法律意见书

致　　：上海商米科技集团股份有限公司

Deutsche Securities Asia Limited（下称“Deutsche Securities”）
Level 60, International Commerce Centre, 1 Austin Road West, Kowloon, Hong Kong

Deutsche Bank AG, Hong Kong Branch[1]（下称“DB Hong Kong”）
Level 60, International Commerce Centre, 1 Austin Road West, Kowloon, Hong Kong

CITIC Securities (Hong Kong) Limited（下称“CITICS”）
18/F, One Pacific Place, 88 Queensway, Hong Kong

CLSA Limited（下称“CLSA”）
18/F, One Pacific Place, 88 Queensway, Hong Kong

ABCI Capital Limited（下称“ABCI Capital”）
11/F, Agricultural Bank of China Tower, 50 Connaught Road Central, Hong Kong

ABCI Securities Company Limited（下称“ABCI Securities”）
10/F, Agricultural Bank of China Tower, 50 Connaught Road Central, Hong Kong

CMB International Capital Limited（下称“CMBI”）
45/F, Champion Tower, 3 Garden Road, Central, Hong Kong

以及，2026年4月21日发布的招股说明书中定义的其他各包销商

[1] Deutsche Bank AG, Hong Kong Branch is incorporated in the Federal Republic of Germany and members' liability is limited.

（Deutsche Securities、CITICS和ABCI Capital统称为“联席保荐人”，DB Hong Kong、CLSA和ABCI Capital统称为“保荐人兼整体协调人”，DB Hong Kong、CLSA、ABCI Capital和CMBI统称为“整体协调人”）

自　　：Bay Winbird, A.P.C.

日期　：2026年4月21日

主题　：美国个人数据合规法律意见

背景

Bay Winbird, A.P.C.（下称“本所”）系一家美国律师事务所。本所受上海商米科技集团股份有限公司（下称“商米集团”）的委托，现就商米集团及旗下涉美国运营的子公司（下统称“公司”）在2022年1月1日至2026年4月13日期间涉及数据处理的美国核心业务的美国个人数据存储合规情况、美国个人数据跨境传输合规情况以及依据公司产品在美国的主要终端商户所在地的个人数据法律所涉个人数据合规情况作出本法律意见书（下称“本意见书”）。本意见书仅用于商米集团拟于近期在中国香港联合交易所有限公司上市（“本次发行上市”）所涉美国个人数据合规法律事项，除了联席保荐人、保荐人兼整体协调人、整体协调人及包销商（定义于与本次发行上市相关的招股书中）外的其他人士或实体不得使用本意见书。其他人士或实体无权以任何方式或为任何目的依赖或信赖本意见书。

事实依据

1. 一份由商米集团填写的美国个人数据合规尽职调查问卷清单（下称“尽职调查问卷”）。

2. 一份由商米集团出具的技术和组织措施清单。

3. 一份由商米集团出具的关于数据合规小组和数据合规官任命的公告。

4. 一份由商米集团出具的数据销毁管理制度。

5. 一份由商米集团出具的数据保存时间记录表。

6. 本所于2026年4月14日通过Westlaw（美国权威法律数据库）完成的公司在美国联邦与各州的诉讼案件检索（下称“案件检索”）。

7. 本所于2026年4月14日通过Westlaw完成的公司在美国联邦和各州的诉讼卷宗检索（下称“卷宗检索”）。

8. 本所于2026年4月14日通过加利福尼亚州司法部官网隐私执法行动名单和数据安全违规名单完成的公司加利福尼亚州数据安全和个人信息保护重大风险事件的检索（下称“加利福尼亚州司法部名单检索”）。

9. 本所于2026年4月14日通过加利福尼亚州隐私保护局官网公告栏目完成的涉及公司执法行动公告检索（下称“加利福尼亚州隐私保护局公告检索”）。

10. 本所于2026年4月14日在俄勒冈州司法部官网消费者隐私栏目完成的新闻检索。

11. 本所于2026年4月14日在俄勒冈州司法部官网完成的数据泄露名单检索。

12. 本所于2026年4月14日在德克萨斯州司法部官网完成的数据安全泄露报告检索。

13. 本所于2026年4月14日在佛罗里达州司法部官网完成的新闻检索。

14. 本所于2026年4月14日通过Westlaw完成的公司在美国联邦与各州的行政决定检索（下称“行政决定检索”）。

15. 商米集团出具并签署的《公司陈述》（Company Statement）。

假设

本意见书是基于以下假设出具的：

1. 本所的观点仅基于美国联邦、加利福尼亚州、俄勒冈州、德克萨斯州和佛罗里达州的个人数据相关成文法截至2026年4月13日已生效的版本和美国普通法，以及截至2026年4月13日可公开获取的信息，不对未来法律法规或司法解释变化承担责任，不针对前述法律之外的其他法律适用性提出法律意见。

