

TC260-PG-2026NA

网络安全标准实践指南

——座舱数据处理安全要求

(征求意见稿 v1.0-202608)

全国网络安全标准化技术委员会秘书处

2026 年 8 月

本文档可从以下网址获得：

www.tc260.org.cn/



全国网络安全标准化技术委员会
National Technical Committee 260 on Cybersecurity of SAC



前 言

《网络安全标准实践指南》（以下简称《实践指南》）是全国网络安全标准化技术委员会（以下简称“网安标委”）秘书处组织制定和发布的标准相关技术文件，旨在围绕网络安全法律法规政策、标准、网络安全热点和事件等主题，宣传网络安全相关标准及知识，提供标准化实践指引。

本《实践指南》得到中国电子技术标准化研究院、小米汽车科技有限公司、北京理想汽车有限公司、国家计算机网络应急技术处理协调中心、上海机动车检测认证技术研究中心有限公司、引望智能技术有限公司、北京航空航天大学等单位的技术支持。

主要编写人员：姚相振、杨思佳、郝春亮、张骁、刘振豪、王秉政、张雨桐、王寒生、王晖、李国强、侯佳美、潘灿杰、闫昭、李兆龙、周学兴、赵剑、郭春辰、戴志成、李实。



声 明

本《实践指南》版权属于网安标委秘书处，未经秘书处书面授权，不得以任何方式抄袭、翻译《实践指南》的任何部分。凡转载或引用本《实践指南》的观点、数据，请注明“来源：全国网络安全标准化技术委员会秘书处”。



全国网络安全标准化技术委员会
National Technical Committee 260 on Cybersecurity of SAC



摘 要

随着汽车座舱功能的日益智能化，座舱语音交互和车内图像视频识别等功能已成为主流车型的标准配置。配备智能化功能的汽车座舱通过车内摄像头、传声器等数据收集装置，收集大量包含敏感个人信息的座舱数据，若处理不当易引发个人隐私泄露和个人权益受损风险。GB/T 41871《信息安全技术 汽车数据处理安全要求》对汽车数据处理活动提出总体要求，但在实际应用中，座舱数据的收集、存储、传输、使用等处理环节仍需要细化的安全指南。

为贯彻落实《中华人民共和国个人信息保护法》《中华人民共和国数据安全法》《网络数据安全管理条例》《汽车数据安全若干规定（试行）》等法律法规和政策要求，本实践指南从座舱数据处理基本要求出发，针对典型功能场景下的座舱数据处理活动提出细化安全要求，为座舱数据处理器规范开展座舱数据处理活动，保护个人信息主体权益提供参考。



目 录

前 言	I
声 明	II
摘 要	III
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 基本要求	2
5 安全要求	3
6 安全管理要求	5





1 范围

本文件给出座舱数据处理安全要求，包括基本要求、安全要求和安全管理要求。

本文件适用于座舱数据处理者开展非营运车辆的座舱数据处理活动，也可作为汽车座舱功能设计研发提供参考。

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 个人信息安全规范

GB/T 37988—2019 信息安全技术 数据安全能力成熟度模型

GB/T 40660—2021 信息安全技术 生物特征识别信息保护基本要求

GB/T 41871—2022 信息安全技术 汽车数据处理安全要求

GB/T 45574—2025 数据安全技术 敏感个人信息处理安全要求

3 术语和定义

GB/T 35273—2020、GB/T 40660—2021、GB/T 41871—2022、GB/T 45574—2025 界定的术语和定义适用于本文件。

3.1 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内收集的个人信息的数据，以及对其进行加工后产生的数据。

注：座舱数据包括座舱内收集的车主、驾驶人、乘车人的人脸、声纹、指纹等生物特征数据、座舱内图像视频数据、座舱内语音对话记录等数据。



[来源：GB/T 41871—2022，3.6]

3.2 座舱数据处理者 cabin data processor

开展座舱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或车载应用服务提供者等。

3.3 智能语音对话 intelligent conversation

依托车载智能语音交互系统，以自然语音作为输入输出媒介，支持多轮上下文理解、连续交互，接收驾乘人员自然口语指令，完成座舱控制、信息检索、问答交互的会话式人机交互功能。

3.4 远程查看 remote viewing

通过车辆外部终端的配套移动应用程序，查看车内摄像头实时收集的图像、视频的功能。

4 基本要求

座舱数据处理者处理座舱数据应符合以下基本要求：

- a) 应符合 GB/T 41871 中全部要求；
- b) 涉及敏感个人信息的，应符合 GB/T 45574—2025 中敏感个人信息相关要求；
- c) 涉及人脸、声纹等生物特征识别信息的，应符合 GB/T 40660—2021 生物特征数据处理相关要求；
- d) 应按 GB/T 45574—2025 中 4.2 所述规则识别座舱数据中的敏感个人信息，在处理涉及敏感个人信息的座舱数据前，应取得用户单独同意；
- e) 除 GB/T 41871—2022 中 6.2 所述特例外，座舱数据不应向车外传输。



