
关于广州遇见小面餐饮股份有限公司
发行 H 股股票并在香港联合交易所有限公司主板上市
涉及中华人民共和国境内数据合规之法律备忘录



嘉源律师事务所
JIA YUAN LAW OFFICES

致：广州遇见小面餐饮股份有限公司（以下简称“发行人”）

关于广州遇见小面餐饮股份有限公司
发行 H 股股票并在香港联合交易所有限公司主板上市
涉及中华人民共和国境内数据合规之法律备忘录

嘉源(2025)-06-248

北京市嘉源律师事务所（以下简称“**本所**”）为在中国注册并经中国司法部批准执业的律师事务所。本所接受发行人委托，担任发行人申请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“**本次发行并上市**”）事宜的中华人民共和国境内（以下简称“**中国境内**”，为本备忘录之目的，不包括中国香港特别行政区、中国澳门特别行政区、中国台湾地区）数据合规法律顾问并开展尽职调查，就发行人及其本次发行并上市涉及的在中国境内实益拥有的子公司及分公司（以下单独或合称“**公司**”）在中国境内的数据合规法律事宜出具本《关于广州遇见小面餐饮股份有限公司发行 H 股股票并在香港联合交易所有限公司主板上市涉及中华人民共和国境内数据合规之法律备忘录》（以下简称“**本备忘录**”）。

本所对公司截至 2025 年 11 月 18 日（“**最后实际可行日期**”）在中国境内经营业务的数据合规情况等特定事项（而非全面事项），出具本备忘录供公司参考。

本所出具本备忘录基于以下前提和假设：

- 1) 公司提供给本所律师的所有文件的复印件、副本、电子文档均与原件或正本相同，且该等文件的内容系真实、准确和完整的，文件上的签字和盖章均是真实、有效的。文件的各方当事人均具有所有必要的授权且经过了所有必要的公示程序或采取了其他必要的行动，以签署文件和执行文件约定的事项，且均已正式授权、签署并交付这些文件。
- 2) 就公司无法提供的文件和资料，本所律师假设其所反映的情况不存在与公司已提供资料所反映的情况不一致甚至相反的情形。
- 3) 公司对本所律师的提问作出书面或口头说明、解释和陈述的有关人员均有完全民事行为能力并已得到适当授权回答本所律师的问题，且所有给予本所律师的说明、解释和陈述都是真实、准确、完全且没有误导的。
- 4) 公司及其相关负责人通过书面、口头方式向本所律师提供的信息是准确、完整的，该等信息已经充分、准确反映了目前公司在相应方面的最新情况。
- 5) 公司提供给本所律师的资料都是有效的，且没有在提供后被修改或更新。文件中所有的陈述和保证均准确，且所有条款均反映了当事人在签署文件时的真实意思。
- 6) 本备忘录得出的结论和建议仅针对截至最后实际可行日期的现行有效规范以及本所了解到的事实性陈述所作出。若后续监管规范或事实情况发生变更，本备忘录现有结论和建议可能不再适用。
- 7) 本所律师没有开展任何技术、商业、财务方面的尽职调查，本所律师在本备忘录中也不对有关技术、审计、投资和商业决策等专业事项发表评论。在本备忘录中涉及该内容时，均为严格按照公司所提供资料的内容引述或按照公司及相关负责人的书面及口头说明、解释、陈述的转述，且所述内容均已实际执行的前提之上，该等引述和转述不表明本所对有关事实、数据、结论的真实性和准确性作出任何明示或默示的认可或保证。
- 8) 本所律师无法采用技术检测手段，对尽调范围内的数据全生命周期处理、数据要素流转的情况，以及网络及数据安全防护措施、安全保障手段、

风险管理制度的执行及实际效果等进行核查验证和技术评估，本备忘录中涉及的该等内容及相应结论，均建立在公司提供的资料及说明真实、准确，且所述内容均已实际执行的前提之上。

- 9) 本备忘录仅包含了本所律师认为对公司的数据合规现有保护样态、内部合规体系建设、公司数据处理行为、网络及数据安全、外部舆论及不良历史事件等有重大影响的法律事实和问题，而非对本所律师了解到的公司全部情况进行描述。

本备忘录仅供公司本次发行并上市之目的使用，不得用作任何其他用途。未经本所事先书面同意，本备忘录（及其复印件）的全部或部分不得被用于任何其他目的，不得披露给与上述事项无关的任何第三方。引用本备忘录内容应保持内容原意，不得擅自增加、修改、曲解、误用、滥用引用内容。

