30th ANNIVERSARY 1992 2022

大成 DENTONS

DENTONS CHINA

「大成 30 周年所庆文集」

智能网联汽车数据合规白皮书

大成律师事务所

课题主持人

余英杰

高级合伙人

地点：大成北京
专业领域：公司与并购、争议解决、银行与金融、资本市场

课题参与人

王哲宇

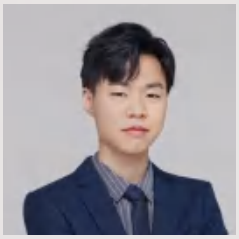
律师

地点：大成北京
专业领域：公司与并购、争议解决、银行与金融、资本市场

吕湛

律师

地点：大成北京
专业领域：公司与并购、争议解决、银行与金融、资本市场



童钰翔

公安部道路交通安全研究中心交通管理法规研究部干部

CONTENTS

引言 001

第一章 数据采集合规要求 003

（一）个人信息 005
（二）车辆运行数据 013
（三）数据采集风险及其合规方案 018

第二章 数据传输与存储合规要求 021

（一）车辆数据传输与存储概述 023
（二）车辆数据传输 023
（三）车辆数据存储 030

第三章 数据加工与使用合规要求 035

（一）数据加工与使用场景与安全措施 037
（二）数据与算法 039
（三）使用数据的特殊注意事项 041

第四章 数据提供与公开合规要求 043

（一）对第三方提供数据的一般要求 045
（二）接收数据的主体 049

附录 057

引言

智能网联汽车，也称自动驾驶汽车。根据工信部、国家标准化委员会《国家车联网产业标准体系建设指南（智能网联汽车）（2017 年）（征求意见稿）》的定义，“智能网联汽车是指搭载先进的车载传感器、控制器、执行器等装置，并融合现代通信与网络技术，实现车与 XX（人、车、路、云端等）智能信息交换、共享，具备复杂环境感知、智能决策、协同控制等功能，可实现‘安全、高效、舒适、节能’行驶，并最终可实现替代人来操作的新一代汽车。”

作为一种具有科技前沿性的交通工具，智能网联汽车已经在世界范围内展现出了广阔的发展前景和丰富的适用场景。在我国，随着智能网联汽车技术的日渐成熟和产业规模的不断扩大，智能网联汽车对于交通强国战略发展和智慧交通建设正发挥出越来越重要的作用。

目前，全国各地广泛开展智能网联汽车道路测试与示范应用，累计已有 40 余个城市开放了智能网联汽车测试与示范应用区域，开放路网超过 7000 公里，发放测试车辆超过 1400 台，测试里程超过 5000 万公里，智能网联汽车产业蓝海风起云涌，已有蓬勃发展之势。

从技术水平来看，L3、L4 级别智能网联汽车上路通行的能力正在日趋成熟，商业化场景也在不断增加。目前，智能网联汽车正式进入上路通行阶段的主要障碍还是来自于立法和监管层面对于新生技术产品的担忧。一方面，相关政策法规的出台和完善速度与智能网联汽车产业发展的进度仍有距离；另一方面，执法管理机关在面对人工智能产品大踏步进入道路交通这种关系公共利益且具有高度风险性的行业时，仍然存在心理上的疑虑和制度准备上的不足。这背后反映出的是智能网联汽车法律规范体系和合规管理体系的不健全。因此，完善智能网联汽车合规体系，建设好智能网联汽车产业法律合规护城河，已经成为行业发展共同的期盼。其中，数据安全无疑是智能网联汽车行业合规建设的重点领域。

智能网联汽车运行过程的本质是一个庞大的数据工程，自动驾驶系统做出的每一个逻辑决策和驾驶行为背后，都需要完成从数据采集、分析，到应用、存储的完整流程，其产生的庞大数据流，与个人隐私、商业秘密、公共利益和国家安全息息相关。可以说，数据是支撑智能网联汽车运行的血液，在车 – 路 – 云 – 网交错纵横的电子管道中一刻不停地奔涌。

智能网联汽车数据安全之所以成为合规体系建设重点领域。一是现有合规体系没有足够关注到智能网联汽车数据的特性。从载体上看，数据信息处理工具既有车载设备，也有路侧设备，既需要实体上的自动驾驶处理系统，也离不开云平台和云计算的贡献；从流程上看，智能网联汽车数据信息涵盖了从采集、处理到存储、删除完整的生命周期，突破了以往数据保护法对于不同数据处理环节之间的边界。因此，相比于一般意义上的数据信息，智能网联汽车数据具有复杂性、集成性、综合性的特点。二是没有建立起智能网联汽车数据安全合规体系。目前智能网联汽车数据保护方向的法律法规、标准并不统一，存在令出多门，各自为战的特点。相关合规要素尚不健全、合规指标尚不完善、合规体系尚不科学。这一情况极大地影响了智能网联汽车产业健康、有序、高速发展。

综上，我们认为，建立一个科学、完备、高效且具有前瞻性和现实指导意义的数据合规发展体系，不仅对于维护智能网联汽车数据安全具有特殊意义，更能够为智能网联汽车产业整体合规、安全发展提供重要支撑。

有鉴于此，本报告在充分考察智能网联汽车产业数据处理流程的基础上，根据现行法律法规和未来一个阶段智能网联汽车政策监管方向，综合全面梳理不同类型、不同阶段、不同环节的智能网联汽车数据处理要求和规范要点，作出具有高度独创性和适用性的合规及法律指引，并就法律层面的重难点环节和高风险事项集中做出合规分析。

特此声明，本报告仅为作者本人自身研究成果，不代表任何组织、机构对于相关政策法规、实践问题的解释或倾向性意见。本报告内容仅供一般性参考，不应视为针对特定事务的法律意见或建议且不应被依赖，不应作为据以做出或不做出法律或商业行为的依据。本报告作者不承担由于相关企业、单位和个人使用本报告或者依赖其任何信息而产生的任何损失。

第一章

数据采集合规要求

数据采集是智能网联汽车数据运行的初始环节、自动驾驶系统决策的前提条件，也是数据合规管理的起点。智能网联汽车数据采集，是指智能网联汽车及其生产、运营等主体，基于智能网联汽车运行和开展其他相关服务的需要，向特定主体、设备、场景等对象收集数据信息的行为。根据《个人信息保护法》《数据安全法》《汽车数据安全管理若干规定（试行）》等相关法律法规、规范性文件的要求，国家倡导数据处理者在数据收集活动中遵循默认不收集原则，即非经自主设定，每次驾驶时默认设定为不收集状态。本章将以列举形式明示智能网联汽车数据收集环节需要收集的主要数据信息，并对其合规要求予以提示。

一、个人信息

智能网联汽车个人信息数据，是指为实现智能网联汽车功能，以电子或者其他方式记录的具有可识别性的自然人信息。根据规范管理要求的不同和产业运行的实际情况，可以将个人信息分为内部人员信息和外部人员信息。

1. 内部人员信息

本节主要论述三部分内容，即内部人员信息采集的对象、范围、方式。

1.1 内部人员信息采集的对象

内部人员，指对于智能网联汽车运行过程具有一定管理、影响、控制能力或责任的自然人，此类人员往往与生产企业或运营主体存在雇佣、租赁、买卖等法律关系。为了实现智能网联汽车运行功能，需要对上述人员进行个人信息采集，并赋予其相应的权限。此类人员主要包括两类：

(1) 智能网联汽车驾驶人 / 安全员

智能网联汽车驾驶人 / 安全员，是指在道路上通行时对车辆具有实时监管、控制、接管义务，并在必要时承担驾驶义务的人员。对于此类人员的称谓，法律规范及行业惯例尚未形成统一，有驾驶人、安全员、车内安全员、乘用人等称呼，在此使用最具代表性的两种。

从驾驶逻辑来看，根据《道路交通安全法（修订建议稿草案）》《GB/T 40429-2021 汽车驾驶自动化分级》等相关法律法规、标准的精神，在有条件自动驾驶（L3）阶段，驾驶人 / 安全员仍需承担注意义务与接管义务，对于车辆具有控制权。因此，智能网联汽车驾驶人 / 安全员的个人信息在一定程度上与车辆驾驶、控制行为直接相关，同时属于智能网联汽车对当事人法律意义上所有权、使用权进行判断的基本数据。

(2) 智能网联汽车安全运行监控人员

智能网联汽车安全运行监控人员，是指智能网联汽车生产、运营企业依照法律法规和经营需要设立的，专门用于监控和维护智能网联汽车运行安全的人员，如智能网联汽车安全运行平台的车辆路况监控人员、远程安全员、调度员、安全运行管理人员等。此类人员一般负责对智能网联汽车总体运行安全进行监控、管理，在一定情况下对智能网联汽车也有暂停自动驾驶功能、远程接管等权限。

从法律关系来看，此类人员与智能网联汽车生产、运营企业一般存在劳动关系，且知晓并掌握相当程度的智能网联汽车运行数据及相关商业秘密，也属于数据安全管理的重点人员。

1.2 内部人员信息采集的范围

内部人员的个人信息采集范围包括：

类别	名称	内容
敏感个人信息	身份证明信息	如姓名、身份证号等可以用于对特定个人进行身份标识和鉴权的信息
	生物识别信息	面部识别、指纹识别等
	财产信息	银行账号、密码等金融支付工具信息
	驾驶行为信息	驾驶策略、驾驶偏好、接管选择、驾驶时的视频影像等
	行踪轨迹信息	行程起始地点、沿途路线、时长、速度、停靠地点等
	自动驾驶系统服务信息	自动驾驶系统开启的时间、状态、功能，自动驾驶决策行为等
	不满十四周岁未成年人的个人信息	不满十四周岁未成年人的身份信息、图像信息以及其他个人信息

类别	名称	内容
一般个人信息	身份信息	用户基本资料等信息
	非自动驾驶系统服务信息	购买、使用生活服务、出行服务及其他辅助性服务的相关信息等
	一般服务订购、订阅、交易信息	一般性服务的交易记录等
	其他个人信息	通讯录信息、信息网络服务衍生信息等

表 1.1

在特定情况下，此类信息经过处理、分析，能够直观或间接反映出个人信息主体的行踪轨迹、消费喜好、驾驶偏好、生活方式、行为习惯、社交圈、心理画像等与私人生活情事密切相关的信息。

1.3 内部人员信息采集的方式

人员类型	授权方式	采集方式
驾驶人	购买、租赁合同，注册成为智能网联汽车终端用户时的注册协议及其附件，购买或 OTA 升级服务时的协议及其附件等	(1) 车载摄录设备及其识别系统 (2) 车载安全设备及其识别系统 (3) 行程轨迹记录设备及车联网系统 (4) 驾驶行为记录设备及其分析系统 (5) 其他功能性服务的信息录入端口
安全员	劳动、劳务合同及其附件、保密协议，内部管理系统登记、注册协议及其附件，员工守则等内部纪律性文件	
安全运行监控人员		(1) 安全运行平台监控系统 (2) 控制决策及接管行为记录设备

表 1.2

2. 外部人员信息

本节主要论述四部分内容，即外部人员信息采集的对象、方式、内容。

2.1 外部人员信息采集的对象

(1) ROBOTAXI 场景下的乘客

根据《道路交通安全法（修订建议稿草案）》《智能网联汽车道路测试与示范应用管理规范（试行）》《交通运输部关于促进道路交通自动驾驶技术发展和应用的指导意见》等相关法律法规、规范性文件的要求，现阶段智能网联汽车上道路通行不能脱离主驾驶人和限定区域通行两项基本要求。因此 ROBOTAXI 将有很大可能是未来一段时间内智能网联汽车重要的商用化模式。ROBOTAXI 场景下的乘客，即通过应用程序或其他方法，接受智能网联出租车旅客运输服务的自然人。

(2) 其他交通参与人

为实现智能网联汽车自动驾驶功能，智能网联汽车车载雷达、摄像头，路侧感知设施和边缘计算单元等设备需要对同一交通环境下的道路交通参与者进行摄录、扫描、识别及数字化处理，从目前的图像采集精度来看，某些情况下被采集信息能够达到个人信息的标准。被采集方一般为同一时空环境下的社会车辆驾驶人、行人等主体。

2.2 外部人员信息采集的范围

(1) 为实现网约车、出租车服务所必需的个人信息采集

对于此类信息采集活动，可以参照现有网约车、出租车应用程序个人信息采集的规范要求，对乘客的联系方式、支付信息等内容进行采集。同时，在网约车、出租车服务的范围内记录乘客单次行程的路线轨迹。

(2)生物识别信息

为满足无人化场景下乘客上下车问题，在使用人脸识别、指纹识别等方式对乘客身份进行认证时，需要采集乘客的生物识别信息。

(3)特定时空条件下的行踪轨迹、行为举止及其数字化表达

特定时空条件，是指当交通活动参与人进入智能网联汽车车载雷达、摄像头或路侧感知设施的探测范围时，一方面其行动作为通行时周围道路环境情况的一部分被影像化方式摄录，用于为自动驾驶系统和智能网联汽车驾驶人提供参考，在一定情况下还将被上传至企业安全运行监控平台用于远程安全监督及评估；另一方面车路协同系统根据被采集者的行动轨迹和状态，将其以不可识别的数字化方式展现在自动驾驶系统当中(如骑自行车的人、行人等)。

