ICS 43.020

CCS T 04

团　体　标　准

T/JSSAE 013—2025

智能网联汽车数据安全要求

Requirements of data security for intelligent and connected vehicles

2025-12-25 发布　　2025-12-30 实施

江苏省汽车工程学会 发 布

目　　次

前　言

本文件按照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这些专利的责任。

本文件由江苏省汽车工程学会提出并归口。

本文件起草单位：清华大学苏州汽车研究院（吴江）、中国移动通信集团江苏有限公司苏州分公司、知行汽车科技（苏州）有限公司、先导（苏州）数字产业投资有限公司、北京交通运输职业学院、苏州数智科技集团有限公司、苏州智行众维智能科技有限公司、江苏智能网联汽车创新中心有限公司、江苏天安智联科技股份有限公司、苏州空地网联科技有限公司、苏州智能交通信息科技股份有限公司、苏州市计量测试院有限公司、苏州清研车联教育科技有限公司、苏州驾驶宝智能科技有限公司、天翼交通科技有限公司、华砺智行（苏州）科技有限公司。

本文件主要起草人：邓晓茜、邱奕飞、宋炜瑾、何乃剑、王佳利、茅志强、缑庆伟、段卫洁、张新敏、刘俊、张春梅、安宏伟、戴一凡、洪涛、薛旸、刘俊、张春梅、沈彧、夏建文、王新新、任学锋。

本文件为首次发布。

智能网联汽车数据安全要求

1 范围

本文件规定了智能网联汽车数据安全的一般要求、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的数据安全管理。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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。

DB4403/T 355—2023 智能网联汽车整车信息安全技术要求

3 术语和定义

下列术语和定义适用于本文件

3.1

汽车数据 vehicle data

汽车设计、生产、销售、使用、运维、报废等过程中涉及的个人信息和重要数据。

[来源：汽车数据安全管理若干规定（试行）,第三条,有改写]

3.2

汽车数据处理 vehicle data processing

汽车数据收集、存储、使用、加工、传输、提供、公开、删除等过程。

4 一般要求

4.1 汽车数据安全管理体系要求

4.1.1 汽车数据处理单位应建立汽车数据安全管理体系，落实汽车数据安全管理制度。

4.1.2 汽车数据处理单位应采取汽车数据安全保护技术措施，保证数据持续处于有效保护和合法利用的状态。

4.1.3 汽车数据处理单位应制定汽车数据安全方针、分析汽车数据安全管理体系内外部环境并确定汽车数据安全管理体系的边界及其适用范围。

4.1.4 汽车数据处理单位应建立汽车数据安全管理机构、确定相关人员职责并形成汽车数据安全文化。

4.1.5 汽车数据处理单位应建立汽车数据分类分级制度，形成数据资产管理台账。

4.1.6 汽车数据安全管理体系应覆盖数据全生命周期，应制定数据收集、存储、使用、加工、传输、提供、公开、删除等过程的具体分级防护要求和操作规程。

4.1.7 汽车数据处理单位在境内收集和产生的个人信息和重要数据应按照有关法律法规规定在境内存储，如需向境外提供，应通过数据出境安全评估。

4.1.8 汽车数据处理单位应针对车辆全生命周期制定数据安全流程管理制度。

注：车辆全生命周期包括车辆的概念设计、产品开发、验证确认、运维及报废等阶段。

4.1.9 汽车数据处理单位应建立汽车数据安全监测和事件管理制度，发现汽车数据安全缺陷、漏洞等风险时，应立即采取补救措施；发生汽车数据安全事件时应立即采取处置措施，按照规定及时告知用户并向有关主管部门报告。

4.1.10 汽车数据处理单位应建立投诉举报处理机制，建立数据安全投诉举报渠道并及时受理、处置数据安全投诉举报。

4.1.11 汽车数据处理单位开展汽车数据处理活动应进行风险管理。

4.2 汽车数据处理的一般要求

4.2.1 汽车数据处理者处理个人信息应符合第 5 章的要求。

4.2.2 汽车数据处理者处理敏感个人信息应符合第 5 章的要求。

4.2.3 汽车数据处理者处理个人信息时，车内处理和默认不收集行为应符合 5.1.1 的要求，精度范围适用应符合 5.3 的要求，显著告知行为应符合 5.2.1 的要求。

4.2.4 汽车数据处理者处理重要数据应符合第 6 章的要求。

4.2.5 汽车数据处理者处理重要数据时，车内处理和默认不收集行为应符合 6.1 的要求，精度范围适用应符合 6.2 的要求。

4.2.6 汽车数据处理者处理的数据既属于个人信息也属于重要数据时，应同时符合第 5 章和第 6 章的要求。

5 个人信息保护要求

5.1 个人信息处理通用要求

5.1.1 汽车数据处理者处理个人信息应具有明确、合理的目的，并应与处理目的直接相关，采取对个人权益影响最小的方式。除非驾驶人自主设定，车辆应默认设定为不收集个人信息的状态；除非取得个人信息主体同意，不应向车外提供个人信息。