如公司向本所提供的相关文件存在法律上的瑕疵或存在其他相反的证据，或前述陈述、保证和承诺不成立、不明确或虚假、有遗漏等，则本备忘录的相关表述与结论需要修正，且本所有权根据新的经证实的事实或文件，另行出具文件进行补充、说明或更正。

基于上述内容，本所按照中国境内律师行业公认的业务标准、道德规范和勤勉尽责精神，出具本备忘录如下：

一、网络安全审查、国家安全审查的适用分析

（一）关于关键信息基础设施运营者

《中华人民共和国网络安全法》（以下简称“《网络安全法》”）第三十五条，《网络安全审查办法》第二条、第五条，《关键信息基础设施安全保护条例》第十九条等规定，关键信息基础设施运营者采购网络产品和服务，影响或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。

《网络安全法》第三十一条，《关键信息基础设施安全保护条例》第二条等规定，“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。《关键信息基础设施安全保护条例》第二条、第八条至第十条等规定，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主管部门、监督管理部门是负责关键信息基础设施安全保护工作的部门（以下简称“**关基保护工作部门**”）；重要行业和领域的主管部门、监督管理部门结合本行业、本领域实际，制定关键信息基础设施认定规则，并报国务院公安部门备案；关基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。

根据公司的说明，截至最后实际可行日期，公司未收到中华人民共和国互联网信息办公室（以下简称“**网信办**”）、中华人民共和国公安部（以下简称“**公安部**”）及其下属单位等关基保护工作部门认定其属于关键信息基础设施运营者的任何通知，公司需依据《网络安全审查办法》第二条、第五条主动申报网络安全审查的可能性较低。

（二）关于赴国外上市

《网络安全审查办法》第七条规定，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，必须向网络安全审查办公室申报网络安全审查。

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。针对前述规定下的网络安全审查义务，本所律师受公司委托，于 2025 年 4 月向中国网络安全审查认证和市场监管大数据中心电话咨询，根据其接线人员的口头答复：赴香港上市不属于《网络安全审查办法》第七条中规定的“赴国外上市”情形，故无需主动申报网络安全审查。

因此，公司无需依据《网络安全审查办法》第七条履行向网络安全审查办公室申报网络安全审查义务。

（三）关于影响或可能影响国家安全

《网络安全审查办法》第二条规定，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，应当进行网络安全审查。

《中华人民共和国数据安全法》（以下简称“**《数据安全法》**”）第二十四条规定，国家建立数据安全审查制度，对影响或者可能影响国家安全的数据处理活动进行国家安全审查。《网络数据安全条例》第十三条规定，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。

针对“影响或可能影响国家安全”的具体认定规则，我国尚未出台明确规定。

《国家安全法》第二条规定，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。《网络安全审查办法》第十条规定了网络安全审查重点评估的国家安全风险因素：（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。

根据已审阅资料及公司的说明，截至最后实际可行日期，公司未收到网信办、公安部及其下属单位等关基保护工作部门认定其属于关键信息基础设施运营者的任何通知，也未收到中华人民共和国工业和信息化部（以下简称“**工信部**”）、网信办、国家市场监督管理总局、中华人民共和国商务部（以下简称“**商务部**”）等行业主管部门及其下属单位将其所处理的数据认定为核心数据、重要数据的任何通知，亦未收到任何部门认定其存在影响或可能影响国家安全的数据处理活动的任何通知。本所律师经公开检索工信部、广东省通信管理局、广州市工业和信息化局、国家市场监督管理总局（食品安全协调司、食品生产经营安全监督管理司、餐饮食品安全监督管理司）、广东省市场监督管理局、广州市广东省市场监督管理局、商务部、广东省商务厅、广州市商务局官方网站，亦未检索到公开的重要数据识别规范和目录。综合公司所处行业、处理的数据类型、性质，公司主营业务涉及上述国家安全风险因素的可能性较低。因此，公司因其业务影响或可能影响国家安全，从而需主动向网络安全审查办公室申报网络安全审查义务或按照国家有关规定进行国家安全审查的可能性较低。

（四）关于网络安全审查办公室依职权主动开展网络安全审查

《网络安全审查办法》第十六条规定，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，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，进行网络安全审查。

