



# 中华人民共和国国家标准

GB 44464—XXXX  
代替 GB/T 44464—2024

## 汽车数据安全问题

Requirements for vehicle data security

（征求意见稿）

本草案完成时间：2026 年 9 月 10 日

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX – XX – XX 发布

XXXX – XX – XX 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 .....                         | 1  |
| 1 范围 .....                       | 3  |
| 2 规范性引用文件 .....                  | 3  |
| 3 术语和定义 .....                    | 3  |
| 4 安全保障要求 .....                   | 5  |
| 5 安全基本要求 .....                   | 6  |
| 6 安全技术要求 .....                   | 7  |
| 7 汽车数据安全保障要求检验方法 .....           | 11 |
| 8 汽车数据安全基本要求检验方法 .....           | 13 |
| 9 汽车数据安全技术要求试验方法 .....           | 15 |
| 10 同一型式判定 .....                  | 25 |
| 11 标准的实施 .....                   | 27 |
| 附 录 A（规范性）车型功能汽车数据处理活动清单要求 ..... | 28 |
| 附 录 B（规范性）车辆常见功能必要个人信息范围要求 ..... | 31 |
| 附 录 C（规范性）个人信息分类分级要求 .....       | 32 |
| 附 录 D（规范性）汽车重要数据识别要求 .....       | 34 |
| 附 录 E（规范性）个人同意例外情形功能清单要求 .....   | 37 |
| 附 录 F（规范性）车辆数据收集设备参数信息清单要求 ..... | 38 |
| 参考文献 .....                       | 39 |



## 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。

本文件代替GB/T 44464—2024《汽车数据通用要求》，与GB/T 44464—2024相比，除结构调整及编辑性改动外，主要技术变化如下：

- 更改了适用范围描述，将“汽车产品及汽车数据处理者”改为“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”（见第1章，2024年版的第1章）；
- 更改了术语“收集”“座舱数据”的定义（见3.2、3.3，2024年版的3.1、3.3）；
- 增加了术语“汽车重要数据”“生物特征识别信息”“用户画像”“汽车数据安全信息”“口令”“车辆识别代号”（见3.1、3.4~3.7、3.14）；
- 删除了术语“汽车数据安全管理体系”“个人信息主体”“误检率”（见2024年版的3.2、3.4、3.11）；
- 更改了“汽车数据安全管理体系要求”描述为“安全保障要求”，更改相关具体要求（见4.1、4.2、4.5~4.8、4.10、4.11，2024年版的4.1）；
- 增加了汽车数据安全工具管理要求（见4.3）；
- 增加了汽车数据安全内部审核、管理评审及持续改进相关要求（见4.4）；
- 增加了个人信息和重要数据管理相关要求（见4.9）；
- 增加了车型汽车数据安全风险评估相关要求（见4.13）；
- 删除了汽车数据处理一般要求（见2024年版的4.2）；
- 增加了安全基本要求（见5.1~5.7）；
- 更改了汽车数据处理通用要求（见6.1，见2024年版的5.1、6.1）；
- 更改了个人同意要求（见6.2，2024年版的5.2）；
- 更改了汽车数据收集要求（见6.3，2024年版的5.3、6.2）；
- 更改了汽车数据存储要求（见6.4，2024年版的5.4、6.3）；
- 更改了汽车数据使用要求（见6.5，2024年版的5.5、6.4）；
- 更改了汽车数据传输要求（见6.6，2024年版的5.6、6.5）；
- 更改了汽车数据删除要求（见6.7，2024年版的5.7、6.6）；
- 删除了个人信息出境要求（见2024年版的5.8）；
- 删除了重要数据出境要求（见2024年版的6.7）；
- 增加了数据出境要求（见6.8）；
- 增加了汽车数据安全保障要求检验方法（见第7章）；
- 增加了汽车数据安全基本要求检验方法（见第8章）；
- 更改了汽车数据安全技术要求试验方法（见第9章，2024年版的第七章、附录B、附录D）；
- 增加了汽车数据安全同一形式判定要求（见第10章）；
- 增加了标准的实施（见第11章）；
- 增加了车型功能汽车数据处理活动清单要求（见附录A）；
- 增加了车辆常见功能必要个人信息范围要求（见附录B）；

- 更改了个人信息分类分级要求（见附录 C，2024 版的附录 A）；
- 增加了汽车重要数据识别要求（见附录 D）；
- 删除了匿名化误检率计算方法（见 2024 年版的附录 C）；
- 增加了个人同意例外情形功能清单要求（见附录 E）；
- 更改了车辆数据收集设备参数信息清单要求（见附录 F，2024 版的附录 D）。

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并归口。

本文件及其所代替文件的历次版本发布情况为：

- 2024年首次发布为GB/T 44464—2024；
- 本次为第一次修订。

# 汽车数据安全要求

## 1 范围

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，描述了相应检验与试验方法。

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。

## 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

**汽车重要数据** vehicle 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、经济运行的汽车数据。

### 3.2

**收集** collect

车辆制造商或者车辆通过一定方式获取汽车数据的行为。

### 3.3

**座舱数据** cabin data

通过摄像头、指纹传感器或传声器等各种方式在汽车座舱内处理的包含个人信息的数据。

[来源：GB/T 41871—2022，3.6，有修改]

### 3.4

**生物特征识别信息** biometric information

对自然人的物理、生物或行为特征进行技术处理得到的、能够单独或者与其他信息结合识别该自然人身份的个人信息。

注1：生物特征识别信息包括个人面部识别特征、虹膜、指纹、基因、声纹、步态、掌纹、耳廓、眼纹等。

注2：生物特征识别信息包含生物特征识别原始信息以及生物特征识别比对信息。

[来源：GB/T 40660—2021，3.3]

### 3.5

**用户画像** user profiling

通过收集、汇聚、分析个人信息，对某特定自然人个人特征，如职业、经济、健康、教育、个人喜好、信用、行为等方面作出分析或预测，形成个人特征模型的过程。

[来源：GB/T 35273—2020，3.8]

3.6

**汽车数据安全信息** vehicle data security information  
与汽车数据安全有关，且与组织的相关性尚未确定的信息。

[来源：GB/T XXXXX—XXXX 《汽车数据安全保障要求》，3.11]

3.7

**口令** password

作为一种需熟记的弱秘密，用于实体鉴别的秘密的字、短语、数字或字符序列。

[来源：GB/T 25069—2022，3.350]

3.8

**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。

3.9

**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。

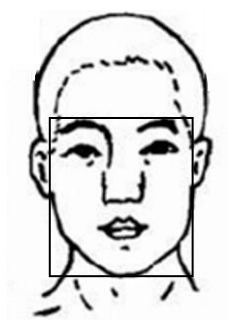


图1 人脸边界框示意图

3.10

**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。

3.11

**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。

3.12

**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。

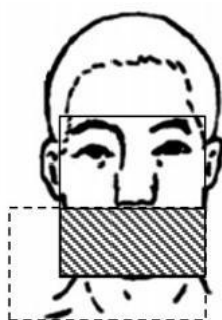


图2 遮盖率示意图

## 3.13

**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。

## 3.14

**车辆识别代号 vehicle identification number; VIN**

为了识别某一辆车，由车辆制造厂为该车辆指定的一组字母。

[来源：GB 16735—2019，3.1]

## 4 安全保障要求

4.1 车辆制造商应建立并实施汽车数据安全管理制度，明确汽车数据安全目标与方针，确定适用范围，识别并协调与汽车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。

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。

4.3 车辆制造商应针对影响汽车数据处理活动安全的工具，建立并实施汽车数据安全工具管理制度。

4.4 车辆制造商应建立并实施汽车数据安全内部审核、管理评审及持续改进制度，且汽车数据安全内部审核的实施频次应不低于每年一次。

4.5 车辆制造商应建立并实施汽车数据安全合作方管理制度，包括能力评估与核验、需求下发、数据安全协议签署和履行情况监督。

注1：合作方包含进行汽车数据安全相关产品开发和数据处理的合同供应商、内外部服务提供方等。内外部服务提供方指通过其他非合同手段约定的数据处理服务提供组织。

注2：数据安全协议包括数据安全接口协议和数据处理协议等，车辆制造商根据数据安全相关产品开发和数据处理的实际业务类型签署。

注3：数据安全接口协议的内容包括但不限于项目及数据安全联络人、各方实施的数据安全活动、各方的数据安全法律责任和权利义务、共享信息和工作成果、数据安全活动的关键节点、数据安全支持终止或功能废止的定义。

注4：数据处理协议的内容包括但不限于数据安全联络人、数据处理目的、期限、范围、方式及要求、各方的数据安全法律责任和权利义务。

4.6 车辆制造商应建立并实施投诉举报处理制度，明确汽车数据安全投诉举报渠道，并具备及时处理用户投诉举报的能力。

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。

注：企业汽车数据管理台账内容包括但不限于数据名称、级别、类别、规模，车型功能汽车数据处理活动清单内容要求见附录A。

4.8 车辆制造商应建立并实施汽车数据全生命周期安全管理制度，针对不同级别数据，制定数据收集、存储、使用、加工、传输、提供、公开、删除等环节的分级防护要求和操作规程。

4.9 车辆制造商应针对个人信息和重要数据建立并实施管理制度，包括：

- a) 个人信息保护影响评估、个人信息主体权利响应及个人信息保护合规审计；
- b) 重要数据识别、目录备案、目录变更及重要数据风险评估管理。

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。

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控、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。

