



特殊的普通合伙 Limited Liability Partnership

北京市朝阳区金和东路 20 号院正大中心 3 号楼南塔 22-24 层及 27-31 层 邮编：100020
22-24/F & 27-31/F, South Tower of CP Center, 20 Jin He East Avenue, Chaoyang District, Beijing 100020, China
电话/Tel: +86 10 5957 2288 传真/Fax: +86 10 6568 1022/1838 www.zhonglun.com

北京市中伦律师事务所

关于

奇瑞汽车股份有限公司

网络安全、数据安全及个人信息保护法律意见书



二〇二五年九月

目 录

免责声明	2
释 义	4
正 文	7
一、 公司处理的数据类型识别	7
二、 汽车数据处理	8
三、 个人信息处理	17
四、 网络安全与数据安全义务的履行	28
五、 公司处理重要数据的合规情况	36
六、 人工智能技术的应用	37
七、 公司无需申报数据出境安全评估或开展标准合同备案等	38
八、 公司无需主动申报网络安全审查	38
九、 结论性意见	41
附件 1: 个人信息的直接收集	43
附件 2: 核心业务主要在线产品清单	45
附件 3: 信息系统网络安全等级保护备案情况	49

免责声明

为出具本“网络安全、数据安全及个人信息保护法律意见书”(以下简称“**意见书**”),北京市中伦律师事务所(以下简称“**本所**”或“**我们**”)针对奇瑞汽车股份有限公司中华人民共和国境内(仅就本意见书而言,不含中华人民共和国香港特别行政区、中华人民共和国澳门特别行政区、中华人民共和国台湾地区)的运营实体、子公司、分公司的网络安全、数据安全及个人信息保护(以下统称“**数据合规**”)自报告期起始之日直至最后实际可行日期内的状况,基于与奇瑞业务相关人员的访谈情况、奇瑞的说明、奇瑞提供的材料及反馈等资料,对奇瑞目前整体运营相关的数据合规状态进行审查。包括对奇瑞的数据合规现状进行了法律尽职调查;审查了奇瑞核心业务的 App、Web 以及小程序的用户交互界面的流程、功能版块,对应的隐私政策及相关个人信息保护规则(包括在线产品、车机端等),以及向监管部门提交的汽车数据年报;评估了奇瑞的汽车数据处理合规现状,以及个人信息收集、使用、共享、存储环节的合规现状;审阅了奇瑞的数据合规内部组织架构、数据合规风险控制制度、策略和机制;评估了现有的奇瑞与供应商、服务商以及第三方合作方的数据相关的合同文本;核查了奇瑞的数据合规情况,是否曾因不合规事件而受到行业监管机构以及主管部门的关于数据合规方面的重大行政处罚,或遭受与数据合规相关的重大仲裁、诉讼。

为出具本意见书,本所审查了奇瑞所提供的网络安全、数据安全及个人信息保护的有关文件、资料的复印件以及奇瑞以其他介质载体提供的相关资料,以及本所认为需要由奇瑞出具的其他文件、资料的复印件及以其他介质载体装载的资料,且向奇瑞和中华人民共和国有关部门进行了必要的沟通和咨询。

奇瑞保证,其向本所提供的资料、文件及以其他介质承载的资料在所有重大方面均为真实、完整、有效、准确的,其所提供的文件中的所有签名、印章是真实有效的,文件的复印件或其他介质载体中所承载的资料均与原件相符,无任何虚假、隐瞒、重大疏漏、误导或者偏差之处。对于本意见书所必须却又无法得到独立证据证实的事实及情况,本所依赖于中华人民共和国有关部门及其负责人员、奇瑞出具的说明、声明或其他证明文件进行判断。

在本意见书中,本所仅根据自报告期起始之日直至最后实际可行日期,奇瑞提供的已经发生或者存在的事实、文件、资料以及本所对该等事实的了解以及有关法律、法规,对于奇瑞的数据合规事宜具有重大影响的法律问题发表法律意见。在本意见书中,本所仅就奇瑞在中华人民共和国境内(仅就本意见书而言,不含中华人民共和国香港特别行政区、中华人民共和国澳门特别行政区、中华人民共和国台湾地区)运营实体的运营和业务,及公司拟首次公开发行境外上市外资股(H股)并在香港联合交易所有限公司主板上市(以下简称“**本次发行上市**”)所涉及到的中华人民共和国境

内（仅就本意见书而言，不含中华人民共和国香港特别行政区、中华人民共和国澳门特别行政区、中华人民共和国台湾地区）的数据合规法律问题发表意见，而未对关于会计、审计等非法律相关专业事项发表意见。本意见书并不依赖有关会计事务所作出的任何审计报告。

本意见书仅供奇瑞本次发行上市之目的使用，公司可将本意见书提供给本次发行上市所聘请的保荐机构及境内外律师供其合理引用或合理信赖，本所有权对引用的相关内容再次审阅并确认。非经本所书面同意，不得用作任何其他目的。

综上，本所及本所律师按照中华人民共和国律师行业公认的业务标准、职业道德规范以及勤勉尽职原则，对奇瑞提供的文件和有关事实，从数据合规的角度进行充分核查验证。根据现行有效的中华人民共和国有关法律、法规和规范性文件，本所现出具本意见书。

释 义

在本意见书中，除非文义另有所指，下列词语具有下述含义：

奇瑞或集团或公司	指	奇瑞汽车股份有限公司及纳入其合并报表的境内控股子公司
奇瑞汽车	指	奇瑞汽车股份有限公司（不含子公司、分公司）
中伦或本所	指	北京市中伦律师事务所
报告期	指	2022 年 1 月 1 日至 2025 年 3 月 31 日
报告期起始之日	指	2022 年 1 月 1 日
最后实际可行日期	指	2025 年 9 月 10 日
《个人信息保护法》	指	《中华人民共和国个人信息保护法》
《数据安全法》	指	《中华人民共和国数据安全法》
《网络安全法》	指	《中华人民共和国网络安全法》
《网数条例》	指	《网络数据安全管理条例》
《民法典》	指	《中华人民共和国民法典》
《汽车数据若干规定》	指	《汽车数据安全若干规定（试行）》
《工信数据管理办法》	指	《工业和信息化领域数据安全管理办法（试行）》
《暂行办法》	指	《生成式人工智能服务管理暂行办法》
《测绘法》	指	《中华人民共和国测绘法》
《境外上市办法》	指	《境内企业境外发行证券和上市管理试行办法》
《个人信息安全规范》	指	GB/T 35273—2020《信息安全技术 个人信息安全规范》
网络数据或数据	指	任何以电子或者其他方式对信息的记录
个人信息	指	以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息
工业数据	指	工业各行业各领域在研发设计、生产制造、经营管理、运行维护、平台运营等过程中产生和收集的数据

汽车数据	指	汽车设计、生产、销售、使用、运维等过程中的涉及个人信息数据和重要数据
重要数据	指	特定领域、特定群体、特定区域或者达到一定精度和规模，一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能直接危害国家安全、经济运行、社会稳定、公共健康和安全的数据 针对汽车数据，包括： （一）军事管理区、国防科工单位以及县级以上党政机关等重要敏感区域的地理信息、人员流量、车辆流量等数据 （二）车辆流量、物流等反映经济运行情况的数据 （三）汽车充电网的运行数据 （四）包含人脸信息、车牌信息等的车外视频、图像数据 （五）涉及个人信息主体超过 10 万人的个人信息 （六）国家网信部门和国务院发展改革、工业和信息化、公安、交通运输等有关部门确定的其他可能危害国家安全、公共利益或者个人、组织合法权益的数据
生成式人工智能技术	指	具有文本、图片、音频、视频等内容生成能力的模型及相关技术
深度合成技术	指	利用深度学习、虚拟现实等生成合成类算法制作文本、图像、音频、视频、虚拟场景等网络信息的技术，包括但不限于： （一）篇章生成、文本风格转换、问答对话等生成或者编辑文本内容的技术 （二）文本转语音、语音转换、语音属性编辑等生成或者编辑语音内容的技术 （三）音乐生成、场景声编辑等生成或者编辑非语音内容的技术 （四）人脸生成、人脸替换、人物属性编辑、人脸操控、姿态操控等生成或者编辑图像、视频内容中生物特征的技术 （五）图像生成、图像增强、图像修复等生成或者编辑图像、视频内容中非生物特征的技术 （六）三维重建、数字仿真等生成或者编辑数字人物、虚拟场景的技术
百度（图商）	指	北京百度网讯科技有限公司
汽车数据年报（2024 年度）	指	《奇瑞汽车股份有限公司汽车数据安全情况报告（2024 年度）》及《奇瑞新能源汽车股份有限公司汽车数据安全情况报告（2024 年度）》
华为	指	华为技术有限公司
雄狮	指	芜湖雄狮汽车科技有限公司
大卓	指	大卓智能科技有限公司
爱咖	指	爱咖生态科技有限公司

CIIO	指	关键信息基础设施运营者
中国证监会或证监会	指	中国证券监督管理委员会
网信部门	指	中央及地方网络安全和信息化委员会办公室或互联网信息办公室

正文

一、公司处理的数据类型识别

根据《数据安全法》第3条¹和《网数条例》第62条²，目前公司处理的相关信息系通过网络处理和产生且以电子方式记录，属于网络数据/数据范畴。

根据《个人信息保护法》第4条³的规定，结合公司提供的资料，奇瑞处理的相关数据包含用户的姓名、手机号码等，员工的姓名、手机号码、邮箱等数据（具体见“三、个人信息处理”），该等数据可以识别和关联相关个人，属于个人信息。

根据《工信数据管理办法》第3条⁴，结合对奇瑞业务模式的了解，公司处理的相关数据包括汽车工业相关的研发设计、生产制造、经营管理、运行维护、平台运营等数据，属于工业数据。

根据《汽车数据若干规定》第3条⁵，根据公司提供的材料，奇瑞处理的相关数据包括汽车使用过程中的匿名化车外视频、图像数据（部分车型的自动驾驶功能实现（研发训练阶段及量产阶段）、

¹ 《数据安全法》第3条：数据是指任何以电子或者其他方式对信息的记录。

² 《网数条例》第62条（一）：网络数据，是指通过网络处理和产生的各种电子数据。

³ 《个人信息保护法》第4条：个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。

⁴ 《工信数据管理办法》第3条：工业和信息化领域数据包括工业数据、电信数据和无线电数据等。工业数据是指工业各行业各领域在研发设计、生产制造、经营管理、运行维护、平台运营等过程中产生和收集的数据。

⁵ 《汽车数据若干规定》第3条：本规定所称汽车数据，包括汽车设计、生产、销售、使用、运维等过程中的涉及个人信息数据和重要数据。

汽车数据处理，包括汽车数据的收集、存储、使用、加工、传输、提供、公开等。

汽车数据处理者，是指开展汽车数据处理活动的组织，包括汽车制造商、零部件和软件供应商、经销商、维修机构以及出行服务企业等。

重要数据是指一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能危害国家安全、公共利益或者个人、组织合法权益的数据，包括：

- （一）军事管理区、国防科工单位以及县级以上党政机关等重要敏感区域的地理信息、人员流量、车辆流量等数据；
- （二）车辆流量、物流等反映经济运行情况的数据；
- （三）汽车充电网的运行数据；
- （四）包含人脸信息、车牌信息等的车外视频、图像数据；
- （五）涉及个人信息主体超过10万人的个人信息；
- （六）国家网信部门和国务院发展改革、工业和信息化、公安、交通运输等有关部门确定的其他可能危害国家安全、公共利益或者个人、组织合法权益的数据。

哨兵模式）、汽车行踪轨迹信息（部分车型的车辆位置查询功能）、车内人脸信息（部分车型的人脸登录功能）、车联网服务实名信息、车联网功能关联的车辆状态数据等，以及汽车销售、运维过程中的用户数据（例如 App 注册信息）等，属于汽车数据。

其中，根据公司提供的资料及公司的说明，针对哨兵模式所处理的车外视频数据，数据出车时均已对车外人脸和车牌采取匿名化处理方案，其构成重要数据的风险可控；针对自动驾驶功能实现（量产阶段的数据上报、研发阶段的数据训练等）所处理的车外视频数据，奇瑞/星途品牌通过与百度（图商）合作，将在奇瑞云端匿名化处理后再由奇瑞使用，本所律师认为，奇瑞/星途品牌的云端数据在匿名化处理前，可能构成重要数据；此外，根据汽车数据年报（2024 年度），公司处理涉及汽车数据的个人信息约 315 万人，已超过 10 万人，不排除落入重要数据⁶。关于奇瑞是否涉及处理重要数据的分析具体见“二、汽车数据处理”。

根据《测绘法》第 2 条⁷、《自然资源部关于加强智能网联汽车有关测绘地理信息安全管理的通知》第 1 条⁸，智能网联汽车在行驶过程中通过车端传感器采集的车辆及周边道路设施的空间坐标、实景影像（视频和影像等环境感知数据）、点云及其属性信息等属于测绘数据，对此等测绘数据的处理属于测绘活动。根据公司准备的汽车数据年报（2024 年度），公司可能就自动驾驶功能实现（量产、研发阶段）涉及车外视频、图像数据及车外雷达数据，结合公司的说明，目前奇瑞系通过与百度（图商）合作以开展自动驾驶的研发及量产应用活动，奇瑞自身不涉及直接处理测绘数据。

综上，公司在业务开展过程中涉及处理个人信息、汽车数据、工业数据，不涉及直接处理测绘数据。

二、汽车数据⁹处理

⁶ 关于 10 万人个人信息数量门槛，根据《网数条例》第 28 条，网络数据处理者处理 1000 万人以上个人信息的，还应当遵守本条例第三十条、第三十二条对处理重要数据的网络数据处理者作出的规定。鉴于《网数条例》刚刚发布，其与《汽车数据若干规定》的关系尚不清晰，据此，关于超过一定数量个人信息构成重要数据的具体阈值（1000 万人/10 万人），存在不确定性。

