深圳数据交易所
SHENZHEN DATA EXCHANGE

ASIAN BUSINESS LAW INSTITUTE

中国-新加坡联合数据合规指引

实务手册

免责声明

重要提示：本文件仅为一般性信息指南，不构成任何法律或其他专业意见。如中英文版本有任何冲突或不一致，中国章节以中文版为准，新加坡章节以英文版为准。

本《中国-新加坡联合数据合规指引：实务手册》（以下简称“本指引”）作为一项公益性合作项目，由深圳数据交易所与亚洲商法研究所（Asian Business Law Institute）牵头，与志愿者专家撰稿人共同编写，旨在为在中新两地开展业务或关注数据合规保护的个人和组织提供通用性的参考信息和指导。

本指引的内容基于截至发布之日所掌握的公开信息和对相关法律法规的理解。本指引的编写方和撰稿人已努力确保本指引所载信息的准确性、完整性和及时性。然而，数据隐私和合规领域的法律法规复杂多变，且可能存在解释上的差异。因此，本指引可能无法涵盖所有相关细节，也无法及时反映所有最新的法律发展、监管要求或实践变化等。

本指引不构成、亦不应被视为任何形式的法律、会计、投资或其他专业意见。本指引中的信息不能取代针对特定情况的专业税务、会计、法律或其他相关专业意见。在做出任何与数据合规相关的具体决策或采取任何相关行动之前，读者应当咨询具备相关资质的专业顾问，并向其提供与特定情况相关的所有事实。

本指引的编写方和撰稿人对本指引所含信息的完整性、准确性或及时性不作任何明示或暗示的保证，包括但不限于对本指引

的功能、适销性和特定用途适用性的保证。对于本指引中的任何错误和疏漏，以及任何人因信赖本指引之全部或任一部分内容而采取或未采取的任何措施或因此而产生的任何后果，本指引的编写方和撰稿人不承担任何责任。

本指引的使用受以下条款约束:

- 本指引仅供信息参考，不得用于任何商业目的。
- 在引用或传播本指引的任何内容时，请务必注明出处，并明确其公益合作性质。
- 本指引的编写方保留随时修改、更新或撤回本指引的权利，恕不另行通知。
- 通过访问、阅读或使用本指引，即表示您已阅读、理解并同意本免责声明的所有条款。

中国章节

01

前言

当今世界，数字经济蓬勃发展，数据已成为驱动经济增长与社会进步的核心动能，跨境数据流动已成趋势。中新两国依托“国际数据港”建设及中新（深圳）智慧城市合作倡议，在数据出境、数字身份互认等领域取得显著成果。2023 年《区域全面经济伙伴关系协定》（RCEP）生效及中新数字政策对话机制的建立，进一步加速了两国数字贸易与数据合作。然而，数据跨境流动在便利企业运营的同时，也面临个人信息保护、商业秘密泄露及国家安全风险等挑战。

中国以《中华人民共和国网络安全法》（以下简称“《网安法》”）《中华人民共和国数据安全法》（以下简称“《数安法》”）《中华人民共和国个人信息保护法》（以下简称“《个保法》”）为核心，结合《促进和规范数据跨境流动规定》（以下简称“《跨境新规》”）等法规，构建了科学高效的监管体系；新加坡则以《个人数据保护法》（PDPA）为基础，巩固了亚太数据枢纽的地位。两国制度协同与差异并存，对企业合规管理提出更高要求。为了妥善应对出海企业数据跨境流动的合规风险，深圳市进一步深化《深圳建设中国特色社会主义先行示范区综合改革试点实施方案（2020－2025 年）》文件精神，探索高效便利安全的数据跨境流动机制，搭建了“1231”跨境数据流动服务体系（“1”套行动方案、+“2”大自贸区+“3”个跨境数据服务平台+“1”个协会），充分发挥前海、河套平台优势，结合深圳数据交易所在跨境数据流动创新实践，探索形成数据跨境负面清单制度，开展“区域出境安全评估”“个人信息保护认证（以下简称“PIP 认证”）”“个人信息出境标

准合同备案”工作，为有需要企业提供一站式数据跨境合规服务，打造衔接深港澳、链通全球的数据跨境深圳方案。

在此背景下，深圳数据交易所与新加坡亚洲商法研究所（ABLI）联合编制《中国-新加坡联合数据合规指引：实务手册》，旨在为中新两国企业提供一套系统、可操作的数据跨境流动规范框架，助力企业在合规前提下加快融入全球数字经济，有效防范“出海”过程中的跨境数据合规风险。本指引立足于对中新两国数据法律体系的系统比较，结合企业实际需求，从主体合规、标的合规及数据跨境流通合规三个层面，全面梳理数据分类分级、重要数据识别、个人信息保护及行业数据管理等关键要点，并辅以外资企业数据出境合规典型案例，为企业提供具有实践指导意义的操作指南。本指引通过助力企业精准把握政策机遇、规避潜在法律风险，将进一步推动中新数据合作走深走实，助力构建开放、包容、公正、安全的全球数字经济治理格局。

编委会

指导单位

深圳市政务服务和数据管理局

深圳市司法局

深圳市前海深港现代服务业合作区管理局

深圳市法学会

支持单位

网络数据安全合规实验室（深圳前海）

主编

王青兰 深圳数据交易所合规部总经理

副主编

胡婧卓 深圳数据交易所数据合规经理

孟洁 北京环球律师事务所合伙人

王艺 北京市环球（深圳）律师事务所合伙人

作者

（以下作者按章节排序）

王青兰 深圳数据交易所合规部总经理

张毅 上海市方达律师事务所合伙人

黎辉辉 上海市方达（北京）律师事务所顾问

黄嘉洁 北京天达共和律师事务所合伙人

马楷阳 万商天勤（深圳）律师事务所律师

李瑞 中伦律师事务所合伙人

蒲昱含 中伦律师事务所律师

徐晨 前中伦律师事务所律师

段志超 北京市汉坤律师事务所合伙人

王雨婷 北京市汉坤律师事务所顾问

孟洁 北京环球律师事务所合伙人

林奕 北京环球（成都）律师事务所顾问

王艺 北京市环球（深圳）律师事务所合伙人

刘嘉颐 北京市环球（深圳）律师事务所主办律师

史晶源 香港西盟斯律师事务所合伙人

赖雨晨 香港西盟斯律师事务所顾问

赖衍禹 前西盟斯律师事务所顾问

吴涵 北京市金杜律师事务所合伙人

姚敏侣 北京市金杜律师事务所律师

编委

陈一芊 深圳数据交易所数据合规经理

胡敏喆 深圳数据交易所数据合规经理

致谢

本指引在编写过程中，得到了杨宇鑫、洪延青、陈梦、麦丽娟、解辰阳、张亚男等多位专家的支持，谨此致以诚挚谢意。

目录

第一章概览与使用指南※

一、引言：中新数字合作的时代背景与指引价值

在全球数字经济浪潮中，数据已超越传统生产要素，成为驱动经济增长、科技创新与社会发展的核心引擎，其跨境流动作为数字经济的血脉，重要性愈发凸显。在此背景下，中国与新加坡于2023年将双边关系升级为“全方位高质量的前瞻性伙伴关系”，为各领域深度合作指明方向，其中数字经济合作尤其是数据跨境流动，正是这一伙伴关系中最具活力与前瞻性的组成部分。自 2013 年起，中国连续成为新加坡最大贸易伙伴，新加坡亦稳居中国最大新增投资来源国地位，深厚的经贸根基为数字领域合作奠定坚实基础；两国在促进全球贸易便利化、推动金融服务创新及共建“数字丝绸之路”等方面拥有广泛共同利益与巨大合作潜力，而数据的高效安全流动，正是实现这些共同目标的关键。

（一）中新数据合作的实践基础与企业需求

中新两国在数据跨境流动领域的合作绝非停留在概念层面，而是通过高层对话机制与标杆项目的深度联动，将战略共识转化为扎实成果。这些合作覆盖广泛且示范效应显著，充分印证了数据流动对区域数字经济发展的核心驱动作用。

