IVISTA

网 联 智 能 与 隐 私 安 全 专 项 测 评

编号：IVISTA-XX-XXX.XX.XX-XX-XX-XXXX

网络与隐私安全
隐私安全试验规程

Cybersecurity and Privacy Security

Privacy Security Test Protocol

（2023 版修订版）

中国汽车工程研究院股份有限公司 发布

目　次

隐私安全试验规程

1 范围

本文件规定了网络与隐私安全测评中隐私安全的测试方法。

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 44495-2024 汽车整车信息安全技术要求

GB/T 35273-2020 信息安全技术 个人数据安全规范

GB/T 41871-2022 信息安全技术 汽车数据处理安全要求

GB/T 44464-2024 汽车数据通用要求

3 术语和定义

以下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、运维等过程中涉及的个人信息和重要数据。

[源：GB/T 41871-2022，3.1]

3.2

汽车数据处理者 vehicle data processor

开展汽车数据处理活动的组织，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。

[源：GB/T 41871-2022，3.5]

3.3

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车主、驾驶人、乘车人、车外人员等有关的各种信息，不包括匿名化处理后的信息。

[源：GB/T 41871-2022，3.2]

3.4

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。

[源：GB/T 41871-2022，3.4，有修改]

3.5

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，包括车辆行踪轨迹、音频、视频、图像和生物识别特征等信息。

[源：GB/T 41871-2022，3.3，有修改]

3.6

座舱隐私数据 cabin privacy 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隐私信息的数据，以及对其进行加工后产生的数据。

[源：GB/T 41871-2022，3.6，有修改]

3.7

个人信息主体 personal information subject

个人信息所标识或者关联的自然人。

[源：GB/T 35273-2020，3.3]

4 试验要求

4.1 试验场地及试验环境

4.1.1 试验场地要求

a）选择宽敞平坦的开放性测试场地或整车屏蔽室，避免无线信号的干扰和反射；

b）开放性测试场地两侧与静止目标车前方 30 米内无任何车辆、障碍物或其他影响试验的物体。

4.1.2 试验环境要求

在测试过程中，避免其他无线设备的干扰，确保测试环境的纯净性。

4.2 车辆准备

4.2.1 系统初始化

试验开始前，可进行试验车辆恢复出厂设置，保持车辆为首次设置状态。

4.2.2 车辆状态确认

a）试验车辆应为新车，行驶里程不高于 5000 公里；

b）车辆抵达试验场地后，检查车辆状态是否完好，确认零部件完整、整车外观无明显损坏、状态指示灯正常、整车上电及自检功能正常、试验相关系统功能正常。若有异常则记录，若异常状态与试验相关，则应对其修复或更换车辆；

c）对于燃油车，确保燃油量达到油箱容积的 50% 以上；对于可外接充电的新能源车辆，电量不低于最大容量的 50%。

4.2.3 功能清单梳理

在开始试验之前，针对所试验车型梳理功能清单，涉及处理个人信息和重要数据的功能清单至少包括以下内容：

a）功能名称；

b）功能说明：至少包含涉及的个人信息和/或重要数据处理必要性；

c）功能对应的数据收集类型、收集方式和收集内容：至少描述该功能是否包含敏感个人信息、个人信息、重要数据，及该功能对应的数据收集方式，若包含敏感个人信息需要明确敏感个人信息的信息类型；