⁷ 《测绘法》第 2 条：本法所称测绘，是指对自然地理要素或者地表人工设施的形状、大小、空间位置及其属性等进行测定、采集、表述，以及对获取的数据、信息、成果进行处理和提供的活动

⁸ 《自然资源部关于加强智能网联汽车有关测绘地理信息安全管理的通知》第 1 条：智能网联汽车在运行、服务和测试过程中，对车辆及周边道路设施的空间坐标、实景影像（视频和影像等环境感知数据）、点云及其属性信息等地理信息数据（含道路拓扑数据）进行采集、存储、传输和处理的行为，属于《中华人民共和国测绘法》规定的测绘活动，应依照测绘法律法规进行规范和管理。

⁹ 承前“一、公司处理的数据类型识别”所述，公司涉及处理汽车数据和工业数据。其中，汽车数据是指与汽车相关的个人信息和重要数据，工业数据的范围则可能超过个人信息和重要数据的范畴，但结合《工信数据管理办法》等相关规定，当前监管关注重点

（一）法律要求

针对涉及汽车数据的个人信息处理，根据《数据安全法》第 32 条¹⁰，《工业数据管理办法》第 14 条¹¹，《汽车数据若干规定》第 4 条、第 6-9 条¹²，GB/T 41871-2022《信息安全技术 汽车数据处理安全要求》等规定，要求相关组织在收集、使用个人信息时，应遵循合法、正当、必要的原则，以及车内处理原则和默认不收集原则，通过用户手册、车载显示面板、语音、汽车使用相关应用程序等显著方式告知个人信息处理规则，并获得相关授权同意或具备其他合法性基础。向车外提供车外个人信息前应当进行匿名化处理。处理敏感个人信息还应当满足加强的合规要求（具有直接服务于个人的目的、显著告知必要性及影响、取得单独同意、提示收集状态和终止收集提供便利、10 个工作日内删除（如个人要求）、处理人脸等生物识别信息应具有增强行车安全目的和充分必要性）。此外，汽车数据处理者应当指定用户权益事务联系人。

仍在于属于个人信息和重要数据的工业数据，故从监管实质层面二者可视为等同。同时，鉴于《工信数据管理办法》关于数据收集、处理的规定较为泛化，且就车企而言，《汽车数据若干规定》等针对汽车数据的监管规则重要性更强，故本部分集中以汽车数据在收集、处理层面的合规要求展开，仅在必要时提及《工信数据管理办法》等关于工信数据的监管要求。下同。

¹⁰ 《数据安全法》第 32 条：任何组织、个人收集数据，应当采取合法、正当的方式，不得窃取或者以其他非法方式获取数据。

¹¹ 《工业数据管理办法》第 14 条：工业和信息化领域数据处理者收集数据应当遵循合法、正当的原则，不得窃取或者以其他非法方式收集数据。

¹² 《汽车数据若干规定》

第 4 条：汽车数据处理者处理汽车数据应当合法、正当、具体、明确，与汽车的设计、生产、销售、使用、运维等直接相关。

第 6 条：国家鼓励汽车数据依法合理有效利用，倡导汽车数据处理者在开展汽车数据处理活动中坚持：车内处理原则，除非确有必要不向车外提供；（二）默认不收集原则，除非驾驶人自主设定，每次驾驶时默认设定为不收集状态；（三）精度范围适用原则，根据所提供功能服务对数据精度的要求确定摄像头、雷达等的覆盖范围、分辨率；（四）脱敏处理原则，尽可能进行匿名化、去标识化等处理。

第 7 条：汽车数据处理者处理个人信息应当通过用户手册、车载显示面板、语音、汽车使用相关应用程序等显著方式，告知个人以下事项：（一）处理个人信息的种类，包括车辆行驶轨迹、驾驶习惯、音频、视频、图像和生物识别特征等；（二）收集各类个人信息的具体情境以及停止收集的方式和途径；（三）处理各类个人信息的目的、用途、方式；（四）个人信息保存地点、保存期限，或者确定保存地点、保存期限的规则；（五）查阅、复制其个人信息以及删除车内、请求删除已经提供给车外的个人信息的方式和途径；（六）用户权益事务联系人的姓名和联系方式；（七）法律、行政法规规定的应当告知的其他事项。

第 8 条：汽车数据处理者处理个人信息应当取得个人同意或者符合法律、行政法规规定的其他情形。

因保证行车安全需要，无法征得个人同意采集到车外个人信息且向车外提供的，应当进行匿名化处理，包括删除含有能够识别自然人的画面，或者对画面中的人脸信息等进行局部轮廓化处理等。

第 9 条：汽车数据处理者处理敏感个人信息，应当符合以下要求或者符合法律、行政法规和强制性国家标准等其他要求：（一）具有直接服务于个人的目的，包括增强行车安全、智能驾驶、导航等；（二）通过用户手册、车载显示面板、语音以及汽车使用相关应用程序等显著方式告知必要性以及对个人的影响；（三）应当取得个人单独同意，个人可以自主设定同意期限；（四）在保证行车安全的前提下，以适当方式提示收集状态，为个人终止收集提供便利；（五）个人要求删除的，汽车数据处理者应当在十个工作日内删除。

汽车数据处理者具有增强行车安全的目的和充分的必要性，方可收集指纹、声纹、人脸、心律等生物识别特征信息。

针对涉及汽车数据的重要数据处理，根据《网数条例》第 31 条、第 33 条¹³，《汽车数据若干规定》第 10 条、第 13 条¹⁴，GB/T 41871-2022《信息安全技术 汽车数据处理安全要求》，重要数据处理者应当指定汽车数据安全负责人，针对提供、委托处理、共同处理等重要数据处理活动开展风险评估，并向主管部门报送年度汽车数据安全情况（即汽车数据年报）。

此外，根据《汽车数据若干规定》第 17 条¹⁵，汽车数据处理者应建立投诉举报渠道，设置便捷

¹³ 《网数条例》

第 31 条：重要数据的处理者提供、委托处理、共同处理重要数据前，应当进行风险评估，但是属于履行法定职责或者法定义务的除外。

风险评估应当重点评估下列内容：（一）提供、委托处理、共同处理网络数据，以及网络数据接收方处理网络数据的目的、方式、范围等是否合法、正当、必要；（二）提供、委托处理、共同处理的网络数据遭到篡改、破坏、泄露或者非法获取、非法利用的风险，以及对国家安全、公共利益或者个人、组织合法权益带来的风险；（三）网络数据接收方的诚信、守法等情况；（四）与网络数据接收方订立或者拟订立的相关合同中关于网络安全的要求能否有效约束网络数据接收方履行网络安全保护义务；（五）采取或者拟采取的技术和管理措施等能否有效防范网络数据遭到篡改、破坏、泄露或者非法获取、非法利用等风险；（六）有关主管部门规定的其他评估内容。

第 33 条：重要数据的处理者应当每年度对其网络数据处理活动开展风险评估，并向省级以上有关主管部门报送风险评估报告，有关主管部门应当及时通报同级网信部门、公安机关。

风险评估报告应当包括下列内容：

（一）网络数据处理者基本信息、网络数据安全管理机构信息、网络数据安全负责人姓名和联系方式等；（二）处理重要数据的目的、种类、数量、方式、范围、存储期限、存储地点等，开展网络数据处理活动的情况，不包括网络数据内容本身；（三）网络数据安全管理制度及实施情况，加密、备份、标签标识、访问控制、安全认证等技术措施和其他必要措施及其有效性；（四）发现的网络数据安全风险，发生的网络数据安全事件及处置情况；（五）提供、委托处理、共同处理重要数据的风险评估情况；（六）网络数据出境情况；（七）有关主管部门规定的其他报告内容。

处理重要数据的大型网络平台服务提供者报送的风险评估报告，除包括前款规定的内容外，还应当充分说明关键业务和供应链网络安全等情况。

重要数据的处理者存在可能危害国家安全的重要数据处理活动的，省级以上有关主管部门应当责令其采取整改或者停止处理重要数据等措施。重要数据的处理者应当按照有关要求立即采取措施。

¹⁴ 《汽车数据若干规定》

第 10 条：汽车数据处理者开展重要数据处理活动，应当按照规定开展风险评估，并向省、自治区、直辖市网信部门和有关部门报送风险评估报告。

风险评估报告应当包括处理的重要数据的种类、数量、范围、保存地点与期限、使用方式，开展数据处理活动情况以及是否向第三方提供，面临的数据安全风险及其应对措施等。

第 13 条：汽车数据处理者开展重要数据处理活动，应当在每年十二月十五日前向省、自治区、直辖市网信部门和有关部门报送以下年度汽车数据安全情况：

（一）汽车数据安全负责人、用户权益事务联系人的姓名和联系方式；（二）处理汽车数据的种类、规模、目的和必要性；（三）汽车数据的安全防护和管理措施，包括保存地点、期限等；（四）向境内第三方提供汽车数据情况；（五）汽车数据安全事件和处置情况；（六）汽车数据相关的用户投诉和处理情况；（七）国家网信部门会同国务院工业和信息化、公安、交通运输等有关部门明确的其他汽车数据安全情况。

¹⁵ 《汽车数据若干规定》第 17 条：汽车数据处理者开展汽车数据处理活动，应当建立投诉举报渠道，设置便捷的投诉举报入口，及时处理用户投诉举报。

的投诉举报入口，及时处理用户投诉举报。

针对测绘数据处理，根据《测绘法》第 27 条¹⁶、《测绘资质管理办法》第 1 条¹⁷、《自然资源部关于加强智能网联汽车有关测绘地理信息安全管理的通知》等规定，开展测绘活动应当具备测绘资质，尤其针对导航电子地图相关数据，无测绘资质主体不得接触。

（二）合规事实

1. 涉及汽车数据的个人信息

针对座舱数据、车联网相关个人信息（行踪轨迹、车联网实名信息等）的处理情况如下：

	奇瑞/星途 ¹⁸	捷途	智界	iCAR
默认不收集座舱数据情况	1. 语音识别/相机功能：在车辆激活时会进行弹窗提醒，用户点击同意后，才会开启该功能（只在车端处理，云端不存储）。 2. DMS 功能：在车辆个人中心注册时进行授权同意。都是默认关闭，只有在用户同意后，才会打开。并且用户可以自行关闭该功能（只在车端处理，云端不存储）。 3. 人脸登录功能：在注册时会采集人脸信息，需经过车主确认点击后进行采集（涉及云端存储特征值）。	1. 语音识别/相机功能：不会主动收集，必须通过车机按键或者唤醒词激活此功能收集数据。 2. DMS 驾驶员状态监控：默认关闭，用户需要在设置中开启对应功能。 3. OMS 车内监测：不会主动收集，仅在锁车后识别出车内人员/物品遗留场景下触发，且不涉及车内数据外发。		1. 语音助手服务：不会主动收集，必须通过车机按键或者唤醒词激活此功能收集音频数据。 2. DMS 驾驶员状态监控：默认关闭，用户需要在设置中开启对应功能。

¹⁶ 《中华人民共和国测绘法》第 27 条：国家对从事测绘活动的单位实行测绘资质管理制度。

从事测绘活动的单位应当具备下列条件，并依法取得相应等级的测绘资质证书，方可从事测绘活动：

（一）有法人资格；（二）有与从事的测绘活动相适应的专业技术人员；（三）有与从事的测绘活动相适应的技术装备和设施；（四）有健全的技术和质量保证体系、安全保障措施、信息安全保密管理制度以及测绘成果和资料档案管理制度。

¹⁷ 《测绘资质管理办法》第 1 条：在中华人民共和国领域和中华人民共和国管辖的其他海域从事测绘活动的单位，应当依照本办法的规定取得测绘资质证书，并在测绘资质等级许可的专业类别和作业限制范围内从事测绘活动。

¹⁸ 涉及瑞虎系列、艾瑞泽系列、星途系列车型。

	奇瑞/星途 ¹⁸	捷途	智界	iCAR
座舱数据车内处理情况	1. 语音功能：部分车内处理，根据车辆功能进行定义，为提高识别的准确率，部分语音会传到云端进行分析处理，返回识别后的指令，但不会进行云端存储，识别完成后即丢弃；相机功能：不会进行云端存储。 2. DMS：在识别到人脸数据后，会进行车辆内部处理，处理完成后即刻丢弃，不存储。 3. 人脸登录功能：会将采集的特征值（已加密）进行云端存储，便于下次登录时的信息比对，确保信息的准确性。此外，处理个人信息的显著告知包含：车载显示面板弹窗提示、汽车使用相关应用程序交互、App 注册协议条款等。	没有对应数据上传至云端，采集策略如下： 1. DVR 行车记录仪：自带 32GB 本地存储，4 小时循环覆盖。 2. 360 全景影像：带拍照功能，存储上限为 34GB，本地存储（系统总内存 64GB，可用于拍照的存储内存为剩余内存）。 3. DMS 驾驶员状态监测：识别到人脸数据后，会进行车辆内部处理，处理完成后即刻丢弃，不存储。 4. OMS 车内监测：识别到车内状态后，会进行车辆内部处理，处理完成后即刻丢弃，不存储。 5. 语音助手服务：语音数据全部在车内处理，不上传至云端。		没有对应数据上传至云端，采集策略如下： 1. DVR 行车记录仪：自带 32GB 本地存储，4 小时循环覆盖。 2. 360 全景影像：带拍照功能，存储上限为 34GB，本地存储（系统总内存 64GB，可用于拍照的存储内存为剩余内存）。 3. ADAS 辅助驾驶：不存储数据，不上传至云端。 4. DMS 驾驶员状态监测：识别到人脸数据后，会进行车辆内部处理，处理完成后即刻丢弃，不存储。 5. 语音助手服务：语音数据处理全部在车内处理，不上传至云端。
车联网相关个人信息	1. 汽车行踪轨迹信息（车辆位置查询信息服务）。 2. 其他个人信息：App 注册信息、车联网实名信息、车辆状态数据，其目的为提供车联网服务以查询车辆状态。	1. 汽车行踪轨迹信息（车辆位置查询信息服务）。 2. 其他个人信息：App 注册信息、车联网实名信息、车辆状态数据，其目的为提供车联网服务以查询车辆状态。	1. 其他个人信息：（华为-鸿蒙 App）App 注册信息、车辆状态数据、车联网实名信息。	1. 汽车行踪轨迹信息（车辆位置查询信息服务）。 2. 其他个人信息：App 注册信息、车联网业务信息（实名认证信息、车辆状态数据）。

