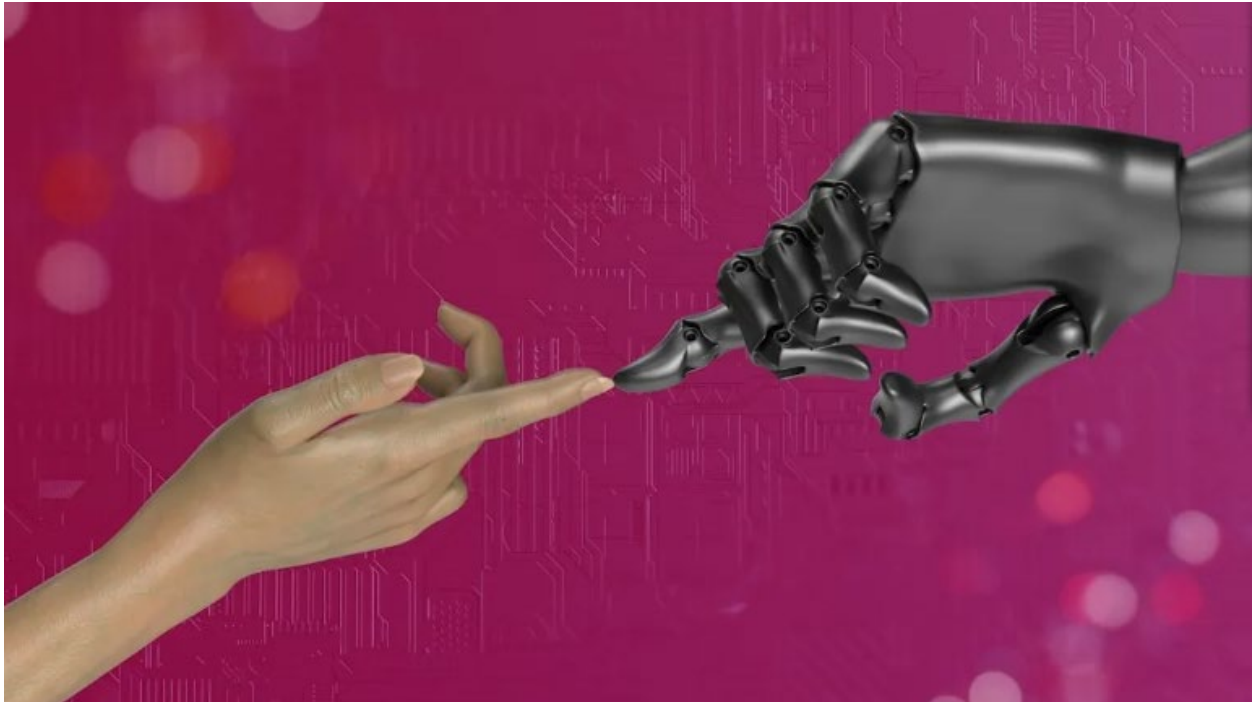


香港《生成式人工智能技术及应用指引》在金融市场上的应用



香港政府数字政策办公室（DPO）在 2025 年 4 月 15 日发布了《香港生成式人工智能技术及应用指引》（指引）。这份指引针对技术开发者、服务提供商和使用者，提供关于生成式人工智能（AI）使用的实用建议，探讨其应用范围、局限性和潜在风险。关键的治理原则着重于解决数据泄露、模型偏见和错误等问题。

指引与香港生成式人工智能研发中心（HKGAI）合作制定，该中心收集了业界意见和实务应用研究，就生成式 AI 提出准确性、问责性及信息安全三方面标准。其主要目标是平衡创新发展和社会责任，建立一个符合香港及各持份者需求的治理框架。该指引旨在促进生成式 AI 安全和负责任地发展，同时鼓励创新和在香港的广泛应用。

在香港开发、部署和应用生成式 AI 技术必须严格遵守所有相关法律、政策和监管标准，包括遵守个人资料（私隐）条例（第 486 章）、人工智能道德框架和《香港生成式人工智能技术及应用指引》，强调保护个人私隐、知识产权和数据安全。

技术开发者必须确保数据收集遵守知识产权法和隐私保护规定，而由人工智能生成的内容不得违反公共道德、隐私权益或现行法律规定。

服务提供商和使用者也有责任防止虚假或有害信息的传播，符合政府的数据治理原则，优先考虑安全的数据流动和合乎道德的人工智能实践。

在金融市场上负责任地应用生成式 AI

2024 年 10 月上旬，香港财经事务及库务局发布了关于在金融市场上负责任地应用 AI 的政策声明，旨在平衡促进 AI 发展的同时，应对与网络安全、知识产权和数据隐私相关的风险。

为了充分利用 AI 的优点并应对其挑战，香港正在采取双轨模式。这一策略在促进金融服务业内的 AI 发展的同时，解决了网络安全、数据隐私和知识产权保护等重要问题。通过与金融监管机构和行业持份者密切合作，这一方法旨在创建一个可持续发展的平衡生态环境，既拥抱机遇又化解风险。最终目标是使金融机构能够负责任地应用 AI，促进创新的同时防范潜在风险。

将 AI 应用于金融服务业具有三个关键特点，称为「3D」：

1. 数据导向（Data-driven）：AI 通过实现先进的数据分析，提高了数据密集型行业的效率和竞争力。
2. 双面效果（Double-edged）：尽管 AI 提供了巨大潜力，但不当使用可能导致重大风险。金融机构必须全方位管控相关风险，确保 AI 作为人类判断的补充工具，增强而非取代人类决策。
3. 充满活力（Dynamic）：AI 促进创新，有助于打造更加活跃和多样化的金融服务生态系统。

为确保 AI 的负责任使用，政府强调保护隐私和知识产权、人为监督、问责、运作弹性、信息安全，以及就业安全的重要性。

金融机构应制定 AI 治理策略，为如何实施及使用 AI 系统提供方向。在 AI 系统的采购、使用及管理上应采用风险为本的方法，而人为监督对缓解潜在风险至关重要。

为了减轻风险，金融机构应实施强大的网络安全防护体系，确保严格遵守数据隐私法规，并尊重知识产权，以防止敏感信息被不当使用。对于验证 AI 输出，人为监督至关重要，以及持续监控以解决随时间而来的模型漂移等问题。机构必须明确披露他们使用 AI 的情况以及模型的基本原则，特别是当 AI 影响业务决策时，确保客户和投资者了解其数据的收集、处理和使用方式，以避免构成歧视性后果。为了保持金融稳定性和运作弹性，机构应制定应急计划，以确保在服务中断或 AI 系统故障时的持续运行。此外，加强的 AI 检测系统对于识别和打击复杂的欺诈行为至关重要，并应鼓励业界合作，以有效对抗网络犯罪威胁。对于员工，提供重新培训和提升技能的计划以帮助他们适应由 AI 技术塑造的职能变革同样至关重要。

政府表明与 AI 相关的风险在现行金融法规和指引中得到了充分的处理。为跟上不断发展的 AI 技术，金融监管机构计划定期审查和修改现行法规。与此同时，香港警务处已与国际组织、不同司法管辖区的执法机构以及行业合作，应对由 AI 带来的网络安全挑战，强调信息分享和合作在打击这些新兴威胁中的重要性。

如想进一步了解我们可如何协助您在金融市场应用生成式人工智能中确保合规，请扫描下方二维码，探索我们量身打造的法律服务。



本资讯内容仅供参考及不应被依据作为法律意见。

© 2025 JCHM Limited. All rights reserved.