在顶层设计层面，两国构建了高层对话平台以系统性推进数字合作：2024 年 6 月 27 日，首届“中新数字政策对话（DPD）”

※ 本章作者王青兰，法学博士，计算机科学与技术博士后。现任深圳数据交易所董事、合规部总经理，深圳市法学会理事，深圳市法学会涉外法治研究会常务副会长，深圳市网络数据合规与流通促进会副会长。

在北京成功举办，标志着两国数字合作迈入机制化、体系化新阶段。这一机制不仅为具体项目提供了有力政策指引与保障，更彰显了双方共建开放、安全、可信数字生态系统的战略决心。

在实践落地层面，合作呈现多点开花、全面布局的态势，尤其在智慧城市与前沿产业生态领域成果丰硕。以19年启动的新加坡—深圳智慧城市合作（SCI）为标志，双方已在数据国际互联互通、跨境贸易与智慧园区等领域推出多批项目；2023年12月的第四次会议上，又新增14个合作项目并为深新前海智慧城市合作创新示范园区揭牌。这些以城市为载体的实践，探索了数据在多元场景的跨境流通应用，为更大规模数据流动积累了宝贵经验。

此类实践在推动中新数字合作落地的过程中，让企业深刻体会到：两国数据治理体系基于各自发展阶段和现实需求形成了特色模式，中国始终坚持“安全与发展并重”的原则，在保障数据安全的同时积极促进有序流动，新加坡则依托市场化机制构建了灵活的合规框架，两者在核心目标上具有高度一致性。

随着合作场景不断丰富，企业在跨境运营、跨境贸易等高频数据流动领域开展业务时，需要精准理解中国在数据分类分级、跨境申报、安全评估等方面的规范要求，这些规则既为数据安全提供了坚实保障，也为企业合规运营指明了清晰路径。因此，一套能系统解读两国治理特色、明晰合规要点的指引，将帮助企业更好把握中国数据合规体系的科学性与便利性，而要做到这一点，首先需要深入了解中国数据合规体系的发展脉络与开放方向，这正是接下来重点阐述的内容。

（二）中国数据合规体系的演进与开放趋势

中国的数字治理体系以《网安法》《数安法》《个保法》为“三驾马车”，构建了以数据分类分级为基础、统筹发展与安全的顶层法律框架。在此基础上，《跨境新规》《数据出境安全评估办法》《个人信息出境标准合同办法》等法律法规共同搭建起完善的制度体系，通过明确数据分类分级规则、跨境豁免场景、安全评估机制、标准合同备案、PIP 认证等措施，结合自由贸易区负面清单与正面操作指引，持续推动数据跨境流动的规范化与便利化。

中国的数据合规体系始终处于动态优化之中，近年来政策调整步伐显著加快，释放出鲜明的开放与发展信号，不仅为在华企业提供了更清晰的合规指引，更彰显了中国参与全球数字治理的积极姿态。2024 年《跨境新规》的出台尤为关键，在严守国家安全与大规模个人信息保护底线的同时，大幅简化常规低风险商业场景中的数据跨境流程，充分体现了中国在数据治理领域的自信与开放，标志着中国在保障安全的前提下，正以更大力度促进数据的有序自由流动。

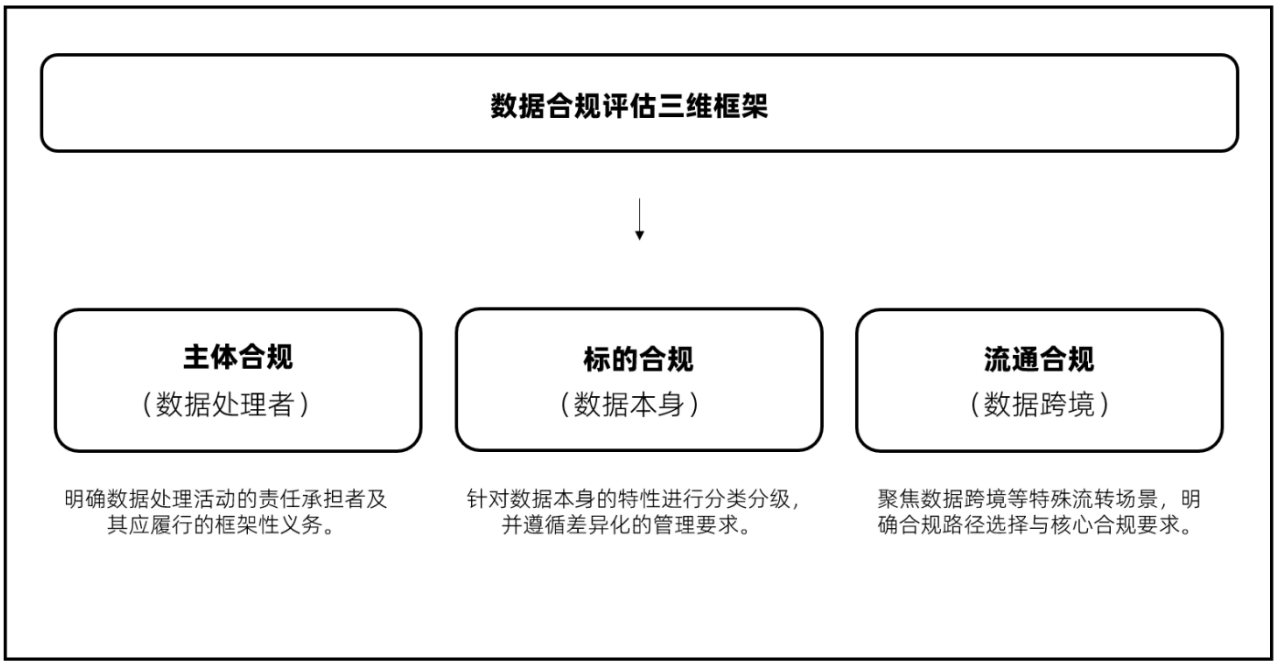
《跨境新规》该规定直面企业关切，实现了多方面突破性进展：一是明确“为订立、履行个人作为一方当事人的合同”“员工管理”这些常见经济活动以及“紧急情况”下个人信息的出境豁免程序，显著降低企业日常运营的合规成本；二是优化“重要数据”识别规则，明确“未被相关部门、地区告知或者公开发布为重要数据的，数据处理者不需要作为重要数据申报数据出境安全评估”，化解了企业对数据分类分级的不确定性；三是创设自贸试验区“负面清单”

制度，授权区域自主划定监管范围，为更高水平开放提供制度创新空间；四是降低了个人信息出境的监管门槛，为中小规模数据流动提供便利。

为构建契合两国法律体系的数据跨境流通合规实务指引，助力企业高效合规开展合作，深圳数据交易所与新加坡亚洲商法研究所（ABLI）联合发起本数据合规指引项目。本指引基于中新法律体系，结合实践需求及编写者的实务经验，从主体合规、标的合规及跨境流通合规三个层面，帮助企业精准理解两国监管政策与制度规范，系统梳理业务中的数据合规场景。接下来，为让读者更清晰地把握中国数据合规的内在逻辑与实践路径，我们将从核心框架入手，详解“主体—标的—流通”的合规体系架构。

二、中国数据合规实务框架与合规逻辑

为帮助读者，特别是来自不同法域的企业实践者快速、系统地理解中国数据合规的内在逻辑，本指引结合法律规定与实践经验，提炼出“主体—标的—流通”三维框架，将复杂的合规要求解构为三个环环相扣的核心环节，形成“谁来处理（主体）—处理什么数据（标的）—数据如何跨境（流通）”的清晰逻辑链条。需要说明的是，这一框架并非法律明文规定的官方体系，而是基于中国数据保护法律法规的核心要求，结合企业合规实践总结的方法论，旨在为企业提供清晰可操作的合规路径。三者相互关联、层层递进，既覆盖数据处理全流程的关键节点，又呼应中国“分类分级、安全可控”的治理理念，助力企业精准识别并落实合规义务。



