

编号：CESI-SC-OD16



网络预约汽车服务数据安全服务认证规则

2025-8-31 发布

2025-8-31 实施

北京赛西认证有限责任公司



前 言

本规则依据《中华人民共和国认证认可条例》制定。本规则明确了对网络预约汽车服务数据安全进行认证的基本原则和要求。

本实施规则由北京赛西认证有限责任公司制订并发布，版权归北京赛西认证有限责任公司所有，任何组织及个人未经北京赛西认证有限责任公司许可，不得以任何形式全部或部分使用。本规则的最终解释权归北京赛西认证有限责任公司所有。

本规则首次发布日期：2023.8.28，实施日期：2023.8.28。

第一次修订（v1.1）日期及内容：2024.3.1，本次换版修订了认证名称、申请范围描述、准许使用的认证标志样式。

第二次修订（v1.2）日期及内容：2025.8.31，本次换版修订了服务特性测评过程、认证证书模板。



目 录

1 适用范围	3
2 认证依据	3
3 认证模式	3
4 认证实施	3
4.1. 认证申请	3
4.2. 申请评审	4
4.3. 认证评价	4
4.3.1. 服务特性测评	4
4.3.2. 文件审查	4
4.3.3. 服务管理审核	4
4.4. 复核、认证决定	5
4.5. 获证后监督	5
4.5.1. 监督的频次和方式	5
4.5.2. 监督的内容	6
4.5.3. 获证后监督结果的评价	6
4.6. 再认证	6
4.7. 认证时限	6
5 认证证书	6
5.1. 证书的保持	7
5.2. 证书的变更	7
5.3. 认证的暂停、撤销和注销	7
6 认证标志	7
附录 A 网络预约汽车服务数据安全能力等级条款表	9
附录 B 认证证书样式	17

1 适用范围

本规则规定了对网络预约汽车服务数据安全进行认证的基本原则和要求。

认证领域或技术领域划分：SC12。

2 认证依据

GB/T 42017-2022 《信息安全技术 网络预约汽车服务数据安全要求》

3 认证模式

服务特性测评+服务管理审核+获证后监督

4 认证实施

4.1. 认证申请

4.1.1 申请范围界定

场所：认证申请方的网络预约汽车服务数据处理活动所在的物理场所。

活动：认证申请方的网络预约汽车服务数据处理活动。

等级：认证申请方的网络预约汽车服务数据安全能力等级。

网络预约汽车服务数据安全能力等级定义如下表所示：

等级名称	等级定义
1 级 基础级	主动地实现了数据处理活动安全要求的计划与执行，但没有形成体系化。
2 级 规范级	实现了数据处理活动安全要求的规范执行。
3 级 卓越级	依据数据处理活动安全要求，不断优化和改进组织的执行。

4.1.2 申请时需提交的文件资料

申请认证应提交正式申请，并随附以下文件：

- 1) 有效法律地位证明复印件及适用时从事相关服务的资质和任何行政许可证明复印件；
- 2) 国家企业信用信息公示系统年度报告电子版；
- 3) 网络预约汽车服务数据安全能力自评价表；
- 4) 其他认证所需相关材料。



4.2. 申请评审

认证机构在 5 个工作日内对申请材料进行评审，确认资料的完整性、准确性和符合性。并将评审结果（包括受理、退回修改、不受理）告知认证申请方。

若决定受理，认证机构根据认证申请资料确定认证方案，并通知认证申请方。

4.3. 认证评价

认证机构对组织的数据安全能力实施服务特性检验、服务能力确认或验证，并出具报告。

4.3.1. 服务特性测评

服务特性测评采用服务特性检验方式。

认证机构委托评估机构依据 GB/T 42017-2022 对组织的网络预约汽车服务数据安全能力相关要求进行公开的服务特性检验，出具服务特性检验报告（即：网络预约汽车服务数据安全能力评估报告）。

简略的评估流程包括：

- 1) 依据组织申请评估的等级，选取相应的标准条款（详见附录 A 网络预约汽车服务数据安全能力等级条款表）；
- 2) 依据 GB/T 42017-2022 标准条款要求，评估能力满足情况。

