ICS 35.040
L80

中华人民共和国国家标准

GB/T XXXXX—XXXX

信息安全技术
网络预约汽车服务数据安全指南

Information security technology—Guide for data security of Online Car-booking Services

（征求意见稿）

本稿完成时间：2020 年 10 月 30 日

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX-XX-XX 发布　　XXXX-XX-XX 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。

本文件由全国信息安全标准化技术委员会（SAC/TC260）提出并归口。

本文件起草单位：北京小桔科技有限公司、中国电子技术标准化研究院、中国网络安全审查技术与认证中心、北京信息安全测评中心、北京三快科技有限公司、北京百度网讯科技有限公司、北京易行出行旅游有限公司、北京假日阳光环球旅行社有限公司、广州祺宸科技有限公司、上海赛可出行科技服务有限公司、艺龙网信息技术（北京）有限公司、红旗智行科技（北京）有限公司、国家计算机网络应急技术处理协调中心、中电长城网际安全技术研究院(北京)有限公司、公安部第三研究所、中国信息通信研究院、中国科学院信息工程研究所、重庆邮电大学、北京市竞天公诚律师事务所上海分所等。

本文件主要起草人：孙铁、胡影、闵京华、陈舒、张娜、房子成、许锐、许静慧、李媛、刘笑岑、宋子奕、徐彩曦、刘华、常博厚、叶俊、刘君、张知行、王文磊、唐迪、戚琳、韩东旭、徐雨晴、袁立志等。

信息安全技术　网络预约汽车服务数据安全指南

1　范围

本文件给出了网络预约汽车服务运营者开展服务时数据收集、存储、使用、共享、公开披露、删除的数据类型、范围、方式和条件，以及数据安全管理要求。

本文件适用于网络预约汽车服务运营者加强数据安全保护，也适用于国家主管部门、第三方评估机构等对网络预约汽车服务数据活动进行监督、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 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

GB/T AAAAA　信息安全技术　移动互联网应用程序（App）收集个人信息基本规范

GB/T BBBBB　信息安全技术　网络数据处理安全规范

GB/T CCCCC　信息安全技术　个人信息收集告知同意指南

3　术语和定义

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

3.1

网络预约汽车服务数据　online car-booking service data

任何以电子或者非电子形式对网络预约出租汽车（简称“网约车”）服务和网络预约巡游出租汽车（简称“出租车”）服务产生的信息的记录。包括乘客数据、驾驶员数据、车辆数据及服务过程中产生和收集的其他数据。

3.2

企业订单　enterprise order

乘客所属企业与网络预约汽车服务运营者建立合作关系，乘客在所属企业设定的范围内产生的乘车费用由所属企业承担的订单。

3.3

行程录音录像　trip audio and video

在网络预约汽车服务过程中，通过车载设备或者驾驶员App收集的车内录音录像数据及其衍生数据。

注：衍生数据包括从视频中抽取的音频和图像等。

3.4

用户 user

使用网络预约汽车服务的个人，通常包括乘客和驾驶员。乘客包括叫车人和实际乘车人。

4 缩略语

以下缩略语适用于本文本：

App 移动互联网应用程序（mobile Internet application）

5 概述

5.1 总则

网络预约汽车服务的个人信息保护按照 GB/T 35273 的规定执行，数据安全保护按照 GB/T BBBBB 的规定执行。

5.2 网络预约汽车服务组成

网络预约汽车服务仅包括网络预约出租汽车（简称“网约车”）服务和网络预约巡游出租汽车（简称“出租车”）服务。网络预约汽车服务的参与相关方包括用户、运营者和第三方。

5.3 网络预约汽车服务数据活动

一次完整的网络预约汽车服务活动，主要包括乘客和驾驶员注册、网络预约汽车服务运营者对驾驶员资质审核、乘客发单、订单匹配、驾驶员接单、行程服务、网络预约汽车服务运营者对安全秩序的维护、支付收款、用户评价等。