d）功能所涉及的各项数据的提示/授权同意/撤回/删除方式；

e）功能所涉及的各项数据是否涉及车外传输；

f）功能是否涉及生物特征识别技术及替代方案说明；

g）功能是否属于满足 4.2.3 节 h）所列举的例外情形及例外情形的说明；

h）例外情形

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的车外个人信息；

——其他符合法律、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。

4.3 试验过程及结果记录

a）试验开始前，对车辆信息进行拍照记录，包括在车左前方 45°对整车进行拍照和车辆铭牌进行拍照；

b）试验完成后，通过拍照或录像的方式记录车辆状态，包括但不限于试验车辆车门状态、仪表盘、中控台显示信息及系统提示等。

5 试验方法

隐私安全试验项目包括座舱隐私安全试验和个人权益保护试验两个部分。具体试验方法见附录 A 和附录 B。

附录 A

座舱隐私安全试验方法

A.1 试验方法

A.1.1 隐私开关默认不开启

A.1.1.1 车内摄像头默认不开启

按照处理个人信息的功能清单，结合隐私政策中关于车内摄像头的使用场景，逐一触发涉及车内摄像头的功能，通过功能描述、提示信息等查看摄像头是否默认不开启。

A.1.1.2 车内麦克风默认不开启

按照处理个人信息的功能清单，结合隐私政策中关于车内麦克风的使用场景，逐一触发涉及车内麦克风的功能，通过功能描述、提示信息等查看麦克风是否默认不开启。

A.1.1.3 车辆定位默认不开启

按照处理个人信息的功能清单，结合隐私政策中关于车辆定位的使用场景，逐一触发涉及车辆定位的功能，通过功能描述、提示信息等检查车辆定位是否默认不开启。

A.1.1.4 其他收集座舱隐私数据的传感器默认不开启

按照处理个人信息的功能清单，选取车内除摄像头、麦克风、车辆定位外其他收集座舱隐私数据的传感器（如指纹传感器、红外传感器等），基于功能描述、提示信息等，查看被测传感器是否默认不开启。

A.1.2 数据默认不出车

A.1.2.1 车内图像、视频数据不出车

按照处理个人信息的功能清单，结合隐私政策中关于车内摄像头的使用场景，逐一触发除4.2.3 h）所列情形外需要向车外提供车内图像、视频数据的功能，试验车辆是否通过功能描述、提示信息等方式向用户告知并取得个人同意，查看是否存在未经用户同意向车外传输车内图像、视频数据的情况。

A.1.2.2 车内录音数据不出车

按照处理个人信息的功能清单，结合隐私政策中关于车内麦克风的使用场景，逐一触发除4.2.3 h）所列情形外需要向车外提供车内录音数据的功能，试验车辆是否通过功能描述、提示信息等方式向用户

告知并取得个人同意，查看是否存在未经用户同意向车外传输车内录音数据的情况。

A.1.2.3 车辆位置数据不出车

按照处理个人信息的功能清单，结合隐私政策中关于车辆定位的使用场景，逐一触发除4.2.3 h）所列情形外需要向车外提供车辆位置数据的功能，试验车辆是否通过功能描述、提示信息等方式向用户告知并取得个人同意，查看是否存在未经用户同意向车外传输车辆位置数据的情况。

A.1.2.4 其他传感器收集的数据默认不出车

按照处理个人信息的功能清单，选取车内除摄像头、麦克风、车辆定位外其他收集座舱隐私数据的传感器（如指纹传感器、红外传感器等），启动相应功能，试验车辆是否通过功能描述、提示信息等方式向用户告知并取得个人同意，查看是否存在未经用户同意向车外传输其他座舱隐私数据的情况。

A.1.3 数据持续收集提示

A.1.3.1 车内图像、视频数据持续收集提示

按照处理个人信息的功能清单，结合隐私政策中关于车内摄像头的使用场景，触发涉及车内摄像头的功能，查看当摄像头在前端运行和在后台运行时，显示仪表或屏幕是否有提示标识或信息。

A.1.3.2 车内音频数据持续收集提示

按照处理个人信息的功能清单，结合隐私政策中关于车内麦克风的使用场景，触发涉及车内麦克风的功能，查看当麦克风在前端运行和在后台运行时，显示仪表或屏幕是否有提示标识或信息。

A.1.3.3 车辆位置数据持续收集提示

按照处理个人信息的功能清单，结合隐私政策中关于车辆定位的使用场景，触发涉及车辆定位的功能，查看当定位功能在前端运行和在后台运行时，显示仪表或屏幕是否有提示标识或信息。

A.1.4 个人隐私数据隔离

A.1.4.1 车主和授权账号数据隔离

分别登录车主账号和授权账号，在如地图、相册、行车记录仪、日历、第三方应用等应用中产生不同数据；分别登录车主账号和授权账号，查看是否可以访问非本账号下产生的数据，测试不同账号之间是否具有数据隔离。