4.12 车辆制造商应建立并实施车辆全生命周期汽车数据安全管理制度，包括以下内容：

- a) 车辆项目的数据安全管理制度，包括但不限于职责分配、数据安全计划、裁剪、数据安全档案、数据安全评估、后开发的发布等内容；
- b) 车辆项目的全生命周期数据安全工程活动管理制度，包括但不限于功能定义、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。

注：后开发包括生产、销售、使用、运维、功能废止、数据安全支持终止等环节。

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。

## 5 安全基本要求

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。

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。

注1：风险处置策略包括规避风险、减少风险、分担风险、接受风险等。

注2：若风险处置策略为减少风险，则制定相应的数据安全目标；若风险处置策略为分担或接受风险，则制定相应的数据安全声明。

5.3 车辆制造商应对依据5.2形成的车辆产品数据安全目标采取数据安全措施，保护车辆不受风险评估中已识别的风险的影响。

5.4 车辆制造商应通过测试来验证5.3形成车辆产品所实施的数据安全措施的有效性。

5.5 车辆制造商应确认针对车辆产品所实施的数据安全措施能够覆盖依据5.2形成的数据安全目标。

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、传感器等传感器调用监测、匿名化处理故障监测。

5.7 车辆制造商应针对车辆产品涉及的汽车数据安全合作方开展汽车数据安全能力评估及核验、数据安全协议签署等活动，识别、管理与合作方相关的数据安全风险。

## 6 安全技术要求

### 6.1 汽车数据处理通用要求

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应符合附录 B 的要求。

6.1.2 车辆在首次处理个人信息前，应以显著方式、清晰易懂的语言真实、准确、完整地向个人信息主体告知个人信息处理规则，具体要求如下。

- a) 告知方式选取产品使用说明书、车载显示终端、语音、短信、汽车使用相关应用程序等任一方式。
- b) 车辆若具备车载显示终端或汽车使用相关应用程序，在设置页面等醒目位置提供个人信息处理规则访问功能。
- c) 告知内容至少包含：
  - 1) 以结构化清单形式列明每项功能处理个人信息的种类、处理各类个人信息的必要性，具体包括：目的、种类、方式、调用权限名称等，并说明处理敏感个人信息对用户权益的影响；
  - 2) 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；
  - 3) 个人信息存储位置、存储期限、到期后的处理方式，或者确定存储位置、存储期限、到期后的处理方式的规则；
  - 4) 便捷的查阅、复制、转移、更正、补充、删除、限制处理个人信息以及删除和/或注销账号、撤回同意的的方法和途径；
  - 5) 用户权益事务联系人的名称或姓名和联系方式；
  - 6) 向第三方提供个人信息的接收方的名称或姓名、联系方式、处理目的、处理方式和个人信息的种类，若适用；
  - 7) 说明取得个人同意的例外情形及其理由，若适用。

注1：首次处理个人信息前包括但不限于车辆激活、车辆功能激活、切换未进行告知及取得同意的账户、系统重置等个人信息处理功能未进行告知及未取得同意的状态。

注2：处理个人信息的情形包括可不取得个人同意的例外情形。

注3：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。

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方式向用户告知更新的具体内容。

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，并配备相应展示规则：

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

6.1.5 处理不满十四周岁未成年人个人信息时，车辆应制定独立的个人信息处理规则。

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。

### 6.2 个人同意要求

### 6.2.1 个人同意一般要求

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，车辆不应在 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。

6.2.1.2 车辆直接向第三方提供个人信息前，应按功能取得用户的单独同意。

6.2.1.3 车辆向车外传输车内的生物特征识别信息时，应在取得车内处理生物特征识别信息的单独同意后再次取得单独同意，法律、行政法规、部门规章和强制性国家标准等另有规定时除外。

### 6.2.2 例外情形

有下列例外情形之一的，车辆处理个人信息准许不取得个人同意：

- a) 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；
- b) 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；
- c) 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；
- d) 法律、行政法规、部门规章和强制性国家标准规定的其他情形；
- e) 仅在车内处理汽车数据且处理的汽车数据仅包含车辆识别代号的功能。

### 6.2.3 个人同意及拒绝的选项设置

车辆应按以下要求设置个人同意及拒绝的选项：

- a) 提供自愿、明确的同意和拒绝的方式；
- b) 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；
- c) 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；
- d) 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。

示例 1：车辆基于用户画像的方式为用户精准推送个性化资讯。

示例 2：车辆基于用户画像以及自动化决策的方式根据用户驾驶习惯及实时路况，为用户智能推荐驾驶模式的功能。

示例 3：车辆基于用户画像及自动化决策，识别用户身份并综合其历史偏好与实时场景，不断优化升级自动调节座椅位置等提升用户体验优化的功能。

### 6.2.4 重新取得个人同意

6.2.4.1 车辆应仅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，若车辆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。

6.2.4.2 当个人信息的处理目的、处理方式、处理种类等情况发生变化时，车辆应重新取得用户同意。

### 6.2.5 个人同意的撤回

6.2.5.1 基于个人同意处理个人信息的情况，车辆应提供有效的撤回个人同意的途径。

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。

## 6.3 汽车数据收集要求

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。

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：

- a) 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；
- b) 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；
- c) 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；
- d) 符合 6.2.2 规定的例外情形不提示收集状态。

示例 1：在状态栏图标提示方式下，语音和定位提示分别以传声器图标和定位图标显示。

示例 2：在状态灯闪烁提示方式下，语音和定位提示分别以红光和黄光显示。

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。

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。

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。

6.3.7 车辆不应在用户同意个人信息处理规则前收集个人信息，不应超出用户同意的目的、方式、种类收集个人信息。

## 6.4 汽车数据存储要求

6.4.1 车辆基于个人同意而处理的个人信息，其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。

6.4.2 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及敏感个人信息，防止其被非授权访问和获取。

## 6.5 汽车数据使用要求

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。

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。

## 6.6 汽车数据传输要求

### 6.6.1 车外传输要求

6.6.1.1 除取得个人同意和满足 6.2.2 例外情形外，车辆不应向车外传输座舱数据。

6.6.1.2 车辆应对向车外传输的重要数据及敏感个人信息实施保密性保护措施。

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。

### 6.6.2 匿名化要求

### 6.6.2.1 匿名化对象

#### 6.6.2.1.1 人脸匿名化对象

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：

- a) 人脸边界框最小边长像素大于等于 28 像素；
- b) 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。

#### 6.6.2.1.2 汽车号牌匿名化对象

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：

- a) 汽车号牌边界框最小边长像素大于等于 16 像素；
- b) 汽车号牌目标内可见范围比值大于 50%且全部可见范围内数字及文字内容均可被识别。

### 6.6.2.2 匿名化处理性能要求

#### 6.6.2.2.1 匿名化检出率

车辆的人脸目标和汽车号牌目标的匿名化检出率均应大于等于90%。

#### 6.6.2.2.2 匿名化效果

满足6.6.2.1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。

### 6.7 汽车数据删除要求

6.7.1 车辆应向用户提供删除车端个人信息的途径或方式，可删除的个人信息不应包括法律、行政法规、部门规章、强制性国家标准中规定必须保留的个人信息。

6.7.2 车辆应满足以下个人信息删除要求：

- a) 在以下情形中，车辆主动删除个人信息，车辆未删除的，个人有权请求删除：
  - 1) 个人信息处理目的已实现、无法实现或者为实现处理目的不再必要；
  - 2) 停止提供产品或服务，或者保存期限已届满；
  - 3) 个人撤回同意；
  - 4) 违反法律、行政法规、部门规章、强制性国家标准或者违反约定处理个人信息；
  - 5) 法律、行政法规、部门规章、强制性国家标准所规定的其他情形。
- b) 法律、行政法规、部门规章、强制性国家标准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，车辆停止除存储和采取必要的安全保护措施之外的处理。

6.7.3 车辆中被删除的汽车数据应不可检索且不可访问。

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。

### 6.8 数据出境要求

车辆不应直接向境外传输数据。

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款限制。

## 7 汽车数据安全保障要求检验方法

### 7.1 检验条件

车辆制造商应具备符合第4章要求的文件化信息，并满足以下要求：

- a) 提交的文件化信息为中文，文件化信息包括相关管理制度与对应的管理记录；
- b) 承载汽车数据安全保障要求的文件化信息正式发布并具备明确的版本信息；
- c) 若因未发生相应事件导致未产生正式管理记录，提供对应的试运行记录；
- d) 提交检验的文件化信息采取防篡改技术进行保存，保存时间不少于3年；
- e) 提供必要资源支持，以验证汽车数据安全保障要求能有效运行。

注：管理记录指管理制度实际执行后产生的相应实施记录。

### 7.2 检验方法

#### 7.2.1 汽车数据安全保障总体要求检验

检验人员应按照以下方法开展检验，确认是否满足4.1的要求：

- a) 检验车辆制造商是否具备符合本文件4.1至4.13要求的汽车数据安全管理制度，车辆制造商是否具备组织层面汽车数据安全管理的规则和过程清单；
- b) 检验汽车数据安全管理制度是否具备汽车数据安全目标与方针；
- c) 检验汽车数据安全管理制度是否具备汽车数据安全管理制度适用范围，适用范围至少明确企业范围和数据范围；
- d) 检验数据范围中的个人信息是否覆盖附录C，数据范围中的汽车重要数据是否覆盖附录D；
- e) 检验汽车数据安全管理制度是否具备与汽车数据安全有关或相互作用的领域的协调机制。