4.3.2. 文件审查

初次认证时进行文件审查。认证机构委派审查组对申请方的服务特性检验报告以及相关佐证材料进行文件审查。

对文件审查中发现的不符合项，申请方应及时修改、补充提交必要的文件，文件整改实施期限原则上不超过 10 个工作日。

审查组出具文件审查报告，给出是否进行现场评价的建议及现场评价中需重点关注的事项。

4.3.3. 服务管理审核

服务管理审核采用服务能力确认或验证方式。

由认证机构审查组进行服务能力确认或验证的现场评价。

4.3.3.1. 评价内容

初次认证时，依据申请方申请的网络预约汽车服务数据安全能力等级和服务特性检验报告，到申请范围内的网络预约汽车服务数据处理活动所在场所现场确认或验证该等级各个条款要求的能力。

各等级对应标准条款如附录 A 所示。

现场评价重点是审查申请方符合 GB/T 42017-2022《信息安全技术 网络预约汽车服务数据安全要求》的情况，针对服务特性检检报告建议的等级进行审查。

4.3.3.2. 评价结论

审查组以评价报告的形式向认证机构报告评价结论。现场评价存在不符合项时，申请方应在认证机构规定的期限内完成整改，审查组采取适当方式对整改结果进行验证。逾期不能完成整改，或整改结果不合格，按现场评价结论不合格处理。

4.4. 复核、认证决定

认证机构应对认证相关的所有信息包括申请评审、评价过程和结论进行复核。

认证机构根据评价、复核以及其他相关的所有信息做出认证决定。

对符合认证要求的，颁发认证证书；对暂不符合认证要求的，可要求认证申请方限期整改，整改后仍不符合的，以书面形式通知认证申请方终止认证。

4.5. 获证后监督

4.5.1. 监督的频次和方式

认证机构在认证证书有效期内，通过认证评价对获得认证的专业机构进行持续监督，年度监督审核至少每个日历年进行一次，初次认证后的第一次监督审查在认证决定日期起 12 个月内进行。若发生下述情况可适当增加监督频次：

- 1) 获证组织的服务活动出现严重质量问题，如：发生网络预约汽车服务数据安全事故或在网络预约汽车服务数据安全方面有重大投诉，并经查实为获证组织责任时；
- 2) 认证机构有足够理由对获证组织服务与认证要求的符合性提出质疑时；
- 3) 有足够信息表明获证组织因变更组织机构、服务场所、环境条件等，可能影响服务符合性或一致性时；
- 4) 违反法律法规、国家行业监督及媒体曝光等重大问题的情况；

5) 发生其他影响符合认证要求的能力变化的特殊情况时。

4.5.2. 监督的内容

监督时至少应评价以下内容：

- (1) 上次评价以来组织活动及运行的资源是否有变更；
- (2) 组织数据安全特性有关的活动是否有效运行；
- (3) 涉及法律法规规定的，相关法律法规或技术标准是发生变化，是否持续符合相关规定；
- (4) 网络预约汽车服务数据安全能力是否持续保持；
- (5) 获证组织对认证标志的使用或对认证资格的引用是否符合相关的规定；
- (6) 是否及时接受和处理投诉；
- (7) 针对投诉的问题，及时制定并实施了有效的持续改进。

监督至少应包括服务管理审核，且在一个认证周期内至少开展一次服务特性检验，监督采用条款抽样的方式开展，抽样条款的数量应不低于认证依据条款的 1/2。

4.5.3. 获证后监督结果的评价

认证机构对证后监督报告和其他相关资料信息进行综合评价，监督结果符合要求的，可保持认证资格，继续使用认证证书和认证标志；对监督复查时发现的不符合项应在认证机构规定期限内完成纠正措施。逾期按认证机构公开文件《服务认证程序规则》的要求执行，并对外公告。