网络预约汽车服务的数据活动及其角色和功能如图 1 所示。

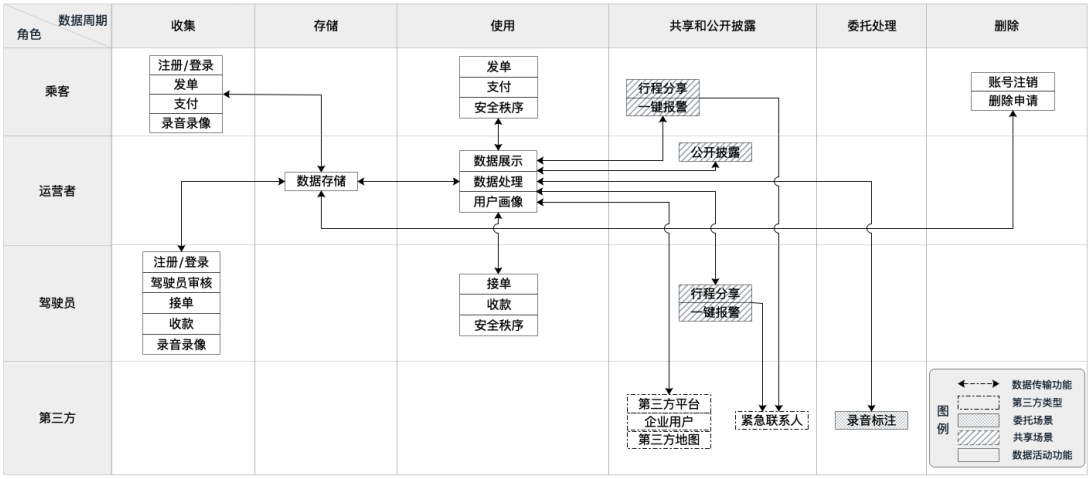

图1 网络预约汽车服务数据活动及其角色和功能

5.4 网络预约汽车服务数据安全风险

网络预约汽车服务数据主要面临如下安全风险：

a) 在数据收集活动中，网络预约汽车服务运营者过度收集乘客和驾驶员的个人信息或者过度索取移动智能终端操作系统权限的风险；

b) 在数据传输、存储和使用活动中，网络预约汽车服务运营者未采取充分安全保护措施，如因链路监听、攻击拖库和权限不当等带来的数据泄露或滥用风险；
c) 在数据共享和公开披露活动中，网络预约汽车服务运营者未经用户同意或者超出必要限度与第三方共享数据或对外公开披露数据的风险。

5.5 网络预约汽车服务数据分类分级

网络预约汽车服务数据类别包括个人信息、车辆行驶数据、统计数据和匿名化数据，依据数据的敏感程度、重要性、保护要求以及一旦泄露、丢失、破坏造成的危害程度等因素分为4个等级，详见附录A。

6 数据收集

6.1 数据收集通用要求

数据收集的通用要求包括：
a) 网络预约汽车服务运营者在收集用户个人信息前，应告知用户并征得用户同意；
b) 用户拒绝提供网络预约汽车服务最小必要个人信息以外的个人信息时，网络预约汽车服务运营者不应拒绝提供网络预约汽车服务；
c) 用户拒绝提供网络预约汽车服务可选业务功能对应的最小必要个人信息时，网络预约汽车服务运营者可拒绝提供对应可选业务功能服务，但不应拒绝提供网络预约汽车服务。

6.2 网络预约汽车服务最小必要个人信息

6.2.1 乘客最小必要个人信息

网络预约汽车服务通过App收集的乘客最小必要个人信息按照GB/T AAAAA附录A.2的规定执行；网络预约汽车安装有车载设备的，收集的个人信息包括行程录音录像。

注：网络预约汽车服务接入到第三方平台时，乘客通过第三方平台提供的服务发单的，乘客个人信息的收集要求适用于第三方平台。

6.2.2 驾驶员最小必要个人信息

网络预约汽车服务运营者收集的驾驶员最小必要个人信息范围见表1。

表1 驾驶员必要个人信息

业务功能	最小必要信息	收集目的及使用要求
用户注册	手机号码	用于标识驾驶员用户和保障账号信息安全
	账号信息：账号、口令	
背景审核	身份证或者其他身份证明	用于审核是否符合法律法规规定的驾驶员资格
	面部识别特征	
	车辆信息：车辆号牌、车身颜色、品牌型号、车辆识别代号	
	驾驶证	
	行驶证	

表1 （续）

业务功能	最小必要信息	收集目的及使用要求
背景审核	车辆保险	用于审核是否符合法律法规规定的驾驶员资格
	信用记录	
	是否有相关犯罪记录	
	网络预约出租汽车驾驶员证（仅网约车收集）	
	网络预约出租汽车运输证（仅网约车收集）	
	车辆监督卡（仅出租车收集）	
接单并运送乘客	位置信息	用于确定用户当前位置，匹配订单。
	行程轨迹	记录驾驶员服务行为，用于核实服务过程、解决司乘纠纷。
	订单信息：出发地、目的地、订单时间、订单里程、订单金额	
	日志信息	
安全秩序	录音录像	用于核实处理涉及用户重要人身财产安全的订单纠纷，预防订单中违法犯罪行为的发生。
	驾驶行为信息	用于加强对驾驶员的驾驶行为监督，提升出行安全
收款	使用何种方式支付	用于用户使用第三方支付方式对约车订单收款
	银行卡号	用于驾驶员提现
风险控制	通讯设备信息	用于防控运营风险

6.3 网络预约汽车服务可选业务功能的最小必要个人信息

在网络预约汽车服务过程中，网络预约汽车服务运营者会提供一些允许用户自主选择是否使用的业务功能。本文件列举了网络预约汽车服务中典型可选业务功能，以及这些业务功能对应收集的最小必要个人信息，典型可选业务功能及对应收集的最小必要个人信息范围见附录B。

