ICS 43.020
CCS T 40

中华人民共和国国家标准

GB/T 44464—2024

汽车数据通用要求

General requirements of vehicle data

2024-08-23 发布　　2024-08-23 实施

国家市场监督管理总局
国家标准化管理委员会　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专利的责任。

本文件由中华人民共和国工业和信息化部提出。

本文件由全国汽车标准化技术委员会(SAC/TC 114)归口。

本文件起草单位：工业和信息化部装备工业发展中心、中国汽车技术研究中心有限公司、北京地平线信息技术有限公司、重庆长安汽车股份有限公司、长城汽车股份有限公司、蔚来汽车科技(安徽)有限公司、上海机动车检测认证技术研究中心有限公司、华为技术有限公司、广州小鹏汽车科技有限公司、比亚迪汽车工业有限公司、高通无线通信技术(中国)有限公司、北京赛目科技股份有限公司、中国信息通信科技集团有限公司、中国软件评测中心(工业和信息化部软件与集成电路促进中心)、北京车和家汽车科技有限公司、北京汽车研究总院有限公司、三六零数字安全科技集团有限公司、斑马网络技术有限公司、梅赛德斯一奔驰(中国)投资有限公司、沃尔沃汽车(亚太)投资控股有限公司、泛亚汽车技术中心有限公司、宝马(中国)服务有限公司、一汽解放汽车有限公司、吉利汽车研究院(宁波)有限公司、国家工业信息安全发展研究中心、国汽(北京)智能网联汽车研究院有限公司、安徽江淮汽车集团股份有限公司、大众汽车(中国)投资有限公司、上海临港绝影智能科技有限公司、北京百度智行科技有限公司、东软睿驰汽车技术(沈阳)有限公司、博泰车联网科技(上海)股份有限公司、上海淞泓智能汽车科技有限公司。

本文件主要起草人：邱彬、吴含冰、孙航、解瀚光、张路、田生明、张小东、金秀莲、夏显召、赵梓健、潘凯、陈金凤、钟益林、王江胜、张亚楠、李广友、侯昕田、白智敏、房家奕、王伟、张春旺、牟洪雨、严敏睿、满志勇、刘帆、李彤、顾今今、吴岩、赵超、夏欢、潘妍、陈桂华、朱陈伟、赵闻、石建萍、程周、祁帅、李予佳、李雪松、滕添益、邹博松、邹雪、唐焱、霍燕燕。

汽车数据通用要求

1 范围

本文件规定了汽车产品在研发设计和生产制造过程中产生和收集的数据的一般要求、个人信息保护要求、重要数据保护要求、审核评估及试验要求，描述了相应试验方法。

本文件适用于汽车产品及汽车数据处理者。

2 规范性引用文件

本文件没有规范性引用文件。

3 术语和定义

下列术语和定义适用于本文件。

3.1

收集 collect

通过一定方式获取汽车数据的行为。

3.2

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

对汽车数据处理活动过程进行规范以确保汽车数据安全的系统性方法。

3.3

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各种方式从汽车座舱收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，有修改]

3.4

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，有修改]

3.5

人脸目标 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。

3.6

人脸边界框 face boundary frame

覆盖人脸目标的最小矩形或旋转矩形。

示例：人脸边界框示意图见图1。

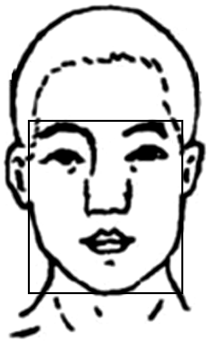

图 1　人脸边界框示意图

3.7

汽车号牌目标　vehicle license plate object

安装于汽车、基材为金属的正式机动车号牌。

注：不包含喷涂的放大号牌、纸质临时机动车号牌。

3.8

汽车号牌边界框　vehicle license plate boundary frame

汽车号牌目标外沿组成的最小矩形或旋转矩形。

3.9

遮盖率　mask covering rate

人脸或汽车号牌边界框内进行匿名化处理的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。其中实线部分为人脸边界框区域，虚线部分为已进行匿名化处理区域，阴影部分为实线部分与虚线部分重叠的区域，遮盖率为阴影部分与实线部分的面积比值。

