ICS 03.220.20
CCS R85

DB3502

福 建 省 厦 门 市 地 方 标 准

DB 3520/T 046.4—2021

网约车运营服务管理 第4部分：信息安全

App-based ride-hailing operation service management—Part 4 :Information security

2021－10－22 发布　　2021－11－22 实施

厦门市市场监督管理局　　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。

本文件是DB3502/T 046《网约车运营服务管理》的第4部分。DB3502/T 046已经发布了以下部分：

——第1部分：运营条件；

——第2部分：服务规范；

——第3部分：运营管理；

——第4部分：信息安全。

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。

本文件由厦门市运输事业发展中心提出。

本文件由厦门市交通运输局归口。

本文件起草单位：厦门市运输事业发展中心、厦门市标准化研究院、厦门未来交通创新研究院、滴滴出行科技有限公司。

本文件主要起草人：王文杰、王文果、翁明鸿、林少雄、吴珊、沈群红、李钊茜、张晓阳、孙铁、刘浩、张旭。

本文件为首次发布。

引　言

推进网约车规范化运营，有利于规范我市网约车管理，进一步提升网约车安全和服务水平。制定《网约车运营服务管理》标准，有助于实现网约车行业规范健康发展，规范各方开展网约车运营服务管理，满足人民群众高品质出行需求。DB3502/T 046拟由六个部分构成。

——第1部分：运营条件，目的在于规范网约车经营者、专职网约车、兼职网约车、网约车驾驶员开展运营所需具备的条件，作为网约车相关主体所遵循的准入依据。

——第2部分：服务规范，目的在于规范网约车经营者及驾驶员的服务、网约车服务档次要求、遗失物归还和服务监督管理，作为网约车相关主体开展服务所需遵循的准则。

——第3部分：运营管理，目的在于规范网约车经营者、线下合作机构的运营管理要求，作为规范网约车相关主体运营管理的依据。

——第4部分：信息安全，目的在于规范网约车经营者、线下合作机构、驾驶员、乘客、管理部门的信息安全要求，作为网约车运营服务管理的信息安全防护依据。

——第5部分：安全与应急，目的在于规范网约车经营者、线下合作机构的安全与应急要求，作为网约车运营安全与应急处置依据。

——第6部分：监督管理，目的在于规范网约车管理部门的监督管理要求，作为管理部门开展网约车监督管理的依据。

网约车运营服务管理 第4部分：信息安全

1 范围

本文件规定了网络预约出租汽车（简称网约车）经营者、网约车线下合作机构、网约车驾驶员、网约车乘客、网约车管理部门的信息安全要求。

本文件适用于网约车运营服务管理活动中的信息安全防护。

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 25069 信息安全技术 术语

GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

GB/T 29245-2012 信息安全技术 政府部门信息安全管理基本要求

GB/T 35273-2020 信息安全技术 个人信息安全规范

DB 3502/T 046.1-2019 网约车运营服务管理 第1部分：运营条件

DB 3502/T 046.2-2019 网约车运营服务管理 第2部分：服务规范

DB 3502/T 046.3-2019 网约车运营服务管理 第3部分：运营管理

3 术语和定义

GB 25069、JT/T 1068、DB3502/T 046.1-2019、DB3502/T 046.2-2019和DB 3502/T 046.3-2019界定的以及下列术语和定义适用于本文件。

3.1

用户 user

使用网约车服务的个人，通常包括乘客和驾驶员。乘客包括约车人和乘车人。

3.2

保密性 information confidentiality

确保信息只被授权人员访问。

3.3

完整性 integrity

包括数据完整性和系统完整性。数据完整性表征数据所具有的特性，即无论数据形式作何变化，数据的准确性和一致性均保持不变的程度；系统完整性表征系统在防止非授权用户修改或使用资源和防止授权用户不正确地修改或使用资源的情况下，系统能履行其操作目的的品质。

3.4

可用性 availability

表征数据或系统根据授权实体的请求可被访问与使用程度的安全属性。

3.5

约车人 booking person

向网络服务平台发送预约用车请求的人，可以不是乘车人。

4 总体要求

4.1 网约车经营者、线下合作机构、管理部门在运营服务管理活动中应按照本文件要求开展信息安全管理工作，确保网约车运营服务管理的信息安全，并接受相关部门、社会各界的监督。