4.6. 再认证

认证机构在认证证书到期前对获证机构进行再认证，再认证过程与初次认证保持一致，再认证条款与初次认证相同。

4.7. 认证时限

认证时限是指自作出受理决定之日起至作出认证决定所实际发生的工作日，一般为 60 个工作日（不包含整改时间）。

5 认证证书

获证组织必须按认证机构公开文件《服务认证程序规则》的要求使用认证证书。

5.1. 证书的保持

认证证书有效期为3年。在有效期内，通过认证机构的获证后监督，保持认证证书的有效性。

证书到期需延续使用的，获证组织应当在有效期届满前6个月内提出认证申请。认证机构应当采用再认证的方式，对符合认证要求的申请换发新证书。

5.2. 证书的变更

认证证书有效期内，获证组织名称、地址，或认证评价内容等发生变化时，获证组织应当向认证机构提出变更申请。认证机构根据变更的内容，对变更申请资料进行评价，确定是否批准变更。如需进行认证评价，还应当在批准变更前进行认证评价。当认证要求（如标准）发生变化时，获证组织应按规定换证，未按规定换发的认证证书自行失效，同时认证机构应予以撤销证书，要求其停止使用认证标志。

认证的变更按照认证机构公开文件《服务认证程序规则》的要求执行。

5.3. 认证的暂停、撤销和注销

当获得认证组织不再符合认证要求时，认证机构对认证证书予以暂停直至撤销，要求其停止使用认证标志。认证申请方在认证证书有效期内可申请暂停或注销认证证书。认证机构采用适当方式对外公布被暂停、注销和撤销的认证证书。

暂停期限为6个月。暂停期限内，获证机构可提出恢复认证的申请，经认证机构评审、批准后，方可使用该证书。在暂停认证期间，获证机构不得继续使用证书和认证标志。暂停期满仍未恢复认证资格的，认证证书自动撤销。

认证的暂停、恢复、撤销、注销及涉及的认证证书和标志使用的具体要求按照认证机构公开文件《服务认证程序规则》执行。

6 认证标志

在认证证书有效期内，获证组织应当按照规定在广告等宣传中正确使用认证证书和认证标志，不得对公众产生误导。

获证组织必须按认证机构公开文件《服务认证程序规则》的要求使用认证标志。

7.1 准许使用的认证标志样式

1) 认证标志样式:



2) 规格: 标志图案的尺寸长宽比例 1:1, 允许线性比例缩放。

3) 颜色: 应使用基本颜色或单一黑色。

7.2 变形认证标志的使用

本规则覆盖的产品不允许使用任何形式的变形认证标志。

7.3 加施方式及位置

获证组织可在通过认证的系统、相关宣传材料上加施认证标志。

附录 A 网络预约汽车服务数据安全能力等级条款表

等级分成：1 级：基础级；2 级：规范级；3 级：卓越级。

基础级包括 47 个条款。规范级新增 21 个条款，合计 68 个条款。卓越级新增 21 个条款，合计 89 个条款。

规范级包含基础级的全部条款要求，卓越级包含基础级和规范级的全部条款要求。所有条款要求都满足时，才能授予相应等级证书。

章节	条款号	条款内容	三级	二级	一级
6 基本 要求	/ / 	网络预约汽车服务运营者数据安全应满足以下基本要求： a) 数据活动应符合 GB/T 41479 要求；	符合		
		b) 个人信息处理活动应符合 GB/T 35273-2020 要求，乘客 App 个人信息收集活动应符合 GB/T 41391-2022 要求；	符合		
		c) 应按照有关要求和标准进行数据分类分级保护，识别网络预约汽车服务涉及的核心数据、重要数据、一般数据，对不同级别的数据采取不同的保护措施。 注 1：国家建立数据分类分级保护制度，按照数据对国家安全、公共利益或者个人、组织合法权益的影响和重要程度，将数据分为核心数据、重要数据、一般数据。 注 2：附录 B 给出了网络预约汽车服务重要数据识别参考规则及数据分类示例。	符合		
		d) 应识别网络预约汽车服务涉及的一般个人信息、敏感个人信息，对个人信息进行标识和分类管理；			符合
		e) 应履行互联网平台运营者义务，如个人信息保护独立监督、制定公平公正的平台规则、隐私政策披露、平台内经营者管理、发布个人信息保护社会责任报告等	符合		
		f) 网络预约汽车服务提供者的数据安全能力应至少符合 GB/T 37988 中的 2 级能力要求；	符合		
		g) 应结合数据处理活动的实际情况，按照有关国家标准定期开展数据安全风险评估；			符合
		h) 应在开展对个人权益有重大影响的个人信息处理活动前，按照 GB/T 39335 进行个人信息保护影响评估； 注 3：对个人权益有重大影响的个人信息处理活动，包括但不限于处理敏感个人信息、利用个人信息进行自动化决策、委托处理个人信息、向其他个人信息处理者提供个人信息、公开个人信息、向境外提供个人信息等。			符合

