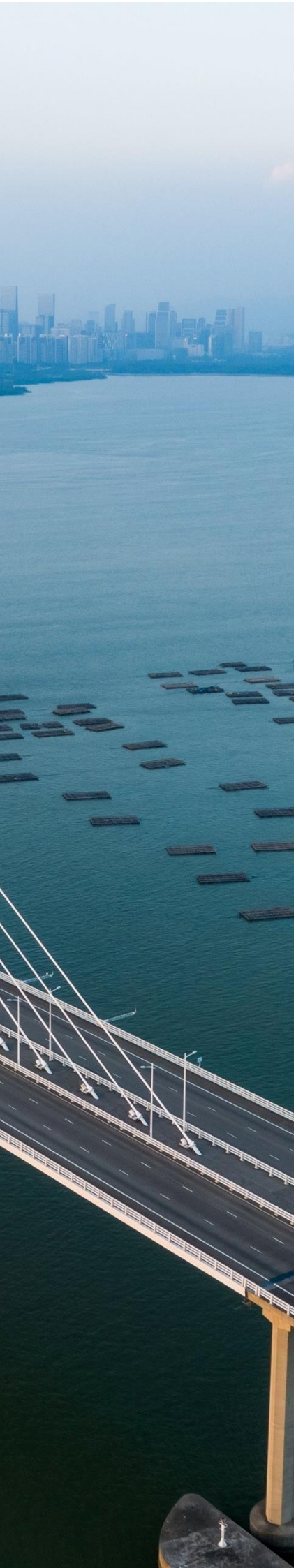
大湾区背景下企业面临的数字化机遇、安全挑战与应对

EY 安永
Building a better working world

导读

粤港澳大湾区的崛起和发展为数字化建设带来重大利好，大湾区各政府出台或即将出台的系列措施保障了数字化进程下的安全和合规，并为政企间、企业间和跨境的数据流通提供了强有力的支持。在享受便利的政策和更广阔的数据资源的同时，企业也面临着更多的数据安全挑战，包括平衡业务需要的同时应对三地不同的数据安全合规要求、应对因三地网络环境差异所增加的安全难度等。为了应对数字化条件下特定的挑战，企业应当提早规划，建立统一的合规标准方案、构建有效的安全合规能力、增强安全管理和安全防护能力，只有有效保障安全和合规，才能够长期和持续发展。



目录

1 数字化是大湾区发展的核心驱动力

2019年2月，中共中央国务院颁布了《粤港澳大湾区发展规划纲要》（以下简称“纲要”），提出了在2035年，大湾区形成以创新为主要支撑的经济体系和发展模式的目标。除了提出战略目标外，《纲要》还明确了一系列以数字化为核心驱动的战略举措，包括:

优化提升信息基础设施

《纲要》提出新一代信息基础设施建设将全面布局互联网协议第六版（IPv6），并在此基础上推进互联网升级改造与宽带扩容。在推动大湾区无线和光纤宽带城市群建设的同时，要建立统一标准，开放数据端口，推进电子签名证书互认工作，建立互联互通的应用平台。深圳特区的智慧城市和数字政府建设通过优化信息基础设施，打通数据接口超2000个，打破各机构间的“信息孤岛”，是《纲要》落地实施的优秀案例。另外，《纲要》还提出优化信息基础设施的同时需加强对通信网络、关键信息系统和重要数据资源保护，建立健全信息安全预警机制，提升网络安全保障水平，从而实现标准统一化、数据开放化、城市智慧化、信息安全化的目标。

加快发展先进制造业

《纲要》提出，应优化制造业布局，通过将互联网、大数据、人工智能与实体经济深度融合，促进产业链上下游深度合作，完善大湾区制造业创新发展体系。据广东省工业和信息化厅的数据显示，省内实现数字化转型的企业有1.5万家，使用云服务技术的企业达到50万家。广东省去年印发的《广东省制造业数字化转型实施方案（2021–2025年）》和《广东省制造业数字化转型若干政策措施》提出，要推动工业企业运用新一代信息技术实施数字化转型，带动企业上云用云，以人工智能带动工业化，降本提质增效。

培育壮大战略性新兴产业

早在2017年，国家发改委就已经通过发布《战略性新兴产业重点产品和服务指导目录》对战略新兴产业的范围进行明确，促进战略性新兴产业对经济增长转型升级、推动高质量发展的引领带动作用。《纲要》也多处指出，在粤港澳大湾区大力建设战略性新兴产业，要依托港澳广深等中心城市的科研资源优势及高新技术产业基础，推动七大战略性新兴产业和四大未来产业发展壮大，也要重点培育新一代信息技术、生物技术、物聯網（IoT）、人工智能、大数据、5G移动互联网、智能机器人、北斗卫星应用等新兴产业的项目，实施一批涵盖信息消费、新型健康技术、高技术服务业等领域的战略性新兴产业重大工程，推动数字化发展，促进经济转型升级。

加快发展现代服务业

伴随着不断提升的技术能力，数字化优势和创新性突破，大湾区各专业服务业正在加快数字化转型。《纲要》提出，要以港澳广深的经济金融优势为基础，建设国际金融枢纽，大力发展有特色的、安全的金融产业。大数据、人工智能和区块链等技术在金融领域的应用推动了传统金融服务公司的数字化转型，大湾区预计将实现更高效、安全、稳定的金融服务。除了金融行业，许多物流业、餐饮服务业等企业也开始利用大湾区充足的网络供应、大量熟练劳动力、完善的物流基础设施以及政府激励和资金支持，在受到新冠肺炎疫情冲击的情况下持续开展业务、加速转型升级。

上述的战略举措与数字化建设密不可分，或属于数字经济范畴，或需依托于数字化的建设。数字化发展已成为大湾区的主要引擎以及基础建设。

《纲要》发布后，粤港澳大湾区接连发布新政，体现在不同的政府发文中，如广东省工业和信息化厅印发的相关规定、中共中央国务院印发的珠海《横琴粤澳深度合作区建设总体方案》、深圳《全面深化前海深港现代服务业合作区改革开放方案》、香港历年发布的《施政报告》等。这些政策将进一步加强香港、澳门、深圳、珠海等大湾区城市在数字基础设施、数字贸易、数字金融、高新科技、智能制造等领域的交流与合作。

2 数据治理与数据安全是未来重点建设方向

数字化建设离不开有效的数据治理与数据安全，而有效的数据治理与数据安全建设也是促进大湾区及两岸三地经济融合的前提条件。为了配合以数字化作为发展引擎的规划，大湾区已逐步制定数据治理与数据安全相关的发展要求与落地措施，如2021年7月5日，广东省政府印发《广东省数据要素市场化配置改革行动方案》（以下简称“行动方案”）。行动方案作为全国首份数据要素市场化配置改革文件，明确了五大方面24项任务，从释放公共数据资源价值、激发社会数据资源活力、加强数据资源汇聚融合与创新应用、促进数据交易流通、强化数据安全保护等方面着力，大力加快培育数据要素市场。

数字化发展的大背景之下，除了上述的行动方案，大湾区各政府正出台或即将出台系列措施，为保障数据的安全和合规、加快政企间、企业间和跨境数据流通提供强而有力的支持，包括但不限于以下方面:

统一数据标准、合规标准及安全标准

▸ 数据标准

数据要素领域标准化专项研究正逐步开展，大湾区内将分阶段、分领域推进数据要素标准化试点，支持行业协会商会、企业和高校院所研究制定数据采集、处理、应用、质量管理等标准规范[1]，为数据流通打下技术性基础。

▸ 合规标准

在广东省、香港特别行政区与澳门特别行政区具备不同法律的背景下，建立大湾区数据流通制度、健全数据权益、交易流通、跨境传输和安全保护等基础性制度规范，明确数据主体、数据控制方、数据使用方权利义务，保护数据主体权益要求[2]是大湾区发展的先决条件之一。