A.1.4.2 游客账号数据隔离

分别登录车主账号和授权账号，在如地图、相册、行车记录仪、日历、第三方应用等应用中产生不

同数据；退出车主账号和授权账号登录，通过游客登录或不登录账号，查看是否可以访问车主账号和授权账号下产生的数据，测试游客账号与其他账号是否具有数据隔离。

A.1.5 车内隐私增强保护功能

A.1.5.1 车内隐私增强保护功能

查验车辆是否具备除上述测试内容外的其他座舱隐私安全措施，如车内摄像头物理遮挡、一键关闭车内敏感数据收集、用户使用记录隐藏等。

a） **一键关闭车内敏感数据收集**

试验车辆是否具有一键关闭车内敏感数据收集的功能，即开启功能后，车内摄像头、麦克风、定位系统等不再收集车内数据，提高车内隐私性。

b） **用户使用记录隐藏**

试验车辆是否具有用户使用记录隐藏功能，即开启用户使用记录隐藏功能后，车内电话号和通话记录、地图搜索历史记录、日历日程等信息会隐藏不可见，提高车内隐私性。

c） **车内摄像头物理遮挡**

试验车辆车内摄像头是否存在物理开关，是否通过配置物理滑盖等方式对车内摄像头进行遮挡，有效保护乘客隐私。

A.2 结果记录

表 A.1 座舱隐私安全结果记录表

项目	试验类型	试验场景	结果记录	结果指标
座舱隐私安全试验	隐私开关默认不开启	车内摄像头默认不开启	车内摄像头是否默认处于不开启状态	□是 □否 □不适用
		车内麦克风默认不开启	车内麦克风是否默认处于不开启状态	□是 □否 □不适用
		车辆定位默认不开启	车辆定位是否默认处于不开启状态	□是 □否 □不适用
		其他传感器默认不开启	其他收集座舱隐私数据的传感器是否默认处于不开启状态	□是 □否 □不适用
	数据默认不出车	车内图像、视频数据不出车	车辆是否存在未经用户同意向车外传输车内图像、视频数据的情况	□是 □否 □不适用
		车内录音数据不出车	车辆是否存在未经用户同意向车外传输车内录音数据的情况	□是 □否 □不适用
		车辆位置数据默认不出车	车辆是否存在未经用户同意向车外传输车辆位置数据的情况	□是 □否 □不适用
		其他传感器收集的数据默认不出车	车辆是否存在未经用户同意向车外传输其他传感器收集的座舱隐私数据的情况	□是 □否 □不适用
	数据持续收集提示	车内图像、视频数据持续收集提示	车内图像、视频数据持续收集时是否存在提示标识或信息	□是 □否 □不适用
		车内音频数据持续收集提示	车内音频数据持续收集时是否存在提示标识或信息	□是 □否 □不适用
		车辆位置数据持续收集提示	车辆位置数据持续收集时是否存在提示标识或信息	□是 □否 □不适用
	个人隐私数据隔离	车主和授权账号数据隔离	车主账号和授权账号是否存在数据隔离	□是 □否 □不适用
		游客账号数据隔离	车辆处于游客模式登录时和车主、授权账号是否存在数据隔离	□是 □否 □不适用
	车内隐私增强保护功能	车内隐私增强保护功能	是否配备如车内摄像头物理遮挡、一键关闭车内敏感数据收集、用户使用记录隐藏等其他座舱隐私安全措施	□是，数量：　项 □否 □不适用

附录 B

个人权益保护试验方法

B.1 试验方法

B.1.1 处理个人信息显著告知

B.1.1.1 个人信息收集告知

查看车机系统个人隐私政策，检查是否告知用户收集个人信息的目的、范围、数据类型、使用方式等，告知内容是否清晰易懂、易于访问，文字无歧义。

B.1.1.2 个人信息共享告知

查看车机系统个人隐私政策，检查是否告知用户在共享或披露个人信息给第三方时的第三方信息和数据使用目的，告知内容是否清晰易懂、易于访问，文字无歧义。

B.1.1.3 个人信息存储告知

查看车机系统个人隐私政策，检查是否告知用户个人信息存储的期限、地点以及超期或不可删除数据时的保护措施，告知内容是否清晰易懂、易于访问，文字无歧义。

B.1.1.4 儿童信息保护告知

查看车机系统个人隐私政策，检查是否告知用户收集儿童个人信息需要监护人同意以及保护儿童信息安全的措施，告知内容是否清晰易懂、易于访问，文字无歧义。

B.1.2 生物特征信息保护

B.1.2.1 生物特征识别信息不出车

按照处理个人信息的功能清单，选取需要收集生物特征识别信息的功能，试验车辆是否通过隐私政策、功能描述、提示信息等方式，明确说明生物特征识别信息仅用于车端对比，查看是否存在向车外传输生物特征识别信息的情况。

