ICS

T/GXDSL

团　　体　　标　　准

T/GXDSL —2026

数智能网联汽车数据安全加工技术规范车载传感器数据全生命周期

Technical Specification for Data Security Processing of Intelligent Connected Vehicles – Full Life Cycle of On-board Sensor Data

（工作组讨论稿）

（本草案完成时间：2026-01-29）

2026 - - 发布　　2026 - - 实施

广西电子商务企业联合会　发布

目　　次

前　言

本文件依据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。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由广西产学研科学研究院提出。

本文件由广西电子商务企业联合会归口。

本文件起草单位：

本文件主要起草人：

本文件为首次发布。

智能网联汽车数据安全加工技术规范车载传感器数据全生命周期

1 引言

为贯彻落实《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等国家法律法规，应对智能网联汽车产业发展带来的新型数据安全挑战，规范车载传感器数据全生命周期安全加工活动，保障个人合法权益，维护国家安全和公共利益，促进数据依法有序利用，支撑汽车产业高质量发展，特制定本技术规范。本标准旨在为相关组织构建系统、科学、可操作的车载传感器数据安全加工体系提供明确指引。

2 范围

本标准规定了智能网联汽车车载传感器数据在全生命周期内，包括采集、传输、存储、加工、使用、提供、公开及销毁等环节的安全加工技术要求、检验方法与管理规范。主要适用于参与智能网联汽车设计、制造、服务、数据处理的相关企业、科研院所及第三方服务机构（以下简称“数据处理者”）开展车载传感器数据安全加工活动。其他涉及汽车数据处理的组织可参照执行。

3 规范性引用文件

下列文件对于本文件的应用必不可少。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

《中华人民共和国数据安全法》（中华人民共和国主席令第 84 号，2021 年 9 月 1 日施行）

《中华人民共和国个人信息保护法》（中华人民共和国主席令第 91 号，2021 年 11 月 1 日施行）

《网络数据安全管理条例》（国务院令第 764 号，2025 年 1 月 1 日施行）

《汽车数据安全管理若干规定（试行）》（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，2021 年 10 月 1 日施行）

GB/T 35273-2020 信息安全技术个人信息安全规范

GB/T 41871-2022 信息安全技术汽车数据处理安全要求

GB/T 42564-2023 智能网联汽车数据安全指南

GB/T 37964-2019 信息安全技术个人信息去标识化指南

GB/T 39335-2020 信息安全技术个人信息安全影响评估指南

4 术语和定义

下列术语和定义适用于本文件。

4.1 车载传感器

安装于智能网联汽车，用于感知车辆自身状态、驾乘人员、车内外环境等物理信息的装置，包括但不限于摄像头、激光雷达、毫米波雷达、超声波传感器、惯性测量单元（IMU）、全球导航卫星系统（GNSS）接收模块等。

4.2 车载传感器数据

通过车载传感器直接或间接采集、生成的各类原始数据、衍生数据及关联数据，可包含车辆运行数据、环境感知数据、生物识别数据、音视频数据等，其中可能涉及个人信息、敏感个人信息及重要数据。

4.3 敏感个人信息

一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括行踪轨迹、金融账户、生物识别、宗教信仰、特定身份、医疗健康、不满十四周岁未成年人的个人信息等，以及车辆相关音视频、图像等（依据《中华人民共和国个人信息保护法》第二十八条及行业特性界定）。

4.4 重要数据

特定领域、特定群体、特定区域或达到一定精度和规模的数据，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、经济运行、社会稳定、公共健康和安全的数据（依据《中华人民共和国数据安全法》及行业监管要求界定）。

