ICS 43.020
CCS T 40

DB4403

深　　圳　　市　　地　　方　　标　　准

DB4403/T 361—2023

智能网联汽车数据安全要求

Requirements of data security for intelligent and connected vehicles

2023-08-22 发布　　2023-09-01 实施

深圳市市场监督管理局　　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。

本文件以推荐性国家标准《汽车数据通用要求》（计划号：20213606-T-339）（2022年10月版本）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。

本文件由深圳市工业和信息化局提出并归口。

本文件起草单位：深圳市工业和信息化局。

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。

本文件适用于具备汽车数据处理功能的车辆及其数据处理者。

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。

GB 14886 道路交通信号灯设置与安装规范

GB 14887 道路交通信号灯

GB/T 38636—2020 信息安全技术 传输层密码协议（TLCP）

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。

[来源：汽车数据安全管理若干规定（试行）,第三条,有改写]

3.3

收集 collect

通过一定方式获取汽车数据的行为。

3.4

汽车数据处理者 vehicle data processor

开展汽车数据处理活动的组织。

注：汽车数据处理者包括汽车制造商、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。

[来源：汽车数据安全管理若干规定（试行）,第三条]

3.5

汽车数据安全管理体系 vehicle data security management system

一种规范汽车数据处理者开展数据处理活动过程中保护汽车数据安全的系统性方法。

3.6

审计 audit

获取审核证据并对其进行客观评价以确定满足审核准则程度的，系统的、独立的和文档化的过程。

[来源：GB/T 25069—2022,3.515]

3.7

个人信息 personal information

以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息。

注：个人信息包括敏感个人信息和一般个人信息，不包括匿名化处理后的信息。

示例：自然人包括车主、驾驶人、乘车人、车外人员等。

[来源：中华人民共和国个人信息保护法,第四条]

3.8

敏感个人信息 sensitive personal information

一旦泄露或者非法使用，可能导致车主、驾驶人、乘车人、车外人员等受到歧视或者人身、财产安全受到严重危害的个人信息。

注：包括车辆行踪轨迹、音频、视频、图像和生物识别特征等信息。

[来源：汽车数据安全管理若干规定（试行）,第三条]

3.9

一般个人信息 general personal information

除敏感个人信息外的其他个人信息。

3.10

座舱数据 cabin data

通过摄像头、红外传感器、指纹传感器或传声器等部件从汽车座舱采集的可能包含个人信息的数据，以及对其进行加工后产生的数据。

[来源：GB/T 41871—2022，3.6]

3.11

匿名化 anonymization

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。

[来源：中华人民共和国个人信息保护法,第七十三条]

3.12

个人信息主体 personal information subject

个人信息所标识的自然人。

[来源：GB/T 35273-2020,3.3，有改写]

3.13

人脸目标 human face object

自然人的头部正面眉毛最上端至颏底线之间、左耳到右耳（不包括耳朵）之间的部分。

3.14

人脸边界框 human face boundary frame

覆盖人脸目标范围的最小矩形或旋转矩形。

示例：人脸范围示意图见图1。

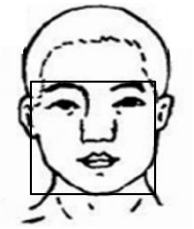

图 1　人脸范围示意图

3.15

汽车号牌目标　vehicle license plate object

基材为金属的准予汽车在中华人民共和国境内道路上行驶的法定标志，其号码是机动车登记编号。

[来源：GA 36-2018,3.1，有改写]

注：本文件所指汽车号牌目标均指基材为金属的正式机动车号牌，不包含喷涂的放大号牌、纸质临时机动车号牌。

3.16

汽车号牌边界框　vehicle license plate boundary frame

汽车号牌外延组成的矩形或旋转矩形。

3.17

遮盖率　coverage rate

对于符合本文件 5.6.2.1 要求的单个匿名化对象，边界框内进行匿名化处理区域与整个边界框区域的面积比值。

示例：遮盖率示意图见图 2，其中实线区域为人脸边界框，虚线部分为匿名化区域，遮盖率为阴影部分与实线区域的面积比值。

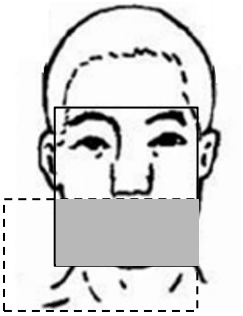

图 2　遮盖率示意图

3.18

检出率　detection rate

某类目标的正检数除以正检数与漏检数之和的数值。

注：漏检数是未被检出的应进行匿名化目标数量。

3.19

误检率　false detection rate

某类目标的误检数与检出目标数的比值。

注：误检数是被检出且不满足目标定义的目标数量。

3.20

重要数据　important data

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。

注：重要数据包括：

——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；

——车辆流量、物流等反映经济运行情况的数据；

——汽车充电网的运行数据；

——包含人脸信息、车牌信息等的车外视频、图像数据；

——涉及个人信息主体超过 10 万人的个人信息；

——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。

[来源：汽车数据安全管理若干规定（试行），第三条]

