ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 41871—2022

信息安全技术　汽车数据处理安全要求

Information security technology—Security requirements for processing of motor vehicle data

2022-10-12 发布　　2023-05-01 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。

本文件由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本文件起草单位：中国电子技术标准化研究院、国家计算机网络应急技术处理协调中心、清华大学、中汽研软件测评(天津)有限公司、国汽(北京)智能网联汽车研究院有限公司、公安部第三研究所、中国科学院自动化研究所、北京理工大学、上海汽车集团股份有限公司、岚图汽车科技有限公司、上海蔚来汽车有限公司、浙江极氪智能科技有限公司、苏州挚途科技有限公司、北京百度网讯科技有限公司、重庆长安汽车股份有限公司、长城汽车股份有限公司、威马汽车科技集团有限公司、华为技术有限公司、北京小马易行科技有限公司、中国汽车工业协会、上海机动车检测认证技术研究中心有限公司。

本文件主要起草人：姚相振、郝春亮、罗璎珞、上官晓丽、张骁、李政、王晖、金涛、胡影、李海东、侯昕田、刘建行、唐迪、洪延青、王姣、刘昊、顾咏梅、朱雪峰、朱颢、张堃博、王秉政、李承泽、吴佳美、司华超、那奇、王磊、韩昭、陈重、王艳华、郭建领、滕添益、潘凯、朱中和、汪向阳、杨丹。

信息安全技术　汽车数据处理安全要求

1　范围

本文件规定了汽车数据处理者对汽车数据进行收集、传输等处理活动的通用安全要求、车外数据安全要求、座舱数据安全要求和管理安全要求。

本文件适用于汽车数据处理者开展汽车数据处理活动，适用于汽车的设计、生产、销售、使用和运维，也适用于主管监管部门和第三方评估机构等对汽车数据处理活动进行监督、管理和评估。

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　信息安全技术　个人信息安全规范

GB/T 40660　信息安全技术　生物特征识别信息保护基本要求

3　术语和定义

下列术语和定义适用于本文件。

3.1

汽车数据　motor 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数据和重要数据。

3.2

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。

3.3

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。

注：敏感个人信息包括行踪轨迹、音频、视频、图像、医疗健康、宗教信仰等个人信息，指纹、心律、声纹、面部识别特征等生物识别特征信息，居民身份证、军官证、工作证、社保卡、居住证等能标识特定身份的个人身份信息，银行账户、鉴别信息(口令)、金融账户等个人财产信息，以及不满十四周岁未成年人的个人信息。

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。

注：重要数据包括军事管理区、国防科工单位以及县级以上党政机关等重要敏感区域的地理信息、人员流量、车辆流量等数据，车辆流量、物流等反映经济运行情况的数据，汽车充电网的运行数据，包含人脸信息、车牌信息等

的车外视频、图像数据，涉及个人信息主体超过10万人的个人信息，有关部门确定的其他可能危害国家安全、公共利益或者个人、组织合法权益的数据等6类数据。

3.5

汽车数据处理者　motor 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。

3.6

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采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。

4　通用安全要求

4.1　汽车数据处理者处理个人信息符合下列要求。

a）　应符合GB/T 35273中的全部要求。

b）　取得个人同意时，应通过至少一种显著方式向个人告知。显著方式包括用户手册单独章条提示、语音播放、车载显示面板单独弹窗提示、汽车使用相关应用程序交互、汽车销售协议单独章条提示、维修服务协议单独章条提示或出行服务应用程序交互等。

c）　应使用清晰易懂的文字向个人信息主体说明收集个人信息的具体情境和必要性。

d）　向个人信息主体告知各类型个人信息的保存期限时，应具体且明确，例如30天或1年等。

e）　向个人信息主体告知其个人信息保存地点时，应将保存地点位置精确到地级市并告知所有保存地点。

f）　应为个人信息主体提供便捷的查阅、复制和删除等个人信息管理功能；提供的产品或服务支持交互操作时，例如提供网站、车载应用程序或移动通信终端应用程序等，个人信息管理功能应为交互式，且其功能入口应处于个人信息主体容易察觉的显著位置。