针对上述个人信息处理活动，各品牌采取的显著告知方式包括：

- 奇瑞/星途：车载显示面板弹窗提示，用户手册单独条款提示，汽车使用相关应用程序交互，官网、公众号发布通知公示，App 协议条款。



- 捷途：车载显示面板弹窗提示，用户手册单独条款提示，官网、公众号发布通知公示, App 协议条款。
- 智界：车载显示面板弹窗提示，用户手册单独条款提示，汽车使用相关应用程序交互，App 协议条款。
- iCAR：车载显示面板弹窗提示，用户手册单独条款提示，汽车使用相关应用程序交互，官网、公众号发布通知公示。

此外，针对汽车座舱个人信息的安全保护，已通过中国汽车技术研究中心安全保护认证，符合 CASTC-A1-2024《整车个人信息安全保护测试规程》的要求。

其中，根据公司的说明，针对智界品牌，车联网服务由华为提供，相关数据处理活动由华为负责和控制，奇瑞仅在车机端部分涉及整车厂功能的隐私政策中作为数据处理者对外披露。

2. 涉及汽车数据的重要数据

针对车外人脸、车牌数据的处理情况如下：

	奇瑞/星途（E03 及 E0Y）	智界（S7 及 R7）	捷途	iCAR
车 外 人 脸、 车 牌 数 据 处 理 情 况	1. 哨兵模式：车外图像（如人脸、车牌等）等数据均在车端进行匿名化处理后，传输车外的云端服务。 2. 自动驾驶功能（自动驾驶数据的上报及训练）：符合《TC260-001 汽车采集数据处理安全指南》中 5.3a 的要求，引入了百度（图商）。车外图像（如人脸、车牌等）等数据由百度（图商）在奇瑞云端先行处理，对人脸、车牌、重要地理信息等脱敏后，再由奇瑞使用。	1. 哨兵模式：车主可通过车机 OOB 页面签署隐私协议，若未签署则无法使用该功能，车主可自行查看车内非匿名化人脸信息，数据出车时会对人脸和车牌号进行匿名化处理；定期 3-6 个月删除一次。 2. 智驾模式：车主可通过车机 OOB 页面签署隐私协议，若未签署则无法使用该功能；该功能涉及图像数据出车收集时会对图像数据加密、匿名化处理，定期 3-6 个月删除一次。	无哨兵模式，不涉及处理车外人脸、车牌数据； 无 L3 级以上自动驾驶功能，不涉及处理车外人脸、车牌数据。	无哨兵模式，不涉及处理车外人脸、车牌数据； 无 L3 级以上自动驾驶功能，不涉及处理车外人脸、车牌数据。

此外，在个人信息数量层面，根据公司准备的汽车数据年报（2024 年度），公司截至 2024 年底处理的涉及汽车数据的个人信息约为 315 万人（已超过 10 万人）。

根据公司提供的汽车数据年报（2024 年度），目前奇瑞汽车已指定某副总经理作为汽车数据安全负责人，并指定数据合规部负责人作为用户权益事务联系人；奇瑞新能源汽车股份有限公司已指定总经理作为汽车数据安全负责人，总监作为用户权益事务联系人。此外，根据公司的说明及提供的隐私政策模版，奇瑞已建立 400 投诉举报渠道，通过车机端隐私政策等方式对外披露。

同时，公司已制定《C032404-W-01 汽车数据分级分类管理规定》《C032404-W-02 汽车数据全生命周期安全管理规定》《C0304-W-02 汽车数据安全风险评估管理规定》。其中《C0304-W-02 汽车数据安全风险评估管理规定》规定了提供、委托处理、共同处理等重要数据处理活动开展风险评估流程。在分类分级层面，根据公司的说明，目前公司正在按照项目制逐步推进涉及汽车数据的分类分级工作。此外，公司已定期向主管部门提交汽车数据年报。

3. 车联网数据及测绘数据整体处理情况

针对奇瑞/星途、捷途品牌：在量产阶段，目前相关隐私政策以奇瑞汽车作为数据处理者对外披露，并由奇瑞集团内雄狮负责提供车联网服务，针对车联网服务所涉及的相关数据处理活动，奇瑞汽车与雄狮系委托关系，双方已签订《数据委托处理协议》。根据公司提供的梳理情况，目前雄狮车联网平台相关系统已取得等保三级备案。在研发阶段，由奇瑞集团内大卓开展自动驾驶研发并处理相关数据，具体数据处理关系为，奇瑞汽车与雄狮签署《数据委托处理协议》（同前），雄狮进一步与大卓签订《数据共享与保护协议》。

针对智界品牌：目前系由奇瑞与华为合作，具体车联网服务由华为提供，车联网的相关数据处理活动由华为负责和控制。

针对 iCAR 品牌：根据公司提供的《iCAR 汽车隐私政策》，其披露的数据处理者为爱咖（奇瑞新能源汽车股份有限公司的全资子公司），并在《iCAR 汽车隐私政策》中披露由关联公司（雄狮）提供车联网服务并处理相关数据的事实，且爱咖与雄狮已签署《数据委托处理协议》。

在测绘数据方面，奇瑞/星途实现自动驾驶功能过程（研发阶段数据训练、量产阶段数据上报）还涉及车外视频、图像数据以及车外雷达数据等测绘数据，目前系通过引入百度（图商）在奇瑞云环境中开展测绘数据处理，并进行车外人脸、车牌以及地理位置脱敏等达到监管要求的脱敏处理后，再由雄狮/大卓处理脱敏后的数据。

（三）合规评估



1. 涉及汽车数据的个人信息

在合法性层面：

- 首先，目前奇瑞/星途、捷途、智界、iCAR 品牌车型的语音识别/相机功能、DMS 驾驶员状态监控功能、OMS 车内监测功能、人脸识别登录功能等符合《汽车数据若干规定》、GB/T 41871-2022《信息安全技术 汽车数据处理安全要求》第 6.1 条等规定关于默认不收集座舱数据的合规要求。
- 其次，针对座舱数据出车的情况：奇瑞/星途品牌车型的 DMS 功能，以及捷途、智界、iCAR 品牌车型的 DVR 行车记录仪功能、360 全景影像（拍照）功能、ADAS 辅助驾驶功能、DMS 驾驶员状态监控功能、OMS 车内监测功能、语音助手服务等符合《汽车数据若干规定》、GB/T 41871-2022《信息安全技术 汽车数据处理安全要求》第 6.2 条等规定关于车内处理的要求；此外，针对奇瑞/星途品牌车型的语音功能，其符合 GB/T 41871-2022《信息安全技术 汽车数据处理安全要求》第 6.2 条关于语音数据车外分析处理的例外场景，而针对奇瑞/星途品牌车型的人脸登录功能，其符合《汽车数据若干规定》、GB/T 41871-2022《信息安全技术 汽车数据处理安全要求》第 4.4 条关于基于行车安全目的而处理人脸等生物识别信息。
- 针对其他车联网相关个人信息，包括汽车行踪轨迹信息、App 注册信息、车联网实名信息、车辆状态数据等，已具备《个人信息保护法》第 13 条“同意”或“履行合同所必需”的合法性基础，且已通过一系列显著方式进行告知（见下），本所律师认为在所有重大方面符合《个人信息保护法》《汽车数据若干规定》关于合法性的要求。

在告知层面，根据车型不同，告知的具体方式略有差别，但在所有重大方面前述场景均已进行显著告知，符合《汽车数据若干规定》第 7 条的要求。

2. 涉及汽车数据的重要数据

结合前述合规事实，针对哨兵模式所处理的车外视频数据，其构成重要数据的风险可控；针对自动驾驶功能实现（量产阶段的数据上报、研发阶段的数据训练等）所处理的车外视频数据，本所律师认为，奇瑞/星途品牌的云端数据在匿名化处理前，可能构成重要数据，但在现有方案下，奇瑞均不涉及直接接触、处理此等重要数据。

同时，由于奇瑞处理的涉及汽车数据的个人信息已超过 10 万人，根据《汽车数据若干规定》第

3 条，此等超过 10 万人的个人信息属于重要数据，进而需遵循《汽车数据若干规定》关于重要数据处理者的义务。具体而言：

公司已指定汽车数据安全负责人及用户权益事务联系人，已建立投诉举报渠道。同时，公司已制定汽车数据相关合规制度，规定了提供、委托处理、共同处理等重要数据处理活动开展风险评估的要求，并正在逐步推进和刷新涉及汽车数据的分类分级工作，且公司定期向主管部门报送年度汽车数据安全情况（即汽车数据年报），在所有重大方面符合《汽车数据若干规定》关于重要数据处理者的合规要求。

3. 车联网相关数据及测绘数据整体处理情况

针对车联网相关数据，现行法律法规及监管实践并未强制要求车联网相关数据必须由整车厂（汽车制造企业）直接处理和控制在，但原则上要求数据处理链条及责任主体明确，具体体现为数据处理协议的签订情况及外部隐私政策等文本的披露情况。就奇瑞/星途、捷途品牌，在量产阶段，均以奇瑞汽车作为数据处理者在隐私政策中对外披露，并在隐私政策的委托处理章节明确将委托关联公司（即雄狮）处理车联网服务相关数据，同时，奇瑞汽车与雄狮签署《数据委托处理协议》，本所律师认为此等合规方案符合当前的法律法规及监管实践；在研发阶段，则由大卓负责车联网服务相关数据处理，具体数据处理关系为，奇瑞汽车与雄狮签署《数据委托处理协议》（同前），雄狮进一步与大卓签订《数据共享与保护协议》。最后，针对 iCAR 品牌，在《iCAR 汽车隐私政策》作为数据处理者的爱咖已与雄狮签署《数据委托处理协议》。

针对自动驾驶功能实现过程中涉及的测绘数据，目前奇瑞系通过与百度（图商）合作，由百度（图商）脱敏并达到监管要求的程度后，再由奇瑞处理，本所律师认为此等处理方案与当前的行业合规实践一致，在所有重大方面符合《测绘法》《测绘资质管理办法》《自然资源部关于加强智能网联汽车有关测绘地理信息安全管理的通知》等关于无测绘资质主体不得接触（原始）测绘数据的合规要求。

综上，本所律师认为公司对于汽车数据的处理在所有重大方面符合《数据安全法》《网数条例》《汽车数据若干规定》《测绘法》等相关规定，不存在可能对本次上市构成重大法律障碍的违法违规事项。

三、个人信息处理¹⁹

（一）个人信息收集

1. 法律要求

根据《个人信息保护法》第6条的规定，个人信息的收集应该满足最小必要原则的要求，收集个人信息，应当限于实现处理目的的最小范围，不得过度收集个人信息。根据《民法典》第1035条²⁰、《网络安全法》第41条²¹及《个人信息保护法》第13条²²规定，公司在收集、使用用户个人信息前，应明确告知用户个人信息处理规则，并获得其授权同意或具备其他合法性基础。根据《网数条例》第22条规定，公司不得在个人明确表示不同意处理其个人信息后，频繁征求同意。

根据《个人信息保护法》第17条、第30条以及《网数条例》第21条的规定，处理个人信息时应向个人告知个人信息处理者的名称或者姓名和联系方式；个人信息处理目的、处理方式、处理种类、保存期限及到期后的处理方式（保存期限难以确定的，应当明确保存期限的确定方法）；个人行使本法规定权利的方式和程序（包括个人查阅、复制、转移、更正、补充、删除、限制处理个人信息以及注销账号、撤回同意的的方法和途径等）。处理敏感个人信息还应向个人告知处理敏感个人信息的必要性以及对个人权益的影响。《网数条例》第21条规定，通过制定个人信息处理规则的方式依法向个人告知的，个人信息处理规则应当集中公开展示、易于访问并置于醒目位置，内容明确具体、清晰易懂。网络数据处理者向个人告知收集和向其他网络数据处理者提供个人信息的目的、方式、种类以及网络数据接收方信息的，应当以清单等形式予以列明。同时，App个人信息保护一直

¹⁹ 承前“一、公司处理的数据类型识别”，本部分不包含“涉及汽车数据的个人信息”。

²⁰ 《民法典》第1035条：处理个人信息的，应当遵循合法、正当、必要原则，不得过度处理，并符合下列条件：（一）征得该自然人或者其监护人同意，但是法律、行政法规另有规定的除外；（二）公开处理信息的规则；（三）明示处理信息的目的、方式和范围；（四）不违反法律、行政法规的规定和双方的约定。

²¹ 《网络安全法》第41条：网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。网络运营者不得收集与其提供的服务无关的个人信息，不得违反法律、行政法规的规定和双方的约定收集、使用个人信息，并应当依照法律、行政法规的规定和与用户的约定，处理其保存的个人信息。

²² 《个人信息保护法》第13条：符合下列情形之一的，个人信息处理者方可处理个人信息：（一）取得个人的同意；（二）为订立、履行个人作为一方当事人的合同所必需，或者按照依法制定的劳动规章制度和依法签订的集体合同实施人力资源管理所必需；（三）为履行法定职责或者法定义务所必需；（四）为应对突发公共卫生事件，或者紧急情况下为保护自然人的生命健康和财产安全所必需；（五）为公共利益实施新闻报道、舆论监督等行为，在合理的范围内处理个人信息；（六）依照本法规定在合理的范围内处理个人自行公开或者其他已经合法公开的个人信息；（七）法律、行政法规规定的其他情形。