#### 7.2.2 汽车数据安全保障组织架构及文化检验

检验人员应按照以下方法开展检验，确认是否满足4.2的要求：

- a) 检验车辆制造商是否具备汽车数据安全组织架构和相关职责，是否具备汽车数据安全组织架构和相关职责的管理记录，包含组织架构和相关职责发布文件和关键岗位的数据安全责任书；
- b) 检验车辆制造商是否具备汽车数据安全资源保障要求，是否具备汽车数据安全资源保障实施记录；
- c) 检验车辆制造商是否具备汽车数据安全人员能力与意识培训制度，是否具备人员能力与意识培训记录；
- d) 检验车辆制造商是否具备汽车数据安全内外部沟通制度，是否具备内外部沟通记录；
- e) 检验车辆制造商是否具备汽车数据安全信息共享制度，是否具备汽车数据安全信息共享管理记录。

注：关键岗位指能获知重要数据和核心数据内容的人员。

#### 7.2.3 汽车数据安全工具管理检验

检验人员应按照以下方法开展检验，确认是否满足4.3的要求：

- a) 检验车辆制造商是否具备汽车数据安全工具管理制度；
- b) 检验车辆制造商是否具备识别出的汽车数据安全工具清单；
- c) 检验车辆制造商是否具备汽车数据安全工具管理的记录。

#### 7.2.4 汽车数据安全审核及持续改进检验

检验人员应按照以下方法开展检验，确认是否满足4.4的要求：

- a) 检验车辆制造商是否具备汽车数据安全内部审核管理制度，是否每年开展汽车数据安全内部审核，是否具备汽车数据安全内部审核的记录；
- b) 检验车辆制造商是否具备汽车数据安全评审制度，是否定期开展汽车数据安全评审，是否具备汽车数据安全评审的记录；
- c) 检验车辆制造商是否具备汽车数据安全持续改进制度，是否具备汽车数据安全持续改进的记录。

#### 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，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，汽车数据安全合作方管理制度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，检验车辆制造商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管理记录，确认是否满足4.5的要求。

#### 7.2.6 汽车数据安全投诉举报管理检验

检验人员应按照以下方法开展检验，确认是否满足4.6的要求：

- a) 检验车辆制造商是否具备投诉举报处理制度，投诉举报处理制度是否明确汽车数据安全投诉举报渠道，是否具备汽车数据安全投诉举报记录；
- b) 检验投诉举报处理制度是否具备投诉举报响应时间及处理时间要求。

#### 7.2.7 汽车数据分类分级及台账管理检验

检验人员应按照以下方法开展检验，确认是否满足4.7的要求：

- a) 检验车辆制造商是否具备汽车数据分类分级管理制度，汽车数据分类分级管理制度是否具备分类规则、分级规则和动态更新规则；
- b) 检验分类分级规则中一般个人信息、敏感个人信息、重要数据是否符合现行法律、行政法规、部门规章和强制性国家标准要求；
- c) 检验汽车数据分类分级管理制度是否具备企业汽车数据管理台账、车型功能汽车数据处理活动清单管理机制，检验车辆制造商是否具备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记录。

#### 7.2.8 汽车数据全生命周期安全管理检验

检验人员应按照以下方法开展检验，确认是否满足4.8的要求：

- a) 检验车辆制造商是否具备汽车数据全生命周期安全管理制度，汽车数据全生命周期安全管理制度是否具备数据收集、存储、使用、加工、传输、提供、公开、删除等环节的分级防护要求和操作规程，检验车辆制造商是否具备汽车数据全生命周期安全管理记录；
- b) 检验汽车数据全生命周期安全管理制度是否符合现行法律、行政法规、部门规章和强制性国家标准要求。

#### 7.2.9 个人信息和重要数据管理检验

检验人员应检验车辆制造商是否具备个人信息和重要数据管理制度，个人信息管理制度是否具备个人信息保护影响评估、个人信息主体权利响应及个人信息保护合规审计机制，重要数据管理制度是否具备重要数据识别、目录备案、目录变更及重要数据风险评估管理机制，检验车辆制造商是否具备个人信息和重要数据管理记录，确认是否满足4.9的要求。

### 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，确认是否满足4.10的要求：

- a) 检验车辆制造商是否具备汽车数据出境管理制度，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，检验车辆制造商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、行政法规、部门规章和强制性国家标准要求。

### 7.2.11 汽车数据安全风险与事件监测管理检验

检验人员应按照以下方法开展检验，确认是否满足4.11的要求：

- a) 检验车辆制造商是否具备汽车数据安全风险与事件的监测与管理制度，汽车数据安全风险与事件的监测与管理制度是否具备汽车数据安全监测、汽车数据安全信息与评估、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等内容，检验车辆制造商是否具备汽车数据安全风险与事件的监测与管理记录；
- b) 检验汽车数据安全风险与事件的监测与管理制度是否符合现行法律、行政法规、部门规章和强制性国家标准要求。

### 7.2.12 车辆全生命周期汽车数据安全检验

检验人员应按照以下方法开展检验并验证，确认是否满足4.12的要求：

- a) 检验车辆制造商是否具备车辆项目的数据安全管理制度，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，检验车辆制造商是否具备车辆项目的数据安全管理制度记录；
- b) 检验车辆制造商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，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，检验车辆制造商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记录。

### 7.2.13 汽车数据安全风险评估检验

检验人员应检验车辆制造商是否具备车型汽车数据安全风险评估制度，车型汽车数据安全风险评估制度是否具备风险评估准备、风险识别、风险分析、风险评价、风险评估总结等环节要求，检验车辆制造商是否具备车型汽车数据安全风险评估记录，确认是否满足4.13的要求。

## 8 汽车数据安全基本要求检验方法

### 8.1 检验条件

8.1.1 车辆制造商应具备文档来说明车辆在开发、生产等过程的数据安全情况，文档包括提交的文档和留存备查的文档。

8.1.2 车辆制造商提交的文档应为中文版本，并至少包含如下内容：

- a) 证明车辆满足第5章要求的总结文档；
- b) 写明文档版本信息的留存备查文档清单。

8.1.3 车辆制造商应以安全的方式在本地留存车辆数据安全相关过程文档备查，完成检验后应对留存备查的文档进行防篡改处理。

8.1.4 车辆制造商应对提交和留存备查的文档与车辆的一致性、可追溯性做出自我声明。

## 8.2 检验方法

### 8.2.1 车辆产品汽车数据处理活动清单检验

检验人员应按照以下方法开展检验，确认是否满足5.1的要求：

- a) 检验车辆制造商是否具备对应车辆的车型功能汽车数据处理活动清单；
- b) 检验对应车辆的车型功能汽车数据处理活动清单内容是否符合本标准附录 A 要求。

### 8.2.2 车辆产品数据安全风险评估检验

检验人员应按照以下方法开展检验，确认是否满足5.2的要求：

- a) 检验车辆制造商是否具备对应车辆的风险评估记录，是否具备已识别的风险；
- b) 检验车辆制造商是否针对对应车辆的已识别的风险采取处置策略；
- c) 检验对应车辆涉及汽车数据处理的各项功能所有已识别的风险是否具备数据安全目标或声明；
- d) 检验对应车辆已识别的数据安全风险中与第 6 章要求相关的风险是否均已形成数据安全目标。

### 8.2.3 车辆产品数据安全措施检验

检验人员应按照以下方法开展检验，确认是否满足5.3的要求：

- a) 检验对应车辆所有数据安全目标是否均具备数据安全措施；
- b) 检验对应车辆每个数据安全目标的数据安全措施是否足以保护车辆不受对应风险影响。

### 8.2.4 车辆产品数据安全验证检验

检验人员应按照以下方法开展检验，确认是否满足5.4的要求：

- a) 检验车辆制造商是否具备对应车辆的验证测试的相关记录，至少包括验证测试方案、验证测试报告、验证测试的评审记录；
- b) 检验对应车辆的验证报告中是否全部数据安全措施经验证测试均证明有效。

### 8.2.5 车辆产品数据安全确认检验

检验人员应按照以下方法开展检验，确认是否满足5.5的要求：

- a) 检验车辆制造商是否具备对应车辆的数据安全确认的相关记录，至少包括确认方案、确认报告、确认的评审记录；
- b) 检验对应车辆的确认报告中是否已确认车辆产品所实施的数据安全措施已覆盖全部数据安全目标。

### 8.2.6 车辆产品数据安全监测及数据记录能力检验

检验人员应检验车辆制造商是否具备对应车辆的与车辆数据安全相关的监测及记录能力证明材料，确认是否满足5.6的要求。

### 8.2.7 车型功能合作方数据安全检验

检验人员应按照以下方法开展检验，确认是否满足5.7的要求：

- a) 检验车辆制造商是否具备对应车辆的汽车数据安全合作方清单；
- b) 检验车辆制造商是否开展对应车辆的汽车数据安全合作方能力评估及核验、数据安全协议签署等活动；

- c) 检验车辆制造商针对对应车辆的汽车数据安全合作方管理是否涵盖汽车数据安全产品开发合作方和数据处理合作方；
- d) 检验车辆制造商针对对应车辆的与汽车数据安全合作方签署的数据安全协议内容是否符合本文件 4.5 要求。

## 9 汽车数据安全技术要求试验方法

### 9.1 总则

测试人员应按照本文件要求,依据车辆制造商提交的车型功能汽车数据处理活动清单及汽车数据安全相关证明材料,对车辆产品进行技术测试,证明车辆制造商对车辆采取的数据安全措施满足本文件规定的要求。

### 9.2 测试准备

#### 9.2.1 汽车数据安全技术要求测试输入文档提交要求

车辆制造商应提交以下文档,且提交的文档应为中文版本。车辆制造商应为所提交的文档与车辆实际开发的一致性、可追溯性做出自我声明,并保证提交材料的准确性和真实性。具体包括。