目前大湾区正积极推进相关工作事项，研究在符合国家法律法规的前提下，如何建立大湾区特色的数据制度与合规标准，促进数据的交互。

[1] *《广东省数据要素市场化配置改革行动方案》第16条*
[2] *《广东省数据要素市场化配置改革行动方案》第18条*

安全标准

在强化数据安全保障方面，行动方案以及其他相关的指导提出了三点建设方向：一是建立数据分类分级和隐私保护制度，建立政府主导、多方参与的数据分类分级保护制度，厘清各方权责边界，制订省市两级各部门及相关行业和领域的重要数据具体目录，对列入目录的数据进行重点保护。健全数据隐私保护和安全审查制度，落实政府部门、企事业单位、社会公众等数据安全保护责任，加强对个人隐私、个人信息、商业秘密、保密商务信息等数据的保护。二是健全数据安全管理机制，健全数据安全风险评估、报告、信息共享、监测预警和应急处置机制。支持有关部门、行业组织、企业、教育和科研机构、有关专业机构等在数据安全风险评估、防范、处置等方面开展协作。三是完善数据安全技术体系，构建云网数一体化的协同安全保障体系，运用可信身份认证、数据签名、接口鉴权、数据溯源等数据保护措施和区块链等新技术，强化对算力资源和数据资源的安全防护，提高数据安全保障能力。这不仅体现了广东省政府在安全标准上的布局，也体现了大湾区各政府的共同努力方向。

统一公共数据资源体系

除了积极推行统一的标准外，大湾区也积极加强统一公共数据资源体系建设，完善人口、法人、空间地理、电子证照等基础数据库，并进一步丰富信用、金融、医疗、交通、生态、市场监管、文化旅游、社会救助、投资项目等主题数据库，以加快政府与企业之间的数据流通。据广东省政务服务数据管理的统计，截至2022年8月，以行政机制主导的一级数据要素市场累计发布数据资源目录3.33万个，为1567个政务部门的1144个业务系统提供517.86亿次数据调用服务[3] 。

在促进数据共享流通的同时，行动方案亦明确了有关公共数据管理机制和扩大公共数据有序开放等方面的公共数据安全保障要求，包括通过制定《广东省公共数据管理办法》，明确各级行政机关和公共企事业单位数据采集、汇聚、共享、使用、管理等要求[4]，以及通过制定《广东省公共数据开放暂行办法》，探索建立公共数据开放清单制度，完善公共数据开放目录管理机制和标准规范，健全公共数据定向开放、授权开放管理制度[5]。

推动粤港澳大湾区数据有序流通

建设粤港澳大湾区大数据中心，支持广州南沙（粤港澳）数据要素合作试验区、珠海横琴粤澳深度合作区建设，探索建立“数据海关”，开展跨境数据流通的审查、评估、监管等工作，是当前大湾区的工作重心。促进跨境流通的数据不仅包括公共数据、金融数据、企业的日常业务数据，也包含医疗等科研合作项目数据。应有序促进数据资源跨境流通，从而逐步实现科学研究数据跨境互联，并在产业发展、社会治理、民生服务等领域形成一批数据应用典型案例。

不难看出，粤港澳大湾区正加快完善数据资源开发利用和治理保护的政策环境，对伴随新经济产生的新治理难题进行规范，就数据交易流通、跨境传输、个人信息和隐私保护、数据安全战略等方面出台一系列政策，为建立完善的数据流通机制奠定良好的基础。

[3] *广东省政务服务数据管理局.《经济网丨专访杨鹏飞：广东数据交易所将“省市共建、广佛协同”，预计年底前建成》*
http://www.21jingji.com/article/20220801/herald/193999eb904a942a317130d2b84f1161.html#:~:text=%E9%80%9A%E8%BF%87%E2%80%9C%E5%BC%80%E6%94%BE%E5%B9%BF%E4%B8%9C%E2%80%9D,%E4%B8%AA%E6%95%B0%E6%8D%AE%E6%9C%8D%E5%8A%A1%E6%8E%A5%E5%8F%A3%E3%80%82

[4] *《广东省数据要素市场化配置改革行动方案》第2条*

[5] *《广东省数据要素市场化配置改革行动方案》第6条*

3 对企业的利好

随着粤港澳大湾区建设向纵深进行，一系列湾区数字化的重大措施滚动推出，为实现数据安全、高效、规范的数据流动和使用创造有利的政策环境。这对大湾区的企业而言，无疑是重大利好，包括：

便利的数据流通

粤港澳大湾区是我国开放程度最高、经济活力最强的区域之一，据国务院发展研究中心旗下中国发展研究基金会发布的《中国城市群一体化报告》预测，2022年粤港澳大湾区GDP达14.76万亿元人民币，超越东京湾区，成为世界经济总量第一的湾区。粤港澳大湾区“9+2”城市多年来的经济融合和民生往来已达到相当密切的程度，随着大湾区建设深入推进，湾区内人流、物流和资金流互联互通的许多瓶颈已得到很大突破。大湾区数据中心的建设、公共数据资源体系建设及包括“数据海关”在内的跨境数据传输的探索，都将进一步突破信息流动的体制机制障碍，带来便利的数据流通环境。在我国《网络安全法》、《数据安全法》、《个人信息保护法》和《数据出境安全评估办法》相继施行后，平衡数据跨境流通的合规性与业务需求是大湾区企业的痛点。在可预见的未来，大湾区数据跨境传输落地措施的探索，将为企业提供解决痛点的思路与便利，成为企业的竞争优势。

更多的数据资源可以利用

便利的数据流通和触手可及的数据资源，意味着大湾区企业可以充分发挥海量数据和丰富应用场景优势，进一步激活数据要素潜能，推动创新驱动发展。

另外，大湾区正推动各地公共数据资源的打通与融合，并积极探索如何在安全与合规前提下，对企业开放相关的资源。这意味着未来在大湾区内，企业不仅可以对内部数据开展便利的跨境流通、对企业间数据进行合规交互，更可最大限度利用公共数据，将数据决策、数据应用的效能最大化。

以下是大湾区背景下，部分数据应用场景样例：

金融领域应用场景

据全球金融中心指数（GFCI）最新数据，2022年，香港、深圳及广州均跻身前30强，香港、深圳及广州分列第3、10和24名，粤港澳大湾区成为罕见的金融中心城市密集区。未来，数字资源可以进一步提升大湾区用户金融服务体验及打造更稳健的金融体系。大湾区金融机构可通过粤港澳共同建设数码身份认证（e-ID）和认识客户（e-KYC）平台，推进远程跨境身份认证，为用户提供更便利的金融服务以进一步加强大湾区资金流动性。数字化金融系统的构建亦能满足金融机构反洗钱等风险管理要求。其次，大湾区金融机构可合法利用粤港澳金融业、电商、互联网及金融科技领域的跨行业海量数据，将用户数据、信用数据以及行为数据等结合，利用大数据处理技术进行数据建模，对用户进行精准画像，追踪分析用户的消费习惯、风险收益偏好等特征信息，进而根据客户的偏好推荐与之匹配的产品及服务，进行针对性的营销，为客户提供更好的服务；同时，可基于历史交易模式建立客户流失预警模型，主动维护和管理客户关系。再者，大湾区金融机构能进一步利用大数据进行客户行为、客户信用度、客户的资产负债状况分析，综合评估信贷风险，建立完善的风险防范体系。

医疗健康领域应用场景

疫情当下，利用大数据分析制订有效的公共卫生发展策略已是政府和公共医疗卫生机构的工作重点之一。大湾区政府和公共卫生医疗机构可以通过大数据追踪疫情以尽可能在疫情蔓延之前把控病毒传播风险，且借助医疗大数据积极主动调配医疗资源，以有效减少重大疾病的发生和诊疗成本，全方位减缓疾病、促进健康。

