

强制性国家标准

《汽车数据安全技术要求》

（征求意见稿）

编制说明

2026年9月

目 次

一、 工作简况 1

二、 编制原则、强制性国家标准主要技术要求的依据及理由 4

三、 与有关法律、行政法规和其他标准的关系 16

四、 与国际标准化组织、其他国家或者地区有关法律法规和标准的比对分析 16

五、 重大分歧意见的处理过程、处理意见及其依据 16

六、 对强制性国家标准自发布日期至实施日期之间的过渡期的建议及理由 16

七、 与实施强制性国家标准有关的政策措施 17

八、 是否需要对外通报的建议及理由 17

九、 废止现行有关标准的建议 17

十、 涉及专利的有关说明 17

十一、 强制性国家标准所涉及的产品、过程或者服务目录 18

十二、 公平竞争审查情况及结论说明 错误！未定义书签。

十三、 其他应当予以说明的事项 18

强制性国家标准《汽车数据安全要求》（征求意见稿）

编制说明

一、工作简况

1.1 任务来源

依据国家标准化管理委员会下达的国标委发〔2026〕19号文件，编号为20261957-Q-339的标准制定项目，制定强制性国家标准《汽车数据安全要求》。

该标准由中华人民共和国工业和信息化部提出并归口，委托全国汽车标准化技术委员会智能网联汽车分技术委员会组织开展修订工作。

1.2 修订背景

随着汽车智能化、网联化水平的持续提高，汽车全生命周期内产生的数据量呈现爆发式增长，涵盖车辆运行数据、用户个人信息以及道路环境数据等多个方面。通过对汽车数据的大规模训练与处理，不仅能够为用户提供更个性化、智能化的服务，提升用户体验，还可为智能网联汽车的发展提供坚实的数据支撑。依托海量数据训练，系统在环境感知、分析决策等方面的准确性与实时性得以增强，从而提升行车安全水平，并显著推动自动驾驶技术的进步与创新。

国家层面已相继出台《智能汽车创新发展战略》《关于印发车联网网络安全和数据安全标准体系建设指南的通知》《关于加强智能网联汽车生产企业及产品准入管理的意见》等一系列政策与规划，明确要求加强数据安全监管，制定并完善相关标准。汽车数据不仅涉及用户隐私安全，一旦泄露可能导致用户遭受诈骗、骚扰、声誉损害等风险，同时也关乎国家安全，如关键道路信息、交通流量数据、OTA源代码、控车指令等若被窃取或篡改，将对国家交通基础设施安全、社会公共安全等构成严重威胁。

近年来，汽车数据安全事件频发。国内外多家车企云平台发生数据泄露，部分企业甚至遭遇勒索，涉及数百万用户个人信息；还有企业车内视频被公开或可被其他同款车型车主随意查看。在国家安全层面，已有企业因违反《网络安全法》《数据安全法》《个人信息保护法》而被处以重罚，另有企业因违规出境汽车数据遭五部委联合约谈。

当前，部分市场在售汽车在数据收集、存储、传输等环节仍缺乏统一规范与有效安全防护措施，导致数据泄露事件时有发生。因此，制定汽车数据安全强制性国家标准显得尤为迫切。该标准可从源头上规范汽车数据处理活动，保障用户数据安全与国家安全，同时通过加强数据治理，有效防范数据泄露与滥用风险，推动智能网联汽车产业健康、可持续发展。

近年来，随着汽车智能网联化水平不断提升和电动化转型持续加速，以智慧座舱、大数据、人工智能为代表的多种应用场景不断涌现，充分释放出数据要素价值。车企纷纷加大在智能化场景的投入与布局，并不断提升汽车数据保护能力。2021年，《数据安全法》和

《个人信息保护法》相继出台，为后续法规与标准的制定提供了明确指引。同年，国家网信办等五部委联合发布《汽车数据安全若干规定（试行）》，以法规形式明确汽车数据处理器应依法合规开展数据处理活动，并提出具体的安全保护要求，同时建立年度报告上报机制，推动各地汽车企业上报自身汽车数据处理情况。

2022年12月，工信部印发《工业和信息化领域数据安全管理办法（试行）》，明确了包括汽车行业在内的工业和信息化领域数据合规处理与利用要求，提出重要数据目录备案制度，并针对十余家汽车企业组织开展了试点评估。2023年11月，工信部联合多部门发布《关于开展智能网联汽车准入和上路通行试点工作的通知》，旨在推动智能网联汽车生产与使用主体加强能力建设，支持相关法律法规及技术标准修订，加快完善智能网联汽车准入管理和道路交通安全管理体系。目前，首批9个智能网联汽车准入试点联合体已进入试点实施阶段。

综上所述，我国汽车产业在数据安全发展方面已积累丰富实践经验。车企、零部件供应商等企业在研发、生产、市场推广等环节，均已深刻认识到数据安全保护的重要性和必要性。尽管在实施标准过程中会短期内增加企业生产经营成本，但从长远看，通过提升产品质量、降低安全事件损失、实现规模效应等途径，能够有效抵消初期投入，并创造额外经济效益。同时，安全标准的实施对保障公共安全、提升社会整体福利意义重大，其社会效益远高于企业短期成本的上升。我国在汽车数据安全标准建设方面具备良好的产业基础、日趋成熟的技术支撑、合理的成本效益预期以及扎实的研究条件，考虑到产业管理与发展的迫切需求，制订强制性国家标准《汽车数据安全要求》势在必行。

1.3 主要工作过程

1.3.1 编制工作启动

为了顺利推进智能网联汽车标准体系建设，全国汽车标准化技术委员会智能网联汽车分技术委员会根据单位申请情况组建了标准起草项目组。

1.3.2 工作组会议讨论情况

1.3.3.1 工作组第一次会议

2025年9月16日在芜湖召开了《汽车数据安全要求》标准起草组启动会暨第一次讨论会议。来自整车企业、零部件供应商和检验检测机构等34家单位的专家和代表参加会议。在会议上，奇瑞汽车股份有限公司、中国第一汽车股份有限公司、广州小鹏汽车科技有限公司和比亚迪汽车工业有限公司的专家分享了企业数据安全实践经验，来自中汽智能科技（天津）有限公司的专家分享了《汽车数据安全要求》的建议框架。与会专家围绕该标准与现有汽车数据安全标准体系的协调关系、对数据安全相关法律法规的支撑作用以及企业保障能力与车型技术要求的具体条款等展开讨论，为本标准的后续工作规划、制定思路及具体技术要点贡献了建设性意见。