2.3 外部人员信息采集的方式

对于 ROBOTAXI 场景下的乘客，可以在注册成为特定应用程序时的用户注册协议及其附件中明确采集的方式、内容和范围，并在实际开展服务的过程中以语音播报、文字推送等形式再次提醒被采集方正在进行个人信息采集。目前我国鲜有招手即停模式的无人化 ROBOTAXI 应用场景尝试，如果未来有此类 ROBOTAXI 模式投入运营，可以考虑在乘客上车后以醒目方式进行屏幕展示和语言播报相结合的方式披露信息采集的内容。

对于其他交通参与人，由于智能网联汽车示范应用道路同样属于公开道路，交通参与人有依法通行的自由，难以事先获得授权许可。但是，智能网联汽车及车联网相关主体可以在安装有路侧感知设施和边缘计算单元的道路入口设置显著的提示标识，以“您已进入信息采集区域”等内容对进入该路段的交通参与者进行提示和告知。

3. 合规要求

智能网联汽车个人信息数据采集的合规要求可以归纳为以下几点：

3.1 最小范围

根据《民法典》《个人信息保护法》《智能网联汽车道路测试与示范应用管理规范(试行)》《汽车数据安全管理若干规定(试行)》等法律法规及相关标准对于个人信息收集的要求，企业主体在收集上述信息时，应当限于实现处理目的的最小范围。范围的确定应基于下列明确且有必要的用途：

(1)保证智能网联汽车使用权及其他人身、财产性权利的行使；

(2)为订立、履行个人作为一方当事人的合同所必需，或者按照依法制定的劳动规章制度和依法签订的集体合同实施人力资源管理所必需；

(3)保障安全驾驶、保护自然人在紧急情况下的生命健康和财产安全、保障及改进包括自动驾驶在内的智能网联汽车各项功能；

(4)进行交通事故、交通违法行为、自动驾驶功能故障、信息网络安全问题等安全事件调查、鉴定；

(5)依法律、行政法规的要求或依行政命令向有权机关提供；

(6)其他履行法定职责、法定义务或实现相关服务功能所必需。

3.2 明确告知

数据处理者应当向个人信息主体明确告知个人信息采集的有关事项，具体要求主要包括以下两个方面：

(1)告知方式

数据处理者应当以显著方式、清晰易懂的语言向个人信息主体告知个人信息采集相关事项。在告知标准上应当满足真实、准确、完整三项要求。即：一是告知内容符合信息采集的实际情况。二是按照一般理性人标准，告知事项能够使被告知人充分理解自身可能被采集的个人信息。三是除法律规定可以不告知的事项外，应当将个人信息采集事项客观、完整、清楚地向被告知人展示。如果受条件限制无法在初次告知时提供完整的告知内容，则可在告知必要事项后提供查询完整内容的方式，并保证该方式的有效和畅通。

(2)告知内容

告知内容包括：

种类	具体内容
个人信息采集的目的与必要性	以列举方式明示被采集个人信息的应用场景，及被采集信息在实现特定功能或服务时确有必要
个人信息采集的方式	收集各类个人信息的具体场景
个人信息采集的种类与规模	车辆行踪轨迹、驾驶习惯、音频、视频、图像和生物识别特征等
停止收集的方式和途径	停止收集的方式和途径，以及个人信息主体要求停止收集的后果
个人信息处理与保存	处理各类个人信息的目的、用途、方式和个人信息保存地点、保存期限，或者确定保存地点、保存期限的规则
查阅、复制与提供	查阅、复制个人信息以及删除车内、请求删除已经提供给车外的个人信息的方式和途径
联系方式与权利救济	数据处理者及其用户权益事务联系人的名称或者姓名、联系方式等重要事项

表 1.3

3.3 知情同意

在个人信息采集活动开始前，数据处理者应当取得个人信息主体的知情与同意。一是对于知情权与同意权的保障。法律法规规定可以在充分保障知情权的基础上默示同意的，个人信息采集方应当充分告知个人信息主体相关信息；法律法规规定基于个人同意处理个人信息的，该同意应当由个人在充分知情的前提下自愿、明确作出；法律法规规定应当取得个人单独同意或者书面同意的，还应取得相应的同意。二是同意的重新取得，个人信息采集方式、范围、内容等事项发生实质性变更的，应重新告知并取得个人信息主体的同意。三是同意的撤回与撤销。个人信息主体有权以直接方式撤回或撤销对于个人信息采集的同意，数据处理者应提供撤销同意、注销账号、接受并处理投诉等服务。个人信息主体撤销同意的，个人信息采集方不得以此影响或停止与该项个人信息采集事项无关的其他服务。同时，数据处理者应严格遵守默认不收集原则，在个人信息主体未明示开启收集设备或功能时，不进行信息收集活动。

3.4 分级管理

在个人信息采集过程中，宜采用分级管理原则，针对不同敏感程度和重要程度的个人信息，采取不同的同意、授权、采集标准。

3.5 限定精度

在进行信息采集时，个人信息采集方应严格限制于为完成相应功能或提供相应服务所必需之范围。对于非必须识别的个人信息，可以采取模糊化或者不可识别方式采集个人信息。此外，路侧感知设施和边缘计算单元属于《个人信息保护法》规定的“在公共场所安装图像采集、个人身份识别设备”。一般除了用于支持智能网联汽车自动驾驶和车路协同服务外，还用于改善交通环境、科学管控车流等智慧交通建设之用途。对于此类设备是否属于《个人信息保护法》规定的“维护公共安全所必需”，应当根据实际情况具体判断。实践中也存在执法机关通过智能网联汽车摄录的通行时周围环境影像确定交通行政违法车辆车牌号和行为人的案例，表明车载摄像头摄录精度已经达到相当程度。因此，如果完成车路协同功能无需精确到个人身份识别，则可以主动调整精度范围，进行匿名化处理，包括删除含有能够识别自然人的画面，或者对画面中的人脸信息等进行局部轮廓化处理等，使所采集图像不能或自功能完成时起不能用于个人身份识别活动。

3.6 风险评估

如个人信息采集方收集的个人信息所涉及个人信息主体超过 10 万人。则属于《汽车数据安全管理若干规定（试行）》规定的“重要数据”，应当按要求进行风险评估，并向有关部门进行报告。

二、车辆运行数据

智能网联汽车车辆运行数据，是指在智能网联汽车设计、生产、测试、销售、使用、运维等过程中产生的与智能网联汽车运行功能有关的各类数据信息。主要包括智能网联汽车运行数据和智能网联汽车车外采集数据。

1. 智能网联汽车运行数据

从数据合规的角度来看，智能网联汽车运行数据主要可以分为两类，第一类是机动车相关信息，是指以电子化形式呈现的机动车各类运行参数、车辆与系统基本信息等等，如车辆运行日志、安全日志、发动机号、车辆识别代码（VIN 码）、唯一设备识别码（IMEI）、各类设备的 MAC 地址、通过温压、车速、轴转速等传感器获取的数据信息等等。在内容上可以参考一般机动车的信息种类和内容。

第二类是自动驾驶系统运行数据，是指在自动驾驶系统运行过程中，系统根据自身程序或人工智能运算逻辑做出判断、决策、指令等行为的程序语言，在特定程序语言的支撑下，自动驾驶系统能够控制智能网联汽车做出诸如加减速、停车避让、急转弯、借道超车、预警、接管提示等等驾驶行为，并且形成虚拟驾驶人的整体驾驶策略和驾驶风格。自动驾驶系统运行数据是智能网联汽车生产企业、自动驾驶系统提供商等主体的关键应用技术，往往涉及到大量知识产权和商业秘密，属于智能网联汽车数据保护的重点对象。

2. 车外采集数据

通过各类设备对外部环境信息此类数据主要可以分为两类：一是静态信息，即智能网联汽车周围及整体运行环境中相对静止的信息，如地图、地理信息中的地形地貌、街道、树木、建筑物、交通标志标线、信号灯、障碍物等内容。二是动态信息，即智能网联汽车周围及整体运行环境处于不断变化的状态，需要实时掌握并更新的信息。如车辆行驶路线、其他交通参与者的行踪轨迹、运行运动状况、人车流量、应急信息、汽车充电网的运行情况、气候与环境条件等内容。

3. 规范要求

对于智能网联汽车运行数据的规范要求，可以分为地理信息采集要求、重要数据采集要求、知识产权及商业秘密保护要求三类。

3.1 地理信息采集要求

地理信息采集活动，可以分为测绘活动与非测绘活动。

名称	内容
非测绘活动	1、车载传感器以及智能网联汽车的制造、集成、销售
	2、对于现有基础测绘成果、导航电子地图的使用行为
测绘活动	1、智能网联汽车安装或集成了卫星导航定位接收模块、惯性测量单元、摄像头、激光雷达等传感器后，在运行、服务和道路测试过程中对车辆及周边道路设施空间坐标、影像、点云及其属性信息等测绘地理信息数据进行采集、存储、传输和处理的行为
	2、路侧感知设施和边缘计算单元对探测范围内的物理空间地理信息进行采集、存储、传输和处理的行为
	3、其他依照《测绘法》《数据安全法》等法律法规规定属于测绘行为的

表 2.3.1

由于测绘行业属于涉及国家安全和公共利益的特殊行业，我国目前对于从事测绘业务的企业采取了资格准入和分类管理机制：

(1) 内资企业

内资企业从事相关数据收集、存储、传输和处理业务的，应依法取得相应测绘资质，或委托具有相应测绘资质的单位开展相应测绘活动。

(2) 外商投资企业

外商投资企业从事相关数据收集、存储、传输和处理业务的，应委托具有相应测绘资质的单位开展相应测绘活动，由被委托的测绘资质单位承担收集、存储、传输和处理相关空间坐标、影像、点云及其属性信息等业务及提供地理信息服务与支持。

测绘资质，是指根据法律法规规定，国家对从事测绘活动的单位实行的测绘资质管理制度。从事测绘活动的单位应当根据法定条件和法定程序，向有权机关提出申请，并在相应的资质等级内从事测绘活动。

(3) 其他要求

此外，建设卫星导航定位基准站的，建设单位应当按照国家有关规定报国务院测绘地理信息主管部门或者省、自治区、直辖市人民政府测绘地理信息主管部门备案。

3.2 重要数据采集要求

根据《数据安全法》第二十一条的精神，国家根据数据在经济社会发展中的重要程度，以及一旦遭到不法侵害，对合法权益造成的危害程度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。《网络数据安全管理条例（征求意见稿）》对重要数据给出了更详细的解释，列举了未公开的政务数据、出口管制数据、国家经济运行数据、重点行业的生产运行数据、达到特定规模或精度的地理、基因等国家基础数据、基础设施的运行数据等六类数据，并设置了兜底条款。在智能网联汽车领域，根据《数据安全法》《网络安全法》《汽车数据安全管理若干规定（试行）》等相关法律法规规定，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，属于智能网联汽车数据中的重要数据，此类重要数据包括但不限于：

(1) 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；

(2) 车辆流量、物流状况、人员流动情况、交通工具使用情况等反映经济运行情况的数据；

(3) 汽车充电网的运行数据；

(4) 包含人脸信息、车牌信息等的车外视频、图像数据；

(5) 交通管制、公安机关道路执勤执法等与交通管理、治安管理、国家安全管理情况相关的数据；

(6) 基础设施数据，根据《公路水路关键信息基础设施安全保护管理办法（征求意见稿）》，国家开始认定公路相关的关键信息基础设施，车路协同过程中道路一侧的云计算平台、大型数据存储设施等关键网络设备的数据，均可能构成重要数据；

(7) 出口管制数据，根据《中国禁止出口限制出口技术目录》，智能网联汽车涉及的人工智能交互界面技术、语音合成技术、密码安全技术等相关的科学技术成果数据，对国家经济有重要影响而被限制出口；

(8) 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。

采集重要数据的信息采集主体在采集相关数据前，应当按照规定开展风险评估，并向省、自治区、直辖市网信部门和有关部门报送风险评估报告。风险评估报告应当包括处理的重要数据的种类、数量、范围、保存地点与期限、使用方式，开展数据处理活动情况以及是否向第三方提供，面临的数据安全风险及其应对措施等。

重要数据的信息采集主体在采集相关数据时，要注意以下合规要点：一是完善备案许可等行政程序。根据《网络数据安全管理条例（征求意见稿）》第二十九条，车企在识别重要数据后十五个工作日内，应当向监管部门汇报处理重要数据的目的、规模、方式、范围、类型等。因此，建议车企在经营过程中，统计人脸信息、车牌信息、车流信息等重要数据处理情况，以便日后识别重要数据并满足监管要求。具体程序与采集对象、采集主体和智能网联汽车通行性质及其所处阶段、智能网联汽车上道路通行的地区等条件密切相关，在道路测试、示范应用、试点准入及上路通行阶段均有不同的管理要求，应当根据实际情况予以区分。二是严格限制采集范围和精度。信息采集者应根据所提供功能服务对数据精度的要求确定摄像头、雷达等的覆盖范围、分辨率，可以在采集时就进行模糊化处理，并避免通过车联网、互联网进行信息处理。三是切实遵守保护国家安全及公共利益。对于涉及国家安全和公共利益的信息，建议建立数据安全清单，对测绘过程中可能涉及到国家安全和公共利益的区域、信息流予以排除。如不慎在测绘或智能网联汽车运行过程中采集到相关信息，应当及时将相关情况向有关部门进行报告，并在最短时间内予以删除，同时将其加入数据安全保护清单。避免将此类数据进行进一步处理、用于商业用途或向不特定多数人公开。