此外，便利的数据流通和丰富的数据资源也在医疗领域发挥不可或缺的作用。粤港澳大湾区医疗服务数字化程度日益提升，其中广州、深圳、珠海、佛山、惠州、中山、江门7个城市已率先建成了市级全民健康信息平台，实现了市域内主要医疗卫生机构间的互联互通、数据共享和业务协同。大湾区人口流量巨大，近年来广东居民南下港澳进行身体检查、牙科服务、医疗美容及大型手术等，或港澳居民北上前往大湾区其他城市的内地医疗机构、养老院接受医疗健康服务的情形日渐增多，而以数据共享流通为湾区医疗健康信息融合奠定基础，是进一步优化大湾区医疗资源的有效利用,实现大湾区居民在各大湾区城市享受便利优质医疗的关键因素。

▶ 电商物流领域应用场景

粤港澳大湾区产业数字化结构不断升级，逐渐成为驱动粤港澳大湾区数字经济发展的主要动力。信息消费规模和电子商务交易额更是居全国首位，跨境电子商务交易量占全国近七成，移动支付占全国三成。近年来，粤港澳大湾区电商物流企业开拓了许多跨境电商服务新领域，如跨境支付服务、海外仓服务、跨境电商语言服务、跨境数据服务等。在跨境电商活动全生命周期流程中，海关等政府部门、境内外消费者、跨境电商企业、平台企业、境内服务商等主体在线上及线下场景深度交织，形成诸多主体之间的数据交互关系。通过大数据、云计算等智能基础设施的建设，把每个物流环节的信息数字化并实现线上连接，推动物流过程透明化，帮助大湾区电商物流企业有效实现提质增效降本，使跨境电商与大数据时代物流共同发展。

更好的数字化基础设施

完善的网络和计算基础设施体系，为粤港澳大湾区企业另一个天然优势。国家“十四五”《纲要》提出加快数字化发展，建设数字中国，广东省“十四五”《规划纲要》也提出建设数字湾区，并明确提出建立粤港澳三地跨境大数据中心[6]。2020年底国家发展改革委发布的《关于加快构建全国一体化大数据中心协同创新体系的指导意见》明确提出，在京津冀、长三角、粤港澳大湾区、成渝等重点区域布局大数据中心国家枢纽节点。目前，粤港澳大湾区内拥有广州、深圳两大国家级超算中心，运算速度和综合技术水平全球领先。信息化基础设施总体水平不断完善，互联网骨干网和城域网不断扩容升级，数据中心产业已经形成以穗港深为核心、阶梯式辐射周边的产业布局，服务器上架率和数据储存量位居国内前茅。按照《广东省5G基站和数据中心总体布局规划（2021-2025年）》的数据中心规划，全省按照“双核九中心”的总体布局，形成广州、深圳两个低时延数据中心核心区和汕头、韶关、梅州、惠州、汕尾、湛江、肇庆、清远、云浮9个数据中心集聚区。到2022年，全省累计折合标准机架数约47万个，平均上架率达到65%。到2025年，全省累计折合标准机架数约100万个，平均上架率达到75%[7]。

另外，与京津冀、长三角地区不同，粤港澳大湾区拥有独特的多样性制度环境：大湾区深圳、珠海两个经济特区，广东自贸区的南沙、前海蛇口和横琴三个片区，还有“一国两制”方针下的香港和澳门两个特别行政区，为跨境数据直连创造了天然条件。近几年，大湾区积极探索建立全球数据港，包括南沙国际数据自贸港，落马洲河套区港深创新及科技园数据中心等，以期数据在安全可控的前提下实现跨境共享流通。

[6] 节录——「推进数据资源汇聚、流通与共享；开展数据跨境流动安全管理试点，探索建立既便利数据流动又确保安全的机制」

[7] 节录——《广东省5G基站和数据中心总体布局规划（2021-2025年）》

4 企业面临的数据安全挑战

对于湾区企业，大湾区一系列的规划与措施无疑对企业在合法合规的情况下打造数字化竞争力有重大利好。然而，企业在享受便利的同时，也将面临更高的挑战。

三地法律不同、业务场景交叉、企业合规压力突出

从法律层面来说，粤港澳大湾区实际涉及三个不同的司法管辖区，三地对于网络安全、隐私保护、跨境信息传输，乃至各专业领域如医疗卫生、金融服务等均有不同的法律法规。法律法规的差异与业务在三个司法管辖区的交叉开展，使企业时刻在数据安全合规的压力下。

在网络安全方面，内地已订立《网络安全法》、《数据安全法》、《网络安全审查办法》以及相关的实施细则，澳门已订立《网络安全法》等，香港目前正在为订立《网络安全法》进行准备工作，计划就立法进行公众咨询。对比其它两地，内地法律对网络运行者、关键信息基础设施运营者及开展数据处理活动等的定义较广，企业需要根据自身业务情况，分析需要满足的具体合规要求。同时，内地“关键信息基础设施运营者”与澳门“关键基础设施营运者”定义有所不同，分别承担的网络安全责任也有所不同，企业应当注意分辨。

在隐私保护方面，三地目前都已订立较全面和完善的保护要求，内地已订立《个人信息保护法》等一系列的配套法律法规和相关指南，香港已订立《个人资料（私隐）条例》及香港个人资料私隐专员公署的相关核准实务守则和指引等，澳门已订立了《个人资料保护法》及澳门个人资料保护办公室所制订的各项指引。三地法律法规要求既有相似的地方，但也并非一致，包括：

对于敏感个人信息和自动化决策的定义略有不同：

内地和澳门地区对处理敏感个人信息以及自动化决策有较为详细的合规要求，香港《个人资料（私隐）条例》中没有明确条文规定，但私隐专员公署有一系列的核准实务守则和相关指引。

对境外处理个人信息有着不同的规定：

内地的《个人信息保护法》除适用于在中华人民境内处理自然人个人信息的活动，更适用特定情况下的境外处理中华人民共和国境内自然人个人信息的活动。香港的《个人资料（私隐）条例》适用任何在香港或从香港控制个人资料收集、持有、处理或使用的资料使用者，个别情况下可以向非港人服务提供者进行执法。澳门的《个人资料保护法》则没有明文境外适用条文，但适用于全部或部分以自动化方法对个人信息的处理、以非自动化方法对存于或将存于人手操作的数据库内的个人信息的处理等情形。

对收集、使用、处理个人信息的要求及个人信息权限有着不同的要求：

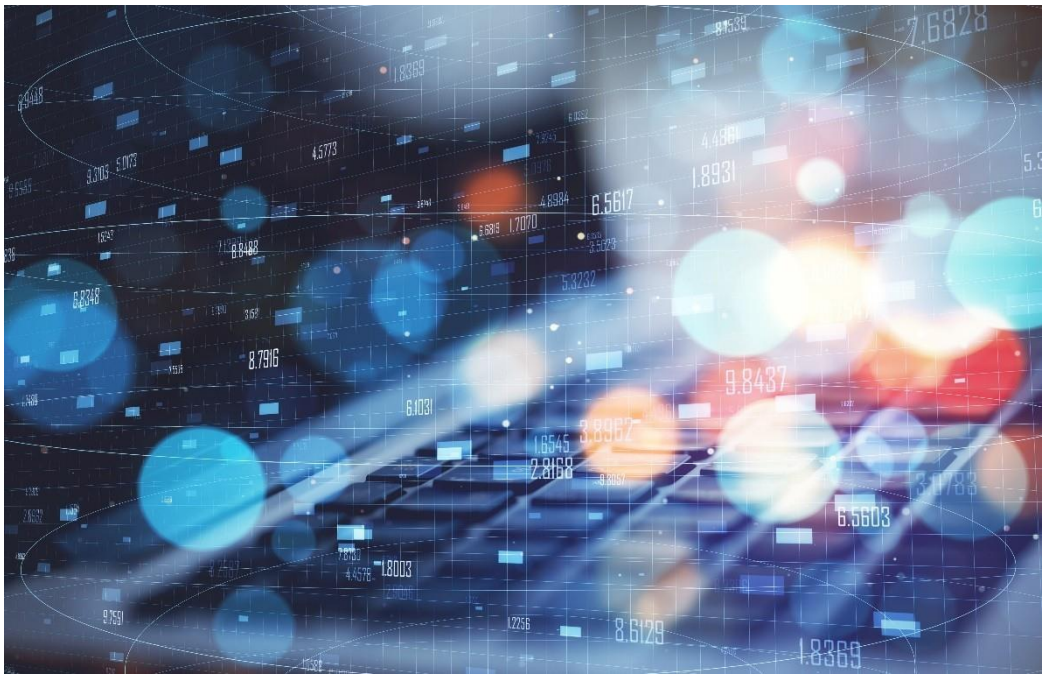
内地的《个人信息保护法》进一步规定了各个必须取得个人单独同意的情形。香港的《个人资料（私隐）条例》包含了多个不同的情形需要不同类型的同意的要求。澳门的《个人资料保护法》明确了处理个人资料、处理敏感资料、披露或传播全部或部分个人资料、转移个人资料至境外等获明确同意的情况。

