

ICS 35.020
L70

YD

中华人民共和国通信行业标准

YD/T 3746—2020

车联网信息服务 用户个人信息保护要求

Specification of Internet of vehicle information
service-User personal information protection

2020-08-31 发布

2020-10-01 实施

中华人民共和国工业和信息化部 发布

目 次

前言	II
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 用户个人信息保护基本原则	1
5 用户个人信息安全保护概述	2
5.1 用户个人信息保护对象	2
5.2 用户个人信息处理环节	2
5.3 用户个人信息保护基本思路	2
6 用户个人信息分类要求	3
6.1 用户个人信息分类方法	3
6.2 用户个人信息分类示例	3
7 用户个人信息敏感性分级要求	5
7.1 用户个人信息敏感性分级方法	5
7.2 用户个人信息敏感性分级示例	5
8 用户个人信息安全保护要求	6
8.1 个人一般信息安全保护要求	6
8.2 个人重要信息安全保护要求	6
8.3 个人敏感信息安全保护要求	6
参考文献	8

前　　言

本标准是“车联网网络与数据安全”系列标准之一，该系列标准的结构及名称预计如下：

- 《车联网无线通信安全技术指南》；
- 《车联网信息服务 数据安全技术要求》；
- 《车联网信息服务 用户个人信息保护要求》；
- 《车联网信息服务平台安全防护技术要求》。

本标准按照 GB/T 1.1—2009 给出的规则起草。

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这些专利的责任。

本标准由中国通信标准化协会提出并归口。

本标准起草单位：中国信息通信研究院、中兴通讯股份有限公司、北京百度网讯科技有限公司。

本标准主要起草人：孙娅萍、田慧蓉、柯皓仁、魏亮、于广琛、董悦、秦国英、马娟、张瑜、袁琦、林兆骥、李显杰。

车联网信息服务 用户个人信息保护要求

1 范围

本标准规定了车联网信息服务用户个人信息保护的信息内容分类、敏感性分级和分级保护要求。

本标准适用于车联网相关的汽车厂商、零部件和元器件供应商、软件提供商、数据内容提供商和服务提供商等在提供服务过程中的用户个人信息保护。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是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

3 术语和定义

下列术语和定义适用于本文件。

3.1

车联网信息服务用户个人信息 subscriber personal information of Internet of vehicle information service

车联网产业相关的汽车厂商、零部件和元器件提供商、软件提供商、数据和内容提供商和服务提供商在提供服务过程中收集的能够单独或与其他信息结合识别用户和涉及用户个人隐私的信息。

注：用户个人信息经处理去除用户身份和个人隐私属性后，不纳入本标准规定的车联网信息服务用户个人信息保护范围。例如，车联网信息服务订阅业务的规模统计信息等。

4 用户个人信息保护基本原则

车联网信息服务用户个人信息保护，一般应按 GB/T 35273—2020 中的要求，遵循其权责一致、目的明确、选择同意、最少够用、公开透明、确保安全、主体参与这八大原则，合理的利用个人信息。

- 权责一致原则：采取技术和其他必要的措施保障个人信息的安全，对其个人信息处理活动对个人信息主体合法权益造成的损害承担责任。
- 目的明确原则——具有合法、正当、必要、明确的个人信息处理目的。

- 选择同意原则：向个人信息主体明示个人信息处理目的、方式、范围、规则等，征求其授权同意。
- 最少够用原则：只处理满足个人信息主体授权同意的目的所需的最少个人信息类型和数量。目的达成后，应及时删除个人信息。
- 公开透明原则：以明确、易懂和合理的方式公开处理个人信息的范围、目的、规则等，并接受外部监督。
- 确保安全原则：具备与所面临的安全风险相匹配的安全能力，并采取足够的管理措施和技术手段，保护个人信息的保密性、完整性、可用性。
- 主体参与原则：向个人信息主体提供能够查询、更正、删除其个人信息，以及撤回统一、注销账户、投诉等方法。

5 用户个人信息安全保护概述

5.1 用户个人信息保护对象

用户个人信息分级保护对象为特定的车联网信息服务，该服务包含用于车联网信息服务的智能网联汽车、车联网信息服务平台、车联网移动智能终端、路侧基础设施等相应设备、系统和平台的应用逻辑和业务流程。