4 一般要求

4.1 汽车数据安全管理体系要求

4.1.1 汽车数据处理者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 汽车数据处理者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 汽车数据处理者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 汽车数据处理者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 汽车数据处理者应建立汽车数据分类分级制度，可参考附录 A，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 汽车数据处理者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 汽车数据处理者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 汽车数据处理者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 汽车数据处理者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 汽车数据处理者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，脱敏处理行为应符合 5.6.1.4 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。具体要求如下：

——告知方式可选取弹窗、文字说明、提示条、提示音、产品说明书、合同书、个人信息保护政策等；

——告知内容应至少包含：

- 处理个人信息的种类、处理各类个人信息的必要性，包括目的、用途、方式等；
- 收集各类个人信息的具体情境以及停止收集的方式和途径；
- 个人信息存储地点、存储期限，或者确定存储地点、存储期限的规则；
- 查阅、复制其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；
- 用户权益事务联系人的姓名和联系方式；

- 法律、行政法规规定的应告知的其他事项。

5.2.2 取得个人同意的选项设置

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要求的功能服务，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。

示例：广告牌、光滑表面倒影中出现的具有人脸目标特征的图像不属于真实人脸目标，不属于匿名化对象。

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

5.6.2.2.1 检出率要求

人脸目标和汽车号牌目标的检出率均应不低于90 %。

5.6.2.2.2 误检率要求

误检率可不大于10 %。

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。除非驾驶人自主设定，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 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 汽车数据处理者宜满足 4.1 要求的符合性评估。

7.2 应按照附录 C 对车辆进行个人信息及重要数据处理试验，并按照附录 E 对车辆进行个人信息匿名化处理试验。

7.3 宜参考附录 F 对车辆进行匿名化误检率试验。

附 录 A
（资料性）
数据分类分级要求

A.1 数据分类分级原则

汽车数据分类分级原则如下：

——科学性：按照汽车数据的多维特征以及相互间客观存在的逻辑关联进行科学和系统化的分类分级；

——实用性：汽车数据的分类分级要保证每个类目下要有数据，不设没有意义的类目；

——扩展性：汽车数据分类分级方案在总体上具有概括性和包容性，能够实现各种类型数据的分类，以及满足将来可能出现的数据类型；

——合法合规性：数据分类分级遵循国家法律法规及行业主管部门有关规定；

——可执行性：数据分类分级规则避免过于复杂以保证数据分类分级的可行性；

——时效性：数据分级具有一定的有效期限，超过有效期限数据级别应按照级别变更策略及时调整；

——稳定性：分类分级要基于智能网联汽车数据最稳定的特征和属性，以保持分类分级结果稳定，并在总体上利于对同一类别或级别的数据适用相同的安全要求；

——显著性：根据数据在产生、收集、使用等方面的成果或内容上的显著特征确定汽车的分类方案。

A.2 数据分类

根据汽车数据的类型、特性及业务使用场景等因素，并综合数据安全管理的总体目标和安全策略要求，对数据资产进行梳理、归类和细分后形成的汽车数据分类见表A.1。

表 A.1 数据分类表

一级分类名称	二级分类名称	定义	示例
车辆基本数据	车辆标识数据	能识别或关联出特定车辆的数据	如汽车号牌、车辆识别号VIN、车辆厂商、商标、品牌、车辆产品型号等
	车辆属性数据	车辆静态属性数据（不能识别或关联出特定车辆的数据）	如车辆外廓尺寸、传动比、轴距、轮距等
	核心零部件标识数据	影响车辆感知、决策、数据记录的核心零部件数据	车载传感器、域控制器、EDR、DSSAD软硬件型号、版本号
	车辆鉴别数据	用于验证车辆及零部件身份的信息	如密码和证书等
	车辆维保数据	车辆的诊断、维修、检查、定期监测、重新编程或重新初始化或远程诊断支持所需的所有信息，这些信息是制造商为其授权经销商和维修商提供的，包括对此类信息的所有后续修订和补充。该信息包括将零件或设备安装到车辆上所需的所有信息	如车辆保险信息、车辆维护信息、车辆保养信息等