2. 本所审阅过的所有文件和记录均准确和完整，文件上的所有签字以及提交给本所之原件均为真实，提交给本所的所有复印件或副本材料与原件一致。

3. 公司未隐瞒任何可能影响美国个人数据合规状态的重大事实。

4. 公司数据处理实践与尽职调查问卷、其所提交文件以及其人员沟通的描述一致。

5. 公司不掌握个人数据所涉消费者的年龄和地理位置。

6. 就对本意见书而言重要的事实问题，本所在我们认为适当的范围内合理依赖商米集团出具的文件、尽职调查问卷以及与商米集团人员的沟通，而未加以独立调查。

7. 本所不对美国任何单一州之判例进行穷尽式检索，本意见书中的普通法分析仅基于美国普通法共通原理与主流判例趋势所作。

法律分析

1. 公司产品在美国的主要终端商户所在地数据立法情况

1) 公司产品在美国的主要终端商户所在地：根据《公司陈述》，公司产品在美国的终端商户所在地集中在加利福尼亚州、德克萨斯州、纽约州、佛罗里达州、伊利诺伊州、马萨诸塞州、乔治亚州、宾夕法尼亚州、北卡罗来纳州、华盛顿州、俄亥俄州。

2) 公司产品在美国的主要终端商户所在地数据立法情况：公司产品在美国的主要终端商户所在地中，2026年4月13日之前已有生效个人数据立法的州为德克萨斯州、佛罗里达州和加利福尼亚州。德克萨斯州与个人数据相关的立法为《德克萨斯州数据隐私和安全法案》（Texas Data Privacy and Security Act，下称“TDPSA”），该法于2024年7月1日生效。佛罗里达州与个人数据相关的立法为《佛罗里达数字权利法案》（Florida Digital Bill of Rights，下称“FDBR”），该法于2024年7月1日生效。加利福尼亚州与个人数据相关的立法为《加利福尼亚州消费者隐私保护法》（California Consumer Privacy Act，下称“CCPA”），该法于2020年1月1日生效。

2. 德克萨斯州个人数据合规分析

1) TDPSA管辖规定：根据TDPSA第541.002条，TDPSA管辖的对象为同时满足以下三个条件的营利性实体：i）在德克萨斯州经营业务或生产德克萨斯州居民消费的产品或服务；ii）处理或出售个人数据；iii）不是美国小企业管理局（United States Small Business Administration）定义的小企业。TDPSA第541.001条第（15）和（19）款进一步规定，个人数据是指与已识别或可识别的消费者相关联或可合理关联的任何信息。TDPSA第541.001条第（7）款将消费者定义为仅在个人或家庭范围内活动的德克萨斯州居民，不包括在商业或雇佣关系下行事的个人。

2) TDPSA个人数据跨境传输规定：TDPSA无专门针对个人数据跨境传输的规定。

3) TDPSA执法与处罚相关规定：根据TDPSA第541.155条，德克萨斯州司法部部长有权对违反TDPSA的实体提起民事诉讼，请求法院对违规实体处以民事罚款和申请禁令。

4) 公司在德克萨斯州的数据处理情况：根据尽职调查问卷以及《公司陈述》，2022年1月1日至2026年4月13日期间，公司在美国的主要业务涉及收集与处理的数据仅限于商业关系下商户和商户员工的信息（即对外代表商户的电子邮件和用户昵称），既不处理也不出售非商业、非雇佣关系下行事的消费者的个人数据。

5) 公司在德克萨斯州的个人数据安全重大风险事件核查：根据尽职调查问卷，公司不涉及德克萨斯州个人数据安全重大风险事件（包括但不限于行政处罚、整改通知、诉讼纠纷等）。根据本所开展的案件检索与卷宗检索，截至2026年4月13日，未发现公司在德克萨斯州存在涉及违反TDPSA的诉讼纠纷。根据本所在德克萨斯州司法部官网开展的数据安全泄露报告检索，截至2026年4月13日，未发现公司被列入德克萨斯州数据安全泄露报告。

6) 结论：2022年1月1日至2024年6月30日期间，德克萨斯州没有生效的个人数据立法；2024年7月1日至2026年4月13日期间，公司不属于TDPSA管辖的实体，不适用TDPSA关于隐私与个人数据安全的规定。根据尽职调查问卷和本所的适当核查，截至2026年4月13日，公司不涉及德克萨斯州个人数据安全重大风险事件。

3. 佛罗里达州个人数据合规分析

1) FDBR管辖规定：根据FDBR第501.703条第（1）款，FDBR管辖的对象为同时满足以下两个条件的营利性实体：i）在佛罗里达州经营业务或生产佛罗里达州居民使用的产品或服务；ii）处理或参与出售个人数据。FDBR第501.702条第（16）和（19）款进一步规定，个人数据是指与已识别或可识别的消费者相关联或可合理关联的任何信息。FDBR第501.702条第（8）款将消费者定义为在个人或家庭范围内活动的佛罗里达州居民，不包括在商业或雇佣关系下行事的个人。

2) FDBR个人数据跨境传输规定：FDBR无专门针对个人数据跨境传输的规定。

3) FDBR执法与处罚相关规定：FDBR第501.72条规定，佛罗里达州法律事务部

（Department of Legal Affairs）可对违反FDBR的实体设定整改期，整改合格则不予起诉，不合格则启动民事诉讼，通过民事诉讼对违规实体处以民事罚款。