5.2 用户个人信息处理环节

车联网信息服务活动过程中用户个人信息的处理过程可以分为收集、保存、使用，以及委托处理、共享、转让和公开披露等环节。对车联网信息服务用户个人信息的保护贯穿于以下四个环节中。

- 收集环节：是指在车联网信息服务活动过程中获得对用户个人信息的控制权的行为，包括由个人信息主体主动提供、通过与个人信息主体交互或记录个人信息主体行为等自动采集，以及通过共享、转让、搜集公开信息间接获取等方式。其中，车联网相关产品或服务的提供者提供工具供个人信息主体使用，提供者不对个人信息进行访问的，则不属于本标准所称的收集行为。例如，车载离线导航软件在车载终端获取用户位置信息后，如不回传至软件提供者，则不属于个人信息收集行为。
- 保存环节：是指对车联网信息服务活动中相关的用户个人信息进行传输、存储和去标识化处理等操作。
- 使用环节：是指将收集和存储的用户个人信息用于车联网信息服务活动，包括但不限于对个人信息的访问、展示、使用、基于不同业务所收集个人信息的汇聚融合、查询、更正、删除等操作。
- 委托处理、共享、转让和公开披露环节：委托处理是指在将车联网用户个人信息控制者委托第三方处理用户个人信息。共享是指用户个人信息控制者向其他控制者提供个人信息，且双方分别对个人信息拥有独立控制权的过程。转让是将个人信息控制权由一个控制者向另一个控制者转移的过程。公开披露是指将用户个人信息向社会或不特定人群发布信息的行为。

5.3 用户个人信息保护基本思路

本标准重点针对用户个人信息保护对象，开展用户个人信息的分类和分级，并围绕用户个人信息保

护的全生命周期各处理环节，提出相应的安全要求，以降低车联网信息服务中用户个人信息的全生命周期相关安全风险，保障车联网信息服务提供方应按照相应级别的管理要求及技术要求对其提供服务过程中涉及的用户个人信息的收集、保存、使用、委托处理、共享、转让和公开纰漏等工作流程进行规范化管理。

6 用户个人信息分类要求

6.1 用户个人信息分类方法

用户个人信息是指车联网信息服务如数据采集传输和使用销毁等过程中与用户密切相关的数据信息，这些数据信息能够一定程度上识别车联网用户个人身份或反映处用户个人活动情况。车联网信息服务用户个人信息细分为用户身份证明类信息、车联网信息服务用户数据和服务内容信息、用户服务相关信息三大类。

用户身份证明类信息：是指车联网信息服务活动过程中与用户自然人身份和标识信息、用户虚拟身份和鉴权信息密切相关的用户个人信息。

车联网信息服务用户数据和服务内容信息：主要指车联网信息服务过程中用户服务内容信息和用户资料信息。其中，用户服务内容信息包括驾驶及行车安全服务信息、生活服务信息、交通出行管理服务信息、交通出行管理服务信息、涉车服务信息、行业营运服务信息；用户资料信息涉及联系人信息、用户私有资料数据和信息服务内容衍生信息等。

用户服务相关信息：指车联网信息服务过程中用户服务使用信息、用户车辆基本标识信息和用户设备、系统和平台信息。

6.2 用户个人信息分类示例

为便于车联网信息服务用户个人信息保护等级划分，将上述用户个人信息分类进一步细化，表 1 给出了用户个人信息分类的具体描述和示例。

表 1 用户个人信息分类示例

用户个人信息类别		用户个人信息范围	用户个人信息示例
A: 用户身份证明类信息	A1: 用户自然身份和标识信息	A1-1: 用户基本资料	姓名、证件类型及号码、年龄、性别、职业、工作单位、地址、宗教信仰、民族、国籍、电话号码等
		A1-2: 用户身份证明	身份证件、军官证、护照、机动车驾驶证、社保卡等证件影印件
		A1-3: 用户生理标识	指纹、声纹、虹膜、脸谱等
	A2: 用户虚拟身份和鉴权信息	A2-1: 普通车联网信息服务身份标识和鉴权信息	电话号码、账号、邮箱地址、用户个人数字证书以及服务涉及的密码、口令、密码保护答案、解锁图案等
		A2-2: 车联网交易类信息服务身份标识和鉴权信息	各类交易账号和相应的密码、密码保护答案、解锁图案、系统或平台中登录的个人银行账号、交易验证码、动态口令、交易信息等