3.3 知识产权及商业秘密保护要求

(1) 准确界定商业秘密范围，建立信息采集商业秘密保护池

商业秘密，是指不为公众所知悉、具有商业价值并经权利人采取相应保密措施的技术信息、经营信息等商业信息。智能网联汽车运行数据中可能会包含大量的商业秘密，包括与技术有关的步骤、算法、数据、计算机程序及其有关文档等技术信息；与经营活动有关的创意、模式、计划、样本、客户信息、数据等经营信息；以及其他符合商业秘密性质的数据信息等。对于此类信息，应当事先建立商业秘密保护清单，并且能够以显著方式告知不特定多数人信息采集者所享有之权利，并建立高效的侵权响应机制。

(2) 有效实现技术与数据相分离

智能网联汽车车辆运行数据往往能够体现出特定的技术内涵和技术方法，因此信息采集主体在信息收集过程中应及时或尽快完成脱敏处理，使被采集数据在对外提供时不能反映出涉及知识产权和商业秘密的数据采集方法、技术、规则，或通过逆向工程还原数据采集过程。

三、数据采集风险及其合规方案

对于数据采集过程中可能存在的合规风险，本节予以列举并进行重点提示。

1. 侵犯被采集方权益的采集行为

侵犯被采集方权益的采集行为，是指在数据采集过程中违反与被采集方之间的采集协议，或者以侵犯被采集方合法权益、国家利益、公共利益的方式进行的数据采集，此类采集行为除了属于侵犯信息主体和公共利益的侵权行为外，还可能属于违反信息采集协议的违约行为。主要的侵权类型包括以下三类：

1.1 无权采集

指信息采集方无采集权而采集信息数据的行为。典型的有：

(1) 未获得个人信息主体同意或在个人信息主体不知情的情况下采集个人信息；

(2) 未取得个人信息主体单独同意或未依法取得个人信息主体书面同意而采集个人敏感信息的；

(3) 没有资质而进行的地理信息测绘；

(4) 没有按照规定提交风险评估报告，并取得特定行政许可而采集重要数据的；

(5) 其他没有数据采集权而进行的数据采集行为。

1.2 越权采集

是指信息采集方超越约定或法定的权限而进行的数据信息采集行为。主要包括：

(1) 超越合同约定信息采集精度、范围、内容等而进行的信息采集；

(2) 超出提示和告知被采集方的信息采集范围而进行的信息采集；

(3) 超出 ODD 限制、驾驶自动化级别要求及其他智能网联汽车相关标准而进行的信息采集；

(4) 超出智能网联汽车测试、示范应用、试点准入、上路通行的区域或范围等限制而进行的信息采集；

(5) 过度采集行为，即超越实现特定目的所必需而进行的数据采集行为；

(6) 其他超过约定、法律法规等的授权或允许而采集信息数据的行为。

2 缺陷性采集

指因技术故障、设计缺陷等原因导致被采集数据信息不符合要求的情形。此类采集行为本身可能并不侵犯被采集方的信息权、隐私权等合法权益，但可能因其采集的数据存在缺陷，从而影响智能网联汽车相关功能和服务的正常运行、开展，进而危及被采集方和其他主体的人身、财产安全和公共安全。缺陷性采集主要包括以下两类：

2.1 错误采集

错误采集，是指由于信息采集设备采集的数据信息出现错误，从而导致与实际情况不一致的情形。如将正在行驶的车辆识别为静止的障碍物；将行人识别为动物；对于前车距离、车速、车道等要素的识别出现明显错误等。

2.2 采集失败

采集失败，指信息采集方因各种原因导致相关设备无法进行信息采集，或无法提供有效数据信息的情形。如无法识别障碍物、车辆、行人等交通环境要素；未能识别出正在执勤执法的交警及其指令、手势；无法识别驾驶人的驾驶状态；无法识别驾驶人、安全员、乘客等主体的身份等等情形。在自动驾驶上道路通行过程中，采集失败是一种具有高度危险性的安全事件，可能导致自动驾驶系统运行故障、产生交通违法行为、紧急状态下驾驶人无法进行接管，甚至发生交通事故等严重后果。

2.3 采集不符合条件

是指智能网联汽车数据信息采集设备采集到的数据不符合采集要求，不能支持智能网联汽车自动驾驶功能及其他相关服务的实现。如数据信息精度、广度不足，采集时间过久等情形。

由于自动驾驶系统的决策往往是在分析被采集信息的基础上做出的，因此此类错误具有极大的交通安全隐患。本节引用一起典型案例进行说明：

2018 年 3 月 18 日晚 10 点左右，Uber 公司的一辆自动驾驶汽车在美国亚利桑那州 Tempe 市发生交通事故，与一名过马路的行人相撞，导致该行人送医后不治身亡。事发时，尽管有一名司机坐在方向盘后面，但是，这辆车当时处于自动控制模式。根据美国国家公路交通安全管理局披露的调查报告，在 Uber 自动驾驶汽车发生车祸前 5.6 秒时车辆就已经检测到了行人，但是系统把她错误识别为汽车。在车祸前 5.2 秒，汽车的自动驾驶系统又把她归类为“其他”，认为她是不动的物体，并不妨碍车辆行驶。之后系统对物体的分类发生了混乱，在“汽车”和“其他”之间摇摆不定，浪费了大量宝贵的时间。车辆未能及时采取刹车措施，最终导致事故发生。

实践表明，智能网联汽车在诸如强光、黑暗等环境条件的作用下，对于数据信息的采集能力可能会有一定程度的减弱。同时，一些较为特殊的场景（如在高速公路上出现的低速行驶的作业车辆），可能超出了现有智能网联汽车信息采集和识别系统的设计验证场景及理解能力，从而导致智能网联汽车无法对其做出准确判断。目前，辅助自动驾驶汽车在国内外都出现了多起因对象识别错误而引起的交通事故。而在未来高级别智能网联汽车大规模上道路通行后，此类事件引起的法律责任和舆论影响存在进一步增加的风险，应当予以高度关注。

第二章

数据传输与存储合规要求

一、车辆数据传输与存储概述

智能网联汽车完成人物识别、地理定位、操作信息、人员监测等信息的采集后，需要对数据进行传输，实现车辆的正常运行。传输行为可分为车内传输与对外传输：车内传输是指，车辆通过车载以太网将采集、加工的数据，传输至车内的其他模块，以供进一步加工与使用；对外传输是指，汽车将数据传输给第三方主体，例如监管平台、仿真平台、安全平台、车路协同系统等，以满足车辆的运行需求。不同的传输方式，对应不同的合规条件。

此外，智能网联汽车接收到采集的数据或传输的数据后，亦需对其进行存储，从技术角度来看，现有技术条件难以也没有必要对智能网联汽车运行过程中产生的海量数据进行完整存储，因此分级化、阶梯化的数据存储机制势在必行。根据存储方式的不同，数据存储可分为本地存储与线上存储两种方式。本地通常会存储实现智能网联汽车各项功能所需要的数据，并基于数据向各个组件发布行动指令。线上存储，则涉及对数据的对外传输，各个平台基于自身的需要，存储相应的数据；或者车辆收集的数据，本身就是第三方于云端存储的数据，例如车辆调取的地图数据，本身存储于地图商的云平台或服务器上，车辆仅存储其所需要的部分道路数据。前述不同的数据存储方式、存储主体与应用场景，会面对不同的监管要求。

二、车辆数据传输

1. 车辆数据传输的基本流程

智能网联汽车进行车内数据传输时，有两种数据传输方式，分别为“端到端”传输与“模块化”传输。端到端式传输是指数据传感器采集到数据后直接加工，将数据与指令直接传输到控制系统，但这种方式缺少可靠的安全措施和可解释性，对于在开放环境中实现自动驾驶的可行性还有待验证。模块化传输是指车辆的驾驶系统包含感知、决策和控制三个主要功能模块，数据按照感知 – 决策 – 控制的顺序进行传输。模块化传输的优势在于，算法可解释性较强，且功能区划分清晰，能够较好地实现功能之间的统筹协作，[1] 是目前主流的传输方式，与智能网联车数据的加工、使用方式相辅相成。

进行车外数据传输时，车辆数据会按照特定频率向接收方传输，具体的传输时间节点、方式，不同的车企采用方式有所不同。传输数据的类型、接收数据的主体等因素，通常取决于智能网联车辆所需的功能。常见的情形如表 3.1 所示：[2]

[1] 张燕咏、张莎等：《基于多模态融合的自动驾驶感知及计算》，载《计算机研究与发展》2020 年 57(9)，第 1783–1784 页。

[2] 参考了中国信息通信研究院：《车联网白皮书（网联自动驾驶分册）》，第 11 页。

数据类型	拟实现功能	接收方
车辆与车辆、行人的随身智能设备、基站等之间的交互数据	从宏观上规划车辆路线，降低事故发生率，缓解拥堵	V2X 云平台
车辆运行数据、地理数据、实时交通情况等数据	从源头识别违法或问题车辆，保障交通安全	监管云平台
位置数据、轨迹数据、始发地 / 目的地、路线需求等数据	结合云平台的高精地图，帮助车辆规划行驶路线	地图商云平台
车辆运行数据、系统日志、操作记录等数据	通过云平台分析各车辆的问题，进行远程系统升级	TSP 云平台 [3]
车辆运行数据、系统数据、对外交互数据等数据	实时监测车辆网络数据的安全风险，保障网络数据安全	数据安全监测平台
传感器识别数据、行驶数据、决策数据、运行数据等一系列车辆驾驶过程中产生的数据	帮助车企训练自动驾驶所需的算法模型，包括人物识别、路线规划等	算法云平台
	构建、优化仿真平台，线上模拟真实环境，加快算法模型训练速度	仿真平台

表 3.1

2. 车辆数据传输的法律性质

结合上文，不同形式下的数据传输，在数据类型、接收主体、传输方式等要素皆有差异，与之相应的法律性质也有所不同，下进行简要分析。

[3] 从实践来看，TSP 平台可能是车企自主研发的，这种情况下便不构成对外传输；也可能是车企对外采购自动驾驶系统，车企负责生成车辆部件，搭载外部厂商的自动驾驶系统，这种情况下便构成对外传输。

2.1 车内传输

《汽车数据安全管理若干规定（试行）》第六条规定，国家鼓励汽车数据依法合理有效利用，倡导汽车数据处理者在开展汽车数据处理活动中坚持车内处理原则，除非确有必要不向车外提供。

进行车内数据传输时，感知模块采集数据后，对其进行初步加工，并将之传输至决策模块；决策模块将各方面数据进行融合，通过深度学习等算法，得出方向、车速、提醒等决策，下发到控制模块；控制模块根据收到的决策，控制车辆各部件进行驾驶，产生车辆的状态数据并反馈至决策模块。

以上车内数据传输均在车辆内部完成，形成了闭环。因此，车内传输数据符合汽车数据的车内处理原则，属于一般的数据处理行为，汽车数据处理者照常履行采集合规、安全保护等基本义务后，即可进行车内数据传输。

2.2 车外传输

车外数据传输不属于《汽车数据安全管理若干规定（试行）》第六条规定的车内处理情形，需论证车外传输的必要性。此外，数据的接收方可能是车企本身运营的平台，也可能存在合作的第三方主体，如果存在第三方接收主体，则不再是一般的数据传输行为，可能构成“委托处理数据”、或“对外提供数据”，存在更为严格的合规要求。本部分仅探讨接收方为车企自身的情形，包括车企自行搭建运营核心算法平台、TSP 平台、安全监测平台的情况；关于向 V2X 平台、监管平台、地图商云平台等第三方传输数据的情形，在第四章中进行论述。

根据《数据安全法》的立法精神，在保护个人、组织合法权益，维护国家主权、安全和发展利益，保障数据安全的前提下，国家促进数据开发利用，允许数据的有序流动。

基于此，笔者认为，不涉及个人、企业合法权益或国家安全的数据，或者应当依法公开的数据，不适用车内处理数据原则。对于涉及自然人个人信息权益的个人信息、车辆数据涉及车企等相关企业数据竞争权益的车辆数据，以及涉及国家安全的关键类型数据，应当按照相关规定予以保护。对于此类数据，可以适用车内处理数据原则，如无必要不对外传输，但关于必要的认定，应当有所不同。具体请见下表 3.2：

数据类型	背后的法益	处理原则
个人信息	个人信息权益，保障自然人的生活安宁、人格尊严等	应当经个人授权
车辆经营数据	企业产品或服务竞争力的来源，能够为企业带来商业价值，促进市场有序竞争	应当经相关企业授权
重要数据、核心数据	实时监测车辆网络数据的安全风险，保障网络数据安全	应当履行法律法规要求的手续
其他数据	数据有序流动，提高社会的运行效率	无需经过授权