1.3.3.2 工作组第二次会议

2025年11月13日在南昌召开了《汽车数据安全要求》标准起草组第二次讨论会议。

来自整车企业、零部件供应商和检验检测机构等 34 家单位的专家和代表参加会议。与会专家围绕汽车数据安全保障能力、汽车数据安全基本要求及汽车数据安全技术要求展开深入讨论，重点就数据范围界定、企业准入与标准衔接、数据出境条款设置、个人信息同意与撤回机制、数据收集提示形式、存储与删除要求、匿名化处理等方面提出了建设性意见。

1.3.3.3 工作组第三次会议

2026 年 1 月 14 日在长春召开了《汽车数据安全要求》标准起草组第三次讨论会议。来自整车企业、零部件供应商和检验检测机构等 34 家单位的专家和代表参加会议。本次会议由各章条牵头单位当前版本草案内容及问题，各参会单位专家讨论建议。与会专家对汽车数据安全保障能力及汽车数据安全基本要求相关内容的协调性，汽车数据安全技术要求各项要求的合理性与可实现性进行充分讨论，会议建议汽车数据安全保障能力及汽车数据安全基本要求两章牵头单位联合讨论并修改相关内容，以提高标准要求的协调性，并针对汽车数据安全技术要求中难以确定的问题开展行业调研，并依据调研结论修改调整草案。

1.3.3.4 第四次工作组会议

2026 年 3 月 24 日-25 日在北京召开了《汽车数据安全要求》标准起草组第四次讨论会议。来自整车企业、零部件供应商和检验检测机构等 34 家单位的专家和代表参加会议。本次会议由各章条牵头单位介绍汽车数据安全基本要求及汽车数据安全技术要求两章的草案调整情况，各单位针对草案变化内容展开讨论，梳理标准要求逻辑，安排各章条牵头单位按讨论结论修改草案。此外，中汽中心介绍了行业调研的基本情况，经与会单位讨论，确定各项问题的处理结论，安排各章条牵头单位按照本次会议中形成的结论修改草案，由检测机构补充检验及测试方法。

1.3.3.5 第五次工作组会议

2026 年 4 月 21 日-23 日在无锡召开了《汽车数据安全要求》标准起草组第五次讨论会议。来自整车企业、零部件供应商和检验检测机构等 34 家单位的专家和代表参加会议。本次会议由中汽中心及中汽智能科技（天津）有限公司相关专家逐条介绍各章条要求及对应的检验与测试方法，各参会单位提出问题并展开讨论。与会专家对标准全文的术语定义、描述用词、前后对应关系、标准要求与检验、测试方法的对应性方面提出了建设性意见和建议，并安排各章条牵头单位会后按照本次会议中形成的结论修改草案。

1.3.3.6 第六次工作组会议

2026 年 5 月 20 日-21 日在南京召开了《汽车数据安全要求》标准起草组第六次讨论会议。来自整车企业、零部件供应商和检验检测机构等 34 家单位的专家和代表参加会议。与会单位围绕数据处理活动清单、数据安全目标、风险评估方法、告知同意机制、个人信息处理规则、合作方管理、权限管理、生物识别信息存储、车外图像视频匿名化处理、删除机制及检验方法等具体条款提出了建设性意见和建议，并安排各章条牵头单位会后按照本次会议中形成的结论修改草案后启动起草组征求意见。

1.3.3.7 第七次工作组会议

2026年6月23日-24日在长春召开了《汽车数据安全要求》标准起草组第七次讨论会议。来自整车企业、零部件供应商和检验检测机构等38家单位的专家和代表参加会议。与会单位针对起草组内征集的意见进行了逐项讨论，重点就汽车数据处理活动清单模板、数据安全概念、监测及记录能力要求、生物识别信息存储、敏感个人信息及重要数据传输保密性措施、车外图像视频匿名化处理、同意豁免条款及检验与测试方法提出建设性意见及建议，并安排检验检测机构就同一型式判定条件开展进一步研究，后续由各章条牵头单位会后按照本次会议中形成的结论修改草案后启动工作组征求意见。

1.3.3.8 第八次工作组会议暨工作组征求意见处理会议

2026年7月20日-21日，面向汽标委智能网联汽车分标委汽车数据标准工作组征求意见，收到33家单位的反馈意见共485条。7月20日-21日召开意见处理会，来自整车企业、零部件供应商和检验检测机构等38家单位的专家和代表参加会议，与会单位针对工作组内征集的意见进行了逐项讨论与处理，其中采纳40条，部分采纳90条，不采纳355条。

1.3.3.9 第九次工作组会议

2026年8月11日召开同一型式判定条件及实施日期专项研讨会，邀请工信部装备工业发展中心参与研讨，来自整车企业、零部件供应商和检验检测机构等共43家单位的专家和代表参加会议，与会单位针对同一型式判定条件及实施日期进行了逐项讨论与处理，会后按照本次会议中形成的结论修改草案。

1.3.3.10 第十次工作组会议

由于国家标准《汽车重要数据识别技术规范》立项进度延后，2026年8月12日召开汽车重要数据目录专项研讨会，来自整车企业、零部件供应商和检验检测机构等共42家单位的专家和代表参加会议，与会单位针对汽车重要数据目录草案在工作组内征集的165条意见进行了逐项讨论与处理，其中采纳43条，部分采纳40条，不采纳82条，会后按照本次会议中形成的结论修改草案，形成公开征求意见材料。

