企业使用人工智能代理进行流程自动化的法律风险

在香港将人工智能应用于流程自动化的企业，必须在《个人资料(私隐)条例》、相关网络安全要求及国家安全法等法规的框架下，谨慎管理复杂的法律风险。香港个人资料私隐专员公署近期的合规评估显示，监管机构会不断加强对人工智能治理及个人资料保护的监察。

香港个人资料私隐专员公署(私隐专员公署)于 2025 年公布已完成对 60 间机构使用人工智能情况的合规评估。在香港金融与科技高度发展的环境下，监管机关对人工智能治理及个人资料保障正不断加强监察，并调整企业将人工智能整合至流程自动化时的监管期望与合规要求。

1. **香港有关人工智能的监管框架**

关键定义及法定条文

人工智能代理指采用机器学习算法，以自治方式执行任务的软件系统，范畴包括但不限于客户互动、营销分析及合规工作。《个人资料（私隐）条例》（第 486 章）规管个人资料的收集、处理及保安。第 2 条将「个人资料」界定为任何与在世个人直接或间接相关的数据，且从该数据可切实可行地确定该个人身份。

私隐专员公署为执行《个人资料（私隐）条例》的法定机关，负责发布指引及进行合规审查。《附表 1》所载之六项数据保护原则构成数据处理义务的基础，涵盖目的与收集（DPP1）、准确性与保留（DPP2）、使用（DPP3）、保安（DPP4）、透明度（DPP5）及存取与更正（DPP6）。

适用法例与指引

在尚无专门人工智能法例的情况下，香港主要依赖现行法例。上述《个人资料（私隐）条例》处理私隐事宜；另有警方科技罪案及网络安全相关部门就网络安全事宜行使监管职能，以及香港金融管理局、证券及期货事务监察委员会等机构发出的行业指引。《中华人民共和国香港特别行政区维护国家安全法》亦在人工智能应用牵涉可能影响国家安全的数据（尤其涉及跨境转移）时，构成适用的规范来源，可参照相关条文。

非具约束力方面，包括私隐专员公署于 2024 年发布的《人工智能：个人资料保障模范框架》，及政府数码政策办公室 2024 年发布的《人工智能道德框架》。该等文件倡导以风险为本的人工智能治理及伦理部署原则。

2. 合规义务与风险缓解策略

来自私隐专员公署合规评估的见解

私隐专员公署于 2025 年的评估指出，受审查机构中有 80%部署了人工智能系统，其中约一半在人工智能系统中处理个人资料。评估未发现违反《个人资料（私隐）条例》的个案，显示多数机构已采取符合数据保护原则的措施。公署强调治理、透明度与风险缓解的重要性，并特别指出保留人为监督以维持问责制在人工智能驱动流程中的关键地位。

建议的治理措施

《个人资料保障模范框架》阐明与数据最少化（与数据使用限制相应）、取得同意、公司治理及事故应变计划相关的义务。私隐专员公署于 2025 年发布的员工使用生成式人工智能指引检查表，亦就内部使用程序提出要求。评估之实证数据显示，受审机构中 79%已设置人工智能治理架构，83%进行了私隐影响评估，92%建立了数据泄露应对机制。企业应建立风险评估、审计日志及透明度机制，以确保遵从条例要求。

营运层面的建议

企业应制定全面的治理框架，包括人工智能政策、监督委员会及员工培训计划。定期合规审计、设置人为介入机制及持续监察不可或缺。法律顾问在厘清数据保护与人工智能治理具关键作用，有助企业进行严格审计并向持份者作出恰当披露。

许多人工智能代理在输出结束时会附上免责声明，说明系统的局限性。该等免责声明一方面可提升对数据当事人的透明度，另一方面亦表明人工智能的输出属建议性，可能存在错误。人工智能能显著加快例行流程、提升处理量及降低营运成本，但在处理具微妙差异、依赖情景或涉及伦理敏感的事务上，其能力较为有限，这类事项通常需要专业判断、同理心或酌情决策。实务上，针对风险较高的决策，常见的部署方式是将自动化代理与人为介入（human-in-the-loop）结合，并设置升级机制及保存依赖人工智能输出的纪录。