通过这一框架，企业可以系统性地审视自身的数据处理活动：首先明确自身作为“主体”的责任与义务，其次识别所处理“标的”的类型与风险等级，最后在涉及数据“流通”（尤其是跨境）时，选择正确的合规路径。这种结构化的方法有助于企业避免合规盲点，建立全面、动态的数据合规管理体系。

（一）主体合规：数据处理者的核心义务

主体合规聚焦于数据处理者（如企业、机构）自身，要求其建立健全内部管理体系。这些义务可归纳为“框架搭建—事前防控—事后处置”三大模块，确保合规工作有章可循、风险可控。

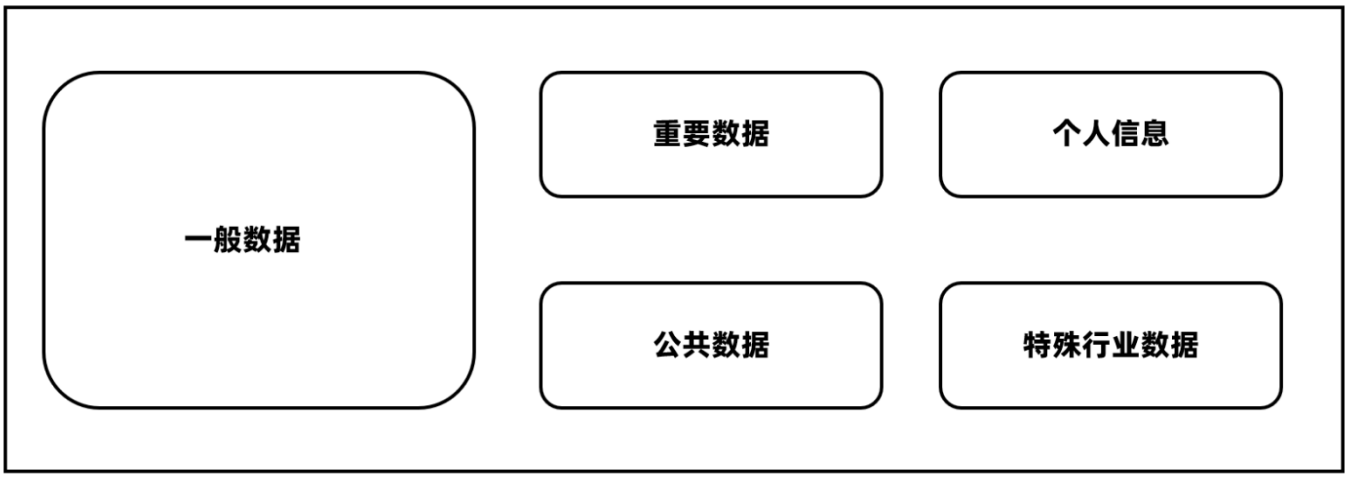
义务类型	核心内容	作用说明
框架搭建	**组织架构**（如依法设立数据安全负责人、个人信息保护负责人）、**制度构建**（如制定数据安全管理总纲、数据分类分级制度、应急预案等）、**人员管理**（如开展合规培训、明确关键岗位人员背景审查等）。	奠定合规基础，明确“谁来管、按什么规则管”，将合规责任落实到具体部门和个人。
事前防控	**数据分类分级**（识别一般、重要、核心数据等）、**外部合作方管理**（评估外部合作方的数据合规与安全能力等）、**风险评估**（在高风险个人信息与重要数据处理活动前开展影响评估）。	在数据处理活动开始前主动识别和评估风险，从源头降低合规隐患，避免被动应对。
事后处置	**安全事件响应**（如启动数据泄露应急预案）、**处置与上报**（采取补救措施，并按规定向监管部门报告和通知受影响的个人）。	在风险事件发生后，能够快速响应、有效止损，并履行法定的报告和通知义务，将负面影响降至最低。

（二）标的合规：不同类型数据的特殊要求

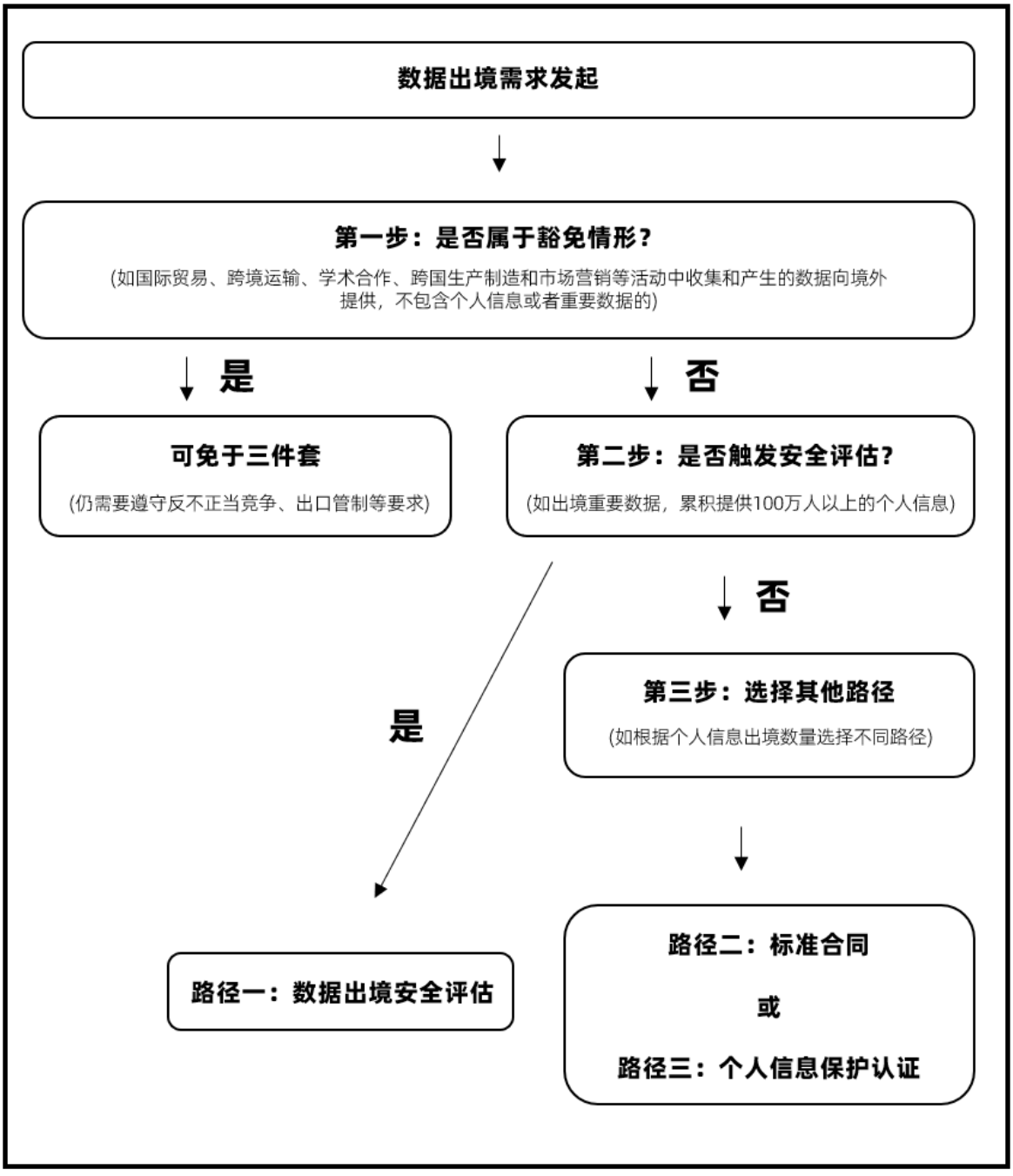
标的合规聚焦数据本身，核心在于“分类分级、差异管理、义务叠加”。中国的数据治理体系从国家安全和数据利用双重视角对数据进行分类，先明确所有数据需遵守的通用合规要求，再针对具有特殊属性的数据（如重要数据、个人信息、公共数据、及特殊行