二、编制原则、强制性国家标准主要技术要求的依据及理由

2.1 标准编制原则

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，参考了《数据安全法》《个人信息保护法》《网络数据管理条例》《汽车数据安全若干规定（试行）》《工业和信息化领域数据安全管理办法（试行）》《互联网应用程序个人信息收集使用规定（征求意见稿）》，充分考虑国内现有相关规定与本标准的统一和协调；并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，还通过验证试验，对检验及测试方案的可行性进行了验证，确定了本标准主要的技术要求及检验与测试方法。

2.2 标准主要内容说明

本标准主要由范围、术语和定义、汽车数据安全保障要求、汽车数据安全基本要求、汽车数据安全技术要求、汽车数据安全保障要求检验方法、汽车数据安全基本要求检验方法、汽车数据安全技术要求测试方法及规范性附录等组成，具体内容及核心条款内容说明如下：

2.2.1 范围

【原文】本文件规定了汽车数据安全保障要求、基本要求、技术要求及同一型式判定，描述了相应检验与测试方法。

本文件适用于M类及N类车辆，不适用于基于已获得型式批准的二类底盘或整车改装的专用汽车。

注：本文件所涉及的汽车数据指车辆制造商在汽车产品的研发设计和生产制造过程中产生、处理的个人信息及重要数据以及汽车产品产生、处理的个人信息及重要数据。

【说明】本文件提及的“汽车数据”的范围与本章“注”中的范围一致。

2.2.2 安全保障要求（第4章）

【原文】4.1 车辆制造商应建立并实施汽车数据安全管理制度，明确汽车数据安全管理制度目标与方针，确定适用范围，识别并协调与数据安全有关或相互作用的领域，并通过相应规则和过程落实管理要求。

【说明】在车辆制造商进行汽车数据安全管理制度时，可能会与质量管理、汽车网络安全管理、信息安全管理、个人信息管理等相关领域有交叉或引用关系，因此车辆制造商应识别并协调与数据安全有关或相互作用的领域。

【原文】4.2 车辆制造商应建立汽车数据安全组织架构，明确相关职责及资源保障，建立并实施人员能力与意识培训、内外部沟通及信息共享制度。

【说明1】车辆制造商明确相关职责，指汽车数据安全组织架构中对应角色的相关职责。

【说明2】本条款要求车辆制造商为实现汽车数据安全提供必要的资源保障，包括但不限于车辆、资金、人员、技术、软硬件设备设施等。

【说明3】信息共享的管理范围包括汽车数据安全信息、汽车数据安全风险、汽车数据安全事件。

【原文】4.7 车辆制造商应建立并实施汽车数据分类分级管理制度，明确分类分级及动态更新要求，建立并实施企业汽车数据管理台账、车型功能汽车数据处理活动清单的管理机制。

【说明】企业汽车数据管理台账，指以企业为对象的汽车数据管理情况的台账，车型功能汽车数据处理活动清单，指以任一具体车型为对象的整车功能汽车数据处理活动清单。

【原文】4.10 车辆制造商应建立并实施汽车数据出境安全管理制度，包括汽车数据出境前内部评估、汽车数据出境法定程序过程管理、汽车数据出境持续跟踪和改进。

【说明】数据出境的相关主管部门已发布多部涉及汽车数据出境管理的法规、部门规章及政策，此处的汽车数据出境法定程序过程管理，特指企业遵照监管部门已发布的法规、部门规章及政策的管理要求进行的汽车数据出境管理工作。

【原文】4.11 车辆制造商应建立并实施汽车数据安全风险和事件的监测与管理制度，包括汽车数据安全监测、汽车数据安全信息分析与评估、汽车数据安全风险管理、汽车数据安全事件管理、汽车数据安全应急预案及演练管理。

【说明】汽车数据安全监测渠道包括车辆制造商内外部。

【原文】4.13 车辆制造商应建立车型汽车数据安全风险评估制度，覆盖风险评估准备、风险识别、风险分析、风险评价、风险评估总结等环节。

【说明】考虑到本标准重点关注车型产品数据安全，因此车型汽车数据安全风险评估制度，是指以车型为对象，针对车型产品的汽车数据安全开展风险评估的管理制度，其在评估范围、评估内容上，与个人信息保护影响评估、重要数据风险评估有所区别。

2.2.3 安全基本要求（第5章）

【原文】5.1 车辆制造商应依据车辆产品功能定义，建立车型功能汽车数据处理活动清单。

【说明】车辆制造商依据产品研发实际进展建立车型功能汽车数据处理活动清单。

【原文】5.2 车辆制造商应依据车辆产品的车型功能汽车数据处理活动清单进行车型汽车数据安全风险评估，分析并识别风险，并对风险采取处置策略，依据处置策略明确各项功能的数据安全目标或声明，并确保数据安全目标或声明覆盖所识别的风险，且已识别的数据安全风险中与第6章要求相关的风险已形成数据安全目标。

【说明1】本条款所要求开展的“车型汽车数据安全风险评估”的方法论需与4.13车辆制造商建立的车型汽车数据安全风险评估制度相匹配。

【说明2】规避风险指通过决定不开始或不继续进行引起风险的活动等消除风险源。

【原文】5.6 车辆制造商应针对车辆产品实施相应措施，具备与车辆数据安全相关的监测及记录能力。

注：车辆数据安全相关的监测包括但不限于摄像头、位置、传声器等传感器调用监测、匿名化处理故障监测。

【说明1】匿名化处理故障监测，指在车端或云端进行监测和记录。

【说明2】匿名化处理故障监测记录，指专项监测记录或搭载此匿名化算法的控制器的故障日志。

【说明3】传感器调用监测，指包含车内外的传感器调用监测。

2.2.4 安全技术要求（第6章）

2.2.4.1 汽车数据处理通用要求（6.1）

【原文】6.1.1 车辆处理个人信息应符合最小必要原则，不应由于用户不同意车辆其他常见功能或非常见功能处理个人信息，而拒绝用户使用该项常见功能，车辆常见功能及其必要个人信息范围见附录 B。