表 3.2

2.2.1 基本车况数据

《国务院办公厅关于促进二手车便利交易的若干意见》第三条提出，加快建立覆盖生产、销售、登记、检验、保养、维修、保险、报废等汽车全生命周期的信息体系。非保密、非隐私性信息应向社会开放，便于查询……将基本车况数据列为公开数据，以促进二手车交易公开透明。因此，车主购买、使用车辆的过程中产生的车辆里程、损耗程度等基本车况数据，经过脱敏后，如果仅能反映某一车辆的情况而无法识别到特定自然人，便可以依据市场规则，进行提供或公开。

司法实践中，余某发现可以通过某 APP 查询自己名下车辆的车况数据，将运营该 APP 的某信息科技企业告上法庭。广州互联网法院认为，基本车况数据经过脱敏后，降低了一般公众将车况数据与第三方信息结合重新识别特定自然人的可能性，不属于个人信息；将车况信息认定为个人隐私，亦不符合一般社会合理认知。[4]

综上所述，基本车况数据经过脱敏后，不构成个人信息，国家鼓励基本车况数据的自由流动。对于企业而言，有条件产生或处理基本车况数据的企业，可面向公众或者算法方、监管方等第三方提供脱敏后的车况数据；企业对基本车况数据进行分析、加工等深度处理后，法律上亦可作为具有数据资源竞争权益予以保护。企业自身同意对外传输后，便不存在法律障碍。举重以明轻，既然可以向公众提供相关数据，那么向车企自身运营的平台传输，自然也具有合法性。

[4] 广州互联网法院，余某诉北京酷车易美网络科技有限公司隐私权纠纷，(2021) 粤 0192 民初 928 号案民事判决书，最高人民法院发布全国法院系统 2021 年度优秀案例。

2.2.2 个人信息

《汽车采集数据处理安全指南》第四条，将车辆采集数据分为四类，分别是车外数据、座舱数据、运行数据与位置轨迹数据，并指出车外数据可能包含人脸、车牌等个人信息，座舱数据可能包含驾驶员和乘员的人脸、声纹、指纹、心律等敏感个人信息；第五条则规定了相关数据的传输原则，未经个人信息主体单独同意，汽车不应通过网络向外传输包含其个人信息的车外数据，且汽车不应通过网络向外传输座舱数据，除非存在例外情形。

以上规定，与《汽车数据安全管理若干规定（试行）》第六条规定的车内处理数据的原则，存在相似的内涵。因此，如果车企希望车外传输前述的座舱数据或者个人信息，应取得个人单独同意，或者将数据进行匿名化处理，从而实现在匿名的情况下监测车内信息，降低车外传输前述数据的合规成本。对于车外数据中的个人信息，实践中较难取得个人同意，匿名化处理成为较优的合规路径。

不过，《汽车数据安全管理若干规定（试行）》第六条也留下了“除非确有必要”的例外，但并未进行说明。《个人信息保护法》第十三条规定，为订立、履行个人作为一方当事人的合同所必需，或者为履行法定职责或者法定义务所必需，或者为应对突发公共卫生事件或紧急情况下为保护自然人的生命健康和财产安全所必需，个人信息处理者可以处理个人信息，而无需取得个人同意。前述的“合同所必需”、“法定所必需”、“紧急情况所必需”，可以作为取得个人同意的豁免，也可以作为“车内处理原则”的例外。

具体而言，《汽车采集数据处理安全指南》第 5.3 条规定了 5 种例外情形，笔者认为确与《个人信息保护法》第十三条规定的例外情形存在一定的对应关系，如下表 3.3：

	汽车采集数据处理安全指南	个人信息保护法	理由
1	为实现 5.1 所述匿名化处理功能，需要通过远程信息服务平台实时执行匿名化处理操作的情形，但应确保原始数据传输到平台后不用于其他目的，并在匿名化处理后得到删除	法定所必需	采取必要措施保障个人信息安全
2	为实现语音识别等直接服务于驾驶人或乘员的功能，需要通过远程信息服务平台实时配合处理座舱数据的情形，但应征得驾驶人同意授权，且确保功能实现后即时删除原始数据及处理结果。	合同所必需	履行语音识别等网络服务合同的义务
3	为实现用户远程监控车内外情况、使用云盘存储用户数据等直接服务于用户的功能，需要通过网络向用户终端设备传输数据或使用远程信息服务平台存储数据的情形，但应在传输以及存储时采取加密等措施，确保用户数据只能由用户终端设备访问，在其他设备以及远程信息服务平台上无法访问	合同所必需	履行远程控制、云盘存储等网络服务合同的义务
4	道路运输车辆、运营车辆依据相关行政管理要求向外传输座舱数据的情形	法定所必需	遵守监管机构的要求
5	道路交通事故发生后按执法部门要求向外传输数据的情形	法定所必需	履行道路安全相关的法定义务

表 3.3

除了《汽车采集数据处理安全指南》第 5.3 条规定的例外情形之外，实践中车辆向车企搭建运营的数据安全监测平台、算法云平台、TSP 云平台等平台传输数据时，同样可以参照适用上述的规则。笔者认为存在下表 3.4 的适用关系：

数据处理者	个人信息保护法	理由
算法云平台	合同所必需	提供车辆行驶的算法服务，决定了车辆如何行驶，履行技术服务合同的义务
TSP 云平台	合同所必需 法定所必需	提供系统升级、更新维护等服务，履行技术服务合同的义务，以及远程更新安全补丁等网络安全的法定义务
数据安全监测平台	法定所必需	履行《网络安全法》《个人信息保护法》等法律要求的数据安全保护义务

表 3.4

综上所述，车外传输个人信息有三种合规路径，其一是将个人信息进行《个人信息保护法》第四条规定的匿名化处理，使之不成为个人信息，降低数据传输的风险；其二是通过购车协议、车载系统协议等方式，取得车主对数据车外传输的同意，满足个人信息车外传输的合规要求；其三是援引《个人信息保护法》第十三条、《汽车采集数据处理安全指南》第 5.3 条等法律规范的豁免条款，使车企无需取得个人同意。

但是，司法实践中对合同所必需等豁免规则与取得个人同意之间的关系，存在不同认识，杭州互联网法院在（2021）浙 0192 民初 8058 号案中认为，合同所必需可用于论证个人信息处理的必要性，规避了与同意之间关系的论证；[5] 杭州互联网法院又在（2021）浙 01 民终 12780 号案中认为，合同所必需等豁免可认定为法定许可的情形，具有合法性基础，不属于违法处理行为。[6]《汽车采集数据处理安全指南》第 5.3 条虽然规定了座舱数据对外传输的例外情形，却并未说明例外情形下是否还需要履行第 5.1 条规定的个人同意。

因此，建议车企对第二条、第三条路径作好充足的合规准备，既通过挂网协议取得用户的同意，再做好数据处理必要性的论证与相关评估，降低可能存在的法律风险。

[5] 杭州互联网法院：黄某某诉某信用管理有限公司个人信息保护纠纷案，（2021）浙 0192 民初 8058 号民事判决书，杭州互联网法院发布个人信息保护十大典型案例之六。

[6] 浙江杭州市中院：吴某某诉上海某信息服务有限公司等违规提供用户个人信息保护纠纷案，（2021）浙 01 民终 12780 号民事裁定书，杭州互联网法院发布个人信息保护十大典型案例之七。

3. 车辆数据传输安全

对于智能网联汽车而言，数据传输是车辆驾驶安全的重点保障环节。数据传输过程中有两类常见的安全风险，分别是传输节点攻击风险与传输通信攻击风险。传输节点攻击中，攻击者会攻击车辆内部节点、云平台节点或者道路设施节点，篡改其中的数据，使车辆接收到的数据失真，从而使车辆的决策模块下达错误的指令，导致交通事故等安全事件的发生；传输通信攻击中，攻击者会直接攻击信道，使数据传输阻塞或瘫痪，使车辆驾驶功能失灵，或者直接截取传输的数据，造成数据泄露等风险。[7] 因此，车企应当重视车辆数据传输安全，依法采取保护措施。

智能网联汽车数据传输的过程中，涉及个人信息、重要数据、车辆基本信息、运行数据等各类数据，特别是车内传输的过程中，各模块会先汇聚、加工各类数据，再向下一个模块传输，情况非常复杂。所以本文不对具体的情形进行分析，而是把握数据传输合规的三个方向，分别是先加密后传输，一方面降低被攻击后数据泄露的风险，另一方面对数据特别是个人信息脱敏后，获取处理的权限；对各节点进行身份认证，并严格限制各主体的数据权限，确保数据管理过程的安全与事后留痕；根据《数据安全法》《网络数据安全管理条例（征求意见稿）》等法律规定，按照网络安全等级制度的要求，依法采取技术手段保障节点与通道的安全。

三、车辆数据存储

使用智能网联汽车产生的数据量非常惊人，正常使用的情况下，即便只保留必要数据，也难以单纯依靠车辆本地进行存储，必须通过服务器、云平台等车外方式进行存储。

除了数据量较大之外，智能网联汽车发生故障或事故后，数据是判断各方权责的重要依据，仅依靠本地存储，事故发生时相关的存储部件一旦被破坏，就会导致重要证据的灭失。如果同时采用车外存储的方式，则更有利于证据固定和证据保留。

因此，与一般的互联网企业不同，智能网联汽车生产、运营企业需要比一般的互联网企业更加关注何如按期存储数据，使其不被后续数据覆盖或者因为事故原因销毁，且同时能满足监管要求。

[7] 工信部网络安全产业发展中心编写组：《数据传输安全白皮书》，第 30–31 页。

1. 车辆本地存储 [8]

本地存储的期限或要求，应当满足事故风险排除及事故数据还原两项要求。《自动驾驶汽车运输安全服务指南（试行）（征求意见稿）》第八条第四款规定，在车辆发生事故或自动驾驶功能失效时，自动记录和存储事发前至少 90 秒至事发后至少 30 秒的运行状态信息。运行状态信息至少包括：车辆基本信息、控制模式变化情况、接收的远程控制指令情况、运行状态、人机交互及车内外影像情况等。如果仅依靠车辆各部件与车载系统进行存储，发生严重事故时，相关硬件可能已经被破坏，无法从中提取相关数据。

因此，此类数据的存储，一方面需要车外存储予以补充，另一方面也可以采用市面上已经产生的“车载黑匣子”产品，以抗冲击抗高温且不联网的形态存储数据，为事故提供数据相关的证据支持，也可以作为线上数据的校对工具。

2. 车外存储

数据的存储同样属于数据处理活动，受到《汽车数据安全管理若干规定（试行）》第六条规定的车内处理数据原则的约束，因此需要对车外存储数据的必要性进行论证。

2.1 车外存储概述的限制

基于车内处理数据的原则，如果没有必要，数据不能在车外存储。但是为了实现远程系统更新、驾驶算法训练等功能，智能网联汽车借助于车外的服务器与云端进行数据存储通常是难以避免的。因此，《汽车采集数据处理安全指南》第六条对车外数据存储的情形进行了特别规定，以满足车外存储需求。

从实践看，北京顺义自动驾驶示范区将数据分为 5 个等级，其中 DL1 级没有对应的数据安全保障等级措施，只有 DL2 级以上的数据，才会有存储期限、存储加密措施、存储访问权限等限制。DL1 级的数据包括车辆基础信息、道路设施基础信息、云平台的基础信息、基础的统计数据以及餐饮、住宿等周边服务信息等，被他人获悉不会对个人或企业的利益造成损害。[9] 因此，对于此类数据的车外存储，一方面节省车辆内部数据的存储空间，另一方面也不会对他人合法权益造成损害，不会限制其车外存储。

对于其他可能对他人合法权益造成影响的数据，《汽车采集数据处理安全指南》第 6.1 条规定，车外数据、位置轨迹数据在远程信息服务平台等车外位置中保存时间均不应超过 14 天。由此可知，对于车外采集获取的数据、位置轨迹数据等敏感的、涉及他人权益的数据，车外存储会对存储时间有所限制，但并未完全予以禁止。除了为车外存储数据留下了空间与限制之外，《汽车采集数据处理安全指南》第 6.2 条进一步对前述限制的 5 种豁免情形进行了说明：