表A.1　数据分类表（续）

一级分类名称	二级分类名称	定义	示例
感知数据	激光雷达数据	通过车载激光雷达获取到的原始数据	点云数据信息
	毫米波雷达数据	通过车载毫米波雷达获取到的原始数据	点云数据或目标物信息
	摄像头数据	通过车载摄像头获取到的原始数据	视频和图片等信息
	超声波雷达数据	通过车载超声波雷达获取到的原始数据	障碍物信息（如与障碍物的相对距离）
	IMU数据	通过车载IMU获取到的原始数据	角速度和加速度等信息
	高精地图数据	相比传统导航地图，能提供精度更高、内容更丰富的道路拓扑、拓扑关系、位置、几何、交通标识、交通信号设施等地图属性，为智能网联汽车提供环境信息的地图的数据	道路信息、车道信息、道路附属设施信息等静态信息，实时路况、交通事件等动态信息
	GNSS数据	通过卫星或基准站获取到的定位数据	载波和伪距（用于计算车的位置）
	V2X数据	通过C-V2X获取到的相关数据	红绿灯、标识、目标物等信息（BSM，RSM，SPAT等消息集）
	语音	通过车载麦克风采集的车内乘员与车机进行语音交互的数据	—
	融合后的目标（机动车及其他道路交通参与者）数据	各感知模块融合后的输出数据	目标物的类型、相对位置、相对速度等
	融合后的交通信息数据	通过车载部件获取到的交通信息数据	交通标志、信号灯、路况信息、限速信息等
	融合后的自然条件数据	通过车载部件获取到的自然条件数据	白天、黑夜、晴天、雨天、雪天、车外温度等
	融合后的道路属性数据	通过车载部件获取到的道路属性数据	道路类别（高速公路、城市道路、乡村路等）
	融合后的自车车身姿态	通过车载部件获取到的车身姿态数据	航向角、横摆角速度、侧倾角速度等
	融合后的自车位置数据	通过车载部件获取到的绝对或相对位置数据	绝对位置信息和相对位置信息
	语义	通过采集到的语音解析得出的与车机交互的一类数据	如用来唤醒车载语音交互系统的特定关键语句等
	声纹	用来识别特定用户身份的声波频段数据	用来完成说话人辨认和确认过程的信息
	其他感知部件采集的数据	以上未能涵盖的车辆感知数据	—
	其他的感知融合数据	以上未能涵盖的车辆感知融合数据	—

表A.1　数据分类表（续）

一级分类名称	二级分类名称	定义	示例
决策数据	人类驾驶员操作数据	由人类驾驶员进行的操作类数据，包含非驾驶控制类数据	如挡位信息、加速踏板开度、刹车踏板开度、转向角度、用户操作指令等
	远程操作数据	通过远程控制指令对车辆进行操作的数据	如车辆远程开关门锁、远程开关空调、远程鸣笛和闪灯等远程启动或泊车等
	系统决策数据	由车辆系统进行的驾驶决策控制类数据	如系统请求的挡位、横向加速度、转向角、转向力矩、纵向加速度、灯光状态、雨刮状态等
运行数据	整车状态数据	车辆在运行工况下的状态数据	如上电状态、控制模式、动力模式、充电状态、挡位、制动状态、剩余油量/电量、车辆控制模式等 如实时车速、横或纵向加速度、航向角、横摆角速度、侧倾角速度、俯仰角速度等
运行数据	系统及部件运行状态数据	表征部件及系统运行状态的数据	如安全气囊状态、GNSS 运行状态、IMU运行状态、驾驶自动化系统运行状态、高精地图运行状态、OBU运行状态、摄像头运行状态、激光雷达运行状态、超声波雷达运行状态、毫米波雷达运行状态、夜视系统运行状态等（正常、异常、表示异常、无效）
	安全日志数据	与安全相关的日志数据	—
	其他日志数据	与安全相关性较低的日志数据	—
	汽车充电网运行数据	—	充电桩类别、编号等
其他数据	用户行为汇聚分析数据	经过处理后的用户数据，无法单独或者与其他信息结合识别特定用户的各种数据	—
	用户身份标识数据	用于标识用户身份的数据	如用户账号、密码等
	用户与座舱交互数据（非操控类数据）	用于描述用户与座舱交互产生的相关数据	如用户通讯录、通讯记录和内容、上网记录等