【说明】附录 B 明确了车辆常见功能及其必要个人信息范围，车辆使用基础功能时所需收集的必要个人信息不得超出附录 B 中的要求，且各功能之间的授权不能互相影响。以基础地图导航功能为例，若用户不同意车辆处理语音交互功能所必需的个人信息，不能影响基础地图导航功能的使用。

【原文】6.1.3 当车辆涉及 6.1.2 的告知内容发生变化时，车辆应更新个人信息处理规则，并通过产品使用说明书、车载显示终端、语音、短信、汽车使用相关应用程序等任一显著方式向用户告知更新的具体内容。

【说明】车辆所有个人信息处理功能告知内容发生变化时均需要向用户告知更新的具体内容。

【原文】6.1.4 车辆如搭载应用程序下载平台，应在应用程序下载页面，清晰准确展示下列信息：

- 应用程序运营者名称或姓名、联系方式；
- 应用程序主要功能介绍；
- 应用程序运行所需具体权限列表；
- 个人信息处理规则文本或者链接。

【说明】应用程序下载平台主要指的在车端可以通过该平台进行新功能下载或使用的功能，主要包括车端应用商店、车端应用市场等。

【原文】6.1.6 车辆应记录和集中展示功能调用摄像头、位置、传声器等传感器的情况，并告知记录规则。

注：记录规则包括记录的传感器类型、传感器调用情况、统计期限、记录保存期限等。

【说明】统计期限指统计传感器调用情况的时间周期，记录保存期限指传感器调用记录在车端保存的期限。车辆制造商可结合功能情况自行定义记录规则中的统计期限及记录保存期限。

2.2.4.2 个人同意一般要求（6.2）

【原文】6.2.1.1 车辆处理个人信息应取得个人同意，处理敏感个人信息应取得单独同意。基于个人同意处理个人信息的情况，若用户拒绝，车辆不得在 48 小时内重新主动申请，切换未进行告知及取得同意的账户、系统重置等情况除外。

【说明 1】车辆处理敏感个人信息应按表 A.2 敏感个人信息分类表中的敏感个人类型取得单独同意。

【说明 2】车辆主动申请个人同意的情形不包括用户主动启动相关功能时应进行的个人信息处理同意。

【原文】6.2.1.2 车辆向第三方提供个人信息前，应按功能取得用户的单独同意。

【说明】第三方指用户、功能运营主体及功能运营主体委托数据处理者以外的组织或个人。

【原文】6.2.3 车辆应按以下要求设置个人同意及拒绝的选项：

——提供自愿、明确的同意和拒绝的方式；

——申请车内摄像头、位置、车内传声器等权限时，以功能为单位，按每项功能所需处理的敏感个人信息逐一取得用户的单独同意；

——通过用户画像、自动化决策等方式处理个人信息并用于服务及体验提升的功能，具备独立、便捷的拒绝方式；

——提供自主设定处理敏感个人信息同意期限的途径，且期限不为仅始终允许或永久。

【说明1】功能的开启与关闭的操作方式不视为同意和拒绝的方式。

【说明2】允许车辆提供的设定处理敏感个人信息同意期限选项包含始终允许或永久。

【原文】6.2.5.2 撤回个人同意，不应影响撤回前基于个人同意已进行的车辆处理个人信息活动的效力。

【说明】用户撤回个人同意前基于个人同意已进行的车辆处理个人信息的活动仍具备相应效力。

2.2.4.3 汽车数据收集要求（6.3）

【原文】6.3.1 除非用户自主设定或符合6.2.2规定的例外情形，车辆应默认设定为不收集个人信息的状态。

【说明】车辆出厂时应默认设定为不收集个人信息的状态，除非用户主动进行设定或符合6.2.2规定的例外情形。车辆弹窗默认勾选同意个人信息处理规则也不视为符合本条款要求。

【原文】6.3.2 车辆收集位置信息及座舱数据中敏感个人信息应提示收集状态，具体要求如下：

——通过产品使用说明书、车载显示终端、语音、短信、汽车使用相关应用程序等方式告知用户不同提示信号和敏感个人信息类型的对应关系；

——在收集期间至少通过光学、声学或触觉信号等方式提示，直至收集结束；

——同种提示方式下，不同种类敏感个人信息的提示以不同形式区分；

——符合6.2.2规定的例外情形不提示收集状态。

【说明】6.3.2对敏感个人信息收集状态的提示方式作出规定。考虑到位置信息和座舱数据属于对个人权益影响较大的敏感个人信息，标准要求车辆必须以至少一种可直接感知的方式向用户提示当前的收集状态，确保用户能够实时知悉相关敏感个人信息的收集情况。同时，为避免提示信息混淆，要求同种提示方式下不同种类敏感个人信息应以不同形式区分提

示，如示例所示的图标区分或颜色区分方式。对符合 6.2.2 要求常态收集的信息进行了额外要求，避免一直提示但无法关闭对用户造成干扰及误导。

【原文】6.3.3 车辆制造商应根据所提供功能服务对数据精度的需求确定车辆摄像头、激光雷达、4D 毫米波雷达等的覆盖范围、分辨率。

6.3.4 因同一数据收集设备支持多个功能服务且所需数据精度要求不同时，车辆应至少有一个功能服务符合 6.3.3 要求。

【说明】本条款依据《汽车数据安全若干规定（试行）》中第六条“精度范围适用原则”制定，要求车辆配备摄像头、激光雷达、4D 毫米波雷达等传感器的相应参数需与功能的数据精度需求相匹配。

【原文】6.3.5 车辆无相关功能或未激活相关功能时，不应调用摄像头、位置、传声器等非必要权限或收集非必要个人信息。

【说明】本条款旨在防止车辆以软件升级功能预留、后台服务等名义未使用到对应功能前提前获取授权或收集非必要个人信息，细化 6.3.1 的“默认不收集”要求。

【原文】6.3.6 车辆不应以个人信息主体不同意收集其个人信息或者撤回同意为由，拒绝提供不需处理个人信息或仅在车内处理车辆识别代号即可实现的功能。

注：车辆不需处理个人信息或仅在车内处理车辆识别代号即可实现的功能包括但不限于启动、制动、转向、换挡、车载无线广播接收系统、雨刮控制、车灯控制、空调、音量控制、间接视野装置调节、车门开启、车门关闭、前后舱盖开启、前后舱盖关闭、座椅调节、座椅通风、座椅加热、方向盘调节、方向盘加热及仪表显示等。