			i) 应按照国家有关标准, 在网络预约汽车服务平台规划建设时开展个人信息安全工程实践, 同步规划、同步建设、同步使用个人信息保护措施;			符合
			j) 网络预约汽车服务平台应符合国家网络安全等级保护相关要求。		符合	
7 收集个人信息	7.1 收集个人信息	/	a) 通过 App 收集乘客必要个人信息应符合 GB/T 41391-2022 中 A.2 的规定; 注 1: GB/T 41391-2022 附录 A 给出了常见类型 App 必要个人信息范围。			符合
			b) 通过 App 收集驾驶员个人信息应限于提供服务或履行法律法规规定的义务所必需; 注 2: 网络预约汽车服务通过 App 收集的驾驶员个人信息范围及使用要求见附录 C 中的 C.1			符合
			c) 扩展业务功能收集的个人信息均应由用户可选提供, 且应限于实现处理目的的最小范围; 注 3: 网络预约汽车服务常见扩展业务功能收集的个人信息范围及使用要求见 C.2	符合		
	7.2 申请系统权限	7.2.1	乘客 App、驾驶员 App 不应申请与 App 业务功能无关的系统权限, 系统权限申请范围及使用要求见附录 D。			符合
		7.2.2	收集行踪轨迹时, 通过系统位置权限收集位置信息不应超过 1 次/s。 注: 单位时间内同时收集 GPS、Wi-Fi、基站信息用于定位校验, 视为一次位置信息收集。		符合	
	7.3 告知同意	/	a) 使用代叫车功能为他人发起服务订单的, 应提示收集乘车人个人信息的情况, 并取得叫车人征得乘车人同意的确认;	符合		
			b) 收集行程录音录像, 应制定单独行程录音录像收集协议, 向用户告知行程录音录像收集方式、收集时间、使用目的、存储和删除规则、收集必要性及对用户个人权益的影响等内容, 行程录音录像收集协议应征得用户单独同意, 行程录音收集协议范式模版示例见附录 E;		符合	
			c) 收集行程录音录像信息的, 应通过短信、车内语音播报等方式告知乘客行程录音录像收集情况;		符合	
			d) 多人乘车的, 应提醒叫车人告知同乘人个人信息收集情况;	符合		
			e) App 系统权限申请应同步告知权限使用目的。			符合
8 数据存储	/	/	a) 网络预约汽车服务个人信息存储期限应为实现个人信息处理目的所必须的最短时间, 超出存储期限后, 应对个人信息进行删除或匿名化处理, 法律法规另有规定的除外;			符合
			b) 如果超出个人信息存储期限, 但法律法规规定的保存期限未届满, 或者删除个人信息从技术上难以实			符合