A.3　重要数据识别参考

A.3.1　分级要素

A.3.1.1　汽车数据分级应评估危害程度和重要程度两个方面，评估要素应至少包括影响对象和影响程度。若数据分级过程中出现多个影响对象，应按照程度的较高等级进行判定。

A.3.1.2　评估数据遭到篡改、破坏、泄露或者非法获取、非法利用后对国家安全、公共利益、个人权

益和企业权益的危害程度的方法见表 A.2。

表 A.2　危害程度评估表

危害程度	影响对象	影响程度	数据一般特征
严重	国家安全	任何	影响国家的安全保卫工作、经济竞争力、科技实力、涉及国家安全的其他事项。 对国家政权、主权、统一和领土完整、人民福祉、经济社会可持续发展和国家其他重大利益造成影响。
严重	公共利益	严重	影响社会公众接受公共服务的活动、使用公共设施的活动、涉及公共利益的其他事项。 对经济运行、社会稳定、公共健康和安全和其他重要社会公共利益造成影响。
中等	个人权益	中等/严重影响	个人敏感信息，一旦泄露或者非法使用，可能导致车主、驾驶人、乘车人、车外人员等受到歧视或者人身、财产安全受到严重危害。
轻度	个人权益	轻度	个人非敏感信息，个人信息主体可被识别，一旦泄露或者非法使用，可能会给个人信息主体合法权益带来负面影响。
无影响	个人权益	无影响	相关数据在任何场景下均无法关联或识别到个人信息主体；或个人信息主体可主动公开或经授权公开的数据。

A.3.1.3　评估汽车数据处理者为处理数据所投入的各项成本、对达成预设目标及可能带来的利益的重要程度方法见表 A.3。

表 A.3　重要程度评估表

重要程度	影响对象	影响程度	数据一般特征
极高	数据处理者所投入的成本	极高	数据处理需在软硬件、技术、人力、经济等方面投入巨大成本
极高	对数据处理者达成预设目标的关键程度	极高	达成预设目标对数据的依赖程度非常高，没有数据支撑无法完成，或者数据起到决定性作用，没有可替代方案
极高	给数据处理者可能带来的利益	极高	数据处理可以给数据处理者在技术进步、业务发展、社会影响、经济收入等方面带来巨大利益，显著地促进技术进步、开拓新的业务模式、提升业务规模、增加业务营收
高	数据处理者所投入的成本	高	数据处理需在软硬件、技术、人力、经济等方面投入较高成本
高	对数据处理者达成预设目标的关键程度	高	达成预设目标对数据的依赖程度较高，数据起到关键性作用，没有可替代方案或者可替代方案成本较高
高	给数据处理者可能带来的利益	高	数据可能给数据处理者在业务发展、技术进步、社会影响、经济收入等方面带来较大利益，有效地促进技术进步、提升业务规模、增加业务营收
中	数据处理者所投入的成本	中	数据处理需在软硬件、技术、人力、经济等方面投入一定成本
中	对数据处理者达成预设目标的关键程度	中	达成预设目标对数据处理有一定依赖，但有可替代方案
中	给数据处理者可能带来的利益	中	数据可能给数据处理者在业务发展、技术进步、社会影响、经济收入等方面带来有限利益

表A.3　重要程度评估表（续）

重要程度	影响对象	影响程度	数据一般特征
低	数据处理者所投入的成本	低	数据处理几乎无额外成本
低	对数据处理者达成预设目标的关键程度	低	数据对达成预设目标无影响
低	给数据处理者可能带来的利益	低	数据无法带来利益

A.3.2　分级要求

汽车数据分级应按照表A.2和表A.3的要求评估数据遭到篡改、破坏、泄露或者非法获取、非法利用后的危害程度和对汽车数据处理者的重要程度，形成的数据分级应符合表A.4的要求。若数据定级要素出现不同程度，应按照程度对应的较高数据级别进行判定。

表 A.4　数据分级表

数据级别	定级要素
S3	危害程度：严重，或 重要程度：极高
S2	危害程度：中等，或 重要程度：高
S1	危害程度：轻度，或 重要程度：中
S0	危害程度：无影响，或 重要程度：低