业数据等）细化专属合规义务。企业需先准确识别数据类型，再匹配合适的合规义务——例如，公共数据需遵循开放共享规则，个人信息需落实主体权利保障，重要数据需执行境内存储与出境安全评估等特殊管控，特殊行业数据则需额外满足行业专属要求。

需特别注意的是，同一数据可能兼具多重属性：某医院的规模化患者诊疗数据，既属于包含敏感信息的个人信息，也可能被认定为重要数据，同时还属于医疗领域的公共数据及特殊行业数据。这种情况下，合规义务需“叠加适用”，企业必须同时满足各类数据的管控要求，确保全维度合规无遗漏。



数据跨境流通是中国数据合规监管的重中之重。其核心规则可概括为“合规路径+条件审核”。企业在向境外提供数据前，必须根据数据类型、数量、敏感程度等因素，判断并选择一条法定的合规路径。



为最大限度发挥本指引的实用价值，我们建议读者结合以下工具和提示进行阅读和实践。

（一）内容索引表

本指引采用“问题导向”设计，您可以根据自身的具体需求，通过下表快速定位到最相关的章节，进行重点阅读。

您的需求	建议阅读章节	核心内容摘要
想了解中国的**数据监管由哪些部门负责**?	第二章 监管体系与部门职责	网信、工信、公安、市监等部门的职责分工与监管重点。
需要为企业**搭建整体的数据合规管理框架**?	第三章 数据处理主体合规要求	组织架构、制度建设、风险评估、应急响应等框架性义务。
如何在业务过程中处理**不同类型**的数据?	第四章 数据标的合规管理规范	针对不同类型数据的分类分级标准与差异化合规要求。
有将数据**传输到中国境外**的需求?	第五章 数据跨境流通合规路径	安全评估、标准合同、保护认证三大路径及豁免情形详解。
希望参考**优秀企业的合规实践案例。**	第六章 良好合规实践指引	外资企业在个人信息保护、数据出境、员工管理等方面的实操案例。
需解决具体合规疑问?	第七章 常见问题与解答	汇总数据出境申报、个人信息行权、重要数据识别等高频问题，提供监管部门官方解释与实务操作建议
需要模板工具支持	附录 2:	提供个人信息保护影响评估报告

您的需求	建议阅读章节	核心内容摘要
	合规示例清单与模板	模板、数据出境风险自评估清单、标准合同填写指南、安全事件应急预案框架等可直接复用的工具

（二）使用提示

综合判断：在处理具体问题时，尤其是涉及数据跨境的场景，需要同时结合“主体合规”、“标的合规”与“流通合规”三章内容进行综合判断。

善用附录：本指引附录部分提供了“术语表”、“常见问题解答”以及可直接下载使用的“合规示例清单与模板”，能有效助力企业快速落地合规要求。

动态关注：数据合规领域法律法规更新频繁，本指引内容截至2025年8月。建议企业保持对立法和执法动态的持续关注，确保合规工作的时效性。

第二章监管体系与部门职责※

数据合规的第一步是什么？答案是了解谁在“管”数据。为此，在解析具体规则前，我们先介绍中国数据保护的主要监管部门。中国数据保护领域的主要监管执法部门包括网信部门、工信部门、公安部门和市场监督管理部门，同时行业主管部门在各自领域的职责范围内亦可对数据保护相关事项行使其法定监管职权。熟悉这些“监管者”，不仅能帮助在华开展业务的实体快速对接正确的联系窗口，还能避免因误解职责而走弯路。

一、网信部门

根据《网安法》第八条，《数安法》第六条和第三十一条，以及《个保法》第六十条和第六十二条的授权，网信部门作为统筹协调部门，负责网络安全、数据安全及个人信息保护工作的总体协调、监督管理与政策制定。国家网信办不仅主要主持制定和出台数据保护法律法规的配套措施，也积极在宏观的网络数据安全和个人信息保护监管和微观的 App 产品隐私保护等领域开展相关的监管和执法活动。

从宏观层面来看，对于企业未履行网络安全、数据安全保护义务，致使系统遭攻击篡改、数据泄露等违法违规问题，国家网信办会指导属地网信部门对违法违规企业依法采取责令改正、警告、罚

※ 本章作者张毅，上海市方达律师事务所合伙人，国际隐私专家协会（IAPP）注册隐私信息保护专家（CIPP/E、CIPP/A）、注册隐私信息管理经理（CIPM）、信息隐私研究员（FIP）；黎辉辉，上海市方达（北京）律师事务所顾问。王艺、段志超、刘嘉颐、王雨婷、史晶源、赖衍禹、赖雨晨亦有贡献。

款等处置处罚措施。对于严重到影响或可能影响国家安全的数据处理活动，国家网信办亦有权按照相关规定依职权发起网络安全审查[1]。同时，网信部门在关键信息基础设施（以下简称“CII”）安全保护、网络产品安全漏洞管理等多个领域亦发挥统筹协调作用。

此外，网信部门在数据出境管理方面，制定了数据出境安全评估、个人信息出境标准合同等相关规则，负责组织数据出境安全评估，对数据出境活动进行指导监督；在个人信息保护方面，负责统筹协调个人信息保护工作，制定了具体规则、标准，以推进个人信息保护社会化服务体系建设。

从微观层面来看，在近年持续开展的 App 合规治理行动中，各地网信部门也会对 App、第三方 SDK、小程序等服务渠道进行技术抽查，并对其中未明示个人信息处理规则、未经同意处理个人信息、未提供账号注销功能等情况进行点名通报和依法下架。此外，网信部门也高度关注线下扫码强制索取个人信息、人脸识别技术滥用等与民众生活密切相关的数据处理场景，对相关领域企业开展集中约谈、专项整治、执法处罚等监管行动。

二、工信部门

工信部以及其地方通信管理局也是数据保护领域重要的监管

[1] 《网络安全审查办法》第 16 条规定，网络安全审查工作机制成员单位认为影响或者可能影响国家安全的网络产品和服务以及数据处理活动，由网络安全审查办公室按程序报中央网络安全和信息化委员会批准后，依照本办法的规定进行审查。

执法机构之一，承担工业和信息化领域数据安全监管职责。主要职责包括：负责工业和信息化领域数据处理者的数据处理活动和安全保护的监督管理，推进数据开发利用和安全标准体系建设，制定数据分类分级等标准规范，指导开展数据分类分级管理工作；对工业和信息化领域数据处理者落实数据安全保护责任义务及管理措施进行监督检查，对违反数据安全相关规定的行为实施行政处罚。

与网信部门类似，工信部门也积极开展微观层面的 App 合规治理行动。作为 App 违法违规收集使用个人信息治理行动的主要执法部门之一，截至本指引发布之日，工信部官方网站已累计通报批评 45 批次侵害用户权益的 App 名单。作为电信领域的主管部门，工信部还会重点关注和打击 App 中显著影响用户体验的功能设计（例如“乱跳转”“弹窗无法关闭”“违规自启动/关联启动”等），并通过专项监管文件细化 App 产业链条上 App 开发运营者、SDK 提供方、应用商店等各方的合规要求[2]。

自 2023 年起，工信部还负责 App 和小程序的备案工作。[3]所有在中国境内向公众提供服务的 App 和小程序均需要在上线前通过网络服务接入商（对于 App 而言是其入网服务商，对于小程序而言是提供接入的应用平台）向工信部申请备案。

---

[2] 比如，工信部在 2021 年（具体可参见《工业和信息化部关于开展信息通信服务感知提升行动的通知》）和 2023 年（具体可参见《工业和信息化部关于进一步提升移动互联网应用服务能力的通知》）的专项行动中均分别细化了 App 合规管理的相关要求。