6.4 网络预约汽车服务最小必要系统权限

网络预约汽车服务最小必要系统权限要求包括：

a) 为保证服务正常开展，乘客App需向乘客申请移动终端操作系统位置信息权限，采集位置信息频率每秒不应超过一次；

b) 为保证服务正常开展，驾驶员App需向驾驶员申请移动终端操作系统位置信息、麦克风和相机权限，采集位置信息频率每秒不应超过一次。

6.5 告知同意

6.5.1 叫车人告知同意

叫车人告知同意按照GB/T CCCCC的规定执行。

6.5.2 代叫车告知同意

代叫车告知同意要求包括：

a) 用户通过代叫车功能为他人代叫车的，网络预约汽车服务运营者应提示叫车人收集使用实际乘车人个人信息的情况，并取得代叫车人已告知并征得实际乘车人同意的确认；

b) 收集录音录像信息的，网络预约汽车服务运营者应通过短信、车内语音播报或其他方式告知实际乘车人录音录像收集情况。

6.5.3 同乘人告知同意

乘客叫车后，有同行人共同乘车的，叫车人宜告知同乘人网络预约汽车服务运营者收集使用个人信息的情况，并征得同乘人的同意。

6.5.4 录音录像信息收集的告知同意

网络预约汽车服务运营者收集行程录音录像信息时，应当制定单独录音录像信息收集协议，向用户告知录音录像信息收集方式、时间、使用用途、存储规则等内容，行程录音录像信息收集协议应征得乘客和驾驶员双方的同意，录音信息收集协议范式模板见附录C。

6.5.5 使用目的变更告知同意

使用目的变更告知同意要求包括：

a) 网络预约汽车服务运营者变更个人信息使用目的，将网络预约汽车服务运营者收集、产生的个人信息用于其他业务类型，应在变更前告知用户变更使用目的的个人信息类型、变更后的使用目的，征得用户明示同意；

b) 网络预约汽车服务运营者对用户使用网络预约汽车过程中的违规行为、纠纷记录等进行加工处理，将分析结果用于其他业务类型的风险控制前，应告知用户。

7 数据存储

数据传输和存储安全要求包括：

a) 网络预约汽车服务运营者通过互联网传输个人信息时，应采用加密等安全措施；

b) 网络预约汽车服务运营者应将乘客和驾驶员的个人身份信息、面部识别特征和行程录音录像数据分开存储；

c) 网络预约汽车服务运营者不宜将行程轨迹和行程录音录像数据存储在办公终端中，宜在有安全防护措施的服务器端存储。

注：采用密码技术时宜遵循密码管理相关国家标准。

8 数据使用

8.1 数据访问控制措施

数据访问控制措施要求包括：

a) 网络预约汽车服务运营者宜采取数据分级策略，将数据分级与数据访问权限进行关联标识，访问权限应明确数据查询、更正、删除、下载等操作，定义不同级别数据访问和访问权限申请审批流程；

b) 网络预约汽车服务运营者应对访问乘客和驾驶员个人信息的权限进行控制。不为投诉处理人员配置非需求触发访问乘客和驾驶员订单信息的权限，投诉处理场景数据使用安全保护要求见附录D。

8.2 个人信息的展示

个人信息展示要求包括：

a) 订单匹配后，网络预约汽车服务运营者向乘客和驾驶员展示对方个人信息用于身份核验时，所展示的个人信息应以满足核验需求为限，可向乘客展示的驾驶员信息包括驾驶员姓氏、头像、实时位置、车辆信息、评价信息，向驾驶员展示的乘客信息包括乘客手机号码最后四位、评价信息；

b) 网络预约汽车服务运营者通过界面展示乘客和驾驶员个人信息的（如显示屏幕），应对需展示的个人信息采取去标识化处理，为去标识化信息提供查看完整信息功能的，应对查看行为留存审计日志，去标识化规则见附录E；

c) 乘客和驾驶员使用行程分享功能将其行程分享给亲友时，向亲友分享的信息包括分享人手机号码、驾驶员姓氏、驾驶员头像、出发地、目的地、实时位置和车辆信息；

d) 订单匹配后，网络预约汽车服务运营者为乘客和驾驶员提供电话沟通渠道时，应使用虚拟号码；

e) 订单完成后，网络预约汽车服务运营者为用户保留纠纷处理的联系通道（例如物品遗失沟通）时，应使用虚拟号码；

f) 驾驶员可以选单的业务类型，应对用户评价内容进行限制，不应用户发布与网络预约汽车服务无关的评价内容；

g) 网络预约汽车服务运营者向乘客、驾驶员展示对方给出的评价内容时，应延时、匿名提供。

8.3 用户画像的使用

用户画像的使用要求包括：

a) 网络预约汽车服务运营者根据用户性别、年龄、饮酒情况或者其他信息进行用户画像，制定派单策略时，应以保护乘客和驾驶员人身和财产安全为原则，尊重用户合法权利；

b) 网络预约汽车服务运营者不应滥用大数据分析等技术手段，基于用户消费记录、消费偏好等设置不公平的交易条件，侵犯用户合法权益。

8.4 驾驶员信用记录的使用

a) 网络预约汽车服务运营者建立驾驶员信用记录用于管理驾驶员的，驾驶员注销账号后，对于驾驶员在服务过程中产生的违反法律法规、违反平台规则的信用记录，以及低于初始分的信用记录，网络预约汽车服务运营者可以持续保存；

b) 驾驶员注销账号后重新注册的，对于驾驶员在服务过程中产生的违反法律法规、违反平台规则的信用记录，以及低于初始分的信用记录，网络预约汽车服务运营者可以恢复。

9 数据的共享、公开披露

9.1 数据共享

9.1.1 数据共享通用要求

数据共享通用要求包括：

a) 网络预约汽车服务运营者与第三方数据共享按照GB/T BBBBB的5.10规定执行；

b) 不应向无业务需要的第三方共享网络预约汽车服务数据。

9.1.2 紧急情况数据共享

紧急情况数据共享要求包括：

a) 用户设置的紧急联系人或者其他亲友以用户人身安全存在重大风险为由，要求查询用户的行程信息和位置信息的，网络预约汽车服务运营者的工作人员应先尝试拨打用户联系电话，在无法联系到用户的紧急情况下，可以向进线人提供相应的行程信息和位置信息。如联系到用户，则应依照用户要求进行处理；

