.。对于开展数据处理活动的主体，可以数据分类分级为基础，形成组织、管理、技术体系相融合的数据安全治理体系。

中华人民共和国个人信息保护法			
发布单位	全国人民代表大会常务委员会	实施时间	2021 年 11 月 1 日
条文号	内容		
第五章 第五十一条	个人信息处理者应当根据个人信息的处理目的、处理方式、个人信息的种类以及对个人权益的影响、可能存在的安全风险等，采取下列措施确保个人信息处理活动符合法律、行政法规的规定，并防止未经授权的访问以及个人信息泄露、篡改、丢失： （一）制定内部管理制度和操作规程； （二）对个人信息实行分类管理； （三）采取相应的加密、去标识化等安全技术措施； （四）合理确定个人信息处理的操作权限，并定期对从业人员进行安全教育和培训；		

	（五）制定并组织实施个人信息安全事件应急预案； （六）法律、行政法规规定的其他措施。

【解读】相较于一般数据，个人信息因对个人权益的影响需要进行专门的保护。为了解决一些企业、机构甚至个人，从商业利益等出发，随意收集、违法获取、过度使用、非法买卖个人信息，利用个人信息侵扰人民群众生活安宁、危害人民群众生命健康和财产安全等问题，在保障个人信息权益的基础上，促进信息数据依法合理有效利用，2021年颁布并施行的《中华人民共和国个人信息保护法》是我国首部关于保护个人信息的专门性法律。这部法律以数据中的“个人信息”为主要规范对象，划定个人信息全生命周期处理的安全保护规则，以保护个人信息权益、促进个人信息合理利用。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。

汽车数据安全管理若干规定（试行）			
发布单位	国家互联网信息办公室、国家发展和改革委员会、工业和信息化部、公安部、交通运输部。	实施时间	2021年10月1日
条文号	内容		
第四条	汽车数据处理者处理汽车数据应当合法、正当、具体、明确，与汽车的设计、生产、销售、使用、运维等直接相关。		
第五条	利用互联网等信息网络开展汽车数据处理活动，应当落实网络安全等级保护等制度，加强汽车数据保护，依法履行数据安全义务。		

【解读】2021年10月1日，国家网信办、工信部等五部委联合发布的《汽车数据安全管理若干规定(试行)》正式施行，作为行业垂直监管的典型，该《规定》聚焦汽车领域个人信息和重要数据的安全风险，从汽车重要数据定义、收集原则、定期报送制度等方面，配套落实《中华人民共和国数据安全法》等上位法律原则在汽车数据领域的具体规范。同时，该《规定》强调了国家加强智能网联汽车网络平台的建设，开展智能网联汽车运行和安全保证服务等，并协同汽车数据处理者加强智能网联汽车网络和数据安全防护。

工业数据分类分级指南（试行）			
发布单位	工业和信息化部办公厅	实施时间	2020年2月27日

条文号	内容
第五条	工业企业结合生产制造模式、平台企业结合服务运营模式，分析梳理业务流程和系统设备，考虑行业要求、业务规模、数据复杂程度等实际情况，对工业数据进行分类梳理和标识，形成企业工业数据分类清单。
第八条	根据不同类别工业数据遭篡改、破坏、泄露或非法利用后，可能对工业生产、经济效益等带来的潜在影响，将工业数据分为一级、二级、三级等 3 个级别。

【解读】2020 年 2 月 27 日，工业和信息化部办公厅印发了《工业数据分类分级指南（试行）》，为企业提供了分类分级的指导依据，指出企业结合行业要求、业务规模、数据复杂程度等实际情况，围绕数据域进行类别梳理，形成分类清单；同时按照每类工业数据遭篡改、破坏、泄露或非法利用后可能带来的潜在影响，将数据划分为 3 个级别

2.2 智能网联汽车数据分类分级相关国标/行标

序号	标准编号	名称	发布机构	实施日期
1	GB/T 36073-2018	《数据管理能力成熟度评估模型》	国家质量监督检验检疫总局 中国国家标准化管理委员会	2018/10/1
2	GB/T 37988-2019	《信息安全技术 数据安全能力成熟度模型》	国家市场监督管理总局 中国国家标准化管理委员会	2020/3/1
3	GB/T 35273-2020	《信息安全技术 个人信息安全规范》	国家市场监督管理总局 国家标准化管理委员会	2020/10/1
4	GB/T 38667-2020	《信息技术 大数据 数据分类指南》	国家市场监督管理总局 中国国家标准化管理委员会	2020/11/1
5	GB/T 41871-2022	《信息安全技术 汽车数据处理安全要求》	国家市场监督管理总局 国家标准化管理委员会	2023/5/1
6	GB/T 41773-2022	《信息安全技术 步态识别数据安全要求》	国家市场监督管理总局 国家标准化管理委员会	2023/5/1
7	GB/T 42128-2022	《智能制造 工业数据 分类原则》	国家市场监督管理总局 国家标准化管理委员会	2023/7/1
8	GB/T 43697-2024	《数据安全技术 数据分类分级规则》	国家市场监督管理总局 国家标准化管理委员会	2024/10/1
9	YD/T 3751-2020	《车联网信息服务 数据安全技术要求》	中华人民共和国工业和信息化部	2020/10/1
10	YD/T 3746-2020	《车联网信息服务 用户个人信息保护要求》	中华人民共和国工业和信息化部	2020/10/1

随着“新四化”的迅速推进，智能网联汽车网络安全与数据安全技术正面临加速迭代演进，产业发展不断深化，当前，车、路、云、网、图的协同发展，致使数据安全正成为影响消费者购车决策的重要因子，而数据分类分级是数据安全的基石。

2024 年 10 月正式实施的国家标准《数据安全技术 数据分类分级规则》，规定了数据分类分级的原则、框架、方法和流程，给出了重要数据识别指南，为各行业各领域的数据处理者开展数据分类分级工作提供了规范性的指导。

《信息安全技术 汽车数据处理安全要求》、行业标准《车联网信息服务 数据安全技术要求》和全国信息安全标准化技术委员会（TC260）发布的技术文件《汽车采集数据处理安全指南》明确了汽车在采集、使用、存储和出境等多个处理环节的安全标准。

系列标准的建立和发布都标志着我国智能网联汽车数据分类分级的规范化和标准化进程正在加速。

3　智能网联汽车数据分类分级面临的挑战

智能网联汽车数据分类分级的落地实施面临着一系列的挑战，涉及技术、法规、基础设施建设、商业模式以及个人隐私保护等多个方面。

3.1 技术挑战

智能网联汽车产生的数据量大且多样，包括结构化和非结构化数据。智能网联汽车通过车载传感器、摄像头、GPS等设备实时收集车辆运行数据、交通信息、环境数据等，这些数据的体量巨大，对数据存储和处理系统提出了高要求。如何有效地对这些数据进行分类和分级，确保数据的准确性和实时性，是一个技术挑战。此外，数据的安全性和隐私保护也是技术层面需要解决的问题。

3.2 法规和标准不完善

智能网联汽车的数据分类分级需要相应的法律法规和标准来指导和规范。目前，相关法规和标准尚不完善，部分条款可能形成制约，给数据分类分级的实施带来了不确定性。

3.3 基础设施建设的挑战

智能网联汽车的发展需要配套的智能基础设施，如智能道路、通信网络等。基础设施的智能化改造需要巨大的投资和长期的周期，且涉及跨部门协调和跨产业协同，这些因素都增加了数据分类分级的难度。