4.2 网约车经营者、线下合作机构、管理部门在个人信息处理活动中应遵循合法、正当、必要的原则，并参照 GB/T 35273-2020 中的要求执行。

4.3 网约车经营者的网络信息安全保护能力应不低于 GB/T 22239-2019 中规定的第二级等级防护要求；网约车线下合作机构、管理部门的网络信息安全保护能力应参照 GB/T 22239-2019 的规定确定等级防护或相关要求。

5 网约车经营者信息安全

5.1 安全管理

5.1.1 基本要求

应确保网约车信息的保密性、可用性和完整性，包括但不限于建立安全管理制度、设立安全管理岗位、处理安全事件、编制应急预案及演练、开展安全检查及优化。

5.1.2 信息安全管理制度

5.1.2.1 应建立符合 GB/T 22239-2019 中第二级及以上安全要求的安全管理制度，对信息安全工作开展管理。

5.1.2.2 应明确网约车经营者信息安全保护的组织机构、岗位职能和人员职责。

5.1.2.3 应对网约车运营服务过程中的信息安全管理流程，信息安全操作规范予以明确。

5.1.2.4 应设置专门的部门及人员负责信息安全管理制度的制定。

5.1.2.5 信息安全管理制度应通过正式、有效的方式向经营者内部全体人员发布，并进行版本控制。

5.1.3 信息安全管理机构

5.1.3.1 应设立信息安全管理工作的职能部门，设立信息安全主管、安全管理各岗位负责人，并规定各负责人职责。

5.1.3.2 应配备足够数量的信息安全管理人员。

5.1.3.3 应根据各部门和岗位的职责明确信息安全授权审批事项、审批部门和批准人。

5.1.3.4 应针对系统变更、物理访问、系统接入、数据传输和数据使用等事项执行信息安全审批过程。

5.1.3.5 应加强经营者内部各类管理人员、组织机构和信息安全管理机构之间的合作和沟通，定期召开协调会议，共同协作处理信息安全问题。

5.1.3.6 应定期进行信息安全管理工作检查与审核，检查内容包括系统日常运行，系统漏洞和数据安全等情况。

5.1.4 信息安全管理人员

5.1.4.1　应对被录用的信息安全管理人员的身份、安全背景、专业资格或资质进行审查，并签署保密协议。

5.1.4.2　应及时终止离岗人员的所有访问权限，收回各种工作证件、钥匙及经营者提供的软硬件设备，并要求继续履行保密义务。

5.1.4.3　应对经营者内部各类工作人员进行信息安全教育和培训，宣贯信息安全责任和惩戒措施。

5.1.4.4　应在外部人员接入受控网络访问系统前提出书面申请，批准后由专人开设账户、分配权限并登记备案，并与外部人员签订保密协议。

5.1.5　信息安全事件处理

5.1.5.1　应形成信息安全事件的监控机制，及时发现系统弱点、可疑事件和安全事件，并向信息安全管理部门报告。

5.1.5.2　应建立信息安全事件报告和处理制度，明确不同类型和影响的事件报告、响应和处置流程，规定信息安全事件现场处理、事件报告和后期恢复等环节的管理职责。

5.1.5.3　应在信息安全事件响应和处置过程中，分析和鉴定事件产生原因，收集证据，记录处理过程，总结经验教训，并追究相关人员责任。

5.1.5.4　应及时将事件相关情况以邮件、信函、电话、推送通知等方式告知受影响的个人信息主体。难以逐一告知个人信息主体时，应采取合理、有效的方式发布与公众有关的警示信息。