[8] 车企在采集数据过程中履行了法律对个人信息、重要数据的义务后，便可依法在车内存储数据，不存在额外的合规障碍，不再赘述。
[9] 《北京市高级别自动驾驶示范区数据分类分级白皮书》第 19–21 页、第 28–32 页。

a) 为优化行驶安全功能而存储的特定场景数据，但每车每天不应超过 3 个连续时间的数据片段，每个片段不应超过 2 分钟。

b) 符合 5.3 c) 要求，用户传输到远程信息服务平台的数据。[10]

c) 由采集训练数据的专用采集车辆或在特定区域行驶的专用测试车辆采集的数据，但车辆外部应有“测试车辆”或“数据采集车辆”及所属单位的显著标识，且驾驶人员为具备授权的特定人员。

d) 新能源汽车、道路运输车辆、网络预约出租汽车依据相关行政管理要求进行存储的数据。

e) 用于生产经营的汽车产生的，生产经营者可控的位置轨迹数据。

从上述规定可以看出，a）项、c）项与 e）项均涉及车辆行驶时所采集的数据，其中 a）项涉及用户驾驶车辆直接行驶获取的数据，因此对数据的存储方式进行了限制，防止车企获取用户完整的轨迹信息；c）项与 e）项则是车企自有训练车辆或者用于生产经营等非生活场景的车辆，不涉及用户的个人信息权益（其中 c 项中驾驶人员依然要给予特别授权），因此给予了车外存储的豁免。训练车辆或非生活用车采集、产生的数据，对于自动驾驶算法模型的构建起到至关重要的作用，对其进行车外存储以便后续进行加工使用，是提供智能网联汽车产品与相关服务所必需的，因此可以给予车外存储的豁免。

关于 b）项的豁免，则是实践中自然人用户常见的使用需求，即通过手机等终端设备远程操纵汽车，例如冬天提前开启空调热车、远程访问车辆信息用以规划行程等，车外存储数据是实现前述功能的前提，因此也能取得车外处理数据的豁免；d）项则是行政管理所需的数据存储，为确保法律规范之间不相互冲突，需要提供车外存储的相应豁免，监管机构进行行政管理有法可依。

综上所述，目前车外存储的业内与监管思路将数据分为三类，第一类是可以自动流动，甚至本身就是公开的数据，无需界定是否车外存储；第二类是需要限制车外存储的数据，会涉及自然人的个人信息权益；第三类则是不涉及自然人生活，为生产经营过程中产生的数据，不受第二类数据存储的相关限制。

[10] 《汽车采集数据处理安全指南》第 5.3 条规定，满足以下条件的，可作为上述条款（汽车不应通过网络向外传输座舱数据）例外情形：c) 为实现用户远程监控车内外情况、使用云盘存储用户数据等直接服务于用户的功能，需要通过网络向用户终端设备传输数据或使用远程信息服务平台存储数据的情形，但应在传输以及存储时采取加密等措施，确保用户数据只能由用户终端设备访问，在其他设备以及远程信息服务平台上无法访问。

2.2 车外存储与委托处理

智能网联汽车产生的数据量极大，生产、运营企业在实际运行过程中可能需要向第三方租用服务器或者采购云存储服务。与向第三方平台提供数据不同，在租用存储服务开展的过程中，第三方仅提供相应的软硬件技术服务，具体的数据调用、删除等行为由生产、运营企业决定，生产、运营企业通过相关的账号下达指令，第三方通过技术手段执行。这种情况下，第三方处理数据的过程中不包含自身的意志，完全是在执行生产、运营企业的指令，不具备共同处理数据、对第三方提供数据的特征，也不满足《个人信息保护法》第七十三条对个人信息处理者“自主决定”的要求，在法律性质上具有委托处理数据的特征。此外，根据《民法典》第二十章第四节的表述，技术服务合同法律关系双方，分别为“委托方”与“受托方”，也可以侧面证明车企租用存储服务的情形下，双方构成委托处理数据的法律关系。因此，提供存储服务的第三方本身无需取得采集数据相应的授权，但应当履行作为委托处理方的相关义务。

不同类型的数据在进行委托处理时，存在不同的合规要求。就个人信息而言，根据《个人信息保护法》第二十一条、第五十五条的规定，在租用存储服务之前，车企应当评估个人信息存储的必要性与风险；签订协议时，车企应当与存储服务商约定好存储的目的、期限、方式、存储个人信息的类型以及保护措施，明确双方的权利义务，并且车企应当监督第三方的存储活动，以保障个人信息的安全，并做好相应的记录。

就重要数据而言，如果车企需要在第三方处存储人脸、车流、十万人以上个人信息等重要数据，根据《网络数据安全管理条例（征求意见稿）》第十二条、第三十二至三十三条，车企租用存储服务之前，应当征得市级以上监管部门的同意，并且应当对下列事项进行安全评估，如果经评估认为可能危害国家安全、经济发展和公共利益，不得租赁存储服务来存储重要数据：

（一）租赁存储服务以及存储数据的目的、方式、范围等是否合法、正当、必要；

（二）数据被泄露、毁损、篡改、滥用的风险，以及对国家安全、经济发展、公共利益带来的风险；

（三）合同中关于数据安全的要求，能否有效约束出租方履行数据安全保护义务；

（四）存储数据过程中出租方提供的管理和技术措施等，是否能够防范数据泄露、毁损等风险。

因此，生产、运营企业应当先行论证租赁存储服务的必要性，例如云端存储有利于算法升级等。在与第三方签署协议时，一是要注意与受托方约定存储数据的目的、范围、存储方式，数据安全保护措施等，评估对方的数据安全保护水平与数据的重要程度是否匹配；二是明确双方的数据安全责任义务与违约责任，确保对方能够依约履行合同；三是要充分监督受托方的存储行为，以免受托方滥用合同权利进行数据处理活动。

上述的审批记录、相关日志记录，车企应当保存至少 5 年。同时，应当自行或者委托数据安全服务机构每年开展一次数据安全评估，形成包含上述内容的评估报告，并在每年 1 月 31 日前将上一年度数据安全评估报告报设区的市级网信部门。前述的相关文件，最终将作为监管机构执法与车企申辩的依据，应予以高度关注。

第三章

数据加工与使用合规要求

加工、使用数据是智能网联汽车智能性的来源，基于加工、使用数据而进行的智能决策包括但不限于识别物体、规划路线、指令下达等。加工与使用数据的合法性来源，以及车内与车外处理的合规要点，与采集、传输、存储等数据处理行为一致，本部分不再赘述；另外，关于车载系统或软件加工、使用个人信息的问题，与网站、互联网 APP 加工、使用个人信息没有本质区别，本部分也不再详细阐释。本部分将就智能网联汽车独特的加工、使用数据的情形与合规要点进行论述。

一、数据加工与使用场景与安全措施

与日常生活中的移动终端相比，智能网联汽车加工、使用数据的方式有较大的差异，需要针对其特性进行合规分析，并采取相应合规措施。

1. 数据加工与使用的场景

智能网联汽车先通过激光雷达、摄像头、相关数据接口等渠道，从外部采集人员车辆、路况、地理位置等数据。随后感知模块汇聚前述数据来识别、了解车辆与周围环境的基本情况，例如聚合地理位置信息、摄像头数据、车辆基本信息等数据，从而相互校对出车辆地理上的绝对位置、与其他车辆的相对位置，帮助车辆进一步作出准确的决策；除了通过汇聚数据来了解周围环境，也需要通过其他的加工手段来筛选、分析数据，避免得出错误的结论，例如多个摄像头与雷达都会识别到前方车辆，需要通过算法确定是同一车辆，而非车前具有多个车辆。[11] 感知模块识别出环境信息后，会将汇聚加工后的数据传输到决策模块，决策模块结合车辆运行数据、用户下达的指令数据等信息，形成路线规划与驾驶策略。

车企于车外对数据进行加工与使用，则常见于车企自行搭建的算法云平台、安全监测平台与 TSP 平台等车外环境。具体而言，车企会将车况数据、环境数据、车辆运行数据等数据汇聚至算法云平台处，在云平台上进行算法模型的搭建与训练。为了加快算法的训练速度，车企汇聚的数据达到一定程度后，会直接基于海量数据搭建自动驾驶仿真平台，自动生成仿真环境，算法直接在仿真环境中进行训练迭代；安全监测平台采集海量的车辆的各类网络数据，构建模型进行攻防演练，从而实现更智能地安全监测；TSP 平台则会采集系统运行数据，综合评判系统的功能、安全措施，从而进行相应的升级措施。

综上所述，无论是采取车内处理还是车外处理，都有可能涉及到数据到汇聚融合，并且可能在此基础上生成新的深度数据。

[11] 举例参考了文章《史上最详细的自动驾驶汽车技术介绍硬件＋软件》，https://cloud.tencent.com/developer/news/366470，2022 年 10 月 15 日访问。

2. 汇聚数据后的合规措施

参照《网络数据分类分级要求（征求意见稿）》附录 E 的规定，如果融合数据对大量多维数据进行关联、分析或挖掘，汇聚了更大规模或分析出更敏感、更深层的数据，安全级别可以升高，但如果结果数据降低了标识化程度等，级别可以降低。

在车内加工使用数据的过程中，感知模块在融合分析摄像头、雷达、高精地图等软硬件传输的数据之后，会识别出行人车辆等周围环境信息，决策模块结合用户指令、运行数据则能产生路线、驾驶策略等更具深度且更涉及隐私的数据；车外加工使用数据的过程则会产生极具商业价值的算法与仿真平台，二者都具备“更大规模、更敏感、更深层”的特征。

因此，无论是车辆感知模块、决策模块分析、汇聚数据，还是算法云平台汇聚了大量多维度的数据后，对算法进行深度训练与升级，均可能导致数据安全级别的升高，与之相应的“自动驾驶大脑”和云平台均应当采取级别更高的数据安全保护措施。车企使用数据前，对数据采取去标识或者加密措施，则可能降低数据保护的安全等级，减少数据安全方面的法律风险。

3. 数据加工使用过程中的安全措施

加工使用数据的过程中的数据安全保护措施包括两类，一类是技术措施，另一类是管理措施。参考北京市自动驾驶示范区的规范，可将数据安全保护标准分为三个等级：[12]

第一档，执行目的明确原则和最少够用原则。技术上，如果是通过外部访问，需要通过加密通道使用数据。管理上，数据使用者只能获取履行职责所需的最小权限，基于权限进行数据访问与使用，且不能批量导出数据。具体对不同的终端设备设置不同的权限，通过对设备的管理实现权限的管理。

第二档，在满足第一档的基础上，技术上对个人信息相关的数据进行匿名化处理，降低数据安全事件带来的损害；管理上，使用数据之前需要对使用者进行身份认证，并且直接限制使用者的人数，降低不法使用、未经授权使用数据

[12] 以下三档的划分，参考了《北京市高级别自动驾驶示范区数据分类分级白皮书》第 21–24 页。

的可能性。同时，对所有使用数据的行为进行记录，实现数据使用情况的可回溯，以便事后界定权责。

第三档，在满足第一档与第二档的基础上，技术上封存原始数据，如果没有必要，终端设备不触碰原始数据，确有必要的，也严格限定数据的查询频率并单独记录日志。对终端设备采用可行执行环境，对关键应用提供安全执行空间；管理上，数据的使用需要经过数据安全主管部门进行审批，并且需要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。外部人员接触数据之前，除了签署保密协议之外，还需进行背景调查与评估。

综上所述，技术上通过加密通道访问 – 数据匿名化 – 可信系统环境分为三档，管理上以权限 – 身份认证 / 人数限制 – 背景调查与评估划分三档，从而实现对数据的分级保护与管理，也为智能网联汽车数据汇聚融合后采取的保护措施提供了参考。

二、数据与算法

算法是智能网联汽车的“智能”所在，既是加工使用数据所需的工具，也是数据加工使用之后的结果之一，二者相辅相成，故而同样是智能网联汽车数据合规的领域。

1. 算法与可解释性

目前，我国关于算法的法律规范多见于在个性化推荐领域，如《个人信息保护法》第二十四条、第七十三条规定的自动化决策、《互联网信息服务算法推荐管理规定》都将对算法的界定限制在自动分析个人的行为习惯、兴趣爱好等个人信息，以及向个人推荐信息的行为上。智能网联汽车的算法并非是“推荐”决策，而是直接操作车辆行驶，具有一定的特殊性。

根据《机器学习算法安全评估规范（征求意见稿）》第 7.4 条，运行部署之前，应当检验算法的可解释性。这是为了证实算法的安全性。如果算法无法被解释，其安全性自然也无法得到证实，智能网联汽车的“智能”也无法为人们相信。具体到标准，第 6.4 条提出，机器学习算法部署运行时，应当能够做到及时、准确、完整、清晰、无歧义地向使用者说明机器学习算法的作用、局限、安全风险和可能的影响，并解释相关应用过程及应用结果；如果部署应用不可解释的算法，应仅作为辅助决策手段，不作为直接决策依据。从该规定进行推理，智能网联汽车的驾驶算法，对于用户而言，也应当具备可解释性，其算法才能投入使用，否则无法作为直接决策的依据。

另一方面，随着智能网联汽车“智能化”程度的提高，人们对人工智能的伦理要求也提上日程。《人工智能伦理安全风险防范指引》将人工智能定义为“利用计算机或其控制的设备，通过感知环境、获取知识、推导演绎等方法，对人类智能的模拟、延伸或扩展”，与智能网联汽车感知路况环境，分析决策驾驶策略的路径如出一辙；其中亦从伦理角度提出，研究开发、部署运行人员应不断提升人工智能的可解释性。国家新一代人工智能治理专业委员会发布的《新一代人工智能伦理规范》第十二条规定，在算法设计、实现、应用等环节，提升透明性、可解释性、可理解性……才能够实现对算法的信赖、预测和监督。