3.4 数据资产化的挑战

智能网联汽车的数据种类繁多，包括但不限于车辆性能数据、驾驶行为数据、乘客个人信息、交通流量数据、道路状况数据等，这些数据既有结构化的，也有非结构化的。智能网联汽车数据的资产化和价值释放是推动产业发展的关键。如何确保数据的有效利用，同时保护数据安全和个人隐私，是一个复杂的问题。此外，数据的权属、交易和流通机制也需要进一步明确和完善。

3.5 国际合作与数据跨境管理场景复杂

在全球化背景下，智能网联汽车的数据跨境管理和国际合作也是一个挑战。如何平

衡国际合作与数据安全，确保数据在全球范围内的合规流通，需要国际间的协调和合作。

综上所述，智能网联汽车数据分类分级的落地实施是一个系统工程，需要行业内外的共同努力，包括技术研发、法规制定、产业链完善、基础设施建设、商业模式创新等等。通过解决这些问题，可以促进智能网联汽车产业的健康发展，实现数据的有效管理和安全保护。

4　smart 数据分类分级的实践

面对数据分类分级带来的各项挑战，在企业如何有效的开展分类分级工作？如何建立合适的数据分类分级体系？如何保障数据安全？等问题。本白皮书参照现行的监管要求，数据分类分级国家标准，以及行业标准等，结合 smart 数据分类分级的实践成果，将从**数据分类分级方法论**到**数据分类分级体系构建运行**再到**数据分类分级工具落地运营**，对数据分类分级工作的全生命周期展开分析。

4.1 数据分类分级方法论

4.1.1 目标&原则

数据分类分级不仅是行业发展的必然趋势，也是保障车辆安全、促进产业发展、满足市场需求的必要手段。客户信息包括个人信息等敏感数据，若未加以妥善分类和保护，一旦泄露可能会对客户隐私造成侵犯，同时也会给企业带来信誉和经济上的损失。smart 在开展数据分类分级工作规划阶段，放在首位的是在数据安全方面的考虑，通过建立清晰的数据分级体系、实施严格的数据分类分级制度，确保敏感数据得到更高级别的安全保护，从而降低数据泄露的风险，提升数据安全。

数据分类分级原则

数据分类分级的原则旨在确保数据在整个生命周期中得到适当的保护，同时满足组织的数据管理和业务需求。

01	02	03	04	05
科学实用原则：	**边界清晰原则：**	**就高从严原则：**	**点面结合原则：**	**动态更新原则：**
从便于数据管理和使用的角度，科学选择常见、稳定的属性或特征作为数据分类的依据，并结合实际需要对数据进行细化分类。	数据分级的各级别应边界清晰，对不同级别的数据采取相应的保护措施。	采用就高不就低的原则确定数据级别，当多个因素可能影响数据分级时，按照可能造成的各个影响对象的最高影响程度确定数据级别。	数据分级既要考虑单项数据分级，也要充分考虑多个领域、群体或区域的数据汇聚融合后的安全影响，综合确定数据级别。	根据数据的业务属性、重要性和可能造成的危害程度的变化，对数据分类分级、重要数据目录等进行定期审核更新。

a) 科学实用原则：从便于数据管理和使用的角度，科学选择常见、稳定的属性或特征作为数据分类的依据，并结合实际需要对数据进行细化分类。

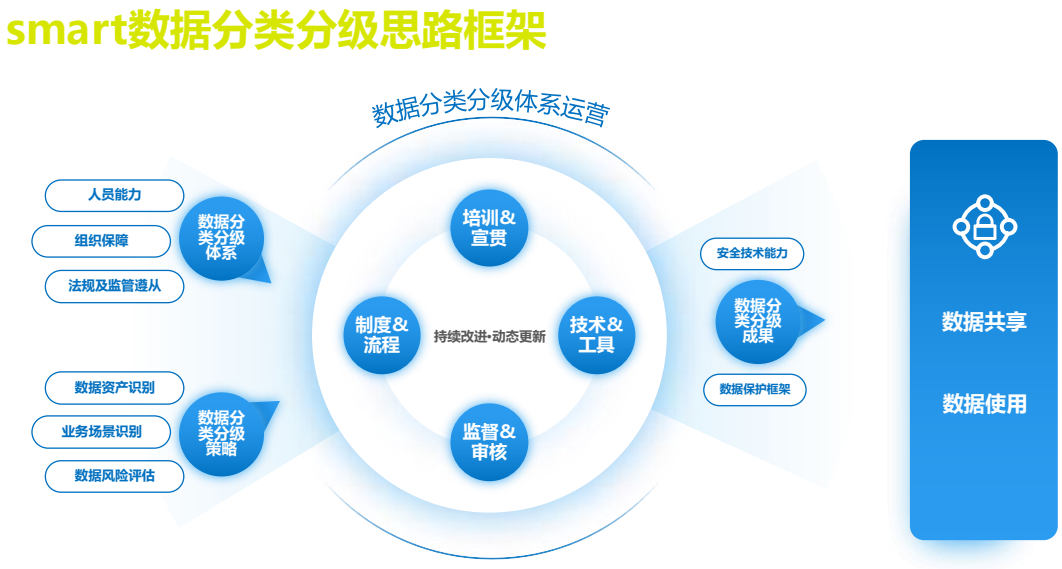
b) 边界清晰原则：数据分级的各级别应边界清晰，对不同级别的数据采取相应的保护措施。

c) 就高从严原则：采用就高不就低的原则确定数据级别，当多个因素可能影响数据分级时，按照可能造成的各个影响对象的最高影响程度确定数据级别。

d) 点面结合原则：数据分级既要考虑单项数据分级，也要充分考虑多个领域、群体或区域的数据汇聚融合后的安全影响，综合确定数据级别。

e) 动态更新原则：根据数据的业务属性、重要性和可能造成的危害程度的变化，对数据分类分级、重要数据目录等进行定期审核更新。

4.1.2 smart 数据分类分级思路框架



首先，组建由数据安全、数据合规、业务等部门专家组成的数据分类分级专项工作组，并对相关人员进行了数据安全法律法规、数据分类分级策略及操作流程的培训；再利用工具对各系统数据进行扫描，创建全面的企业数据资产清单，包括数据来源、类型、存储位置、使用方式等，最后，对数据资产进行价值和风险评估，确定数据的敏感性和重要性。

其次，充分结合数据资产清单及评估结果，根据数据的特性和用途，制定数据分类分级策略。同时，将分类分级规则集成到数据分类分级系统工具中，为每项数据资产打上分类分级的标签，确保数据分类分级系统与现有的数据存储、处理和传输系统集成，实现自动化管理。

紧接着，根据数据分类分级策略，对现有数据安全管理制度进行优化，构建数据分类分级体系，明确数据访问、传输、使用、处理等生命周期的安全规则，依据规则实施加密、访问控制、数据备份、安全审计等技术保护措施，在公司内部通过培训与宣贯，加强数据安全管理体系的落地性。