b) 网络预约汽车服务运营者宜为用户提供开启或者关闭紧急联系人查询信息授权的功能。用户事先开启紧急联系人查询用户个人信息授权的，紧急联系人要求获取用户个人信息时，网络预约汽车服务运营者可以直接提供；

c) 在用户使用一键报警或者其他紧急情况下，网络预约汽车服务运营者可以向用户设置的紧急联系人共享其行程信息、位置信息和报警情况。

9.1.3 企业订单数据共享

企业订单数据共享要求包括：

a) 网络预约汽车服务运营者应与企业用户约定企业订单中乘客个人信息的共享规则，在征得乘客明示同意后，可向乘客所属企业共享的个人信息包括：乘客姓名、乘客手机号码、出发地、目的地和支付信息；

b) 乘客在企业订单过程中发生安全事件，人身财产安全受到损害或者威胁的，乘客所属企业向网络预约汽车服务运营者索要乘客行程中安全事件信息的，可以予以提供。

9.1.4 第三方地图数据共享

网络预约汽车服务接入第三方地图服务，为乘客和驾驶员提供路径规划、导航服务时，在征得乘客明示同意后，可共享通讯设备信息、实时位置和路线规划信息，不应共享乘客或驾驶员的手机号码及身份信息。

9.1.5 第三方平台数据共享

网络预约汽车服务接入到第三方平台时，乘客通过第三方平台提供的服务发单的，网络预约汽车服务运营者与第三方平台应约定在服务中共享的个人信息类型，不应超出约定范围共享个人信息。在征得乘客和驾驶员明示同意后，第三方平台数据共享要求包括：

a) 订单匹配后，第三方平台可向网络预约汽车服务运营者共享乘客的用户标识符、手机号码、发单城市、出发地、目的地和通讯设备信息；

b) 订单匹配后，网络预约汽车服务运营者可向第三方平台共享驾驶员的用户标识符、手机号码、姓氏、实时位置、完成订单量、车辆信息和评价信息；

c) 网络预约汽车服务运营者和第三方平台作为支付渠道的一方可向另一方共享乘客支付信息；

d) 乘客申请发票时，第三方平台可向网络预约汽车服务运营者共享电子发票投递所需的电子邮箱或纸质发票邮寄所需的收件人信息；
e) 处理乘客或者驾驶员投诉时，网络预约汽车服务运营者和第三方平台可共享必要的乘客和驾驶员的身份信息及投诉记录信息。

9.2 违法违规信息的公开披露

网络预约汽车服务运营者公开披露违法违规信息时，应对乘客或者驾驶员的身份信息进行去标识化处理，去标识化规则见附录B。

10 典型场景数据安全保护措施

10.1 行程录音录像数据安全通用要求

行程录音录像数据是网络预约汽车服务中敏感的个人信息，网络预约汽车服务运营者应制定行程录音录像数据安全管理规范重点保护，明确行程录音录像数据生命周期中收集、传输、存储、使用、披露和销毁等环节的安全控制措施。行程录音录像数据安全管理范式模板见附录F。

10.2 行程录音录像的收集

对网络预约汽车服务运营者行程录音录像的收集要求包括：

a) 行程录音通过驾驶员App或车载设备收集，行程录像通过车载设备收集，宜优先使用车载设备收集录音；
b) 驾驶员App生成的行程录音文件应在上传完成后删除，不应在移动终端留存；
c) 车载设备应采取必要的安全防护，防范非授权访问，禁用或屏蔽调试接口，防范物理接口分析入侵。

10.3 行程录音录像的存储

对网络预约汽车服务运营者行程录音录像的存储要求包括：

a) 收集的行程录音录像数据存储时间不宜超过7天，当乘客或驾驶员有尚未解决完毕的纠纷时，对应的行程录音录像数据可以适当延长保存期限，在纠纷处理完毕且超过约定存储时限的应删除；
b) 宜为乘客和驾驶员提供已完成订单的行程录音录像删除服务，对无纠纷和投诉等需求的订单行程录音录像删除申请在取得乘客和驾驶员确认后予以处理。

10.4 行程录音录像的使用

对网络预约汽车服务运营者行程录音录像的使用要求包括：

a) 网络预约汽车服务运营者应与用户明确约定行程录音录像的使用用途，并严格按照约定用途使用行程录音录像，不应超出约定用途使用行程录音录像；
b) 应对行程录音采取技术措施使录音可识别录音内容但无法识别用户身份，如对音频信息的基频进行改变等；
c) 应对行程录像采取技术措施对乘客和驾驶员面部识别特征模糊化处理，如采取检测技术在视频中定位乘客面部位置，对面部识别特征遮挡处理等。