4) 公司在佛罗里达州的数据处理情况：根据尽职调查问卷以及《公司陈述》，2022年1月1日至2026年4月13日期间，公司在美国的主要业务涉及收集与处理的数据仅限于商业关系下商户和商户员工的信息（即对外代表商户的电子邮件和用户昵称），既不处理也不出售非商业、雇佣管辖下行事的消费者的个人数据。

5) 公司在佛罗里达州的个人数据安全重大风险事件核查：根据尽职调查问卷，公司不涉及佛罗里达州个人数据安全重大风险事件（包括但不限于行政处罚、整改通知、诉讼纠纷等）。根据本所开展的案件检索与卷宗检索，截至2026年4月13日，未发现公司在佛罗里达州存在涉及违反FDBR的诉讼纠纷。根据本所在佛罗里达州司法部官网开展的新闻检索，未发现公司被列入FDBR违规相关新闻。

6) 结论：在2022年1月1日至2024年6月30日期间，佛罗里达州没有生效的个人数据立法；在2024年7月1日至2026年4月13日期间，公司不属于FDBR管辖的实体，不适用FDBR关于个人数据安全的规定。根据尽职调查问卷和本所的适当核查，截至2026年4月13日，公司不涉及佛罗里达州个人数据安全重大风险事件。

4. 加利福尼亚州个人信息与数据合规分析

1) CCPA管辖适用分析

a) CCPA管辖规定：根据CCPA第1798.140条第（d）款，在加利福尼亚州开展商业活动，收集消费者[2]个人信息（Personal Information）[3]，并且符

[2] 依据CCPA第1798.140条第（i）款，消费者是指《加利福尼亚州法典》第18编第17014条定义的加利福尼亚州居民，包括：i) 非因临时或短暂目的在加利福尼亚州停留的自然人；ii) 在加利福尼亚州定居但因临时或短暂目的离开该州的任何自然人。

[3] 依据CCPA第1798.140.条第（v）款，个人信息指直接或间接识别、关联、描述特定消费者或家庭的信息，包括身份信息、商业信息、生物特征识别信息、网络活动信息、地理位置数据、教育信息、工作信息、财务信息、医疗健康信息等。

合以下任一条件的企业，属于CCPA管辖范围内的覆盖企业：i) 2020年至2024年，每年的年总收入[4]超过2500万美元，则下一日历年受CCPA管辖；2025年的年总收入超过2662.5万美元，则2026年受CCPA管辖；ii) 2020年至2022年，每年单独或组合购买、为企业商业目的接收、出售[5]或共享[6]5万及以上消费者（人）、家庭（户）或设备（台）的个人信息；2023年起，每年单独或组合购买、出售或共享10万及以上消费者（人）或家庭（户）的个人信息；iii) 每年出售或共享消费者个人信息的收入达到当年总收入50%。控制或受控于CCPA覆盖企业，且共用品牌和消费者个人信息的实体，也属于CCPA管辖的对象。

b) 商米集团在美运营主体与业务：根据尽职调查问卷，2022年1月1日至2026年4月13日期间，商米集团及旗下涉美国运营的子公司中，在美国开展商业活动并收集数据的主体包括：商米集团，SUNMI TECHNOLOGY HK LIMITED（中国香港注册，2022年首次在美国开展商业活动），SUNMI GLOBAL PTE. LTD.（新加坡注册，2023年首次在美国开展商业活动），SUNMI TECHNOLOGY US INC.（美国注册，2021年首次在美国开展商业活动）。SUNMI TECHNOLOGY HK LIMITED、SUNMI GLOBAL PTE. LTD.和SUNMI TECHNOLOGY US INC.是商米集团控制的全资子公司，共用品牌“SUNMI”和部分个人信息。公司属于物联网科技公司，核心业务系为商用领域提供智能IoT设备及相应配套的“端、云”一体化服务，公司面向美国的主要业务如下：i) 商米集团生产硬件产品和提供服务；ii) SUNMI TECHNOLOGY US INC.负责提供营销服务；iii) 2022年至2023年期间，商米集团主要通过渠道商[7]将硬

[4] CCPA未就年总收入（Annual Gross Revenue）进行界定，普遍共识是指企业的全美总收入，结合CCPA的表述，本意见书的年总收入指在一个完整的日历年度（1月1日至12月31日），在不扣除任何成本的前提下，企业在全美国境内的所有收入的总和。

[5] 依据CCPA第1798.140.条第（ad）（1）款，销售/出售（Sell）指企业通过金钱或其他有价值的对价，将消费者的个人信息提供给第三方的行为。

[6] 依据CCPA第1798.140条第（ah）款，共享（Share）是指为了跨情境行为广告，以口头、书面、电子或其他方式将消费者的个人信息共享、出租、发布、披露、传播、转让或其他方式提供给第三方，无论是否出于金钱或其他有价值的对价，包括企业与第三方之间为企业利益而进行跨情境行为广告的交易，而企业在其中没有交换金钱。

