

人工智能中的健康数据与生物识别数据之监管风险

人工智能为香港企业带来创新，但同时亦需谨慎处理健康与生物识别数据以确保私隐与合规



人工智能的应用正在改变商业环境，使金融、医疗、零售和科技等行业的企业能够提升运营效率并提供个人化服务。处理敏感个人资料，例如健康记录和生物识别标识，是许多人工智能应用的基础，为创新提供了重大机遇。然而，这些技术进展亦引发对私隐同数据保护的关注，并受到香港《个人资料（私隐）条例》（第 486 章）的严格监管。违反《个人资料（私隐）条例》可能导致罚款、法律责任和声誉损害。个人资料私隐专员公署于 2024 年发布了《人工智能：个人资料保护模范框架》，以指导机构管理人工智能相关的私隐风险。本文探讨《个人资料（私隐）条例》、《人工智能：个人资料保护模范框架》、处理敏感数据的监管风险、合规策略以及不断演变的监管环境，为香港的商业经营者提供实用指引。

《个人资料（私隐）条例》

《个人资料（私隐）条例》规管个人资料的收集、处理和使用，个人资料定义为任何直接或间接与一名在世的个人有关的数据，从该数据直接或间接地确定有关个人的身分是切实可行的；及该数据的存在形式令予以查阅及处理均是切实可行的。这包括敏感的健康记录（例如医疗诊断、遗传档案）和生物识别标识（例如面部扫描、指纹）。该条例适用于在香港辖区内运营的所有机构，由个人资料私隐专员公署管理，并以六项数据保护原则为结构：

1. 目的与收集原则：个人资料必须为与机构功能直接相关的合法目的而收集。
2. 准确性与保留原则：数据必须准确、更新，且不超出其预定目的。
3. 使用原则：资料仅可用于收集时的目的，除非获得进一步同意。
4. 保安原则：必须采取合理措施保护数据免受未经授权的访问、丢失或滥用。
5. 信息原则：必须通过个人资料收集声明告知个人其数据的用途。
6. 查阅与更正原则：个人有权查阅和更正其个人资料。

不遵守这些原则可能导致个人资料私隐专员公署发出执法通知，违反通知构成刑事罪行，可被罚款最高 50,000 港元，加上每日罚款 1,000 港元及监禁两年。错误处理敏感数据亦可能导致声誉损害和民事索偿。一经再次定罪，最高可被判罚款 100,000 港元及监禁 2 年，加上每日罚款 2,000 港元。

《人工智能：个人资料保护模范框架》

个人资料私隐专员公署于 2024 年 6 月 11 日发布了《人工智能：个人资料保护模范框架》，以应对人工智能系统处理个人资料（特别是健康记录和生物识别标识）所带来的私隐风险。该非约束性框架扩展了 2021 年《开发及使用人工智能道德标准指引》，针对使用人工智能系统的机构，提供《个人资料（私隐）条例》合规性和道德使用人工智能的结构化指引。框架包括 4 个关键领域：

1. 人工智能策略与治理：建立由高级管理层支持的人工智能策略，对人工智能供货商进行《个人资料（私隐）条例》合规性尽职调查，组建跨学科人工智能治理委员会，并培训员工了解资料私隐和伦理。
2. 风险评估与人工监督：进行风险评估以评估私隐、法律和伦理影响，并制定书面缓解计划。需要人工监督以验证人工智能决定。
3. 人工智能定制与管理：尽量减少个人资料使用，测试系统的安全性和公平性，并维护人工智能事件应对计划以解决违规问题。
4. 持份者参与：透明披露人工智能使用情况，解释决策过程，并提供个人查阅或更正数据的机制，符合信息原则。

监管风险

在香港，人工智能处理健康记录和生物识别标识为企业带来重大监管风险。例如，保险公司可能为风险评估或健康计划收集生物识别数据（如遗传档案或健康指标），但须严格遵守《个人资料（私隐）条例》。资料泄露是一个主要威胁，因为这些数据类型是网络攻击的主要目标。未经授权访问医疗提供者的人工智能系统或零售商的面部识别工具可能导致罚款、执法行动和客户信任下降。未经同意将健康数据用于未授权目的（如市场营销）违反使用原则，可能引发监管处分。未能透明披露人工智能驱动的数据处理做法违反信息原则，可能损害客户信心。来自有缺陷训练数据的算法偏见可能导致歧视性结果，例如有偏见的信贷评估或招聘决定，使机构面临法律和伦理挑战。过分依赖自动决策而无人工监督可能侵犯个人根据查阅与更正原则质疑人工智能生成结果的权利。

合规策略

为减轻这些风险，机构必须采取与《个人资料（私隐）条例》和《人工智能：个人资料保护模范框架》一致的措施。在部署人工智能系统之前进行私隐影响评估，有助于识别和缓解敏感数据的私隐风险。例如，实施人工智能面部识别的零售商应使用私隐影响评估数据暴露风险并实施保护措施。资料最小化，符合准确性与保留原则，涉及仅收集必要资料并在可行情况下匿名化以限制泄露风险。人工监督确保人工智能决定的公平性和准确性，例如在医疗环境中验证人工智能诊断。包括加密和定期审计在内的安全措施对于保护数据免受网络威胁至关重要。通过清晰的个人资料收集声明进行透明沟通，告知个人人工智能数据处理做法，确保符合信息原则。对《个人资料（私隐）条例》义务和《人工智能：个人资料保护模范框架》伦理指引的员工培训促进负责任的数据处理。

监管环境的演变

香港的监管框架正在适应个人资料处理的挑战。在未来，金融和医疗等行业可能制定特定指引，企业需制定相应的合规计划。全球标准，如欧盟《通用数据保护条例》，强调严格的数据保护和问责制，与香港的监管方向一致。企业应加强数据治理和制定泄露应对协议，以满足这些要求。

结语

人工智能处理敏感健康和生物识别资料为香港企业提供了重大机遇，但需严格遵守《个人资料（私隐）条例》和采纳《人工智能：个人资料保护模范框架》。数据泄露、未授权数据使用、算法偏见和缺乏透明度的风险可能导致面临罚款、法律责任和声誉损害。通过实施私隐影响评估、数据最小化、人工监督、强大安全措施、沟通透明和员工培训，机构可减轻这些风险并负责任地利用人工智能。随着香港监管环境的演变，预计将有《个人资料（私隐）条例》修订和进一步的人工智能指引，企业必须保持积极主动以确保合规并维持竞争力。

如欲了解 JML 可如何协助您应对利用人工智能处理敏感数据的法律挑战，确保符合《个人资料（私隐）条例》及《人工智能：个人资料保护模范框架》，请扫描下方二维码，探索我们的法律服务。



本文内容仅供参考及不应被依据作为法律意见。

© 2025 JCHM Limited. All rights reserved.