而在跨境方面，三地的法律法规的要求也存在不同，包括：

- 对于数据本地化，内地的《网络安全法》和《个人信息保护法》等法律法规对数据本地化有具体的要求，而香港的《个人资料（私隐）条例》及澳门的《个人资料保护法》和《网络安全法》均没有明文数据本地化要求。

- 对于跨境传输，内地的《网络安全法》、《个人信息保护法》和《数据出境安全评估办法》等法律法规对跨境传输的条件进行了规定，包括通过安全评估、个人信息保护认证、按标准合同与境外接收方订立合同等。香港的《个人资料（私隐）条例》对跨境转移个人信息有相关规定，但该些规定尚未实施。澳门的《个人资料保护法》和《网络安全法》对跨境传输有作出部分规定，且列明了例外的情况。

内地、香港和澳门三地对网络安全、隐私保护、跨境信息传输的主要法律规定的异同及应对难点的具体内容请参考附录。



当前的合规能力难以应对安全挑战

面对三地数据安全和隐私保护的法律交叉以及冲突复杂的法律环境，企业需要具备充分的安全合规能力，否则将难以应对与业务交融的各类数据安全与合规问题。良好的数据安全合规能力包括：

▸ 至上而下的安全合规文化

建立至上而下的安全合规文化，才能确保安全合规在企业内部有效执行。这要求企业管理层、业务主管在内的上下全员能够准确认识到网络安全和隐私合规的重要性，但许多企业目前难以建立至上而下的安全合规文化，原因包括：

部分管理层合规意识不足，未能充分了解数字化转型中网络安全和隐私保护的重要性，仍将网络安全和隐私保护看作是企业普通合规事项、IT内部控制事项。

部分企业仍然将安全与IT捆绑，然而在数字化变革下，安全问题已不是简单的IT问题；企业关键部门和董事会对安全信任不足或理解不足，安全沟通存在障碍，难以实现跨业务部门合作，安全不可避免地被其他业务职能和业务领域绕过。

部分企业缺少全面的安全合规培训，目前对于员工的培训主要还是局限与工作岗位相关的工作内容和技能的培训，并未涉及安全合规培训，只有较少管理层目前开展过安全合规和建设的培训。

完备的组织架构

完备的网络安全组织架构是进行安全合规的基石。通过贯穿企业的网络安全组织架构，能够有效打通管理、IT、业务等部门的沟通屏障，最大限度地调动网络安全和隐私合规的能动性和积极性。部分企业目前难以形成完备、有效的组织架构的主要原因包括：

- 部分企业对安全合规的认知仍然处于原始状态，认为涉及法律法规相关的问题就得一刀切地交给法务部门。实际上，安全合规同时涉及管理、IT、业务、内控等部门，单靠法务部门难以覆盖到安全合规的方方面面，并不能很好地处理所有问题，反而增加了合规隐患。

- 部分企业虽然设立了网络安全组织架构，但在实际的运作中，未能很好地将合规工作职责在不同部门之间进行区分，导致安全合规的工作无法有效地落地执行。

充足的人力资源支持

在完备的组织架构下，企业应当配备充足的人力资源，及时对安全问题做出有效的响应。部分企业目前难以配备充足的人力资源，主要原因包括：

- 部分企业不了解安全合规的相关要求，且不同部门之间的职责划分不清晰，无法对人员进行更好的安排。

- 安全合规人才力量不足，拥有网络安全专业背景和技术能力的人员严重匮乏。

完善的合规管理框架和运行机制

建立健全的合规管理框架和运行机制，是企业推动网络安全和隐私合规管理的先决条件，在此基础上才能够确保工作开展有据可依，管理责任落实到人。部分企业难以建立完善的合规管理框架和运行机制，主要原因包括：

- 部分企业管理层及员工安全合规意识不足，组织架构不成熟，缺少相应的人力资源，从现实条件来看，难以建立完善的合规管理框架和运行机制。
- 三地数据安全和隐私保护的法律交叉背景下，想要将不同的合规要求融入现有的安全管理框架和运行机制当中，存在一定难度。

全面的网络安全和隐私合规能力

具备全面的网络安全和隐私合规能力，才能确保安全合规的全面执行。部分企业难以建立全面合规能力的主要原因包括：

- 作为安全合规建设中比较重要的环节，隐私保护在企业内部缺少体系支撑，从制度层面难以满足合规要求，无从指导工作的落地执行。
- 部分企业已建立合规体系，但在组织架构、人力资源等方面难以提供支持，导致相关的流程和机制无法有效落地。

对于大部分湾区企业来说，由于种种的客观因素限制，当前的合规应对能力难以应对数字化发展带来的新挑战，如何在合理配置资源的前提下，建立有效的数据安全合规体系，将成为湾区企业的痛点。

三地网络环境等差异增加安全防御难度

粤港澳三地的网络环境等存在多种差异，例如：

网络环境差异

内地服务器线路访问受服务商的存储和流量限制、需经过标准流程向有关部门备案后方可使用，而香港、澳门地区服务器由网络运营商线路接入国际宽带，免备案且不受线路限制。在这种区别之下，香港、澳门地区的网络环境相对复杂，企业的IT资产也暴露在相对复杂的网络环境之下。由于内地的信息资产成为攻击的目标的可能性越来越高，如何在不同的网络环境之下，对信息资产进行保护，是企业面临的挑战。

技术和安全标准差异

三地的技术和安全标准存在差异，例如在加密算法的使用中，许多内地企业会使用国内的标准，如公钥密码算法（SM2）、摘要算法（SM3）、分组密码算法（SM4），香港、澳门地区企业常使用国际通用的商用算法，如RSA、DES等；再例如内地目前已经建立了相对落地的安全标准，而香港、澳门地区目前仍然缺少一套比较成熟的网络安全标准。在这样的技术和网络安全标准差异之下，企业如何进行管理，也是面临的挑战之一。

用户习惯差异

三地用户在网络的使用上也存在差异，例如澳门、香港地区用户主要使用的社交类应用为WhatsApp、Facebook等，内地用户主要使用微信、微博等，面临用户习惯差异，企业在进行统一安全监管的过程中存在困难。其次，在后疫情时代，许多企业员工被迫在家办公，家庭网络与办公网络的边界越来越模糊，企业如何管理安全和隐私问题，也成为难点。