			现的，应停止除存储和采取必要的安全保护措施之外的处理；			
			c) 应将行踪轨迹、人脸识别数据、行程录音录像与其它类型的个人信息分开存储； 注：人脸识别数据属于生物识别信息，通常包括人脸图像、面部识别特征。		符合	
			d) 应采取加密措施存储敏感个人信息，包括但不限于身份证、驾驶证、行驶证、人脸识别数据、行程录音录像、银行卡号和行踪轨迹；	符合		
			e) 采集的行踪轨迹和行程录音录像数据应存储在有安全保障措施的服务器端；			符合
			f) 应采取数据容灾备份措施，关键数据应采取异地容灾；			符合
			g) 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。			符合
9 数据使用和加工	9.1 数据访问控制	/	a) 应遵循最少够用、职责分离的原则，按照数据分级建立相应的数据访问控制措施和访问权限申请审批流程，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阅、更正、删除、下载等操作；		符合	
			b) 应对人脸识别数据、行踪轨迹、行程录音录像等高级别数据访问权限进行严格限制；		符合	
			c) 应对访问乘客和驾驶员个人信息的行为采取访问控制措施，投诉处理场景数据安全保护要求见附录 F，其他业务场景下的账号安全管理、数据访问控制等安全保护措施应遵照投诉处理场景要求执行。			符合
	9.2 个人信息展示	/	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宜包括驾驶员姓氏、驾驶员头像、手机号码后四位、实时位置、车辆品牌、车身颜色、车辆号牌和服务评价结果，向驾驶员展示的乘客信息宜包括乘客手机号码最后四位和服务评价结果；	符合		
			b) 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；			符合
			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，向亲友分享的信息应包括驾驶员姓氏、驾驶员头像、出发地、目的地、实时位置和车辆信息；			符合
			d) 向乘客、驾驶员展示评价内容时，应延时、匿名提供；		符合	
			e) 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，对查看个人信息行为留存审计日志，			符合

			数据脱敏规则示例见附录 G。			
	9.3 用户画像使用	/	a) 不应利用大数据分析等技术手段，基于用户消费记录、消费偏好等对个人在交易价格等交易条件方面实行不合理的差别待遇；	符合		
			b) 根据用户个人信息进行用户画像，制定派单策略时，应遵循公平、公正原则，保护乘客和驾驶员人身和财产安全，尊重乘客消费者权益和驾驶员劳动者权益；	符合		
			c) 基于用户出行习惯为用户提供上下车地点、常用路线推荐的，应为用户提供关闭选项；		符合	
			d) 通过自动化决策方式进行信息推送、商业营销，应同时提供不针对其个人特征的选项，或者向个人提供便捷的拒绝方式；		符合	
			e) 基于用户画像的推荐功能应允许用户自主选择。			符合
	9.4 驾驶员信用记录使用	/	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，应留存驾驶员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；			符合
			b) 驾驶员注销账号后重新注册/登录的，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，网络预约汽车服务提供者宜予以恢复。			符合
10 数据提供和公开	10.1 数据提供	10.1.1 数据提供基本要求	a) 应按照最小必要原则确定数据提供的类型、方式、用途和数量，建立不同级别数据提供保护措施和审批流程；			符合
			b) 行程录音录像、人脸识别数据、行踪轨迹等敏感个人信息和重要数据传输，应采取加密、完整性保护等安全措施；			符合
			c) 向他人提供用户个人信息，应向用户告知接收方的名称或姓名、联系方式、处理目的、处理方式和个人信息种类，并取得个人的单独同意；			符合
			d) 不向无业务需要的第三方提供网络预约汽车服务用户个人信息；			符合
			e) 因兼并、重组、破产等原因需要转移数据的，应明确数据转移方案，数据接收方应继续履行相关数据安全保护义务。			符合
		10.1.2 紧急情况下数据提供	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，要求查阅用户的行程信息和位置信息的，网络预约汽车服务提供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，应提供相应的行程信息和位置信息。如联			符合