[7] 渠道商是批发商、经销商、零售商等第三方中间商。

件产品销售至美国各州；2023年起，硬件产品的美国销售主体由商米集团更换至SUNMI TECHNOLOGY HK LIMITED和SUNMI GLOBAL PTE. LTD.。

c) 公司2021年至2025年的年总收入：根据尽职调查问卷，2021年和2022年，商米集团在美国的年总收入均超过了2500万美元；2023年，公司各主体在美国的年总收入均未超过2500万美元；2024年，SUNMI GLOBAL PTE. LTD.在美国的年总收入超过了2500万美元；2025年公司各主体在美国的年总收入均未超过2662.5万美元。

d) 公司购买、接收、出售和共享消费者个人信息的情况：根据尽职调查问卷以及《公司陈述》，2020年至2022年，公司不存在购买和为企业商业目的接收、出售或共享消费者个人信息的行为；2023年1月1日至2026年4月13日期间，公司不存在购买、出售和共享消费者个人信息的行为。

e) 结论：仅根据尽职调查问卷，就本所所知，公司在2022年、2023年和2025年属于CCPA管辖的企业，适用CCPA的规定；公司在2024年和2026年不属于CCPA管辖的企业，不适用CCPA的规定。

2) 披露义务分析

a) CCPA披露义务规定：根据CCPA第1798.100条第（a）款，企业在收集消费者个人信息时，应当告知所收集的个人信息类别，收集与使用个人信息的目的、用途，是否出售或共享个人信息，个人信息保存期限或确定保存期限的标准，消费者享有的个人信息权利等事项。CCPA第1798.100条第（b）款规定，收集个人信息前的告知方式应当清晰、醒目，如在网站首页显示告知内容。CCPA第1798.135条第（a）款规定，企业网站主页应显示选择拒绝出售、共享个人信息和选择限制使用敏感个人信息（Sensitive personal information）[8]的标题与链接。根据CCPA第1798.130条第（5）款，企业应当定期更新隐私政策，披露个人信息收集与处理的情况、消费者享有的个人信息权利以及消费者请求行使个人信息权利的途径。

[8] 依据CCPA第1798.140.条第（ae）款，敏感个人信息是指证件信息、完整的财务账户访问信息、精准地理位置、种族或民族、公民或移民身份、宗教信仰、邮件或短信的内容、基因遗传数据、神经数据、唯一生物特征识别信息、健康信息、性生活或性取向的个人信息。根据CCPA第1798.120.条，自2026年1月1日起，16岁以下消费者的个人信息也被视为敏感个人信息。

b) 公司业务环节个人信息处理情况：根据尽职调查问卷，公司在2022年、2023年和2025年主要业务开展中存在收集与处理美国居民个人信息的情形，其中面向美国的应用程序为商米助手（SUNMI Assistant）；面向美国的网站包括：商米全球官网（SUNMI Official Website，网址：https://www.sunmi.com/en/），商米账户中心（SUNMI Account Center，网址：https://account.sunmi.com），商米合作伙伴平台（SUNMI Partner Platform，网址：https://partner.sunmi.com），商米数字店铺（SUNMI Digital Store，SUNMI Assistant APP的网页版，网址：https://store.sunmi.com），商米开发者（SUNMI developer，网址：https://developer.sunmi.com/en-US/），商米北美网站（SUNMI North America Website，网址：https://www.sunmi.us/en-US/）。根据尽职调查问卷，公司2022年、2023年和2025年收集的美国居民个人信息类型包括电话、电子邮箱地址、用户昵称、用户头像和性别，不涉及加利福尼亚州消费者敏感个人信息，也不涉及加利福尼亚州消费者个人信息的共享、销售，公司涉美国居民个人信息的主要业务环节详情见下表：

表 2 公司业务环节与数据处理情况

业务环节	数据处理情况说明		产品/服务对象	涉及的美国居民个人信息类型
销售环节	公司在大部分情况下，通过渠道商客户进行设备销售，仅收集少量渠道商客户的联系人信息等；此外，渠道商客户可能注册商米合作伙伴平台，以使用相关服务。 少部分情况下，直接对接终端商户销售，该场景涉及终端商户的个人信息。		渠道商客户、终端商户	商户联系人的昵称、邮箱
云端部署环节	公司提供设备且客户采购DMP服务	设备数据会存储于公司处，对于设备数据而言，公司为数据控制者。 渠道商客户需注册使用商米合作伙伴平台实现设备管理。	渠道商客户	商户联系人的邮箱、昵称
	客户采购公司定制化设备	设备数据虽存储于公司处，对于设备数据而言，公司是受托处理角色，渠道商客户为数据	渠道商客户	商户联系人的邮箱、昵称