最后，依托现有安全技术能力，根据结合实际设计好的数据保护框架，对数据的共享、数据使用等数据处理活动施行有效的安全管理，提升数据流动安全。

4.1.3 方法（分类、分级、动态更新）

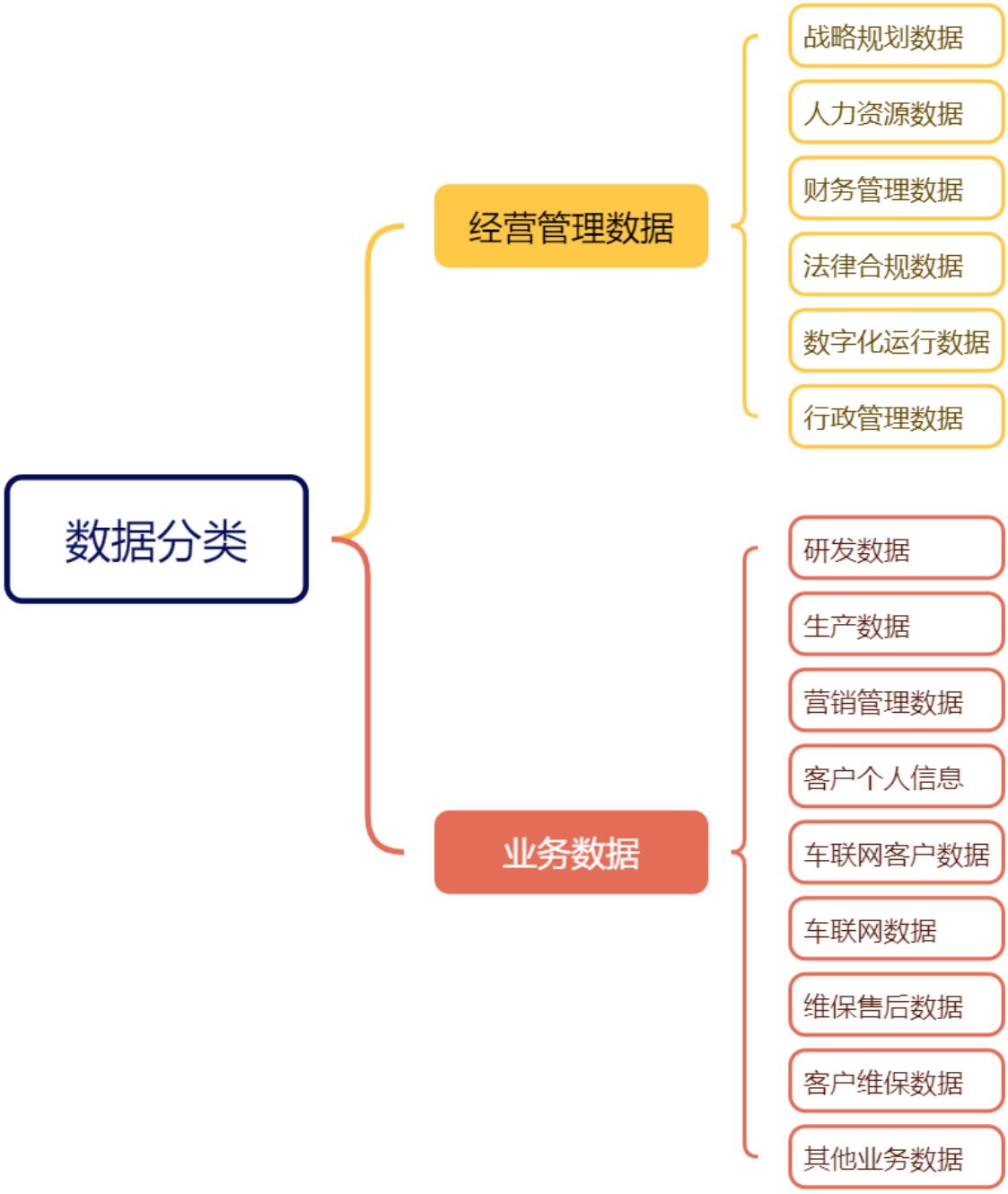
数据分类分级工作是确保数据安全、提高运营效率和促进技术创新的重要基础。随着车联网技术的发展，车辆与外界的连接越来越广泛，产生了大量的数据，这些数据不仅包括车辆本身的运行数据，还包括用户的个人信息以及行驶环境的相关信息。因此，对这些数据进行有效的分类和分级管理变得尤为重要。依据 smart 数据分类分级工作思路，我们先进行了全面的数据资产盘点，梳理出数据资产清单，清单内容包括：数据来源、类型、存储位置、使用方式等，接着对数据资产进行价值和风险评估，确定数据的敏感性和重要性，为制定准确的数据分类分级策略做足准备。

4.1.3.1 分类方法

数据分类分级的重点在于对数据的分类与分级，依据《汽车数据安全管理若干规定（试行）》《工业和信息化领域数据安全管理办法（试行）》等国家及行业指导意见，我们根据 smart 数据资产清单及评估结果，结合数据的特性和用途，制定了详细的数据分类标准，从企业管理视角来进行划分，分为对内经营管理数据和对外业务数据，经营管理数据细分为：战略规划数据、人力资源数据、财务管理数据、法律合规数据、数字化运行数据、行政管理数据，六个大类；业务数据依据“研、产、销“[1]一体化结构分为：研发数据、生产数据、营销管理数据、客户个人信息、车联网客户数据、车联网数据、维保售后数据、客户维保数据以及其他业务数据等[2]。

[1] 注：客户信息作为企业重点保护和关注的数据，在“研、产、销”每个阶段都可能会涉及，个人信息和始终是业务息息相关的，因此本白皮书建议的数据分类方法，将客户信息融合进业务数据中做分类。

[2] 数据分类规则示例详见附录一


数据分类
经营管理数据
战略规划数据
人力资源数据
财务管理数据
法律合规数据
数字化运行数据
行政管理数据
业务数据
研发数据
生产数据
营销管理数据
客户个人信息
车联网客户数据
车联网数据
维保售后数据
客户维保数据
其他业务数据

4.1.3.2 分级方法

依据《汽车数据安全管理若干规定（试行）》《工业和信息化领域数据安全管理办法（试行）》等国家及行业指导意见，根据数据在经济社会发展中的重要程度，从影响程度和影响对象两个方面考虑，采用定性指标来识别并判定数据的等级，先整体将数据分为**核心数据、重要数据、一般数据**，从而形成分级规则矩阵表，如下：

数据级别确定规则表			
影响对象	影响程度		
	特别严重危害	严重危害	一般危害
国家安全	核心数据	核心数据	重要数据
经济运行	核心数据	重要数据	一般数据
社会秩序	核心数据	重要数据	一般数据
公共利益	核心数据	重要数据	一般数据
组织权益、个人权益	一般数据	一般数据	一般数据

1.核心数据

其中，**核心数据**[3]的定义为对领域、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，一旦被非法使用或共享，可能直接影响政治安全的重要数据；结合 smart 数据资产评估结果，当前 smart 暂不涉及**核心数据**，因此在开展数据分级工作过程中对于**核心数据**为“保持关注”状态。

2.重要数据

根据《汽车数据安全管理若干规定（试行）》中对**重要数据**[4]的定义，**重要数据**是指一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能危害国家安全、公共利益或者个人、组织合法权益的数据，包括：

（一）军事管理区、国防科工单位以及县级以上党政机关等重要敏感区域的地理信息、人员流量、车辆流量等数据；

[3] 注：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、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。

[4] 注：重要数据的定义依据网信办、发展改革委、工业和信息化部、公安部、交通运输部 2021 年 08 月 16 日发布的《汽车数据安全管理若干规定（试行）》。