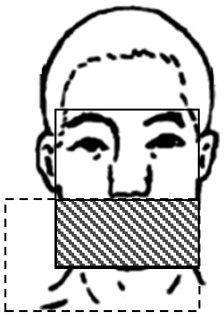

图 2　遮盖率示意图

3.10

检出率　detection rate

人脸或汽车号牌目标的正检数占应检数的百分比。

注 1：正检数是按照本文件要求已进行匿名化处理的目标数量。

注 2：应检数是按照本文件要求应进行匿名化处理的目标数量。

3.11

误检率　false detection rate

人脸或汽车号牌目标的误检数占检出目标数的百分比。

注 1：检出目标数是被标记为匿名化对象并进行匿名化处理的目标数量。

注 2：误检数是检出目标数中不满足本文件匿名化对象定义的目标数量。

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并实施汽车数据安全管理体系，采取汽车数据安全保护技术措施，保证汽车数据持续处于有效保护和合法利用的状态。

4.1.2 汽车数据处理者应制定汽车数据安全目标、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。

4.1.3 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。

4.1.4 汽车数据处理者应建立汽车数据分类分级制度，形成汽车数据资产管理台账。

注：汽车数据分类分级示例见附录 A。

4.1.5 汽车数据处理者应针对汽车数据全生命周期，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。

4.1.6 汽车数据处理者至少应针对研发设计和生产制造等车辆全生命周期环节制定数据安全流程管理制度。

注：运维及报废等其他环节参照执行。

4.1.7 汽车数据处理者如需存储在中华人民共和国境内收集和产生的个人信息和重要数据，应在境内存储；如需向境外提供，应通过数据出境安全评估。

4.1.8 汽车数据处理者应建立汽车数据安全风险监测和事件管理制度，发现汽车数据安全风险时，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，并应按照规定对重要数据的处理活动定期开展风险评估，向有关主管部门报送风险评估报告。

4.1.9 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处理用户投诉举报。

4.1.10 汽车数据处理者应建立对数据处理相关方的数据安全管理制度，包括签订数据安全协议、核验数据安全保护能力等内容。

4.2 汽车数据处理一般要求

4.2.1 汽车数据处理者处理汽车产品研发设计和生产制造过程中产生和收集的个人信息时，应符合第 5 章的要求，强制性国家标准规定的其他情形除外；汽车产品应具备相应的能力，保障汽车数据处理者处理个人信息时符合第 5 章的要求或者符合法律、行政法规和强制性国家标准规定的其他情形。

4.2.2 汽车产品应具备相应的能力，保障汽车数据处理者处理个人信息时车内处理和默认不收集应符合 5.1 的要求，精度范围适用应符合 5.3 的要求，采用匿名化进行脱敏处理应符合 5.6 的要求，显著告知应符合 5.2 的要求。

4.2.3 汽车数据处理者处理汽车产品研发设计和生产制造过程中产生和收集的重要数据时，应符合第 6 章的要求，强制性国家标准规定的其他情形除外；汽车产品应具备相应的能力，保障汽车数据处理者处理重要数据时符合第 6 章的要求或者符合法律、行政法规和强制性国家标准规定的其他情形。

4.2.4 汽车数据处理者处理的汽车产品研发设计和生产制造过程中产生和收集的数据既属于个人信息又属于重要数据时，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 有下列例外情形之一的，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；