4.2　汽车数据处理者处理敏感个人信息符合下列要求。

a）　应对每项敏感个人信息取得个人信息主体单独同意，不应一次性针对多项敏感个人信息或多种处理活动取得同意。

注：汽车数据处理者为驾驶人提供语音识别功能需要处理语音数据，可针对该功能单独弹窗取得驾驶人同意，也可在告知同意中针对该功能设置可勾选的单独选项取得驾驶人同意。

b）　取得个人信息主体单独同意时，处理敏感个人信息的同意期限不应设置为“始终允许”或“永久”。

注：汽车数据处理者为语音识别功能需要处理语音数据，取得个人信息主体单独同意时，可为个人信息主体提供单次、七天、三个月和一年等选项。

c）　为了在收到删除个人信息请求后十个工作日内完成删除，原则上应建立个人信息结构化目录，实现个人信息的可追溯管理。

d）　原则上不应以改善服务质量、提升用户体验以及研发新产品等为目的处理敏感个人信息。

4.3　汽车数据处理者持续收集敏感个人信息符合下列告知要求。

a）　应通过车载显示面板图标或信号装置指示灯的闪烁或长亮等方式提示收集状态。

b）　持续提示收集敏感个人信息时，应根据信息类型的不同设置差异明显且清晰易懂的提示。

注：可通过摄像图标闪烁或长亮提示正在收集车内视频数据，通过录音图标闪烁或长亮提示正在收集车内语音数据，通过斜向上三角图标的闪烁或长亮提示正在收集位置数据。

4.4　汽车数据处理者处理人脸、声纹或指纹等生物识别特征信息符合下列要求。

a）　应评估是否具有增强行车安全的目的和充分的必要性。

注：增强行车安全的目的包括身份验证以及驾驶人状态监测等。

b） 应符合 GB/T 40660 的全部要求。

4.5 汽车数据处理者在个人信息保护方面设置的用户权益事务联系人符合下列要求。

a） 应具备个人信息保护和个人权益保护等方面的专业知识。

b） 应及时受理并处置个人信息保护方面的投诉和举报。

c） 应对外告知准确有效的姓名和联系方式，联系方式包括电话号码、邮箱地址、网址或即时通信平台账号等；不便对外告知真实姓名的，应告知长期且固定使用的别名。

4.6 涉及座舱数据、位置轨迹数据、车外视频和车外图像数据，以及涉及个人信息主体超过 10 万人的个人信息，汽车数据处理者应依法在中华人民共和国境内存储。

4.7 汽车数据处理者处理重要数据，一般应在完成脱敏处理后再进行其他处理；处理个人信息，一般应在匿名化处理或去标识化处理后再进行其他处理。

5 车外数据安全要求

汽车数据处理者对车外数据进行匿名化处理符合以下要求。

a） 车外数据未完成匿名化处理前，不应向车外提供。

b） 经过匿名化处理的视频以及图像应无法复原且无法关联个人信息主体，包括以下实现方式：

1） 完整删除：处理图像时，将包含人脸以及车牌等个人信息的图像直接删除；处理视频时，删除视频中所有包含人脸以及车牌等个人信息的视频帧；

2） 局部轮廓化处理：将视频以及图像中包含人脸以及车牌等个人信息的区域彻底擦除，或者将这些区域替代为无法关联个人信息主体且不可复原的其他图像。

c） 匿名化处理过程中，除分析确定包含人脸以及车牌等个人信息的区域，以及对这些区域进行删除或局部轮廓化处理外，不应进行人脸比对、步态分析以及语音识别等其他处理。

d） 匿名化处理完成后，过程数据应立即删除，不应向车外提供。

6 座舱数据安全要求

6.1 除非驾驶人自主设定，汽车应默认设定为不收集座舱数据的状态，包括不打开车内的摄像头、传声器、红外传感器和指纹传感器等部件，当驾驶人通过实体按键或触摸按键等方式主动选择后才能开始收集，汽车可根据驾驶人设定，保持驾驶人选择的状态或恢复默认状态。

6.2 汽车不应向车外提供座舱数据，下列情形除外。

a） 为实现语音识别功能以实时判断汽车控制指令，将语音指令数据在车外处理，取得个人信息主体同意，功能实现后即时删除原始数据及处理结果。

b） 为实现远程查看车内情况或云存储功能，向使用者提供数据，取得个人信息主体同意，并采取安全措施，除使用者外的其他组织和个人不能访问。

c） 道路运输车辆依据相关规定向所属运输企业监控平台、公共管理平台和监管机构传输数据。

d） 出租汽车和公共汽车等营运车辆向监管机构传输数据。

e） 道路交通事故发生后按执法部门要求传输数据。

6.3 汽车数据处理者应提供便利的终止收集座舱数据的方式，包括实体按键、语音控制、触摸按键以及汽车使用相关应用程序等。在保证行车安全以及人身安全的情况下，驾驶人选择终止收集后，应关闭车内传声器和摄像头等收集座舱数据的部件。为保证行车安全以及人身安全，下列情况可不关闭相关部件：

a） 正在提供公路营运服务的道路运输车辆持续收集座舱数据；

b） 正在提供出行服务的公共汽车持续收集座舱数据。

7 管理安全要求

7.1 汽车数据处理者开展汽车数据风险评估，评估内容一般包括汽车数据识别、数据处理活动识别、汽车数据安全风险识别和风险分析及评价等，可采取自评估或第三方评估的形式进行。

7.2 汽车数据安全管理负责人应由汽车数据处理者主要负责人或分管数据安全负责人担任，并应熟悉我国数据安全和个人信息保护政策法规，具备安全管理工作经历。

7.3 汽车数据处理者应建立健全安全事件应急处置机制，每年至少开展一次应急演练，并宜通过汽车数据存证、汽车数据溯源等机制支撑安全事件发生后的取证分析。

7.4 汽车数据处理者应通过电话或即时通信平台等方式受理汽车数据安全投诉，在接到投诉后一般在10个工作日内处理完成，并对处理过程以及处理结果进行完整记录。

7.5 汽车制造商应全面掌握其生产的整车所含各零部件收集、传输数据情况，对零部件供应商处理汽车数据的行为进行约束和监督，汽车数据向外传输的完整情况应每年或在出现重大变更时向用户披露。

8 特例

除有需要外，本文件各项要求不适用于以下数据处理活动：

a） 警车、消防车、救护车以及工程救险车等执行紧急任务时的汽车数据处理活动；

b） 装置有专用设备或器具的作业车辆在封闭场所内从事作业活动时的汽车数据处理活动；

c） 测试车辆在封闭场地开展科研以及定型试验等活动时的汽车数据处理活动。