A.3.3　数据定级规则参考

数据定级要素主要从影响对象和影响程度两方面进行考虑，具体如下：

a)　汽车重要数据安全等级不低于 S2；
b)　同一数据由于数据量的增加可能会造成数据级别上升；
c)　不同种类数据的组合可能会造成数据级别上升。

A.3.4　数据分类分级映射参考

数据分类分级的映射关系可参考附录 B。

A.4　个人信息识别参考

以下列举汽车数据处理者处理较为广泛的个人信息作为示例，若存在表中未列举的个人信息类型可参考3.7和3.8进行判定。

表A.5　个人信息分类分级示例表

分类	分级	
	一般个人信息	敏感个人信息
个人基本资料	个人姓名、出生日期、电子邮箱地址、住址、个人电话号码、年龄、性别、家庭关系	—
个人身份信息	个人账户的系统账号（不包含密码）	身份证、驾驶证、个人账户的系统账号（包含密码）
个人车辆标识	车辆VIN、车牌号、行驶证	—
个人生物识别信息	—	个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部特征等数据，数据能够识别或确定自然人的独特标识
个人财产信息	—	银行账号、鉴别信息（口令）、存款信息（包括资金数量、支付收款记录等）、房产信息、信贷记录、征信信息、交易和消费记录、流水记录等、虚拟货币、虚拟交易、游戏类兑换码等虚拟财产、风评记录、资产信息 、信用记录
个人通信信息	短信、彩信、电子邮件以及个人通信的数据（元数据）	通信记录和内容
联系人信息	电子邮箱地址列表	通讯录、好友列表、群组列表
个人应用操作信息	通过日志存储的个人信息主体操作记录，如应用或软件使用记录、点击记录、收藏列表	网站浏览记录
个人常用设备信息	描述个人常用设备基本情况的信息，如硬件序列号、设备MAC地址、软件列表、唯一设备识别码	—
个人位置信息	—	行踪轨迹、精准定位信息、住宿信息、经纬度
其他信息	—	个人音频、视频、图像数据

注1：直连通信范围较小且车辆持续移动，导致数据接收者难以持续获得车辆的行驶路线，车辆行踪泄露风险较低，因此，通过直连通信发送的车辆位置和车辆历史位置信息均可不视为敏感个人信息。

注2：通过将标识车辆的信息（如标识和/或假名证书）频繁随机变化使得直连通信范围内的数据接收者凭借自身资源和技术手段无法识别特定自然人，属于一种匿名化技术。

附 录 B
（资料性）
数据分类与分级映射表

汽车数据分类与分级的映射关系参见表B.1，分级划分参考A.3.2。

表 B.1 数据分类与分级映射表

一级分类名称	二级分类名称	分级映射
车辆基本数据	车辆标识数据	S1/S0
	车辆属性数据	S0
	核心零部件标识数据	S1
	车辆鉴别数据	S1/S2
	车辆维保数据	S1/S2
感知数据	激光雷达数据	车外的个人生物特征数据S2； 车外的个人非生物特征数据S1； 其他车辆车牌S2； 车牌以外的其他车辆信息S0； 车内的个人生物特征（人脸、声纹、指纹等）S2； 车流、人流等交通信息数据S3； 自然条件数据S0； 测绘数据S3； 行踪轨迹数据S2； 单点位置数据（不包含高程）S1/S2。
	毫米波雷达数据	
	摄像头数据	
	超声波雷达数据	
	IMU数据	
	高精地图数据	
	GNSS数据	
	V2X数据	
	语音	
	融合后的目标（机动车及其他道路交通参与者）数据	
	融合后的交通信息数据	
	融合后的自然条件数据	
	融合后的道路属性数据	
	融合后的自车车身姿态	
	融合后的自车位置数据	
	语义	
	声纹	
	其他感知部件收集的数据	
	其他的感知融合数据	
决策数据	人类驾驶员操作数据	挡位信息S2； 加速踏板开度S2； 刹车踏板开度S2； 转向盘角度S2
	远程操作数据	S1/S2