——在合理范围内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；

——法律、行政法规和强制性国家标准等规定的其他情形。

汽车数据处理者应通过用户手册、车载显示面板、语音、汽车使用相关应用程序等至少一种形式说明取得个人同意的例外情形及理由。

5.1.3 除取得个人同意和满足 5.1.2 所列例外情形外，汽车不应向车外提供座舱数据。

5.1.4 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。

5.1.5 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。

5.1.6 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；

——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，除存储和采取必要的安全保护措施之外，汽车数据处理者应停止处理个人信息。

5.2 个人同意

5.2.1 个人同意一般要求

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。以上两种情形应通过至少一种显著方式向个人告知，清晰地说明处理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。

——告知方式可选取用户手册、车载显示面板、语音、汽车使用相关应用程序等。

——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

汽车数据处理者应按以下要求设置取得个人同意的选项：

——提供同意和拒绝的方式；

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

5.2.3 重新取得个人同意

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 当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时，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撤回个人同意的途径。

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

5.4 个人信息存储

5.4.1 车辆应采取安全访问技术、加密技术或其他安全技术保护存储在车内的敏感个人信息，防止其被非授权访问和获取。

5.4.2 车辆应采取安全防御机制保护存储在车内的车辆识别代号（VIN）等用于车辆身份识别的数据，防止其被非授权删除和修改。

注：防止数据被非授权删除和修改的安全防御机制包括安全访问技术、只读技术等。

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 不应将个人生物特征识别作为实现个人身份认证功能的唯一手段。

5.6 个人信息传输

5.6.1 车外传输要求

5.6.1.1 车辆应对向车外发送的敏感个人信息实施保密性保护措施。

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或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 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：

——人脸边界框最小边长像素大于或等于 32 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。

注 1：可见范围比值指人脸目标可见范围与人脸目标的面积比值，其中可见范围为人脸边界框内能直接观察到的人脸目标的区域。

注 2：广告牌、光滑表面倒影中出现的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或等于 16 像素；

——汽车号牌目标无遮挡且可识别全部数字及文字内容。

5.6.2.2 匿名化处理性能要求

5.6.2.2.1 匿名化检出率

人脸目标和汽车号牌目标的匿名化检出率均应大于或等于 90%。

注：匿名化检出率计算方法见附录 B。

5.6.2.2.2 匿名化误检率

人脸目标和汽车号牌目标的匿名化误检率均宜小于或等于 10%。

注：匿名化误检率计算方法见附录 C。

5.6.2.3 匿名化效果

满足 5.6.2.1 要求并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 若个人请求删除敏感个人信息，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且不可访问。

5.8 个人信息出境

车辆不应直接向境外传输个人信息等数据。

注：用户使用浏览器访问境外网站、使用通信软件向境外传递消息、自主安装可能导致数据出境的第三方应用等用户自主行为不受本条限制。

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数据的状态，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时，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

车辆应采取安全访问技术、加密技术或其他安全技术保护存储在车内的重要数据，防止其被非授权访问和获取。

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

车辆应对向车外发送的重要数据实施保密性保护措施。

6.6 重要数据删除

被删除的重要数据应不可检索且不可访问。

6.7 重要数据出境

车辆不应直接向境外传输重要数据等数据。

注：用户使用浏览器访问境外网站、使用通信软件向境外传递消息、自主安装可能导致数据出境的第三方应用等用户自主行为不受本条限制。

7 审核评估及试验要求

7.1 汽车数据处理者应通过满足 4.1 要求的符合性评估。

7.2 应根据附录 B 对车辆进行个人信息匿名化处理试验，应根据附录 D 对车辆进行个人信息及重要数据处理试验，并满足各试验对应的要求。

7.3 宜根据附录 C 对车辆进行匿名化误检率试验。

附 录 A
（资料性）
汽车数据分类分级示例

A.1 数据分类分级原则

汽车数据分类分级原则如下。

——合规性：遵循国家法律法规及相关主管部门有关规定；符合工业和信息化领域数据安全管理相关标准要求。

——科学性：按照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：确保每个类目下要有数据，不设没有意义的类目。