- a) 按照附录 A 填写的车型功能汽车数据处理活动清单。
- b) 按照附录 E 填写的个人同意例外情形功能清单。
- c) 按照附录 F 填写的车辆数据收集设备参数信息,并满足以下要求:
  - 1) 覆盖用于收集汽车数据的摄像头、激光雷达和 4D 毫米波雷达等传感器;
  - 2) 传感器型号为公开可查或由车辆制造商提供文件证明;
  - 3) 清晰的各传感器安装位置描述;
  - 4) 功能解释部分明确传感器对应的功能及各功能所需的分辨率、覆盖范围。

#### 9.2.2 汽车数据安全技术要求测试条件准备

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;
- 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) 车辆制造商应提供敏感个人信息及重要数据存储情况及对应的权限策略、对应存储个人信息的解密方法等测试支撑材料;
- 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。

9.2.2.2 测试人员应在涉及驾驶相关功能的数据安全测试时,将车辆置于底盘测功机或其他安全测试环境中。

### 9.2.3 汽车匿名化测试准备

#### 9.2.3.1 车辆制造商应完成以下准备工作。

- a) 进行匿名化处理测试的车辆匿名化处理及向车外传输相关功能能够正常运行。
- b) 提供明确的匿名化处理及向车外传输相关功能开启条件。
- c) 支持匿名化处理后的视频图像数据的采集和读取。

#### 9.2.3.2 测试人员应完成以下准备工作。

- a) 测试过程中额外安装测试记录设备并进行记录，至少记录以下内容：
  - 1) 测试时间轴及测试时长；
  - 2) 测试车辆周边环境视频信息。
- b) 测试记录设备分辨率不小于（1920×1080）像素，视频采样帧率不小于 30fps。
- c) 测试记录设备的安装、运行不影响测试车辆原有配置及其数据处理功能的正常运行。

### 9.3 汽车数据处理通用要求测试

#### 9.3.1 个人信息处理的最小必要测试

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，依据附录B车辆常见功能必要个人信息范围确认车辆是否存在对应的功能类型，仅同意车辆常见功能必要个人信息且拒绝非必要个人信息，测试车辆常见功能是否可以使用其基本功能服务，确认车辆是否符合6.1.1的要求。

#### 9.3.2 个人信息处理显著告知测试

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、首次处理个人信息状态恢复方式和个人同意例外情形功能清单，将车辆设定为首次处理个人信息状态，启动测试车辆各项个人信息处理功能并打开告知内容，测试以下内容，确认车辆是否符合6.1.2的要求。

- a) 测试车辆是否选取产品使用说明书、车载显示终端、语音、短信、汽车使用相关应用程序等任一方式向用户进行告知。
- b) 车辆若具备车载显示终端或汽车使用相关应用程序，测试是否在设置页面等醒目位置提供个人信息处理规则访问功能。
- c) 测试车辆告知内容是否涵盖以下要求：
  - 1) 以结构化表格或结构化固定列项形式列明每项功能处理个人信息的种类、处理各类个人信息的必要性，具体包括：目的、种类、方式、调用权限名称等，并说明处理敏感个人信息对用户权益的影响；
  - 2) 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；
  - 3) 个人信息存储位置、存储期限、到期后的处理方式，或者确定存储位置、存储期限、到期后的处理方式的规则；
  - 4) 便捷的查阅、复制、转移、更正、补充、删除、限制处理个人信息以及删除和/或注销账号、撤回同意的的方法和途径；
  - 5) 用户权益事务联系人的名称或姓名和联系方式；
  - 6) 向第三方提供个人信息的接收方的名称或姓名、联系方式、处理目的、处理方式和个人信息的种类，若适用。
- d) 测试车辆是否可在指定路径查找到例外情形涉及功能提示信息，且该信息可被车辆使用者自行查找。
- e) 测试车辆例外情形告知内容是否涵盖以下要求：

- 1) 以结构化表格或结构化固定列项形式列明每项功能处理个人信息的种类、处理各类个人信息的必要性，具体包括：目的、种类、方式、调用权限名称等；
- 2) 收集各类个人信息的具体情境；
- 3) 取得个人同意的例外情形的理由。

### 9.3.3 个人信息处理规则变化告知测试

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个人信息告知内容变化方法，确认个人信息告知内容变化方法中发生变化前的告知内容，基于车辆制造商提供个人信息告知内容变化方法进行个人信息告知内容变更，变更完成后测试发生变更功能的个人信息处理规则是否进行了更新，并测试车辆是否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，确认车辆是否符合6.1.3的要求。

### 9.3.4 应用程序下载平台告知测试

测试人员应按照车辆制造商提供的应用程序下载平台清单，使用车辆搭载的应用程序下载平台，测试以下内容，确认车辆是否符合6.1.4的要求：

- a) 应用程序下载平台下载页面展示规则是否包含应用程序运营者名称或者姓名、联系方式；
- b) 应用程序下载平台下载页面展示规则是否包含应用程序主要功能介绍；
- c) 应用程序下载平台下载页面展示规则是否包含应用程序运行所需具体权限列表；
- d) 应用程序下载平台下载页面展示规则是否包含个人信息处理规则文本或者链接；
- e) 应用程序下载平台中的应用程序下载页面是否包含应用程序运营者名称或者姓名、联系方式；
- f) 应用程序下载平台中的应用程序下载页面是否包含应用程序主要功能介绍；
- g) 应用程序下载平台中的应用程序下载页面是否包含应用程序运行所需具体权限列表；
- h) 应用程序下载平台中的应用程序下载页面是否包含个人信息处理规则文本或者链接。

### 9.3.5 未成年人个人信息处理规则测试

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，确认处理不满十四周岁未成年人个人信息的功能，测试车辆处理不满十四周岁未成年人个人信息的功能是否制定独立的个人信息处理规则，确认车辆是否符合6.1.5的要求。

### 9.3.6 车辆传感器调用情况告知测试

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，确认调用摄像头、位置、传声器等传感器的功能，测试以下内容，确认车辆是否符合6.1.6的要求：

- a) 测试车辆是否告知记录规则；
- b) 测试记录规则是否包含记录的传感器类型、传感器调用情况、统计期限、记录保存期限等内容；
- c) 使用对应功能并生成记录内容，测试功能是否记录和集中展示功能调用摄像头、位置、传声器等传感器情况。

## 9.4 个人同意要求测试

### 9.4.1 个人同意一般要求测试

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首次处理个人信息状态恢复方式，通过车辆制造商输入将车辆恢复至首次处理个人信息状态，启动个人信息处理功能（例外情形除外）并测试以下内容，确认车辆是否符合6.2.1.1、6.2.1.2和6.2.1.3的要求：

- a) 若车辆涉及个人信息处理，测试车辆处理一般个人信息时是否取得个人同意；
- b) 若车辆涉及敏感个人信息处理，测试车辆处理敏感个人信息时是否取得单独同意；
- c) 若车辆向第三方提供个人信息，测试车辆处理个人信息时是否按功能取得单独同意；
- d) 将车辆恢复至首次处理个人信息状态，拒绝选取的个人信息处理功能，将车辆静置 48 小时且在此期间间断性地使用车辆不处理个人信息的功能，测试在此 48 小时内车辆是否重新主动申请授权同意；
- e) 若车辆涉及向车外传输车内的生物特征识别信息，测试车辆在取得车内处理生物特征识别信息的单独同意后是否再次取得单独同意，法律、行政法规、部门规章和强制性国家标准等另有规定时除外。

#### 9.4.2 例外情形测试

测试人员应按照车辆制造商提供的个人同意例外情形功能清单，若车辆存在涉及例外情形的功能，测试例外情形的功能是否符合以下任一情形，确认车辆是否符合6.2.2的要求：

- a) 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；
- b) 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；
- c) 因保证行车安全和财产安全需要，无法征得个人同意收集到车外个人信息；
- d) 法律、行政法规、部门规章和强制性国家标准等规定的其他情形；
- e) 仅在车内处理汽车数据且处理的汽车数据仅包含车辆识别代号的功能。

#### 9.4.3 个人同意及拒绝的选项设置测试

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首次处理个人信息状态恢复方式，通过车辆制造商输入将车辆恢复至首次处理个人信息状态，启动个人信息处理功能，例外情形除外，并测试以下内容，确认车辆是否符合6.2.3的要求：

- a) 测试车辆个人信息处理功能授权设置是否提供自愿且明确的同意与拒绝方式；
- b) 测试车辆申请车内摄像头、位置、车内传声器等权限时，是否以功能为单位，按每项功能所需处理的敏感个人信息类型逐一取得用户单独同意；
- c) 测试车辆用户画像、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，是否具备独立、便捷的拒绝方式；
- d) 测试车辆是否支持自主设定敏感个人信息的授权期限，且期限是否不为仅始终允许或永久。

#### 9.4.4 期限届满重新取得个人同意测试

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、首次处理个人信息状态恢复方式和期限届满到达方式，通过车辆制造商输入将车辆恢复至首次处理个人信息状态，授权存在同意期限的个人信息处理功能，例外情形除外，通过期限届满到达方式实现各项个人信息处理功能的同意期限届满后，测试车辆是否具备重新取得个人同意并记录重新取得个人同意的方式，确认车辆是否符合6.2.4.1的要求。

#### 9.4.5 个人信息变更重新取得个人同意测试

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、首次处理个人信息状态恢复方式和个人信息情况变化方法，通过车辆制造商输入将车辆恢复至首次处理个人信息状态并取得该项功能