基于上述原因，各大车企在研发智能网联汽车的过程中，车内数据处理的算法采用模块化模式而非端到端模式，也是因为模块化模式的“可解释性”相对更强，更符合对法律趋势对算法的要求。

2. 算法与可控性

算法可控性，一方面是指用户有权对是否以及在什么程度上使用人工智能算法进行选择；另一方面是指，算法本身是否具有值得信赖的可控性，以及出现差错的概率、后果是否可控，即《新一代人工智能伦理规范》所称的“保障人类拥有充分自主决策权……确保人工智能始终处于人类控制之下”。

在智能网联汽车领域，算法的可控性往往决定了车辆行驶的安全性，与乘客的人身、财产安全和道路交通安全息息相关，车企需要根据技术与行业规范，对算法进行测试与检查，才能在实践中尽可能确保车辆的行驶安全。例如，根据《机器学习算法安全评估规范（征求意见稿）》第 7.3 条对算法进行可复现性、鲁棒性测试，从而使算法在相同环境下做出相同的决策，并且能够尽可能排除噪声与无效数据的干扰。

三、使用数据的特殊注意事项

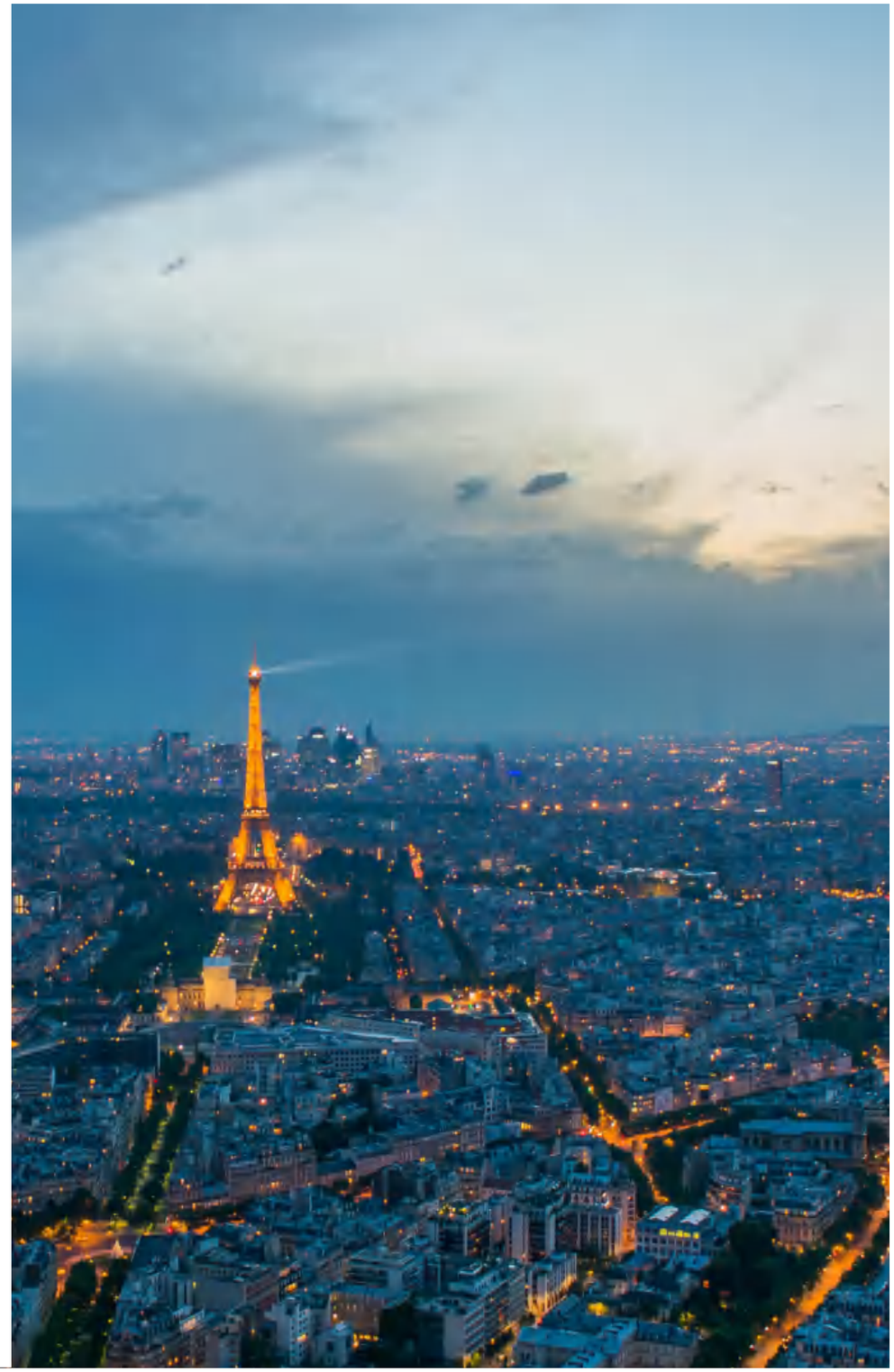
智能网联汽车的运行过程是对机动车驾驶行为的直接控制，关系到车上乘客及其他道路交通参与人的人身财产安全。因此，相比于其他人工智能应用场景，智能网联汽车数据使用存在额外要求，即不能影响车辆的正常驾驶，不能危及车辆的行驶安全。

实践中，曾经出现某两家知名车企在车主驾驶车辆的过程中，突然在导航界面弹出广告，遮挡住了导航视线，引发了舆情事件。[13] 此类广告弹窗可能导致驾驶员走错路口，甚至分心关闭广告导致交通事故，造成严重后果。

广告信息的推送的背后是对个人信息的加工、使用。车企会根据车主购车时的个人信息，结合行车习惯、购买的网络服务等其他个人信息，向车主推送广告。如果依法取得了车主的个人同意，并设置了便捷的关闭路径，则推送广告属于正常的商业行为。

但是，如果智能网联汽车在行驶状态，尤其是人类接管状态弹出广告，则很可能对车辆的驾驶造成影响。建议车企设计车载系统与软件的过程中，根据车辆的行驶状态，对应用的权限作不同的安排。在车辆行驶的过程中，导航、驾驶等应用的权限应当优先于娱乐、广告等应用的权限，避免二者冲突对车辆的行驶造成影响。而不宜仅仅按照《个人信息保护法》《互联网弹窗信息推送服务管理规定》等规范中对于手机、电脑等应用场景下的互联网弹窗的有关规定对智能网联汽车设备弹窗进行管理。

[13] 罗力铖：《汽车中控弹窗广告须依法治理》，载《法制日报》2022 年 10 月 12 日版。



第四章

数据提供合规要求

数据提供与公开是智能网联汽车数据合规管理的重要一环。智能网联汽车数据的提供，是指智能网联汽车及其生产、运营等主体基于行政机关、个人等主体和场景的需要，向其他主体提供数据信息的行为，且该主体如何处理数据无法为提供方所控制。根据相关法律法规、规范性文件的要求，国家倡导数据处理者在数据收集活动中遵循默认不收集原则、车内处理原则、脱敏处理原则。基于以上原则，智能网联车数据的提供要遵守基本的数据法的相关规范，还应当满足具体的法规、规章制度对汽车数据提供的合规要求。本章将展示智能网联汽车数据提供环节，并对其合规要求予以提示。

1. 对第三方提供数据的一般要求

向第三方提供数据，增加了数据处理的主体，也相应增加了数据安全的风险，因此法律数据提供有额外的规定。本部分将对个人信息、企业数据资源的对外提供进行论述。关于重要数据的对外提供，《网络数据安全管理条例（征求意见稿）》第三十二条将委托处理重要数据与提供（共享）重要数据并列规定，可参考白皮书第三部分数据传输与存储合规要求，3.2.2 车外存储与委托处理中关于重要数据委托处理的合规要求。

1.1 车内个人信息的提供

根据《个人信息保护法》第二十三条的规定，信息处理者向其他个人提供其所处理的个人信息，原则上需要满足三个条件，一是向个人告知接收方的名称或者姓名、联系方式、处理目的、处理方式和个人信息的种类并经过个人的单独同意。二是接收方应当在上述处理目的、处理方式和个人信息的种类等范围内处理个人信息。三是变更原先的处理范围的，应当重新取得个人同意。《个人信息保护法》第十三条规定了在例外情形下，个人信息提供不需要取得个人同意。如为履行合同所必需、为履行法定职责或者法定义务所必需、为应对突发公共卫生事件，或者紧急情况下为保护自然人的生命健康和财产安全所必需；为公共利益实施新闻报道、舆论监督等行为，在合理的范围内处理个人信息等。

下表对智能网联汽车场景下无需取得个人同意的情形予以示例：

序号	数据处理主体	必要性来源	用途
1	V2X 云平台	合同所必需	帮助车辆规划路线，降低事故发生风险，履行技术服务合同的义务
2	算法云平台	合同所必需	提供车辆行驶的算法服务，决定了车辆如何行驶，履行技术服务合同的义务
3	地图商云平台	合同所必需	提供行车导航、车辆定位等服务，履行技术服务合同的义务
4	TSP 云平台	合同所必需 履行法定义务所必需	提供系统升级、更新维护等服务，履行技术服务合同的义务，以及远程更新安全补丁等网络安全的法定义务
5	数据安全监测平台	履行法定义务所必需	履行《网络安全法》《个人信息保护法》等法律要求的数据安全保护义务
6	监管平台	履行法定义务所必需 紧急情况所必需	履行道路安全、数据保护相关的法定义务，以及紧急情况下对车辆下达远程指令，以避免事故的发生等。

表 5.1

但是，实践中取得个人同意与取得单独同意之间的关系，尚没有明确结论。《个人信息安全规范》附录 C 表 C1 中提到，个人使用过程中以弹窗等形式“单独”告知，并取得同意，可以推测以“弹窗形式”取得的同意属于单独同意。不过，业内常见的隐私文件中以单设链接、单设条款形式列出等其他方式，是否属于单独同意，仍然存在疑问。

因此，建议车企与相关信息接收方，尽可能做到以单独界面的形式取得用户的同意，并通过个人信息共享清单的形式向用户告知。同时，做好数据对外提供必要性的论证与评估，为援引《个人信息保护法》第十三条做好准备，降低潜在的法律风险。

1.2 车外个人信息

智能网联汽车在行驶的过程中不断进行图像采集，被采集方可能是社会车辆的驾驶人或路上行人，某些情况下被采集信息或能够达到个人信息的标准。对于此类数据的提供，原则上仍应征得个人的单独同意，但是现实中的可操作性较低；因此，较优合规路径为匿名化处理。《汽车数据安全管理若干规定（试行）》规定，因保证行车安全需要，无法征得个人同意采集到车外个人信息且向车外提供的，应当进行匿名化处理，包括删除含有能够识别自然人的画面，或者对画面中的人脸信息等进行局部轮廓化处理等，使之不再构成个人信息，从而无需承担法律法规对“提供个人信息”所规定的义务。

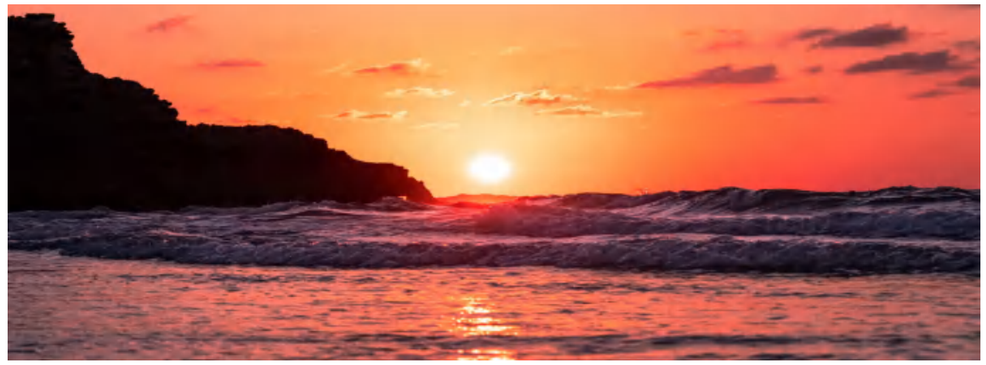
1.3 智能网联汽车运行数据提供

智能网联汽车运行数据包括机动车相关信息以及自动驾驶系统运行数据。其中，值得关注的是运行数据权益的归属，进而分析其提供的合规要求。自动驾驶系统运行数据是车企或者自动驾驶系统提供商等主体关键技术的基石，往往涉及知识产权和商业秘密等核心竞争力，属于相关企业数据保护的重点对象。

司法实践中，杭州铁路法院认为，长期经营积累聚集而成的数据资源整体，可以为权利人开发衍生产品获取增值利润和竞争优势的机会，权利人享有竞争权益。[14] 车辆训练以及上路实测产生、积累而成的数据，对于车企而言，可以帮助开发优化算法模型、构建仿真平台等业务开展，构成对车企的竞争权益；此外，杭州中院认为，经过权利人投入大量智力劳动成果，通过深度开发与系统整合，最终形成与原始数据无直接对应关系的独立衍生数据，可以为权利人实际控制和使用，并带来显著经济利益的，权利人应享有独立的财产性权益。[15] 因此，车企对车辆运行数据等原始数据的深度加工，最终形成算法、仿真平台等独立产品，也享有竞争权益。