【说明】本条款规定了车辆基本功能与个人信息处理同意之间的独立性要求。无论用户是否同意处理个人信息，车辆必须提供车辆已配备的不需处理个人信息或仅在车内处理车辆识别代号即可实现的功能。

2.2.4.5 汽车数据使用要求（6.5）

【原文】6.5.1 车辆基于个人同意处理生物特征识别信息的，使用生物特征识别信息进行身份识别时，应同时提供不基于生物特征识别信息的其他身份识别方式。

【说明】本条款参考《人脸识别技术应用安全管理规定（试行）》第十条制定，车辆使用生物识别特征信息进行身份识别时，如人脸登录、指纹登录等，应同时提供不基于生物特征识别信息的登录方式，如账号口令登录、二维码扫描登录等。

【原文】6.5.2 车辆在显示、输入或设置网络支付平台登录口令、支付口令（包括网络支付交易口令、快捷支付口令、银行卡支付口令等）时应提供隐藏全部或部分信息的方式。

【说明】该条款仅针对网络支付平台登录口令、支付口令提出要求，蓝牙配对码、WIFI 登录密码等不属于标准要求范围内。

2.2.4.6 汽车数据传输要求（6.6）

【原文】6.6.1.2 车辆应对向车外发送的重要数据及敏感个人信息实施保密性保护措施。

【说明】通信通道加密也视为一种保密性保护措施。

【原文】6.6.1.3 因保证行车安全和财产安全需要，无法取得个人同意收集到车外个人信息且向车外传输的，应在车端进行匿名化处理，包括删除含有能够识别自然人及汽车号牌信息的画面，降低分辨率使得无法识别自然人及汽车号牌信息或者对画面中的人脸信息和汽车号牌信息等进行局部轮廓化处理等，匿名化处理应符合 6.6.2 的要求。匿名化处理完成后，过程数据不应向车外提供。

【说明 1】本条款要求车辆具备的匿名化处理能力指车辆整体的匿名化处理能力，不区分功能、控制器。

【说明 2】向车外传输的方式包括但不限于蜂窝通信、近场通信、有线或接口连接等。

【原文】6.6.2.1.1 车辆至少应对图像或视频中满足以下要求的人脸目标进行匿名化处理：

- 人脸边界框最小边长像素大于等于 28 像素；
- 人脸边界框内可见范围比值大于 50%且可见范围内眼睛、鼻子或嘴清晰可见。

【说明】经统计分析，人脸边界框最小边长像素大于等于 28 像素，小于 32 像素的人脸目标仍可识别该自然人身份，且近年行业整体技术能力逐步提升，故提高相应匿名化处理技术指标。

【原文】6.6.2.1.2 车辆至少应对图像或视频中满足以下要求的汽车号牌目标进行匿名化处理：

- 汽车号牌边界框最小边长像素大于等于 16 像素；
- 汽车号牌目标内可见范围比值大于 50%且可识别数字及文字内容。

【说明】车牌目标参数同时满足上述条件作为应检对象。

2.2.4.7 汽车数据删除要求（6.7）

【原文】6.7.4 若车辆存在账号管理功能，车辆应为用户提供车内删除账号个人信息功能。用户在车辆启动本地账户个人信息删除功能后，车辆应删除或匿名化处理车内存储的该账号相关个人信息，法律、行政法规、部门规章、强制性国家标准另有规定的除外。

【说明 1】车辆的账号管理功能不包含第三方应用程序的账号管理功能。

【说明 2】车机恢复出厂设置不视为删除账号个人信息功能。

2.2.5 汽车数据安全管理体系检查方法（第7章）

2.2.5.1 检验方法（7.2）

【原文】7.2.5 汽车数据安全合作方管理检验

检验人员应检验车辆制造商是否具备汽车数据安全合作方管理制度，是否涵盖汽车数据安全相关产品开发合作方和数据处理合作方，是否具备能力评估及核验、需求下发、数据安全协议签署和履行情况监督等要求，是否具备汽车数据安全产品开发合作方和数据处理合作方的合作方汽车数据安全记录，判定是否满足4.5的要求。

【说明】需求下发记录，指车辆制造商下发给数据处理合作方或数据安全相关产品开发合作方的数据安全需求文件。

【原文】7.2.10 汽车数据出境管理检验

检验人员应按照以下方法开展检验并验证，判定是否满足4.10的要求：

a) 检验是否具备汽车数据出境管理制度，是否具备汽车数据出境前内部评估、汽车数据出境法定程序过程管理、汽车数据出境持续跟踪和改进要求，是否具备汽车数据出境管理记录；

b) 检验汽车数据出境管理制度是否符合现行法律法规和部门规章要求。

【说明】本条款所述持续跟踪和改进要求覆盖数据出境期限到期、目的变更、接收方变更、数据量级变化、法律环境变化等触发条件，并保留跟踪记录及整改记录。

【原文】7.2.12 车辆全生命周期汽车数据安全管理体系检验

检验人员应按照以下方法开展检验并验证，判定是否满足4.12的要求：

a) 检验是否具备车辆项目的数据安全管理制度，是否具备职责分配、数据安全计划、裁剪、数据安全档案、数据安全评估、后开发的发布等要求，是否具备车辆项目的数据安全记录；

b) 检验是否具备车辆项目的全生命周期数据安全工程活动管理制度，是否具备功能定义、数据处理活动分析、风险评估、数据安全目标和声明、数据安全概念、安全需求开发、集成和验证、数据安全确认、生产控制管理、事件监测处置、支持终止及功能废止等活动的要求，是否具备车辆项目的全生命周期数据安全工程活动管理记录。