的个人信息同意，基于车辆制造商提供的个人信息情况变化方法进行变更，变更完成后启动相应功能，测试车辆是否重新取得个人同意，确认车辆是否符合6.2.4.2的要求。

#### 9.4.6 个人同意撤回途径测试

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，授权个人信息处理功能（例外情形除外），按照车型功能汽车数据处理活动清单中的撤回方式撤回功能的个人同意，测试功能是否存在撤回个人同意的途径，并确认撤回个人同意后的功能状态，确认车辆是否符合6.2.5.1的要求。

#### 9.4.7 个人同意撤回活动效力影响测试

测试人员应按照车型功能汽车数据处理活动清单，对被测试的个人信息处理功能进行授权，触发个人信息处理活动，撤回该功能的个人同意，测试功能撤回授权后是否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，确认车辆是否符合6.2.5.2的要求。

### 9.5 汽车数据收集要求测试

#### 9.5.1 个人信息默认不收集测试

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、首次处理个人信息状态恢复方式，通过车辆制造商输入将车辆恢复至首次处理个人信息状态，启动个人信息处理功能，例外情形除外，测试功能是否默认设定为不收集个人信息的状态，确认车辆是否符合6.3.1的要求。

#### 9.5.2 敏感个人信息收集提示测试

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，启动车辆收集位置信息及座舱数据中敏感个人信息的功能并取得个人同意，触发功能使其处于收集状态，并测试以下内容，确认车辆是否符合6.3.2的要求：

- a) 测试车辆是否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；
- b) 测试车辆在收集期间是否通过光学、声学或触觉信号等至少一种方式进行提示，直至收集结束；
- c) 测试车辆收集位置信息及座舱数据中敏感个人信息的提示方式是否与提示收集状态的规则一致；
- d) 若车辆不同种类敏感个人信息提示方式相同，测试是否不同种类敏感个人信息的提示以不同形式区分；
- e) 测试车辆符合6.2.2规定的例外情形是否不提示收集状态。

#### 9.5.3 最小精度范围适用测试

测试人员应按照车辆制造商提供的车辆数据收集设备参数信息、导出并解码所收集的原始车辆数据的方法，测试通过分析车辆数据收集设备收集的原始车辆数据的参数信息，开展以下测试，对比车辆数据收集设备参数信息中各项功能所需的数据收集设备精度，记录测试结果，确认车辆是否符合6.3.3和6.3.4的要求：

- a) 根据车辆制造商提供的车辆数据收集设备参数列表测试传感器是否具备对应的功能和采样参数、来源说明；
- b) 测试传感器采样参数及对应的功能的采样需求是否一致；
- c) 若单一传感器涉及多个功能，测试传感器是否至少有一个功能服务与其精度对应。

#### 9.5.4 无相关功能或未激活相关功能个人信息调用测试

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、预装汽车数据处理功能相关软件安装包及相关技术资料以及涉及汽车数据处理的系统的接入方式和调试权限，确认功能所有个人信息处理类型，确保个人信息处理功能处于未激活状态，通过工具和车辆制造商测试输入对功能的摄像头、位置、传声器数据处理状态进行测试，测试个人信息处理功能处于未激活状态下是否进行汽车数据处理，确认车辆是否符合6.3.5的要求。

#### 9.5.5 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测试

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首次处理个人信息状态恢复方式，通过车辆制造商输入将车辆恢复至首次处理个人信息状态，拒绝所有车辆个人信息处理功能的授权，测试拒绝授权后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是否可以正常使用，确认车辆是否符合6.3.6的要求。

#### 9.5.6 提前和超范围收集个人信息测试

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、首次处理个人信息状态恢复方式、预装汽车数据处理功能相关软件安装包及相关技术资料以及涉及汽车数据处理的系统的接入方式和调试权限，确认功能所有个人信息处理类型，通过车辆制造商输入将车辆恢复至首次处理个人信息状态，在未进行个人信息同意前通过工具和车辆制造商测试输入对功能的个人信息数据处理类型进行测试，测试是否在用户同意个人信息处理规则前收集个人信息，单独启动除例外情形外的个人信息处理功能，通过工具和车辆制造商测试输入对功能的个人信息数据处理情况进行测试，测试个人信息数据处理情况是否超出用户同意的目的、方式、种类收集个人信息，确认车辆是否符合6.3.7的要求。

### 9.6 汽车数据存储要求测试

#### 9.6.1 个人信息存储规则一致性测试

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以及涉及汽车数据处理的系统的接入方式和调试权限，确定各功能将个人信息存储在车端的存储期限或存储规则说明，使用功能并存储个人信息，通过调试接口和数据存储地址测试数据是否存储在车端，确认个人信息存储在车端后，通过触发相关机制或调试相关权限使得在车端存储个人信息的超过存储期限或存储规则，再次通过调试接口和数据存储地址测试数据是否删除，确认车辆是否符合6.4.1的要求。

#### 9.6.2 重要数据及敏感个人信息存储安全性测试

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，确认测试整车，依次触发车辆记录重要数据及敏感个人信息的功能，并按照以下测试方法依次开展测试，确认车辆是否符合6.4.2的要求：

- a) 若采用安全访问技术保护存储的重要数据及敏感个人信息，依据车型功能汽车数据处理活动清单中的重要数据及敏感个人信息存储区域和地址范围说明，通过车辆制造商提供的处理涉及汽车数据处理的系统的接入方式和调试权限和权限策略，使用未添加访问控制权限的用户访问存储的重要数据及敏感个人信息，测试是否能非授权访问重要数据及敏感个人信息；
- b) 若采取加密技术保护存储的重要数据及敏感个人信息，依据车型功能汽车数据处理活动清单中的重要数据及敏感个人信息存储区域和地址范围说明，通过车辆制造商提供的处理涉及汽车数据处理的系统的接入方式和调试权限和权限策略，使用软件分析工具提取存储的重要数据及敏感个人信息，测试是否为密文存储；

- c) 依次触发车辆记录重要数据及敏感个人信息的功能，然后依据车辆制造商提供的处理涉及汽车数据处理的系统的接入方式和调试权限进入系统，进行重要数据及敏感个人信息检索，测试是否可检索出不在车型功能汽车数据处理活动清单中存储的重要数据及敏感个人信息。

## 9.7 汽车数据使用要求测试

### 9.7.1 身份识别方式测试

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，选择使用个人生物特征识别信息进行身份识别的功能，停止收集个人生物特征识别信息，测试身份识别功能是否可以通过其他方式正常运行，记录测试结果，确认车辆是否符合6.5.1的要求。

### 9.7.2 口令脱敏测试

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，依次触发车辆显示、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)的功能，测试功能使用时是否提供了隐藏部分或全部信息的方式，确认车辆是否符合6.5.2的要求。

## 9.8 汽车数据传输要求测试

### 9.8.1 座舱数据车内处理测试

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、传输数据包的数据解密方式、涉及汽车数据处理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，测试数据包中是否存在座舱数据，记录测试结果，确认车辆是否符合6.6.1.1的要求。

### 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

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，确认车辆是否符合6.6.1.2的要求。

### 9.8.3 车外视频图像车外传输匿名化处理测试

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个人信息是否进行匿名化处理，记录测试结果，确认车辆是否符合6.6.1.3的要求。

### 9.8.4 匿名化要求测试

#### 9.8.4.1 匿名化处理性能要求测试过程

测试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，测试过程开启测试记录设备。

#### 9.8.4.2 匿名化处理性能要求测试结束条件

##### 9.8.4.2.1 总体要求

匿名化处理性能要求测试应在满足9.8.4.2.2和9.8.4.2.3的要求后结束。

#### 9.8.4.2.2 测试图片及视频要求

测试过程中收集的图片或视频应满足以下要求，并按照9.8.4.3的测试方法进行处理：

- a) 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；
- b) 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；
- c) 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；
- d) 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。
- e) 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。

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：

- a) 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；
- b) 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；
- c) 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；
- d) 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。

#### 9.8.4.3 测试结果处理

##### 9.8.4.3.1 测试数据读取

9.8.4.3.1.1 测试结束后，读取测试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。

9.8.4.3.1.2 测试结束后，读取测试记录设备可反应实际行驶过程的视频。

9.8.4.3.1.3 基于 9.8.4.3.1.1 中读取的数据进行以下处理：

- a) 若测试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；
- b) 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。

9.8.4.3.1.4 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。

##### 9.8.4.3.2 遮盖率计算过程

根据9.8.4.3.1.3处理的测试结果，计算遮盖率。

##### 9.8.4.3.3 检出率计算过程

9.8.4.3.3.1 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：

- a) 满足 6.6.2.1.1 要求并进行匿名化处理；
- b) 遮盖率大于等于 50%。

9.8.4.3.3.2 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：

- a) 满足 6.6.2.1.1 要求；
- b) 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 3 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 3 匿名化漏检数结果示例

9.8.4.3.3.3 人脸目标检出率计算方法，按照公式（1）计算人脸目标检出率，确认是否符合 6.6.2.2.1 要求。

$$R_{df} = \frac{N_{af}}{N_{af} + N_{mf}} \dots\dots\dots (1)$$

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 9.8.4.3.3.1 要求的正检数；
- $N_{mf}$  ——满足 9.8.4.3.3.2 要求的漏检数。

9.8.4.3.3.4 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：

- a) 满足 6.6.2.1.2 要求且进行匿名化处理；
- b) 遮盖率大于等于 50%。

9.8.4.3.3.5 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：

- a) 满足 6.6.2.1.2 要求；
- b) 遮盖率小于 50%。

9.8.4.3.3.6 汽车号牌目标检出率计算方式，按照公式（2）计算汽车号牌目标检出率，确认是否符合 6.6.2.2.1 要求。

$$R_{dv} = \frac{N_{av}}{N_{av} + N_{mv}} \dots\dots\dots (2)$$

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 9.8.4.3.3.4 要求的正检数；
- $N_{mv}$  ——满足 9.8.4.3.3.6 要求的漏检数。