——扩展性：具有概括性和包容性，能够实现各种类型数据的分类和分级，以满足将来可能出现的数据类型及数据级别。

——显著性：根据数据内容的显著特征确定数据的分类方案。

——可行性：避免规则过于复杂以保证数据分类分级的可行性。

——时效性：具有一定的有效期限并及时调整。

——稳定性：基于数据最稳定的特征和属性，对同一级别的数据适用相同的安全要求。

A.2 数据分类

汽车数据处理者依据相关法律法规及标准要求对汽车产品在研发设计和生产制造过程中产生和收集的数据进行分类。

A.3 数据分级

A.3.1 分级要素

A.3.1.1 要素类型

汽车数据处理者根据影响对象和影响程度对汽车产品在研发设计和生产制造过程中产生和收集的数据进行分级。

A.3.1.2 影响对象

影响对象指汽车产品在研发设计和生产制造过程中产生和收集的数据遭到篡改、破坏、泄露或者非法获取、非法利用后受到影响的对象，包括国家安全、行业安全、组织安全、个人权益，其中：

——影响对象为国家安全的情况，是指数据一旦遭到泄露篡改、破坏或者非法获取，可能会对国家政治安全、国家经济安全、国家公共安全、国家资源安全、国家科技安全、国家网络安全等造成影响；

——影响对象为行业安全的情况，是指数据一旦遭到泄露篡改、破坏或者非法获取，可能会对汽车行业供应链安全、汽车行业关键设施、汽车行业核心技术等造成影响；

——影响对象为组织安全的情况，是指数据一旦遭到泄露篡改、破坏或者非法获取，可能会对组织技术研究和产品开发、组织生产制造、组织运营等造成影响；

——影响对象为个人权益的情况，是指数据一旦遭到泄露篡改、破坏或者非法获取，可能导致自然

人的人格尊严或人身、财产安全等个人信息主体合法权益受到侵害。

A.3.1.3 影响程度

影响程度从高到低可分为严重危害、一般危害、轻微危害、无影响。对不同影响对象进行影响程度判断时，采取的基准不同。如果影响对象是国家安全、行业安全，则以国家、社会或行业领域的整体利益作为判断影响程度的基准；如果影响对象仅是组织或个人权益，则以组织或公民个人的权益作为判断影响程度的基准。

A.3.2 分级方法

汽车产品在研发设计和生产制造过程中产生和收集的数据分级方法见表 A.1，分为核心数据、重要数据、一般数据。其中重要数据中关系国家安全、国民经济命脉、重要民生、重大公共利益等数据属于核心数据。

表 A.1 数据分级方法

影响对象	影响程度			
	严重危害	一般危害	轻微危害	无影响
国家安全	重要数据	重要数据	重要数据	一般数据
行业安全	重要数据	重要数据	一般数据	一般数据
组织安全	一般数据	一般数据	一般数据	一般数据
个人权益	一般数据	一般数据	一般数据	一般数据
注：如果影响大规模的组织或个人权益，影响对象可能不只包括组织权益或个人权益，也可能对国家安全、行业安全造成影响。				

示例：在汽车产品研发设计过程中，收集和产生的与汽车行业竞争力相关的高价值敏感数据属于重要数据，如与行业核心技术竞争力相关、代表行业先进水平或泄露后对行业发展产生重大影响的算法开发所使用的数据等。

