Legal Risks of Enterprises Using AI Agents for Process Automation

Enterprises harnessing AI for process automation in Hong Kong must adeptly navigate the complex juridical landscape governed by, among others, the Personal Data (Privacy) Ordinance (PDPO), ancillary cybersecurity mandates, and the national security law. Recent compliance assessments by Hong Kong's Privacy Commissioner for Personal Data (PCPD) underscore the intensifying regulatory scrutiny on AI governance and personal data protection.

The Hong Kong Office of the Privacy Commissioner for Personal Data (PCPD) announced in 2025 the conclusion of compliance assessments on the utilization of artificial intelligence (AI) by 60 organizations. Since then, this initiative has brought about the intensifying regulatory scrutiny on AI governance and the protection of personal data, shaping expectations for enterprises integrating AI into process automation within Hong Kong's sophisticated financial and technological ecosystem.

I. Regulatory Framework Governing AI in Hong Kong

Key Definitions and Statutory Provisions

AI agents constitute autonomous software systems employing machine learning algorithms to execute tasks, including but not limited to customer engagement, marketing analytics, and regulatory compliance. The Personal Data (Privacy) Ordinance (Cap. 486) (PDPO) regulates the collection, processing, and security of personal data, defined under section 2 as any data relating directly or indirectly to a living individual from which it is practicable to identify that individual.

The PCPD serves as the statutory authority responsible for enforcing the PDPO, promulgating guidelines, and undertaking compliance reviews. The six Data Protection Principles (DPPs) under Schedule 1 to the PDPO form the cornerstone of data handling obligations, encompassing purpose and collection (DPP1), accuracy and retention (DPP2), use (DPP3), security (DPP4), openness (DPP5), and access and correction (DPP6).

Applicable Legislation and Guidelines

In the absence of bespoke AI legislation, Hong Kong relies on existing statutory regimes. The PDPO addresses privacy concerns, augmented by cybersecurity obligations under the purview of the Cybersecurity and Technology Crime Bureau of the Hong Kong Police Force, and sectorial directives from regulators such as the Hong Kong Monetary Authority (HKMA) and the Securities and Futures Commission (SFC). The Law of the People's Republic of China on Safeguarding National Security in the Hong Kong Special Administrative Region (National Security Law) also imposes obligations where AI applications involve data potentially impinging on national security, particularly in cross-border transfers pursuant to Article 43.

Non-binding instruments include the PCPD's "Artificial Intelligence: Model Personal Data Protection Framework" (issued in 2024) and the Digital Policy Office's "Ethical Artificial Intelligence Framework" (2024), which advocate for ethical AI deployment and risk-based governance, are also in place

II. Compliance Obligations and Risk Mitigation Strategies

Insights from PCPD Compliance Assessments

The PCPD's 2025 assessments reported that 80% of the scrutinized organizations deployed AI, with half processing personal data therein. Notably, no contraventions of the PDPO were detected, evidencing compliance to the DPPs. The PCPD accentuated the imperatives of governance, transparency, and risk attenuation, with particular emphasis on human oversight to preserve accountability in AI-driven processes.

Prescribed Governance Measures

The Model Personal Data Protection Framework outlines obligations concerning data minimization (aligned with DPP3), procurement of consent (DPP1), institutional governance, and contingency planning for incidents. PCPD's "Checklist on Guidelines for the Use of Generative Artificial Intelligence by Employees" (2025) prescribes internal protocols for AI utilisation. Empirical data from the assessments indicate that 79% of entities have maintained AI governance structures, 83% executed privacy impact assessments, and 92% established data breach response mechanisms. Enterprises are advised to perform risk evaluations, audit logs, and transparency protocols to conform with PDPO stipulations.

Operational Recommendations

Enterprises ought to formulate comprehensive governance frameworks, encompassing AI policies, oversight committees, and staff training programs. Periodic compliance audits, integration of human-in-the-loop mechanisms, and ongoing surveillance are indispensable. Legal advisors are instrumental in defining and mapping the application of data protection and AI governance measures, facilitating rigorous audits and efficacious stakeholder disclosures.

Many AI agents include end-of-output disclaimers indicating system limitations. Such disclaimers serve to increase transparency for data subjects and to signal that AI outputs are advisory and may be fallible. AI can substantially accelerate routine processes, improve throughput, and reduce operating costs, but it is less capable of resolving highly nuanced, context-dependent, or ethically sensitive matters that require professional judgment, empathy, or discretionary decision-making. In practice, deployments commonly combine automated agents with human-in-the-loop review for higher-risk decisions, escalation protocols, and records documenting supervised reliance on AI outputs.