依照本法其他有关规定，处理个人信息应当取得个人同意，但是有前款第二项至第七项规定情形的，不需取得个人同意。

是工业和信息化部等监管部门的执法重点，按照工业和信息化部的整治行动说明，“小程序”同样纳入到 App 个人信息保护执法行动的审查范围内，并参照 App 个人信息保护相关要求进行了合规审查

²³。

根据《网数条例》第 24 条规定，因使用自动化采集技术等无法避免采集到非必要个人信息或者未依法取得个人同意的个人信息，以及个人注销账号的，网络数据处理者应当删除个人信息或者进行匿名化处理。

2. 合规事实

公司当前收集个人信息的渠道可分为直接收集与间接收集，涉及收集个人信息的主体类型包括潜在客户、C 端消费者（主要为车主）、合作方（例如经销商、供应商等）员工、公司内部员工、候选人。截至 2025 年 8 月 18 日，涉及中华人民共和国境内（仅就本意见书而言，不含中华人民共和国香港特别行政区、中华人民共和国澳门特别行政区、中华人民共和国台湾地区）个人信息主体规模如下：

总计（未去重）	各品牌所涉数量
潜在客户：约 2560 万人	奇瑞/星途：约 1410 万人 捷途：约 800 万人 iCAR：约 350 万人
车主：约 307 万人	奇瑞/星途：奇瑞 2024 年约 70 万人；星途约 30 万人 捷途：150 万人 iCAR：约 54 万人 智界：约 3 万人
合作方员工：约 14.14 万人	经销商员工：11.29 万人 供应商员工：约 2.85 万人
公司内部员工：约 2.3 万人	奇瑞/星途：约 0.3 万人 捷途：约 1.3 万人 iCAR：约 0.5 万人 智界：约 0.2 万人
候选人：2025 年约 6.5 万人	奇瑞/星途：约 1.6 万人 捷途：约 2.6 万人 iCAR：约 0.3 万人 智界：约 2 万人

²³ 根据《工业和信息化部关于开展纵深推进 APP 侵害用户权益专项整治行动的通知》规定，APP 指可以下载、安装、升级的应用软件，包括小程序等新应用形态。根据全国信息安全标准化技术委员会秘书处发布的《关于发布〈网络安全标准实践指南-移动互联网应用程序（App）收集使用个人信息自评估指南〉的通知》（信安秘字[2020] 40 号）说明，小程序等运营者可参考《网络安全标准实践指南-移动互联网应用程序（App）收集使用个人信息自评估指南》的适用条款进行自评估。

1) 直接收集

从业务流程层面，公司主要在购车业务、经销商及供应商等合作方管理、员工管理、招聘管理四个方面涉及直接收集个人信息。其中购车业务涉及直接收集个人信息的环节包括潜在客户营销、试乘试驾、车辆销售、车主关系管理及运营、售后支持、增值服务、客户服务、客户调研，收集的个人信息主要为个人基本资料、个人身份信息、车辆信息、车辆相关服务信息、网络身份标识信息及设备信息、位置信息等；经销商、供应商等合作方管理主要涉及收集合作方员工的个人基本资料、个人工作信息、网络身份标识信息及设备信息等；员工管理主要涉及收集员工的个人基本资料、个人身份信息、个人教育工作信息，以及与薪酬发放、报销及考勤相关的金融账户、生物识别、打卡位置信息等；招聘管理主要涉及收集候选人的个人基本信息、个人教育工作信息等。具体个人信息收集渠道/目的及类型见附件 1。

从在线产品层面，在购车业务中，公司通过自有网站、App、小程序提供潜在客户营销、试乘试驾、车辆销售、车主关系管理及运营、售后支持、增值服务、客户服务等在线业务流程，以及注册登录、经销商或服务网点查询、车辆绑定及远程车辆管理等其他类型的在线服务。此外，公司额外收集与特定在线服务有关的个人信息。公司在核心业务中运营的主要在线产品及收集个人信息场景见附件 2。

除上述场景外，根据公司提供的资料，公司运营过程中开展大数据爬取活动，但不涉及收集个人信息。公司留存了大数据爬取活动的操作日志可供审计和评估。

2) 间接收集

根据公司提供的资料，公司主要在潜在客户营销、试乘试驾、车辆销售、客户调研、售后协助（智界）、经销商员工管理、招聘管理的业务场景中从第三方间接收集个人信息。其中，潜在客户营销、试乘试驾、车辆销售场景中，公司会通过第三方社交、直播或短视频、电商平台获得潜在客户留资、预约信息和购车订单；客户调研场景中，公司会委托第三方调研公司开展线下座谈会并收集参会人员信息；售后协助场景中，公司经营的智界品牌车型会从华为获得车主的有关售后反馈、保修索赔和客诉信息以提供车辆售后相关服务；经销商员工管理场景中，公司会通过使用腾讯提供的企业微信应用收集经销商准入资料、进行人员管理、开展培训等；招聘管理场景中，公司会通过第三方招聘平台、第三方提供的招聘系统和背景调查服务收集候选人的有关信息。

3. 合规评估

1) 直接收集

业务场景			合法性评估	
业务环节	个人信息主体类型	个人信息收集渠道/目的	对个人信息处理活动进行告知	取得有效的合法性基础
购车业务				
潜在客户营销	C 端消费者（潜在客户）	- 潜在客户在公司自有 App、小程序和网站留资 - 潜在客户在车展等线下活动或经销商线下留资	- 公司已通过产品隐私政策中的“购车咨询”“信息推送”等目的实现有关告知； - 公司已在线下配置相应的个人信息收集告知文本。	<u>适用个人信息主体授权同意的合法性基础。</u> - 公司已通过允许用户勾选隐私政策的方式获得授权同意； - 公司已通过允许个人信息主体签署同意告知文本的方式获得授权同意。
试乘试驾	C 端消费者（潜在客户）	- 通过自有小程序、App、网站进行预约 - 实际体验服务	- 公司通过自有小程序、App 及网站的隐私政策告知用户试乘试驾场景的个人信息收集情况。 - 试驾用户在实际体验服务前需签订纸质版试驾协议，其中包含个人信息处理条款并告知了驾驶证等证件信息的收集和处理情况。	<u>在预约试驾时适用个人信息主体的授权同意的合法性基础。</u> - 公司通过自有小程序、App 及网站预约试驾页面允许用户勾选隐私政策的方式取得同意。 <u>在实际体验服务时适用为订立、履行个人作为一方当事人的合同所必需的合法性基础。</u> - 在实际体验服务前，试驾用户需签订试驾协议，符合前述合法性基础的适用条件。
车辆销售	车主	- 通过经销商购车 - 通过公司自有小程序、App 及网站订购 - 开通、购买 SIM 卡流量	- 公司通过自有小程序、App 及网站隐私政策和向车主提供的《个人信息收集处理知情同意书》进行告知。	<u>适用为订立、履行个人作为一方当事人的合同所必需的合法性基础。</u> - 车主在购买车辆时需签订购车合同，符合前述合法性基础的适用条件；且公司允许车主在购车时签署《个人信息收集处理知情同意书》以获得同意。
车主关系管理	车主	- 建立车主档案 - 通过公司自有小程序、App 及网站等进行社区运营及内容传播	- 公司通过购车时向车主提供的《个人信息收集处理知情同意书》告知建立车主档案的个人信息处理场景，并告知车主信息将	<u>适用个人信息主体授权同意的合法性基础。</u> - 公司通过允许车主签署《个人信息收集处理知情同意书》取得个人信息主体的授权同意。

业务场景			合法性评估	
业务环节	个人信息主体类型	个人信息收集渠道/目的	对个人信息处理活动进行告知	取得有效的合法性基础
及运营		- 活动组织 - KOC 客户运营 - 售后营销	- 被用于服务跟踪、电话回访、客户调研、营销推广、活动邀请等目的。 - 公司亦通过自有小程序、App 及网站隐私政策告知社区运营及内容传播、活动报名等处理场景。	- 公司在自有小程序、App 及网站注册登录页面允许用户勾选隐私政策以获得授权同意。
售后支持	车主	- 保修管理与索赔 - 维修保养 - 道路救援 - 车辆故障检测	- 公司通过购车时向车主提供的《个人信息收集处理知情同意书》对车辆售后、车辆保养和维修服务场景进行告知，并在 App 隐私政策中告知了维修保养及道路救援的处理场景。	<u>适用为订立、履行个人作为一方当事人的合同所必需及为履行法定义务所必需的合法性基础。</u> - 针对车辆售后服务，公司系依据车主签署的购车合同履行合同义务，且依据《家用汽车产品修理、更换、退货责任规定》履行法定义务，具备合法性基础。
增值服务	车主/C 端消费者	- 车辆充电服务 - 家用充电桩服务 - 车辆续保服务 - 周边产品销售或奖励发放 - 旧车置换咨询业务	- 公司通过自有 App、小程序、网站隐私政策告知了相应个人信息处理场景。	<u>适用个人信息主体授权同意的合法性基础。</u> - 公司在自有小程序、App 及网站注册登录页面允许用户勾选隐私政策。
客户服务	车主/C 端消费者	- 服务记录	- 公司通过自有 App、小程序、网站隐私政策告知了客户服务的个人信息处理场景。 - 公司客服提供服务前均会提示来电个人电话将被录音。	<u>适用个人信息主体授权同意的合法性基础。</u> - 公司在自有小程序、App 及网站注册登录页面允许用户勾选隐私政策。

业务场景			合法性评估	
业务环节	个人信息主体类型	个人信息收集渠道/目的	对个人信息处理活动进行告知	取得有效的合法性基础
客户调研	车主/C 端消费者	- 车主回访及调研 - 部分品牌（星途）会在产品上市前后开展调研、举办用户座谈等活动	公司通过购车时向车主提供的《个人信息收集处理知情同意书》对客户调研目的进行告知。	<u>适用个人信息主体授权同意的合法性基础。</u> 公司通过允许车主签署《个人信息收集处理知情同意书》取得个人信息主体的授权同意。
B 端合作方管理				
经销商管理	经销商员工	通过自有网站进行经销商加盟	公司通过自有网站所提供的隐私政策进行告知。	<u>收集加盟意向：适用个人信息主体授权同意的合法性基础，或适用按照依法制定的劳动规章制度和依法签订的集体合同实施人力资源管理所必需的合法性基础。</u> 在通过网站收集加盟意向信息时，公司通过允许个人信息主体勾选隐私政策的方式获得同意。另一方面，经销商员工向公司提供其个人信息亦属于自身在供职单位的履职行为，由经销商作为个人信息处理者确保具备有关合法性基础。
供应商管理	供应商员工	- 注册 - 访客管理	在供应商准入时的 SRM 系统注册页面中，公司通过《注册条款》中个人信息保护条款告知将对用户个人信息进行处理。	<u>适用个人信息主体授权同意，或适用按照依法制定的劳动规章制度和依法签订的集体合同实施人力资源管理所必需的合法性基础。</u> 在公司供应商准入时的 SRM 系统注册页面中，系统用户通过签署《注册条款》中个人信息保护条款进行同意。另一方面，供应商员工向公司提供其个人信息亦属于自身在供职单位的履职行为，其合法性取决于供应商作为个人

业务场景			合法性评估	
业务环节	个人信息主体类型	个人信息收集渠道/目的	对个人信息处理活动进行告知	取得有效的合法性基础
				信息处理者是否有效具备前述合法性基础，公司反馈已通过协议的方式统一对供应商提出数据合规要求。整体公司未存在重大违反法律法规要求的情况。
员工管理				
员工管理	公司员工	- 建立员工档案 - 薪酬福利管理 - 因公差旅与报销 - 考勤管理	- 公司通过《奇瑞员工隐私政策》向公司员工告知个人信息处理情况。	<u>适用按照依法制定的劳动规章制度和依法签订的集体合同实施人力资源管理所必需的合法性基础。</u> - 公司已具备前述合法性基础。
招聘管理				
招聘管理	候选人	- 招聘管理	- 公司通过《奇瑞应聘者隐私政策》向候选人告知个人信息处理情况。	<u>适用个人信息主体授权同意的合法性基础。</u> - 公司在面试阶段允许候选人线上勾选《奇瑞应聘者隐私政策》以取得授权同意。

根据公司提供的在线产品信息，并经本所律师公开核查，公司主要业务在线产品均通过隐私政策并配置个人信息收集清单、第三方个人信息共享清单的形式告知个人信息收集处理情况及相关个人信息处理规则，包括个人信息处理者的名称和联系方式，处理个人信息的目的、方式、种类，个人信息保存期限和到期后的处理方式、个人信息主体行使权利的方法和途径等，并通过勾选同意等方式获得用户同意。个人信息收集处理活动与主要业务环节及特定在线产品功能具有直接相关目的，在各功能、场景下对于相应个人信息的收集均具有直接相关以及合理必要的合法性基础。本所律师认为公司在运营主要业务在线产品的过程中不存在重大的合规障碍。

2) 间接收集

对于公司涉及间接收集个人信息的场景，首先，根据公司的说明，对于公司的第三方供应商而言，在准入阶段公司会要求其提供包含数据合规内容的承诺函或签订有关数据处理的协议。同时公司已通过《IT-II-3-12 采购及供应商个人数据合规管理规定（试运行）》明确引入供应商前、与供应商合作期间、与供应商合作结束后的供应商管理方面的数据合规要求。在涉及从第三方平台或合作方间接获得个人信息的情况下，公司处理该等个人信息的合法性依赖于第三方平台或合作方向用户进行告知及获得同意或取得其他合法性基础。因此，公司在前述个人信息收集方面不存在重大违反法律法规相关要求的情况。