（二）车辆流量、物流等反映经济运行情况的数据；

（三）汽车充电网的运行数据；

（四）包含人脸信息、车牌信息等的车外视频、图像数据；

（五）涉及个人信息主体超过 10 万人的个人信息；

（六）国家网信部门和国务院发展改革、工业和信息化、公安、交通运输等有关部门确定的其他可能危害国家安全、公共利益或者个人、组织合法权益的数据。

结合 smart 数据资产评估结果，分析当前会涉及**重要数据**，因此在开展数据分级工作过程中对于**重要数据**在“保持关注”的基础上，根据监管要求，我们开展“重要数据”梳理和识别，并进行“重要数据”目录的构建[5]。

3.一般数据

结合 smart 数据资产盘点结果，根据实际，针对“**一般数据**”，从数据对两个影响对象（对个人用户合法权益和对企业合法权益）分别影响的程度考虑和分析，将“**一般数据**”再分为一般一级（DL1）、一般二级（DL2）、一般三级（DL3）、一般四级（DL4）。

数据安全级别	级别定义	企业合法权益影响程度	个人合法权益影响程度	传播范围
一般一级 (DL1)	对企业内部、外部人员和组织均可以公开的数据。数据遭到篡改、破坏、泄露或者非法获取、非法利用，基本不会对企业及个人合法权益造成危害。	无危害	无危害	具有公共传播属性，可对外公开发布，转发传播，但也需要考虑公开的数据量和类别，避免由于类别较多或数量过大被用于关联分析。
一般二级 (DL2)	可在企业内部公开，数据一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能会对企业及个人合法权益造成较小或轻微危害。	轻微危害	轻微危害	通常在企业内部、关联方共享和使用，或签署保密协议后的三方人员可查阅的信息。经企业相关方授权后方可向组织外部开放。
一般三级 (DL3)	是企业或个人的关键数据，对个人权益或企业利益有极大影响，如泄露会造成严重性后果。	一般危害	一般危害	仅能由授权企业内部机构或人员访问，如涉及数据传输和开放，须得到足够授权。
一般四级 (DL4)	是企业或个人的敏感/重要的数据，对个人权益或企业根本利益有决定性影响，如泄露会造成灾难性后果。	严重危害	严重危害	按照批准授权列表严格管理，须经过严格审批、评估后，在受控范围内传输和开放。