5.1.2 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：

—— 用于紧急情况下为保护自然人的生命健康和财产安全所必需的功能；

—— 处理个人自行公开或者其他已经合法公开的个人信息；

—— 因保证行车安全需要，无法征得个人同意收集到车外个人信息。

5.1.3 其它符合法律、行政法规和强制性国家标准等规定的情形。汽车数据处理者应通过产品说明书、合同书、个人信息保护政策等至少一种形式提供取得个人同意的例外情形及理由。

5.1.4 撤回个人同意，不影响撤回前基于个人同意已进行的个人信息处理活动的效力。

5.1.5 基于个人同意而处理的个人信息，存储期限应与取得同意的个人信息存储期限或其规则一致。

5.1.6 除取得个人同意外，汽车不应向车外提供座舱数据。

5.1.7 有下列情形之一的，汽车数据处理者应主动删除个人信息或匿名化处理，汽车数据处理者未删除的，个人有权请求删除：

—— 处理目的已实现、无法实现或者为实现处理目的不再必要；

—— 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；

—— 个人撤回同意；

—— 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。

5.1.8 法律、行政法规规定的其他情形。法律、行政法规规定的保存期限未届满，或者删除个人信息从技术上难以实现的，个人信息处理者应停止除存储和采集必要的安全保护措施之外的处理。

5.2 个人同意的取得

5.2.1 显著告知

汽车数据处理者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，通过至少一种显著方式向个人告知，清晰地说明个人信息的具体情境和必要性，并提供便捷的查阅、复制和删除等个人信息管理功能。

5.2.2 取得个人统一的选项设置

向个人进行符合5.2.1要求的显著告知后，汽车数据处理者应取得个人同意并按照如下要求设置取得个人同意的选项：

——提供同意和拒绝同意的方式；

——处理敏感个人信息提供自主设定同意期限的途径，且期限不应设置为始终允许或永久。

5.2.3 重新取得个人同意的要求

5.2.3.1 汽车数据处理者应在取得的同意期限内处理个人信息，当个人同意期限届满后，若汽车数据处理者仍有必要继续进行除删除外的个人信息处理活动，应重新取得个人同意。

5.2.3.2 个人信息的处理目的、处理方式和处理的个人信息种类发生变更的，汽车数据处理者应重新取得个人同意。

5.2.4 个人同意的撤回

汽车数据处理者应提供个人撤回同意的途径。

5.3 个人信息收集

5.3.1 收集个人信息时，汽车数据处理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。

5.3.2 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，至少应有一个功能服务符合5.3.1要求，针对其他不符合5.3.1的功能服务，汽车数据处理者应做出合理说明。

5.4 个人信息存储

个人信息的存储应符合DB4403/T 355—2023中对于个人信息存储的相关要求。

5.5 个人信息使用

5.5.1 使用个人信息时，汽车数据处理者应采取访问控制措施，防止非授权访问存储的个人信息。

5.5.2 车辆个人身份认证功能不应仅使用个人生物特征识别信息。

5.6 个人信息传输

5.6.1 车外传输要求

5.6.1.1 向车外传输个人信息应符合 DB4403/T 355—2023 中对于个人信息传输的相关要求。

5.6.1.2 因保证行车安全需要，无法征得个人同意收集到车外个人信息且向车外提供的，应进行匿名化处理，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。匿名化处理应符合 5.6.2 的要求，匿名化处理完成后，过程数据应及时删除，不应向车外提供。

5.6.2 匿名化要求

5.6.2.1 匿名化对象

5.6.2.1.1 人脸匿名化对象

汽车数据处理者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：

——人脸目标对应的人脸边界框最小边长像素大于等于 32 像素；

——人脸目标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。

注：可见范围比值指人脸目标框内可见范围与人脸目标边界框的面积比值，其中可见范围为人脸由于旋转、遮挡等导致部分不可直接观察时，人脸目标框内可直接观察无遮挡的人脸目标的矩形面积。

5.6.2.1.2 汽车号牌匿名化对象

汽车数据处理者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；

——汽车号牌全部数字及文字内容无遮挡且可识别。

注：边界框高度指汽车号牌边界框上沿至下沿的距离。

5.6.2.2 匿名化处理性能要求

人脸目标和汽车号牌目标的检出率均应不低于90%。

5.6.2.3 匿名化效果要求

已进行匿名化处理的人脸目标和汽车号牌目标应无法被识别。

5.7 个人信息删除

5.7.1 个人请求删除敏感个人信息的，汽车数据处理者应在 10 个工作日内完成删除，法律、行政法规另有规定的按照其规定执行。

5.7.2 被删除的个人信息应不可检索、不可访问。

5.8 个人信息出境

5.8.1 个人信息通过车辆出境应符合 DB4403/T 355—2023 的要求。

5.8.2 个人信息通过其他方式确需向境外提供的，应符合法律法规的有关规定。

6 重要数据保护要求

6.1 重要数据处理通用要求

汽车数据处理者处理重要数据应具有明确、合理的目的，并应与处理目的直接相关。除非驾驶员自主设定，车辆应默认设定为不收集重要信息的状态，不应向车外提供重要数据。

6.2 重要数据收集

6.2.1 收集重要数据时，汽车数据处理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。

6.2.2 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，至少应有一个功能服务符合6.2.1的要求，针对其他不符合6.2.1要求的功能服务，汽车数据处理者应做出合理说明。