（二）个人信息使用

1. 法律要求

《个人信息保护法》第6条规定，处理个人信息应当具有明确、合理的目的，并应当与处理目的直接相关，采取对个人权益影响最小的方式。《个人信息保护法》第24条规定，个人信息处理者利用个人信息进行自动化决策，应当保证决策的透明度和结果公平、公正，不得对个人在交易价格等交易条件上实行不合理的差别待遇；通过自动化决策方式向个人进行信息推送、商业营销，应当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。

2. 合规事实

公司主要基于“（一）个人信息收集”部分所述目的存储、使用所收集的个人信息，其中，对于车主的个人信息，公司运用智慧营销平台对车主档案信息进行用户画像人群分析，以开展市

场研究、向车主进行调研等活动；对于 C 端消费者的个人信息，公司在主要运营的 App 中使用用户的手机号码、用车城市以及用户身份信息为用户提供个性化推送服务。

3. 合规评估

公司已在《个人信息收集处理知情同意书》向车主告知生成客户画像的个人信息使用目的，且该等间接画像不会精准关联至个人。公司通过 App 隐私政策向用户告知了个性化推送使用个人信息的情况，并提供了在产品内便捷关闭个性化推送的方式。在个人信息使用活动的管理上，公司制定了《CIT-III-024 IT 系统数据合规开发管理规范》，通过 IT 项目隐私合规准入评估的方式确保项目开发过程即能采取规避或消减数据合规潜在风险的规划方案，并符合数据合规义务和要求，能够有效减少公司个人信息使用活动超出目的限制的风险。此外，在内部进行客户数据调取时需经过审批流程，确认数据用途、权限以及保护措施。综上，公司对个人信息的使用活动不存在重大违法违规情形。

（三）个人信息共享

1. 法律要求

《个人信息保护法》第 20 条规定，两个以上的个人信息处理者共同处理个人信息应当约定各自的权利和义务，第 21 条规定委托处理个人信息应当与受托人约定委托处理的目的、期限、处理方式、个人信息的种类、保护措施以及双方的权利和义务等，并对受托人的个人信息处理活动进行监督；第 23 条规定向其他个人信息处理者提供其处理的个人信息的，应当向个人告知接收方的名称或者姓名、联系方式、处理目的、处理方式和个人信息的种类，并取得个人的单独同意。以及向其他个人信息处理者提供个人信息的场景提出协议约束、《网数条例》第 12 条明确了网络数据处理者向其他网络数据处理者提供、委托处理个人信息的协议约束及监督要求²⁴。

2. 合规事实

公司向外部第三方共享个人信息的场景主要为与经销商之间的数据交互，根据公司在《奇瑞

²⁴ 《网数条例》第 12 条：网络数据处理者向其他网络数据处理者提供、委托处理个人信息和重要数据的，应当通过合同等与网络数据接收方约定处理目的、方式、范围以及安全保护义务等，并对网络数据接收方履行义务的情况进行监督。向其他网络数据处理者提供、委托处理个人信息和重要数据的处理情况记录，应当至少保存 3 年。

网络数据接收方应当履行网络数据安全保护义务，并按照约定的目的、方式、范围等处理个人信息和重要数据。

两个以上的网络数据处理者共同决定个人信息和重要数据的处理目的和处理方式的，应当约定各自的权利和义务。

品牌许可销售服务合同》中与经销商约定的数据合规条款以及签订的数据处理协议，公司与经销商之间为委托处理关系，协议中约定的委托处理场景主要包括潜在客户管理、试乘试驾、车辆购买、开通 SIM 卡流量、售后协助、车主档案、产品/售后满意度调研、客诉处理。此外，公司引入一系列服务提供商提供业务支持，包括充电桩邮寄、基于售后服务质量管控的目的对售后录音进行分析、在线商城订单管理、用户洞察、产品传播及用户形象包装、客户服务、物流运输、关键岗位背景调查等场景，并在车辆续保业务方面与外部第三方存在业务合作，涉及对外提供个人信息。

在关联公司内部数据共享方面，公司主要由关联公司提供充电地图、旧车置换信息查询、周边产品电商订单管理等服务，在此过程中向关联公司共享相关个人信息。

3. 合规评估

在**个人信息对外提供的告知及单独同意义务**上，针对当前识别的对外提供场景：在协助车主办理车辆续保时，车主在 App 提交续保申请后，将进入由保险公司提供的在线页面，并展示有关相关隐私政策并获得车主的同意，对公司而言合规风险较低。

在与**第三方个人信息共享的管理及协议约束**方面，根据公司提供的资料，公司当前已制定《IT-III-1-5-5 数据共享管理办法》《IT-II-3-12 采购及供应商个人数据合规管理规定（试运行）》《IT-III-3-20-1 数据处理协议填写管理规范》对第三方数据共享场景进行合规审核、管理。公司在与主要的个人信息共享方即经销商之间的合作协议附件中统一要求签署数据处理协议，同时积极推进与其他涉及数据交互的第三方之间的数据处理协议签署，例如与车辆续保的第三方已签署数据处理协议，约定双方的权利义务；与背景调查公司之间已签订个人信息保护条款，要求未经权利人许可，不得对任何第三方透露信息；未经公司同意，不得将获得的个人信息用于其他目的等。综上，公司将持续推进数据处理协议或条款签署工作，积极满足与第三方之间就个人信息处理活动建立协议约束等的法律要求，在该等事项上基本符合合规要求，不存在重大的合规障碍。

（四）个人信息存储

1. 法律要求

根据《个人信息保护法》第 19 条²⁵和第 47 条²⁶、《个人信息安全规范》第 6.1 条²⁷的规定，公司应针对处理的个人信息设定存储期限，该存储期限应为实现处理目的所必需的最短时间，法律法规另有规定的除外。存储期限届满后或者处理目的已实现等情况下，应对相关个人信息进行删除或匿名化处理。

2. 合规事实

公司已制定《IT-III-3-9 个人数据留存和处置管理规定》，明确了数据合规部及各业务单位在个人数据留存和处置方面的职责要求，明确各业务单位根据业务实际情况制定合理的个人数据留存期限，并落实该规定中对个人数据留存、处置的要求。该规定明确个人数据的保留时间不应超过收集和处理目的所需的时间，并明确了数据存储期限最小化原则、数据处理的必要性和合理性原则，以及基于法律要求、业务需求、合同义务等情形下的数据保留情形；在数据处置层面，该规定要求在保留期限结束时，应及时、安全地从所有系统或应用程序中删除个人信息（法律要求、业务需求等特殊情况除外）。在上述规定的执行层面，公司已根据前述规定要求制定业务个人数据留存期限参考表，由各业务单位具体落实。

3. 合规评估

从内部管理维度，公司在所有重大方面符合《个人信息保护法》等规定关于数据存储及删除的要求；从具体落地维度，由各业务单位确定和落实自身数据存储期限的方式以实现整体管理，公司将持续关注各业务单位关于完成数据存储期限记录表及开展删除等处置工作的执行情况，例如要求其定期向数据合规部报告执行情况，确保落实到位。

综上，本所律师认为公司对于个人信息的处理在收集、使用、共享、存储等环节符合《个人

²⁵ 《个人信息保护法》第 19 条：除法律、行政法规另有规定外，个人信息的保存期限应当为实现处理目的所必要的最短时间。

²⁶ 《个人信息保护法》第 47 条：有下列情形之一的，个人信息处理者应当主动删除个人信息；个人信息处理者未删除的，个人有权请求删除：

（一）处理目的已实现、无法实现或者为实现处理目的不再必要；（二）个人信息处理者停止提供产品或者服务，或者保存期限已届满；（三）个人撤回同意；（四）个人信息处理者违反法律、行政法规或者违反约定处理个人信息；（五）法律、行政法规规定的其他情形。

法律、行政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现的，个人信息处理者应当停止除存储和采取必要的安全保护措施之外的处理。

²⁷ 《个人信息安全规范》第 6.1 a) 条：个人信息存储期限应为实现个人信息主体授权使用的目的所必需的最短时间，法律法规另有规定或者个人信息主体另行授权同意的除外。

《个人信息保护法》《网数条例》等相关法律规定，不存在可能对本次上市构成重大法律障碍的违法违规事项。

四、网络安全与数据安全义务履行

（一）组织架构

1. 法律要求

《网络安全法》第 21 条²⁸规定，网络运营者应任命网络安全负责人，落实网络安全保护责任。根据《数据安全法》第 27 条²⁹、《网数条例》第 30 条³⁰及 GB/T 44464-2024《汽车数据通用要求》第 4 条³¹的规定，重要数据处理者应任命数据安全负责人及数据安全管理机构，数据安全负责人的职责范围包括：研究提出数据安全相关重大决策建议；制定实施数据安全保护计划和数据安全事件应急预案；开展数据安全风险监测，及时处置数据安全风险和事件；定期组织开展数据安全宣传教育培训、风险评估、应急演练等活动；受理、处置数据安全投诉、举报；按照要求及时向网信部门和主管、监管部门报告数据安全情况等。《个人信息保护法》第 52 条³²规定，处理个人信息达到国家网信部门规定数量的个人信息处理者应当指定个人信息保护负责人，负责对个人信息处理活动以及采取的保护措施等进行监督。

2. 合规事实

在网络与数据安全机构的设立上，目前公司由集团进行一体化支持，**在决策层面**，公司设立总公司级数字化和信息化管理委员会，主要负责审定集团网络安全战略与发展规划、集团网络安全年度工作计划、集团网络安全政策、制度和体系建设规划；审定网络安全投资；领导推进网络安全等级保护工作负责指导并监督集团及下级板块、分子公司贯彻落实各项网络安全工作。

²⁸ 《网络安全法》第 21 条：网络运营者应该制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任。

²⁹ 《数据安全法》第 27 条：重要数据的处理者应当明确数据安全负责人和管理机构，落实数据安全保护责任。

³⁰ 《网数条例》第 30 条：重要数据的处理者，应当明确数据安全负责人，成立数据安全管理机构。

³¹ GB/T 44464-2024《汽车数据通用要求》第 4.1.3 条 汽车数据处理者应建立汽车数据安全管理机构，确定相关人员职责。

³² 《个人信息保护法》第 52 条：处理个人信息达到国家网信部门规定数量的个人信息处理者应当指定个人信息保护负责人，负责对个人信息处理活动以及采取的保护措施等进行监督。个人信息处理者应当公开个人信息保护负责人的联系方式，并将个人信息保护负责人的姓名、联系方式等报送履行个人信息保护职责的部门。

在管理层面，公司主要由管理推进办公室（信息安全管理部）和各子公司的直接负责人负责制定、更新网络安全相关政策标准；对网络安全项目进行规划、评审和质量控制；对企业网络安全工作的开展进行日常管理和监督。在执行层面，公司由数字化智能中心和业务部门多板块开展执行工作，主要负责汇报网络安全风险、支持安全与合规审计和考评、实施网络安全整改项目、提供人力支持及 IT 技术支持。同时，数字化智能中心下设数据合规部，整体负责数据合规管理工作。

在网络安全、数据安全及个人信息保护负责人的设置方面，公司当前已任命网络安全负责人，并设立数据安全合规保护官牵头组织和推进数据安全合规、个人信息保护工作。同时，公司也已指定汽车数据安全负责人及用户权益事务联系人。

3. 合规评估

公司已任命网络安全负责人，并设立数据安全合规保护官推进数据安全及个人信息保护工作。同时，作为汽车数据处理者，公司已任命数据安全负责人及数据安全管理机构。综上，奇瑞不存在组织架构方面的重大合规风险。

（二）制度体系

1. 法律要求

《数据安全法》第 21 条³³明确提出数据分类分级的要求，国家将根据在经济社会发展中的重要程度，以及一旦遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者个人、组织合法权益造成的危害程度对数据实行分类分级保护；结合《个人信息保护法》第 51 条³⁴、《网数条例》第 5 条³⁵等法律法规的规定，数据识别和分类分级管理是企业开展数据治理的基本要求。

³³ 《数据安全法》第 21 条：国家建立数据分类分级保护制度，根据数据在经济社会发展中的重要程度，以及一旦遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者个人、组织合法权益造成的危害程度，对数据实行分类分级保护。国家数据安全工作协调机制统筹协调有关部门制定重要数据目录，加强对重要数据的保护。关系国家安全、国民经济命脉、重要民生、重大公共利益等数据属于国家核心数据，实行更加严格的管理制度。各地区、各部门应当按照数据分类分级保护制度，确定本地区、本部门以及相关行业、领域的重要数据具体目录，对列入目录的数据进行重点保护。

³⁴ 《个人信息保护法》第 51 条：个人信息处理者应当根据个人信息处理目的、处理方式、个人信息的种类以及对个人权益的影响、可能存在的安全风险等，采取下列措施确保个人信息处理活动符合法律、行政法规的规定，并防止未经授权的访问以及个人信息泄露、篡改、丢失：（二）对个人信息实行分类管理……（五）制定并组织实施个人信息安全事件应急预案。

³⁵ 《网数条例》第 5 条：国家根据网络数据在经济社会发展中的重要程度，以及一旦遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者个人、组织合法权益造成的危害程度，对网络数据实行分类分级保护。

在网络与数据安全管理制度方面,《网络安全法》第 21 条规定,网络运营者应当按照网络安全等级保护制度的要求,制定内部安全管理制度和操作规程,确定网络安全负责人,落实网络安全保护责任,保障网络免受干扰、破坏或者未经授权的访问,防止网络数据泄露或者被窃取、篡改。《数据安全法》第 27 条规定,开展数据处理活动应当依照法律、法规的规定,建立健全全流程数据安全管理制度,组织开展数据安全教育培训,采取相应的技术措施和其他必要措施,保障数据安全。