A.3.3 其他原则

数据分级除表 A.1 中的方法外遵循以下原则：

a) 同一数据由于数据量的增加可能会造成数据级别上升；

b) 不同种类数据的组合可能会造成数据级别上升。

A.4 个人信息分类分级示例

个人信息分类分级示例见表 A.2。

表 A.2　个人信息分类分级示例

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、家庭关系等	—
个人身份信息	个人账户的系统账号等(不包含密码)	身份证、驾驶证、个人账户的系统账号等(包含密码)
个人车辆标识	VIN、车牌号、行驶证等	—
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
个人财产信息	—	虚拟财产、风评记录、资产信息、信用记录等
个人通信信息	短信、电子邮件以及个人通信等	通信记录和内容等
联系人信息	电子邮箱地址列表等	通讯录、好友列表、群组列表等
个人应用操作信息	应用或软件使用或点击记录、收藏列表等	网站浏览记录等
个人常用设备信息	硬件序列号、设备 MAC 地址、软件列表、唯一设备识别码等	—
个人位置信息	—	行踪轨迹、精准定位信息、经纬度等
其他信息	—	个人音频、视频、图像数据等

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。

注 3：一般个人信息指除敏感个人信息外的其他个人信息。

附 录 B
（规范性）
个人信息匿名化处理试验方法

B.1 试验条件

B.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。

B.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。

B.1.3 若具备提供匿名化区域范围文件的能力，匿名化区域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（人脸目标、汽车号牌目标）和记录时间。

B.2 试验设备

B.2.1 试验设备记录内容

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。

B.2.2 试验记录设备精度

试验记录设备分辨率应不小于(1 920×1 080)像素，视频采样帧率应至少为 30 f/s。

B.2.3 试验记录设备安装及运行

试验记录设备的安装、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。

B.2.4 试验结果标注能力要求

B.2.4.1 标注能力图片集要求

选取 500 张已进行匿名化处理的图片和 500 张未进行匿名化处理的图片组成图片集进行标注能力验证，图片集应满足以下要求。

——未进行匿名化处理的图片集：

- 至少包含 200 个人脸目标及 200 个汽车号牌目标；
- 具备各人脸目标、汽车号牌目标边界框各边长真实像素值的说明文档；
- 具备各人脸目标可见范围面积真实值的说明文档。

——已进行匿名化处理的图片集：

- 至少包含已进行匿名化处理的 200 个人脸目标及 200 个汽车号牌目标；
- 具备各人脸目标、汽车号牌目标边界框各边长真实像素值的说明文档；
- 具备各人脸目标可见范围面积真实值的说明文档；
- 具备经过匿名化处理的各人脸目标和汽车号牌目标匿名化区域面积及遮盖率真实值的说明文档；

- 与未进行匿名化处理的图片集无相同图片。

注：图片集中的图片为非试验过程中收集的图片。

B.2.4.2 标注精度要求

在开展 B.5.1 的图片标注处理前，导入满足 B.2.4.1 的图片集并对标注能力进行验证，标注精度应满足以下要求。

——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或等于 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，比值大于或等于 0.9 且小于或等于 1.1 的边界框数量占所有人脸边界框数量的 98％以上。

——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或等于 11 像素时：

- 当汽车号牌边界框最小边长像素真实值小于或等于 20 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差值绝对值，其平均值小于或等于 1 像素；
- 当汽车号牌边界框最小边长像素真实值大于 20 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，其平均值大于或等于 0.9 且小于或等于 1.1。

——在未进行匿名化处理的图片集中，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或等于 27 像素时，计算可见范围面积的标注值与真实值的比值，其平均值大于或等于 0.9 且小于或等于 1.1。

——在未进行匿名化处理的图片集中，按照 5.6.2.1 的要求进行标注，识别出的实际应检的人脸目标、汽车号牌目标的数量与图片中实际的应检数的比值大于或等于 0.99 且小于或等于 1.01。

——在已进行匿名化处理的图片集中，对所有已进行匿名化处理的对象进行标注并计算遮盖率，其中对于遮盖率小于 100％的匿名化对象，通过标注计算的遮盖率和真实遮盖率差值绝对值的平均值小于或等于 5％。

——在已进行匿名化处理的图片集中，按照 5.6.2.1 的要求进行标注，计算人脸目标、汽车号牌目标正检数、漏检数，与真实正检数、漏检数的比值大于或等于 0.98 且小于或等于 1.02。