[3] 参见《工业和信息化部关于开展移动互联网应用程序备案工作的通知》。

三、公安部门

在数据保护领域，公安部门更专注于网络安全语境下的数据保护事项及刑事犯罪领域的执法活动，主要负责网络安全等级保护工作的监督、检查、指导，对互联网服务提供者和联网使用单位开展安全监督检查；依法打击利用网络产品安全漏洞实施的违法犯罪活动，对涉嫌违法处理个人信息、危害网络安全等违法犯罪行为进行查处；在 CII 安全保护中，加强安全保卫，防范打击针对和利用 CII 实施的违法犯罪活动。此外，公安部门在个人信息保护领域同样承担着重要的实务职责。比如个人信息处理者依据《个保法》第五十七条规定对安全事件进行报告时，实践中通常均由公安部门负责依法受理相关主体的报案。

以网络安全等级保护工作为例，公安部门作为该项工作主管部门，会通过“日常走访+年度检查”的方式巡查企业是否存在未妥善落实网络安全等级保护工作的情况，其中就涉及与数据保护措施充分性相关的问题，比如数据是否加密存储、是否设置妥善的访问权限控制、是否部署防数据泄露工具等。实践中，如遇企业发生数据泄露，公安部门还可能会视情节严重程度确定是否开展“一案双查”，即既对引发数据泄露的违法犯罪嫌疑人进行调查，也对涉案企业是否存在未履行数据安全保护义务开展调查。

四、市场监督管理部门

市场监督管理部门在数据领域监管中，主要负责从消费者权益保护、规范网络交易，以及反不正当竞争、反垄断等角度开展数据保护监管工作。

结合市场监督管理部门过往执法情况，其在消费者权益保护方面会重点关注违规收集和对外提供个人信息的行为，比如房产租售、小贷金融、教育培训、保险经纪、美容健身、装饰装修、旅游住宿、快递、电话营销等。

此外，市场监督管理部门也会从规范市场竞争秩序的角度开展执法。比如 2024 年 9 月上海市市场监督管理局公布了一起行政处罚决定，认定某金融信息科技企业在债券声讯经纪实时交易数据的特定相关市场具有支配地位，并实施了拒绝交易与附加不合理交易条件，构成了滥用市场支配地位的违法行为——该案也被誉为“中国数据反垄断执法第一案”。

除行政执法外，中国国家市场监督管理总局（“市监总局”）也会参与制定与个人信息和数据保护相关的认证规则，企业申请数据安全管理认证、个人信息出境、PIP 认证均需遵守市监总局出台的相关认证规则和要求。

五、行业主管部门与其他

随着数据保护问题在近年逐步成为社会与行业关注的重点问题，各领域的行业主管部门作为最熟悉行业实务操作与数据处理情况的机构，通常也会在职责范围内制定针对自身行业的数据安全管理办法，并在特定情况下履行其数据保护职责，以推进数据保护的监管工作。

以下是国务院和若干行业主管部门（或联合网信部门）发布的与数据保护相关的主要法律法规与监管要求。

发文部门	规范名称
国务院	《人类遗传资源管理条例》
国务院	《公共安全视频图像信息系统管理条例》
国家网信办、国家发展和改革委员会、工信部、公安部、交通运输部	《汽车数据安全管理若干规定（试行）》
中国人民银行	《征信业务管理办法》
国家金融监督管理总局	《银行保险机构数据安全管理办法》
财政部、国家网信办	《会计师事务所数据安全管理暂行办法》
工信部	《工业和信息化领域数据安全管理办法（试行）》
自然资源部	《自然资源领域数据安全管理办法》 《关于加强智能网联汽车有关测绘地理信息安全管理的通知》
国家卫生健康委、国家中医药局、国家疾控局	《医疗卫生机构网络安全管理办法》

国家数据局作为统筹推进数字中国、经济、社会规划和建设，实施国家大数据战略的部门，虽然现阶段暂未直接开展特定的数据保护监管执法行动，但其在推动数据要素确权与立法、引导数据要素市场发展，以及统筹数据资源整合共享与开发利用、推进数字基础设施布局规划和建设方面发挥着积极主导作用。

此外，虽然其并非典型意义的执法机关，消费者协会依法有权

针对侵害众多消费者个人信息合法权益的行为提起公益诉讼[4]，实践中已经有多地省级消费者协会通过提起个人信息保护公益诉讼的方式维护广大消费者的合法权益。

六、国家数据安全协调机制

为破解数据安全治理中跨领域、跨层级的复合型难题，中央国家安全领导机构主导建立了国家数据安全工作协调机制。国家数据安全工作协调机制作为依据《数安法》第五条确立的国家级数据安全治理核心机制，其设立与运行始终贯穿总体国家安全观，是统筹数据安全与发展的重要制度安排。从治理逻辑看，数据安全具有覆盖领域广泛性、风险传导整体性和应急响应即时性等突出特征，而单一部门存在监管范围有限性、权责划分独立性和跨部门协作程序性等客观约束。协调机制通过建立常态化跨部门、跨领域统筹联动机制，为系统性的数据风险治理提供了制度保障。

协调机制的核心职责体系涵盖三大维度：在制度建设层面，根据《网络数据安全管理条例》（以下简称“《网数条例》”）依法统筹协调有关部门制定重要数据目录和核心数据认定标准，为数据分类分级保护提供基础性制度依据，例如在工业、自然资源等重点领域指导行业主管部门精准划定数据保护重点范围（具体可见《工业和信息化领域数据安全管理办法》《自然资源领域数据安全管理办法》）；在风险防控层面，牵头建立集中统一的数据安全风险评估、

[4] 《消费者权益保护法》第47条规定，对侵害众多消费者合法权益的行为，中国消费者协会以及在省、自治区、直辖市设立的消费者协会，可以向人民法院提起诉讼。

信息共享与监测预警体系，强化重大数据安全事件的跨部门应急处置能力，严防系统性风险扩散蔓延；在安全审查层面，组织实施国家数据安全审查，对影响或者可能影响国家安全的数据处理活动进行严格把关，同时负责核心数据共享等关键环节的风险评估与统筹协调。

第三章数据处理主体合规要求※

随着《网安法》《数安法》《个保法》三大数据保护基础法律及其配套法规和实施细则（《网数条例》、《个人信息保护合规审计办法》（以下简称“《个保审计办法》”））的出台与实施，中国数据保护监管机构的执法行动也在不断加强，数据合规治理工作已成为了企业合规工作的重要任务之一。

良好的数据合规体系既可以引导员工在日常业务实践中遵循数据保护规则，避免员工因合规意识不足而违规操作，继而给企业带来合规风险，也能够成为实际发生违法违规的数据处理行为时，企业证明其不存在主观过错的有力证据，为划分和切割企业责任与违规个人责任提供必要支持。搭建数据合规体系、以数据保护打造自身品牌价值，对企业经营亦大有裨益。

一、组织架构

※ 本章作者张毅，上海市方达律师事务所合伙人，国际隐私专家协会（IAPP）注册隐私信息保护专家（CIPP/E、CIPP/A）、注册隐私信息管理经理（CIPM）、信息隐私研究员（FIP）；黎辉辉，上海市方达（北京）律师事务所顾问。王艺、段志超、马楷阳、刘嘉颐、王雨婷亦有贡献。

中国现行数据保护法律法规对企业的数据保护组织架构的要求分散于多项制度中，体现了分类管理、分级保护的立法思路。例如，《网安法》要求网络运营者确定“网络安全负责人”（第 21 条），要求关键信息基础设施运营者（以下简称 “CIIO”）应设置“专门安全管理机构和安全管理负责人”（第 34 条）；《数安法》要求重要数据处理者应当明确“数据安全负责人和管理机构”（第 27 条）[5]；《个保法》要求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应当指定“个人信息保护负责人”（第 52 条）；《网数条例》规定处理 1000 万人以上个人信息的处理者及重要数据处理者应当明确“网络数据安全负责人和管理机构”（第 28 和 30 条）；《个保审计办法》要求处理个人信息超过 100 万人的处理者应当指定“个人信息保护负责人”（第 12 条）；《儿童个人信息网络保护规定》要求网络运营者指定“专人”负责儿童个人信息保护（第 8 条）。