5 安全要求

5.1 语音唤醒

座舱数据处理者处理语音唤醒相关数据，安全要求如下：

- a) 除驾驶人自主设定外，车内传声器应默认不收集座舱数据；
- b) 采用车载显示面板提示语音数据收集状态时，应在车内人员易于观察的位置持续显示；仅通过单一位置显示不足以使相关车内人员感知的，宜通过其他车内显示终端补充提示；
- c) 车载应用服务通过调用接口等方式通过车内传声器收集座舱数据时，应向车内人员提示调用设备的服务名称；
- d) 应为用户提供临时关闭传声器的便捷方式；临时关闭传声器不应改变用户已做出的授权使用传声器收集语音数据状态的时间；
- e) 传声器处于停止收集状态时，宜向用户告知可能受到影响的功能；
- f) 为识别唤醒词临时存储语音数据的，存储时长不应超过完成唤醒识别所需的最小时长；
- g) 涉及声纹的座舱数据应在车端独立空间存储，不应与个人信息一起存储；
- h) 用户唤醒智能语音交互系统，传声器进入语音数据收集状态后，在预设时长内未接收到有效指令的，应退出数据收集状态；
- i) 应建立误唤醒数据处置机制。判定为误唤醒时，应及时退出语音交互状态，并删除误唤醒后的语音数据及过程数据；
- j) 应向用户告知智能语音对话功能被误唤醒情况下相关语音数据的传输、保存和删除等处理情况；
- k) 座舱语音唤醒数据原则上应在车内处理，确需传输到车外处理的，应优先传输实现相关功能所必要的语音文本；确需传输原始音频



的，应向用户说明传输的必要性、目的、数据范围、保存期限和删除方式，并取得用户单独同意。

5.2 智能语音对话

座舱数据处理者处理智能语音对话功能相关数据，安全要求如下：

- a) 应为用户提供开启和关闭车载智能语音对话功能的方式；
- b) 智能语音对话持续开启过程中，应为用户提供拒绝保存智能对话记录的选项；
- c) 原则上不应保存用户的智能对话记录，确需保存的，应向用户说明保存必要性、保存位置和保存期限；并通过车端、配套移动应用程序、语音指令或者其他便捷方式，向用户提供查询、删除对话记录的方式；
- d) 使用用户智能语音对话记录用于模型训练和产品优化的，应取得用户单独同意，并经匿名化处理，确保对话记录无法识别到对应的个人信息主体；
- e) 用户拒绝将对话记录用于模型训练和产品优化的，不应影响智能语音对话功能使用；
- f) 使用第三方服务提供者提供智能语音对话服务的，汽车制造商应通过合同约定座舱数据提供方式、存储期限、处理方式、采取的安全保护措施以及双方责任和义务。

5.3 驾驶员状态监测系统

座舱数据处理者处理驾驶员状态监测系统功能相关数据，安全要求如下：

注：驾驶员状态监测系统是指安装于座舱内，通过图像采集与车载智能算法实时识别驾驶员疲劳、分心、脱手等危险状态，并输出预警或整车干预指令的车载安全监测系统。

- a) 应告知用于驾驶员状态监测系统功能的摄像头位置；



- b) 摄像头收集数据范围不应包含车内其他人员；
- c) 所收集驾驶员人脸数据应在车内处理，宜采用即采即抛技术。

5.4 远程查看

座舱数据处理者处理远程查看功能相关数据，安全要求如下：

- a) 应为远程查看功能提供单独开启和关闭方式；
- b) 应对申请远程查看者进行身份验证；
- c) 远程查看启动前，应向车内人员告知车内摄像头位置、开启及关闭的方式；
- d) 远程查看功能启动时，应通过车载显示界面、指示灯、声音或者其他方式向车内显著提示；车内存在人员时，应在取得车内同意后再启动，并为车内人员提供终止远程查看功能的便捷方式；
- e) 仅提供实时远程查看功能的，不应存储车内图像视频；
- f) 在远程查看过程中提供截图或者录制功能的，应在传输和存储过程中采取加密、访问控制等安全防护措施，图像视频的查看、下载、删除操作，应仅对持有车辆对应访问权限的授权用户开放；
- g) 座舱数据处理者不应有权限访问远程查看过程中产生的图像视频数据。

6 安全管理要求

座舱数据处理者开展座舱数据处理活动，安全管理要求如下：

- a) 座舱数据处理者应按照 GB/T 45574—2025 识别其中涉及的敏感个人信息，并依据业务类型或数据类型建立敏感个人信息目录并及时更新；



- b) 座舱数据处理活动应留存完整操作日志不少于 1 年；涉及敏感个人信息的座舱数据的处理活动应留存完整操作日志不少于 3 年，日志内容应包括访问人员、访问时间、用户身份及操作类型等；
- c) 座舱数据处理者应明确可处理座舱数据人员的权限范围，不应超出权限处理数据；
- d) 座舱数据处理者的数据安全能力宜符合 GB/T 37988-2019 三级要求；
- e) 座舱数据处理者应定期开展数据安全培训，提升相关从业人员的数据安全保护意识和能力；
- f) 座舱数据处理者应制定数据安全事件应急预案，发生数据安全事件时，及时按照预案开展处置，并按规定向相关管理部门报告；
- g) 汽车制造商应全面掌握其生产的整车座舱内所包含的各零部件和车载应用服务收集、传输数据的情况，通过合同方式对零部件供应商和车载应用服务提供者的座舱数据处理行为进行约束，并对其履行合同情况进行监督。





参 考 文 献

- [1] 中华人民共和国个人信息保护法
- [2] 中华人民共和国数据安全法
- [3] 网络数据安全管理办法
- [4] 汽车数据安全管理办法（试行）
- [5] GB/T 36464.1—2020 信息技术 智能语音交互系统 第1部分：通用规范
- [6] GB/T 42574—2023 信息安全技术 个人信息处理中告知和同意的实施指南