#### 9.8.4.4 裁剪、删除帧、降低分辨率等技术测试结果处理

##### 9.8.4.4.1 测试数据读取

9.8.4.4.1.1 测试结束后，读取测试车辆已进行技术处理后的图片或视频。

9.8.4.4.1.2 测试结束后，读取测试记录设备可反应实际行驶过程的视频。

9.8.4.4.1.3 基于 9.8.4.4.1.1 中读取的数据进行以下处理：

- a) 若测试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；
- b) 在直接输出或抽帧后的图片中标注人脸目标和汽车号牌目标的漏检数；
- c) 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的图片的尺寸和分辨率。

##### 9.8.4.4.2 检出率计算过程

9.8.4.4.2.1 按照 9.8.4.3.3.2 的测试方法，分析人脸目标是否存在漏检指标，确认是否符合 6.6.2.2.1 要求：

- a) 若存在漏检人脸目标，则人脸目标检出率为 0%；
- b) 若不存在漏检人脸目标，则人脸目标检出率为 100%。

9.8.4.4.2.2 按照 9.8.4.3.3.5 的测试方法，分析汽车号牌目标是否存在漏检指标，确认是否符合 6.6.2.2.1 要求：

- a) 若存在漏检汽车号牌目标，则汽车号牌检出率为 0%；
- b) 若不存在漏检汽车号牌目标，则汽车号牌检出率为 100%。

#### 9.8.4.5 匿名化处理效果评估

##### 9.8.4.5.1 机器识别测试

###### 9.8.4.5.1.1 人脸不可识别性测试

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，确认是否符合 6.6.2.2.2 要求。

###### 9.8.4.5.1.2 汽车号牌不可识别性测试

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，确认是否符合 6.6.2.2.2 要求。

##### 9.8.4.5.2 人工识别测试

9.8.4.5.2.1 分别随机挑选 100 张已经完成匿名化处理的图片，由测试人员对计入人脸目标正检数和汽车号牌目标正检数的匿名化目标进行识别。

9.8.4.5.2.2 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，确认是否符合 6.6.2.2.2 要求。

9.8.4.5.2.3 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，确认是否符合 6.6.2.2.2 要求。

#### 9.9 汽车数据删除要求测试

##### 9.9.1 个人信息删除途径测试

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以及对应个人信息的解密方法,选取个人信息存储在车端的功能,通过涉及汽车数据处理的系统的接入方式和调试权限以及车型功能汽车数据处理活动清单中的个人信息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车辆制造商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,确认车辆是否符合6.7.1的要求。

### 9.9.2 特定情形个人信息删除测试

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以及对应个人信息的解密方法,选取汽车数据存储在车端的相关功能,通过涉及汽车数据处理的系统的接入方式和调试权限以及车型功能汽车数据处理活动清单中的个人信息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车辆制造商提供的解密方法进行解密确认个人信息数据内容,按照以下方法测试在车端存储个人信息的车辆功能是否进行了删除,确认车辆是否符合6.7.2的要求:

- a) 各功能若适用 6.7.2 a) 中的删除情形,执行删除后,测试被删除的个人信息是否在车端已删除,若未删除,查找是否存在用户请求删除个人信息的途径,并通过用户请求删除个人信息的途径,测试个人信息是否被删除;
- b) 若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。

### 9.9.3 删除的汽车数据不可检索、不可访问测试

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,选取汽车数据存储在车端的相关功能,通过涉及汽车数据处理的系统的接入方式和调试权限以及车型功能汽车数据处理活动清单中的个人信息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车辆制造商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访问与检索测试,确认车辆是否符合6.7.3的要求。

### 9.9.4 本地删除账号以及便捷性测试

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测试登录账号,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,根据车型功能汽车数据处理活动清单在该账户下生成存储在车端的个人信息,通过涉及汽车数据处理的系统的接入方式和调试权限以及车型功能汽车数据处理活动清单中的个人信息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车辆制造商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,确认车辆是否符合6.7.4的要求。

## 9.10 数据出境测试

测试人员应开启车辆全部移动蜂窝通信通道和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3600s,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6.8的要求。

## 10 同一型式判定

## 10.1 直接视同条件

如符合下述规定，则视为同一型式：

- a) 汽车数据安全保障要求相关内容有效且其签发日期未超过三年；
- b) 车型涉及汽车数据处理功能及其汽车数据处理活动相同或减少；
- c) 车型涉及汽车数据处理功能对应的数据安全措施相同；
- d) 车辆具备与数据安全相关的监测和记录能力的控制器生产企业、硬件型号和软件版本号（不影响监测和记录规则的除外）相同；
- e) 摄像头、传声器或指纹传感器等收集车内汽车数据的传感器类型相同或减少；
- f) 摄像头、传声器或指纹传感器等收集车内汽车数据的传感器数量相同或减少；
- g) 收集车外数据的摄像头、激光雷达、4D毫米波雷达数量相同或减少；
- h) 同一收集车外数据的摄像头、激光雷达、4D毫米波雷达覆盖范围、分辨率、安装位置相同；
- i) 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）的控制器数量相同或减少；
- j) 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）的控制器生产企业、硬件型号和软件版本号（不影响汽车数据处理活动及其安全措施或汽车数据处理活动减少的除外）相同；
- k) 车辆匿名化算法生产企业和版本相同；
- l) 车辆实现匿名化算法的控制器硬件型号、软件版本号（不影响匿名化处理策略除外）和生产企业相同；
- m) 车辆需要进行匿名化处理的功能相关的摄像头等采集设备的硬件型号、主要参数配置（采样分辨率、采样视场角、采样帧率）和生产企业相同；
- n) 车辆触发匿名化处理的规则（需要进行匿名化处理的功能、匿名化处理的触发条件和处理逻辑）相同；
- o) 车辆搭载的应用程序下载平台数量相同或减少，且应用程序下载平台名称及下载页面展示规则相同。

注1：因车型涉及汽车数据处理功能及其汽车数据处理活动减少，导致车型涉及汽车数据处理功能对应的数据安全措施减少视为车型涉及汽车数据处理功能对应的数据安全措施相同。

注2：车型涉及汽车数据处理功能及其汽车数据处理活动减少时，同一收集车外数据的摄像头、激光雷达、4D毫米波雷达覆盖范围减少、分辨率降低也视为相同。

注3：匿名化处理策略包括匿名化方式、匿名化过程关键参数。

注4：匿名化方式分为高斯模糊、马赛克、色块、降低分辨率、删除帧等。

注5：匿名化处理过程关键参数包括存储后处理或实时处理，以及进行匿名化处理的图像视频的分辨率、匿名化处理后的图像视频的分辨率。

注6：匿名化处理逻辑相同指需要进行匿名化处理的功能相关的摄像头、控制器及调用的匿名化处理算法相同。

## 10.2 检验检测验证后视同判定条件

如车型发生涉及本文件10.1的变更，在符合下述规定时，仅需对变更参数相关的要求进行补充检验检测，经审批许可后获得扩展：

- a) 汽车数据安全保障要求相关内容有效且其签发日期未超过三年；
- b) 车辆具备与数据安全相关的监测和记录能力的控制器生产企业、硬件型号和软件版本号（不影响监测和记录规则的除外）相同；
- c) 摄像头、传声器或指纹传感器等收集车内汽车数据的传感器类型相同或减少；

- d) 摄像头、传声器或指纹传感器等收集车内汽车数据的传感器数量相同或减少；
- e) 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）的控制器数量相同或减少。

## 11 标准的实施

对于新申请型式批准的车型，自本文件实施之日起开始执行。

对于已获得型式批准的车型，自本文件实施之日起第13个月开始执行。

附 录 A  
(规范性)  
车型功能汽车数据处理活动清单要求

车辆制造商应按照表A.1建立并维护车型功能汽车数据处理活动清单。其中，存储地理位置的填报粒度应至少精确到地级市，若采用分布式存储或云存储，应列出所有数据副本所在的地级市。

表 A.1 车型功能汽车数据处理活动清单

| 车型功能基础信息 |    |         |          |      |                                       | 数据处理基本信息            |        |               |      |      |      |         |           |         |         |       |       | 通用信息   |        |        | 收集信息   | 传输信息 |         |             | 存储信息   |      |             |      | 删除信息 |      |
|----------|----|---------|----------|------|---------------------------------------|---------------------|--------|---------------|------|------|------|---------|-----------|---------|---------|-------|-------|--------|--------|--------|--------|------|---------|-------------|--------|------|-------------|------|------|------|
| 车型       | 功能 | 子功能（如有） | 搭载功能的控制器 | 功能描述 | 是否为通过用户画像、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 | 该功能调用摄像头、位置、传声器权限情况 | 数据处理目的 | 数据处理器及受托方（如有） | 数据名称 | 数据级别 | 数据类别 | 是否为个人信息 | 是否为敏感个人信息 | 是否为座舱数据 | 是否为车外数据 | 合法性解释 | 必要性解释 | 数据处理方式 | 取得同意路径 | 提示信息路径 | 撤回同意路径 | 收集方式 | 是否向车外传输 | 车外传输是否需要匿名化 | 数据接收地点 | 存储地点 | 存储地理位置（地级市） | 存储方式 | 存储期限 | 删除方式 |
|          |    |         |          |      |                                       |                     |        |               |      |      |      |         |           |         |         |       |       |        |        |        |        |      |         |             |        |      |             |      |      |      |

