香港企业需遵守的数据安全合规要求

香港的数据安全法规要求企业建立严格的合规体系，以保护数据安全，避免严重的业务、法律和声誉风险。

在不断上升的网络安全威胁下，数据安全合规对包括但不限于上市公司及其高级管理层或内部合规团队在内的香港企业至关重要。有效的合规保障敏感数据，支持企业管治，并在高度互联的商业环境中减轻法律及声誉风险。

香港数据安全的法律框架

《个人资料（私隐）条例》（私隐条例）（第 486 章）管辖香港的个人资料处理，规定公私营机构在收集、使用、保存及保护个人资料时的原则。2021 年, 私隐条例的修订引入了恶意揭露身份(起底) 的罪行并加重罚则。一经循公诉程序定罪，最高可被处罚款港币一百万元及监禁五年。

法例确立了六项数据保护原则（DPPs），以确保数据公平及知情收集、安全处理、仅用于既定目的及最少保存期限。数据当事人享有查阅及更正资料的权利。六项原则包括:

- **DPP1**：收集目的及方式—个人资料必须依法公平收集，且只用于与数据用户职能直接相关的目的。所收数据应适当而非过量，且当事人必须知悉目的、是否自愿提供及其查阅及更正的权利。
- **DPP2**：准确性及保存期限—数据用户须尽合理步骤确保个人资料准确及最新，且不应超出目的所需保存。第 26 条规定未删除不再需要数据属违法，处罚罚款。
- **DPP3**：数据使用—个人资料只可用于原收集目的，除非得到当事人明确同意。私隐条例第 6A 部分适用于直接促销，要求使用前须明确知情同意。未经授权的直接促销可导致重罚及监禁。
- **DPP4**：数据安全—数据用户必须采取所有可行措施防止未经授权访问、处理、遗失或破坏个人资料。此义务经合同延伸至数据处理者。
- **DPP5**：公开及透明—数据用户必须公开其数据政策，所持个人资料种类及使用目的。
- **DPP6**：查阅及更正—数据当事人有权查阅及更正资料。数据用户必须于法律规定时间及方式内处理此类申请，或提供拒绝理由及保存拒绝纪录。

私隐条例亦设有平衡私隐及公共利益的豁免，如预防罪案、保障健康及法律程序，此类豁免需个案评估。个人资料私隐专员公署（私隐专员公署）积极推动强制通报及按企业组织营业额比例罚款，提升执法能力。

网络安全法及关键基础设施保护

除了根据普通法和通用法律要求的网络安全防护之外，《保护关键基础设施（计算机系统）条例》(第 653 章) 将于 2026 年 1 月生效，并规定关键基础设施营运者需建立网络安全管理计划，进行风险评估，并接受监管。这些规定旨在提升与香港经济及社会息息相关部门的网络安全及运营韧性，与国际标准接轨。

关键基础设施（CI）包括能源、信息科技、银行金融、空陆海运输、医疗、电讯及广播等指定行业的重要资产。第二类为其他被扰乱后会严重影响社会或经济功能的设施（如大型体育场及科研园区）。水务及应急救援等政府运营服务不属其内。关键基础设施营运者（CIO）是被指定负责运营此类设施的实体，指定由专员或授权机关根据其重要性决定。

指定 CIO 须遵守三大法定义务：(1) 组织架构管理（确保管治、分配资源、责任分明）；(2) 预防措施（进行风险评估，实施网络安全控制及漏洞管理以降低风险）；(3) 事故通报（实时侦测、报告及应对安全事故，并在法定时间内通知当局）。

条例要求年度风险评估、每两年进行独立审计及重大事件快速通报，当局有权调查和处理违规事项。违规罚款由 50 万至 500 万港元，并对持续违法处以每日罚款，对象为组织非个人。

该法由安全局新设置的关键基础设施专员办公室执行，负责指定、合规及执法工作。虽适用于在港或由港管辖的系统，无域外执法权，但 CIO 须在港提供相关数据，即使数据位于海外。