注：当投诉处理必须要使用行程录音录像中用原始音频基频和面部识别特征时，可不采取音频基频改变和面部识别特征遮挡等处理措施。

10.5 行程录音录像的共享

对网络预约汽车服务运营者行程录音录像的共享要求包括：

a) 除依据法律法规规定或经用户明示同意，网络预约汽车服务运营者不应向第三方共享行程录音录像；

b) 网络预约汽车服务运营者在向第三方共享行程录音录像时，应经过审批，并采用加密等保护措施；

c) 网络预约汽车服务运营者宜配备专用终端设备用于行程录音录像数据的共享输出，并留存记录。

注:采用密码技术时宜遵循密码管理相关国家标准。

10.6 行程录音的委托处理

对网络预约汽车服务运营者行程录音的委托标注处理要求包括：

a) 委托行为用于提升录音准确识别能力增强行程安全风险处置水平；

b) 委托行为不应超出已征得用户授权同意的使用范围；

c) 应对委托行为进行个人信息安全影响评估，经评估风险可控后进行委托行为；

d) 将行程录音提供给受委托方前，应采取以下保护措施：

1) 向受委托方提供行程录音时，不应提供行程录音所属用户的个人身份信息；

2) 在满足处理需求的前提下，筛选并删除行程录音中描述个人身份信息的内容；

3) 将行程录音分割为最小听音分片并打散，使之无法重新组装还原为原始文件；

4) 将行程录音切片随机分发给不同的标注人员，避免切片还原为原始文件；

5) 仅允许标注人员通过流式播放听音，通过技术措施防范行程录音被下载。

e) 应对受委托方进行监督，方式包括但不限于：

1) 通过合同等方式规定受委托方的责任和义务；

2) 发现受委托方未充分履行安全责任和义务时，及时停止委托行为，并要求受委托方删除行程录音。

附 录 A
（资料性）
网络预约汽车服务数据分类分级

A.1 网络预约汽车服务数据类别范围

网络预约汽车服务数据包括个人信息、车辆行驶数据、统计数据和匿名化数据。具体数据类别范围如下：

a) 个人信息，网络预约汽车服务运营者在网络预约汽车服务过程中收集使用的个人信息，个人信息详细分类参照GB/T 35273附录A；
b) 车辆行驶数据，网络预约汽车服务运营者在网络预约汽车服务过程中收集的与车辆行驶有关的数据，包括车辆行驶速度、违章处罚情况等；
c) 统计数据，网络预约汽车服务运营者对收集的个人信息、车辆行驶数据等进行统计分析后得出的汇总数据，包括用户数、订单量和里程总数等；
d) 匿名化数据，网络预约汽车服务运营者对收集的个人信息进行匿名化处理后得出的数据，包括匿名化后的订单信息、行驶轨迹等。

A.2 网络预约汽车服务数据分级

网络预约汽车服务运营者宜对数据进行分级标识或列出清单，数据分级应综合考虑数据的敏感程度、重要性、保护要求以及一旦泄露、丢失、破坏造成的危害程度等因素；对行踪轨迹、面部识别特征、行程录音录像等敏感数据应在在数据分级中从高考虑。根据数据重要程度、敏感度和泄露后带来的危害宜将数据划分为以下4级：

a) 第1级：可完全公开使用的数据。包括可以通过公开途径获取的数据，例如网络预约汽车服务运营者通过官网、公众号等公开渠道发布的统计数据等。
b) 第2级：可在较大范围内供访问使用的数据。例如不能标识个人身份的数据，在履行必要申请审批后用于统计分析。
c) 第3级：在较小范围内供访问使用的数据，如果未经授权披露，可能会对数据主体造成较高程度的损害。例如可以直接标识个人身份的数据，限于履行工作岗位职责的人员访问使用。
d) 第4级：仅在极小范围内且在严格限制条件下供访问使用的数据，如果未经授权披露，可能会对数据主体造成严重程度的损害。例如行程录音录像，当发生投诉时才能授权访问查询。

附 录 B
（规范性）
典型可选业务功能及对应收集的最小必要个人信息

表B.1给出了乘客App典型可选业务功能及对应收集的最小必要个人信息。

表B.1 乘客 App 典型可选业务功能及对应收集的最小必要个人信息

典型可选业务功能	对应收集的最小必要个人信息	收集目的及使用要求
代叫车	实际乘车人姓名、电话号码	用于驾驶员联系实际乘车人，接实际乘车人上车
添加紧急联系人	紧急联系人姓名、电话号码	当乘客使用一键报警功能或者遇到其他紧急情况时，用于将相应情况通知紧急联系人。
添加常用地址	家的地址、公司地址	用于乘客更快捷输入订单出发地、目的地
在线沟通	虚拟号码通话录音、在线沟通内容记录	用于核实事实，处理用户纠纷
评价	评价内容	用于解决纠纷，建立用户信用评价机制
客服	乘客与投诉处理人员的沟通内容	用于记录纠纷处理情况
开具发票	发票信息、纸质发票收集收件人信息、电子发票收集电子邮箱	用于开具发票