4.最低参考级别

特定类型一般数据的最低参考级别如下：

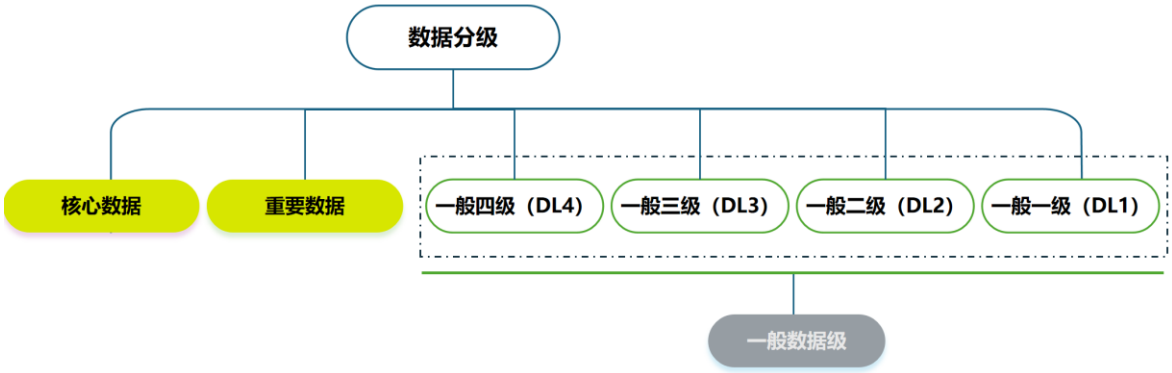
a）敏感个人信息不低于 4 级，一般个人信息不低于 2 级；

[5] 重要数据目录示例详见附件二：“重要数据”目录

b）内部员工个人信息不低于 2 级；

c）有条件开放/共享的公共数据级别不低于 2 级，禁止开放/共享的公共数据不低于 4 级。

综上所述，数据分级如下[6]。



4.1.3.3 动态更新情形

数据分类分级需特别注意结合企业实际和业务场景，动态调整划分，如出现下列情形之一的，应根据动态更新原则，重新定级。

a) 数据内容发生变化，导致原有数据安全级别不再适用。

b) 数据内容未发生变化，但数据时效性、数据规模、数据应用场景、数据加工处理方式等发生变化。

c) 多个原始数据直接合并，导致原有安全级别不再适用合并后的数据。

d) 因对不同数据选取部分数据进行合并形成的新数据，导致原有数据安全级别不再适用合并后的数据。

e) 不同数据类型经汇聚融合形成新的数据类别，导致原有数据级别不再适用于汇聚融合后的数据。

f) 因国家或行业主管部门要求，导致原定数据级别不再适用。

g) 需对数据安全级别进行变更的其他情形。

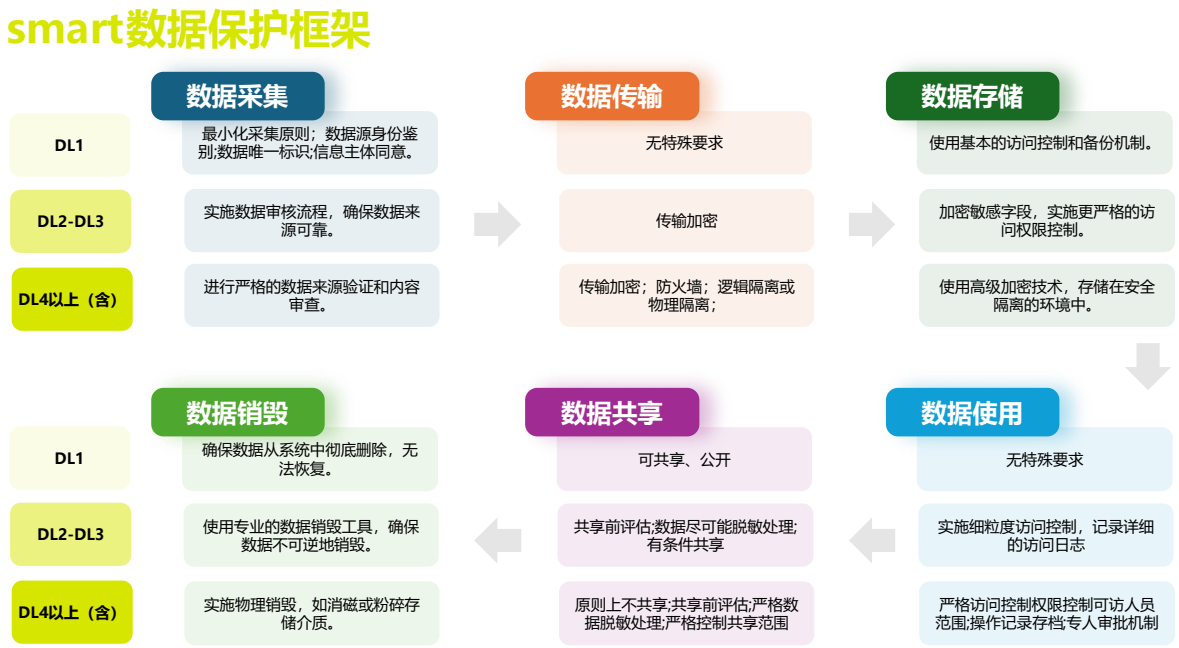
数据变化定级参考：

数据发生变化导致安全级别变化的规则，包括但不限于：

[6] 数据分级规则详见附录一。

措施或情形	安全级别变化
数据体量增加到特定规模，导致社会重大影响。	升级
达到国家有关部门规定精度的数据。	升级

4.1.4 保护框架



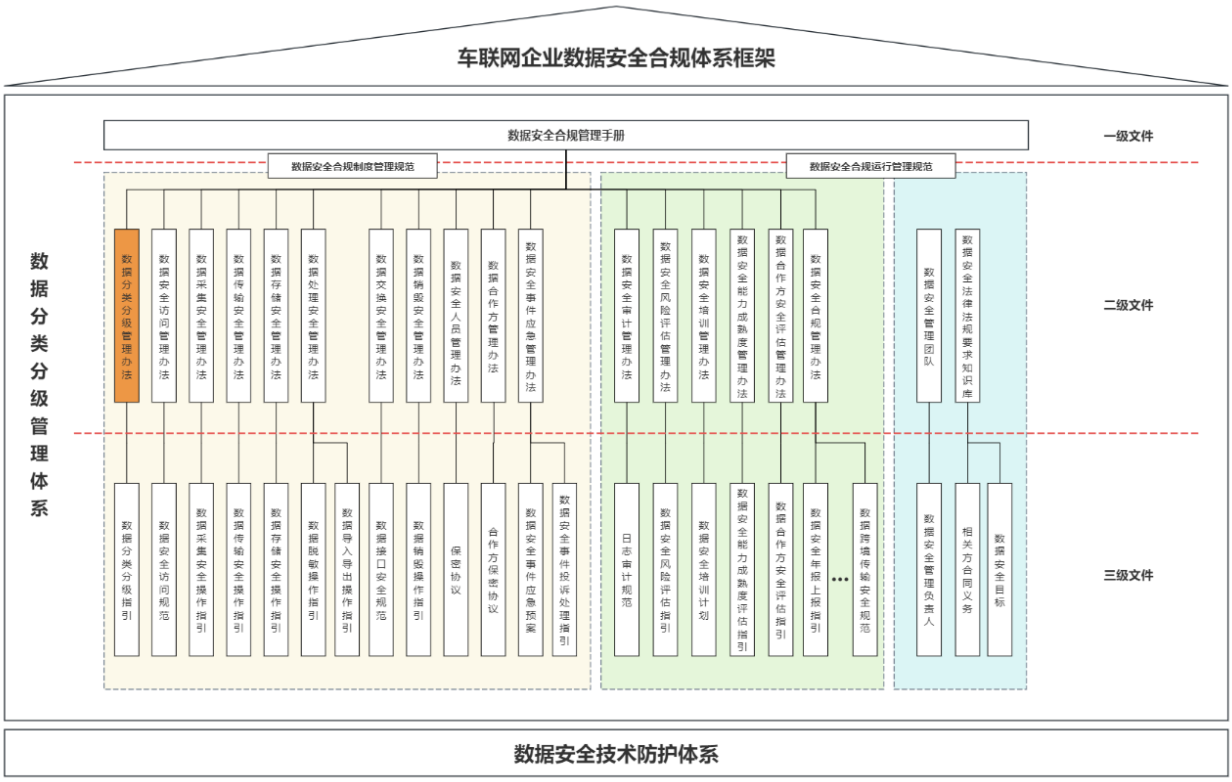
4.2 数据分类分级体系构建与运行

4.2.1 人员能力

对于数据安全人员的能力要求是多方面的，需涵盖管理、运营、技术、合规等多个层面。具体包括：

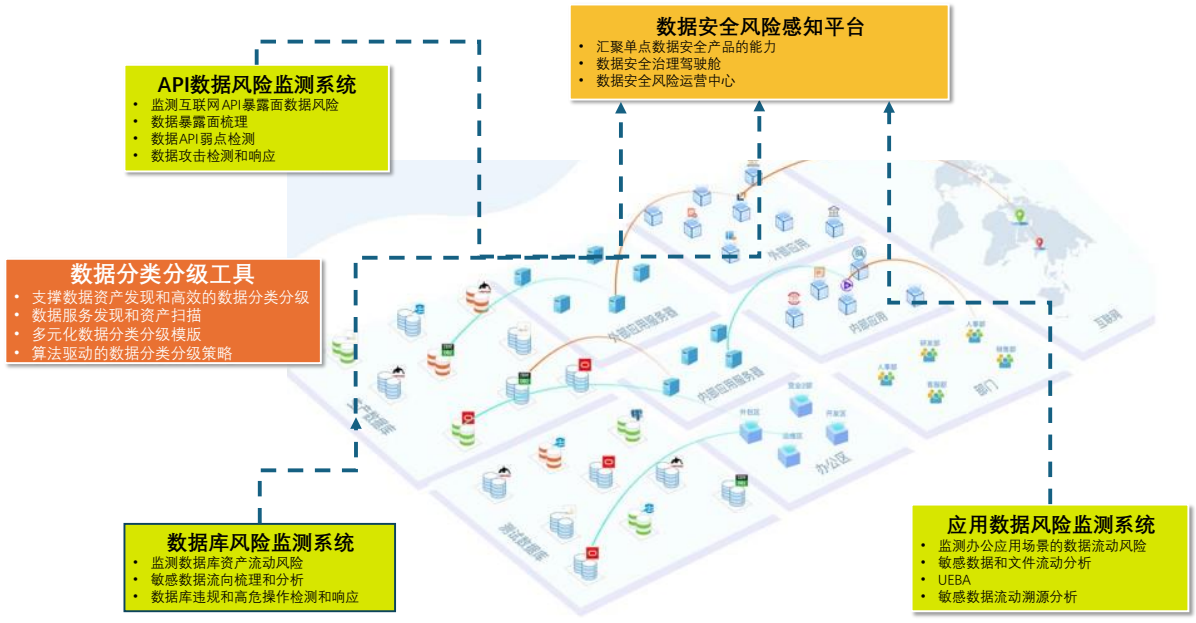
4.2.2 组织保障

4.2.3 体系构建



4.3 数据分类分级工具落地运营

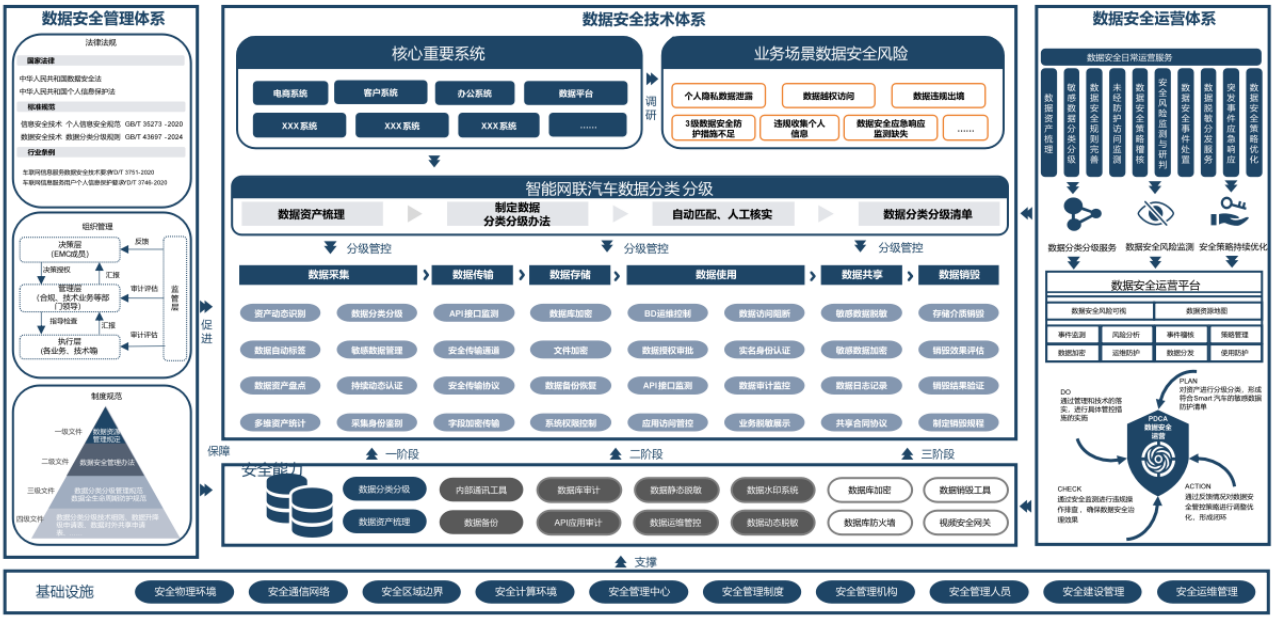
smart 数据安全防护体系



5　数据安全治理

大多数新能源汽车企业已构建了侧重于网络和信息系统安全的防护体系，围绕新能源汽车业务场景的数据全生命周期管理保护仍处于起步阶段。以新能源汽车产业数据为核心的安全治理体系是一个内部相互依存、紧密关联的生态系统。制度规范体系能为技术防护体系的构建提供明确方向，并为运营管理体系中的组织建设和人员能力培养提供根本遵循；运营管理体系确保制度规范的有效实施，使技术防护体系发挥实效；技术防护体系作为关键支撑，为制度规范和运营管理提供强大技术手段；数据安全应急响应和监督审计体系则为整个框架提供保障，构建了以新能源汽车产业数据为中心的可持续安全治理体系，全面提升企业的数据安全治理能力，如下图所示。

