TC260

全国信息安全标准化技术委员会技术文件

TC260-001

汽车采集数据处理安全指南

Security guidelines for processing vehicle collected data

2021-10-08 发布

全国信息安全标准化技术委员会发布

目 次

前　言

本文件由全国信息安全标准化技术委员会（SAC/TC260）发布。

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、上海蔚来汽车有限公司、岚图汽车科技有限公司。

本文件主要起草人：杨建军、姚相振、上官晓丽、郝春亮、罗璎珞、张骁、王晖、金涛、胡影、侯昕田、刘建行、唐迪、洪延青、王姣、顾咏梅、朱颢、张堃博、李承泽、吴佳美、司华超。

汽车采集数据处理安全指南

1 范围

本文件规定了对汽车采集数据进行传输、存储和出境等处理活动的安全要求。

本文件适用于汽车制造商开展汽车的设计、生产、销售、使用、运维，也适用于主管监管部门、第三方评估机构等对汽车采集数据处理活动进行监督、管理和评估。不适用于警车、消防车、救护车、工程救险车等执行紧急任务时的汽车采集数据，以及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采集数据。

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 7258 机动车运行安全技术条件

GB/T 25069 信息安全技术 术语

GB/T 35273 信息安全技术 个人信息安全规范

3 术语和定义

GB 7258、GB/T 25069、GB/T 35273界定的以及下列术语和定义适用于本文件。

3.1

汽车 vehicle

由动力驱动、用于载运人员货物的非轨道承载的车辆。

3.2

汽车采集数据 vehicle collected data

通过汽车传感设备、控制单元采集的数据，以及对其进行加工后产生的数据。

注：不包含通过网络或物理接口获取的其他系统或设备的数据。

3.3

远程信息服务平台 telematics service platform

用于车辆管理或者提供信息服务的远程系统。

4 汽车采集数据内容

汽车采集数据主要包括：

a) 车外数据：通过摄像头、雷达等传感器从汽车外部环境采集的道路、建筑、地形、交通参与者等数据，以及对其进行加工后产生的数据；

注1：交通参与者是指参与交通活动的人，包括机动车、非机动车、其他交通工具的驾驶员与乘员，以及其他参与交通活动相关的人员。

注2：车外数据可能包含人脸、车牌等个人信息以及车辆流量、物流等法律法规标准所规定的重要数据。

b） 座舱数据：通过摄像头、红外传感器、指纹传感器、麦克风等传感器从汽车座舱采集的数据，以及对其进行加工后产生的数据；

注3：座舱数据可能包含驾驶员和乘员的人脸、声纹、指纹、心律等敏感个人信息。

注4：座舱数据不包括对汽车采集数据处理产生的操控记录数据。

c） 运行数据：通过车速传感器、温度传感器、轴转速传感器、压力传感器等从动力系统、底盘系统、车身系统、舒适系统等电子电气系统采集的数据；

注5：运行数据包含整车控制数据、运行状态数据、系统工作参数、操控记录数据等。

d） 位置轨迹数据：基于卫星定位、通信网络等各种方式获取的汽车定位和途经路径相关的数据。

5 传输要求

5.1 未经个人信息主体单独同意，汽车不应通过网络向外传输包含其个人信息的车外数据，已进行匿名化处理的视频、图像数据除外。

注 1：匿名化处理包括对视频、图像中可识别个人身份的人脸、车牌等信息进行擦除等，确保无法利用视频、图像数据识别个人身份。

注 2：通过网络向外传输是指通过移动通信网络、无线局域网、充电桩接口等方式，向位于车外的设备、系统传输。

5.2 汽车不应通过网络向外传输座舱数据。

5.3 满足以下条件的，可作为上述条款的例外情形。

a） 为实现 5.1 所述匿名化处理功能，需要通过远程信息服务平台实时执行匿名化处理操作的情形，但应确保原始数据传输到平台后不用于其他目的，并在匿名化处理后得到删除。

b） 为实现语音识别等直接服务于驾驶人或乘员的功能，需要通过远程信息服务平台实时配合处理座舱数据的情形，但应征得驾驶人同意授权，且确保功能实现后即时删除原始数据及处理结果。

c） 为实现用户远程监控车内外情况、使用云盘存储用户数据等直接服务于用户的功能，需要通过网络向用户终端设备传输数据或使用远程信息服务平台存储数据的情形，但应在传输以及存储时采取加密等措施，确保用户数据只能由用户终端设备访问，在其他设备以及远程信息服务平台上无法访问。

d） 道路运输车辆、运营车辆依据相关行政管理要求向外传输座舱数据的情形。

e） 道路交通事故发生后按执法部门要求向外传输数据的情形。

6 存储要求

6.1 车外数据、位置轨迹数据在远程信息服务平台等车外位置中保存时间均不应超过14天。

6.2 满足以下条件的数据，可作为上述条款的例外。

a） 为优化行驶安全功能而存储的特定场景数据，但每车每天不应超过 3 个连续时间的数据片段，每个片段不应超过 2 分钟。

b) 符合 5.3 c)要求，用户传输到远程信息服务平台的数据。
c) 由采集训练数据的专用采集车辆或在特定区域行驶的专用测试车辆采集的数据，但车辆外部应有“测试车辆”或“数据采集车辆”及所属单位的显著标识，且驾驶人员为具备授权的特定人员。
d) 新能源汽车、道路运输车辆、网络预约出租汽车依据相关行政管理要求进行存储的数据。
e) 用于生产经营的汽车产生的，生产经营者可控的位置轨迹数据。

7 数据出境要求

7.1 车外数据、座舱数据、位置轨迹数据不应出境；运行数据如需出境，应当通过国家网信部门组织开展的数据出境安全评估。
7.2 汽车制造商应为主管监管部门开展数据出境情况的抽查工作提供技术手段，包括传输的数据格式、便于读取的数据展示方式等。

8 其他要求

8.1 汽车制造商应对整车的数据安全负责，全面掌握其生产的整车所含各零部件采集、传输数据情况，对零部件供应商处理汽车采集数据的行为进行约束和监督，并将汽车采集数据向外传输的完整情况对用户披露。
8.2 为执行相关行政管理要求采集的数据应仅用于行政管理要求明确规定的目的。