B.3 匿名化处理性能要求试验过程

B.3.1 试验车辆启动车外人脸目标及汽车号牌目标图像或视频匿名化处理和车外传输功能。

B.3.2 试验过程开启试验记录设备。

B.4 匿名化处理性能要求试验结束条件

B.4.1 总体要求

匿名化处理性能要求试验应在满足 B.4.2 和 B.4.3 的要求后结束。

B.4.2 试验历尽性要求

收集的数据应包括 B.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 张或视频应不小于 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。

B.4.3 试验图片及视频要求

试验过程中收集的图片或视频应满足以下要求：

——若试验车辆输出图片，图片收集时间间隔大于或等于 1 s 的图片数量不少于 500 张；

——若试验车辆输出视频，每段视频时长不小于 10 s，所有视频总时长不小于 1 000 s；

——满足本文件要求需要进行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；

——满足本文件要求需要进行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。

B.5 试验结果处理

B.5.1 试验数据读取

B.5.1.1 试验结束后，读取试验车辆已进行匿名化处理的图片或视频，若可读取匿名化区域范围文件，读取该文件。

B.5.1.2 试验结束后，读取试验记录设备可反映实际行驶过程的视频。

B.5.1.3 基于B.5.1.1读取的数据进行以下处理：

——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秒提取图片数量应不多于1张，提取图片总数量应不少于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、人脸目标可见范围和已进行匿名化处理的区域。

B.5.1.4 在读取匿名化处理的图片、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。

B.5.2 遮盖率计算过程

根据B.5.1.3处理的试验结果，计算遮盖率。

B.5.3 检出率计算过程

B.5.3.1 人脸目标正检数计算方式

当人脸目标均满足以下要求时，应计入人脸目标的正检数：

——满足5.6.2.1.1的要求并进行匿名化处理；

——遮盖率大于或等于50%。

B.5.3.2 人脸目标漏检数计算方式

当人脸目标均满足以下要求时，应计入人脸目标的漏检数：

——满足5.6.2.1.1的要求；

——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B.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B.1 匿名化漏检数结果示例

B.5.3.3 人脸目标检出率计算方法

按照公式(B.1)计算人脸目标检出率。

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

式中：

R_{df} ——人脸目标检出率；

$N_{af}+N_{mf}$ ——人脸目标应检数；

N_{af} ——满足 B.5.3.1 要求的正检数；

N_{mf} ——满足 B.5.3.2 要求的漏检数。

B.5.3.4 汽车号牌目标正检数计算方式

当汽车号牌目标满足以下要求时，应计入汽车号牌目标的正检数：

——满足 5.6.2.1.2 的要求且进行匿名化处理；

——遮盖率大于或等于 50%。

B.5.3.5 汽车号牌目标漏检数计算方式

当汽车号牌目标满足以下要求时，应计入汽车号牌目标的漏检数：

——满足 5.6.2.1.2 的要求；

——遮盖率小于 50%。

B.5.3.6 汽车号牌目标检出率计算方法

按照公式(B.2)计算汽车号牌目标检出率。

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

式中：

R_{dv} ——汽车号牌目标检出率；

$N_{av}+N_{mv}$ ——汽车号牌目标应检数；

N_{av} ——满足 B.5.3.4 要求的正检数；

N_{mv} ——满足 B.5.3.5 要求的漏检数。

B.6 匿名化处理效果评估

B.6.1 机器识别试验方法

B.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目标正检数的所有匿名化目标进行识别，例如开源模型、公安模型等。评估任一计入人脸目标正检数的匿名化目标是否被识别为人脸目标。

B.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目标正检数的所有匿名化目标进行识别，例如 CRNN 算法等。评估任一计入汽车号牌目标正检数的匿名化目标的汽车号牌内容是否可全部识别。