4.5 数据安全加工

在保障数据安全的前提下，对车载传感器数据进行的一系列处理活动，包括但不限于清洗、标注、脱敏、匿名化、融合、分析、建模、仿真等。

4.6 匿名化

指个人信息经过处理无法识别特定自然人且不能复原的过程（依据《中华人民共和国个人信息保护法》第七十三条）。

5 数据安全加工基本原则

5.1 合法正当原则

数据处理活动必须严格遵守国家法律法规、部门规章及强制性国家标准，遵循正当、诚信原则，不得损害国家利益、社会公共利益和他人合法权益。

5.2 权责一致原则

数据处理者对其数据处理活动负责，建立覆盖数据全生命周期的安全责任制，采取必要措施保障数据安全，履行数据安全保护义务。

5.3 目的明确与最小必要原则

数据处理应具有明确、合理、具体的目的是仅限于实现处理目的的最小范围，采取对个人权益影响最小的方式，收集最小类型和数量的数据，存储最短必要时间。

5.4 知情同意原则

处理个人信息前，应以显著方式、清晰易懂的语言真实、准确、完整地向个人告知相关事项，并取得个人的单独同意。法律、行政法规规定不需取得个人同意的除外。

5.5 安全防护原则

采取与数据安全风险等级相适应的技术措施和管理手段，确保数据保密性、完整性和可用性，防范数据泄露、篡改、丢失、滥用和非法访问。

5.6 车内处理与匿名化优先原则

在保障车辆功能安全和服务质量的前提下，优先在车内完成数据处理。确需向车外提供的，优先进行匿名化或去标识化处理。生物特征等敏感个人信息的原始数据原则上不得向车外提供。

6 数据全生命周期安全加工技术要求

6.1 数据采集安全要求

6.1.1 采集告知与同意：通过车载交互界面等显著方式，向用户告知数据处理者身份、联系方式、处理目的、方式、种类、保存期限、用户权利行使方式及渠道等，并取得同意。处理敏感个人信息须取

得单独同意。告知文本应易于阅读和理解。同意记录（含时间戳、内容、关联标识）应安全存储且防篡改，保存期限自操作发生之日起不少于 3 年。

6.1.2 采集最小化与精度控制：数据采集范围、频率、精度应严格限于实现服务功能所必需。例如，环境感知传感器的探测范围、分辨率，车辆状态传感器的测量精度与范围，均应以满足功能安全与性能下限为基准进行优化设置，避免过度采集。

6.1.3 用户控制与默认配置：应为用户提供便捷的数据采集管理功能，如全局或分项开关。对于座舱音视频、车外面部识别等涉及高度敏感场景的数据采集，应遵循“默认不收集”或“默认关闭”原则。用户关闭后，相应数据不应上传至车外。

6.2 数据传输安全要求

6.2.1 传输加密：车内外数据传输必须采用强加密措施。车云传输应采用 TLS 1.3 或更高版本的安全通信协议。车内跨安全域或关键数据传输应采用符合汽车电子网络安全要求的通信安全协议或应用层加密。敏感数据传输应实施增强加密。

6.2.2 身份认证与访问控制：建立严格的身份认证机制，确保通信端点（如车载终端、云端服务器）身份的真实性。实施网络访问控制策略，限制未授权设备的接入。通信会话应设置超时断开机制。

6.2.3 传输完整性保护：应采用校验码、数字签名等技术保证数据传输过程中的完整性，能够检测数据是否被篡改。

6.3 数据存储安全要求

6.3.1 存储位置与期限管理：在中国境内运营中收集和产生的重要数据和个人信息，应在境内存储。确需向境外提供的，须通过国家网信部门组织的安全评估。数据存储期限应为实现处理目的所必需的最短时间，并明确告知用户。法律法规另有规定的，从其规定。

6.3.2 存储加密：存储态的数据，尤其是个人信息和重要数据，必须进行有效加密。加密算法应符合国家密码管理部门的要求。加密密钥应进行全生命周期安全管理，与加密数据分开存储。

6.3.3 访问控制与安全存储环境：对存储数据的访问应实施严格的权限管理，遵循最小权限原则。存储系统应部署在安全可控的环境中，云端存储系统应满足国家网络安全等级保护相关要求。

6.4 数据加工安全要求

6.4.1 加工前预处理：加工前应对数据进行分类分级，对包含个人信息的数据进行脱敏或匿名化处理。匿名化处理应遵循相关国家标准，确保处理后的信息无法识别特定个人且不能复原。

6.4.2 加工环境安全：数据加工应在安全隔离的环境中进行，实施严格的访问控制与操作审计。加工平台应具备防病毒、防攻击等安全防护能力。

6.4.3 算法模型安全：使用数据进行算法训练和模型开发时，应采取措施防止模型记忆和泄露原始敏感信息。对外提供或部署模型时，应对模型进行安全性评估。

6.5 数据使用、提供与公开安全要求

6.5.1 使用权限控制：建立基于角色和属性的精细化访问控制机制，确保数据仅被授权人员在授权范围内访问和使用。所有数据访问行为应被完整日志记录。

6.5.2 提供与共享管理：向其他组织提供数据前，应进行安全影响评估，除法律、行政法规另有规定外，应重新向个人告知并取得同意。应与数据接收方通过合同等形式明确双方数据安全保护责任和义务。