实践中，不少企业已设置了专门的数据保护团队，或者任命了专门的数据保护负责人，以满足数据保护法律法规的要求。鉴于数据保护团队通常要求具备必要的个人信息保护专业知识，大多数企业的数据保护部门职责通常不会由信息安全或者网络安全部门兼任，前者更侧重数据（尤其是个人信息）全生命周期的合规治理与隐私保护工作，后者则主要负责网络安全维护和一般数据安全

5 重要数据是中国数据保护法律法规项下的特有概念，是指特定领域、特定群体、特定区域或者达到一定精度和规模，一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能直接危害国家安全、经济运行、社会稳定、公共健康和安全的数据。

保护等更具有技术导向性的工作。数据保护部门的职责范围一般需要涵盖个人信息保护制度和流程的建立和实施、产品服务的合规与风险评估、数据保护咨询和培训、处理用户行权和投诉举报以及应对数据安全事件等工作事项。

二、制度构建与人员管理

尽管存在个别例外，中国现行的数据保护法律法规大多对企业应制定的内部规章制度和操作流程未作细化要求，而是侧重于提出概括的规定。比如，《数安法》仅规定数据处理者应“建立健全全流程数据安全管理制度”（第 27 条）；《个保法》在整体内控要求方面仅采用“制定内部管理制度和操作规程”的表述（第 51 条）。这种立法模式在为企业建章立制保留灵活性的同时，也对企业在合规实践中如何识别和优先建立关键性制度提出了更高的自主性和能动性要求。

实践中，企业在建立数据保护制度体系时通常会考虑以下方面：（1）为确保制度建设的系统性和规范性，企业内部应首先制定具备纲领性、指导性的政策文件，例如“数据保护总纲/总则”或类似政策，作为后续具体制度制定的依据；（2）对于法律法规明确提出的制度建设要求，应予以优先落实。例如，全流程数据安全管理制度、个人权利行使受理与处理机制、安全事件应急预案、重要数据管理规范、数据分类分级管理机制等，制度的缺失可能在监管检查或事件处置中被视为不合规的表现，因此具有较高的优先级；（3）对于跨国企业而言，在不同法域开展业务时，依据当地法律法规的具体要求，对内部合规体系进行针对性调整与适配，已然成为全球

合规实践中的普遍共识和常规做法。同样，对于在华跨国企业而言，虽然在全球层面建立了集团通用的合规制度，但是考虑到中国数据保护法律法规的特殊性，建议对相关制度进行“本地化”调整，或在全球制度中增设适用于中国市场的专章。例如，在数据安全事件应急预案中加入向中国监管部门报告及向受影响个人信息主体进行通知的机制。再例如依据中国法的要求，定制适用于中国的个人信息保护影响评估流程和内容;(4)在涉及多个业务部门协同配合的关键数据保护流程方面，如数据内外部传输管理、数据出境自评估与监测制度等，制定成文的规章制度有助于提升制度执行力和员工合规意识，也有利于企业内部的统一执行。

在完成制度构建后，企业应通过内部宣贯、教育培训、考核奖惩等机制，来确保员工对相关规章制度的遵从。实践中，建议企业应将要求员工遵从相关数据保护制度的规定明确体现在劳动合同（附录）、员工手册、入职或定期培训等书面材料中，并妥善留存员工参与培训、签署或者确认相关材料的记录，作为自证合规的证据。此外，企业还应注意遵从部分特殊人员的管理义务。比如，《网安法》要求 CIIO 应对安全管理负责人和关键岗位的人员进行安全背景审查（第 34 条）;《网数条例》则要求掌握有关主管部门规定的特定种类、规模的重要数据的网络数据处理者，应当对网络数据安全负责人和关键岗位的人员进行安全背景审查（第 30 条）。

三、数据分类分级管理

与制度构建要求相类似，中国数据保护法律法规项下的数据安全管理要求通常以目的或结果为导向的规定范式为主，并辅以

安全措施作为参考示例[6]。这种立法方式体现了安全措施与数据安全风险相匹配的监管理念，允许企业根据业务规模、数据体量和敏感程度选定贴合的安全措施，从而避免因过度合规而引发不必要的企业成本。

在这种风险匹配的框架下，企业需要首先明确不同类型、敏感程度数据的保护要求，通过数据分类分级衔接法律要求与企业实践，为差异化安全策略提供基础，确保措施与风险精准适配。中国数据分类分级制度依托多层次法律文件构建，形成了系统性的制度支撑与规范指引，具体来说：《网安法》首次提出“重要数据”概念，为数据分级奠定基础；《数安法》明确要求建立数据分类分级保护制度，界定关系国家安全、国民经济命脉等数据为核心数据并实施更为严格的管理；《个保法》通过对不同类别个人信息的差异化处理，推动数据分类制度细化；《网络安全审查办法》将“核心数据”“重要数据”相关风险纳入国家安全审查重点评估范畴；《网数条例》进一步界定了重要数据内涵，并通过专章的形式规范重要数据安全管理。

在企业开展分类分级工作时，《GB/T43697-2024 数据安全技术

[6] 比如，《网安法》第 21 条要求网络运营者应“采取数据分类、重要数据备份和加密等措施”，第 42 条要求网络运营者“应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失”；《数安法》第 27 条要求数据处理者“采取相应的技术措施和其他必要措施，保障数据安全”；《个保法》第 51 条要求个人信息处理者应“对个人信息实行分类管理”和“采取相应的加密、去标识化等安全技术措施”，以“防止未经授权的访问以及个人信息泄露、篡改、丢失”。

数据分类分级规则》（以下简称“《数据分类分级规则》”）作为核心指引，明确了科学实用、边界清晰、就高从严、点面结合、动态更新五项基本原则，为企业提供了清晰的操作遵循。

分类环节可按照“行业领域—业务范围—业务属性”的逻辑逐步细化：先依据所属行业（如工业、金融、电信等）划定大类，再结合企业运营模式和业务流程细化至具体板块，最终根据数据的实际业务属性确定细分类型，形成贴合行业特点的专属分类规则。具体到内部操作实践，“分类”可以按照业务条线与内部职能的划分进行[7]，目的在于锚定对应的领域监管要求以及内部负责部门，以便在实际数据安全管理工作中能够做到“专人专管”。

分级则需结合数据在经济社会中的重要程度，以及泄露、滥用等风险可能造成的危害后果，将数据划分为核心数据、重要数据和一般数据三个级别。具体操作可以遵循“确定分级对象—识别关键要素（如数据领域、规模、精度等）—分析影响范围与程度—综合评定级别”的流程，确保分级结果精准反映数据安全风险，为后续差异化保护措施的制定提供扎实依据。

在分类分级的基础上，企业需要对照法律法规明确列举的安全措施要求以及自身信息系统对应的等级保护要求（比如《GB/T22239-2019 信息安全技术网络安全等级保护基本要求》），并参照其他信息和数据安全保护的国际标准（比如《ISO/IEC27001

[7] 比如，根据业务条线和职能部门的划分，企业通常可以将数据分为客户（用户）数据、研发数据、系统运维数据、财务数据、人事数据、其他经营管理数据等类别。

信息安全管理体系》标准和《ISO/IEC27701 隐私信息管理体系》标准），选定必要的安全措施并结合数据的类型和级别进行差分式保护。常见的数据安全措施包括（静态和动态）数据加密与屏蔽、访问控制与权限管理、数据备份与恢复、流量监控与异常监测、日志审计与监控等。

