《智能网联汽车数据安全要求》（送审稿）
编制说明

一、项目背景

欧盟于 2018 年 5 月 25 日起正式生效的《一般数据保护条例（General Data Protection Regulation）》，主要针对个人对数据的控制和权限，包含一般规定，原则，数据主体的权利，数据控制人员或处理器的职责，个人数据转移到第三国，监管机构，会员国之间的合作，违反的责任，责任或处罚权利等内容。该法规主要规范了个人信息的保护，不能完全满足我国法律法规对重要数据的保护要求。

ISO 27701 《Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines》是 ISO 27001 和 ISO 27002 在隐私方面的扩展，并为个人隐私数据保护提供了除 ISO 27001 和 ISO 27002 之外的额外的指导。该标准有关隐私信息管理体系（PIMS）的相关要求对于本文件规范的汽车数据安全管理体系有借鉴意义，该标准并未对个人信息保护全生命周期的安全保护提出技术要求，因此不能完全满足行业对标准技术要求指导的需求，特别是车外人脸车牌等个人信息匿名化处理方面。

国外方面，欧盟、美国等相继出台数据安全相关政策法规，我国汽车、交通、信息等行业的骨干企业、科研院所及高校等也在积极开展智能网联汽车重要数据与个人信息的安全保护，加快推进智能网联汽车数据安全政策法规落地，对智能网联汽车数据安全要求及对应测试要求标准需求强烈。有必要制定本文件，指导深圳地区智能网联汽车相关企业落实数据安全政策要求并采用配套检测方法进行测试验证。本文件的制定对于落实数据安全和个人信息保护相关法规要求具有重要作用，有利于数据资源的开发利用和开放共享，有助于推动自动驾驶技术的产品研发和服务创新，能够进一步促进深圳市智能网联汽车产业高质量发展。

二、工作简况

（一）任务来源

深证市政府为服务产业发展，构建企业廉洁合规、智能网联汽车管理等相关标准体系，助力全市经济社会高质量发展。根据《中华人民共和国标准化法》《广东省标准化条例》等规定，深圳市市场监督管理局决定对《企业廉洁合规治理指南》《智能网联汽车自动驾驶系统技术要求》等 12 项地方标准予以立项，受深圳市工信局开展本项目，本文件以推荐性国家标准《智能网联汽车 数据通用要求》草案（征求意见稿）（计划号：20213606-T-339）（2022.10.28）为基础制定，主要用于支持深圳市智能网联汽车准入管理工作的实施。

（二）主要起草过程

2.1 起草过程综述

受深圳市市场监督管理局委托，中汽研软件测评（天津）有限公司根据申请情况成立标准起草项目组，确定中汽研软件测评（天津）有限公司为牵头单位，并在此基础上明确了任务和分工，积极开展标准的预研、起草及征求意见等工作。自标准制定工作启动以来，牵头单位多次组织项目组成员单位召开项目组会议，分析了欧盟、美国等地的国际数据安全保护和个人信息保护标准法规现状和国内推荐性国家标准《智能网联汽车 数据通用要求》内容，编写了标准草案，最终完成了标准的公开征求意见稿。

2022 年 12 月 5 日～2022 年 12 月 9 日，通过电子邮件的方式征求了深圳市交通运输局、深圳市公安局交通警察局、深圳市发展和改革委员会、深圳市市场监督管理局、中国银行保险监督管理委员会深圳监管局、深圳市政务服务数据管理局、深圳市住房和建设局、深圳市人民政府国有资产监督管理委员会、深圳市前海深港现代服务业合作区管理局、各区政府（福田区、罗湖区、南山区、宝安区、龙岗区、坪山区、龙华区、光明区、大鹏新区、深汕特别合作区）的意见，并根据意见修改标准草案。

2.2 历次项目组会议

2.2.1 项目组第一次会议

智能网联汽车数据安全要求标准项目组第一次会议于 2022 年 8 月 17 日在线上召开，会议就标准的制定背景、范围、框架和主要内容进行了详细的讨论。

会议明确：该标准以深圳市地方标准进行立项；该标准将参考国内正在制定的推荐性国家标准《智能网联汽车 数据通用要求》草案进行编制。并面向项目组成员单位征集意见。

2.2.2 标准符合性调研

为了尽快推进标准研制进程，为标准制定提供依据，面向项目组成员单位对 2023 年 6 月前地方标准符合性情况开展调研评估活动，针对数据分级分类、个人信息保护技术情况、重要数据安全技术情况进行问卷调查。调研结果发现：针对车外人脸车牌匿名化处理，多家车企尚未完成开发工作，完成车端部署时间尚未确定，其他技术要求企业已基本完成技术部署，在 2023 年 6 月前可符合标准要求。