域外，欧盟也对车辆数据的交易做出了尝试——2018 年 10 月关于自动驾驶车辆注册的投票，其中 7A 条款“自动驾驶汽车产生的数据是自动生成的，其本质不具有创造性，所以不适用于版权保护或数据库权利”，可以理解为不需要经过车主同意，汽车制造商可以收集自动驾驶汽车产生的数据并处置，这些数据中就可能包含可以对车辆 GPS 轨迹、激光点云数据等测绘数据。汽车制造商有权将这些数据卖给保险公司、市场研究机构、广告公司等。[16]

目前国内智能网联汽车生产、运营、数据处理往往涉及到多个企业，因此，对于数据权利的归属，智能网联汽车生产企业和自动驾驶系统提供商应当在数据产生、处理之前就进行约定，避免就这些数据以及之后的知识产权归属引发纠纷。



[14] 浙江省杭州市中级人民法院：深圳某计算机公司、某科技（深圳）公司与浙江某网络公司、杭州某科技公司不正当竞争纠纷案，（2020）浙 01 民终 5889 号民事裁定书，杭州互联网法院发布数据和算法十大典型案例之三。

[15] 浙江省杭州市中级人民法院：淘宝（中国）软件有限公司诉安徽美景信息科技有限公司不正当竞争纠纷案，（2018）浙 01 民终 7312 号民事判决书，杭州互联网法院发布数据和算法十大典型案例之一。

[16] 国家测绘地信局测绘发展研究中心：《发展研究 | 发展自动驾驶需要进一步研究测绘法律相关逻辑》，https://www.sohu.com/a/404314933_505861，2022 年 10 月 15 日访问。

二、接收数据的主体

数据对外提供所增加的风险，主要由数据接收方的介入而产生。因此，根据数据接收方主体的不同，法律也对此有不同的要求。

1. 向行政机关提供

行政机关对于智能网联汽车的管理和服务体现在智能网联汽车从生产到运行的全过程当中。在生产、测试环节，生产需要向有关部门备案并取得特定许可；在日常运营中，有关部门会对智能网联车的数据处理做出要求，运营者有义务配合监管；在发生安全事件时，运营者有义务向主管机关进行报告，并配合调查提供相应的数据。

1.1 道路测试安全性自我声明

《智能网联汽车道路测试与示范应用管理规范（试行）》规定，道路测试主体应提供智能网联汽车道路测试安全性自我声明，并由省、市级政府相关主管部门进行确认，包括道路测试主体、车辆识别代号、测试驾驶人姓名及身份证号、测试时间、测试路段、区域及测试项目等信息。其中，测试时间原则上不超过 18 个月，且不得超过安全技术检验合格证明及保险凭证的有效期。道路测试安全性自我声明应随同以下证明材料提交至省、市级政府相关主管部门。需要提供的信息包括：道路测试主体、测试驾驶人和道路测试车辆的基本情况；道路测试车辆的自动驾驶功能等级声明以及自动驾驶功能对应的设计运行条件说明，包括设计运行范围、车辆状态和驾驶人状态等；道路测试车辆设计运行范围与拟进行道路测试路段、区域内各类交通要素对应关系说明等数据。

1.2 配合行政管理和行政监督

智能网联汽车上路之后，行政机关依法要对车辆运行情况，数据安全保护情况等进行监管。一是针对传统道路运输、旅客运输企业的规范要求，同样适用于智能网联汽车旅客运输业务。如《道路运输车辆动态监督管理办法》规定，道路旅客运输企业和道路危险货物运输企业监控平台应当接入全国重点营运车辆联网联控系统（以下简称联网联控系统），并按照要求将车辆行驶的动态信息和企业、驾驶人员、车辆的相关信息逐级上传至全国道路运输车辆动态信息公共交换平台。道路货运企业监控平台应当与道路货运车辆公共平台对接，按照要求将企业、驾驶人员、车辆的相关信息上传至道路货运车辆公共平台，并接收道路货运车辆公共平台转发的货运车辆行驶的动态信息。公安机关交通管理部门、应急管理部门根据需要可以通过道路运输车辆动态信息公共服务平台，随时或者定期调取系统中的全国道路运输车辆动态监控数据。道路运输企业是道路运输车辆动态监控的责任主体。为了保证动态信息能够及时传送，道路运输经营者应当选购安装符合标准的卫星定位装置的车辆，并接入符合要求的监控平台，在监控平台中完整、准确地录入所属道路运输车辆和驾驶人员的基础资料等信息，并及时更新。

二是专门针对智能网联汽车相关企业的规范管理要求。目前对于智能网联汽车的规范管理体系尚不健全，且多处于试点阶段，但是从目前的规范制定情况来看，国家已经对智能网联汽车产业勾勒出了大致的管理路径。目前国家对于智能网联汽车信息监管的总体要求是，加强智能（网联）汽车网络平台建设，开展智能（网联）汽车入网运行和安全保障服务等，协同汽车数据处理者加强智能（网联）汽车网络和汽车数据安全防护。2020 年，发改委等十一部委共同发布《智能汽车创新发展战略》，明确提出建设国家级智能汽车大数据云控基础平台。2020 年 9 月 27 日，工业和信息化部“2020 年产业技术基础公共服务平台项目——智能网联汽车数据交互与综合应用公共服务平台建设”在长沙开始建设。国家监管的介入，能够助力建设我国智能网联汽车数据标准和全生命周期管理体系，推动构建融运行监测、安全预警、测试评价等多场景综合应用为一体的智能网联汽车数据新生态。

1.3 配合调查、事故处理

主动报告义务：智能网联汽车发生交通违法行为、交通事故，以及数据泄露、黑客劫持或涉及到国家安全等事件时，有义务向主管机关进行报告，并配合调查。

配合调查义务：《数据安全法》第三十五条规定，公安机关、国家安全机关因依法维护国家安全或者侦查犯罪的需要调取数据，应当按照国家有关规定，经过严格的批准手续，依法进行，有关组织、个人应当予以配合。

保存与处理义务：《道路运输车辆动态监督管理办法》规定，监控人员应当实时分析、处理车辆行驶动态信息，及时提醒驾驶员纠正超速行驶、疲劳驾驶等违法行为，并记录存档至动态监控台账；对经提醒仍然继续违法驾驶的驾驶员，应当及时向企业安全管理机构报告，安全管理机构应当立即采取措施制止；对拒不执行制止措施仍然继续违法驾驶的，道路运输企业应当及时报告公安机关交通管理部门，并在事后解聘驾驶员。动态监控数据应当至少保存 6 个月，违法驾驶信息及处理情况应当至少保存 3 年。对存在交通违法信息的驾驶员，道路运输企业在事后应当及时给予处理。

记录和传输义务：《自动驾驶汽车运输安全服务指南（试行）》规定：“从事运输经营的自动驾驶汽车应当具备车辆运行状态记录、存储和传输功能，向运输经营者和属地交通运输主管部门及时传输相关信息。在车辆发生事故或自动驾驶功能失效时，自动记录和存储事发前至少 90 秒至事发后至少 30 秒的运行状态信息。运行状态信息至少包括：车辆基本信息、控制模式变化情况、接收的远程控制指令情况、运行状态、人机交互及车内外影像情况等。”

2. 向用户提供

用户可能调取的信息包括与自身有关的信息，如被采集的个人信息，这类信息依照现有的数据法律法规，应当向个人提供；但是和用户无关或没有直接关联的信息，如运行状态信息等等，应当如何提供也是理论和实务中有待解决的问题。下面将以一则案例探讨用户知情权和企业商业秘密之间的边界，并提出合规处理建议。

2021 年 8 月 3 日晚，张某驾驶特斯拉 Model3 在小区保安入口处刹车失灵，径直上坡撞上侧墙，双气囊弹出，致车内人员受伤。张某称，事后去找特斯拉，要求特斯拉提供事故发生前半小时的完整数据，但特斯拉只提供非常简单且证明车子无物理故障的数据。郑州市郑东新区市场监管局认为这属于消费者知情权，责令特斯拉无条件向上海车展维权当事人张女士提供该车发生事故前半小时完整行车数据。

车主的法益为《消费者权益保护法》第八条所赋予的知情权，即消费者作为商品交易中信息弱势方应得到利益保护的权利体现。而经营者的法益则是散见于《中华人民共和国反不正当竞争法》第九条、《关于审理侵犯商业秘密民事案件适用法律若干问题的规定》等法律法规以及解释性文件中的商业秘密，是经营者与同行竞争并实现经济效益的核心。当消费者的知情权与经营者对行车数据复制部分的用益物权、商业秘密保护的法益产生冲突时，应当优先考虑消费者知情权的利益，兼顾经营者商业秘密的保护。经营者应尽可能地在保护商业秘密且在不影响消费者个人隐私权保护的前提下，公布消费者在使用或接受经营者提供的商品或服务过程中，由于消费者自身主观原因而产生的但由经营者实际控制的数据的复制件。[17]

3. 向境外主体提供

由于跨境数据处理活动事关国家安全，国家对于向境外提供的数据进行严格管理。对于特定的数据类型、接收主体有更为严格的限制，例如《汽车采集数据处理安全指南》规定车外数据、座舱数据、位置轨迹数据不应出境；对于外国国家机关，《数据安全法》第三十六条规定，非经中华人民共和国主管机关批准，境内的组织、个人不得向外国司法或者执法机构提供存储于中华人民共和国境内的数据。

基于此，智能网联汽车在运营过程中产生、收集的数据，应当遵守《数据安全法》以及相关法规、规范性文件的规定。从相关规定来看，国家对重要数据出境的要求较为苛刻，仅提供了数据安全评估一种出境途径；对个人信息出境方式的要求相对宽松、多元，根据重要程度不同，依次提供了安全评估、安全认证与标准合同三种方式。

[17] 张旭阳：《消费者知情权视角下行车数据使用的合理性模式建构》，载微信公众号《贸法论丛》，2022 年 10 月 15 日访问。

3.1 数据安全评估

根据《数据出境安全评估办法》第四条，车企具有相关情形的，应当通过所在地省级网信部门向国家网信部门申报数据出境安全评估，通过评估后方可进行数据出境的行为。下表列出相关情形，并进行举例以供参考：

序号	法定情形	举例
1	数据处理者向境外提供重要数据	例如车企对境外主体提供 / 许可核心自动驾驶算法、提供包含人脸与车牌的车外采集影像等数据
2	关键信息基础设施运营者和处理 100 万人以上个人信息的数据处理者向境外提供个人信息	运营关键信息基础设施的单位，例如高精地图厂商对外提供个人信息
		例如用户超过 100 万人的大型车企向境外主体提供个人信息
3	自上年 1 月 1 日起累计向境外提供 10 万人个人信息或者 1 万人敏感个人信息的数据处理者向境外提供个人信息；	例如已经与境外主体建立稳定合作关系、具有一定规模的汽车厂商，以境外的软件与服务器，处理国内用户的个人信息，为国内用户提供服务。
4	国家网信部门规定的其他需要申报数据出境安全评估的情形	/

表 5.2

根据《数据出境安全评估办法》第六条与第八条的规定，车企进行数据安全评估前，应当先进行数据出境风险自评估，随后再进行数据安全评估程序，下表列出相关情形，并进行举例：

序号	自评估内容	相关的安全评估内容	举例
1	数据出境和境外接收方处理数据的目的、范围、方式等的合法性、正当性、必要性	数据出境的目的、范围、方式等的合法性、正当性、必要性	例如为了训练境外的算法，采集国内个人信息是否必要
2	出境数据的规模、范围、种类、敏感程度，数据出境可能对国家安全、公共利益、个人或者组织合法权益带来的风险；	出境数据的规模、范围、种类、敏感程度……	例如个人信息泄露后被用于电信诈骗的概率；地理信息推测出敏感区域的概率等
3	境外接收方承诺承担的责任义务，以及履行责任义务的管理和技术措施、能力等能否保障出境数据的安全	数据安全和个人信息权益是否能够得到充分有效保障；	数据接收方是否具有较强的技术实力，内部管理结构是否稳定等
4	数据出境中和出境后遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等的风险，个人信息权益维护的渠道是否通畅等	出境中和出境后遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等的风险；	例如数据传输过程中的加密措施是否合理，数据（比如军事区域地理信息）泄露后的后果是否可以承受等
5	与境外接收方拟订立的数据出境相关合同或者其他具有法律效力的文件等（以下统称法律文件）是否充分约定了数据安全保护责任义务	数据处理者与境外接收方拟订立的法律文件中是否充分约定了数据安全保护责任义务	参见《数据出境安全评估办法》第九条
6	其他可能影响数据出境安全的事项	境外接收方所在国家或者地区的数据安全保护政策法规和网络安全环境对出境数据安全的影响；境外接收方的数据保护水平是否达到中华人民共和国法律、行政法规的规定和强制性国家标准的要求	法治情况不佳、缺乏健全数据保护法律的国家，或者法律保护水平较低的国家，可能无法对其国内的企业提供数据
		遵守中国法律、行政法规、部门规章情况	相关企业是否被我国政府处罚，或者是否于我国败诉等
		国家网信部门认为需要评估的其他事项	/