B.6.2 人工识别试验方法

B.6.2.1 分别随机挑选100张已经完成匿名化处理的图片，由试验人员对计入人脸目标和汽车号牌目标正检数的匿名化目标进行识别。

B.6.2.2 评估任一计入人脸目标正检数的匿名化目标是否可确定双眼、鼻子和嘴的全部轮廓范围。

B.6.2.3 评估任一计入汽车号牌目标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 C
（资料性）
匿名化误检率计算方法

C.1 人脸目标误检数计算方式

当匿名化对象满足以下要求时，计入人脸目标的误检数：

——被试验车辆匿名化系统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。

若匿名化对象中包含广告牌、光滑表面倒影中出现的人脸目标图像，不计入误检数。按照法律、行政法规和强制性国家标准等规定的其他要求对除汽车号牌及人脸外的其他目标物进行脱敏处理的，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，计入误检数。

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，计入误检数。

示例 3：匿名化区域与人脸目标有交集，不计入误检数。

C.2 人脸目标检出数计算方式

被试验车辆匿名化系统标记为人脸目标的匿名化对象的总数量。

C.3 人脸目标误检率计算方法

人脸目标误检率计算方法见公式(C.1)。

$$R_{Ff} = N_{Ff} / N_{df} \qquad \cdots\cdots (C.1)$$

式中：

R_{Ff} ——人脸目标误检率；

N_{Ff} ——满足 C.1 要求的误检数；

N_{df} ——满足 C.2 要求的检出数。

C.4 汽车号牌目标误检数计算方式

当匿名化对象满足以下要求时，计入汽车号牌目标的误检数：

——被试验车辆匿名化系统标记为汽车号牌目标并进行匿名化处理；

——与任一汽车号牌目标不存在交集。

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。

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汽车号牌目标图像，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，计入误检数；

示例 2：匿名化区域与汽车号牌目标有交集，不计入误检数。

C.5 汽车号牌目标检出数计算方式

被试验车辆匿名化系统标记为汽车号牌目标的匿名化对象的总数量。

C.6 汽车号牌目标误检率计算方法

汽车号牌目标误检率计算方法见公式(C.2)。

$$R_{Fv} = N_{Fv} / N_{df} \quad \cdots\cdots (C.2)$$

式中：

R_{Fv} ——汽车号牌目标误检率；

N_{Fv} ——满足 C.4 要求的误检数；

N_{df} ——满足 C.5 要求的检出数。

附 录 D
（规范性）
个人信息和重要数据处理试验方法

D.1 试验输入信息

试验开始前，应提供以下信息：

a） 试验车辆涉及的处理个人信息和重要数据的功能清单；

b） 撤回个人同意途径清单；

c） 符合表 D.1 的试验车辆数据收集设备参数信息；

d） 试验车辆存储个人信息和重要数据的存储地址。

表 D.1 数据收集设备参数

序号	设备类型	设备型号	分辨率	覆盖范围	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）	激光雷达/摄像头	××品牌及产品号	1 280×960	水平视场角：×× 垂直视场角：××	车辆正前方	自动泊车	非标准功能在此进行解释	
2								

D.2 个人同意试验方法

D.2.1 按照处理个人信息的功能清单，启动除 5.1.2 所列例外情形外的试验车辆各项个人信息处理功能，检查并记录告知方式、告知内容和个人同意的方式，判定试验结果是否符合 5.2.1、5.2.2 的要求。

D.2.2 按照处理个人信息的功能清单，当各项个人信息处理功能的同意期届满后，启动除 5.1.2 所列例外情形外的试验车辆各项个人信息处理功能，检查是否重新取得个人同意并记录个人同意的方式，判定试验结果是否符合 5.2.3.1 的要求。

D.2.3 按照处理个人信息的功能清单，变更部分功能的个人信息处理目的、处理方式或处理的个人信息种类，启动相应功能，检查是否重新取得个人同意并记录个人同意的方式，判定试验结果是否符合 5.2.3.2 的要求。