表 B.1　数据分类与分级映射表（续）

一级分类名称	二级分类名称	分级映射
决策数据	系统决策数据	AD系统请求挡位S2； AD系统请求横纵向加速度S2； AD系统请求转向角S2； AD系统请求转向力矩S2； AD系统请求纵向力矩S2； AD系统请求车辆灯光/雨刮状态S2
运行数据	整车状态数据	上电、充电状态S2； 控制、动力模式S2； 挡位信息S2； 制动状态S2； 车灯、雨刮、安全带状态S2； 电池SoH S2； 当前油量、电量数据S2； 累计里程数据S2 实时车速S2； 横纵向加速度S2； 航向角S2； 横摆、侧倾、俯仰角速度S2； 平均和瞬时油耗/电耗S2等
	系统及部件运行状态数据	GNSS运行状态S2； IMU运行状态S2； AD系统运行状态S2； OBU运行状态S2； 各类传感器运行状态S2； OBU、TBox运行状态S2
其他数据	安全日志数据	S2
	其他日志数据	S1
	汽车充电网运行数据	S2/S3
	用户行为汇聚分析数据	S1/S2
	用户身份标识数据	S1
	用户与座舱交互数据（非操控类数据）	S1

附 录 C
（规范性）
个人信息和重要数据处理试验方法及要求

C.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（参数信息应符合附录 D 的要求）；
——试验车辆存储个人信息和重要数据的存储地址。

C.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。

C.3 个人同意的取得试验方法

C.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。
C.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。
C.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。
C.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。

C.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。

C.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。

C.6 个人信息和重要数据传输试验方法

C.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。
C.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。

C.7 个人信息和重要数据删除试验方法

C.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。

C.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。

附 录 D
（规范性）
雷达、摄像头等数据收集设备参数

雷达、摄像头等数据收集设备参数见表D.1、D.2和表D.3。 摄像头数据收集设备参数

序号	摄像头型号	分辨率	水平视场角、垂直视场角（度）	安装位置	涉及功能（有标准要求，依据标准要求填写）	功能解释（若需）及必要性分析	备注
1	示例：××品牌及产品号	示例：1280×960	示例：水平120°、垂直	示例：车辆正前方	示例：自动泊车	非标准功能在此进行解释	
2							

表 D.2 激光雷达数据收集设备参数

序号	激光雷达型号	分辨率	水平视场角、垂直视场角（度）	安装位置	涉及功能	必要性分析
1						
2						
3						

表 D.3 其他传感器数据收集设备参数

序号	其他传感器型号	分辨率	覆盖范围	安装位置	涉及功能	必要性分析
1						
2						
3						

附 录 E
（规范性）
个人信息匿名化处理试验方法

E.1 试验车辆

E.1.1 应提供需要进行个人信息匿名化处理相关的功能清单并明确匿名化处理所涉及的相关传感器信息。

E.1.2 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。

E.1.3 若具备提供匿名化区域范围文件的能力，区域化范围文件可包括矩形、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。

E.2 试验设备

E.2.1 试验记录内容

试验过程中应额外安装试验记录设备并进行记录，至少记录以下内容：

——试验时间轴及试验时长；

——试验车辆周边环境视频信息。

E.2.2 试验记录设备精度

视频收集设备分辨率应不小于(1920×1080)像素，视频采样帧率应至少为30 fps。

E.2.3 试验记录设备安装及运行

试验设备的安装、运行不应影响试验车辆原有配置及其个人信息收集和传输功能的正常运行。

E.2.4 试验结果标注能力要求

E.2.4.1 标注能力图片要求

选取500张已进行匿名化图片和500张未进行匿名化图片进行标注能力验证，图片应满足以下要求：

——未进行匿名化图片集要求如下：

- 至少包含200张人脸目标及200张汽车号牌目标；
- 各人脸目标、车牌目标具备边界框各边长真实像素值说明文档；
- 各人脸目标、车牌目标具备可见范围面积的真实值说明文档。

——已进行匿名化图片集要求如下：

- 至少包含已进行匿名化的200张人脸目标及200张汽车号牌目标；
- 具备各匿名化人脸目标和汽车号牌目标边界框、可见范围各边长真实像素值说明文档；
- 具备各匿名化人脸目标和汽车号牌目标匿名化区域面积及遮盖率的真实值说明文档；
- 与未进行匿名化图片集无相同图片。

注：图片集中的图片非试验过程收集的图片。

E.2.4.2 位置标注能力要求

在开展 E.6.1 的图片标注处理前，应对匿名化目标标注能力进行验证，导入满足 E.2.4.1 的图片集，且满足以下要求：

——在未进行匿名化处理的图片集中，对各图片的人脸边界框进行标注，当人脸边界框最小边长像素真实值大于等于 27 像素时，计算所有边界框的最小边长像素标注值与真实值的比值，平均值大于等于 0.9 且小于等于 1.1；