表 5.3

3.2 个人信息安全认证

《个人信息保护法》第三十八条规定，个人信息处理者因业务等需要，确需向中华人民共和国境外提供个人信息的，应当具备下列条件之一：

（一）依照本法第四十条的规定通过国家网信部门组织的安全评估；

（二）按照国家网信部门的规定经专业机构进行个人信息保护认证；

（三）按照国家网信部门制定的标准合同与境外接收方订立合同，约定双方的权利和义务；

（四）法律、行政法规或者国家网信部门规定的其他条件。

由此可以推理，个人信息的跨境提供，不一定需要进行数据安全评估，也可以通过个人信息保护认证、签订标准合同或其他方式来履行个人信息出境的法定手续。《个人信息跨境处理活动安全认证规范》在摘要中指出，本实践指南依据有关政策法规要求，为落实《个人信息保护法》建立个人信息保护认证制度提供认证依据，确系个人信息保护认证的下位规范。

根据《个人信息跨境处理活动安全认证规范》的规定，个人信息跨境处理活动认证属于国家推荐的自愿性认证，鼓励而非强制个人信息处理者和境外接收方在跨境自愿申请；同时，也并非适用于所有类型的个人信息跨境处理，仅适用于跨国公司或者同一经济、事业实体下属子公司或关联公司之间的个人信息跨境处理活动，或者境外处理中国境内自然人个人信息，以向境内自然人提供产品或者服务或分析、评估境内自然人的行为，即跨国车企的关联公司之间跨境处理个人信息，或者境外车企向中国境内出售智能网联汽车从而处理个人信息的，才适用个人信息跨境处理活动认证。如果是车企向外国的非关联主体提供个人信息，则不适用该认证。

具体到认证的内容，主要会从双方签订的协议是否可以保障个人信息权益，双方的组织管理结构中是否包含个人信息保护机构，双方约定跨境处理个人信息的规则，个人信息保护影响评估，个人信息保障机制等多方面进行。

3.3 标准合同

根据《个人信息保护法》第三十八条规定，除了数据安全评估、个人信息保护认证之外，签订标准合同也是合规手续之一。网信办出台了《个人信息出境标准合同规定（征求意见稿）》，但标准合同的适用存在四个前提条件，即个人信息提供者非关键信息基础设施运营者；处理个人信息不满 100 万人的；自上年 1 月 1 日起累计向境外提供未达到 10 万人个人信息的；自上年 1 月 1 日起累计向境外提供未达到 1 万人敏感个人信息的，与数据安全评估互斥。

标准合同的内容，包括个人信息出境的目的、类型、敏感程度、数量等情况；双方保护个人信息的责任与义务，以及为防范个人信息出境可能带来安全风险所采取的技术和管理措施等；境外接收方所在国家或者地区的个人信息保护政策法规对遵守合同条款的影响；个人信息主体的权利，以及保障个人信息主体权利的途径和方式等内容，与数据安全评估、个人信息保护认证的内容大体一致。

签订标准合同，并不免除个人信息保护影响评估的义务。双方完成标准合同的签约后，自合同生效之日起十个工作日内向所在地省级网信部门备案，并同时提交标准合同与个人信息保护影响评估报告。

4. 向社会公布

在一些舆情较大的安全事件中，智能网联汽车生产、运营企业可能面临社会公众要求企业公开部分数据参数的情况，由于此类参数往往涉及个人隐私、商业秘密与技术信息，彼此无法完全剥离或做匿名化处理，对此类信息是否公开，如何公开，目前尚无系统的合规性论述。

2021 年 4 月 19 日，上海车展上一位特斯拉车主身穿“刹车失灵”白 T 恤站上车顶维权。特斯拉方坚称，刹车未失灵。紧接着，网络媒体上掀起了一场声势浩大的“讨特”运动，公众舆论迅速聚焦到一个点：行驶数据。三天后，特斯拉对外公布了车辆事故发生前一分钟的数据。数据显示，刹车前车辆时速为 118.5 千米每小时，驾驶员刹车后车辆持续降速，时速降至 48.5 千米每小时发生碰撞。从第一次刹车到碰撞间隔时间约为 4.5 秒左右。数据公布后，车主家属指责特斯拉侵犯个人隐私权，要求撤销数据。

企业何时可以公布数据，在此可以参照《个人信息保护法》第十三条规定，在紧急情况下为保护自然人的生命健康和财产安全所必需、为公共利益实施新闻报道、舆论监督等行为，在合理的范围内处理个人信息。在具体情景上体现为，当自动驾驶系统确实存在缺陷，可能危及不特定多数人的人身财产安全或者公共利益，企业就具有向社会公布特定数据的义务。除此之外，企业出于商业决策，有为自己澄清事实的考量，也会自主选择公开相关数据。当自动驾驶系统确实存在缺陷可能产生危害，或企业主动决定向社会公开时，可以将基本车况等数据经过脱敏后，降低一般公众将车况数据与第三方信息结合重新识别特定自然人的可能性减少被认定为个人信息和个人隐私的可能性，尽量降低合规风险。

附录

法律法规、规章、标准引用清单

一、法律

序号	
1	中华人民共和国民法典
2	中华人民共和国刑法
3	中华人民共和国行政处罚法
4.	中华人民共和国行政强制法
5	中华人民共和国行政诉讼法
6	中华人民共和国数据安全法
7	中华人民共和国网络安全法
8	中华人民共和国个人信息保护法
9	中华人民共和国测绘法
10	中华人民共和国反不正当竞争法
11	中华人民共和国消费者权益保护法
12	中华人民共和国道路交通安全法（修订建议稿草案）

二、司法解释

1	最高人民法院关于审理侵犯商业秘密民事案件适用法律若干问题的规定

三、行政法规

1	国务院办公厅关于促进二手车便利交易的若干意见
2	网络数据安全管理条例（征求意见稿）

四、地方性法规（经济特区法规）

序号	
1	深圳经济特区智能网联汽车管理条例

五、部门规章、部门规范性文件

1	机动车登记规定
2	测绘资质管理办法
3	道路运输车辆动态监督管理办法
4	道路交通事故处理工作规范
5	公安机关办理行政案件程序规定
6	智能网联汽车道路测试与示范应用管理规范（试行）
7	汽车数据安全管理若干规定（试行）
8	智能汽车创新发展战略
9	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
10	交通运输部关于促进道路交通自动驾驶技术发展和应用的指导意见
11	工业和信息化部关于加强智能网联汽车生产企业及产品准入管理的意见
12	自动驾驶汽车运输安全服务指南（试行）
13	公路工程适应自动驾驶附属设施总体技术规范（征求意见稿）
14	互联网弹窗信息推送服务管理规定
15	中国禁止出口限制出口技术目录
16	数据出境安全评估办法
17	公路水路关键信息基础设施安全保护管理办法（征求意见稿）
18	自动驾驶汽车运输安全服务指南（试行）（征求意见稿）
19	个人信息出境标准合同规定（征求意见稿）

六、地方政府规章、地方规范性文件

序号	
1	上海市智能网联汽车测试与应用管理办法
2	北京市自动驾驶车辆道路测试管理实施细则（试行）

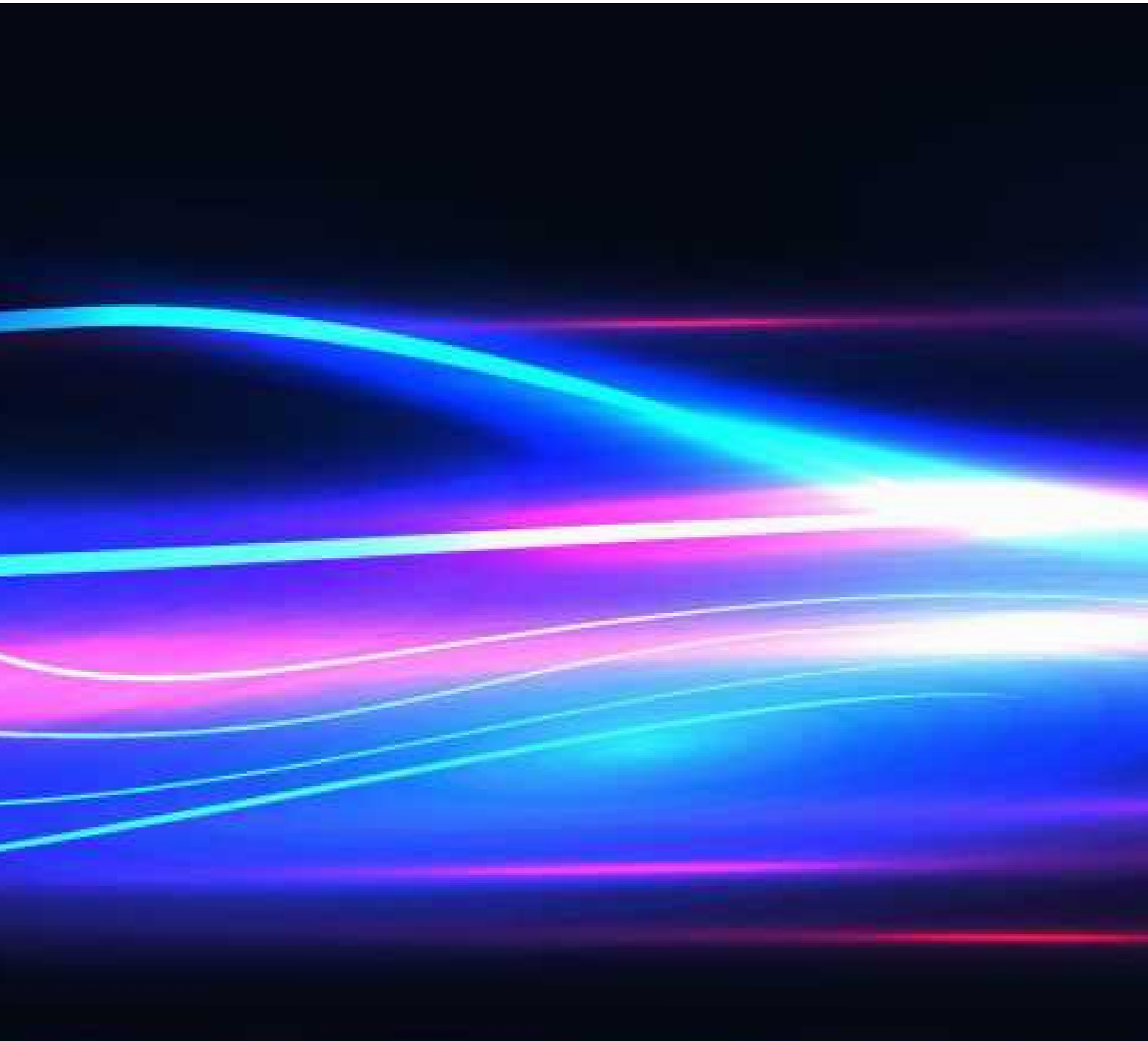
七、标准

1	国家车联网产业标准体系建设指南（智能网联汽车）（2022 年版）
2	测绘资质分类分级标准
3	GB 7258 机动车运行安全技术条件
4	GB/T 40429–2021 汽车驾驶自动化分级
5	GB/T 35274—2017 信息安全技术大数据服务安全能力要求
6	GB/T 35658 道路运输车辆卫星定位系统平台技术要求
7	GB/T 19056 汽车行驶记录仪
8	YD/T 2781–2014 电信和互联网服务用户个人信息保护定义及分类
9	YD/T 2782–2014 电信和互联网服务用户个人信息保护分级指南
10	YD/T 3746—2020 车联网信息服务 用户个人信息保护要求
11	JT/T 808 道路运输车辆卫星定位系统终端通信协议及数据格式
12	JT/T 809 道路运输车辆卫星定位系统平台数据交换 检索报告
13	JT/T 794 道路运输车辆卫星定位系统车载终端技术要求
14	JT/T 808 道路运输车辆卫星定位系统终端通信协议及数据格式
15	TC260–PG–20211A 人工智能伦理安全风险防范指引
16	TC260–001 汽车采集数据处理安全指南
17	TC260–PG–20222A 个人信息跨境处理活动安全认证规范
18	网络数据分类分级要求（征求意见稿）
19	机器学习算法安全评估规范（征求意见稿）

30th ANNIVERSARY
1992
2022

大成 DENTONS

DENTONS
CHINA



大成律师事务所

微信扫描二维码
关注公众号

地址: 北京市朝阳区朝阳门南大街10号
兆泰国际中心B座 16–21 层
邮编: 100020
总机: +86 10 5813 7799
传真: +86 10 5813 7788
网站: www.dentons.com
邮箱: beijing@dentons.cn

© 2022 大成。大成是一家通过其成员律所和联盟机构向全球范围的客户提供法律服务的全球法律执业机构。 此文件未包含提供法律或其它咨询建议的意图，请勿根据文件内容采取或不采取行动。如需查看法律声明，请访问dentons.com。