四、外部合作方管理

在真实业务场景中，数据处理链条通常会涉及多家企业共同协作，各方之间既可能是相互独立的数据处理者，也可能是共同决定处理目的与方式的共同数据处理者，还可能是委托与受委托处理数据的关系。《个保法》明确要求在委托处理个人信息的场景项下，个人信息处理者与受托方应当就委托处理的事宜进行约定，在对外提供个人信息时则应当向个人告知接收方的名称或者姓名、联系方式、处理目的、处理方式和个人信息的种类，并取得个人的单独同意。《网数条例》在《个保法》的基础上对多方数据协助场景的合规要求进行了进一步细化，根据《网数条例》的要求，只要企业向其他数据处理者提供、委托处理个人信息和重要数据，就应当通过合同具体约定处理事宜，并对接受方履行义务的情况进行监督。

实践中，在与第三方开展涉及数据交互的合作时，企业一般会通过在主合作协议中加入数据处理章节或者拟定独立的数据处理协议的方式约定双方的权利义务。为了充分落实“监督”义务，企业通常会在合同条款中主张审计或者与审计相类似的权利，比如要求对方提供能够证明其遵守数据处理合同义务的材料以供查阅。

若该等合作对公司业务、数据处理合法性存在重大影响，或涉及强制性法律规定义务（如下文所述风险评估等），建议企业对相关合作方开展必要的准入尽调。可通过负面信息检索、安全能力资质验证、要求披露数据来源、查验隐私文本与授权样本、签署承诺函等手段，评估外部合作方的数据合规与安全能力，提前识别潜在风险。

五、风险评估机制

中国数据保护法律法规项下的风险评估要求主要包括《个保法》项下的个人信息保护影响评估（第 55 条），《数安法》项下的重要数据风险评估（《数安法》（第 30 条）、《网数条例》（第 31 和第 33 条），以及在数据出境合规机制（即数据出境安全评估、标准合同备案等）中衍生的类似评估[8]。

根据《个保法》的相关规定，个人信息处理者在开展对个人权益有重大影响的处理活动前应该开展个人信息保护影响评估[9]。鉴于评估流程涉及业务、安全、法务等多个部门联动与合作，不少跨国企业会在集团层面选择部署自动化工具协助开展评估。值得注意的是，部分企业隐私评估工具及其框架主要是基于《通用数据保

[8] 根据《数据出境安全评估办法》第 6 条和第 8 条，申报数据出境安全评估应当提交“数据出境风险自评估报告”，该等报告重点评估数据出境可能对国家安全、公共利益、个人或者组织合法权益带来的风险。根据《个人信息出境标准合同办法》第 5 条，个人信息处理者向境外提供个人信息前，应当开展个人信息保护影响评估。

[9] 根据《个保法》第 55 条的规定，该等处理活动主要包括处理敏感个人信息；利用个人信息进行自动化决策；委托处理个人信息、向其他个人信息处理者提供个人信息、公开个人信息；向境外提供个人信息；以及其他对个人权益有重大影响的个人信息处理活动。

护条例》（GDPR）制定的，企业在使用该类工具时应当结合中国法的要求和标准（比如《个保法》第 55 和 56 条，《GB/T39335-2020 信息安全技术个人信息安全影响评估指南》）进行本地定制化开发，以确保触发评估场景和评估内容的完整性。

根据《网数条例》的规定，“重要数据风险评估”则主要分为两类，一类是因特定处理活动触发的风险评估[10]，另一类是年度处理活动风险评估[11]。目前，工业和电信领域已经发布了数据安全风险

---

[10] 《网数条例》第 31 条：重要数据的处理者提供、委托处理、共同处理重要数据前，应当进行风险评估，但是属于履行法定职责或者法定义务的除外。

风险评估应当重点评估下列内容：（一）提供、委托处理、共同处理网络数据，以及网络数据接收方处理网络数据的目的、方式、范围等是否合法、正当、必要；（二）提供、委托处理、共同处理的网络数据遭到篡改、破坏、泄露或者非法获取、非法利用的风险，以及对国家安全、公共利益或者个人、组织合法权益带来的风险；（三）网络数据接收方的诚信、守法等情况；（四）与网络数据接收方订立或者拟订立的相关合同中关于网络数据安全的要求能否有效约束网络数据接收方履行网络数据安全保护义务；（五）采取或者拟采取的技术和管理措施等能否有效防范网络数据遭到篡改、破坏、泄露或者非法获取、非法利用等风险；（六）有关主管部门规定的其他评估内容。

[11] 第 33 条：重要数据的处理者应当每年度对其网络数据处理活动开展风险评估，并向省级以上有关主管部门报送风险评估报告，有关主管部门应当及时通报同级网信部门、公安机关。

风险评估报告应当包括下列内容：（一）网络数据处理者基本信息、网络数据安全管理机构信息、网络数据安全负责人姓名和联系方式等；（二）处理重要数据的目的、种类、数量、方式、范围、存储期限、存储地点等，开展网络数据处理活动的情况，不包括网络数据内容本身；（三）网络数据安全管理制度及实施情况，加密、备份、标签标识、访问控制、安全认证等技术措施和其他必要措施及其有效性；（四）发现的网络数据安全风险，发生的网络数据安全事件及处置情况；（五）提供、委托处理、共同处理重要数据的风险评估情况；（六）网络数据出境情况；（七）

评估规范及细则:《工业和信息化领域数据安全风险评估实施细则（试行）》和《YD/T3956-2024 电信领域数据安全风险评估规范》。随着各行业和领域重要数据识别工作的逐步推进和深入，该等风险评估的澄清说明与操作指导将得到进一步丰富和完善。

在实践中，很多企业面临的一大挑战是难以区分各类评估工作的触发条件和内容要求，我们以下表进行简要归纳说明。

评估类型	个人信息保护影响评估	重要数据风险评估	数据出境安全评估
法律依据	《个保法》第55、56条	网数条例第31、33条	《网安法》第37条、《个保法》第38条、《数据出境安全评估办法》、《跨境新规》
触发情形	事前评估 •处理敏感个人信息 •利用个人信息进行自动化决策 •委托处理个人信息、向其他个人	事前评估 •提供、委托处理、共同处理重要数据前 年度评估 •每年进行，且年度风险评估报告须向省级以上主管部门报送	事前评估 •向境外提供重要数据 •CIIO向境外提供个人信息（豁免情形除外） •非CIIO自当年1月1日起累计向境外提供100万人以上个人信息（不含

有关主管部门规定的其他报告内容。

处理重要数据的大型网络平台服务提供者报送的风险评估报告，除包括前款规定的内容外，还应当充分说明关键业务和供应链网络数据安全等情况。

评估类型	个人信息保护影响评估	重要数据风险评估	数据出境安全评估
	信息处理者提供个人信息、公开个人信息 •向境外提供个人信息 •其他对个人权益有重大影响的个人信息处理活动		敏感个人信息）或者 1 万人以上敏感个人信息（豁免情形除外）
实施方	个人信息处理者	重要数据处理者	数据处理者
评估内容	•个人信息的处理目的、处理方式等是否合法、正当、必要 •对个人权益的影响及安全风险 •所采取的保护措施是否合法、有效并与风险程度相适应	•提供、委托处理、共同处理网络数据，以及网络数据接收方处理网络数据的目的、方式、范围等是否合法、正当、必要 •提供、委托处理、共同处理的网络数据遭到篡改、破坏、泄露或者非法获取、非法利用的风险，以及对国家安全、公共利	•数据出境的目的、范围、方式等的合法性、正当性、必要性 •境外接收方所在国家或者地区的数据安全保护政策法规和网络安全环境对出境数据安全的影响；境外接收方的数据保护水平是否达到中华人民共和国法律、行政法规的规定和