数据安全措施

私隐条例为数据安全指引提供全面实用框架，帮助机构遵守 DPP4，要采取所有可行措施防止未经授权或意外的存取、处理、遗失及误用个人资料。

在管治方面，建议机构建立有效的数据安全管理架构，按规模及风险制定，包括委任专责数据安全主任负责合规及事件应对，制定明确数据安全政策，并持续培训员工提高意识，明确个人责任。

物理及技术控制方面，强调多层防护：物理措施包括控制数据中心及服务器室的出入，保障便携设备安全，妥善销毁含个人资料的媒体。技术控制包括强化身份验证（如多因素认证）、按角色分配访问权限，仅限授权人员存取数据，并对个人资料传输及存储加密，防止拦截或未经授权的披露。

运营保障措施同样重要：组织应定期备份数据并安全储存备份副本，以在事件发生时维持资料完整性和可用性。保持详细的审计日志有助于及时检测和调查异常或违规行为。及时的修补程序管理以及更新的防病毒和防恶意软件解决方案对于减轻漏洞和保护系统免受外部威胁至关重要。

关于系统和网络安全，将安全措施融入系统生命周期（从开发、测试到部署和维护）是必不可少的。网络保护措施，如防火墙、入侵检测与防御系统以及网络分段，有助于降低暴露风险并有效遏制违规行为。

透过持续培训、宣传和员工审查培养安全意识文化，降低人为错误或内部威胁风险。另应定期测试完整事件应对计划，快速识别、控制及修复安全事故，包括按规定需通报时及时通报，确保面对不断演变威胁的准备。

综合以上措施，为合规、风险缓解及保障数据当事人权利提供坚实保障。

国家安全法及跨境数据转移

《中华人民共和国香港特别行政区维护国家安全法》(国家安全法)主要包含与分裂国家、颠覆国家政权、恐怖活动和勾结外国有关的罪行；虽然它没有建立通用的数据安全制度，但企业组织应确保数据处理不违反适用的国家安全法规定和相关指示。

《粤港澳大湾区个人信息跨境流动标准合同》（大湾区标准合同）由香港创新科技及工业局与中华人民共和国(中国)网信办联合推出，是一项自愿便利措施，促进香港与广州、深圳、珠海、佛山、惠州、东莞、中山、江门及肇庆九个大湾区城市之间安全合规的个人数据跨境转移。

该合同规范个人信息处理者及接收方的数据保护责任，确保跨境转移的个人数据得到充分保护。合同明确禁止转移数据于大湾区以外，包括母公司或子公司。合同不适用于区外转移及政府指定的重要数据。

转移前，个人信息处理者须取得数据当事人同意，于备案前三个月完成个人信息保护影响评估，并于合同生效后 10 个工作日内向香港数字政策办公室（数字办）及广东网信办完成备案。双方须遵守大湾区实施指引及香港私隐条例。

该便利措施简化监管要求，将影响评估范围由六大类减至三类，取消数据转移量限制，加快备案流程。企业组织可同一合同涵盖多业务场景，双向流动须签两份合同。备案须提交签署的合同、承诺书及身份核实文件，数字办审核后发出正式确认。

此外，中国于 2024 年 3 月生效的《促进和规范数据跨境流动规定》（《规定》），通过明确安全评估申报标准及界定标准合同和个人信息保护认证的免除条件，完善了监管环境。该《规定》简化了合规流程，并延长了数据出境安全评估结果的有效期，从而促进了香港与内地之间数据合作的便利化。此外，政府部门持续推动信息科技基础设施和网络安全措施的建设，以保障跨境数据交流的安全与韧性，确保与不断演变的数字治理标准保持一致。这种合作进一步巩固了香港作为数据枢纽的地位，促进中国及国际数据流的融合，推动国家和区域数字经济的发展目标。

违规后果

违规者可被罚款最高一百万港元及监禁五年，适用于未经授权披露或恶意揭露身份等严重罪行。违反私隐专员公署发出的执法通知，可导致罚款、监禁及按日计算的持续罚款。关键基础设施营运者的网络安全违规罚款最高达五百万港元。数据相关民事赔偿及声誉损害索赔进一步强调合规重要性。私隐专员公署将加强审计、违规调查及国际合作以推动执法。