智能网联汽车数据安全治理框架



将数据分为研发数据、生产数据、营销管理数据、客户个人信息、车联网客户数据、车联网数据、维保售后数据、客户维保数据等分类，使数据更易于理解、访问和管理，降低了数据搜索和整理的时间成本。同时，通过数据分类能更好地发现数据之间的关联性和规律性，提高了数据分析结果的说服力和可信度，为业务决策提供了准确的数据支持，为数据分析提供了清晰的思路和基础数据支撑。其次，在汽车行业各个部门之间频繁地交换和共享数据资源，通过统一的分类标准进行归类整理，建立了统一的数据资源

目录，提升了各部门根据需求发现数据的管理效率，推动业务发展。

数据的分类促进了数据的使用和共享，同时数据分级的结果也弥补了数据治理中安全保护的不足，为不同级别数据的隐私和安全差异化保护提供指导方向。通过数据分级确定数据的重要性和敏感性，依据不同数据的级别制定分级安全保护措施，可以避免“一刀切”带来的问题。这种差异化的安全保护策略促进了数据使用的同时保护了数据的安全，有效地防止了数据泄露和滥用的风险，确保了数据的合规性和可信度。因此，数据的分类与分级在提升数据利用效率的同时，保障了数据自由使用的数据安全，全面支持数据治理，促进企业业发展与决策。

5.1 数据分类增强数据分析决策与管理能力

5.1.1 数据分类增强数据分析与决策能力

■ **客户数据分类**：包括客户基本资料信息、服务历史和客户反馈等，通过对这些数据的分析，可以帮助企业了解客户偏好，进行个性化营销活动，从而制定有效的营销策略和服务方案，提高客户满意度和忠诚度。

■ **营销管理数据分类**：包括销售数据、市场趋势、竞争对手信息等，通过对销售数据、市场趋势等信息进行数据分析，可帮助企业制定更有效的营销策略。

■ **研发数据分类** ：包括设计参数、测试数据、仿真结果等，通过对这些数据分析，可以帮助企业优化产品设计、提高产品质量和性能，同时预测市场需求和趋势，指导新产品开发方向。

■ **生产数据分类**：包括生产过程中的数据，如生产效率、设备故障率、原材料消耗等，通过对这些数据分析，可以帮助企业优化生产流程、降低生产成本，预测设备维护需求，提前安排维修计划，减少生产中断时间。

■ **车联网数据分类**：包括车联网客户数据和车辆运行数据，通过对这些数据分析，可以帮助企业了解车辆使用情况和客户需求，为产品改进和服务优化提供依据。

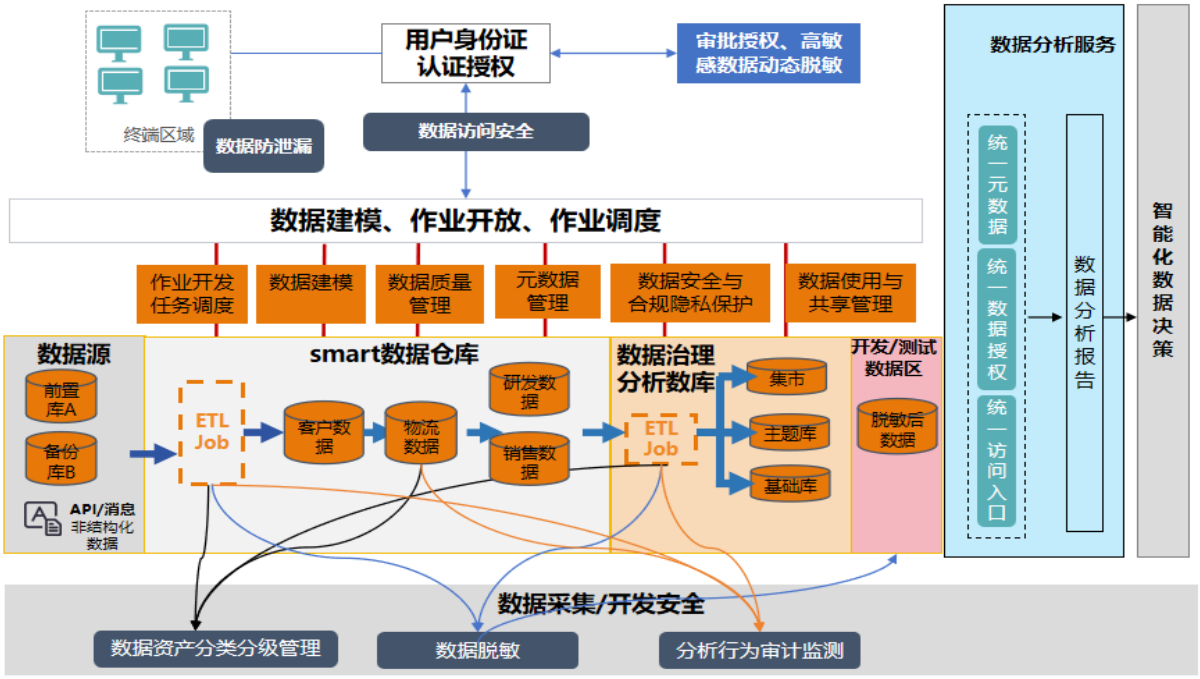
■ **维保售后数据分类**：包含维修记录和保养信息，过对这些数据深入分析，可以帮助企业减少车辆故障率和维修时间，提高车辆使用效率和客户满意度。同时，维保数据的分析还可以为产品设计和制造提供改进建议，提升产品质量和可靠性。