【说明】数据安全概念指数据处理及其操作环境的安全需求，以及数据安全控制措施相关信息的集合。

2.2.7 汽车数据安全技术要求测试方法（第9章）

2.2.7.1 汽车数据安全测试条件准备（9.2.2）

【原文】9.2.2.1 车辆制造商依据9.2确定的测试范围，提供必要的测试输入支持完成测试，具体包括：

a) 测试环境应无信号干扰，车辆应处于正常上电、可运行状态，数据安全被测功能应处于开启状态；

- b) 车辆制造商应提供车辆首次处理个人信息状态恢复方式；
- c) 车辆制造商应提供车辆个人信息处理情况变化方法、个人信息告知内容变化方法以及期限届满到达方式；
- d) 车辆制造商应提供应用程序下载平台清单以及应用程序下载平台下载页面展示规则；
- e) 车辆制造商应提供导出并解码所收集的原始车辆数据的方法；
- f) 车辆制造商应提供支持测试实施所需的预装汽车数据处理功能相关软件安装包及相关技术资料；
- g) 车辆制造商应提供涉及汽车数据处理的系统的接入方式和调试权限；
- h) 车辆制造商应提供处理流程、权限策略、脱敏/加密方案、硬件安全模块安装位置说明文档等测试支撑材料；
- i) 车辆制造商应提供传输数据包的数据解密方式；
- j) 车辆制造商应提供测试登录账号。

【说明 1】车辆制造商应提供的导出并解码所收集的原始车辆数据，主要指的是通过车辆摄像头采集的原始视频或图像数据。

【说明 2】车辆制造商应提供支持测试实施所需的预装汽车数据处理功能相关软件安装包及相关技术资料。相关软件安装包例如，车辆独立应用程序以及系统应用程序的 APK 安装包等；相关技术资料包括但不限于预装汽车数据处理功能相关软件的 API 调用接口、相关证书等。

2.2.7.2 汽车数据传输要求测试（9.8）

【原文】9.8.1 座舱数据车内处理测试方法

测试人员应按照车辆制造商提供的车型功能汽车数据处理活动清单、数据解密方式、车辆处理个人信息的系统的接入方式和调试权限，选取除所列例外情形外需要向车外提供座舱数据的功能，启动相应功能，测试车辆是否发出向车外提供座舱数据的个人同意请求，在功能运行期间使用车辆制造商提供的端口和访问权限使用网络数据抓包工具进行数据抓包，利用工具分析其中是否存在座舱数据，记录测试结果，判定车辆是否符合 6.6.1.1 的要求。

【说明】本条需要遍历车辆制造商提供的车型功能汽车数据处理活动清单中所有涉及座舱数据的功能（除所列例外情形外）。如所有涉及向车外提供座舱数据的功能在未取得个人同意的情况下，均未向车外传输座舱数据，视为满足本条款要求。

【原文】9.8.2 重要数据及敏感个人信息车外传输保密性保护测试方法

测试人员应按照车辆制造商提供的车型功能汽车数据处理活动清单、涉及汽车数据处理的系统的接入方式和调试权限，触发车辆向外传输重要数据及敏感个人信息的功能，使用车辆制造商提供的端口和访问权限抓取传输的数据包，测试是否对车辆传输的重要数据及敏感个人信息进行加密，判定车辆是否符合 6.6.1.2 的要求。

【说明】本条通过抓取通讯数据包，检查是否使用加密算法或通信通道加密对车辆传输的重要数据及敏感个人信息进行加密。本条不对加密算法的强度进行要求。

【原文】9.8.3 车外视频图像车外传输匿名化处理测试方法

测试人员应按照车辆制造商提供的车型功能汽车数据处理活动清单，启动符合 6.6.1.3 所规定情形的相应功能，测试车辆对外传输的车外个人信息是否进行匿名化处理，记录测试结果，判定车辆是否符合 6.6.1.3 的要求。

9.8.4 匿名化要求测试方法

【说明】收集车外视频图像且向车外传输的相关功能需要满足本条款要求。本条款规定了匿名化处理性能要求的测试过程要求、匿名化处理性能要求测试结束条件（其中包括了测试历尽性的要求，需要对车辆所有涉及匿名化处理功能的摄像头进行数据采集和分析，若车辆采用不同类的匿名化算法，需要每一种类型均开展试验进行测试）、测试结果处理要求、匿名化效果评估要求。依据车辆制造商提供的匿名化处理策略，试验输入会有不同，如处理策略为传输为裁剪后的视频图像，则应提供裁剪前对应的匿名化后的视频图像；如若匿名化处理方式为删除帧、降低分辨率等技术手段，则应提供原始视频图像。

【原文】9.8.4.2.3 若匿名化处理方式为裁剪、删除帧、降低分辨率等技术手段，应提供技术手段处理后对应的视频图像，满足以下要求，并按照 9.8.4.4 的测试方法进行处理：

- 若测试车辆输出图片，图片收集时间间隔大于等于 2s 的图片数量不少于 500 张；
- 若测试车辆输出视频，每段视频时长不少于 10s，所有视频总时长不少于 1000s；
- 收集的数据应包括 9.2.3 所列各传感器收集的图片或视频，各传感器对应的被测图片应不少于 10 张或视频应不少于 20s；
- 若匿名化处理方式为降低分辨率，要求人脸目标数量和汽车号牌目标数量均不少于 200 个，其中相同人脸目标在不同图片内分别计数。
- 收集的数据应包括 9.2.3 所列各传感器收集的图片或视频，各传感器对应的被测图片应不少于 10 张或视频应不少于 20s，且至少包含需要进行匿名化处理的 1 个人脸目标或 1 个汽车号牌目标。