D.2.4 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，判定试验结果是否符合 5.2.4 的要求。

D.3 个人信息和重要数据收集试验方法

按照试验车辆雷达和摄像头等数据收集设备的参数信息，对比功能清单中各项功能所需的数据收集设备精度，记录试验结果，判定试验结果是否符合 5.3 和 6.2 的要求。

D.4 个人信息和重要数据存储试验方法

D.4.1 按照个人信息和重要数据处理功能清单和存储地址清单，确认测试零部件，依次触发车辆记录

敏感个人信息、重要数据的功能，并按照以下测试方法依次开展测试，判定试验结果是否符合 5.4.1、6.3 的要求：

a) 若采用安全访问技术保护存储的敏感个人信息和重要数据，依据敏感个人信息、重要数据存储区域和地址范围说明，通过零部件调试接口，使用未添加访问控制权限的用户访问存储的敏感个人信息和重要数据，测试是否能非授权访问敏感个人信息和重要数据；

b) 若采取加密技术保护存储的敏感个人信息和重要数据，依据敏感个人信息、重要数据存储区域和地址范围说明，通过零部件调试接口，使用软件分析工具提取存储的敏感个人信息和重要数据，测试是否为密文存储；

c) 依次触发车辆记录敏感个人信息和重要数据的功能，然后依据系统登录方式进入系统，对测试零部件进行敏感个人信息和重要数据检索，测试是否可检索出不在敏感个人信息和重要数据功能清单和存储地址清单中存储的敏感个人信息和重要数据。

D.4.2 按照车辆内存储的 VIN 等用于车辆身份识别的数据清单及存储地址，确定测试零部件，使用软件分析工具非授权删除和修改存储在车辆内的 VIN 等用于车辆身份识别的数据，判定车辆是否满足 5.4.3、6.3.3 的要求。

D.5 个人信息使用试验方法

按照处理个人信息的功能清单，选择使用个人生物识别信息进行身份认证的功能，停止收集个人生物识别信息，检查相应的身份认证功能是否正常运行，记录试验结果，判定试验结果是否符合 5.5.2 的要求。

D.6 个人信息和重要数据传输试验方法

D.6.1 按照处理个人信息的功能清单，选取除 5.1.2 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，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，判定试验结果是否符合 5.1.3 的要求。

D.6.2 按照处理个人信息、重要数据的功能清单，触发车辆向外传输敏感个人信息、重要数据的功能，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，检查是否对车辆传输的敏感个人信息、重要数据进行加密，判定试验结果是否符合 5.6.1.1 和 6.5 的要求。

D.6.3 按照处理个人信息的功能清单，启动符合 5.6.1.2 所规定情形的相应功能，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，判定试验结果是否符合 5.6.1.2 的要求。

D.7 个人信息和重要数据删除试验方法

D.7.1 按照处理个人信息的功能清单，选取涉及处理敏感个人信息的功能，若相应功能涉及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，判定试验结果是否符合 5.7.1 的要求。

D.7.2 按照个人信息和重要数据处理功能清单，选取个人信息和重要数据存储在车端的相关功能，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，判定试验结果是否符合 5.7.2 和 6.6 的要求。

D.8 个人信息和重要数据出境试验方法

开启车辆全部移动蜂窝通信通道和无线局域网（WLAN）通信通道，依次模拟测试车辆处于未上电、仅上电、各项预装的数据传输功能正常启用的状态，并使用网络数据抓包工具对对外通信网络通道同时抓包，且总抓包时长不少于 3 600 s，解析通信报文数据，检查目的 IP 地址中是否包含境外 IP 地址，判定车辆是否满足 5.8 和 6.7 要求。

参 考 文 献

[1] GB/T 35273—2020 信息安全技术 个人信息安全规范
[2] GB/T 41871—2022 信息安全技术 汽车数据处理安全要求