根据公司的说明，截至最后实际可行日期，公司未受到网络安全审查办公室、网信办、公安部等部门基于国家安全或其他任何理由对公司进行网络安全审查方面的任何调查，也未就此收到任何询问、通知或警告。如上文“一、（三）关于影响或可能影响国家安全”分析，公司主营业务涉及影响或可能影响国家安全风险因素的可能性较低，公司亦未收到任何部门认定其存在影响或可能影响国家安全的数据处理活动的任何通知，因此，公司因其业务被网络安全审查工作机制成员单位认为影响或可能影响国家安全，由网络安全审查办公室依职权主动进行网络安全审查的可能性较低。

（五）分析结论

综上分析，截至最后实际可行日期，公司无需依据《网络安全审查办法》第七条履行申报网络安全审查义务，公司被要求依据《网络安全审查办法》第二条、第五条主动申报网络安全审查，或被要求依据《数据安全法》第二十四条、《网络数据安全条例》第十三条主动申报国家安全审查义务的可能性较低。但是，鉴于当前网络安全及数据合规领域规则变动频繁，相关法律法规的颁布及修订存在不确定性，若相关规则发生变动、监管部门意见变化导致前述结论所依赖的前提条件不再成立，不排除前述分析结论随之发生变化的可能性。

二、数据出境安全评估的适用分析

《数据出境安全评估办法》于 2022 年 7 月 7 日发布并于 2022 年 9 月 1 日起施行；《促进和规范数据跨境流动规定》（以下简称“《数据跨境规定》”）于 2024 年 3 月 22 日颁布并施行。根据上述规定，数据处理者向境外提供数据，符合下列条件之一的，应当通过所在地省级网信部门向国家网信部门申报数据出境安全评估：（1）数据处理者向境外提供重要数据；（2）关键信息基础设施运营者和处理 100 万人以上个人信息的数据处理者向境外提供个人信息；（3）自当年 1 月 1 日起累计向境外提供 100 万人个人信息（不含敏感个人信息）或者 1 万人敏感个人信息的数据处理者；及（4）国家网信部门规定的其他需要申报数据出境安全评估的情形。关键信息基础设施运营者以外的数据处理者在以下情形应当与境外接收方订立个人信息出境标准合同或者通过个人信息保护认证：（1）

自当年1月1日起累计向境外提供10万人以上、不满100万人个人信息（不含敏感个人信息）；（2）自当年1月1日起累计向境外提供不满1万人敏感个人信息。前述情形属《数据跨境规定》第三条至第六条规定情形的，免于申报数据出境安全评估、订立个人信息出境标准合同或通过个人信息保护认证。

根据已审阅资料及公司的说明，截至最后实际可行日期，公司未将在中国境内收集和产生的数据传输至境外，境外机构、组织或者个人也无法查询、调取、下载、导出公司存储在中国境内的数据，公司亦不涉及《中华人民共和国个人信息保护法》（以下简称“《个人信息保护法》”）第三条第二款所规定的在境外处理境内自然人个人信息的情况。因此，公司无需依照前述《数据出境安全评估办法》等相关规定申报数据出境安全评估或履行其他数据出境相关义务。

三、网络安全、数据安全、个人信息保护合规情况

（一）网络安全、数据安全合规治理体系和技术措施

根据已审阅资料及公司的说明，公司依照《数据安全法》《网络安全法》《个人信息保护法》等法律法规的要求，进行数据合规内控管理制度的建设，截至最后实际可行日期，公司制定并实施的网络安全与个人信息保护相关的内控管理制度主要包括：《信息安全管理制度》《网络安全管理制度》《个人信息保护制度》《数据全生命周期安全管理规定》《数据分类分级制度》《网络举报及投诉处理制度》等。公司已经建立了数据合规和个人信息保护管理体系，信息技术部是公司履行网络安全及个人信息保护职责的管理机构，负责制定、完善公司内部数据合规相关制度，协调市场部、营运部、法务部、人力资源部等各部门共同贯彻落实数据合规相关制度及具体工作执行；针对公司的重要信息系统，公司已履行网络安全等级保护备案手续。

根据已审阅资料及公司的说明，公司在技术安全保护措施方面，针对信息系统访问控制制定并实施了一系列管理制度及保护措施，包括但不限于：采取了通信加密、存储加密、数据备份和通信校验等多种技术手段，并实施定期备份策略，记录和审计数据备份和恢复策略；采购了WAF服务（Web应用防火墙），对Web应用流量进行过滤、检测和阻止，防范恶意请求；使用了云平台监控服务来监控网络运行情况、云主机安全，实时监测和拦截恶意软件和病毒的传播，并依据《网络安全管理制度》通过技术手段持续监测、记录网络运行状态和安全事件，将相关日志保留至少六个月，以便于问题追踪和分析等。