【说明 1】图片收集时间间隔大于等于 2s 与 9.8.4.3.1 测试数据读取每 2 秒提取图片数量应不多于 1 张的要求一致。

【说明 2】对匿名化处理方式的类别进行描述，并对同一车辆的不同匿名化处理方式的采集最小数据集提出要求。

【原文】9.8.4.4 裁剪、删除帧、降低分辨率技术测试结果处理

【说明】对除轮廓化处理以外的匿名化方式提出专项测试方法。

【原文】9.8.4.5.1.1 人脸不可识别性测试方法

选择两种具备人脸识别功能的算法模型对计入人脸目标正检数的所有匿名化目标进行识别，判定是否符合 6.6.2.2.2 要求。

【说明】删除开源模型、公安模型的举例，避免误导生产企业匿名化算法技术路径的确定。

【原文】 9.8.4.5.1.2 选择两种具备数字、字母、文字识别功能的算法模型对计入汽车号牌目标正检数的所有匿名化目标进行识别，判定是否符合 6.6.2.2.2 要求。

【说明】删除对 CRNN 算法等举例，避免误导生产企业匿名化算法技术路径的确定。

2.2.7.3 汽车数据删除用要求测试（9.9）

【原文】9.9.1 个人信息删除途径测试方法

测试人员应按照车辆制造商提供的个人信息的功能清单，选取个人信息存储在车端的功能，通过调试接口和数据存储地址确认个人信息数据内容，若数据进行了加密需要根据企业提供的解密方法进行解密确认个人信息数据内容，根据车辆向用户提供的删除车辆本地个人信息的途径或方式尝试删除个人信息，测试删除情况，记录测试结果，判定车辆是否符合 6.7.1 的要求。

【说明】车辆向用户提供的删除车辆本地个人信息的途径或方式包括但不限于恢复出厂设置、注销账号、删除按钮等。

【原文】9.9.2 特定情形个人信息删除测试方法

测试人员应按照车辆制造商提供的个人信息的功能清单，选取汽车数据存储在车端的相关功能，通过调试接口和数据存储地址确认个人信息数据内容，若数据进行了加密需要根据企业提供的解密方法进行解密确认个人信息数据内容，测试在车端存储个人信息的车辆功能是否进行了删除，判定车辆是否符合 6.7.2 的要求。测试应确认以下信息：

- a) 判定删除方式是否为车辆主动删除、匿名化处理或个人请求进行删除；
- b) 各功能是否具备清晰的删除个人信息的规则；
- c) 删除个人信息的规则说明至少包括 6.7.2 规定的 5 项情形；
- d) 各功能进行个人撤回同意操作后，测试是否在车端已删除，若未删除，查找是否存在用户请求删除个人信息的途径；
- e) 该功能涉及收集的数据包含无法在车端删除的个人信息，车辆制造商是否提供相关声明文档，说明申请删除后该个人信息不再进行除存储和必要的安全保护措施外的其他处理活动。

【说明】本条款所述必要的安全措施包括但不限于加密、匿名化、访问控制等。如企业无法实现个人撤回同意操作后删除个人信息，但可以提供请求删除个人信息的途径，则能满足本条款的要求。

【原文】9.9.3 删除的汽车数据不可检索、不可访问测试方法

测试人员应按照车辆制造商提供的汽车数据处理功能清单，选取汽车数据存储在车端的相关功能通过调试接口和数据存储地址确认个人信息数据内容，若数据进行了加密需要根据

企业提供的解密方法进行解密确认数据内容，请求删除汽车数据，对删除的数据内容在车端进行测试，记录测试结果，判定车辆是否符合 6.7.3 的要求。

【说明】本条款是针对汽车数据删除机制的有效性进行验证。通过车辆制造商提供的调试接口权限进入存储路径，如文件无法被检索或文件中的汽车数据无法被检索，均满足本条要求。

【原文】9.9.4 本地删除账号以及便捷性测试方法

测试人员应按照车辆制造商提供的车型功能汽车数据处理活动清单和用户账号，测试车辆是否存在账号管理功能。若车辆存在账号管理功能，测试是否在车端提供了便捷的本地账号删除的功能，根据企业功能清单在该账户下生成存储在车端的个人信息，通过调试接口和数据存储地址确认个人信息数据内容，若数据进行了加密需要根据企业提供的解密方法进行解密确认个人信息数据内容，进行车端删除账号操作，测试存储在车端的个人信息是否进行删除或进行匿名化处理，记录测试结果，判定车辆是否符合 6.7.4 的要求。

【说明】本条款仅对车端删除账号提出要求，不对手机端、企业平台端注销账号、解绑账号提出要求。如车辆具备账号管理功能，账号管理功能具备账号删除机制，通过调试接口进入存储路径后，验证删除机制有效（不可检索、不可访问），则满足本条款要求。

2.2.8 同一型式判定（10）

与 GB/T 44464—2024 相比，增加同一型式判定条件和标准的实施。

【说明 1】匿名化处理也是一种数据安全措施。

【说明 2】安装位置指相关部件在车辆上安装的相对位置，如前挡风玻璃中央。

【说明 3】车辆涉及汽车数据处理功能（不包含仅在车内处理车辆识别代号即可实现的功能）的控制器数量指车辆的涉及汽车数据处理的控制器的总量，不包含仅在车内处理车辆识别代号即可实现的功能。

2.3 主要试验（或验证情况）分析

为支撑标准制修订工作，起草组组织了标准验证活动，于 2026 年 7 月 7 日—7 月 19 日在汽车数据标准工作组内征集标准验证活动参与单位。征集结束后，于 7 月 20 日—7 月 29 日完成参与企业综合审核、筛选及配对工作，综合考量检验与测试核心需求、参与单位技术实力、车辆适配性等因素，最终共有中国第一汽车集团有限公司、赛力斯汽车有限公司、比亚迪汽车工业有限公司、东风汽车集团股份有限公司、上汽大众汽车有限公司、大众汽车中国科技有限公司、蔚来汽车科技（安徽）有限公司、小米汽车科技有限公司、斯堪尼亚研发（江苏）有限公司等 18 家车辆制造商，以及中汽智能科技（天津）有限公司、上海机动车检测认证技术研究中心有限公司、襄阳达安汽车检测中心有限公司、招商局检测车辆技术研究院有限公司、长春汽车检测中心等 11 家技术机构通过参与单位筛选。2026 年 7 月 30 日召开验证试验启动会，会后车企与对应技术机构开展专项对接，由车辆制造商准备相