III. Legal and Operational Risks Associated with AI Deployment

Risks Pertaining to Data Privacy and Accountability

Vulnerabilities inherent in AI systems, such as inadvertent incorporation of personal data into training models or algorithmic biases, may be exposed to breaches or misuse, invoking liability under the PDPO. Pursuant to section 64(1), unauthorized disclosure or use of personal data obtained without the data subject's consent, if causing harm or pecuniary loss, attracts penalties of up to HK$1,000,000 and

imprisonment for five years. Further, under section 26, failure to erase personal data no longer required for the purpose of collection constitutes a contravention, potentially leading to enforcement notices or fines.

Accountability complications emerge when AI outputs influence stakeholders, potentially infringing directors' fiduciary duties under sections 465-466 of the Companies Ordinance (Cap. 622), requiring directors to act in good faith and exercise due care, skill, and diligence. In listed companies, erroneous AI-generated disclosures may trigger prospectus liabilities under the Securities and Futures Ordinance (Cap. 571), exposing entities to civil claims for misleading statements. Enterprises must establish clear attribution of responsibility for AI decisions to mitigate vicarious liability under common law principles.

Cross-Border Transfers and National Security Imperatives

Hong Kong does not require data localization, permitting cross-border transfers subject to compliance with DPP3 (restricting use to stated purposes) and relevant sector guidelines, such as the HKMA's Supervisory Policy Manual on Outsourcing (SA-2). If AI systems process data potentially related to national security, this may engage provisions of the National Security Law aimed at preventing risks like subversion or collusion with foreign forces. Cross-border AI data flows could draw attention if they raise national security concerns, potentially leading to regulatory review and applicable penalties for any identified offences.

Inadequate cybersecurity can expose businesses to PDPO enforcement, including fines of up to HK$1,000,000 for unauthorized data disclosure under section 64. While breach notification is not mandatory, the PCPD recommends prompt reporting where appropriate. Businesses should adopt practical measures, such as encryption and access controls, to address data exfiltration risks, including AI-specific issues like prompt injections.

Challenges Arising from AI Hallucinations and Errors

AI hallucinations—where generative models yield ostensibly credible yet erroneous or fabricated content—pose acute risks in juridically sensitive domains, such as compliance reporting or dispute adjudication. Dependence on flawed AI outputs could give rise to negligence claims under common law tort principles, where claimants must establish duty of care, breach, and causation, with foreseeability assessed. In professional services, this may extend to breaches of implied terms in contracts or statutory duties under the Supply of Services (Implied Terms) Ordinance (Cap. 457) and professional negligence.

For instance, in the US case of Mata v. Avianca (2023), a lawyer relied on ChatGPT to generate and cite legal precedents in a court filing, which were later discovered to be entirely fabricated, resulting in sanctions from the court for negligence and submitting misleading information.

The absence of a legal personality for AI would lead to accountability being devolved to developers for design deficiencies (potentially product liability under the Sale of Goods Ordinance (Cap. 26)) or deployers for operational lapses. Human supervision, complemented by safeguards against biased outcomes that contravenes the Sex Discrimination Ordinance (Cap. 480), Race Discrimination Ordinance (Cap. 602), or analogous enactments, mitigates inaccuracies and protects entities from potential discrimination claims and damages.

Fragmentation of Oversight and Technological Flux

The decentralised regulatory architecture, involving the PCPD, HKMA, SFC, and emerging oversight from the Innovation, Technology and Industry Bureau, work together to set up compliance standards. Specifically, the expeditious evolution of AI technologies amplifies uncertainties, necessitating adaptive governance to target regulatory infringements and loopholes, an example of which is the expansion of Unsolicited Electronic Messages Ordinance (Cap. 593) to include AI-driven marketing or the Copyright Ordinance (Cap. 528) for IP issues in AI training data.

Conclusion

Enterprises harnessing AI for process automation in Hong Kong must adeptly navigate the complex juridical terrain landscape governed by the PDPO, ancillary cybersecurity mandates, and the National Security Law. Through meticulous and thorough governance measures, pre-emptive compliance initiatives, and secured cybersecurity measures, entities can alleviate risk and mitigate threats such as those from AI hallucinations and technological advancements. Sustained vigilance and compliance with regulatory directives is paramount for prudent AI integration in this evolving environment.

If you would like to mitigate data privacy and cybersecurity risks in AI adoption, scan the QR code below to know more about us and access our legal services.

Information in this update is for general reference only and should not be relied on as legal advice.