表B.2给出了驾驶员App典型可选业务功能及对应收集的最小必要个人信息。

表B.2 驾驶员 App 典型可选业务功能及对应收集的最小必要个人信息

典型可选业务功能	对应收集的最小必要个人信息	收集目的及使用要求
添加紧急联系人	紧急联系人姓名、电话号码	当驾驶员使用一键报警功能或者遇到其他紧急情况时，网络预约汽车服务运营者将相应情况通知紧急联系人
在线沟通	虚拟号码通话录音、在线沟通内容记录	用于核实事实，处理用户纠纷
评价	评价内容	用于解决纠纷，建立用户信用评价机制
客服	驾驶员与投诉处理人员的沟通内容	用于记录纠纷处理情况

注 1：用户拒绝提供可选业务功能及对应最小必要个人信息的，只影响用户使用相应的可选业务功能，不应影响用户使用其他业务功能。

注 2：可选业务功能收集最小必要个人信息以外的个人信息，应允许用户自主选择是否提供。用户拒绝提供的，不影响用户使用可选业务功能。

注 3：网络预约汽车服务运营者通过调用通讯录收集紧急联系人姓名、电话号码的，应允许用户拒绝开启通讯录权限，以手动输入紧急联系人姓名、电话号码。

注 4：本附录仅列举了较为典型的网络预约汽车服务乘客 App 及驾驶员 App 的可选业务功能，各网络预约汽车服务乘客 App 及驾驶员 APP 提供的可选业务功能可能会有所差别，本表格未予明确的可选业务功能，可以根据需要实现的服务目的判断其最小必要个人信息范围。

附 录 C
（资料性）
行程录音收集协议范式模板

为提升XXXX服务产品安全能力、更好地处理XXXX服务的司乘纠纷，XXXX服务上线录音功能。本协议将向您说明XXXX服务收集使用录音信息的情况，请您务必认真阅读本协议，在确认充分了解后慎重决定是否同意本协议。您点击同意后，本协议生效，对您及XXXX均具有法律约束力。

1.您同意本协议后，使用XXXX服务时，XXXX将通过软件或硬件设备录取您后续全部行程中的车内环境声音信息（包括您及车上人员交谈或肢体动作产生的声音），且后续行程不再做单独提示。受技术条件影响，XXXX各项服务在不同城市上线录音功能的时间不同，具体以XXXX显示的录音状态为准。

2.录音将通过XXXX驾驶员App或其他具备录音功能的软件或硬件进行。录音仅在驾驶员、乘客均同意的情况下开启。如乘客使用的App版本未及时更新，无法对录音进行授权，则录音不开启。

3.录音起始时间：

a)录音自订单行程开始时起（预约订单自驾驶员到达乘客出发地时起），至行程结束后适当时间停止（具体以驾驶员App显示的录音状态为准）。乘客自进入车辆后至离开车辆时，将同时被采集录音信息；

b)其他上线录音功能的服务的录音起始时间以XXXXApp另行告知为准。

4.如您是代他人叫车，在代叫车前请务必告知被代叫车人行程内录音信息收集情况，并征得被代叫车人同意后，方可为其叫车。

5.为保障用户的隐私，录音将实时上传至XXXX服务器，用户无法自行下载、调取或播放录音。

6.录音信息将用于以下明确列明的使用场景：

a)作为服务运营者处理用户纠纷的依据；

b)为维护用户人身安全等重大合法利益，或情况紧急又很难得到用户同意的；

c)用于抽查检测用户是否存在违反平台用户规则的行为；

d)用于系统分析，设计、开发、应用保护用户安全的辅助工具或产品。

7. XXXX将严格保护用户个人信息安全，除以下情况外，我们不会向其他人共享您的录音信息：

a)相关机关依据法定程序调取；

b)用户持法律文件依法调取。

8.录音保存期限为7日。如遇差评、投诉、尚未处理完毕的纠纷等，将适当延长录音保存期限。

9.用户使用的手机等硬件设备故障、网络状态不稳定、App版本过旧以及不可抗力等因素均可能导致录音失败，您对此表示理解，如遇此类问题，XXXX不需承担责任。

10.XXXX将严格按照本协议约定收集使用用户录音信息。本协议对相关内容未作明确约定的，以XXXX《个人信息保护及隐私政策》约定为准。

附 录 D
（规范性）
投诉处理场景数据安全保护要求

D.1 人员安全管理

对网络预约汽车服务运营者投诉处理人员安全管理要求包括：

a) 在投诉处理人员上岗前签署保密协议，声明对用户个人信息保护相关要求；
b) 对投诉处理人员开展必要的安全培训，培训内容包括但不限于：网络安全法律法规、社会工程学、网络安全管理制度，通过考核方可上岗；
c) 对投诉处理系统访问权限执行严格的申请审批控制，仅对履行投诉处理服务岗位职责的人员开放权限，在投诉处理人员工作岗位调整或离职时，及时关闭撤销所拥有的系统权限。

D.2 账号安全管理

对网络预约汽车服务运营者投诉处理系统账户安全管理要求包括：

a) 定义并维护投诉处理系统人员账号信息，对投诉处理人员岗位职责、角色和业务类型进行定义说明，对不同岗位、角色、业务类型投诉处理人员数据访问范围进行限定；
b) 采取多因素身份验证措施，防止身份冒用和账号共享，同一投诉处理人员不能在不同终端上同时登录，对投诉处理人员登录投诉处理系统网络地址进行限定。