——在未进行匿名化处理的图片集中，对各图片的汽车号牌边界框进行标注，当汽车号牌边界框最小边长像素真实值大于等于 11 像素时，应满足以下要求：

- 当人脸和汽车号牌边界框最小边长像素真实值小于等于20像素时，最小边长像素标注值与真实值最小边长像素差值绝对值的平均数不超过1像素；
- 当人脸和汽车号牌边界框最小边长像素真实值大于等于20像素时，最小边长像素标注值与真实值比值的平均值大于等于0.9且小于等于1.1。

——在未进行匿名化图片集中，对人脸目标进行可见范围标注，当人脸可见范围小于 100 %的目标且人脸边界框最小边长像素大于等于 27 像素时，计算可见范围面积的标注值与真实值的比值，其平均值大于等于 0.9 且小于等于 1.1；

——在未进行匿名化图片集中，按照 5.6.2.1 要求进行标注，识别出的人脸目标、汽车号牌目标应检数与图片中的实际应检数比值的平均值不小于 0.99 且不大于 1.01；

——在已进行匿名化图片集中，对已进行匿名化图片的匿名化对象进行标注并计算遮盖率，遮盖率小于 100 %的匿名化对象中，计算遮盖率和真实遮盖率差值绝对值的平均数不超过 5 %；

——在已进行匿名化的图片集中，按照 5.6.2.1 要求进行标注，计算人脸目标、汽车号牌目标正检数、漏检数，对比与图片中的实际正检数、漏检数比值的平均值不小于 0.98 且不大于 1.02。

E.3 匿名化处理性能要求试验过程

E.3.1 试验车辆启动车外人脸及汽车号牌图像或视频数据匿名化处理和车外传输功能。

E.3.2 试验过程应开启试验记录设备。

E.4 匿名化处理性能要求试验结束条件

E.4.1 总体要求

匿名化处理性能要求试验应在满足 E.4.2 和 E.4.3 的要求后结束。

E.4.2 试验历尽性要求

收集的数据应包括E.1.1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10 s，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。

E.4.3 匿名化对象数量要求

匿名化对象数量应满足以下要求：

——若试验车辆输出图片，采集间隔大于等于 1 s 的图片数量不小于 500 张；

——若试验车辆输出视频，每段视频不少于 10 s，总长度不小于 1000 s；

——经过匿名化处理的人脸目标数量不少于 200 个，其中相同人脸目标在不同图片内分别计数；

——经过匿名化处理的汽车号牌目标数量不少于 200 个，其中相同汽车号牌目标在不同图片内分

别计数。

E.5 匿名化处理性能要求试验结果处理

E.5.1 试验结果后处理

E.5.1.1 试验过程中或试验结束后，于试验车辆读取已进行匿名化处理的图像或视频，若存在且可读取匿名化区域范围文件，读取该文件。

E.5.1.2 试验过程中或试验结束后，于试验记录设备读取可反映实际行驶过程的图像和（或）视频。

E.5.1.3 基于 6.1.1 读取数据进行以下后处理：

——若试验车辆输出的文件包含匿名化处理后的视频，相隔固定帧数或相隔固定时间间隔进行抽帧处理且每 2 s 提取图片不大于 1 张、提取图片数量应不少于 500 张；

——在直接输出或抽帧后的图片中标注人脸边界框、汽车号牌边界框和已进行匿名化区域。

E.5.1.4 在读取匿名化处理的图像、视频和对视频进行抽帧及标注处理过程中，不应改变匿名化处理后图片的尺寸和分辨率。

E.5.2 遮盖率计算过程

根据E.6.1.3处理的试验结果，计算遮盖率。

E.5.3 检出率计算过程

E.5.3.1 人脸目标正检数计算方式

当人脸目标满足以下要求时，应记入人脸目标的正检数：

——满足5.6.2.1.1要求并进行匿名化处理；

——交并比大于等于50 %。

E.5.3.2 人脸目标漏检数计算方式

当人脸目标满足以下要求时，应记入人脸目标的漏检数：

——满足5.6.2.1.1要求；

——遮盖率小于50 %。

示例：图片中存在已佩戴口罩的人脸目标如图 E.1 所示，人脸目标未进行匿名化处理，根据人脸目标边界框比对，可见范围大于 50 %，可见范围内包括眉毛和眼睛，可清晰定位，该目标计入漏检数。