3. 与人工智能部署相关之法律及营运风险

涉及私隐与问责的风险

人工智能系统的固有弱点，例如在训练模型时无意中纳入个人资料，或算法出现偏差，可能导致数据泄露或滥用，从而触发《个人资料（私隐）条例》下的法律责任。根据该条例第 64(1)条，未经许可披露或使用个人资料，如致伤害或金钱损失，可处以最高港币 1,000,000 元罚款及监禁五年。此外，根据第 26 条，未能按时删除为收集目的所需之个人资料亦属违例，监管机关可发出执行通知或处以制裁。

当人工智能的输出影响各持份者时，可能触犯《公司条例》（第 622 章）第 465 至 466 条项下规定的公司董事的受托责任（要求董事本着诚信原则，善意行事，并以应有的谨慎、技能和勤勉履行其职责），问责难题随之产生。就上市公司而言，人工智能错误产生之披露或陈述，可能触及《证券及期货条例》（第 571 章）之招股书及相关责任，令公司面临因误导性陈述而引致的民事追偿。企业应就人工智能决策明确划分责任，以减低因替代责任或其他民事责任而产生的风险。

跨境转移与国家安全考虑

香港并无数据本地化的普遍要求，容许数据跨境转移，但须遵守数据使用限制（与《个人资料（私隐）条例》相关）及有关行业监管指引，例如香港金融管理局就外判及使用外部供货商所发的监督指引(SA-2)。若人工智能系统处理可能涉及国家安全的资料，则可能触及《中华人民共和国香港特别行政区维护国家安全法》之规定；跨境数据流通若引发国家安全疑虑，或会引致监管审查及进一步的法律后果。

欠缺全面的网络安全措施可能使企业面临私隐法例的执法风险，包括就未经授权披露而承担罚则。虽然现时并无统一的强制通报义务，但私隐专员公署建议在适当情况下尽快向有关当局报告资料外泄事件。企业应采取实务性保安措施，例如加密、访问控制及记录，以防范数据外泄，同时注意人工智能的威胁，如 AI 提示注入等。

人工智能「幻觉」与错误带来的挑战

生成式模型出现「幻觉」——即产出看似可信但实际错误或虚构的内容——在法律敏感领域（如合规报告或争议处理）构成重大风险。倚赖错误的人工智能输出可能引致普通法上的疏忽责任，原告须证明存在注意义务、违反该义务及因果关系，并考虑可预见性。在专业服务范畴，亦可能构成违反合约之默示条款或专业疏忽，并涉及相关法例或行业守则所规定的义务。

例如，在美国案件 Mata v. Avianca（2023）中，一名律师在法庭档中倚赖 ChatGPT 生成并引用法律先例，而该等所称先例其后被发现完全为捏造，法院因该律师的疏忽及提交误导性资料而对其施以制裁。

由于人工智能并非法律主体，相关责任通常由开发者（就设计或产品缺陷而言）或部署者（就营运与监督不足而言）承担。人为监督可减低错误风险，并应采取措施防止模型产生偏见或歧视性结果，以免触犯其他相关法例，从而招致歧视索偿及赔偿责任。

监管分散与技术快速演变之挑战

香港现时的监管架构呈多机构参与的情况，涉及包括私隐专员公署、香港金融管理局、证券及期货事务监察委员会及创新科技及工业局等机构。此种分散的监管架构增加了合规的复杂性。另方面，人工智能技术迅速更新，令合规范畴出现不确定性。企业须采取具弹性的治理及合规安排，以避免触犯不同法例或指引，例如就人工智能驱动的营销活动须留意《非应邀电子讯息条例》（第 593 章）之规定，以及在使用训练数据时遵守《版权条例》（第 528 章）之要求。

结论

在香港将人工智能应用于流程自动化的企业，须在《个人资料（私隐）条例》、相关网络安全要求及国家安全法的框架下，谨慎部署及管理风险。透过建立严谨的治理架构、先行的合规措施及完善的网络保安，企业可以减低包括由人工智能幻觉及技术快速变迁所带来的风险。持续监察并与监管指引保持一致，对在不断发展的环境下谨慎采用人工智能至为重要。

若您希望在采用人工智能时减低数据私隐及网络安全的风险，请扫描下方二维码，了解我们的服务并与我们联系获取所需的法律服务。

本信息内容仅供参考及不应被依据作为法律意见。