2.2.3 项目组第二次会议

智能网联汽车数据安全要求标准项目组第二次会议于 2022 年 8 月 25 日在线上召开，会议对面向项目组征集的 42 条意见进行了处理。

三、确定标准主要内容的依据，以及与国内领先、国际先进标准的对标情况

本文件编写符合 GB/T 1.1—2020《标准化工作导则 第 1 部分：标准化文件的结构和起草规则》的规定起草。起草过程，充分考虑国内外现有相关标准的统一和协调；标准的要求充分考虑了国内当前的行业技术水平，对草案内容进行多次征求意见和充分讨论。

本文件基于我国产业实际技术发展及产品应用现状自主制定，未采用国际法规或标准。

本文件第三章是依据《中华人民共和国个人信息保护法》、《汽车数据安全管理若干规

定（试行）》、《GB/T 35273-2020 信息安全技术 个人信息安全规范》、推荐性国家标准《智能网联汽车 数据通用要求》草案（征求意见稿）（计划号：20213606-T-339）等文件进行编制的。

本文件第四章、第五章、第六章是是依据《中华人民共和国个人信息保护法》、《汽车数据安全管理若干规定（试行）》、推荐性国家标准《智能网联汽车 数据通用要求》草案（征求意见稿）（计划号：20213606-T-339），结合《深圳经济特区智能网联汽车管理条例》对数据安全的要求进行编制的。

本文件第七章、附录 A、附录 B、附录 C、附录 D 是依据推荐性国家标准《智能网联汽车 数据通用要求》草案（征求意见稿）（计划号：20213606-T-339）进行编制的。

本文件与现行相关法律、行政法规及标准协调一致，无重叠、冲突或矛盾。

四、主要条款的说明以及主要技术指标、参数、试验验证的论述

（一）适用范围

本文件规定了智能网联汽车数据的一般要求、个人信息保护要求、重要数据保护要求、审核评估要求等。

本文件适用于智能网联汽车及其数据处理者。

（二）主要技术内容

2.1 标准框架

本文件适用于智能网联汽车及其数据处理者。

本文件规定了智能网联汽车数据的一般要求、个人信息保护要求、重要数据保护要求、审核评估要求等，主要技术内容包括：

①汽车数据安全管理体系要求及相应的审核评估方法；

②针对数据全生命周期的个人信息保护技术要求，包括个人信息匿名化处理技术要求；

③针对数据全生命周期的重要数据保护技术要求；

④个人信息保护和重要数据保护相应的试验方法。

2.2 标准范围

【原文】本本文件适用于智能网联汽车及其数据处理者。

【说明】所有处理智能网联汽车数据的组织，包括汽车制造商、零部件和软件供应商、经销商、维修机构以及出行服务企业等，均适用于本文件。

2.3 汽车数据安全管理体系

【原文】汽车数据处理者应建立汽车数据安全管理体系。

【说明】本条款要求汽车数据处理者建立汽车数据安全管理体系。汽车数据安全管理体系应符合4.1章节的要求，汽车数据处理者可在企业整体管理体系的不同子部分包含4.1章节规范的汽车数据安全管理体系的必要元素，不必要建立单独的汽车数据安全管理体系。

2.4 取得个人同意的例外

【原文】满足以下例外情形时，汽车数据处理者处理个人信息可不取得个人同意：

——提高车辆行驶安全性且不向车外传输个人信息的功能，例如驾驶员注意力监测功能等；

——用于事故或紧急救援的服务功能，例如车载事故紧急呼叫系统等；

——处理个人自行公开或者其他已经合法公开的个人信息；

——无法通过有效的技术手段取得个人同意的情形；

——其他为了满足法律、行政法规、地方性法规、部门规章、规范性文件、具有强制效力的国家标准要求处理个人信息的情形。

【说明】本条要求参考《个人信息保护法》第十三条和《汽车数据安全管理若干规定（试行）》第八条，通过在项目组内对汽车数据的实际应用场景进行分析，得出汽车数据涉及的符合法律法规的可不取得个人同意的情形。