图 E.1 匿名化漏检数结果示例

E.5.3.3 人脸检出率计算方式

按照公式（E.1）计算人脸检出率。

$$R_{df} = N_{af}/(N_{af} + N_{mf}) \cdots\cdots (E.1)$$

式中：

R_{df} ——人脸检出率；

$N_{af} + N_{mf}$——人脸应检数；

N_{af} ——满足E.5.3.4要求的正检数；

N_{mf} ——满足E.5.3.5要求的漏检数。

E.5.3.4 汽车号牌正检数计算方式

当汽车号牌目标满足以下要求时，应记入汽车号牌目标的正检数：

——满足5.6.2.1.2要求且进行匿名化处理；

——遮盖率大于等于50 %。

E.5.3.5 汽车号牌漏检数计算方式

当汽车号牌目标满足以下要求时，应记入汽车号牌目标的漏检数：

——满足5.6.2.1.2要求；

——遮盖率小于50 %。

E.5.3.6 汽车号牌检出率计算方式

按照公式（E.2）计算人脸检出率。

$$R_{dv} = N_{av}/(N_{av} + N_{mv}) \cdots\cdots (E.2)$$

式中：

R_{dv} ——汽车号牌检出率；

$N_{av} + N_{mv}$——汽车号牌应检数；

N_{av} ——满足E.5.3.4要求的正检数；

N_{mv} ——满足E.5.3.5要求的漏检数。

E.6 匿名化处理方法确认

E.6.1 机器识别试验方法

E.6.1.1 人脸不可识别性试验方法

选择两种具备人脸识别功能的算法模型对计入人脸正检数的所有匿名化目标进行识别。例如开源模型（insightface）和公安模型。

E.6.1.2 汽车号牌不可识别性试验方法

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正检数的匿名化目标进行识别，例如CRNN算法。

E.6.2 人工识别试验方法

E.6.2.1 分别随机挑选100张已经完成匿名化处理的图片，由人工对计入人脸和汽车号牌正检数的匿名化目标进行识别。

E.6.2.2　评估任一计入人脸正检数的匿名化目标双眼、鼻子、嘴巴是否均无法确定全部轮廓范围。

E.6.2.3　评估任一计入汽车号牌正检数的匿名化目标的汽车号牌内容是否可全部识别。

附 录 F
（资料性）
匿名化误检率试验方法

F.1 人脸误检数计算方式

当匿名化目标满足以下要求时，应记入人脸目标的误检数：
——被标记为人脸目标并进行匿名化处理；
——与任一人脸目标不存在交集。

注：若匿名化目标中包含广告牌、光滑表面倒影中出现的具有人脸目标特征的图像，不计入误检数。按照要求进行脱敏处理的除车辆号牌及人脸外的其他目标物不计入误检数。

示例1：动物面部进行匿名化处理且标记为人脸目标，记入误检数。

示例2：匿名化区域出现于头部上方、与人脸目标无交集且标记为人脸目标，记入误检数。

示例3：匿名化区域与人脸目标有交集，不计入误检数。

F.2 人脸检出数计算方式

被试验车辆匿名化系统标记为人脸的匿名化对象的总数量。

F.3 人脸误检率计算方式

人脸误检率计算方法见公式（F.1）。

$$R_{Ff} = N_{Ff}/N_{df} \quad \text{(F.1)}$$

式中：
R_{Ff}——人脸误检率；
N_{Ff}——满足F.1要求的误检数；
N_{df}——满足F.2的检出数。

F.4 汽车号牌误检数计算方式

当匿名化目标满足以下要求时，应记入汽车号牌目标的误检数：
——被系统标记为汽车号牌并进行匿名化处理；
——与任一汽车号牌目标不存在交集。

注1：若匿名化目标中包含电动自行车、摩托车号牌、机动车临时号牌并标记为汽车号牌目标，不计入误检数。

注2：若匿名化目标中包含喷涂的放大汽车号牌、广告牌、光滑表面倒影中出现的具有汽车号牌目标特征的图像，不计入误检数。

示例1：电线杆、垃圾桶等区域出现匿名化区域且标记为汽车号牌目标，记入误检数。

示例2：匿名化区域与汽车号牌目标有交集，不计入误检数。

F.5 汽车号牌检出数计算方式

被标记为汽车号牌目标的匿名化对象的总数量。

F.6 汽车号牌误检率计算方式

汽车号牌误检率计算方法见公式（F.2）。

$$R_{FV} = N_{Fv}/N_{df} \quad \text{(F.2)}$$

式中：

R_{FV}——人脸误检率；

N_{Fv}——满足F.4要求的误检数；

N_{df}——满足F.5的检出数。