D.3 工单有效期限制

网络预约汽车服务运营者根据业务需要限定已处理完成的投诉工单有效期，及时关闭投诉处理人员已处理完成订单数据的权限。

D.4 数据防泄漏

网络预约汽车服务运营者投诉处理系统应采取页面安全水印技术，对投诉处理人员的操作行为进行监控，防止系统数据泄露。

D.5 安全审计

网络预约汽车服务运营者应部署自动化审计系统，收集、记录和监测个人信息查询、更正、删除及下载等处理活动，包括但不限于以下内容：

a) 审计日志内容包括：账号、网络地址、操作时间、操作行为、操作结果等；
b) 根据审计数据进行统计分析，支持生成审计报表；
c) 根据审计数据分析挖掘个人信息违规查询、违规下载、违规外发等异常行为，并通过实时告警通知安全管理人员进行处置。

注：网约预约汽车服务运营者其他业务场景下的人员安全管理、账号安全管理、数据防泄漏和安全审计等数据安全保护措施参照投诉处理场景相关要求执行。

附 录 E
（资料性）
网络预约汽车服务数据去标识化规则

表E.1给出了网络预约汽车服务数据去标识化规则。

表E.1 网络预约汽车服务数据去标识化规则

序号	数据类型	去标识化规则	备注
1	姓名	展示第一个字，后面都隐藏。如：张*	
2	手机号码	显示前 3 位，后 4 位，中间隐藏。如：188****8888	
3	固定电话号码	显示前 3 位，后 4 位，中间隐藏。如：010****8888	
4	地址信息	显示省/市/县区信息，街道地址隐藏。如：山东省青岛市市南区**街道**	
5	坐标信息	显示前 3 位，后 3 位隐藏。如：经度 113.***、纬度 22.4***	在 App 中可对乘客和驾驶员展示未脱敏位置信息
6	车辆号牌	显示前 3 位和最后 1 位，中间 3 位隐藏。如：京A8***8	
7	发动机号码	显示前 3 位和最后 2 位，中间 2 位隐藏。如：888**8K	
8	车辆识别代号	显示前 13 位和最后 1 位，中间 3 位隐藏。如 LSGJR88U88K88***8	
9	身份证号	显示前 3 位，后 2 位，中间隐藏，如：110**********33	

附 录 F
（资料性）
行程录音录像数据安全管理范式模板

行程录音录像安全管理范式模板包括行程录音录像保护的目的、范围、依据、术语定义、安全要求、处罚措施和维护更新等内容。

表F.1给出了行程录音录像数据安全管理范式模板。

表F.1 行程录音录像数据安全管理范式模板

行程录音录像数据安全管理范式模版	编写要求
1、目的 ● 行程录音录像数据为敏感个人信息，应采用安全管理和技术措施进行重点保护。 ● 为了保护行程录音录像数据，降低信息资产被泄露或破坏的风险，特制定本规范，保证用户个人信息不受侵害。 ……	说明本规范的制定的目的
2、适用范围 ● 本规范适用于任何与行程录音录像数据有关的行为，包括行程录音录像数据生命周期中的收集、传输、存储、使用、披露、销毁等环节的安全控制。 ……	说明本规范的适用范围或适用场景
3、规范依据 ● 《中华人民共和国网络安全法》 ● 《信息安全技术 个人信息安全规范》(GB/T35273—2020) ……	列举本规范制定时依据的国家法律法规
4、术语定义 ● 网络预约汽车服务过程中，通过车载录像设备收集的行程录音录像数据或者通过App收集的行程录音数据，及其衍生数据。 ● 安全区域：为满足查询行程录音录像信息安全要求设立的物理封闭区域（例如某层楼或某房间）称为安全区域。 ……	对本规范中出现的名词术语进行定义说明
5、行程录音录像数据安全要求 本要求围绕行程录音录像数据的生命周期各环节提出，根据此要求执行行程录音录像数据安全工作。在不违反以下原则的情况下，可以根据业务场景进行安全要求的细化。 **（1）行程录音录像数据收集** a) 采集行程录音录像数据必须通过乘客同意； b) 行程录音录像数据自产生之时起需全程加密。加密要求如下： 密码算法…… 秘钥长度…… c) 不得留存未加密行程录音录像数据； …… **（2）行程录音录像数据传输** 在传输行程录音录像数据时，应遵守以下安全要求： a) 在进行行程录音录像传输时，链路应加密； b) 禁止使用第三方网盘、即时聊天工具等方式传输行程录音录像数据； ……	详细说明行程录音录像数据在收集、传输、存储、使用、披露及删除销毁环节应采取的安全措施。