5.1.2 数据分类提升部门间数据协同共享效率

通过数据分类，企业可以建立起一个清晰、有序的数据资源目录，明确各类数据的存储位置和访问方式方便数据的查找和使用，进一步推动数据管理和使用的效率与准确性。

- **数据资源目录的清晰化：**数据分类使得企业能够按照特定的标准或属性（如数据类型、来源、用途等）将数据归类整理，从而形成一个结构化的数据资源目录。 这样的目录极大地方便了数据的查找和使用，减少了员工在海量数据中搜索信息的时间成本。
- **统一的数据管理平台：**有了清晰的数据分类，企业可以搭建一个统一的数据管理平台，该平台能够集中存储、管理和维护各类数据。统一管理平台不仅提高了数据的利用率，还通过标准化的数据处理流程确保了数据的一致性和准确性。
- **数据共享与协同的加强：** 在汽车行业，研发、生产、销售、服务等部门之间需要频繁地交换和共享数据。数据分类能够明确各个部门所需的数据类型和范围，从而建立起一个高效的数据共享平台。该平台可以实现数据的快速传递和实时更新，确保各部门能够及时获取最新的数据资源。同时，通过平台上的数据协同工具，各部门之间可以更加紧密地合作，共同推动业务的发展。

5.2 数据分级为数据治理提供差异化的安全保护支撑



智能网联汽车数据治理分级保护场景方案图的要求可以总结为以下几个方面，包括数据访问安全、数据资产分类分级管理、建立开测/测试数据脱敏区、数据处理行为全面审计监测，以下是对这些要求的详细展开：

■ **数据使用、开发、运维的数据访问安全**

1. 数据开发工具、用户等建立数据权限申请审批流程，根据用户访问权限动态进行数据细粒度授权，防止非授权访问通过身份认证鉴权。高危操作事前审批、事中控制和监视防止元数据库的随意访问、发布

2. 数据访问默认客户个人敏感信息动态脱敏展示，保护客户个人隐私安全。

3. 部署终端 DLP 防止数据被拷贝、外发等数据泄露风险。

■ **数据资产分类分级管理：**定期扫描发现数据库资产、数据资产、数据量形成数据地图，对数据进行分类分级标记掌握数据用户的权限情况，监控其变化掌握数据流向，对违规流动及时监测预警。

■ **建立开测/测试数据脱敏区：**敏感数据流转形成新的主题库或集市，对敏感数据脱敏保存到开发测试数据区来进行数据分析。

数据处理行为全面审计监测：对数据共享访问行为，包括数据库、API 等维度进行全面审计监测，并对敏感数据共享嵌入数据水印，为事件分析和追溯体用依据。

6 结语

随着新技术发展，自动驾驶、全息通信等场景将从实现 0 到 1 的突破，逐步落实为 1 到N的复制拓展，会进一步促进数据流转的场景更加丰富。在享受数据合作共享、流通、交易、跨境流转等场景带来的便利和好处的同时，我们应该认识到随着业务和数据处理活动的复杂化，不同应用间共享和共同处理数据，数据处理活动中存在模糊的边界,导致侵犯用户个人信息权益的事件屡屡发生。海量收集用户个人信息和记录用户行为，数据汇聚关联分析、智能化应用产生的影响，可能超出了单独企业主体能够承担风险的范围。随着 5G 和智能网联应用的发展，急需一个连贯的、基础的数据安全治理框架来应对数据安全和隐私保护问题，确保数据流转的合法性和可靠性。

通过数据分类分级以及安全治理建设项目的落地实施，帮助正处在数字化转型背景下的整车厂商提升了整体数据安全防护能力和数据安全管理水平。近年来,围绕数据生命周期全过程,融合技术、管理和运营。确保汽车制造数据的采集、传输、存储、使用、共享安全，做到汽车制造数据不被截获、篡改、窃取，以此促进汽车制造领域高速安全发展，为企业日常业务安全运转保驾护航。

附录一：“一般数据”分类分级示例

数据分类（示例）				数据定级（示例）			
				一般数据			
数据类型	二级子类	三级子类	数据内容	一般一级（DL1）	一般二级（DL2）	一般三级（DL3）	一般四级（DL4）
业务数据	研发数据	研发设计	源代码、设计图纸、整车造型图（未发布前）、造型数据等				✓
	生产数据	计划与产能数据	月产量计划、年产量计划、生产状态、排产状态、预计生产周期、产能等			✓	
	营销管理数据	商品信息	商品名称、商品类别、商品型号、商品参数、商品价格、商品评论等		✓		
		门店信息	交付中心名称、门店名称、门店地址、门店联系方式等	✓			
		试驾数据	预约单号、预约状态、试驾类型、试驾车型、试驾时间、试驾地址、试驾内容等			✓	
		订单信息	订单编号、订单渠道、订单状态、购车方式、订单数量等			✓	
		订单支付信息	订单价格、订单优惠金额、付款方式、支付渠道、折扣金额、实付金额、支付流水号、支付金额、退款金额等			✓	
	客户个人信息	个人基本概况信息	生日、性别、民族、国籍、家庭关系等		✓		
		个人基本信息	个人姓名、个人电话号码、电子邮箱、详细住址等			✓	

数据分类（示例）				数据定级（示例）			
				一般数据			
数据类型	二级子类	三级子类	数据内容	一般一级（DL1）	一般二级（DL2）	一般三级（DL3）	一般四级（DL4）
业务数据	客户个人信息	个人身份基本信息	工作证、出入证等			✓	
		个人身份信息	可直接标识自然人身份的信息，如身份证、军官证、护照、驾驶证、社保卡、居住证、港澳台通行证等证件号码、证件照片或者影印件等				✓
		个人教育工作背景	个人职业、工作单位等		✓		
		网络身份标识信息	用户头像、昵称、个性签名、个人信息主体账号、用户 ID、即时通信账号、网络社交用户账号、IP 地址等		✓		
		网络身份鉴别信息	账户登录密码、银行卡密码、支付密码、账户查询密码、交易密码、银行卡有效期、银行卡片验证码（CVN 和 CVN2）、短信验证码、密码提示问题答案、手机客服密码、个人数字证书等				✓
		通信及互联网信息行为数据	在业务服务过程中用户的操作记录和行为数据，如网页浏览记录、Cookie、发布的社交信息、收藏列表等			✓	
		个人常用设备信息	包括可变更的唯一设备识别码（AndroidID/IDFA/IDFV/OAID 等）、不可变更的唯一设备识别码（IMEI、IMSI、MEID、VIN、设备 MAC 地址、硬件序列号、ICCID 等）				✓