关技术文档与车辆，由技术机构对相应技术文档与车辆开展检验与测试，共同执行标准验证相关活动。

后续验证工作计划推进，期间定期召开线上或线下会议同步标准验证进展，并预计于2026年9月中下旬召开标准验证活动总结会，针对验证试验情况进行说明，并针对标准内容提出修改意见并纳入标准处理流程。

三、与有关法律、行政法规和其他标准的关系

本标准是我国智能网联汽车管理的重要内容；与现行相关法律、法规、规章及相关标准没有冲突或矛盾。

四、与国际标准化组织、其他国家或者地区有关法律法规和标准的比对分析

截至目前，国际汽车数据安全领域的规制框架已初步形成，主要由三项重要的国际及区域性法规构成，呈现出多层面、系统化的特点。在联合国层面，UN R155 法规已生效，这是全球首个针对车辆网络安全及网络安全管理体系的统一技术法规。它从管理流程、车辆型式认证、持续监控与事件响应等多个维度，对车辆数据在整个生命周期中的保密性、完整性和可用性提出了全面要求，旨在系统性降低网络攻击导致的数据风险。在区域层面，欧盟凭借两部高效力法规发挥着引领作用。但该法规更侧重于提升车辆产品的网络安全，并未直接对车辆产品的数据安全提出明确具体的要求。

欧盟《通用数据保护条例》（GDPR）为处理个人数据设立了严格标准，强调对自然人基本权利与自由的保护，并确保数据在欧盟范围内的自由流动，是所有在欧运营车企必须遵守的基本数据保护法。随后生效的《数据法案》（Data Act）则进一步扩大了规制范围，侧重于非个人数据，旨在促进数据在不同主体（如企业、用户、政府机构）间的公平访问、共享与利用，并建立了防止非法数据访问的保障机制，为物联网数据经济提供了新的规则。以上2项法规通用性更强，适用于欧盟地区各个行业。此外，联合国及欧盟地区并未制定针对汽车数据安全的专项技术法规。

本标准将充分借鉴国际先进经验，主要参考联合国 UN R155 法规的技术框架，系统构建覆盖车辆全生命周期的数据安全要求；同时融合欧盟《通用数据保护条例》（GDPR）中关于个人数据权利保护的核心原则，以及《数据法案》（Data Act）所倡导的数据共享与流通机制，明确企业在数据收集、存储、处理、传输等环节的责任与义务。本标准将立足我国汽车产业发展实际和数据安全监管需要，突出强制性标准的约束力，旨在建立适应中国国情、兼顾安全与发展的汽车数据安全管理制度，为智能网联汽车的健康发展提供坚实保障。

五、重大分歧意见的处理过程、处理意见及其依据

无。

六、对强制性国家标准自发布日期至实施日期之间的过渡期的建议及理由

由于该标准涉及企业汽车数据安全保障能力建设及调整、车辆功能开发调整、检验检测机构试验准备等问题，建议预留一段时间的过渡期，为各相关方预留充分准备时间：

本标准建议实施日期：2028-07-01

实施过渡期：

- （1）对于新申请车辆型式批准的车型，自本文件实施之日起开始执行；
- （2）对于已获得车辆型式批准的车型，自本文件实施之日起第13个月开始执行。

七、与实施强制性国家标准有关的政策措施

本标准的实施监督管理部门是工业和信息化部、国家市场监督管理总局。

根据《国务院对确需保留的行政审批项目设定行政许可的决定》，工信部负责对汽车产品实施准入管理。对不符合强制性标准要求的產品，工信部不允许进入公告目录，进行生产。主要法规依据包括：

1. 《道路机动车辆生产企业及产品准入管理办法》（工信部 2018 年第 50 号令）第六条规定：申请道路机动车辆产品准入的，生产的道路机动车辆产品应当能够符合安全、环保、节能、防盗等技术标准以及工业和信息化部制定发布的安全技术条件。
2. 《道路机动车辆生产企业及产品准入管理办法》（工信部 2018 年第 50 号令）第三十九条规定：违反本办法规定，未经准入擅自生产、销售道路机动车辆产品的，工业和信息化部应当依照《中华人民共和国道路交通安全法》第一百零三条第三款的规定予以处罚。
3. 《中华人民共和国产品质量法》第十三条规定：可能危及人体健康和人身、财产安全的工业产品，必须符合保障人体健康和人身、财产安全的国家标准、行业标准。
4. 《中华人民共和国产品质量法》第四十九条规定：生产、销售不符合保障人体健康和人身、财产安全的国家标准、行业标准的产品的，责令停止生产、销售，没收违法生产、销售的产品，并处违法生产、销售产品（包括已售出和未售出的产品，下同）货值金额等值以上三倍以下的罚款；有违法所得的，并处没收违法所得；情节严重的，吊销营业执照；构成犯罪的，依法追究刑事责任。

八、是否需要对外通报的建议及理由

本标准强制性国家标准，涉及进出口贸易，为促进国际贸易便利性，作为WTO成员国，有义务向WTO各成员通报即将实施的重要标准情况。因此，依据WTO有关规定，建议通报。

九、废止现行有关标准的建议

建议废止GB/T 44464—2024《汽车数据通用要求》。

十、涉及专利的有关说明

本标准不涉及专利。

十一、强制性国家标准所涉及的产品、过程或者服务目录

本标准涉及的产品为 M 类及 N 类车辆，不适用于基于已获得型式批准的二类底盘或整车改装的专用汽车。

十二、其他应当予以说明的事项

根据《国家标准化管理委员会关于国家标准起草中开展公平竞争审查的通知》，全国汽车标准化技术委员会智能网联汽车分技术委员会联合标准起草单位，对本标准正在开展公平竞争审查工作。

2026 年 9 月 10 日