示例 1：车型：具体车型代号。

示例 2：功能：0 级驾驶自动化功能。

示例 3：子功能（如有）：自动紧急制动（AEB）。

示例 4：搭载功能的控制器：辅助驾驶域控制器。

示例 5：功能描述：车辆低速前行时，在自车即将与前方目标物体（车辆、VRU、通用静止障碍物）发生碰撞时发出预警提醒并自动实施制动，以降低车辆速度，从而尽可能降低正面碰撞程度。

示例 6：是否为通过用户画像、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：是/否。

示例 7：该功能调用摄像头、位置、传声器权限情况：调用了 XXX 摄像头权限、车辆位置权限、XXX 传声器权限。

示例 8：数据处理目的：收集即将与车辆前方目标物体发生碰撞时的前方车外视频、图像以及位置信息，以发出预警提醒并自动实施制动。

示例 9：数据处理者及受托方（如有）：车企/XXX 供应商/XXX 服务商。

示例 10：数据名称：位置信息。

示例 11：数据级别：一般数据/重要数据。

示例 12：数据类别：导航数据。

示例 13：是否为个人信息：是/否。

示例 14：是否为敏感个人信息：是/否。

示例 15：是否为座舱数据：是/否。

示例 16：是否为车外数据：是/否。

示例 17：合法性解释：取得同意/其他例外情形。

示例 18：必要性解释：XXX 所必须。

示例 19：数据处理方式：收集/传输/存储/使用/删除。

示例 20：取得同意路径：首次启动车辆/点击账号登录应用/点击人脸录入/自动弹窗等。

示例 21：提示信息路径：通过应用的首次弹窗的《隐私政策》进行提示。

示例 22：撤回同意路径：在 XXX 应用 XXX 界面取消授权。

示例 23：收集方式：车端收集/用户录入。

示例 24：是否向车外传输：是/否。

示例 25：车外传输是否需进行匿名化：是/否。

示例 26：数据接收地点：XXX 平台/无。

示例 27：存储地点：车端-XXX 部件/XXX 系统/XXX/XXX.XXX 文件/XXX 平台/XXX 数据中心。

示例 28：存储地理位置（地级市）：XXX 市。

示例 29：存储方式：长期存储/覆盖存储。

示例 30：存储期限：至 XXXX 年 X 月 X 日/永久/未明确。

示例 31：删除方式：到期删除/实时删除。

## 附录 B

(规范性)

## 车辆常见功能必要个人信息范围要求

车辆常见功能必要个人信息范围应符合表B.1。

表 B.1 车辆常见功能必要个人信息范围

| 序号 | 功能类型     | 基本功能服务     | 必要个人信息                           | 使用要求                                                                     |
|----|----------|------------|----------------------------------|--------------------------------------------------------------------------|
| 1  | 基础地图导航功能 | 定位、导航      | 位置信息                             | 用于确定用户位置，提供地图搜索展示和导航服务；<br>导航场景下因持续定位获得的行踪轨迹，应仅用于本次路线导航，完成导航后应及时删除或匿名化处理 |
|    |          |            | 车辆识别代号，唯一设备识别码、硬件序列号、出发地、到达地     | 用于用户自主输入出发地、到达地进行路线规划和导航                                                 |
| 2  | 语音交互功能   | 进行车辆语音交互   | 车辆识别代号，唯一设备识别码、硬件序列号、个人音频        | 用于车辆语音交互功能的使用                                                            |
| 3  | 车辆账号管理功能 | 可以进行车辆账号登录 | 车辆识别代号，唯一设备识别码、硬件序列号、个人电话号码、账号口令 | 用于车辆个人用户账号的登录                                                            |

附 录 C  
(规范性)  
个人信息分类分级要求

C.1 车辆制造商应按照表 C.1 进行个人信息分类与识别。

表 C.1 个人信息分类表

| 分类       | 个人信息                                                                                                                                                                       |
|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 个人基本资料   | 个人姓名、生日、年龄、电子邮箱地址、住址、个人电话号码、性别、家庭关系                                                                                                                                        |
| 个人身份信息   | 身份证、军官证、护照、驾驶证、个人账户的系统账号、特定身份信息                                                                                                                                            |
| 生物特征识别信息 | 人脸、个人基因、声纹、步态、眼纹、虹膜、指纹、掌纹、耳廓等生物特征识别信息                                                                                                                                      |
| 网络身份标识信息 | 用户账号、用户标识符（用户ID）                                                                                                                                                           |
| 个人教育工作信息 | 教育经历、职业、职位                                                                                                                                                                 |
| 个人财产信息   | 金融账户、消费记录、收入状况、借款信息、虚拟财产、风评记录、资产信息、信用记录、征信信息                                                                                                                               |
| 宗教信仰信息   | 个人信仰的宗教、加入的宗教组织、宗教组织中的职位、参加的宗教活动和特殊宗教习俗等个人信息                                                                                                                               |
| 医疗健康信息   | ——与个人的身体或心理的伤害、疾病、残疾和疾病风险或隐私有关的健康状况信息，如病症、既往病史、家族病史、传染病史、体检报告和生育信息等；<br>——在疾病预防、诊断、治疗、护理和康复等医疗服务过程中收集和产生的个人信息，如医疗就诊记录(如医疗意见、住院志、医嘱单、手术及麻醉记录、护理记录和用药记录)、检验检查数据(如检验报告和检查报告)等 |
| 身份鉴别信息   | 账号口令、数字证书                                                                                                                                                                  |
| 个人通信信息   | 通信记录和内容、短信、电子邮件、个人通信                                                                                                                                                       |
| 联系人信息    | 通讯录、好友列表、电子邮箱地址列表、群组列表                                                                                                                                                     |
| 个人上网记录   | 网页浏览记录、应用或软件使用或点击记录、收藏列表                                                                                                                                                   |
| 个人设备信息   | 硬件序列号、设备MAC地址、软件列表、唯一设备识别码如国际移动设备识别码（IMEI）等                                                                                                                                |
| 个人位置信息   | 交通出行信息、行踪轨迹信息、经纬度                                                                                                                                                          |
| 个人标签信息   | 用户标签、画像信息                                                                                                                                                                  |
| 个人车辆标识   | 车辆识别代号、车牌号、行驶证                                                                                                                                                             |
| 其他信息     | 个人音频、视频、图像数据、不满十四周岁未成年人个人信息、性取向、性生活、犯罪记录信息                                                                                                                                 |

C.2 车辆制造商应按照表 C.2 进行敏感个人信息分类与识别。

表 C.2 敏感个人信息分类表

| 分类       | 敏感个人信息 |
|----------|--------|
| 生物特征识别信息 | 个人基因   |
|          | 人脸     |
|          | 声纹     |

| 分类                                                                                                                                                                                                                               | 敏感个人信息                                                                                                                                                                     |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                                                                                                                                  | 步态                                                                                                                                                                         |
|                                                                                                                                                                                                                                  | 指纹                                                                                                                                                                         |
|                                                                                                                                                                                                                                  | 掌纹                                                                                                                                                                         |
|                                                                                                                                                                                                                                  | 眼纹                                                                                                                                                                         |
|                                                                                                                                                                                                                                  | 耳廓                                                                                                                                                                         |
|                                                                                                                                                                                                                                  | 虹膜                                                                                                                                                                         |
|                                                                                                                                                                                                                                  | 其他生物特征识别信息                                                                                                                                                                 |
| 宗教信仰信息                                                                                                                                                                                                                           | 个人信仰的宗教、加入的宗教组织、宗教组织中的职位、参加的宗教活动和特殊宗教习俗等个人信息                                                                                                                               |
| 特定身份信息                                                                                                                                                                                                                           | 残障人士身份信息、不适宜公开的职业身份信息等个人信息                                                                                                                                                 |
| 医疗健康信息                                                                                                                                                                                                                           | ——与个人的身体或心理的伤害、疾病、残疾和疾病风险或隐私有关的健康状况信息，如病症、既往病史、家族病史、传染病史、体检报告和生育信息等；<br>——在疾病预防、诊断、治疗、护理和康复等医疗服务过程中收集和产生的个人信息，如医疗就诊记录(如医疗意见、住院志、医嘱单、手术及麻醉记录、护理记录和用药记录)、检验检查数据(如检验报告和检查报告)等 |
| 金融账户信息                                                                                                                                                                                                                           | 个人的银行、证券、基金、保险和公积金等账户的账号及口令；公积金联名账号、支付账号、银行卡磁道数据(或芯片等效信息)；和基于账户信息产生的支付标记信息和个人收入明细等个人信息。                                                                                    |
| 行踪轨迹信息                                                                                                                                                                                                                           | 精准定位信息、连续精准定位轨迹信息、车辆行驶轨迹信息和人员连续的活动轨迹信息等个人信息                                                                                                                                |
| 不满十四周岁未成年人个人信息                                                                                                                                                                                                                   | 不满十四周岁未成年人的个人信息                                                                                                                                                            |
| 其他敏感个人信息                                                                                                                                                                                                                         | 居民身份证照片、性取向、性生活、征信信息、犯罪记录信息和显示个人身体私密部位的照片或视频信息等个人信息                                                                                                                        |
| <p><b>注1：</b>个人的体重、身高、血型、血压和肺活量等基本体质信息，如与个人的疾病和医疗就诊无关，则认为不属于敏感个人信息范畴。</p> <p><b>注2：</b>通过调用个人移动通信终端精准位置权限采集的位置信息是精准定位信息，通过网络地址等测算的粗略位置信息不是精准定位信息，连续采集的精准定位信息可用于生成行踪轨迹。</p> <p><b>注3：</b>犯罪记录，是指我国国家专门机关对犯罪人员的客观记载，如罪名和刑罚等记录。</p> |                                                                                                                                                                            |