（二）个人信息保护合规情况

根据已审阅的资料及公司的说明，并经本所律师适当核查，公司是一家现代中式面馆经营者，公司自主研发并运行了“遇数点餐平台-遇见小面+系统”（以下简称“**点餐系统**”），自营及特许经营餐厅的终端用户均可使用移动设备便捷地通过使用点餐系统前端网络产品（即“遇见小面+”微信小程序、“遇见小面”支付宝小程序及遇见小面 H5 点餐，下同）享受配餐、外卖、会员活动等服务。公司已制定并在点餐系统前端网络产品公示了《隐私政策》《第三方信息共享清单》《个人信息收集清单》，告知用户其个人信息处理的具体规则，包括公司收集、使用个人信息的情况以及收集敏感个人信息对用户权益造成的影响、个人信息权益响应机制等内容。公司曾委托第三方移动应用安全公司对遇见小面+小程序移动应用进行检测并出具的《遇见小面+小程序个人隐私合规检测报告》，根据该等报告，遇见小面+小程序移动应用经隐私合规专项测评不存在个人隐私违规问题。

根据已审阅的资料及公司的说明，公司在个人信息保护合规方面，根据业务场景进行了个人信息影响评估和个人信息保护合规内部审计工作，依据《个人信息保护法》第五十二条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，公司已通过《隐私政策》对外披露了个人信息保护负责人的联系方式，并已根据《关于开展个人信息保护负责人信息报送工作的公告》履行了信息报送手续。公司内控制度《个人信息保护制度》明确了信息技术部作为个人信息保护机构，主要职责包括：全面统筹实施组织内部的个人信息安全工作；制定、签发、实施、定期更新隐私政策和相关规程；建立、维护和更新组织所持有的个人信息清单（包括个人信息的类型、数量、来源、接收方等）和授权访问策略；组织开展个人信息安全影响评估、个人信息安全培训、个人信息保护审计；在产品或服务上线发布前进行检测，避免未知的个人信息收集、使用、共享等处理行为等事项。

（三）数据合规相关的重大诉讼、行政处罚、举报和投诉等情况

根据已审阅资料及公司的说明，并经本所律师适当核查，自 2022 年 1 月 1 日至最后实际可行日期，公司没有因违反网络安全、数据安全、个人信息保护法律规定的重大或正在进行的诉讼、仲裁、行政处罚，没有发生过重大网络安全和数据安全事件，没有收到或发出过与网络安全、数据安全、个人信息保护相关的警告函、律师函、声明，不存在网络安全、数据安全、个人信息保护受到企业客户、用户的重大投诉或举报等情况。

四、数据合规整体结论

针对中国境内日益加强的数据合规监管态势，公司已采取多维度、多环节的网络安全及数据合规保护措施，以尽可能确保其遵守现行有效的法律法规。公司未收到网信办、公安部及其下属单位等关基保护工作部门认定其属于关键信息基础设施运营者的任何通知。公司没有因违反网络安全、数据安全、个人信息保护法律规定的诉讼、仲裁、行政处罚，没有发生过重大网络安全和数据安全事件，没有收到或发出过与网络安全、数据安全、个人信息保护相关的警告函、律师函、声明，不存在网络安全、数据安全、个人信息保护受到企业客户、用户的重大投诉或举报等情况，也未涉及任何行政机关因网络安全审查或国家安全审查而进行的调查、通知、警告或处罚。公司亦密切跟进现有规范及监管发展，持续开展合规工作并保持对监管动向的敏感。

自 2022 年 1 月 1 日至最后实际可行日期，公司未因违反网络安全、数据安全及个人信息保护的监管要求而发生导致主营业务无法持续开展且无法整改的根本性瑕疵，公司已在所有重大方面基本满足网络安全、数据安全、个人信息保护方面的现行有效法律法规的要求。

鉴于中国境内的网络安全、数据安全、个人信息保护领域相关法律法规、监管要求处于不断发展变化中，公司在后续业务经营过程中应持续保持对合规要求的敏感度，积极配合最新监管规范，落实相应合规义务。

（以下无正文）

（本页无正文，为《关于广州遇见小面餐饮股份有限公司发行 H 股股票并在香港联合交易所有限公司主板上市涉及中华人民共和国境内数据合规之法律备忘录》之签字页）

北京市嘉源律师事务所

北京市嘉源律师事务所

2025 年 11 月 27 日