5.1.6　应急预案及演练

5.1.6.1　应分析不同类型信息安全事件的影响程度和范围，制定有效的应急预案，包括应急处理流程、系统恢复流程、数据恢复流程等。

5.1.6.2　应定期对系统和数据安全相关人员进行应急预案培训，定期开展应急预案演练。

5.1.7　安全检查

5.1.7.1　应制定信息安全检查计划和方案，明确检查范围、对象和方法。

5.1.7.2　应定期开展信息安全检查，记录检查活动，分析潜在信息安全风险。

5.1.7.3　应持续改进信息安全管理制度，优化信息安全事件处理流程和应急预案。

5.2　信息安全

5.2.1　数据收集

5.2.1.1　采集乘客的个人信息，分为乘客必要信息和可选信息，必要信息的采集应用于网约车基础服务，可选信息的采集应用于乘客自主选择的可选业务功能，不得超越提供网约车业务所必需的范围。乘客必要信息和乘客可选信息具体如下：

a)　乘客必要信息包括身份信息、位置信息、订单信息、交易信息、通信设备信息等。

b)　乘客可选信息包括实际乘车人姓名及手机号码、紧急联系人姓名及手机号码、家庭住址、公司地址、虚拟电话号码通话录音、App 端内在线沟通记录、服务评价、乘客与客服的通话记录、发票信息、纸质发票收件地址、电子发票收件邮箱等。

5.2.1.2　采集驾驶员的个人信息，分为驾驶员静态信息和动态运营信息，不得超越提供网约车业务所必需的范围。驾驶员静态信息和动态运营信息具体如下：

a)　驾驶员静态信息包括身份信息、车辆信息、许可信息、收款信息、通信设备信息等。

b) 驾驶员动态运营信息包括位置信息、行程轨迹、订单信息、行程录音、行程驾驶行为信息等，网约车安装有智能车载设备的，收集的驾驶员动态运营信息包括行程录像。

5.2.1.3 为保障服务正常开展，需向乘客申请移动终端操作系统位置信息权限，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，网络预约汽车服务App采集位置信息频率每秒不应超过一次。

5.2.1.4 应通过其服务平台以显著方式向个人信息主体告知采集和使用用户个人信息的目的、方式、范围，保障其知情权，并获得个人信息主体的授权同意。

5.2.2 数据传输

5.2.2.1 基本要求

应根据业务情况确定数据传输的类型、方式和数量，采取数据加密等保护措施，不向无关第三方传输网约车驾驶员与乘客信息数据。

5.2.2.2 安全区域边界

数据传输网络安全区域边界应符合GB/T 22239-2019中规定的第二级安全要求中关于边界防护和访问控制的相关要求。

5.2.2.3 紧急情况下数据传输

在紧急情况下数据传输应遵循如下要求：

a) 用户设置的紧急联系人以用户人身安全存在重大风险为由，要求网约车经营者提供用户信诚信息和位置信息的，网约车经营者应先尝试联系用户，如无法联系到用户则向紧急联系人提供相应信息，如联系到用户，则按用户要求处理。

b) 网约车经营者应为用户提供紧急联系人查询信息授权功能。用户授权紧急联系人查询用户个人信息的，紧急联系人要求获取用户个人信息时，网约车经营者应予以提供。

c) 网约车经营者应提供“一键呼叫”功能，用户遇紧急情况使用时，能够实现向网约车平台发送车辆实时动态信息及人员信息。

5.2.2.4 地图服务数据传输

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，可向地图服务方传输通信设备信息、实时位置和路线规划信息，不应传输乘客或驾驶员的手机号码及身份信息。

5.2.2.5 第三方平台数据传输

接入第三方平台，乘客可通过第三方平台发单的，网约车经营者与第三方平台应约定传输个人信息类型，传输信息应以为乘客提供网约车服务所必须的信息为限。

5.2.2.6 网络支付数据传输

网约车服务中乘客使用网络支付的，在征得乘客明示同意后，网约车经营者可向网络支付机构传输支付时间、支付金额、支付渠道等支付信息。

5.2.2.7 司乘沟通信息

应在司乘沟通环节提供如下保障：

a) 网约车经营者应采用“虚拟号码”技术，保障驾驶员、乘客真实手机号码互不可见。订单结束或取消后，虚拟号码自动失效，确保驾驶员乘客之间不能再互相联系，避免个人手机号码泄露。
b) 网约车经营者应提供司乘间即时通讯服务，司乘双方可通过 App 互相发送文字或语音信息联系行程事宜，行程结束后联系通道自动关闭。