在打造大湾区数据跨境流通环境的过程中，由于各地现有的网络环境、技术和安全标准、用户习惯均存在差异，增加了企业的安全防护难度，形成了新的管理挑战。

5 企业应当如何应对挑战

应对三地法律的差异

企业考虑大湾区数据治理和安全的合规策略，实现跨境数据流通，必须小心考虑三地法律法规的异同，使其合规战略能同时满足三地不同法律法规的要求，形成一套精准符合三地法律的合规解决方案，切实执行、应对和满足三地监管机构的要求。三地法律虽存在差异但并无冲突内容，在业务高度融合、交叉的情况下，一套方案符合三地法律的总体数据合规制度，是较为推荐的路径。此外，企业更要时刻留意三地的法律法规发展，以使合规解决方案符合三地最新的规定。

目前，在数据合规与安全方面，大湾区企业需优先考虑的是两方面内容：

▸ 隐私保护

在隐私保护方面，三地对于个人信息的收集、使用、处理个人信息的要求及个人信息主体权利均有交叉及重合之处，企业应着力融合三地的法律要求，对其收集、使用、处理个人信息建立统一体系应对，制订同时适用三地法律法规要求的隐私政策和声明，并在具体细节上对三地不同的法律以及企业在三地不同的服务内容进行修订。例如，香港要求对任何直接促销的行为作合规管理，而内地及澳门则要求企业必须考虑对跨境个人信息传送、自动化决策、敏感个人信息处理等具体情形作合规管理等。

▸ 跨境数据

粤港澳大湾区数据流动合规渠道

数据作为数字经济的基本要素之一，讲求时效性和标准化，因此数据流动的机制应基于一个轻巧和标准的流程。除了期待“数据海关”等措施加速跨境数据流通的审查、评估、监管等工作之外，根据国际趋势，企业通过建立标准合同模板以及获得相应的保护能力认证，也是未来大大降低数据标准转换以及企业合规的成本，使数据要素顺畅跨境流通的关键之一。

标准合同条款：由于粤港澳三地当前还没有数据互通机制（如：白名单机制），可以考虑在企业层面采用商务合同的方式，建立数据跨境流动的标准条款，定义数据发送方和接收方双方的责任、权利和义务以及应有的保护措施。通过标准合同条款，不但可以确保数据的互通性和安全性，同时可以确保数据跨境流动符合相关的法例法规要求[8]，增强三地企业互信，促进数据流动。

企业数据保护能力认证：粤港澳大湾区可以考虑由独立的第三方遵照同一套数据治理评估标准和报告框架体系，对企业的数据保护能力进行独立评估，出具第三方鉴证报告证明企业在数据治理和保护方面的能力，并根据评估结果决定数据是否应当发送予接收方[9]。该举措将方便企业在提供充分的数据安全保障的前提下进行跨境数据整合，例如跨境集团公司在确保数据治理和保护能力的前提下，充分利用不同地区市场的商业数据，拓展业务版图。

建议通过探讨大湾区的实际情况，配合三地的监管法规、政策和市场意见等方面的要求，明确各持份方的责任归属、权利和义务，例如法律约束力、保密协议、个人数据保护措施和中止数据传输条款等。

粤港澳大湾区涉及跨境数据流动的企业合规对策

跨境数据流动的合规对于企业的风险管理尤为重要，特别是涉及国际贸易、跨境支付、大数据、云计算等领域的数字科技企业。跨境数据流动的合规，具有一定的难度和复杂性。建议企业从以下几个方面出发，结合企业内部实践情况，积极探寻合规对策和路径。

- **明确跨境数据流动的法律法规**

首先要对跨境数据流动相关的法律规则有充分认识，不仅包括本国的法律规则，也包括与数据业务有关的其他法域的法律规则。必要时，企业也应当咨询相关领域的法律专业人士，为法律规则的适用情况提供指导。

[8] *例如，欧盟提供数据于欧盟内外传输的标准合同条款（SCC），协助持份者遵守欧盟《通用数据保护》条例（GDPR）。同时，为提升战略区域合作的一体化，东盟发布了东盟跨境数据流动示范合同条款（MCC）供成员国使用，促进数据在《东盟数据管理框架》下自由流动。*

[9] *现时，在缺乏充分性认定的情况下，欧盟还为企业提供了遵守适当保障措施条件下的数据转移机制，包括批准的行为准则（Code of Conduct）及批准的认证机制（Certification Mechanism）。*

梳理企业运营过程中的数据

在现阶段，企业应梳理日常业务运营过程中可能涉及的所有数据类型及具体的信息字段，以作为初步识别工作的基础。企业需确定所在行业是否已存在成文的识别标准或识别方法，若无，企业需从现行有效的法律法规所提出的重要数据的概念出发，判断各类数据落入重要数据范围可能性的高低，对于极有可能会构成重要数据的数据，企业应积极履行《数据安全法》提出的数据安全保护义务。同时，与主管部门保持密切联系，并积极跟进后续配套性指引文件及细则的出台，届时采取更全面、更有针对性的合规对策。

完善企业数据安全内控制度

跨境数据流动的合规，不仅是数据跨境传输转移过程中的合规，数据采集、数据加工处理等前序步骤，都会影响数据是否可以跨境传输，以及是否需要履行审批程序。因此，企业需要就数据管理建立一套完善的内控制度，从业务合同签署到实际业务操作，给予企业人员明确的指引，降低企业违规的风险。根据《数据安全法》关于处理者的数据安全保护义务，相关内控制度至少应当包括全流程数据安全管理制度、风险监测和安全事件应对制度、重要数据风险评估报告制度等等。

建立企业内部数据跨境传输机制

法律规则对于不同主体赋予的数据合规义务各有差异。例如，根据《网络安全法》的规定，关键信息基础设施的运营者要比一般的网络运营者承担更为严格的数据安全保护义务。因此，企业需要结合自身业务，依据适用的法律规则，正确定位自身角色，方可明确自身需要承担的义务，及需要遵守的规定。

考虑到国内目前对于重要数据及关键信息基础设施运营者的认定尚未完全清晰，建议企业应首先通过梳理相关规则、与行业主管部门沟通等方式确定企业自身是否可能落入关键信息基础设施范围内。同时，梳理在日常业务运营过程中可能涉及的数据跨境传输场景，即便某些企业被认定为关键信息基础设施运营者的可能性较小，但是对于有可能涉及重要数据跨境传输的业务场景，同样建议企业在开展数据传输行为前，积极开展内部自评估工作，并与监管部门保持密切沟通。

构建安全合规能力

为构建健全的网络安全合规能力，企业可以从以下几个方面入手：

明确数据安全管理部门

数据安全与传统的信息安全不同，它既包含了IT安全，也涉及法律合规、内控以及业务安全。因此，如果由传统的安全团队或法务团队负责，从知识面与能力而言，难以完全覆盖数据安全相关需求；从职能层面，难以起到跨部门、跨业务板块的统筹协调效果。

为了能够有效执行安全合规管理策略和制度，企业需建立或指定数据安全管理部门。依据公司业务规模以及与数据安全的关联程度，该部门可以采用独立的形式存在或由原来的职能部门兼任。

数据安全管理部门应具备以下职能：

- 制定数据管理制度文件，明确各个层级、各个部门的数据安全合规管理职责
- 推动企业的数据安全合规管理，完善企业合规管理体系
- 规范企业的数据收集、存储、使用、加工、传输、提供、公开等工作机制
- 促进企业的制度规范建设、管理措施的设计与执行、数据安全技术应用的更新等，确保企业数据安全合规

此外，满足特定条件下，企业应当指定网络安全和隐私保护负责人，负责对企业的网络安全和隐私合规措施进行监督。网络安全和隐私保护负责人应当承担的职责如下：

- 全面统筹实施组织内部的网络安全和隐私保护工作，对企业的网络安全和隐私保护负直接责任
- 组织制定网络安全和隐私保护工作计划并督促落实
- 制定、签发、实施、定期更新网络安全和隐私保护政策和相关规程
- 组织开展网络安全和隐私风险评估，督促整改
- 与监督、管理部门保持沟通，通报或报告网络安全和隐私保护事件处置等情况等