			系到用户，则应依照用户要求进行处理；			
			b) 宜为用户提供紧急联系人查询用户个人信息授权选项，用户已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，网络预约汽车服务提供者应予以提供；		符合	
			c) 在用户使用一键报警或者其他紧急情况下，应向用户设置的紧急联系人提供其行程信息、位置信息和报警情况。		符合	
		10.1.3 企业 订单 数据 提供	a) 应要求企业在提供员工个人信息前，获得员工单独同意；		符合	
			b) 应与企业约定企业订单中乘客个人信息的提供规则，在征得乘客单独同意后，向乘客所属企业提供享的订单信息包括：出发地、目的地和支付信息、订单时间和里程；			符合
			c) 乘客在企业订单过程中发生安全事件，人身和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提供者索要乘客行程中安全事件信息的，应予以提供。			符合
		10.1.4 地图 服务 方数 据提 供	网络预约汽车服务接入地图服务，为乘客和驾驶员提供路径规划、导航服务时，不应提供乘客或驾驶员的手机号码及身份信息。		符合	
		10.1.5 第三 方服 务平 台数 据提 供	网络预约汽车服务接入到第三方服务平台，乘客通过第三方服务平台发起订单的，网络预约汽车服务提供者应遵循必要原则，与第三方服务平台约定提供的个人信息范围，并限于网络预约汽车服务所必需。			符合
11 数据 出境	/	10.2 违法违 规信息 公开披 露	/	网络预约汽车服务提供者对用户违法违规信息公开披露时，应对乘客或驾驶员的个人信息进行去标识化处理。		符合
		/	/	a) 网络预约汽车服务在境内运营所收集和产生的个人信息、重要数据和业务数据应在境内存储，法律法规另有规定的除外；		符合

12 乘客和驾驶员个人信息权利			b) 应对网络预约汽车服务运营中数据出境行为进行监测, 及时发现并阻止违规数据出境, 如对租用的网络链路进行出境流量分析、对服务 APP 与境外网络通信行为进行检测分析等;		符合	
			c) 根据业务发展和运营情况, 每年应自行或委托第三方机构对数据出境至少进行一次数据出境风险评估。			符合
	12.1 个人信息查阅和复制	/	a) 应为乘客和驾驶员提供在线个人信息查阅服务, 个人信息查阅服务应简单方便、易于操作;			符合
			b) 乘客查阅的个人信息应包括但不限于账号信息、手机号码、实名信息、紧急联系人、常用地址、账户余额、行程订单;		符合	
			c) 驾驶员查阅的个人信息应包括但不限于手机号码、实名信息、个人头像、车辆信息、紧急联系人、账户余额、行程订单、流水明细、服务评价;	符合		
			d) 为用户提供在线个人信息复制功能时, 应提供口令保护以防范个人信息副本泄露或被窃取。		符合	
	12.2 个人信息更正或补充	/	a) 应为乘客和驾驶员提供在线个人信息更正或补充服务, 个人信息更正或补充服务应简单方便、易于操作;			符合
			b) 乘客更正或补充的个人信息应包括但不限于账号信息、手机号码、常用地址、紧急联系人;			符合
			c) 驾驶员更正或补充的个人信息应包括但不限于账号信息、手机号码、个人头像、车辆信息、紧急联系人。			符合
	12.3 个人信息投诉	/	a) 应建立涉及乘客和驾驶员的个人信息安全的投诉咨询渠道, 如客服、电子邮件等;			符合
			b) 应对手机号码、身份证、车辆信息、行程订单和行程录音录像等个人信息的滥用、泄露的投诉进行核实处理, 并向投诉者及时反馈处理结果;			符合
			c) 应对乘客、驾驶员的投诉受理及处理进行记录、归档, 对投诉处理满意度和实效性进行跟踪检查, 改进投诉管理机制, 提高个人信息申诉服务水平。		符合	
			d) 应对投诉者提供的信息严格保密, 保护投诉者权益。			符合
	12.4 个人撤回同意	/	a) 应为用户提供在线面部识别特征授权撤回同意功能, 收集面部识别特征为履行合同所必需的除外;			符合
			b) 应为乘客和驾驶员提供便捷的系统权限撤回同意管理入口。			符合