在个人信息保护管理制度方面,《个人信息保护法》第 51 条规定,个人信息处理者应当根据个人信息的目的、处理方式、个人信息的种类以及对个人权益的影响、可能存在的安全风险等,制定内部管理制度和操作规程,确保个人信息处理活动符合法律、行政法规的规定,并防止未经授权的访问以及个人信息泄露、篡改、丢失。此外,根据《个人信息保护法》第 51 条的要求,个人信息处理者应制定并组织实施个人信息安全事件应急预案,该应急预案应能够帮助个人信息处理者满足《个人信息保护法》第 57 条有关个人信息安全事件的通知与补救要求。

2. 合规事实

根据公司提供的资料,奇瑞现阶段于奇瑞汽车与并表子公司范围内已基本构建网络安全、数据安全及个人信息保护制度体系。

在数据分类分级方面,根据公司提供的资料,公司目前在制度层面明确分类分级方法并开展数据资源盘点与分类分级管理工作,具体而言:

- 汽车数据方面:公司当前在《C032404-W-01 汽车数据分级分类管理规定》中结合公司的业务领域及产品情况,制定了数据分类分级规范,综合数据安全管理的总体目标和安全策略要求。
- 个人信息方面:公司制定了《IT-III-3-8 个人数据分类分级管理规定》并开展个人信息分类分级工作。在个人信息分级层面,公司按照个人信息数据一旦遭到篡改、破坏、泄露或者非法获取、非法利用后所造成的危害影响大小分为 1-4 级,并对具体分级制定了相应的保护要求。
- 企业数据方面:公司目前发布了《IT-III-1-5-1 数据安全规范》《数据分类分级策略标准》。在数据分级层面,公司将数据分为核心商密、普通商密、内部资料、外部公开四个类别,并针对不同的类别就其数据收集、存储、传输等制定了不同的数据管理要

求。

在网络安全管理方面，公司已在整体层面制定《IT-II-1-2-2 信息安全管理规范》，并配套《IT-III-1-1-18 系统账号与权限管理规范》《S0603-W-01 信息系统应急处置管理办法》《信息安全与保密管理违规行为通报标准管理条例（暂行）》《CIT-II-27 容量管理规范》《CIT-II-19 日志安全管理规定》《AM-II-3-1 秘密载体保密管理规定》《IT-III-1-2-3 信息安全事件分类标准及管理规范》等，明确公司的安全管理机构、安全管理制度、个人信息安全管理、信息系统应急管理信息、信息系统日志管理、信息系统账号权限管理等内容。

在数据安全方面，公司已在整体层面制定《IT-III-1-5-1 数据安全规范》，并配套《IT-III-1-5-5 数据共享管理办法》《IT-III-3-20-1 数据处理协议及填写管理规范》《CIT-III-024 IT 系统数据合规开发管理规范》《IT-III-3-18-1 视频监控数据合规管理规范》等，对公司各类数据处理及管理活动进行指导与规范。公司亦制定《C032404-W-02 汽车数据全生命周期安全管理规定》及《C0304-W-02 汽车数据安全风险管控管理规定》，从数据采集、传输、存储、处理、交换、销毁等环节明确了不同的汽车数据安全管理要求，并通过风险评估机制确保安全要求的落实。

在个人信息处理方面，公司已在整体层面制定《IT-I-3 个人数据总则》，并配套《IT-II-3-16 隐私影响评估管理规定（试运行）》《IT-II-3-1 隐私政策及 Cookies 政策管理规定》《IT-III-3-7 个人数据违规事件响应管理规定》《IT-II-3-12 采购及供应商个人数据合规管理规定》《IT-III-3-2 个人数据处理合法性基础评估管理规定》《T-III-3-14 个人数据合规审查审计管理规定》《IT-III-3-9 个人数据留存和处置管理规定》等，明确个人数据处理的基本原则和合规管理要求等，基本确立内部个人信息保护制度体系。

3. 合规评估

根据前述合规事实，公司目前已构建涵盖数据分类分级、信息安全管理、数据安全以及个人信息保护等多个重要维度的制度体系，不存在制度体系方面的重大合规风险。

（三）网络运行管理

1. 法律要求

《网络安全法》第 21 条³⁶明确规定网络运营者应当按照网络安全等级保护制度的要求，履行

³⁶ 《网络安全法》第 21 条：国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：

（一）制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；
（二）采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施；

安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改，包括采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施；采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；采取数据分类、重要数据备份和加密等措施。《网络安全法》第 22 条³⁷明确，网络产品、服务应当符合相关国家标准的强制性要求，《网络安全法》第 23 条规定网络关键设备和网络安全专用产品（例如路由器、交换机、防火墙、入侵检测系统等）应当按照相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求后，方可销售或者提供。《网络安全法》第 22 条明确，网络产品、服务的提供者发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。结合《网络产品安全漏洞管理规定》第 7 条的规定，企业作为网络产品、服务的提供者，发现其网络产品存在安全缺陷、漏洞等风险时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告，具体而言，应在 2 日内向工业和信息化部报送漏洞信息，并及时进行修补，将修补方式告知可能受影响的产品用户。《网络安全法》第 25 条³⁸及《个人信息保护法》第 51 条³⁹均要求制定安全事件应急预案。企业应制定网络安全事件应急预案及数据或个人信息安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险。根据《网络安全法》第 42 条⁴⁰及《个人信息

（三）采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；

（四）采取数据分类、重要数据备份和加密等措施；

（五）法律、行政法规规定的其他义务。

³⁷ 《网络安全法》第 22 条：网络产品、服务应当符合相关国家标准的强制性要求。网络产品、服务的提供者不得设置恶意程序；发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。网络产品、服务的提供者应当为其产品、服务持续提供安全维护；在规定或者当事人约定的期限内，不得终止提供安全维护。

³⁸ 《网络安全法》第 25 条：网络运营者应当制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险；在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告。

³⁹ 《个人信息保护法》第 51 条：个人信息处理者应当根据个人信息处理目的、处理方式、个人信息的种类以及对个人权益的影响、可能存在的安全风险等，采取下列措施确保个人信息处理活动符合法律、行政法规的规定，并防止未经授权的访问以及个人信息泄露、篡改、丢失：（五）制定并组织实施个人信息安全事件应急预案。

⁴⁰ 《网络安全法》第 42 条：网络运营者应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。在发生或者可能发生个人信息泄露、毁损、丢失的情况时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

安全规范》第 11.7 条⁴¹关于加强信息安全管理及审计的要求，公司作为网络运营者，应加强对自身运营的信息系统的安全审计工作，不定时由公司或外部有合法资质的专业第三方开展信息安全审计工作，留存信息安全审计报告，及时定位信息安全问题并予以处理。

2. 合规事实

根据公司提供的资料，公司目前已经取得 ISO 27001 认证，认证范围包含奇瑞汽车、国际公司、信息公司以及营销公司。公司采取了一系列网络安全保障措施，所部署的网络运行安全保护相关系统及采取的安全技术措施包括防火墙、WAF、防病毒、网络安全态势感知等，同时公司针对重要系统及数据库设立了备份恢复机制，操作系统每周备份，保留 2 周时间，数据库每天备份，保留 2-4 周时间。此外，公司定期委托第三方开展信息安全实战攻防演练，识别安全问题并进行整改。

在安全事件层面，公司制定了《S0603-W-01 信息系统应急处置管理办法》对信息系统应急处理职责分配、风险分析、预防预警、应急处置流程及应急保障措施等进行了规定，并制定《信息安全应急指导 2024 版》确立了信息安全应急组织架构，明确了应急领导小组及应急响应执行小组名单及工作职责；同时公司制定了《网络攻击类事件应急预案》《有害程序事件应急预案》《网页篡改事件应急预案》针对后门攻击、漏洞攻击、钓鱼邮件、有害程序攻击、网页篡改等涉及网络安全的事项发生后的应急处置流程及应急保障措施等进行了规定。在此基础上，公司定期组织相关的应急演练实战活动并进行复盘总结。

公司目前通过天网安全运营平台检测、记录网络运行状态，交换机内日志存储期限超过六个月，独立日志平台存储期限亦超过六个月。在网络产品和服务采购上，网络关键设备的采买需遵循公司招议标流程，公司会按照项目招标的形式进行网络安全产品的采购，以单个项目为单位签订合同及保密协议。在安全漏洞管理上，公司配置了漏洞管理系统联动公司漏洞扫描设备，将漏洞扫描数据定期同步至漏洞管理平台，实现漏洞修复必要性、修复状态的判断，并记录漏洞修复跟踪和闭环情况。

⁴¹ 《个人信息安全规范》第 11.7 条：对个人信息控制者的要求包括：a) 应对个人信息保护政策、相关规程和安全措施的有效性进行审计；b) 应建立自动化审计系统，监测记录个人信息处理活动；c) 审计过程形成的记录应能对安全事件的处置、应急响应和事后调查提供支撑；d) 应防止非授权访问、篡改或删除审计记录；e) 应及时处理审计过程中发现的个人信息违规使用、滥用等情况；f) 审计记录和留存时间应符合法律法规的要求。

3. 合规评估

公司采取了一系列网络安全保护措施，包括监测、记录网络运行状态、网络安全事件的技术措施，且留存的日志期限符合不少于六个月的法定要求，同时建立了日志管理制度。截至最后实际可行日期，公司未发生过重大网络安全、数据安全、个人信息安全事件。

根据公司提供的资料及公司的说明，公司曾应工业和信息化部“数安护航”专项行动要求，对车联网数据安全风险进行排查与防范。后续，公司会定期开展网络安全及数据安全审计工作，排查安全风险，确保相关安全技术及管理措施运行的有效性。

（四）网络安全等级保护

1. 法律要求

《网络安全法》第 21 条⁴²及《网络安全法》相关配套标准⁴³要求国内实行网络安全等级保护制度，网络运营者应按照等级保护制度要求，落实相应的技术保护及组织管理措施。《数据安全法》第 27 条进一步明确，利用互联网等信息网络开展数据处理活动，应当在网络安全等级保护制度的基础上，履行上述数据安全保护义务。公安部在《贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见》中进一步强调，网络运营者应当根据网络安全等级保护制度要求，对所运营的业务系统开展等级评估及测评工作。对于经测评为二级及以上等级的信息系统，网络运营者应上报至所在地公安机关进行备案，获取相应的等保备案证明。第三级以上网络运营者应委托符合国家有关规定的等级测评机构，每年开展一次网络安全等级测评，并及时将等级测评报告提交受理备案的公安机关和行业主管部门。

2. 合规事实

根据公司提供的资料，公司当前已建立符合 ISO 27001 且等同于或高于网络安全等级保护二级要求的信息安全体系和网络安全基础环境配置，并对集团所有信息系统规划、建设和运维统一安全要求。在备案方面，公司当前已完成车联网系统网络安全等级三级备案，且已完成若干核心业务系统的网络安全等级二级备案。在网络安全等级保护工作的推进计划上，公司曾聘请外部网

⁴² 《网络安全法》第 21 条：国家实行网络安全等级保护制度……

⁴³ 包括 GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》、GB/T 22240-2020《信息安全技术 网络安全等级保护定级指南》、GB/T 25058-2019《信息安全技术 网络安全等级保护实施指南》等。

络安全专家对公司信息系统全局进行定级评审，持续推进剩余信息系统的测评及备案工作，在集团层面亦与测评机构签订网络安全等级保护测评框架协议，为集团内实体提供统一服务标准。此外，公司亦与所在地公安网警保持沟通，根据其意见有序开展测评和备案工作。公司信息系统网络安全等级保护备案情况见附件 3。

3. 合规评估

公司已根据与所在地公安网警的沟通，按照其意见开展测评和备案工作，并优先针对高风险系统开展相关等保测评和备案工作，不存在网络安全等级保护方面的重大合规风险。

公司后续会保持与所在地公安网警的沟通，对剩余信息系统是否需要进行网络安全等级保护测评或备案进行持续排查和梳理，并持续开展网络安全等级保护为三级的信息系统年度测评和备案工作，及时将等级测评报告提交受理备案的公安机关和行业主管部门，核实相关系统是否仍满足三级保护标准。

（五）培训及人员管理

1. 法律要求

《数据安全法》第 27 条⁴⁴明确要求企业应组织开展数据安全教育和培训，保障数据安全。《个人信息保护法》第 51 条第（四）款要求个人信息处理者合理确定个人信息处理的操作权限，并定期对从业人员进行安全教育和培训。《网数条例》第 30 条规定，掌握有关主管部门规定的特定种类、规模的重要数据的网络数据处理者，应当对网络数据安全负责人和关键岗位的人员进行安全背景审查，加强相关人员培训。

2. 合规事实

根据公司提供的资料，公司借助线上平台对于新入职的技术岗位员工统一开展信息安全培训；对于在职员工，公司通过多样化的方式（H5 页面推送、在线测试、钓鱼邮件演练以及举办信息安全宣传周等活动）开展信息安全培训。公司亦面向内部员工开展了个人信息保护等数据合规方面的培训。此外，在人员管理的关键环节上，公司涉及数据安全的关键岗位员工会签订《网络安全

⁴⁴ 《数据安全法》第 27 条：开展数据处理活动应当依照法律、法规的规定，建立健全全流程数据安全管理制度，组织开展数据安全教育和培训，采取相应的技术措施和其他必要措施，保障数据安全。

和保密管理目标责任书》，明确考核指标、网络安全管理职责以及奖惩规定。公司在进行人员背调过程会涉及一定的安全背景审查，并在与员工签订的劳动协议中约定相关的保密条款；在员工离职时，人力资源部门将依据管理规定，对特定人员进行信息安全审计，确保离职人员的系统账号在接到人力资源部门通知后的3个工作日内迅速冻结，并在3个月内妥善删除该账号，防止因人员流动而引发的数据安全风险。