制定跨地区的数据安全制度与流程

数据安全合规并不是一次性的任务，在业务不断变化、应用服务不断迭代的今天，若缺少有效运行的合规机制，企业将始终暴露在风险之下，因此，企业需建立行之有效的制度与流程。

由于大湾区企业在三地的业务高度融合与交叉，针对这种情况，较为理想的方案是融合三地法律，建立企业集团层面的总体合规框架以及落地的标准与规范，针对各地要求，在特定控制点上提供个性化设置。

结合目前的法律法规，完善的数据安全制度与流程需优先考虑以下方面：

个人信息安全影响评估（Privacy impact analysis）

从合规意义上理解，个人信息安全影响评估是企业满足特定条件下需要开展的工作，国家也出台了GB/T 39335-2020 《信息安全技术 个人信息安全影响评估指南》对企业的相关工作作出指引。

此外，个人信息安全影响评估也是企业内部识别隐私风险、合规风险的重要手段。在数据安全层面，大部分企业当前尚未建立成熟的流程，难以识别新业务、新系统带来的风险，更多依赖项目参与者的主观意识与认知，导致合规风险持续存在。完善的个人信息安全影响评估内容包括触发条件、涉及的人员与组织、流程与节点、评估的标准与要求、通过标准等，能协助企业有效识别与度量风险，避免过度依赖主观意识。

隐私保护设计（Privacy by design）

为将隐私管理和隐私实践更好的嵌入到技术、业务和产品实践当中，企业需要将隐私纳入新系统和流程的设计规范与管理流程的初始环节中。从系统的需求提出、系统实施直至系统维护阶段，都应当持续开展隐私影响评估，制定相应保护要求，将风险管控前置的同时，也避免后期花费大量人力物力对系统进行整改。

数据留存

企业应当在全面了解业务流程和数据使用的基础上，根据法律法规要求留存数据，并制定相应的留存计划，确保战略要求符合最短的留存期限规定。此外，在符合法规、数据保留制度、消费者要求以及其他业务需求的基础上，企业应当与业务部门建立伙伴关系，从而了解数据的生命周期和流转过程，并衔接数据安全的各个层面，从而建立高效的数据处置程序，以实现业务发展并满足保留和处理要求。

数据主体权利（DSR）

三地的法规要求分别对个人信息收集处理过程中数据主体的权利做出了一定程度上的规范。结合来看，涉及到的权利包含知情权、访问权、纠正权、被遗忘权、限制处理权、反对全和可携带权等。在三地法规要求的基础上，企业应当建立完善的个人信息主体权利响应的流程和机制，从而落实数据主体权利保障工作。当个人提出此类请求时，个人信息处理者应明示个人行使相应权利的有效且便捷途径，并做出及时的响应。

授权同意管理

内地的《网络安全法》以及《个人信息保护法》、香港的《个人资料（私隐）条例》和澳门的《个人资料保护法》都对个人信息收集过程中对个人同意的获取，以及需要获取单独同意的特殊场景进行了要求。在复杂的合规要求背景下，企业不仅要在收集个人信息时获得授权同意，也要在保证合法性基础的前提下，基于授权同意来对数据的处理方式进行限制。此外，根据《个人信息保护法》第十五条，基于个人同意处理个人信息的，个人有权撤回其同意。因此，企业除了在用户触点保障用户撤回授权同意的权利，也应当在内部数据处理平台中及时同步授权同意的状态。

数据跨境

当前，内地现有的法律法规及各类监管文件，例如《网络安全法》、《数据安全法》、《个人信息保护法》、《数据出境安全评估办法》等，都对数据跨境做出了要求。此外，香港的《个人资料（私隐）条例》和澳门的《个人资料保护法》中虽然也有数据跨境相关的要求，但是强度相较于内地的法规较低。这些要求对跨境数据的传输、数据的使用者和处理者等角色都做出了严格的规定。在跨境过程中，企业应当在各地法规要求的指导下，制定详细的数据出境计划，对该数据出境计划的合法性和正当性进行深度评估。此外，企业应当基于合规要求，对企业现状开展差距分析，制定补救措施，从而建立完整的跨境数据传输管理机制。

明确合规流程中的职责分工

数据安全合规绝不是数据安全管理部门的责任，数据安全能够在企业内部落地实施，需要众多部门的共同参与，明确各部门各自的责任，例如：

数据安全部门作为数据安全合规的牵头部门，负责组织相关的制度和流程编写、监督安全的落地实施等。	IT部门应当协助数据安全部门，通过技术方式将数据安全管理手段融入日常的业务和产品，并嵌入到企业系统及业务开展过程中，例如实施访问控制、加密、脱敏、防泄漏手段等。	业务部门如销售团队、产品团队、采购团队等应当配合数据安全部门，从业务角度出发对企业拥有的数据进行系统性的梳理，包括确定数据处理者、了解数据的形式、存储方式、保留时间等，并在各自的业务领域范畴内结合数据治理要求开展并落实具体的数据安全管理工作等。	合规或法务部门应当结合法律法规和监管要求对数据安全管理框架进行完善，并开展定期的合规检查和风险评估等。

只有统筹协调各方资源，整合各部门管理诉求差异，明确职责与分工，才能形成有效的多方联动机制和可落地的管理组织架构。

把控数据出境后的风险

数据出境风险的把控，不仅局限在如何合规地将数据传输出境外，更需考虑传输到境外后的安全控制，落实对数据的安全管控义务，否则出境后发生安全事件导致个人信息或其他重要数据泄露，企业仍需负上相关责任。

数据出境后的风险管理，包括但不限于：

- 严格身份认证和访问控制：严格限制出境后的数据访问权限，仅向具有充分业务需求的对象开放数据范文，建立充足颗粒度的访问权限控制，防止未授权访问超出权限的数据。

- 严格限制数据的使用和再传输范围：严格限制处理手段，不进行超出原目的的数据处理。此外，更要控制数据的再传输。任何与数据出境时评估、申报内容不符的处理行为，都应当重新评估与处理，避免将出境后的重要数据、个人信息作为普通数据进行随意处置。

平衡业务需要，提升隐私保护能力

虽然大湾区未来将带来更便利的数据跨境流通机制，但企业的合规义务与责任并未减少，企业仍需保障流通前后的数据安全，避免对国家发展、社会造成负面影响。此外，由于相关措施仍在制定中，就当前的情况而言，企业难以平衡合规要求、用户体验以及业务需要。相关的痛点不仅存在于企业间的流通，更存在于企业内部不同实体之间的数据流通过程。

结合当前的发展形势以及行业实践，建议企业在规划跨地区数据融合与统一应用时，可考虑通过业务流程控制或隐私计算等技术手段，实现数据的“可用不可见”，在不直接提供原始数据的前提下，通过提供计算后的标签、汇总信息或分析平台，实现数据的跨实体使用，实现数据所有权和数据使用权之间的分离，从而有效降低相关的安全风险以及合规风险。

加强安全管理能力

在考虑合规能力的同时，企业也需构建完善的安全管理能力，防范与应对各类安全威胁。企业可从以下两个方面加强安全管理能力：

▸ 数据安全管理

在2021年6月，第十三届全国人大常委会通过的《数据安全法》中明确提出“国家建立数据分类分级保护制度，根据数据在经济社会发展中的重要程度，以及一旦遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者个人、组织合法权益造成的危害程度，对数据实行分类分级保护”，面对不断加大的数据安全监管力度，企业根据法规的要求，建立健全全流程的数据安全管理体系。

在数据资产识别方面，企业可参考2022年出台的《信息安全技术 重要数据识别指南（征求意见稿）》，了解重要数据的识别因素，遵循聚焦安全影响、突出保护重点、衔接既有规定、综合考虑风险、定性定量结合和动态识别复评的原则识别企业内重要数据，规范化重要数据描述格式。