13 行程录音录像数据安全要求	12.5 个人信息删除	/	a) 应为乘客和驾驶员提供个人信息在线删除服务或通过客服提供删除服务;			符合
			b) 应为乘客和驾驶员提供在线账号、紧急联系人、常用地址和订单删除服务;			符合
			c) 应为乘客和驾驶员提供行程录音录像删除服务。	符合		
	12.6 乘客和驾驶员注销账户	/	a) 应为乘客和驾驶员提供在线账号注销服务;			符合
			b) 账号注销应简单方便, 可立即实现, 有未完成订单, 未处理完毕纠纷的除外;			符合
			b) 账户注销后, 对于法律法规规定或者双方约定的期限届满的, 应立即删除或者匿名化处理;		符合	
			d) 账户注销功能不应增加收集个人信息。			符合
	13.1 行程录音录像数据安全基本要求	/	行程录音录像数据是网络预约汽车服务中的敏感个人信息。网络预约汽车服务提供者应制定行程录音录像数据安全规范, 在行程录音录像数据收集、使用、存储、删除等环节采取安全控制措施进行重点保护。行程录音录像数据安全规范范式模版示例见附录 H。			符合
	13.2 行程录音录像的收集	/	a) 收集行程录音录像应取得驾驶员和乘客单独同意, 并在每次行程录音前单独提示, 行程录音宜通过驾驶员 App 或车载设备收集、行程录像宜通过车载设备收集;		符合	
			b) 收集的行程录音录像数据如需保存, 应保存在车内, 经用户单独同意才可上传, 紧急情况下为保护自然人的生命健康安全所必需的除外;	符合		
			c) 应对车载设备采取必要的安全防护, 包括但不限于授权访问、数据加密、禁用或屏蔽调试接口。		符合	
	13.3 行程录音录像的使用	/	a) 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;	符合		
			b) 应对行程录音录像采取水印技术防范录音转录和录像截取等泄露风险;	符合		
			c) 宜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, 对音频信息的基频进行改变等; 注: 音频基频指每一个人声音的声纹特征, 通过该特征能将不同人的声音进行有效的区分识别。	符合		
			d) 应对行程录像采取技术措施, 对车外人员面部识别特征、车外车辆号牌、车内乘客面部识别特征模糊化处理, 如采取检测技术在视频中定位人员面部位置、	符合		



			对面部识别特征遮挡处理等。			
	13.4 行程录音录像 的存储与删除	/	a) 应为乘客和驾驶员提供已完成订单的行程录音录像删除渠道，在一次行程服务完成后，如乘客和驾驶员对行程安全确认无误，应能向网络预约汽车服务提供者提出删除本次行程录音录像数据请求，网络预约汽车服务提供者应在 3 天内删除行程录音录像；	符合		
			b) 收集的行程录音数据存储时间不应超过 7 天，当乘客或驾驶员有未处理完毕纠纷时，对应的行程录音数据适当延长保存期限，纠纷处理完毕且超过约定存储期限的应删除。	符合		

注：黄色是一级所需满足的条款；绿色是二级所需满足的新增条款；红色是三级所需满足的新增条款。

附录 B 认证证书样式

	
网络预约汽车服务 数据安全服务认证证书	
证书编号: CESIxxDSRH1xxxxRx OID 编号: 1.2.156.1.2. CESIxxDSRH1xxxxRx	
兹证明	
XXXXXXXXXXXXX 公司 (统一社会信用代码: XXXXXXXXXXXXXXXX) (XXXXXXXXXXXXXXXXXXXXX)	
数据安全达到 GB/T 42017-2022 《信息安全技术 网络预约汽车服务数据安全要求》 等级 X: (XX 级) 认证模式 服务特性测评+服务管理审核+获证后监督 认证规则 CESI-SC-OD16《网络预约汽车服务数据安全服务认证规则》	
涉及的场所及相关活动: 地址: XXXXXXXXXXXXXXXXXXXX 活动: XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	
(本证书有效性依据发证机构的定期监督获得保持, 证书有效性信息请登录 www.cc.cesi.cn 进行查询) (本证书信息可在国家认证认可监督管理委员会官方网站 www.cnca.gov.cn 上查询)	
颁证日期: 20xx 年 xx 月 xx 日 有效期至: 20xx 年 xx 月 xx 日	
	签发人: 
北京赛西认证有限责任公司	
地 址: 北京市东城区安民里八号一号楼 2 层 客服电话: 4000719000 网址: www.cc.cesi.cn	
	