B.1.2.2 身份认证方式唯一性

按照处理个人信息的功能清单，触发需要进行身份认证的功能，拒绝提供生物特征识别信息，试验是否支持通过其他途径进行用户身份认证。

B.1.3 个人信息授权与撤回

B.1,3.1 取得个人同意

查看车机系统个人隐私政策、产品说明书或功能介绍页，测试启用功能时是否提供了同意和拒绝的方式，并说明了取得个人同意的例外情形及理由。

B.1.3.2 敏感个人信息单独同意

按照处理个人信息的功能清单，逐一启动除4.2.3 h）所列情形外的试验车辆的各项涉及处理敏感个人信息的功能，试验是否存在单独同意敏感个人信息处理的选项。

B.1.3.3 敏感个人信息自主设定同意期限

按照处理个人信息的功能清单，启动除4.2.3 h）所列情形外的试验车辆各项个人信息处理功能，试验处理敏感个人信息时个人信息主体是否可以自主设定同意期限的数值，或是否可以自主从所提供选项中选择同意期限，并且同意期限不可设定为永久。

B.1.3.4 个人信息同意期届满重新取得同意

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，逐一启动除4.2.3 h）所列情形外的试验车辆各项个人信息处理功能，试验个人同意期届满后，是否重新取得个人同意。

B.1.3.5 撤回个人同意

按照处理个人信息的功能清单，除4.2.3 h）所列情形外，撤回各项功能的个人同意，撤回同意方式包括但不限于：提供权限开关按钮、注销账号、人工服务等方式，试验各项功能是否提供撤回个人同意的途径，并且撤回个人同意后，不影响撤回前基于个人同意已进行的个人信息处理活动效力。

B.1.4 个人行权机制

B.1.4.1 查阅、复制权

查看车企提供的个人行权渠道，试验是否存在查阅、复制权的行使渠道。

B.1.4.2 更正、补充权

查看车企提供的个人行权渠道，试验是否存在更正、补充权的行使渠道。

B.1.4.3 删除权

查看车企提供的个人行权渠道，试验是否存在删除权的行使渠道。

B.1.4.4 投诉、举报渠道及处理

查看车企提供的个人行权渠道，试验是否建立了便捷的投诉举报渠道，并且在隐私政策规定时间内

处理了用户的投诉举报。

B.2 结果记录

表 B.1 个人权益保护结果记录表

项目	试验类型	试验场景	结果记录	结果指标
个人权益保护试验	处理个人信息显著告知	个人信息收集告知	隐私政策是否告知用户收集个人信息的目的、范围、数据类型、使用方式等，告知内容清晰易懂、易于访问，文字无歧义	□是 □否 □不适用
		个人信息共享告知	隐私政策是否告知用户在共享或披露个人信息给第三方时的第三方信息和数据使用目的	□是 □否 □不适用
		个人信息存储告知	隐私政策是否告知用户个人信息存储的期限、地点以及超期或不可删除数据时的保护措施	□是 □否 □不适用
		儿童信息保护告知	隐私政策是否告知用户收集儿童个人信息需要监护人同意以及保护儿童信息安全的措施	□是 □否 □不适用
	生物特征信息保护	生物特征识别信息不出车	车辆是否不收集生物特征识别信息，或通过隐私政策、功能描述、提示信息等方式，明确说明生物特征识别信息仅用于车端对比，不存在向车外传输生物特征识别信息的情况	□是 □否 □不适用
		身份认证方式唯一性	是否支持通过除生物特征识别信息之外的其他途径进行用户身份认证	□是 □否 □不适用
	个人信息授权与撤回	取得个人同意	是否提供同意和拒绝同意的途径，并说明取得个人同意的例外情形及理由	□是 □否 □不适用
		敏感个人信息单独同意	是否存在单独同意敏感个人信息的选项	□是 □否 □不适用
		敏感个人信息自主设定同意期限	是否可以自主设定同意期限的数值，或自主从所提供的选项中选择同意期限，并且同意期限不可设置为永久	□是 □否 □不适用
		个人信息同意期届满重新取得同意	个人同意期限届满后，继续进行除删除外的个人信息处理，是否需要重新取得个人同意	□是 □否 □不适用
		撤回个人同意	是否具备撤回个人同意的途径，且撤回个人同意后，不影响撤回前基于个人同意已进行的个人信息处理活动效力	□是 □否 □不适用
	个人行权机制	查阅、复制权	查阅、复制权的行使渠道是否合理有效	□是 □否 □不适用

		更正、补充权	更正、补充权的行使渠道是否合理有效	□是 □否 □不适用
		删除权	删除权的行使渠道合理有效	□是 □否 □不适用
		投诉、举报渠道及处理情况	是否建立了便捷的投诉举报渠道，并且在隐私政策规定时间内处理了用户的投诉举报	□是 □否 □不适用