表F.1　（续）

行程录音录像数据安全管理范式模版	编写要求
（3）行程录音录像数据存储 线上存储应符合以下要求： a) 行程中录音录像文件应加密存储在独立的存储集群； b) 严格控制存储集群访问权限，必须获得相应的授权后才可以访问； …… 线下存储应符合以下要求： c) 保存行程录音录像数据的介质（例如纸质文件、光盘等）应当保存在有锁的柜子中或独立的封闭区域（如档案室等），并留存使用记录； …… **（4）行程录音录像数据使用** a) 使用行程录音录像数据必须经过审批； b) 行程录音录像应接入水印标识； c) 必须在安全区域内访问行程录音录像数据； d) 禁止利用右键、下载工具等方法下载行程录音录像数据； e) 访问行程录音录像数据的人员必须签署保密协议，并向访问人员提供回执确认； f) 除法律规定的情形外，行程录音录像数据不得向第三方提供，对第三方提供前必须经过XXXX审批； …… **（5）行程录音录像数据披露** a) 不得擅自通过各种媒介对外披露（包括但不限于亲友、客户及第三方合作方）披露工作中接触到行程录音录像数据； b) 对外披露行程录音录像数据必须经过XXX部门审批； …… **（6）行程录音录像数据删除销毁** a) 行程录音录像保存的期限：默认存储X天，有差评投诉保存X天，有重大投诉保存至投诉工单关闭； b) 行程录音录像数据在使用完毕后应进行删除； c) 包含行程录音录像数据的纸质文件应通过碎纸机销毁； ……	
6、安全区域及终端安全要求 **（1）安全区域物理安全要求** 行程录音录像的查询使用在封闭的安全区域内完成，安全区域应至少采取以下安全保护措施： a) 安全区域出入口安排专人值守并配置电子门禁系统，控制、鉴别和记录出入的人员； b) 安全区域与外部连接的通风口、窗户等通道部署防盗报警装置； c) 电子门禁系统与警报系统联动或具备警报功能，并采取指纹或人脸识别等技术进行身份核实防范身份冒用； d) 配置视频监控系统，对人员活动行为进行全方位监控； e) 对进入物理区域的人员随身携带的物品进行限制，禁止携带手机、相机、录音笔、优盘等电子设备； f) 配备专门的安全运营人员，对物理区域的运行进行安全审计，采取措施包括但不限于： 1) 根据物理区域安全管理要求监督进入员工行为，如身份核验、禁止携带物品的监督提醒； 2) 采取定时和不定时巡查，对发现的异常、告警和故障等及时记录并上报，采取必要的纠正措施； 3) 抽检视频监控和门禁记录，排查违规行为和安全隐患。 ……	详细说明安全区域及终端设备应采取的安全措施。

表F.1 （续）

行程录音录像数据安全管理范式模版	编写要求
（2）安全区域内终端设备安全要求 用于行程录音录像查询使用的终端设备采取必要的技术防护措施，包括但不限于： a) 网络准入控制：对终端设备进行身份认证、安全检查，非授权设备禁止访问行程录音和行程录像信息； b) 网络行为监控：对终端设备文件操作访问、上网行为、网络协议等进行管控和审计，禁止具备即时通讯、公有云存储等与录音录像无关的互联网应用，防止外发、泄露行程录音和行程录像信息泄露； c) 网络防病毒：及时更新系统补丁并采取恶意代码防护措施，防范病毒、木马、蠕虫、间谍软件等恶意程序传播感染； d) 端口管控：对终端设备的通用串行总线和蓝牙等外部连接进行管控，防范非法外联，设置专用听音设备，禁止随意插拔更换。 ……	
7、处罚措施 ● 明令禁止违反该制度规定的行为，具体的处罚措施包括： a) 通报批评：…… b) 警告：…… c) 解除劳动关系：…… d) 移交司法机关：…… …… ● 鼓励对违反本规范要求违规使用行程录音录像数据的行为进行检举。 ……	详细说明违反本规范对相关人员的处罚措施，可列举说明各类处罚条款。
8、维护更新 ● 本规范由……制定和解释。 ● 本规范自公布之日起施行，员工有义务及时阅读，了解行程录音录像数据安全要求，并遵照执行。 ……	

参 考 文 献

[1] GB/Z 28828—2012 信息安全技术 公共及商用服务信息系统个人信息保护指南

[2] 《中华人民共和国网络安全法》 2016 年 11 月 7 日第十二届全国人民代表大会常务委员会第二十四次会议通过

[3] 《全国人大常委会关于维护互联网安全的决定》 2000 年 12 月 28 日第九届全国人民代表大会常务委员会第十九次会议通过

[4] 《全国人大常委会关于加强网络信息保护的决定》 2012 年 12 月 28 日第十一届全国人民代表大会常务委员会第三十次会议通过

[5] 《中华人民共和国电子商务法》 2018 年 8 月 31 日第十三届全国人民代表大会常务委员会第五次会议通过

[6] 《电信和互联网用户个人信息保护规定》 2013 年 7 月 16 日中华人民共和国工业和信息化部令第 24 号公布，自 2013 年 9 月 1 日起施行

[7] 《移动互联网应用程序信息服务管理规定》2016 年 6 月 28 日国家互联网信息办公室发布，自 2016 年 8 月 1 日起实施

[8] 《网络交易管理办法》经中华人民共和国国家工商行政管理总局局务会审议通过，自 2014 年 3 月 15 日起施行

[9] 《网络预约出租汽车经营服务管理暂行办法》2016 年 7 月 14 日经交通运输部第 15 次部务会议通过，并经工业和信息化部、公安部、商务部、工商总局、质检总局、国家网信办同意，自 2016 年 11 月 1 日起施行

[10] 《中华人民共和国刑刑法修正案（七）》 2009 年 2 月 28 日第十一届全国人民代表大会常务委员会第七次会议通过

[11] 《中华人民共和国刑刑法修正案（九）》 2015 年 8 月 29 日第十二届全国人民代表大会常务委员会第十六次会议通过