5.2.3 数据存储

5.2.3.1 应遵守国家网络和信息安全有关规定，所采集的个人信息和生成的业务数据，应当在中国大陆境内存储，保存期限不少于 2 年，除法律法规另有规定外，不得外流。

5.2.3.2 应对涉及安全类投诉的相关数据进行永久保存。

5.2.3.3 应将个人身份信息、面部识别特征和行程录音录像数据分开存储。

5.2.3.4 采集的行程轨迹和行程录音录像数据不应存储在办公终端中，应在有安全防护措施的服务器端存储。

5.2.3.5 应部署数据容灾备份系统，关键数据宜采取异地备份，采用同步或异步方式实时在线备份数据。

5.2.3.6 应制定灾难恢复预案并定期演练，一旦灾难发生能在短时间内恢复数据，保障信息系统的业务连续性。

5.2.4 数据使用

5.2.4.1 规范数据使用的范围

应遵守如下数据使用范围要求：

a) 网约车经营者可在用户明示同意的前提下，使用前述个人信息进行用户个人信息展示、用户画像使用和驾驶员信用记录使用；
b) 未经用户明示同意，网约车经营者不得使用前述用户个人信息用于开展其他业务；
c) 除按规定向监管部门提供有关信息，配合国家机关依法行使监督检查权或刑事侦查权外，网约车经营者不得向任何第三方提供驾驶员和乘客的姓名、联系方式、家庭住址、银行账户或支付账户、地理位置、出行线路等个人信息，不得泄露地理坐标、地理标志物等事关国家安全的敏感信息。

5.2.4.2 个人信息展示

在展示个人信息时应遵循如下要求：

a) 订单匹配后，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名、照片、手机号码、实时位置、车辆信息和服务评价结果，向驾驶员展示的乘客信息包括乘客手机号码最后四位和服务评价结果；
b) 订单匹配后，为乘客和驾驶员提供电话沟通渠道时，应使用虚拟电话号码；
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) 订单完成后，为用户保留纠纷处理的联系通道（例如物品遗失沟通）时，应使用虚拟电话号码；
e) 向乘客、驾驶员展示对方给出的评价内容时，应延时 24 小时及以上，且匿名展示；
f) 应对内部业务系统需展示的用户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。

5.2.4.3 用户画像使用

在开展用户画像时应遵循如下要求：

a) 根据用户个人信息进行用户画像，制定派单策略时，应以保护用户人身和财产安全为原则，尊重用户合法权利；
b) 根据用户画像进行个性化展示时，应显著区分个性化展示的内容和非个性化展示的内容；
c) 不应利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。

注：基于个人信息主体所选择的特定地理位置进行展示、搜索结果排序，且不因个人信息主体身份不同展示不一样的内容和搜索结果排序，则不属于个性化展示。

5.2.4.4 驾驶员信用记录使用

在使用驾驶员信息记录时应遵循如下要求：

a) 建立驾驶员信用记录用于驾驶员管理时，驾驶员注销账号后，对于驾驶员曾在服务过程中产生的违反法律法规和违反平台规则的信用记录，以及低于初始分的信用记录，网约车经营者在提供服务期间可持续保存；
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，网约车经营者宜予以恢复驾驶员信用记录。

6 线下合作机构信息安全

6.1 车辆管理线下合作机构信息安全

6.1.1 管理要求

6.1.1.1 应建立信息安全管理制度，对车辆信息安全开展管理工作。
6.1.1.2 应建立租赁经营信息管理档案，并按照要求向管理部门报送数据信息。
6.1.1.3 应建立符合信息安全管理制度的管理岗位，负责实施租赁经营服务中的信息安全管理工作。
6.1.1.4 发生重大信息安全事故时，应及时向管理部门报告，并采取有效补救措施。
6.1.1.5 应定期开展信息安全检查，记录检查活动，分析潜在信息安全风险。

6.1.2 信息安全

6.1.2.1 不应泄露网约车车辆车牌号码、车牌颜色、车辆厂牌、车辆类型、车辆型号、所属车主、车身颜色、车辆照片、网约车运输证或兼职网约车备案证等车辆信息。
6.1.2.2 不应泄露车辆保险公司、保险号、保险类型、保险金额、保险生效时间及保险到期时间等信息。