2.5 个人信息删除

【原文】有下列情形之一的，汽车数据处理者应当主动删除个人信息或匿名化处理：

a) 处理目的已实现、无法实现或者为实现处理目的不再必要；

b) 汽车数据处理者停止提供产品或者服务，或者保存期限已届满；

c) 个人撤回同意；

d) 汽车数据处理者违反法律、行政法规或者违反约定处理个人信息；

e) 法律、行政法规规定的其他情形。

【说明】本条要求参考《个人信息保护法》第四十七条和《网络数据安全管理条例（征求意见稿）》第二十二条，且匿名化处理后的个人信息不再属于个人信息，因此适用于本条款规定的情形之一的，处理个人信息的汽车数据处理者应主动删除个人信息或对个人信息进行匿名化处理。匿名化处理应符合本文件匿名化处理的要求。

2.6 附录E （资料性）汽车数据安全管理体系符合性评估细则

【原文】汽车数据安全管理体系符合性评估细则。

【说明】通过前期摸底调研结果和行业反馈，部分企业已建立汽车数据安全管理体系且可基本符合本文件对汽车数据安全管理体系的相关要求。附录E可作为开展汽车数据安全管理体系符合性评估的参考。

2.7 附录C （规范性） 个人信息匿名化处理试验方法

【说明】个人信息匿名化处理试验方法在标准过程中提出硬件在环和整车试验两套试验方案。通过摸底试验，硬件在环的方案无法保证多型号、多分辨率摄像头的适配性问题，同时暂时不具备根据不同摄像头采集方案的调整能力，无法实现标准中对于试验一致性的要求。但实车试验方案存在无法获取真值的情况，故在试验方法确定过程中充分考虑无真值前提下

的结果评估方案，现阶段附录C的试验方法通过试验验证可以在无真值的前提下保证试验的一致性。

2.8 C.1.1 车辆要求

【原文】进行个人信息匿名化处理的试验车辆应满足以下要求：

——具备对包含车外人脸目标及汽车号牌目标的图像或视频数据进行匿名化处理及向车外传输的能力；

——具备明确的匿名化处理及向车外传输相关功能开启条件。

【说明】由于各类车辆开启匿名化处理及向车外传输相关功能的条件具有较大差异性，部分车辆可能为保证带宽和算力需求，对于传输图片数量限制较高，导致数据采集周期过长。通过验证试验，建议企业可通过调整功能开启条件的方式实现加速试验的目的，而本条款仅针对该版本的试验车辆软硬件进行测试。对于调整开启条件的车型，若存在软件版本变更等问题，也建议企业可以通过声明的方式，保证不同软件版本下的匿名化处理效果一致性。

2.9 C.1.2 匿名化化区域范围文件

【原文】可提供具备提供匿名化区域范围文件的能力，匿名化范围文件至少包括矩形、椭圆形或旋转矩形等匿名化标注区域、匿名化对象性质（人脸、汽车号牌目标）和记录时间。

【说明】匿名化区域范围文件可作为判定匿名化区域、匿名化目标性质的支撑，当出现部分匿名化区域性质的争议时，提供证据支持，但企业反馈量产车型输出该文件存在难度，经过试验验证，确定该文件可作为可选项，非必须提供内容。

2.10 C.2.1 试验记录内容

【原文】试验过程中应通过试验记录设备至少记录以下内容：

——试验时间轴；

——试验车辆纵向速度；

——记录试验车辆的试验里程和试验时长；

——试验车辆周边环境视频信息。

【说明】试验过程需要测试机构安装试验设备记录，保证后续数据的可溯源性，当出现争议的匿名化目标物和结果时，可通过加装的记录设备为判定依据提供支撑。

2.11 C.2.4 试验结果标注能力要求

【原文】在开展C.6.1的图片标注处理前，应对匿名化目标标注能力进行评估且满足以下要求：

——若人脸或汽车号牌边界框的范围可覆盖匿名化区域，有无原始图片的交并比误差为±5%；

——若人脸或汽车号牌边界框的范围不完全覆盖匿名化区域，有无原始图片的交并比误差为±10%。

其中，用于评估标注能力的人脸和汽车号牌目标数量应分别不少于500个。

【说明】由于试验过程无法提供真值比对，故对于测试机构的匿名化图片标注能力提出要求。在标注匿名化处理图片前，可以通过使用具有真值的匿名化图片库进行标注能力训练和测试，只有满足要求的标注系统和标注人员可以开展匿名化图片标注，保证标注结果的一致性。通过多位具备丰富的标注人员评估得出标准的相关参数。该条款将作为标注能力的基本要求。