3. 合规评估

公司在当前的运营实践中已经采取信息安全及数据合规相关培训及人员管理举措，不存在培训及人员管理方面的重大合规风险。

综上，本所律师认为公司在组织架构、制度体系、网络运行管理、网络安全等级保护、培训及人员管理等方面已适当履行《网络安全法》《数据安全法》《个人信息保护法》《网数条例》等法律法规要求的网络安全与数据安全义务，不存在可能对本次上市构成重大法律障碍的违法违规事项。

五、公司处理重要数据的合规情况

针对涉及汽车数据的重要数据，如“二、汽车数据处理”所述，公司在所有重大方面符合《汽车数据若干规定》等规定针对关于重要数据处理者的合规要求。

针对非汽车数据的重要数据，如“三、个人信息处理”所述，公司处理的个人信息已超过1000万人（未去重，含潜客、车主等C端消费者、合作方员工、公司内部员工、候选人），根据《网数条例》第28条，处理1000万人以上个人信息的，应当遵守《网数条例》第30条、第32条⁴⁵关

⁴⁵ 《网数条例》第30条：重要数据的处理者应当明确网络数据安全负责人和网络数据安全管理机构。网络数据安全管理机构应当履行下列网络数据安全保护责任：（一）制定实施网络数据安全管理制度、操作规程和网络数据安全事件应急预案；（二）定期组织开展网络数据安全风险监测、风险评估、应急演练、宣传教育培训等活动，及时处置网络数据安全风险和事件；

（三）受理并处理网络数据安全投诉、举报。

网络数据安全负责人应当具备网络数据安全专业知识和相关管理工作经历，由网络数据处理器管理层成员担任，有权直接向有关主管部门报告网络数据安全情况。

第32条：重要数据的处理者因合并、分立、解散、破产等可能影响重要数据安全的，应当采取措施保障网络数据安全，并向省级以上有关主管部门报告重要数据处置方案、接收方的名称或者姓名和联系方式等；主管部门不明确的，应当向省级以上数据安全工作协调机制报告

于重要数据处理者的合规义务，包括明确网络数据安全负责人（由管理层成员担任）和网络数据安全管理机构（履行制定管理制度、操作规程和安全事件应急预案，定期组织开展风险监测、风险评估、应急演练、培训，及时处置安全事件，受理并处理网络数据安全投诉、举报等义务），因合并、分立、解散、破产等可能影响重要数据安全的，应当采取措施保障网络数据安全，并向有关主管部门报告。

如“四、网络安全与数据安全义务的履行”所述，公司已任命了网络安全负责人并设置数据安全合规保护官牵头组织和推进数据安全合规、个人信息保护工作，设立了网络数据安全管理机构，负责履行《网数条例》项下的前述义务，在所有重大方面符合《网数条例》针对处理超过 1000 万人个人信息的网络数据处理者的合规要求。

综上，本所律师认为公司在重要数据处理方面已适当履行《网数条例》《汽车数据若干规定》等法律法规要求的合规义务，不存在可能对本次上市构成重大法律障碍的违法违规事项。

六、人工智能技术的应用

根据《暂行办法》第 2 条⁴⁶，利用生成式人工智能技术面向中国境内公众提供生成式人工智能服务的，适用《暂行办法》，并在上线前应当根据《暂行办法》等规定履行安全评估和大模型备案等合规程序。此外，根据《互联网信息服务深度合成管理规定》第 2 条、第 19 条⁴⁷规定，在中国境内应用深度合成技术提供互联网信息服务的，还应当开展深度合成服务算法备案及安全评估等合规程序。

根据公司提供的材料，雄狮的 LionCarmind 产品涉及面向中国境内的公众提供生成式人工智能服务和算法推荐服务，**目前已经完成大模型备案（备案号：Anhui-LionButterfly-2025032000**

掌握有关主管部门规定的特定种类、规模的重要数据的网络数据处理者，应当对网络数据安全负责人和关键岗位的人员进行安全背景审查，加强相关人员培训。审查时，可以申请公安机关、国家安全机关协助。

⁴⁶ 《暂行办法》第 2 条：利用生成式人工智能技术向中华人民共和国境内公众提供生成文本、图片、音频、视频等内容服务（以下称生成式人工智能服务），适用本办法。

⁴⁷ 《互联网信息服务深度合成管理规定》第 2 条：在中华人民共和国境内应用深度合成技术提供互联网信息服务，适用本规定。法律、行政法规另有规定的，依照其规定。

第 19 条：具有舆论属性或者社会动员能力的深度合成服务提供者，应当按照《互联网信息服务算法推荐管理规定》履行备案和变更、注销备案手续。

04) 以及生成合成类算法备案(备案号: 网信算备 340207327545401250021 号、网信算备 340207327545401250013 号)。此外, 公司拟在未来上线卓行智驾大模型、端到端 E2E 大模型, 并正在研发 VLA 多模态模型, 此等大模型可能属于生成式人工智能技术及深度合成技术, 据此, 上线此等大模型服务将适用《暂行办法》《互联网信息服务深度合成管理规定》, 并应当开展大模型备案、深度合成服务算法备案以及涉及的安全评估, 根据公司的说明, 在相关大模型正式上线并对外提供服务前, 公司将确保已完成相关备案、安全评估程序。

七、公司无需申报数据出境安全评估或开展标准合同备案等

《个人信息保护法》第三章、《促进和规范数据跨境流动规定》《数据出境安全评估办法》《个人信息出境标准合同办法》及《汽车数据若干规定》第 11 条⁴⁸规定, 如涉及向境外提供个人信息的, 应当取得合法性基础(例如单独同意)、开展个人信息保护影响评估, 并根据其具体出境数量及出境场景, 可能需履行数据出境安全评估、标准合同备案或个人信息保护认证等义务; 如涉及重要数据的, 应当在境内存储, 确需向境外提供的, 应申报数据出境安全评估。

根据《数据出境风险自评估报告》⁴⁹、汽车数据年报(2024 年度)等材料, 公司出境数据包括品牌信息、内部车型、外部车型、物料信息、整车数据(未绑定)、T-BOX 设备数据、蓝牙设备信息、IHU 设备信息、合格证信息、车辆识别号列表(未绑定)、OTA 升级包签名信息、OTA 升级包程序、PKI 证书, 均不涉及个人信息及重要数据, 即公司不涉及个人信息或重要数据出境。

综上, 公司现阶段无需履行《个人信息保护法》《促进和规范数据跨境流动规定》《数据出境安全评估办法》《个人信息出境标准合同办法》《汽车数据若干规定》等规定项下关于申报数据出境安全评估或开展标准合同备案的合规要求。

八、公司无需主动申报网络安全审查

《网络安全审查办法》已于 2022 年 2 月 15 日正式生效实施, 其中规定了三种需要进行网络

⁴⁸ 《汽车数据若干规定》第 11 条: 重要数据应当依法在境内存储, 因业务需要确需向境外提供的, 应当通过网信部门会同国务院有关部门组织的安全评估。未列入重要数据的涉及个人信息数据的出境安全管理, 适用法律、行政法规的有关规定。

⁴⁹ 根据公司的说明, 公司已就该报告内容征得网信部门及自贸区主管机构的沟通确认。

安全审查的情形，包括：（1）掌握超过 100 万用户个人信息的网络平台运营者赴国外上市；（2）CIIO 采购网络产品和服务影响或者可能影响国家安全；及（3）网络平台运营者开展数据处理活动，影响或者可能影响国家安全。根据公司反馈的信息，截至最后实际可行日期，公司未收到有关主管部门认定其为 CIIO 的通知，也未因开展数据处理活动被有关部门认定为影响或者可能影响国家安全；同时监管机构并未认定“赴港上市”属于“赴国外上市”情形。

（一） 赴香港上市相关网络安全审查风险

《网络安全审查办法》并未对“国外上市”作出进一步解释或诠释。根据《出境入境管理法》第 89 条，由中国内地前往香港特别行政区被认定为“出境”。而“国外”一词，虽未在法律文件中有明确定义，但根据其含义进行一般理解，国内外涉及国境的划分，属于主权概念，而香港是中华人民共和国不可分割的一部分，当然属于我国主权领土范围内。由于《网络安全审查办法》使用的表述是“国外上市”，而不是“境外上市”，而香港属于“境外”而非“国外”，因此在香港上市不属于“在国外上市”。就公司本次发行上市是否需要申报网络安全审查的事宜，本所律师认为不属于《网络安全审查办法》第 7 条规定的赴国外上市的情形。

因此，本所律师认为公司本次发行上市不属于《网络安全审查办法》第 7 条规定的需要主动申报网络安全审查的情形。

（二） CIIO 采购网络产品和服务相关网络安全审查风险

根据《网络安全审查办法》第 2 条、第 5 条的规定，CIIO 采购网络产品和服务的，应当预判该产品和服务投入使用后可能带来的国家安全风险。影响或者可能影响国家安全的，应当向网络安全审查办公室申报网络安全审查。根据《关键信息基础设施安全保护条例》第 2 条的规定，关键信息基础设施，是指公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域的，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统等。同时，《关键信息基础设施安全保护条例》第 10 条规定，保护工作部门根据认定规则负责组织认定本行业、本领域的关键信息基础设施，及时将认定结果通知运营者，并通报国务院公安部门。

截至最后实际可行日期，公司未收到相关监管部门通知公司被认定为 CIIO。因此本所律师认为，公司目前无需根据《网络安全审查办法》第 2 条、第 5 条的规定申报网络安全审查。

(三) 网络平台运营者开展数据处理活动相关网络安全审查风险

根据《网络安全审查办法》第2条的规定，网络平台运营者开展数据处理活动，影响或者可能影响国家安全的，应当按照本办法进行网络安全审查。《网数条例》第13条规定，网络数据处理者开展网络数据处理活动，影响或者可能影响国家安全的，应当按照国家有关规定进行国家安全审查。《网络安全审查办法》第16条规定，网络安全审查工作机制成员单位认为影响或者可能影响国家安全的网络产品和服务以及数据处理活动，将由网络安全审查办公室按程序报中央网络安全和信息化委员会批准后，依照规定进行审查。由于《网络安全审查办法》《网数条例》均未对“影响或者可能影响国家安全”做出进一步规定，基于《中华人民共和国国家安全法》对国家安全的定义⁵⁰以及《网络安全审查办法》第10条列举的七项在网络安全审查中应重点评估的国家安全风险因素⁵¹，公司可以从以下五点考虑是否参与任何可能导致国家安全风险的活动：（1）是否实施全面的数据收集、储存及保护程序；（2）是否发生过任何数据泄露，或违反数据保护及隐私法律法规而对业务经营造成重大不利影响的事件；（3）是否遭受来自网信部门、中国证监会或任何其他相关政府部门与网络安全或数据隐私或任何网络安全审查有关的任何重大调查、问询或制裁；（4）是否被任何部门告知被列为CIIO；（5）上市完成后，公司是否会受到任何外国政府控制。结合公司提供的资料及公司的说明，考虑到公司内部对数据处理活动的管理情况以及公司截至最后实际可行日期并未被主管部门认定为CIIO⁵²，本所律师认为，公司不会因数据处理活动影响或者可能影响国家安全而被要求进行网络安全审查。

⁵⁰ 《中华人民共和国国家安全法》第2条：国家安全是指国家政权、主权、统一和领土完整、人民福祉、经济社会可持续发展和国家其他重大利益相对处于没有危险和不受内外威胁的状态，以及保障持续安全状态的能力。

⁵¹ 《网络安全审查办法》第10条：网络安全审查重点评估相关对象或者情形的以下国家安全风险因素：

- （一）产品和服务使用后带来的关键信息基础设施被非法控制、遭受干扰或者破坏的风险；
- （二）产品和服务供应中断对关键信息基础设施业务连续性的危害；
- （三）产品和服务的安全性、开放性、透明性、来源的多样性，供应渠道的可靠性以及因为政治、外交、贸易等因素导致供应中断的风险；
- （四）产品和服务提供者遵守中国法律、行政法规、部门规章情况；
- （五）核心数据、重要数据或者大量个人信息被窃取、泄露、毁损以及非法利用、非法出境的风险；
- （六）上市存在关键信息基础设施、核心数据、重要数据或者大量个人信息被外国政府影响、控制、恶意利用的风险，以及网络信息安全风险；
- （七）其他可能危害关键信息基础设施安全、网络安全和数据安全的因素。

⁵² 《关键信息基础设施安全保护条例》第10条：保护工作部门根据认定规则负责组织认定本行业、本领域的关键信息基础设施，及时将认定结果通知运营者，并通报国务院公安部门。

我们已于 2025 年 1 月 10 日、2025 年 2 月 14 日与中国网络安全审查认证和市场监管大数据中心（网络安全审查办公室设在国家互联网信息办公室，具体工作委托中国网络安全审查认证和市场监管大数据中心承担）进行电话沟通。根据其回复，就公司本次发行上市而言，公司无需主动申报网络安全审查。

综上，根据现行监管制度，基于公司当前数据处理活动现状及与监管侧的咨询结果，本所律师认为公司无需就本次发行上市主动申报网络安全审查。

九、结论性意见

综上所述，本所律师认为：自报告期起始之日直至最后实际可行日期内，奇瑞在所有重大方面均符合现行有效的中华人民共和国境内（仅就本意见书而言，不包括中华人民共和国香港特别行政区、中华人民共和国澳门特别行政区、中华人民共和国台湾地区）有关网络安全、数据安全、个人信息保护的法律法规的规定，即不存在重大数据合规（包括网络安全、数据安全、个人信息保护）风险，不存在因数据合规（包括网络安全、数据安全、个人信息保护）问题引致的重大诉讼、仲裁或重大处罚，未发生任何重大网络安全、数据安全和个人信息安全事件，不存在因监管要求而导致其业务无法持续开展且无法整改的情况。奇瑞数据合规现状不存在对公司的业务运营、财务表现及对本次发行上市产生重大不利影响的情形，自报告期起始之日直至最后实际可行日期，奇瑞无需就本次发行上市主动申报网络安全审查。