数据分类（示例）				数据定级（示例）			
				一般数据			
数据类型	**二级子类**	**三级子类**	**数据内容**	**一般一级（DL1）**	**一般二级（DL2）**	**一般三级（DL3）**	**一般四级（DL4）**
业务数据		个人位置信息	能定位到行政区、县级等的粗略位置信息，如地区代码、城市代码等				✓
	车联网客户数据	客户车辆数据-配置数据	车辆型号、车辆颜色、底盘编号、控制器号、电池编号、变速箱号等		✓		
		客户车辆数据-标识数据	车架号、发动机号、车牌号			✓	
		车联网生活服务信息	车联网生活服务相关的内容信息，如广播服务等用户个人信息			✓	
		客户交通出行管理服务信息	信号灯信息推送、红绿灯车速引导、闯红灯预警、车辆信息动态交换采集、违法信息抓拍上报、停车诱导和管理、交通流量疏导、交通应急信息发布等服务中相关的用户个人信息			✓	
	车联网数据	车辆基础数据	车辆基础数据，软件开发商、类别、版本等车载及移动终端基础数据，平台开发商、运营商、平台操作系统、版本等车联网服务平台基础数据	✓			
		车辆工况数据	车辆在运行工况下的特征数据，如动力系统：驻车怠速、行车怠速、车辆起步、平缓加速、急加速等			✓	
		车联车控数据	智能决策车控类数据，如线控制动与驱动、线控转向、自动变速等相关的数据			✓	

数据分类（示例）				数据定级（示例）			
				一般数据			
数据类型	二级子类	三级子类	数据内容	一般一级（DL1）	一般二级（DL2）	一般三级（DL3）	一般四级（DL4）
业务数据		外部道路环境数据	外部道路情况、路面情况、道路限速情况、外部行人信息、外部车辆信息、路标信息、外界的通信信息等			✓	
		公共交通安全管理控制数据	公共交通安全管控类数据，如道路交通安全预警、信号灯信息推送、交通流量疏导、交通应急信息发布等相关的数据		✓		
		交通出行管理控制数据	交通出行管控类数据，如红绿灯车速引导、闯红灯预警、车辆信息动态交换采集、违法信息抓拍上报、停车诱导和管理等相关的数据			✓	
		车载应用服务数据	信息娱乐类使用记录数据，如天气预报、广播、网站浏览等相关的数据			✓	
	维保售后数据	车辆预检信息	服务项目、预检单号、预检单状态、故障现象、客户需求、来源渠道等		✓		
		车辆维修数据	类型、价格、配件数、配件费、预计交车时间、维修方案、渠道、里程、终检时间、维修工单号等			✓	
		车辆保养	保养里程、保养时间等			✓	
	客户维保数据	爱车养护数据	养护项目、频次、保养里程等			✓	
		爱车改装数据	改装位置、价格、次数等			✓	
		爱车维修数据	维修位置、维修地点、维修次数等			✓	

数据分类（示例）				数据定级（示例）			
				一般数据			
数据类型	二级子类	三级子类	数据内容	一般一级（DL1）	一般二级（DL2）	一般三级（DL3）	一般四级（DL4）
经营管理数据	战略规划数据	品牌战略规划数据	公司开展品牌管理活动有关文档等数据，如商业计划书、尽调问题报告				✓
	人力资源数据	招聘岗位数据	公司对外发布招聘岗位产生的信息，如招聘职位、招聘人数等	✓			
		应聘人员数据	应聘人员产生的信息，如简历、背景调查报告等			✓	
		档案管理数据	公司记录的员工档案信息数据，如人事档案、履历、员工岗级、征信报告、体检报告等				✓
		薪资数据	公司记录的员工薪资待遇数据，如工资、津贴、奖金、福利、定薪标准及薪资等级等				✓
	财务管理数据	税务管理信息	公司在税款形成、申报、缴纳等过程中产生的各类经营管理数据，如企业所得税季度申报表、企业所得税年度申报表、增值税及附加税费申报表等			✓	
	法律合规数据	法律事务数据	指涉及企业有关法律事务的数据，如合同签署、商务谈判、法律纠纷及诉讼事件处理情况、对外发送的公函等			✓	

数据分类（示例）				数据定级（示例）			
				一般数据			
数据类型	**二级子类**	**三级子类**	**数据内容**	**一般一级（DL1）**	**一般二级（DL2）**	**一般三级（DL3）**	**一般四级（DL4）**
经营管理数据	数字化运行数据	办公软件资源数据	指办公环境所需的基础软件和软件产品说明，如操作系统的安装包、升级包、硬件产品管理信息以及其相关说明文档等		✓		
	行政管理数据	章程制度文档	指企业为维护正常的工作秩序，依照法律、法令、政策而制定的具有规范性、指导性与约束力的章程制度电子文档数据，如公司章程、公司财务管理制度、公司资产管理制度、质量体系文件、信息安全体系文件、数据安全体系文件、个人隐私保护安全体系文件、采购体系文件、售后体系文件等		✓		

附录二：“重要数据”目录示例

重要数据梳理识别情况汇总表【示例】										
序号	数据名称	数据一级分类	数据二级分类	数据三级分类	数据四级分类	数据级别	数据载体	数据来源	敏感字段数据及规模	
									字段名称	数据量（单位：条）
1【示例】	购车客户信息表	业务数据	客户个人信息	个人基本信息	/	重要数据	数据库	购车营销系统	车主姓名、手机号、电子邮箱	约 10 万条

参考文献

序号	参考
1	《中华人民共和国网络安全法》
2	《中华人民共和国数据安全法》
3	《中华人民共和国个人信息保护法》
4	《汽车数据安全管理若干规定》（试行）
5	《工业数据分类分级指南》（试行）
6	《数据管理能力成熟度评估模型》
7	《信息安全技术 数据安全能力成熟度模型》
8	《信息安全技术 个人信息安全规范》
9	《信息技术 大数据 数据分类指南》
10	《网络安全标准实践指南—网络数据分类分级指引》
11	《信息安全技术 重要数据识别指南》（征求意见稿）
12	《信息安全技术 网络数据分类分级要求》（征求意见稿）
13	《信息安全技术 汽车数据处理安全要求》
14	《信息安全技术 步态识别数据安全要求》
15	《智能网联汽车 数据通用要求》（征求意见稿）
16	《智能制造 工业数据 分类原则》
17	《智能网联汽车 自动驾驶数据记录系统》（征求意见稿）
18	《汽车整车信息安全技术要求》（征求意见稿）
19	《数据安全技术 数据分类分级规则》
20	《车联网信息服务 数据安全技术要求》
21	《车联网信息服务 用户个人信息保护要求》
22	数据分类分级、制定重要数据目录试点成果分享（5）—优秀案例：《重要数据识别规则》——网信上海 https://mp.weixin.qq.com/s/v7dkqdV0FVdzjcMwgqrVhw
23	《北京市高级别自动驾驶测试示范区数据分类分级白皮书》——北京市高级别自动驾驶示范区 https://mp.weixin.qq.com/s/qfYw_uE04MJq9snBvrcRLQ
24	《数据安全治理实践指南（3.0）》——数据安全推进计划 https://mp.weixin.qq.com/s?__biz=Mzg3NjY3MDE3MA==&mid=2247489899&idx=1&sn=a55e25c74d418de4e47ddbda9a4ccfa3&chksm=cf2fe4def8586dc8acfec094167b3fcefa44ab85af6b82987a145bdaa0f29340721003268126&scene=21&version=4.1.22.8031&platform=win&nwr_flag=1#wechat_redirect

25	《中国（上海）自由贸易试验区临港新片区数据跨境流动分类分级管理办法（试行）》 https://www.lingang.gov.cn/html/website/lg/index/government/file/1756018881550389249.html