6.5.3 数据公开：原则上不得公开未匿名化的原始车载传感器数据。因学术研究、公共服务等确需公开的，必须进行彻底的匿名化处理，并评估其重标识风险。

6.6 数据销毁安全要求

6.6.1 销毁时效与方式：数据超出保存期限或处理目的完成后，应及时安全销毁。销毁应确保数据不可恢复。电子数据应采用多次覆写等不可逆的技术手段；物理存储介质应采用消磁、粉碎等物理破坏方式。

6.6.2 销毁记录与审计：数据销毁过程应记录，记录内容应包括销毁的数据描述、时间、方法、操作人员等。销毁记录应妥善保存以备审计。

7 检验方法

7.1 检验依据

检验工作应依据本标准第 5 章规定的技术要求，并参考相关国家标准和行业标准执行。

7.2 检验项目与方法

检验应覆盖数据全生命周期各关键环节，主要项目及方法如下：

7.2.1 采集告知与同意合规性检验：核查告知文本内容、呈现方式及用户同意记录的真实性、完整性和防篡改性。

7.2.2 数据最小化采集检验：审查数据采集策略文档，并通过技术测试验证实际采集范围、频率、精度是否符合声明目的的最小必要要求。

7.2.3 传输安全检验：检测数据传输通道是否采用规定的加密协议和算法，验证身份认证机制和完整性保护措施的有效性。

7.2.4 存储安全检验：核查存储加密配置、访问控制策略及密钥管理情况，验证备份与恢复机制的有效性。

7.2.5 加工安全检验：检查数据脱敏或匿名化处理流程是否符合标准，评估加工环境的安全隔离与防护水平，测试算法模型的抗逆向攻击能力。

7.2.6 使用与提供安全检验：审计数据访问日志，验证权限控制是否有效，审查数据对外提供或共享的合规流程与协议。

7.2.7 销毁有效性检验：审查销毁记录，并采用技术工具尝试恢复已销毁数据，验证销毁的不可逆性。

7.3 检验结果判定

所有检验项目均符合本标准技术要求时，判定为合格。若有关键项（如涉及个人信息和重要数据的加密、匿名化、同意获取等）不符合要求，则判定为不合格，需整改后重新检验。检验报告应客观、完整、准确，由具备资质的检验人员签署并加盖检验机构公章。

8 管理规范

8.1 组织与人员管理

数据处理者应建立数据安全管理体系，明确数据安全负责人和管理部门。定期对全体员工开展数据安全法律法规、技术标准和意识培训，关键岗位人员须通过专项考核。

8.2 风险评估与应急处置

每年至少开展一次全面的数据安全风险评估，重点评估重要数据和敏感个人信息处理活动的风险，并根据评估结果改进防护措施。制定数据安全事件应急预案，定期组织演练。发生数据安全事件时，应立即采取处置措施，并按规定及时向主管部门报告。

8.3 审计与监督

建立覆盖数据全生命周期的安全审计制度，定期对数据处理活动进行合规性审计。审计日志应长期保存，确保可追溯。

8.4 合作方与供应链管理

通过合同等方式明确供应商、合作伙伴等第三方在数据安全方面的责任和义务，并定期对其数据安全保护能力进行监督和评估

9 附则

本标准由广西电子商务企业联合会负责解释。本标准自发布之日起试行，试行期为一年。试行期满后，根据实施反馈情况进行修订和完善。各相关单位可依据本标准制定具体的实施细则。若本标准与国家新颁布的法律法规或强制性标准有不一致之处，应以国家法律法规和强制性标准为准。本标准所引用的规范性引用文件如有更新，其最新版本适用于本标准。广西电子商务企业联合会将根据技术发展和应用需求，适时组织对本标准的复审与修订工作，以保障其持续的先进性和适用性。本标准的有效实施，有赖于各级医疗机构、主管部门、技术服务商和各相关方的共同努力，通过规范智慧医院数据互联互通共享技术，推动医疗健康数据资源有效整合与安全共享，提升医疗服务质量和效率，促进智慧医院建设规范化发展，为推进健康中国建设提供技术支撑。