（以下无正文，为《北京市中伦律师事务所关于奇瑞汽车股份有限公司之网络安全、数据安全及个人信息保护法律意见书》之签字页）



附件 1：个人信息的直接收集

业务环节	个人信息主体类型	个人信息收集渠道/目的、类型 ⁵³
购车业务		
潜在客户营销	C 端消费者（潜在客户）	- 潜在客户在公司自有 App、小程序和网站留资：个人基本资料 - 潜在客户在车展等线下活动或经销商线下留资：个人基本资料
试乘试驾	C 端消费者（潜在客户）	- 通过自有小程序、App、网站进行预约：个人基本资料、预约服务信息、个人位置信息 - 实际体验服务：个人基本资料、个人身份信息
车辆销售	车主	- 通过经销商等渠道购车：个人基本资料、个人身份信息、车辆订单相关信息 - 通过公司自有小程序、App 及网站订购：个人基本资料、个人身份信息、车辆订单相关信息 - 开通、购买 SIM 卡流量：个人基本资料、个人身份信息、车辆信息、流量订单信息
车主关系管理及运营	车主	- 建立车主档案：个人基本资料、个人身份信息、个人教育工作信息（选填）、个人资产信息（选填）、推荐人个人基本资料（选填）等 - 通过公司自有小程序、App 及网站等进行社区运营及内容传播：个人操作记录。 - 活动组织：个人基本资料、个人身份信息（如活动过程中需购买保险、预订交通住宿等） - KOC 客户运营：个人基本资料、车辆信息、网络身份标识信息、个人教育工作信息 - 售后营销：个人基本资料、车辆信息
售后支持	车主	- 保修管理与索赔：个人基本资料、个人身份信息、车辆信息等 - 维修保养：个人基本资料、车辆信息、预约服务信息 - 道路救援：个人基本资料、车辆信息、救援服务信息 - 车辆故障检测：个人基本资料、车辆信息、救援服务信息
增值服务	车主/C 端消费者	- 车辆充电服务：车辆信息、个人设备信息、充电服务信息 - 家用充电桩服务：个人基本资料、安装服务信息（选填） - 车辆续保服务：个人基本资料、车辆信息、投保信息、购车信息 - 周边产品销售或奖励发放：个人基本资料、收货与订单信息 - 旧车置换咨询业务（线上）：个人基本资料、个人身份信息、车辆信息

⁵³ 根据品牌及具体场景不同，公司所收集的具体字段将有所差异。

业务环节	个人信息主体类型	个人信息收集渠道/目的、类型 ⁵³
客户服务	车主/C 端消费者	- 服务记录：个人基本资料、网络身份标识信息、客户服务信息
客户调研	车主	- 车主回访及调研（电话回访）：个人基本资料、回访录音 - 部分品牌（星途）会在产品上市前后开展调研、座谈等活动： ①产品调研：个人基本资料、个人身份信息、个人工作信息、个人资产信息、购车情况和偏好等 ②用户座谈：个人基本资料
B 端合作方管理		
经销商管理	经销商员工	- 通过自有网站进行经销商加盟意向收集：个人基本资料、个人工作信息
供应商管理	供应商员工	- SRM 系统供应商账号注册：个人基本资料、网络身份标识信息、设备信息 - 访客管理：个人基本资料、个人身份信息、生物识别信息、保险信息
员工管理		
员工管理	公司员工	- 入职体检报告、基本资料登记信息、劳动合同信息等 - 员工档案：个人基本资料、个人身份信息、个人工作信息等 - 行政管理：个人基本资料、个人工作信息、生物识别信息、打卡位置信息等 - 培训管理：个人基本资料、个人工作信息、考核信息、打卡位置等 - 绩效与薪酬管理：个人基本资料、个人工作信息、个人身份信息、金融账户信息 - 因公差旅与报销：个人基本信息、个人工作信息、行程信息、银行账号 - 员工关系管理：个人基本信息、个人身份信息 - 企业文化建设：个人基本信息、个人身份信息等
招聘管理		
招聘管理	候选人	- 招聘管理：个人基本信息、个人教育工作信息、背景调查信息、个人健康生理信息等

附件 2：核心业务主要在线产品清单

形态	名称	涉及收集个人信息的功能	在线收集的个人信息
网站	奇瑞官网	- 潜客营销：购车咨询（包括大客户及新零售咨询） - 试乘试驾：预约试驾 - 车辆销售：金融服务申请 - 增值服务：二手车业务咨询 - 经销商加盟 - 其余在线服务：注册登录、经销商/售后网点查询、在线客服	✓ C 端消费者信息 ✓ 拟加盟经销商联系人信息 ✓ 用户设备信息、日志信息
网站	奇瑞风云官网	- 试乘试驾：预约试驾 - 经销商加盟 - 其余在线服务：注册登录、经销商/售后网点查询、在线客服	✓ C 端消费者信息 ✓ 拟加盟经销商联系人信息 ✓ 用户设备信息、日志信息
网站	iCAR 汽车官网	- 试乘试驾：预约试驾 - 车辆销售：车辆订购 - 售后支持：预约保修服务等 - 增值服务：商品订购 - 经销商加盟 - 其余在线服务：注册登录、经销商查询、在线客服	✓ C 端消费者信息 ✓ 拟加盟经销商联系人信息 ✓ 用户设备信息、日志信息
网站	捷途汽车官网	- 潜客营销：购车咨询（包括大客户及新零售咨询） - 试乘试驾：预约试驾 - 增值服务：旧车置换咨询 - 经销商加盟 - 其余在线服务：经销商查询、在线客服	✓ C 端消费者信息 ✓ 拟加盟经销商联系人信息 ✓ 用户设备信息、日志信息
网站	星途汽车官网	- 试乘试驾：预约试驾 - 其余在线服务：经销商查询、客户服务	✓ C 端消费者信息 ✓ 用户设备信息、日志信息
网站	奇瑞新能源官网	- 试乘试驾：预约试驾 - 售后支持：预约售后服务 - 其余在线服务：在线客服	✓ C 端消费者信息 ✓ 用户设备信息、日志信息
APP	奇瑞汽车	- 试乘试驾：预约试驾 - 车辆销售：车辆订购 - 售后支持：售后服务预约、道路救援、充电服务、私桩报装等 - 车主关系维护及运营：社区运营、活动报名、尊贵身份申请等 - 增值服务：商品订购、福利推荐等	✓ C 端消费者信息 ✓ 用户设备信息、日志信息

形态	名称	涉及收集个人信息的功能	在线收集的个人信息
		其余在线服务：注册登录、车辆绑定及远程控制、经销商/权益查询、在线客服等	
APP	iCAR 汽车	- 试乘试驾：预约试驾 - 车辆销售：车辆订购、心愿单 - 售后支持：预约保修、道路救援、充电服务、车机流量、充电桩绑定、取送车服务 - 车主关系管理及运营：用户社区、活动报名、车主留言、好友邀请、车主俱乐部 - 增值服务：商品订购 - 其余在线服务：注册登录、销售中心/服务中心查询、车辆绑定及远程控制、在线客服、搜索	✓ C端消费者信息 ✓ 用户设备信息、日志信息
APP	Hi 星途	- 试乘试驾：预约试驾 - 车主关系管理及运营：用户社区、活动报名、星推官招募 - 售后支持：预约服务、道路救援、充电服务 - 增值服务：商品订购 - 其余在线服务：注册登录、车辆绑定及远程控制、在线客服	✓ C端消费者信息 ✓ 用户设备信息、日志信息
APP	星途星纪元	- 试乘试驾：预约试驾 - 车辆销售：车辆订购 - 增值服务：商品订购 - 售后支持：预约服务、道路救援、充电服务 - 车主关系管理及运营：用户社区、活动报名 - 其余在线服务：注册登录、服务网点查询、车辆绑定及远程控制、在线客服	✓ C端消费者信息 ✓ 用户设备信息、日志信息
APP	捷途汽车	- 试乘试驾：预约试驾 - 车辆销售：车辆订购 - 售后支持：预约维保、道路救援、充电服务 - 增值服务：商品订购 - 车主关系管理及运营：用户社区，车主权益、活动报名、车主创作活动、3D改装 - 其余在线服务：注册登录、车辆绑定及远程控制、经销商/驿站/充电桩/旅行权益查询、在线客服	✓ C端消费者信息 ✓ 用户设备信息、日志信息
APP	E 奇赢	注册登录、营销任务分享	✓ 经销商员工信息 ✓ 用户设备信息、日志信息
微信小程序	奇瑞小奇同学汇小程序	- 售后服务：预约售后、道路救援、充电服务 - 增值服务：商品订购 - 车主关系管理及运营：车主认证、车主等级权	✓ C端消费者信息 ✓ 用户设备信息、日志信息

形态	名称	涉及收集个人信息的功能	在线收集的个人信息
		益、用户社区、活动报名、福利推荐、尊贵身份认证 • 其余在线服务：注册登录、经销商查询、在线客服	
微信小程序	奇瑞官方网站	• 试乘试驾：预约试驾 • 其余在线服务：注册登录、经销商查询、在线客服	✓ C端消费者信息 ✓ 用户设备信息、日志信息
微信小程序	风云新能源官方网站	• 试乘试驾：预约试驾 • 经销商加盟 • 其余在线服务：注册登录、经销商查询、在线客服	✓ C端消费者信息 ✓ 拟加盟经销商联系人信息 ✓ 用户设备信息、日志信息
微信小程序	奇瑞官方商城	• 潜在客户营销：活动报名 • 车辆销售：车辆订购 • 增值服务：商品订购 • 其余在线服务：注册登录	✓ C端消费者信息 ✓ 用户设备信息、日志信息
微信小程序	星途星纪元	• 车辆销售：车辆订购 • 售后服务：预约售后 • 车主关系管理及运营：用户社区、活动报名 • 其余在线服务：注册登录、服务网点查询	✓ C端消费者信息 ✓ 用户设备信息、日志信息
微信小程序	EXEED 星途试驾	• 试乘试驾：预约试驾 • 其余在线服务：运营资讯互动	✓ C端消费者信息 ✓ 用户设备信息、日志信息
微信小程序	EXEED 星途商城	• 车辆销售：车辆订购 • 其余在线服务：注册登录	✓ C端消费者信息 ✓ 用户设备信息、日志信息
微信小程序	EXEED 星途试驾助手	• 登录、经销商查看试驾信息	✓ 经销商账号信息 ✓ 用户设备信息、日志信息
微信小程序	iCAR 汽车	• 试乘试驾：预约试驾 • 车辆销售：车辆订购 • 售后支持：预约保修、道路救援 • 增值服务：商品订购 • 车主关系管理及运营：用户社区、活动报名 • 其余在线服务：注册登录、在线客服、销售中心/服务中心查询	✓ C端消费者信息 ✓ 用户设备信息、日志信息
微信小程序	JETOUR 捷途	• 试乘试驾：预约试驾 • 车辆销售：车辆订购 • 车主关系管理及运营：活动报名、权益预定 • 其余在线服务：注册登录、经销商/驿站查询、在线客服、预约到店	✓ C端消费者信息 ✓ 用户设备信息、日志信息

形态	名称	涉及收集个人信息的功能	在线收集的个人信息
微信 小程序	捷途山海	• 试乘试驾：预约试驾 • 车辆销售：车辆订购 • 车主关系管理及运营：活动报名、权益预定 • 其余在线服务：注册登录、经销商/驿站查询、在线客服、预约到店	✓ C端消费者信息 ✓ 用户设备信息、日志信息

附件 3：信息系统网络安全等级保护备案情况

序号	系统名称	已完成的网络安全等级保护备案情况
1.	车联网系统	三级
2.	飞书（第三方系统）	三级
3.	奇瑞客服系统	二级
4.	数字营销平台（iCar 运营平台）	二级
5.	普思认证信息	二级
6.	新能源管理	二级
7.	奇瑞车主用户运营平台	二级
8.	捷途 CRM（捷途亿客）	二级
9.	捷途 APP	二级
10.	奇瑞 CGBOM 系统	二级
11.	奇瑞邮件信息系统	二级
12.	奇瑞变更管理系统	二级
13.	采购质量交互系统	二级
14.	竞品数据库系统	二级
15.	奇瑞 CAE 平台数据管理系统	二级
16.	奇瑞经销商协同平台	二级
17.	奇瑞帆软报表系统	二级
18.	奇瑞车主俱乐部	二级
19.	奇瑞智能发票管理系统	二级
20.	奇瑞采购管理平台	二级
21.	奇瑞供应商协同平台	二级
22.	奇瑞尺寸系统	二级
23.	集团数据防泄漏系统	二级
24.	奇瑞 FAQ 知识库系统	二级
25.	奇瑞电子目录管理	二级
26.	集团员工共享服务平台	二级
27.	星途助手 APP 和 Hi 星途 APP	二级
28.	集团财务共享中心报账	二级
29.	集团资金管理	二级
30.	集团合同管理	二级
31.	奇瑞全面预算系统	二级
32.	奇瑞国际经销商管理系统	二级
33.	集团大数据分析平台	二级
34.	奇瑞电子招议标系统	二级
35.	奇瑞发票管理平台	二级
36.	奇瑞汽车车主 APP	二级
37.	集团统一身份认证平台	二级
38.	奇瑞采购管理平台	二级

序号	系统名称	已完成的网络安全等级保护备案情况
39.	奇瑞备件仓储管理	二级
40.	乘用车智慧运营控制塔	二级
41.	企业资源计划管理系统	二级
42.	物料拉动系统	二级
43.	客户关系管理系统	二级
44.	国内经销商交流系统	二级
45.	国际经销商交流系统	二级
46.	供应商交互平台	二级
47.	备件物流系统	二级
48.	资金管理系统	二级
49.	制造执行系统	二级
50.	高级计划排程管理系统	二级
51.	产品数据管理系统	二级
52.	企业应用集成平台	二级
53.	奇瑞官网	二级