业务环节	数据处理情况说明		产品/服务对象	涉及的美国居民个人信息类型
	（OEM模式）且客户使用公司提供的DMP服务	控制者，渠道商客户需注册使用商米合作伙伴平台实现设备管理。		
	公司直接向终端商户提供设备	公司会收集设备数据，公司是数据控制者。 商户需注册使用商米合作伙伴平台实现设备管理。	商户	商户联系人的邮箱、昵称
设备使用环节	设备通常不会收集终端消费者数据。 终端商户如果使用应用店铺（设备之中的App）、数字店铺、商米助手等产品，需要注册商米账户，公司会收集终端商户的账户注册数据、店铺数据、员工数据等（店铺信息和员工信息均为用户自行填写，数据均归用户所有）。		商户及商户员工	商户联系人及员工的邮箱、昵称、头像（昵称和头像可不设置）、性别
设备售后环节	在售后报修环节，终端商户可以自行或通过公司合作伙伴填写设备报修信息。		渠道商客户和商户	商户联系人的姓名、邮箱、电话

c) 公司披露义务履行情况：本所查阅了公司主要网站在2022年、2023年和2025年有效的在线隐私政策，所查阅的隐私政策链接均展示在网站首页，所查阅的隐私政策内容均披露了CCPA规定收集前应告知的基本事项以及请求行使个人信息权利的途径。

d) 结论：依据尽职调查问卷，就本所所知，公司在2022年、2023年和2025年不适用CCPA关于消费者敏感个人信息限制使用和个人信息共享、销售的披露义务的规定。依据尽职调查问卷以及《公司陈述》，并经本所对公司主要网站2022年、2023年和2025年有效隐私政策的查阅，本所认为公司2022年、2023年和2025年主要业务所涉消费者个人信息收集措施基本符合CCPA关于收集前告知义务的规定。

3) 消费者个人信息权利响应义务分析

a) CCPA个人信息权利响应规定：根据CCPA第1798.105条、第1798.106条、

第1798.110条、第1798.115条、第1798.120条、第1798.121条、第1798.125条、第1798.130条等规定，消费者有权请求删除、更正、访问其个人信息，有权拒绝出售、共享其个人信息（即选择退出权），有权限制使用其敏感个人信息，且不因行使权利而受到企业的歧视，非完全线上运营的企业应向消费者提供至少两种联系渠道，并在45天内或合理的延长期限内响应消费者的权利请求。

b) 公司的消费者权利响应义务履行情况：公司主要网站在2022年、2023年和2025年有效的在线隐私政策均对CCPA所要求的删除权、更正权和访问权进行了描述，用户可通过隐私政策中提供的两种途径行使权利，公司承诺可在15天内或其他法定期限内响应用户的权利请求，隐私政策未显示因消费者行使权利而降低服务质量或提高价格的歧视情形。另外，根据尽职调查问卷，公司2022年、2023年和2025年主要业务不涉及加利福尼亚州消费者敏感个人信息，也不涉及加利福尼亚州消费者个人信息的共享、销售。

c) 结论：依据尽职调查问卷，公司在2022年、2023年和2025年不适用CCPA关于消费者敏感个人信息限制权和选择退出权的响应义务规定。依据尽职调查问卷以及《公司陈述》，并经本所对公司主要网站2022年、2023年和2025年有效隐私政策的查阅，本所认为，公司2022年、2023年和2025年主要网站所涉消费者个人信息权利响应措施基本符合CCPA的规定。

4) 数据最小化义务分析

a) CCPA数据最小化规定：CCPA第1798.100条第（c）款规定，企业必须将收集、使用保存和共享消费者个人信息的范围限制在合理、必要且与实现允许的处理目的相称的范围内。

b) 公司数据最小化义务履行情况：公司主要网站在2022年、2023年和2025年有效的在线隐私政策均声明所收集的个人信息类型与业务必要性匹配，并承诺不会超出隐私政策声明的目的与范围收集和使用个人信息；隐私政策还声明仅在所述目的需要的最短期限内保存个人信息，若服务或运营终止将会删除或匿名化处理个人信息。商米集团提交的《数据保存时间记录表》显示，商米集团针对不同的数据类型规定了不同的数据保留期限，在商业协议履行结束、与客户终止合作以及技术或数据不再被需要时，将于合理期限内删除相关数据，其中客户联系人数据将在商

业目的最终终止6个月后予以删除。

c) 结论：依据尽职调查问卷、商米集团所提交文件并经本所对公司主要网站2022年、2023年和2025年有效隐私政策的查阅，本所认为，公司2022年、2023年和2025年主要业务所涉数据最小化措施符合CCPA关于数据最小化义务的规定。

5) 数据安全保护义务分析

a) CCPA数据安全规定：CCPA第1798.100条第（e）款规定，企业必须实施合理的安全措施，以保护个人信息免遭未经授权或非法的访问、破坏、使用、修改、披露。

b) 公司数据安全保护义务履行情况：根据商米集团提交的《技术和组织措施清单》，商米集团规定了保密措施、确保完整性的措施、确保可用性和抗逆性措施、定期审查措施等保护数据安全的措施。根据尽职调查问卷，公司对美国居民个人信息采取了https加密传输措施。根据尽职调查问卷，公司组建了专门的数据安全团队，发布了《关于数据合规小组和数据合规官任命的公告》以任命数据合规小组、外部数据合规官以及规定团队成员的定位、职责；公司每年至少组织一次针对公司员工的数据合规培训。

c) 结论：根据尽职调查问卷和商米集团所提交文件，就本所所知，公司已通过制定制度、采取加密措施、组建专门团队以及定期员工培训等措施，履行了CCPA规定的数据安全保护义务。