6.2 驾驶员管理线下合作机构信息安全

6.2.1 管理要求

6.2.1.1 应建立信息安全管理制度，对驾驶员信息安全开展管理工作。
6.2.1.2 应建立驾驶员信息管理档案，并按照要求向管理部门报送数据信息。

6.2.1.3　应建立符合信息安全管理制度的管理岗位，负责实施网约车驾驶员线下管理中的信息安全管理工作。
6.2.1.4　发生重大信息安全事故时，应及时向管理部门报告，并采取有效补救措施。
6.2.1.5　应定期开展信息安全检查，记录检查活动，分析潜在信息安全风险。

6.2.2　信息安全

6.2.2.1　采集的驾驶员个人信息主要包括姓名、手机号码、身份证、驾驶证、行驶证、网约车驾驶员证、网约车运输证或兼职网约车备案证等，不应超越提供网约车驾驶员线下管理业务所必需的范围。
6.2.2.2　应通过协议等显著方式告知驾驶员信息采集和使用目的、方式、范围，保障其知情权。
6.2.2.3　不应泄露网约车驾驶员个人信息。

7　驾驶员和乘客信息安全

7.1　乘客不宜向驾驶员透露约车人或乘车人的姓名及联系方式等个人信息。
7.2　驾驶员不应询问和泄露乘客的姓名、联系方式、家庭住址、乘车地址、出行线路等个人信息。
7.3　乘客不应询问和泄露驾驶员的姓名、联系方式、家庭地址等个人信息。

8　管理部门信息安全

8.1　管理要求

8.1.1　基本要求

管理部门开展信息安全管理应遵循GB/T 29245-2012中的相关规定。

8.1.2　建立信息泄露报告制度

发生信息泄露后，应及时采取有效补救措施，告知相关信息主体，并按规定向上级管理部门及信息安全管理部门报告。

8.1.3　安全审计与监督

8.1.3.1　应按如下要求对网约车经营者开展安全审计与监督：

a)　应组织第三方对网约车经营者开展信息安全审计，发布年度信息安全报告；
b)　应组织或委托专业机构，对网约车经营者在本市产生的信息安全性和可能存在的风险每年至少进行一次检测评估，并对检测评估情况及采取的改进措施提出网络安全报告；
c)　审计记录和留存时间应符合法律法规的要求。

8.1.3.2　管理部门应接受网络安全监管部门等相关部门的监督管理，并接受社会各界监督。

8.2　信息安全

8.2.1　数据接入

管理部门应督促网约车经营者按照规定的要求将真实可信、符合行业监管需求的运营服务数据接入厦门市网约车监管平台。

8.2.2 数据存储

管理部门应要求网约车经营者，对接入厦门市网约车监管平台的数据保存不少于2年，数据存储介质防护管理应符合GB/T 29245-2012 中5.7的要求。

8.2.3 系统防护

管理部门应按照GB/T 29245-2012 中5.3的要求开展信息系统防护管理。

8.2.4 终端防护

管理部门所使用的终端计算机应按照GB/T 29245-2012 5.6终端计算机防护管理的要求开展防护工作。

参 考 文 献

[1]《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

[2]《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

[3]《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

[4]《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

[5]《网络交易监督管理办法》国家市场监督管理总局令第37号公布，自2021年5月1日起施行

[6] 《网络预约出租汽车经营服务管理暂行办法》2016年7月27日交通运输部、工业和信息化部、公安部、商务部、工商总局、质检总局、国家网信办发布，根据2019年12月28日《交通运输部 工业和信息化部 公安部 商务部 市场监管总局 国家网信办关于修改<网络预约出租汽车经营服务管理暂行办法>的决定》修正

[7] 《小微型客车租赁经营服务管理办法》 交通运输部令2020年第22号

[8] 《网络预约出租汽车监管信息交互平台总体技术要求（暂行）》 交办运〔2016〕180号

[9] GB 28827.4-2019 信息技术服务 运行维护 第4部分：数据中心服务要求