在数据分级分类方面，企业可参考《网络安全标准实践指南--网络数据分类分级指引》、《工业数据分类分级指南（试行）》等实施指南，从数据的业务影响、合规风险、社会影响范围等维度，并结合现有公司内部的规章制度以及实际的操作层面的要求来做数据分析和梳理，形成分级分类标准。从制度层面明确数据从收集、传输、存储、加工、使用直至销毁的全生命周期各环节，对不同的类别和级别的数据建立差异化管控要求和技术保护策略。

企业还可参考一些业界标准，如数据管理能力成熟度管理模型（DCMM）和数据安全能力成熟度模型（DSMM），以数据生命周期的六大阶段：数据采集、数据传输、数据存储、数据处理、数据交换和数据销毁为主线，从组织建设、制度流程、技术与工具和人员能力几个方面评估安全实现能力，建立符合企业自身特性的数据安全管理体系，实现持续的数据全生命周期标准管理。

网络安全管理

网络安全管理作为支撑数据安全的底层安全能力，对企业整体的防控具有重要意义。目前粤港澳三地在信息安全体系建设方面缺乏通用性的安全标准，港澳两地还未出台信息安全管理体系条款，而大陆司法管辖区内已有网络安全等级保护作为面向全社会的通用性成熟安全管理要求。

考虑到业务的交叉性，以及部分场景，如数据跨境到香港、澳门后仍然需要满足安全管控义务，大湾区企业，无论是否在内地物理部署了应用系统，均可参考《信息安全技术网络安全等级保护基本要求》建设企业内信息安全管理体系，包括安全管理制度、安全管理机构、安全管理人员、安全建设制度与安全运维制度。

随着网络合规风险加剧，企业应建立面向全体员工的合规培训机制，在员工职业生涯的各关键节点组织安全意识教育和安全管理制度宣传培训，并定期组织合规意识及合规管理要求培训，形成有效的合规责任考核机制。

企业还应建立合规举报查处的流程和机制并保持举报查处机制通畅，持续不断地对合规流程进行优化及改进。

加强安全防护能力

大湾区作为境内、境外的数据交互节点，大湾区中的企业除管理能力外，也需具备充分的安全技术防护能力，才能保障业务的运作，并在享受国家提供的数据流通便利情况下，履行相应的义务。为加强安全防护能力，企业应当建立良好的网络韧性基础。

与安全管理能力类似，考虑到网络安全等级保护是三地较为完善与成熟的安全要求，企业无论是否在境内部署系统，均可以等级保护作为基线建立安全技术防护能力。以往企业往往误以为仅有在境内备案的系统才需按照等保要求加固，忽略了等保本身对企业总体防护的指导意义以及等保作为三地最权威安全标准的实用价值。在大湾区的背景下，等保是最为实用安全标准，既可以提升企业能力，也能向监管证明企业业务在各地均满足我国要求的安全义务。

网络安全等级保护制度2.0文件中展示了以一个中心（安全管理中心）、三重防御（安全计算环境、安全区域边界、安全通信网络）为基础的"等级保护安全框架"思想，企业可遵照此思想要求，从安全物理环境、安全通信网络、安全区域边界、安全计算环境和安全管理中心技术层面去规划企业内部安全防护框架，例如安全计算环境层面中明确了控制点包含身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范、可信验证、数据完整性、数据保密性、数据备份恢复、剩余信息保护和个人信息保护，且针对不同的等级控制点有对应详细的控制要求，对企业来讲有极高的实践参考价值。

企业可以以等保2.0作为标准，建立良好的网络韧性基础，实现以网络安全运营为导向的主动防御和感知机制。

除了国内的安全标准外，企业也可以根据自身的实际情况，选择性参考国际相关标准。例如，NIST SP 800-160 Vol.2 Developing Cyber Resilient Systems:A Systems Security Engineering Approach中给出了网络韧性系统的定义和构建过程。在安全威胁已经成为不可避免的情况下，网络韧性可以帮助企业在遭受攻击时减少损失。

6 结语

大湾区的发展为企业通过数字化建设获得竞争优势带来前所未有的机遇与可能。一方面，便利渠道与更广阔的数据资源意味着大湾区企业将面临更大的安全和合规挑战，包括：

- 三地在网络安全、隐私保护和跨境的法律法规的不同，企业需要同时应对
- 当前的合规能力难以应对安全挑战和风险
- 网络环境等差异增加了安全防御的难度

另一方面，在面临这些安全和合规风险的同时，建议企业从以下几个方面提升和加强安全和合规能力：

- 应对三地不同的法律法规，建立一套精准的合规标准方案，能够覆盖隐私保护和跨境的内容，切实执行并应对和符合三地监管机构的要求
- 全面提升合规能力，包括改善组织架构、优化制度流程、明确职责分工、把控出境后风险、提升隐私保护能力等内容
- 构建完善的安全管理能力，防范与应对各类安全威胁
- 加强安全防护能力，建立良好的网络韧性基础

企业需谨记，在享受国家绿色通道的同时，必须有效保障数据安全与合规，履行守护国家安全、保障用户权益等义务与责任。企业需提早布局、通盘考虑，方能在享受利好的同时，确保持续发展。

附录：三地法律法规对比

领域	条款对比			应对难点
	内地	香港	澳门	
网络安全法律	▸《网络安全法》及《数据安全法》等，及相关实施实则，例如《网络安全审查办法》等	▸香港暂时并未针对网络安全作出专门立法，但要遵守《个人资料（私隐）条例》的个人资料安全和披露规定	▸《网络安全法》等	任何在粤港澳大湾区进行数据处理，必须留意并同时符合三地不同的网络安全要求。当中尤其要考虑： ▸内地法律对网络运营者、关键信息基础设施运营者及开展数据处理活动等的定义较广，须分析所提供的服务的监管要求 ▸内地“关键信息基础设施运营者”与澳门“关键基础设施的公共及私人营运者”的定义有所不同，其网络安全责任也有不同 ▸即使香港并未针对网络安全作出专门立法，新修订的《个人资料（私隐）条例》对未获同披露个人资料引入更为宽松条文，可视为广泛地涵盖任何个人资料处理者因未尽网络安全责任，罔顾资料披露会否对资料当事人造成伤害的潜在刑责
网络安全法律规管范围	▸网络运营者、网络产品、服务、数据处理者及关键信息基础设施运营者等，关键信息基础设施运营者包括公共通信及信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等行业，以及其他拥有一旦遭到破坏、丧失功能或数据泄露，可能严重危害国家安全、国计民生，及/或公共利益的重要网络设施、信息系统等	▸资料使用者、其聘用的第三方资料处理者等	▸关键基础设施的公共及私人营运者，而就私人营运者而言，包括供水；银行、财务及保险业；视听广播；经营固定或流动的公共电信网络，提供互联网接入服务等12类的住所在澳门或外地的私法实体等	
网络安全责任	▸网络运营者须按网络安全等级保护制度履行一系列的安全保护义务 ▸网络产品、服务应当符合相关国家标准的强制性要求及通过相关安全认证 ▸提供网络服务须要求用户提供真实身份信息 ▸制定网络安全事件应急预案 ▸关键信息基础设施运营者须履行进一步安全保护义务，包括在采购网络产品和服务可能有国家安全审查要求，进行安全风险抽查检测，网络安全应急演练等 ▸建立健全全流程数据安全管理制度，采取相应的技术措施和其他必要措施，保障数据安全 ▸对影响或者可能影响国家安全的数据处理活动进行国家安全审查	▸任何资料使用者须采取所有切实可行的步骤确保其持有的任何个人资料受到保障，不会遭到未获准许或意外的查阅、处理、删除、丧失或使用 ▸资料使用者也须确保聘用第三方资料处理者处理个人资料，无论是在香港或香港以外聘用，均必须有合约规范的方法或其他方法保障个人资料的安全 ▸最新修订更进一步对未获同意披露个人资料列为刑事罪行，当中只要披露者是意图或罔顾是否对资料当事人蒙受任何指明伤害（包括人身、财产或心理等伤害），即属犯罪	▸设立具能力执行网络安全内部保护措施的网络安全管理单位 ▸从具备适当资格及专业经验且以澳门特别行政区为常居地的人士中指定网络安全主要负责人及其替代人 ▸采取措施确保预警及应急中心能随时联络网络安全主要负责人及其替代人 ▸建立网络安全的投诉和举报机制 ▸制定网络安全管理制度及相关的内部操作程序 ▸按照网络安全管理制度及适用的技术规范，采取与网络安全的保护、检视、预警及应对有关的网络安全事故内部措施 ▸每年向有关监管实体提交网络安全报告 ▸允许预警及应急中心和监管实体部门的代表进入其设施及资讯网络，并向该等人员提供所要求的资料	