6) 第三方合规管理义务分析

a) CCPA第三方合规管理规定：CCPA第1798.100条第（d）款规定，企业向第三方出售、共享个人信息时，应当签订协议，约定CCPA相关个人信息保护事项。

b) 公司第三方合规管理义务履行情况：依据尽职调查问卷以及《公司陈述》，公司在2022年、2023年和2025年不涉及出售、共享加利福尼亚州消费者个人信息的行为。

c) 结论：根据尽职调查问卷以及《公司陈述》，就本所所知，公司在2022年、2023年和2025年不适用CCPA关于出售、共享的相关第三方合规管理义务规定。

7) 个人信息跨境传输合规分析：CCPA无专门针对个人信息跨境传输的规定，因此，2022年1月1日至2026年4月13日期间，公司在加利福尼亚州不涉及CCPA规定下的个人信息跨境传输合规问题。

8) CCPA执法与处罚相关规定：根据CCPA第1798.155条、第1798.199.10条、第1798.199.40条、第1798.199.90条等规定，加利福尼亚州隐私保护局（California Privacy Protection Agency）有权对CCPA违规企业采取行政执法行动，加利福尼亚州司法部部长有权通过民事诉讼对CCPA违规企业实施处罚。CCPA第1798.185条要求加利福尼亚州司法部部长立法规定，对存在消费者隐私安全重大风险的企业，施加风险评估（Risk Assessment）和网络安全审计义务。2025年，加利福尼亚隐私保护局修订了《CCPA规则》（California Consumer Privacy Act Regulations），根据修订后的《CCPA规则》第7150条，自2026年1月1日起，企业在进行以下几类个人信息处理活动之前必须开展风险评估：i) 出售、共享个人信息；ii）处理敏感个人信息；iii）使用自动化决策技术（Automated Decisionmaking Technology，简称“ADMT”）[9]对消费者做出重大决策；iv）利用对消费者的行为进行自动化推断和侧写；v）训练自动化决策技术；vi）其他被认定为可能对消费者隐私或安全构成重大风险的处理活动。截至2026年4月13日，加利福尼亚州暂未有关于网络安全审计义务的立法生效。

9) 公司在加利福尼亚州个人信息保护与数据合规重大风险事件核查：根据尽职调查问卷以及《公司陈述》，就本所所知，公司在2026年不适用CCPA关于个人信息处理风险评估的规定。根据尽职调查问卷并经本所开展的加利福尼亚州司法部名单检索和加利福尼亚州隐私保护局公告检索，截至2026年4月13日，未发现公司被列入加利福尼亚州司法部隐私执法行动名单、加利福尼亚州司法部数据安全违规名单；截至2026年4月13日，未发现公司被列入加利福尼亚州隐私保护局执法行动公告。根据本所开展的案件检索与卷宗检索，截至2026年4月13日，未发现公司在加利福尼亚州存在涉及违反CCPA的诉

[9] 根据《CCPA规则》第7001条第（e）款，自动化决策技术是指任何处理个人信息并通过计算替代或实质性替代人类决策的技术。其中，“实质性替代人类决策”指企业仅依据该技术输出结果作出决策，且不涉及人类参与。人类参与要求人工审核者：（i）掌握解读并运用技术输出结果进行决策的能力；（ii）审核分析技术输出结果及任何与决策制定或变更相关的其他信息；（iii）基于（ii）项分析结果拥有决策制定或变更的权限。替代人类决策或实质性替代人类决策的用户画像（profiling）分析属于自动决策技术范畴。网页托管、域名注册、网络连接、缓存服务、网站加载、数据存储、防火墙、防病毒、反恶意软件、垃圾邮件及自动呼叫过滤、拼写检查、计算器、数据库及电子表格等服务不属于自动决策技术范畴，前提是这些服务不替代人类决策。

讼纠纷。

5. 美国数据存储地数据合规分析

1) 数据存储地个人数据立法：根据尽职调查问卷以及《公司陈述》，2024年1月1日之前，公司收集的数据均未存储在美国境内；2024年1月1日起，公司在美国收集的数据存储在美国俄勒冈州的AWS服务器中。美国俄勒冈州于2023年颁布了《俄勒冈州消费者隐私保护法》（Oregon Consumer Privacy Act，下称“OCPA”），该法于2024年7月1日生效。

2) OCPA管辖规定：根据OCPA第646A.572条，受OCPA管辖的对象为在俄勒冈州开展商业活动，或生产面向俄勒冈州居民的产品或服务，并在日历年内控制或处理以下任一类个人数据的实体：

   a) 控制或处理10万名或以上的俄勒冈州消费者的个人数据，不包括仅为完成支付交易而处理的个人数据；

   b) 当超过25%的总收入来自个人数据销售时，控制或处理25,000名或以上的俄勒冈州消费者的个人数据；

   OCPA第646A.570条第（13）款进一步规定，个人数据是指与消费者相关联或可合理关联的数据、衍生数据或任何唯一标识符，或与家庭中一名或多名消费者相关联、可识别其身份或可合理关联的设备数据。OCPA第646A.570条第（7）款将消费者定义为居住在俄勒冈州且以商业或雇佣关系以外的身份行事的自然人。