表 1 用户个人信息分类示例（续）

用户个人信息类别	用户个人信息范围	用户个人信息示例
B: 车联网信息服务内容类用户数据信息	B1: 用户服务内容信息	B1-1: 驾驶及行车安全服务类信息 智能辅助驾驶相关服务场景下的车辆驾驶行为、行经路线等信息；车联网在车辆防碰撞（如碰撞预警、紧急刹车预警、变道预警、车辆失控预警、异常车辆预警等）、车车编队辅助和防撞人或物等服务中相关的用户个人信息
		B1-2: 生活服务信息 车联网生活服务相关的内容信息，如个人数据文件、邮件服务、广播服务、网页浏览、购物、在线音乐和视频服务、天气预报及推送、社交服务、移动办公服务等用户个人信息
		B1-3: 交通出行管理服务信息 车联网在交通动态信息通知服务（如信号灯信息推送、红绿灯车速引导、闯红灯预警等信息）中相关的个人信息； 车联网在浮动车交通管理（如车辆信息动态交换采集、违法信息抓拍上报、停车诱导和管理、交通流量疏导、交通应急信息发布等）服务中相关的用户个人信息
		B1-4: 涉车服务信息 车联网在涉车服务（如 UBI 保险和交易、分时租赁和约车拼车、车辆检修保养救援）等相关的用户个人信息
		B1-5: 行业营运服务信息 车联网在行业营运服务中相关的内容信息（如公交、处在、物流、换位、港口、景区等运营车辆管理），如与车况和位置信息上报、远程控制、越界和超速预警、特定区域特定路线特定行业下自动驾驶等相关的用户个人信息
	B2: 用户资料信息	B2-1: 联系人信息 通信录、好友列表等用户资料数据； 车内蓝牙配对拷贝的联系人列表
		B2-2: 用户私有资料数据 用户云存储、终端、SD 卡等存储的用户文字、多媒体等资料数据信息
		B2-3: 信息服务内容衍生信息 基于定位及导航服务内容分析获取的车辆活动轨迹、精准定位信息、个人生活习惯、健康状况等资料信息
C: 用户服务相关信息	C1: 用户服务使用信息	C1-1: 业务订购、订阅关系 业务订购信息、业务注册时间、修改、注销状况信息等
		C1-2: 服务记录 车联网信息服务平台、智能网联汽车及车联网智能终端中存储或缓存的直接或间接产生的用户操作记录，如信息服务中心涉及的照片、音频、视频、通话记录等；浏览的新闻或购物浏览器访问的网址列表；娱乐软件记录、汽车远程操控指令记录、语音服务的系统备份信息、网页购物记录等

表1 用户个人信息分类示例（续）

用户个人信息类别		用户个人信息范围	用户个人信息示例
C: 用户服务相关信息	C1: 用户服务使用信息	C1-3: 日志	反映用户操作记录的如日志信息、日志文件等
		C1-4: 交易服务信息	交易信息、消费记录、流水记录等
	C2: 用户车辆基本标识信息	C2-1: 车辆基本资料	车辆类型、车辆品牌、车辆型号、车辆底盘型号、发动机号、燃油种类、车牌号、发动机号、车辆识别代码（VIN码）等
	C3: 用户设备、系统和平台信息	C3-1: 设备、系统或平台信息	硬件型号、唯一设备识别码 IMEI、设备/系统/平台 MAC 地址、SIM 卡 IMSI 信息等

7 用户个人信息敏感性分级要求

7.1 用户个人信息敏感性分级方法

综合考虑车联网信息服务中用户个人信息的敏感程度和在发生用户个人信息泄露或滥用等事件后对用户人身和财产等方面的危害程度进行敏感性分级。本标准将车联网信息服务用户个人信息划分为个人敏感信息、个人重要信息和个人一般信息。