领域	条款对比			应对难点
	内地	香港	澳门	
隐私保护法律	▸《网络安全法》及《个人信息保护法》等	▸《个人资料（私隐）条例》及香港个人私隐专员公署的相关核准实务守则和指引等	▸《个人资料保护法》及澳门个人资料保护办公室所制订的各项指引	隐私保护方面，无论内地、香港和澳门都有全面性的隐私保护和个人资料保护要求，但三地法律相关要求既有相似的地方，但也并非完全一致，当中尤其要注意： ▸相关场景所收集的个人信息，是否涉及任何敏感个人信息或者自动化决策等（三地法律相关定义也略有不同） ▸所处理的个人信息的相关个人处于什么地区
隐私保护法律的适用范围及境外适用性	▸《个人信息保护法》除适用于在中华人民境内处理自然人个人信息的活动，更适用特定情况下的境外处理中华人民共和国境内自然人个人信息的活动： ▸以向境内自然人提供产品或者服务为目的 ▸分析、评估境内自然人的行为 ▸法律、行政法规规定的其他情形	▸《个人资料（私隐）条例》适用任何在香港或从香港控制个人资料收集、持有、处理或使用的资料使用者 ▸此外，最新修订使执法机关可向非港人服务提供者送达停止披露通知，要求他们采取停止披露行动，并且可以透过留置、邮递、传真及/或电子邮件到境外的最后为人所知的地址	▸《个人资料保护法》适用于： ▸全部或部份以自动化方法对个人资料的处理 ▸以非自动化方法对存于或将存于人手操作的资料库内的个人资料的处理 ▸以公共安全为目的对个人资料的处理 ▸对可以认别身份的人的声音和影像进行的录像监视、以及以其他方式对这些声音和影像的取得、处理和传播 ▸一般而言，《个人资料保护法》没有明文境外适用条文	
收集、使用、处理个人信息的要求及个人信息权利	▸《网络安全法》及《个人信息保护法》均有详细要求 ▸《个人信息保护法》进一步规定各个必须取得个人单独同意的情形，包括处理敏感个人信息、公开其处理的个人信息向其他个人信息处理者提供其处理的个人信息、向中华人民共和国境外提供个人信息等。也有例外情况	▸《个人资料（私隐）条例》有详细要求，包括附表一的六项保障资料原则 ▸有多个不同的情形需要不同类型的同意，包括使用个人资料于新的目的，或移转该资料，核对程序，直接促销等。亦需留意条例仔细的豁免情形 ▸新增未获同意披露个人资料，罔顾是否造成资料当事人指明伤害的罪行	▸《个人资料保护法》有详细要求 ▸一般必须于处理个人资料、处理敏感资料、披露或传播全部或部分个人资料、转移个人资料至境外等获明确同意，亦需留意《个人资料保护法》容许特定无需同意的情况	
关于敏感个人信息，及自动化决策的规定	▸对处理敏感个人信息有详细要求，包括： ▸须有特定的目的 ▸充分的必要性 ▸采取严格保护措施 ▸对自动化决策有详细要求，包括： ▸保证决策的透明度和结果公平、公正 ▸应当同时提供不针对其个人特征的选项，或者向个人提供便捷的拒绝方式 ▸不得对个人在交易价格等交易条件上实行不合理的差别待遇	▸没有明确条文规定，但私隐专员公署有一系列的核准实务守则和指引等，对于相关行为作出规定，违反相关规定可能成为违反条例的证据	▸有详细要求，包括： ▸分别有禁止以及容许处理敏感资料的规定 ▸法律列出个人会受到和不受到自动化决定约束的权利的情形	

领域	条款对比			应对难点
	内地	香港	澳门	
数据本地化要求	▸《网络安全法》及《个人信息保护法》规定以下信息必须境内存储，跨境提供必须进行相关安全评估: ▸关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据 ▸国家机关处理的个人信息 ▸处理个人信息达到国家网信部门规定数量的个人信息处理者在中华人民共和国境内收集和产生的个人信息	▸《个人资料（私隐）条例》没有明文数据本地化的要求 ▸须留意个别专业或行业是否有具体数据本地化要求	▸《个人资料保护法》及《网络安全法》均没有明文数据本地化要求	部分企业同时涉及大陆和香港业务，包含大量数据出境的场景，需要同时应对三个地区的法律法规，尤其需要注意: ▸业务是否需要符合法律法规的数据本地化要求。这一方面，必须留意内地的要求，适当地将必须在中国内地存储的信息存储在境内 ▸业务个人信息跨境传送的性质，是否分别已经符合三地的法律及相关法规和监管机构指引的要求
跨境信息传送的要求	▸《数据出境安全评估办法》要求数据处理者向境外提供数据，符合有关情形之一的，应当进行数据出境安全评估: ▸关键信息基础设施的运营者收集和产生的个人信息和重要数据 ▸出境数据中包含重要数据 ▸处理个人信息达到一百万人的个人信息处理者向境外提供个人信息 ▸累计向境外提供超过十万人以上个人信息或者一万人以上敏感个人信息 ▸国家网信部门规定的其他需要申报数据出境安全评估的情形	▸香港《个人资料（私隐）条例》第33条对跨境转移个人资料有相关规定，但该些规定尚未实施 ▸跨境传送个人信息时，必须符合所有《个人资料（私隐）条例》关于向第三方提供个人资料的规定，且企业应遵守个人私隐专员出台对跨境个人信息传送的相关指引	▸有作出规定，包括: ▸须确保接收转移资料当地的法律体系能确保适当的保护程度 ▸须遵守《个人资料保护法》其他规定 ▸但也有例外情况（即在接收方不能确保适当的保护程度，亦可在一定情况作跨境转移个人资料）	

联系我们

陈永诚
大湾区咨询服务主管合伙人
安永咨询服务有限公司
+852 2629 3751
vincent.chan@hk.ey.com

胡立基
华南区咨询服务主管合伙人
安永（中国）企业咨询有限公司
+86 20 2881 2731
winson.woo@cn.ey.com

朱莎莎
咨询服务理高级经理
安永咨询服务有限公司
+852 3758 5879
juliet.zhu@hk.ey.com

官嘉健
咨询服务高级经理
安永（中国）企业咨询有限公司
+86 20 2838 1113
alvin.guan@cn.ey.com

安永 | 建设更美好的商业世界

安永的宗旨是建设更美好的商业世界。我们致力帮助客户、员工及社会各界创造长期价值，同时在资本市场建立信任。

在数据及科技赋能下，安永的多元化团队通过鉴证服务，于150多个国家及地区构建信任，并协助企业成长、转型和运营。

在审计、咨询、法律、战略、税务与交易的专业服务领域，安永团队对当前最复杂迫切的挑战，提出更好的问题，从而发掘创新的解决方案。

APAC no. 03014465
ED None

ey.com/china

关注安永微信公众号
扫描二维码，获取最新资讯。