3) OCPA个人数据跨境传输规定：OCPA无专门针对个人数据跨境传输的规定。

4) OCPA执法与处罚相关规定：根据OCPA第646A.589条，俄勒冈州司法部部长有权对违反OCPA的实体提起民事诉讼，请求法院对违规实体处以民事罚款、申请禁令以及请求违规实体赔偿损失。

5) 公司在俄勒冈州的个人数据处理情况：根据尽职调查问卷和《公司陈述》，公司在俄勒冈州的AWS服务器存储的全美用户注册数量如下：2024年7月1日至2024年12月31日，用户注册数量为102名；2025年用户注册数量为727名；2026年1月1日至4月13日用户注册数量为870名。根据尽职调查问卷以及《公司陈述》，2022年1月1日至2026年4月13日期间，公司在美国的主要业务

涉及收集与处理的数据仅限于商业关系下商户和商户员工的信息(即对外代表商户的电子邮件和用户昵称），公司AWS服务器存储的美国用户信息均为商业关系下商户或商户员工的信息，公司既不处理也不出售以非商业关系、非雇佣关系身份行事的消费者的个人数据。根据尽职调查问卷和《公司陈述》，2022年1月1日至2026年4月13日期间，公司不存在将个人数据从美国境内传输至美国境外的情形。

6) 公司在俄勒冈州的个人数据安全重大风险事件核查：根据尽职调查问卷，公司不存在俄勒冈州个人数据安全重大风险事件（包括但不限于行政处罚、整改通知、诉讼纠纷等）。根据本所开展的案件检索与卷宗检索，截至2026年4月13日，未发现公司在俄勒冈州存在涉及违反OCPA的诉讼纠纷。根据本所在俄勒冈州司法部官网消费者隐私栏目开展的新闻检索和数据泄露名单检索，截至2026年4月13日，未发现公司被列入OCPA违规相关新闻与数据泄露名单。

7) 结论：根据尽职调查问卷以及《公司陈述》，在2022年1月1日至2023年12月31日期间，公司不存在于美国本土存储数据的情形。在2024年1月1日至2024年6月30日期间，公司在美国本土数据存储所在地俄勒冈州没有生效个人数据立法；在2024年7月1日至2026年4月13日期间，公司不属于OCPA管辖的实体，不适用OCPA关于个人数据与消费者隐私保护的规定。根据尽职调查问卷和本所的适当核查，截至2026年4月13日，公司不涉及俄勒冈州个人数据安全重大风险事件。

6. 美国联邦个人数据跨境传输合规分析

1) 美国联邦关于个人数据跨境传输的规定：根据2024年2月28日发布的第14117号总统行政令《防止受关注国家访问美国敏感个人数据和政府相关数据》（Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern）（下称“《14117行政令》”）和美国司法部于2025年1月8日发布并于2025年4月8日生效的《防止受关注国家或相关实体获取美国敏感个人数据和政府相关数据的规定》（Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons）（下称“《14117行政令最

终规则》”），依据美国法律设立的法律主体与“受关注国家”及其相关的“涵盖主体”实体的跨境传输受规制的数据时，需要根据不同的数据类型履行相应的合规义务。根据《14117行政令最终规则》，“受规制的数据类型”为美国人敏感个人数据和美国政府相关数据；根据《14117行政令最终规则》第202.249条，“美国人敏感个人数据”是指美国人的个人标识符、精确的地理位置数据、生物标识符、人体数据、个人健康数据、个人财务数据及其任意组合；根据《14117行政令最终规则》第202.222条，“美国政府相关数据”指特定的政府地理位置信息和联邦政府（包括军方和情报机构）前雇员/承包商或现雇员/承包商或者前任高级官员的敏感个人数据，无论数量多少。

2) 公司在美国的个人数据跨境传输情况：根据尽职调查问卷与《公司陈述》，2022年1月1日至2026年4月13日期间，公司在美国的主要业务涉及收集与处理的数据仅限于商业关系下商户和商户员工的信息（即对外代表商户的电子邮件和用户昵称），不涉及美国人的敏感个人数据和美国政府相关数据，公司不存在将个人数据从美国境内传输至美国境外的情形。

3) 结论：2022年1月1日至2025年4月7日，美国联邦没有生效的个人数据跨境传输相关立法，公司的主要业务在美国联邦不涉及个人数据跨境数据合规问题。2025年4月8日至2026年4月13日期间，公司在美国的主要业务不涉及美国人的敏感个人数据和美国政府相关数据，不涉及《14117行政令最终规则》所规制的个人数据类型，不适用《14117行政令最终规则》关于数据跨境传输的规定。

7. 美国普通法分析

1) 美国普通法原则：美国普通法（Common Law）普遍承认基于侵权法、合同法及衡平法理之义务。虽然各州判例存在差异，但企业个人数据合规问题通常适用的美国普通法原则主要包括以下几个方面：i）过失原则，行为人负有合理注意义务，若因疏忽或未尽义务导致他人损害，可能构成过失；ii）履约与违约，当存在明示或默示契约时，契约相对人应当履行契约，若违反约定，可能构成违约；iii）侵权责任，当行为人侵犯了他人享有的权利，基于适用的归责原则，行为人可能构成侵权，受害者可通过民事诉讼要求赔偿。相对于成文法和行政法规，以上普通法原则较为抽象，往往用于事后纠纷的