2.12 C.4 匿名化处理性能要求试验过程

【原文】试验过程可分单次完成或多次完成。

【说明】为保证不对技术路线进行限制，本文件内不对车辆是否实时上传数据及通过何种方式上传数据提出要求，企业可根据自身外发链路对匿名化结果进行上传，实时上传、分次、分阶段上传或试验结束后上传数据均被允许。

2.13 C.5.2 试验速度要求

【原文】除C.5.2.2和C.5.2.3情形外，根据匿名化处理及向车外传输相关功能的开启条件中最大开启速度T1和最小开启速度T2选取采集的速度范围，试验过程应至少在以下关键速度范围内采集匿名化结果。

【说明】通过行业调研，车辆在不同速度下，由于抖动、采集频率等因素影响，对于图片匿名化效果存在差异，如果车辆多速度范围内可开启功能，试验速度选择也应该覆盖不同速度段。

（三）主要试验（或验证）情况分析

3.1 试验综述

2022 年 8 月-9 月《智能网联汽车数据通用要求》标准起草组征集试验车辆和检测机构，共征集到 2 家具备匿名化解决方案的企业（小鹏汽车与百度）和一家检测机构（中汽研汽车检验中心（天津））共同开展验证试验，同时面相所有参与标准制定单位征集匿名化处理结果，计划通过现场试验方式完成本次验证试验。2022 年 9 月至 10 月先后完成两家企业测试车辆的标准验证试验，并委托中汽研汽车检验中心（天津）集中对试验结果进行处理，总结试验过程中的经验和问题，进一步完善标准草案。

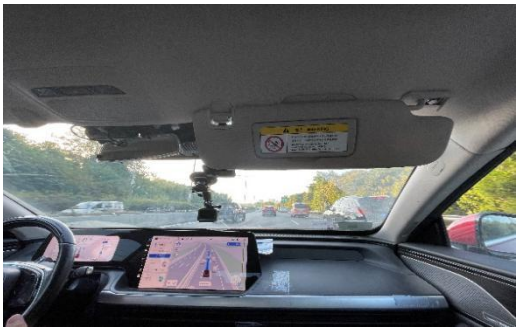
3.2 试验过程及结论

（1）实车试验结果

标准验证试验于 10 月 14 日、10 月 21 日分别于北京、广州对小鹏、百度提供的测试车辆进行测试。依据标准要求，试验人员首先确定试验关键速度区间、车辆所搭载的视觉传感器位置和所采集数据向外部输出的方式。试验开始后，于设定路线正常行驶，行驶过程中同步开启车外信息采集、记录和传输功能。试验结束后，读取车端数据并通过数据抽帧、数据标注等方式计算匿名化结果的检出率、误检率，评估匿名化效果的不可识别性。被测车辆情况如表 1 所示，试验过程如图 1 至图 6 所示。

表 1 实车试验结果

序号	试验过程说明
1	采集图像范围：前向、左侧向、右侧向、后向共 4 个摄像头； 输出物：图片 分辨率：1828*948 和 1280*960 可开启条件：仅在快速路和高速触发 记录时间：数据采集时间共 1.5 天 道路类型：城区、高速、快速路
2	采集图像范围：前视 输出物：视频 分辨率：1920*1080 采集速度：30、40、50、60km/h 道路类型：城区 记录时间：0.5 天

试验结果：被测车辆均可通过车端采集对图像进行匿名化处理，但由于开启条件差异，部分测试车辆收集图片速度较慢，按照该技术方案试验需进行 1-2 月。通过与技术支持人员沟通，形成通过调整程序适当放宽上传条件方案，最终实现图片的快速收集，并通过比对匿名化结果，放宽开启条件未对匿名化效果产生影响。试验结束后，通过对试验结果的分析，可以实现在无原始图片的前提下对于匿名化的检出率、误检率进行评估，试验方法具备可操作性。

五、是否涉及专利等知识产权问题

本文件不涉及专利。

六、重大意见分歧的处理依据和结果

无。

七、实施标准的措施建议

无。

八、其他需要说明的事项

无。