IVISTA

网 联 智 能 与 隐 私 安 全 专 项 测 评

编号：IVISTA-CIPS-SM-CSPS.PS-TP-A0-2023

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）

中国汽车工程研究院股份有限公司 发布

目　次

1 范围 1
2 规范性引用文件 1
3 术语和定义 1
4 试验要求 2
5 试验方法 4
附录 A 座舱隐私安全试验方法 5
附录 B 个人权益保护试验方法 8
附录 C 数据出境安全试验方法 11

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/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

20214422-Q-339 汽车整车信息安全技术要求

20213606-T-339 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

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]

3.5

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]

3.6

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，应对试验车辆左前 45 度和车辆铭牌进行拍照；

b）试验车辆安装音视频拍摄设备，拍摄记录整个试验过程，拍摄视角至少满足如下要求：

——应记录试验车辆车门状态与指示灯信息；

——应记录试验车辆仪表盘、中控台显示信息及系统提示。

5 试验方法

隐私安全试验项目包括座舱隐私安全试验、个人权益保护试验及数据出境安全试验 3 个部分。具体试验方法见附录 A-附录 C。

附录 A

座舱隐私安全试验方法

A.1 试验方法

A.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，选取包含车内摄像头的功能，通过功能描述、提示信息等检查各功能是否存在默认开启的情况。

A.1.2 车内图像、视频数据不出车

按照处理个人信息的功能清单，选取除4.2.3 h）所列例外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.1.3 车内麦克风默认不开启

按照处理个人信息的功能清单，选取包含车内麦克风的功能，通过功能描述、提示信息等查看麦克风是否默认不开启。

A.1.4 车内录音数据不出车

按照处理个人信息的功能清单，选取除4.2.3 h）所列例外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.1.5 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，选取包含车内除摄像头、麦克风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）的功能，基于功能描述、提示信息等，查看被测传感器是否处于默认不开启状态。

A.1.6 其他收集座舱隐私数据的传感器数据默认不出车

按照处理个人信息的功能清单，选取包含车内除摄像头、麦克风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）的功能，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.1.7 多账号隔离

使用授权账号对个人信息进行访问，查看是否可以正常访问和处理；使用其他授权账号对个人信息进行访问，查看是否可以访问非本账号下产生的个人信息，测试不同账号之间是否存在个人信息隔离。

A.1.8 数据非授权访问

使用授权账号对数据存储区进行访问，查看是否可以正常访问，且尝试使用非授权账号对数据存储区进行访问，查看是否可以进行正常访问，测试对非授权账号是否进行访问限制。

A.1.9 其他座舱隐私安全措施

查验车辆是否具备其他座舱隐私安全措施，如车内摄像头设置物理遮挡、车内设置主驾隐私模式、车内设置隐私声盾、车内设置隐私玻璃等。

a）车内摄像头设置物理遮挡

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。

b)车内设置主驾隐私模式

试验车辆是否具备主驾隐私模式，如：进入该模式后，蓝牙电话通话记录隐藏，仅在仪表显示来电通知，中控屏不显示来电通知。

c）车内设置隐私声盾

试验车辆是否有隐私声盾功能，即通过消音技术对车内乘客对话声音进行抵消，在后排乘客打电话、开会议等场景中提供隐私保护。

d）车内设置隐私玻璃

试验车辆是否安装隐私玻璃，即在透光率大于等于70%的前提下，试验是否对车窗采用特殊涂层，提高车内隐私性。

A.2 结果记录

表 A.1 座舱隐私安全结果记录表

项目	试验场景	结果记录	结果指标
座舱隐私安全试验	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
	其他收集座舱隐私数据的传感器默认不开启	其他收集座舱隐私数据的传感器是否处于默认不开启状态	□是 □否 □不适用
	其他收集座舱隐私数据的传感器默认不出车	车辆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	□是 □否 □不适用
	多账号隔离	车辆存在多个可登录账号时，不同账号之间是否存在个人信息隔离	□是 □否 □不适用
	数据非授权访问	是否对非授权账号进行访问限制	□是 □否 □不适用
	其他座舱隐私安全措施	是否配备如车内摄像头设置物理遮挡、车内设置主驾隐私模式、车内设置隐私声盾、车内设置隐私玻璃等其他座舱隐私安全措施	□是，数量： 项 □否

附录 B

个人权益保护试验方法

B.1 试验方法

B.1.1 处理个人信息告知与同意

按照处理个人信息的功能清单，启动除4.2.3 h）所列例外情形的试验车辆各项个人信息处理功能，查看告知与同意信息是否内容全面、清晰易懂、易于访问，文字是否有歧义。

显著告知信息应包括但不限于：

a）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；

b）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；

c）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；

d）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；

e）用户权益事务联系人的姓名或名称和其联系方式；

f）法律、行政法规规定的应当告知的其他事项。

B.1.2 取得个人同意

通过查看车机系统个人隐私政策、产品说明书或功能介绍页，测试是否提供了拒绝同意的途径，并说明了取得个人同意的例外情形及理由。

B.1.3 撤回个人同意

按照处理个人信息的功能清单，除4.2.3 h）所列例外情形外，撤回各项功能的个人同意，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 个人信息存储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，启动除4.2.3 h）所列例外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，继续进行除删除外的个人信息处理时，是否重新取得个人同意。

B.1.5 敏感个人信息单独同意

按照处理个人信息的功能清单，启动除4.2.3 h）所列例外情形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.1.6 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）所列例外情形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.1.7 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.1.8 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.1.9 个人行权渠道

查看车企提供的个人行权渠道，是否建立了便捷的个人行使权利的申请受理和处理机制，拒绝个人行使权利的请求的，是否会说明理由。

B.1.10 查阅、复制权

查看车企提供的个人行权渠道，试验查阅、复制权的行使渠道是否合理有效。

B.1.11 更正、补充权

查看车企提供的个人行权渠道，试验更正、补充权的行使渠道是否合理有效。

B.1.12 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	告知与同意信息是否内容全面、清晰易懂、易于访问，文字无歧义	□是 □否 □不适用
	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
	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
	个人信息存储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
	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
	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
	个人行权渠道	是否建立了便捷的个人行使权利的申请受理和处理机制，拒绝个人行使权利的请求的，是否会说明理由	□是 □否 □不适用
	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
	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

附录 C

数据出境安全试验方法

C.1 试验方法

测试人员应开启车辆全部移动蜂窝通信通道、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，且抓包时长不少于 3600 s，解析通信报文数据。测试是否在车端抓取或捕获的数据中发现境外IP；若发现境外IP，测试是否存在直接向境外传输数据的行为；若测试过程中发现存在向境外传输数据的行为，则通知企业，由企业配合在10个工作日内提供自证资料，证明数据传输行为的合规性。

注 1：车辆不应直接向境外传输数据；

注 2：出境数据基本信息的记录和出境数据保存政策可以确保数据传输的透明性和追溯性，法规要求向境外提供重要数据的，应向国家网信部门报送汽车数据在境外的保存地点、期限、范围和方式，并提供相关记录；

注3：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试验限制。

C.2 结果记录

表 C.1 数据出境安全结果记录表

结果记录	结果指标
是否在车端抓取或捕获的数据中发现境外 IP	□是 □否 □不适用
发现境外 IP 后，检测是否存在直接向境外传输数据的行为	□是 □否 □不适用
若测试过程中发现存在向境外传输数据的行为，企业是否配合在 10 个工作日内提供自证资料	□是 □否 □不适用