解决，但难以事先规定企业在具体情境下的行为特征。

2) 公司对美国普通法原则的履行情况：根据尽职调查问卷、商米集团提供的文件、《公司陈述》、诉讼检索和行政决定检索，2022年1月1日至2026年4月13日期间，公司已通过制定数据安全制度、采取数据最小化措施、采取https加密传输措施、规定不同的数据保留期限、组建专门团队处理应急事件以及定期员工培训等合规工作保障个人数据安全，公司在美国的主要业务不存在需要事后适用美国普通法原则的个人数据相关纠纷。

3) 结论：根据尽职调查问卷、商米集团提供的文件、《公司陈述》、诉讼检索和行政决定检索，本所未发现2022年1月1日至2026年4月13日期间公司在美国开展主要业务过程中所涉个人数据安全事项存在严重违反美国普通法原则的情形。

法律意见

1. 公司在全美境内的个人数据安全重大风险事件核查

1) 诉讼检索：根据本所开展的案件检索，截至2026年4月13日，未发现公司在美国联邦与各州存在涉及个人数据安全的诉讼纠纷。根据本所开展的卷宗检索，截至2026年4月13日，未发现公司在美国联邦与各州存在涉及个人数据安全的诉讼纠纷。

2) 行政决定检索：根据本所开展的行政决定检索，截至2026年4月13日，未发现公司在美国联邦与各州存在涉及个人数据安全的行政决定。

3) 结论：根据尽职调查问卷以及本所开展的案件检索、卷宗检索、行政决定检索，截至2026年4月13日，未发现公司在美国联邦和各州存在个人数据安全重大风险事件（包括但不限于执法行动、行政处罚、整改通知、诉讼纠纷等）。

2. 结论

基于且受限于上述情况及至文尾所列之情况，本所意见如下：

根据上述核查和分析，本所认为，在2024年1月1日至2024年6月30日期间，公司的数据存储地俄勒冈州没有生效的个人数据立法；2024年7月1日至2026年4月13日期间，公司在美国的数据存储地俄勒冈州的个人数据立法OCPA无专门针对个人数据跨境传输的规定，同时，公司未达到OCPA的管辖门槛，不适用OCPA的规定。2022年1月1日至2024年6月30日期间，除加利福尼亚州以外，公司产品在美国主要终端商户所在地均没有生效的个人数据立法。2024年7月1日至2026年4月13日期间，公司产品在美国的主要终端商户所在地德克萨斯州个人数据立法TDPSA和佛罗里达州个人数据立法FDBR均没有专门针对个人数据跨境传输的规定，同时，公司未达到TDPSA和FDBR的管辖门槛，不适用TDPSA和FDBR的规定。2022年、2023年和2025年期间，公司在美国加利福尼亚州开展主要业务过程中采取了必要的个人信息保护合规措施，基本符合CCPA关于消费者个人信息权利保障的主要规定。2024年和2026年，公司未达到CCPA管辖门槛，因此不适用CCPA的规定。2022年1月1日至2026年4月13日期间，公司在加利福尼亚州不涉及个人信息处理风险评估和网络安全审计，同时，由于CCPA无专门针对个人数据跨境传输的规定，公司在加利福尼亚州不涉及CCPA规定下的个人数据跨境传输合规问题。2022年1月1日至2026年4月13日期间，公司在美国开展主要业务过程中所涉个人数据安全事项不存在严重违反美国普通法原则之情形。2022年1月1日至2025年4月7日期间，美国联邦没有生效的个人数据跨境传输相关立法；2025年4月8日至2026年4月13日期间，公司不适用美国联邦涉及个人数据跨境传输的立法《14117行政令最终规则》的数据跨境传输规定。截至2026年4月13日，公司在美国联邦与各州不存在重大的个人信息与数据保护违规风险事件（包括但不限于执法行动、行政处罚、整改通知、诉讼纠纷等），不存在对公司业务运营及对本次发行上市产生重大不利影响的情形，公司在美国的运营在重大方面符合适用的美国数据法律法规。但是，根据CCPA的规定，公司仍应在网站披露事项等方面进行完善和整改。另外，鉴于美国对个人数据合规的日趋严格，建议公司密切关注美国个人数据相关立法与执法动态，及时调整合规措施，以满足美国关于个人数据合规的最新要求。

本所的上述意见受限于第三方意见常规引用的美国联邦、美国加利福尼亚州、美国俄勒冈州、德克萨斯州和佛罗里达州的成文法和美国普通法，我们并不在本意

见书中就任何其它司法管辖区域的法律发表意见。此外，我们未在本意见书中就任何郡、县、市或特定的行政区域（无论是通过联邦、州，或是地区层面的立法行为所创设或授权的行政区域）的任何法规、条例、行政决定、规则或规定发表意见。本意见书于文首所示之日出具，本所不就此后可能令我们关注的变化向您承担提醒义务。

Bay Winbird, A.P.C.

Bay Winbird, A.P.C.