个人敏感信息：是指在车联网信息服务过程中相关的用户个人信息，一旦被泄露、被非法提供或被滥用后会给用户人身和财产带来严重危害，极易导致个人名誉、身心健康受到损害或歧视性待遇等个人信息。如在发生用户个人信息泄露事件后，将导致个人信息主体及个人信息的收集或使用组织丧失对个人信息的控制能力，造成个人信息扩散范围和用途的不可控。且某些用户个人信息泄露后，被以违背个人信息主体意愿的方式直接使用或与其他信息进行关联分析，可能度个人信息主体权益带来重大风险。或在发生个人信息滥用时间后，某些个人信息在被超出授权合理界限时（如变更处理目的、扩大处理范围等），可能对个人信息主体权益带来重大风险。

个人重要信息：是指在车联网信息服务过程中相关的用户个人信息，在被泄露、被非法提供或被滥用后会给用户人身和财产带来较大危害，甚至一定程度上影响个人名誉和身心健康。

个人一般信息：是指在车联网信息服务过程中相关的用户个人信息，在被泄露、被非法提供或被滥用后会给用户带来一定危害，但相对影响范围和程度有限，不会对财产和人身安全构成危害。

7.2 用户个人信息敏感性分级示例

依据车联网信息服务用户个人信息分类和敏感性分级方法，表2给出了用户个人信息敏感性分级要素。

表2 用户个人信息敏感性分级要素

用户个人信息敏感性等级	用户个人信息敏感性等级要素
个人敏感信息	A1-2: 用户身份证明
	A1-3: 用户生理标识
	A2-2: 车联网交易类信息服务身份标识和鉴权信息

表 2 用户个人信息敏感性分级要素（续）

用户个人信息敏感性等级	用户个人信息敏感性等级要素
个人重要信息	A1-1: 用户基本资料
	A2-1: 普通车联网信息服务身份标识和鉴权信息
	B1-1: 驾驶及行车安全服务信息
	B1-2: 生活服务信息
	B1-3: 交通出行管理服务信息
	B1-4: 涉车服务信息
	B1-5: 行业运营服务信息
	B2-1: 联系人信息
	B2-2: 用户私有资料数据
	B2-3: 信息服务内容衍生信息
	C1-2: 服务记录
	C1-3: 日志
	C1-4: 交易服务信息
	C2-1: 车辆基本资料
	C3-1: 设备、系统或平台信息
个人一般信息	C1-1: 业务订购、订阅关系

8 用户个人信息安全保护要求

8.1 个人一般信息安全管理要求

个人一般信息安全管理基本要求：应实施基本的技术和管理措施确保车联网用户个人信息访问控制安全。例如，应针对用户个人信息采取必要的访问控制措施。

8.2 个人重要信息安全管理要求

个人重要信息安全管理基本要求：应实施必要的技术和管理措施，保护用户的知情权和选择权，保护用户个人信息的机密性和完整性，确保用户个人信息访问控制安全，建立用户个人信息安全管理规范。例如，在收集和转移用户个人信息时应征得用户同意，在信息的收集和转移的传输过程应采取必要的加密措施，保障数据的机密性和完整性，应对信息采取严格访问控制措施，应定义严格的用户个人信息各生命周期（包括信息收集、保存、使用、委托处理、共享、转让和公开披露等各个环节）安全管理规范，应设置内部的数据审批流程及制度。

8.3 个人敏感信息安全管理要求

个人敏感信息安全管理基本要求：应实施严格的技术和管理措施，保护用户的知情权和选择权，保护用户个人信息的机密性和完整性，确保车联网用户个人信息访问控制安全，建立严格的用户个人信息

安全管理规范以及数据实时监控机制。例如，在收集、转移和使用用户个人信息时应征得用户同意，在信息的存储以及收集和转移的传输过程中应使用高强度的加密措施，保障数据的机密性和完整性，应对信息采取严格访问控制措施，应定义严格的用户个人信息各生命周期（包括信息收集、保存、使用、委托处理、共享、转让和公开披露等各个环节）安全管理规范，应设置内部的数据审批流程及制度，并对用户个人信息的使用进行实时监控及预警。

参 考 文 献

- [1] GB/T 35274—2017 信息安全技术 大数据服务安全能力要求.
 - [2] YD/T 2781—2014 电信和互联网服务 用户个人信息保护 定义及分类.
 - [3] YD/T 2782—2014 电信和互联网服务 用户个人信息保护 分级指南.
-