6.3 重要数据存储

重要数据的存储应符合DB4403/T 355—2023中对于敏感个人信息存储的相关要求。

6.4 重要数据使用

使用重要数据时，汽车数据处理者应采取访问控制措施，防止非授权访问存储的重要数据。

6.5 重要数据传输

向车外传输重要数据应符合DB4403/T 355—2023中对于敏感个人信息传输的相关要求。

6.6 重要数据删除

被删除的重要数据应不可检索、不可访问。

6.7 重要数据出境

重要数据通过车辆出境应符合DB4403/T 355—2023的要求。重要数据通过其他方式确需向境外提供的，应符合法律法规的有关规定。

7 审核评估要求

7.1 数据处理

汽车数据处理者宜满足4.1要求的符合性评估。

7.2 个人信息及重要数据处理

7.2.1 试验输入信息

试验开始前，送检厂商应提供如下信息：

——试验车辆处理个人信息和重要数据的功能清单；

——撤回个人同意方式清单；

——试验车辆雷达和摄像头参数信息；

——试验车辆存储个人信息和重要数据的存储地址。

7.2.2 个人信息和重要数据处理通用试验方法

按照DB4403/T 355—2023附录A进行试验，试验结果应符合5.4、5.5.1、5.6.1.1、5.8、6.3、6.4、6.5和6.7的要求。

7.2.3 个人同意的取得试验方法

7.2.3.1 按照处理个人信息的功能清单，启动除5.1.2所列例外情形的试验车辆各项个人信息处理功能，检查是否具备告知方式，并记录告知方式、告知内容和个人同意的方式，试验结果应符合5.2.1和5.2.2的要求。

7.2.3.2　按照处理个人信息的功能清单，除 5.1.2 所列例外情形外，当各项个人信息处理功能超出同意期限后，启动各项功能，检查是否重新取得个人同意并记录个人同意的方式，试验结果应符合 5.2.3.1 的要求。

7.2.3.3　按照处理个人信息的功能清单，变更部分功能的处理目的、处理方式或处理种类，启动该功能，检查是否重新取得个人同意并记录个人同意的方式，试验结果应符合 5.2.3.2 的要求。

7.2.3.4　按照处理个人信息的功能清单，除 5.1.2 所列例外情形外，撤回各项功能的个人同意，记录各项功能撤回个人同意的途径，试验结果应满足 5.2.4 的要求。

7.2.4　个人信息和重要数据收集试验方法

基于收集个人信息和重要数据的雷达和摄像头等数据收集设备参数，对比功能列表中各项功能所需的收集设备精度需求，记录对比结果，对比结果应符合5.3和6.2的要求。

7.2.5　个人信息使用试验方法

基于个人信息处理的功能清单，选择需要使用个人生物特征识别信息进行身份认证的功能，撤销个人生物特征信息同意，检查相关功能是否仍可通过其他方式正常运行，记录试验结果，试验结果应符合5.5.2的要求。

7.2.6　个人信息和重要数据传输试验方法

7.2.6.1　按照处理个人信息的功能清单，选取需要向车外提供座舱数据的功能，启动该功能，检查车辆是否发出向车外提供座舱数据的个人同意请求，记录试验结果，试验结果应符合 5.1.5 的要求。

7.2.6.2　按照处理个人信息的功能清单，对于符合 5.6.1.2 规定的情形，逐项启动相关功能，检查车辆 对外传输的个人信息是否进行匿名化处理，记录试验结果，试验结果应符合 5.6.1.2 的要求。

7.2.7　个人信息和重要数据删除试验方法

7.2.7.1　基于个人信息处理功能清单，选取涉及处理敏感个人信息的功能，若该功能对应的敏感个人信息存储在车端，请求删除敏感个人信息，检查删除情况，记录试验结果，试验结果应符合 5.7.1 的要求。

7.2.7.2　基于个人信息和重要数据处理功能清单，选取涉及处理个人信息和重要数据的功能，若该功能对应的个人信息和重要数据存储在车端，请求删除个人信息和重要数据，对删除的数据内容在车端进行检索，记录检索结果，试验结果应符合 5.7.2 和 6.6 的要求。

7.3　应对车辆进行个人信息匿名化处理试验。

7.4　应对车辆进行匿名化误检率试验。