新兴技术及人工智能的管治

香港政府在 2024 年发表的政策宣言明确金融部门负责任应用人工智能（AI）的框架。该框架采用双轨策略，促进金融机构采用 AI 的同时应对相关风险，包括网络安全、数据私隐及知识产权保护。

金融机构应制定全面的 AI 管治策略，指导 AI 系统的采购、使用及管理，采用风险为本的方法，重视人为监督以有效减少风险。为支持行业，香港科技大学提供自研 AI 模型、计算资源及咨询服务，支持本地部署或 API 和网络接口方式。

监管机构已将 AI 相关风险纳入现有规例和指引，并将随技术发展（如可解释人工智能）持续调整确保监管框架灵活应变。

执法部门加强国际合作应对 AI 相关网络挑战，并加强对公众 AI 风险与机遇的教育。

香港证券及期货事务监察委员会及香港金融管理局对金融业 AI 应用发布了具体指引及规则。

其他考虑：反洗钱、良性竞争和治理

有效的反洗钱机制依赖于对敏感金融和个人资料的安全管理。保障数据的机密性、完整性和可用性，是防止资金被非法利用的关键。香港《反洗钱及反恐怖分子资金筹集守则》（2023 年 6 月发布）结合金融行动特别工作组标准，强调风险为本的方法，要求企业组织建立完善的客户尽职调查（CDD）和持续监控机制，以识别和管理洗钱及恐怖融资风险。

企业组织须确保数据收集与处理过程安全可靠，严格执行访问控制、加密和日志审计，防止数据泄露和篡改。持续的资料监控有助于及时发现可疑交易，及时向金融情报单位报告。管理层应强化反洗钱政策，落实员工培训和合规监督，确保反洗钱与数据保护措施同步推进。只有将数据安全融入反洗钱体系，企业组织才能有效防范洗钱风险，符合法规要求，保护金融体系的完整性和声誉。

香港政府对人工智能相关运营设立了关键指引，以确保其合乎伦理、促进公平竞争并减少社会危害。这些指引包括严格遵守个人资料保护法，保障个人信息安全，防止误用；在道德层面，要求人工智能系统具备透明度、可解释性及人为监督，防止歧视性或偏见结果的产生；在竞争方面，措施限制垄断数据和不公平数据使用行为。此类规范还注重人工智能运营所依赖的数据中心的韧性和安全性，以防范系统性风险，并抑制可能危害社会秩序或公共利益的有害应用。通过完善的治理架构及持续更新的法规，香港致力于推动负责任的人工智能创新，确保该技术能够积极、公平地促进经济与社会发展。

数据治理涵盖多个核心元素，包括数据的整合、应用、开放与共享；数据安全；基础设施建设；产业规划；以及与不同标准和监管框架的衔接等。香港政府采取多轨并行的策略，从政策、法规及指引，到配套设施，全面构建符合香港实际情况的数据治理体系。2022 年 12 月公布的《香港创新科技发展蓝图》将「推动数字经济发展，建设智能香港」及「加快香港数字经济与智能城市发展步伐，提升市民生活质素」列为四大发展方向和八大重点策略之一，彰显香港致力于以数据为本，抓紧数字经济机遇，积极融入国家发展全局。

对香港企业组织的建议

香港的数据安全面临复杂且不断演变的法律环境，企业组织必须采取全面且复合的合规与管治方法。在线经营涉及众多交叉的法律责任，包括私隐保护、网络安全、国家安全、人工智能伦理、竞争法以及跨境数据治理。香港企业组织应避免孤立地处理这些问题，而应建立结构化的框架，系统性地将所有相关法律及标准纳入其营运和策略决策中。

企业组织可采用结构化方法，将适用的法律与标准纳入日常运作及策略规划。具体而言，这包括实施相应的数据治理措施、定期进行风险评估以及持续提供员工培训，同时保留因应法规与指引而变更的弹性。审慎且主动的方案有助达成法定责任、提升持份者信心，并在数码市场中维持竞争力。

如您正在寻求就香港的数据私隐与网络安全事务获取务实、以业务为本的法律意见支持，请扫描下面的二维码存取我们的服务。

本信息内容仅供参考及不应被依据作为法律意见。