附 录 D  
(规范性)  
汽车重要数据识别要求

车辆制造商应按照表D. 1进行汽车重要数据识别，符合表D. 1提出的任意一个识别规则的数据属于汽车重要数据。

表 D. 1 汽车重要数据目录

| 序号 | 数据类别                           | 数据项                                                              | 判定条件                                                                                                                                                                     |
|----|--------------------------------|------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1  | 驾驶自动化功能训练/<br>测试关键数据<br>(感知数据) | 激光雷达和4D毫米波雷达点云数据                                                 | ——反映重要敏感区域(军事管理区、国防科工单位以及县级以上党政机关等)地理信息、人员流量、车辆流量;<br>——涉及10万台以上车辆收集的包含精确目标物信息的;<br>——连续覆盖超过10公里或累计超过350公里国内道路                                                           |
| 2  |                                | 视频、图像数据                                                          | ——反映重要敏感区域(军事管理区、国防科工单位以及县级以上党政机关等)地理信息、人员流量、车辆流量;<br>——包含车外人脸和汽车号牌;<br>——涉及1万条以上敏感个人信息或10万条以上个人信息;<br>——涉及10万台以上车辆收集的能够反映经济运行情况;<br>——连续覆盖超过10公里或累计超过350公里国内道路, 并与轨迹关联的 |
| 3  |                                | 位置轨迹数据: GNSS速度、时间戳、载波、伪距、经纬度信息、行驶轨迹等                             | 涉及10万台以上车辆                                                                                                                                                               |
| 4  | 驾驶自动化功能训练/<br>测试关键数据<br>(决策数据) | 驾驶员决策数据集: 档位信息、加速踏板开度、制动踏板开度、方向盘转向角等                             | 与感知数据融合频率不小于10Hz, 连续时长不小于30s, 总时长不低于2000小时                                                                                                                               |
| 5  |                                | 自动驾驶或组合驾驶辅助系统决策数据集或预测数据集: 档位信息、加速踏板开度、制动踏板开度、转向角、转向力矩、灯光状态、雨刮状态等 | 与感知数据融合频率不小于10Hz, 连续时长不小于30s, 总时长不低于2000小时                                                                                                                               |
| 6  | 驾驶自动化功能训练/<br>测试关键数据<br>(运行数据) | 自动驾驶与人工切换数据集                                                     | 包含切换时刻前2s, 与车辆感知、决策数据融合且频率不小于10Hz, 连续时长不小于30s, 总时长不低于2000小时                                                                                                              |
| 7  |                                | 车辆状态数据集: 车速、车辆航向角、车辆侧倾角速度、横摆角速度、横纵向加速度等                          | 与感知数据融合且频率不小于10Hz, 连续时长不小于30s, 总时长不低于2000小时                                                                                                                              |

| 序号 | 数据类别   | 数据项                           | 判定条件                                                                                                                                               |
|----|--------|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| 8  | 研发过程数据 | 新能源关键技术的设计模型、图纸、方案、技术文档、测试报告等 | ——代表行业先进水平（汽车领域国家科技计划（含国家重大专项、重点研发计划）项目或获得国家级重大科技奖项的相关成果或全球首套高端装备相关技术）；<br>——在《中国禁止出口限制出口技术目录》《中华人民共和国两用物项出口管制清单》《两用物项和技术进出口许可证管理目录》中涉及的我国汽车领域特有技术 |
| 9  |        | 涉及车辆横纵垂运动控制及四门两盖开关控制程序源代码     | 非开源且涉及境内运行联网车辆的                                                                                                                                    |
| 10 |        | 自动驾驶或组合驾驶辅助系统/功能的源代码及算法       | 非开源且涉及境内运行联网车辆的                                                                                                                                    |
| 11 |        | 项目规划和实施过程中产生的技术文件、过程数据及技术报告   | ——涉及国家重大科技计划（含国家重大专项、重点研发计划）或国家级重大科技奖项的相关数据；<br>——在《中国禁止出口限制出口技术目录》《中华人民共和国两用物项出口管制清单》《两用物项和技术进出口许可证管理目录》中涉及的我国汽车领域特有技术                            |
| 12 | 生产过程数据 | 涉及自动化产线的冲压工艺参数                | ——涉及国家重大科技计划（含国家重大专项、重点研发计划）或国家级重大科技奖项的相关数据；<br>——在《中国禁止出口限制出口技术目录》《中华人民共和国两用物项出口管制清单》《两用物项和技术进出口许可证管理目录》中涉及的我国汽车领域特有技术                            |
| 13 |        | 涉及视觉引导的焊接工艺的基础工艺参数            | ——涉及国家重大科技计划（含国家重大专项、重点研发计划）或国家级重大科技奖项的相关数据；<br>——在《中国禁止出口限制出口技术目录》《中华人民共和国两用物项出口管制清单》《两用物项和技术进出口许可证管理目录》中涉及的我国汽车领域特有技术                            |
| 14 |        | 车辆生产控制的智能排程算法                 | ——涉及国家重大科技计划（含国家重大专项、重点研发计划）或国家级重大科技奖项的相关数据；<br>——在《中国禁止出口限制出口技术目录》《中华人民共和国两用物项出口管制清单》《两用物项和技术进出口许可证管理目录》中涉及的我国汽车领域特有技术                            |
| 15 |        | 其他产线规划和生产过程中产生或收              | ——涉及国家重大科技计划（含国家重大专项、重                                                                                                                             |

| 序号 | 数据类别 | 数据项                                               | 判定条件                                                                                                                                              |
|----|------|---------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
|    |      | 集的设备参数、工艺参数、控制程序源代码或算法文件                          | 点研发计划)或国家级重大科技奖项的相关数据;<br>——在《中国禁止出口限制出口技术目录》《中华人民共和国两用物项出口管制清单》《两用物项和技术进出口许可证管理目录》中涉及的我国汽车领域特有技术                                                 |
| 16 | 其他   | 座舱语料数据                                            | 经过标注用于座舱功能算法开发且体现国内群体特征的非公开的语料数据。                                                                                                                 |
| 17 |      | 安全驾驶功能升级软件包对应的源代码                                 | 同时涉及升级境内运行车辆的;升级车辆远程控制功能的,不包含通过近场通信的方式实现的控制功能;升级车辆启动行驶、动力丢失、紧急制动、巡航控制、车道保持、充放电控制、电池温度控制等功能的                                                       |
| 18 |      | 汽车行业关键信息基础设施数据                                    | 被认定为本行业、本领域的关键信息基础设施                                                                                                                              |
| 19 |      | 汽车行业核心技术数据                                        | ——代表行业先进水平(汽车领域国家科技计划(含国家重大专项、重点研发计划)项目或获得国家级重大科技奖项的相关成果或全球首台套高端装备相关技术);<br>——在《中国禁止出口限制出口技术目录》《中华人民共和国两用物项出口管制清单》《两用物项和技术进出口许可证管理目录》中涉及的我国汽车特有技术 |
| 20 |      | 未公开的汽车漏洞信息、事件信息(如恶意程序攻击、信息泄露等)、网络与数据安全重大发现与重要研究成果 | 能够引发汽车领域,按照国家相关规定定义的的重<br>大(二级)及以上的网络安全事件、重大及以上的数据安全事件的                                                                                           |
| 21 |      | 汽车产能数据                                            | 未公开产能数据                                                                                                                                           |
| 22 |      | 汽车芯片、电池等供需情况数据                                    | 涉及未公开的行业整体供需情况、供应商及用户整体统计分布情况的                                                                                                                    |
| 23 |      | 其他重要数据                                            | 按照法律、行政法规、部门规章和强制性国家标准识别申报的以及行业监管部门评估确定的其他汽车重要数据                                                                                                  |

附 录 E  
(规范性)

个人同意例外情形功能清单要求

车辆制造商应依据表E. 1填写个人同意例外情形功能清单。

表 E. 1 个人同意例外情形功能清单

| 序号 | 功能 | 例外情形 | 数据类型 | 理由 | 说明路径 |
|----|----|------|------|----|------|
|    |    |      |      |    |      |
|    |    |      |      |    |      |

附 录 F  
(规范性)

车辆数据收集设备参数信息清单要求

车辆制造商应依据表F.1填写车辆数据收集设备参数信息清单。

表 F.1 车辆数据收集设备参数信息清单

| 序号 | 设备类型 | 设备品牌 | 设备生产企业 | 设备硬件型号 | 设备软件版本号 | 采样分辨率 | 采样覆盖范围 | 安装位置 | 涉及功能 | 功能解释及必要性分析 | 备注 |
|----|------|------|--------|--------|---------|-------|--------|------|------|------------|----|
|    |      |      |        |        |         |       |        |      |      |            |    |
|    |      |      |        |        |         |       |        |      |      |            |    |

## 参 考 文 献

- [1] GB 16735—2019 道路车辆 车辆识别代号（VIN）
  - [2] GB/T 25069—2022 信息安全技术 术语
  - [3] GB/T 35273—2020 信息安全技术 个人信息安全规范
  - [4] GB/T 40660—2021 信息安全技术 生物特征识别信息保护基本要求
  - [5] GB/T 41871—2022 信息安全技术 汽车数据处理安全要求
  - [6] GB/T XXXXX—XXXX 汽车数据安全保障要求
-