评估类型	个人信息保护影响评估	重要数据风险评估	数据出境安全评估
		益或者个人、组织合法权益带来的风险 •网络数据接收方的诚信、守法等情况 •与网络数据接收方订立或者拟订立的相关合同中关于网络数据安全的要求能否有效约束网络数据接收方履行网络数据安全保护义务 采取或者拟采取的技术和管理措施等能否有效防范网络数据遭到篡改、破坏、泄露或者非法获取、非法利用等风险 •有关主管部门规定的其他评估内容	强制性国家标准的要求 •出境数据的规模、范围、种类、敏感程度，出境中和出境后遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等的风险 •数据安全和个人信息权益是否能够得到充分有效保障 •数据处理者与境外接收方拟订立的法律文件中是否充分约定了数据安全保护责任义务 •遵守中国法律、行政法规、部门规章情况 •国家网信部门认为需要评估的其他事项
形式要求	适用标准合同向境外提供个人信息的，评估报告	参考《工业和信息化领域数据安全风险评估实施细则（试行）》，评估报告应	须严格按照《数据出境安全评估申报指南》进行

评估类型	个人信息保护影响评估	重要数据风险评估	数据出境安全评估
	须按照网信部门发布的模板撰写其余场景可参考推荐性国标《GB/T39335-2020 信息安全技术个人信息安全影响评估指南》	当包括数据处理者基本情况、评估团队基本情况、重要数据的种类和数量、开展数据处理活动的情况、数据安全风险评估环境，以及数据处理活动分析、合规性评估、安全风险分析、评估结论及应对措施等	

六、安全事件响应与处置

《数安法》《个保法》及《网数条例》均对数据（含个人信息）安全事件的响应与处置提出了明确要求[12]，该等响应与处置的规定基本都要求企业在安全事件发生时立即启动预案，采取措施防止危害扩大、消除安全隐患，按照规定向有关主管部门报告，并视安全事件的严重程度判定是否应通知相关个人[13]。

2023 年公布的《网络安全事件报告管理办法（征求意见稿）》（尚未正式出台或生效）对网络安全事件的范围、分级、响应与处

12 《数安法》第 29 条、《个保法》第 57 条以及《网数条例》第 11 条。

13 比如，《个保法》第 57 条允许企业在“采取措施能够有效避免信息泄露、篡改、丢失造成危害”的情况下选择不通知个人；但是，如果监管部门认为可能造成危害的，仍然有权要求企业通知相关个人。

置要求进行了规定。其中，“网络安全事件”指由于人为原因、软硬件缺陷或故障、自然灾害等，对网络和信息系统或其中的数据造成危害，对社会造成负面影响的事件。由此可见，网络安全事件的范围将涵盖数据安全事件，后者的响应与处置也应遵从相关规定。根据该征求意见稿，网络运营者在发生网络安全事件时，属于较大、重大或特别重大网络安全事件的（比如涉及 100 万人以上个人信息泄漏的，或者重要数据泄露或被窃取对国家安全和社会稳定构成较严重威胁的），应当于 1 小时内按照《网络安全事件信息报告表》进行报告[14]。

网信、公安和工信等监管部门依据各自在网络安全或数据保护领域的职责内有设置安全事件报告义务，为企业数据安全事件处置提供了多层面指引。由于各部门职能侧重不同，企业在发生安全事件时，应有针对性地研判事件性质和类型，准确落实事件信息报告，保障监管部门及时掌握情况。实践中，建议企业应关注安全事件发生地是否已出台针对网络安全事件报告的协调机制，以便能够及时地履行报告义务。此外，跨国企业虽然通常制定信息安全

14 根据《网络安全事件报告管理办法（征求意见稿）》第 5 条，事件报告至少包括:（一）事发单位名称及发生事件的设施、系统、平台的基本情况;（二）事件发现或发生时间、地点、事件类型、已造成的影响和危害，已采取的措施及效果。对勒索软件攻击事件，还应当包括要求支付赎金的金额、方式、日期等;（三）事态发展趋势及可能进一步造成的影响和危害;（四）初步分析的事件原因;（五）进一步调查分析所需的线索，包括可能的攻击者信息、攻击路径、存在的漏洞等;（六）拟进一步采取的应对措施以及请求支援事项;（七）事件现场的保护情况;（八）其他应当报告的情况。

事件应急预案，但此类预案往往侧重于内部事件预警、响应和处置，而缺乏对监管报告和受影响主体通知等外部义务的具体指引。建议企业在制定或完善相关制度时，可参考以下要点：

分级报告机制：依据《工业和信息化领域数据安全事件应急预案（试行）》等规定，区分数据安全事件的危害程度（如特别重大、重大、较大、一般），并在符合法定条件时，按规定时限向主管机关上报。

个人信息主体通知要求：如事件涉及个人信息且对个人造成危害，应在规定时间内通知受影响个人信息主体。这一要求虽然在全球多数数据保护立法中均有体现，但需要特别注意各法域对通知时限、内容等的具体规定。就中国法规要求而言，通知内容一般应包括：

- 事件基本情况（涉及的个人信息种类、事件原因等）；
- 风险情况及可能危害后果；
- 已采取的补救措施；
- 个人可采取的减轻风险的建议；
- 企业联系方式以便后续沟通。

企业应结合中国国内法规及新加坡本地监管要求，进一步完善应急预案，确保合规应对数据安全事件。

第四章数据标的合规管理规范※

在中国开展业务时确保数据合规，首先需要理解中国数据治理的基本逻辑。中国的数据管理体系采用双重视角进行分类：从国家安全角度，根据数据的重要程度划分为核心数据、重要数据和一般数据，这一分类体系源于《数安法》，旨在通过分级管理强化对涉及国家安全数据的保护力度；从数据利用角度，“数据二十条”根据数据的主体归属和用途，将数据区分为个人信息、公共数据和企业数据，从而在保障安全的基础上，推动数据要素的合理流通与高效利用。

上述分类体系体现了中国在数据治理方面的政策导向：一方面通过分级管理，强化对核心数据和重要数据的保护，防范国家安全风险；另一方面，通过分类管理平衡数据安全与数据要素流通的关系。此外，不同行业基于其特性还需遵守特定的数据管理要求。下文将简要描述中国数据分级分类的逻辑，并对重要数据、个人信息、公共数据、一般数据、特殊行业数据分别进行阐述。

一、一般数据通用要求※

※ 本章作者黄嘉洁，北京天达共和律师事务所合伙人；马楷阳，万商天勤（深圳）律师事务所律师；李瑞，中伦律师事务所合伙人；段志超，北京市汉坤律师事务所合伙人；孟洁，北京环球律师事务所合伙人；蒲昱含，中伦律师事务所律师；徐晨，前中伦律师事务所律师；王雨婷，北京市汉坤律师事务所顾问；林奕，北京环球（成都）律师事务所顾问。王艺、张毅、史晶源、刘嘉颐、黎辉辉，赖衍禹、赖雨晨亦有贡献。

※ 本章作者黄嘉洁律师，天达共和律师事务所合伙人，拥有中国及美国法律双重专业背景，担任多家央企国企、上市公司、行业头部公司的合规顾问，致力于合规与风险治理、数据与网络安全领域工作。广东省涉外新锐律

为什么需要关注一般数据的通用合规管理要求？

实务中，在企业（尤其是不直接面向 C 端消费者服务的企业）的管理实践中普遍存在一个合规盲区：只要数据不涉及个人信息或重要数据，对于其他“一般数据”不存在法律法规上的合规管理义务，任意管理和使用一般数据不存在合规风险。

然而，企业对于一般数据的使用需要遵守《网安法》《数安法》等法规的合规要求。另外，随着 2024 年 8 月 30 日《网数条例》的正式出台，第二章一般规定中，明确规定了企业在处理一般数据时应遵循的合规准则和底线。一般数据的合规管理虽然不如重要数据和个人信息严格，但仍需从数据分类分级、处理合法性、全生命周期安全、风险防控及制度保障等多维度落实要求。

（一）一般数据的定义

关于一般数据的定义，根据国家标准《数据分类分级规则》的规定，一般数据是核心数据、重要数据之外的其他数据。

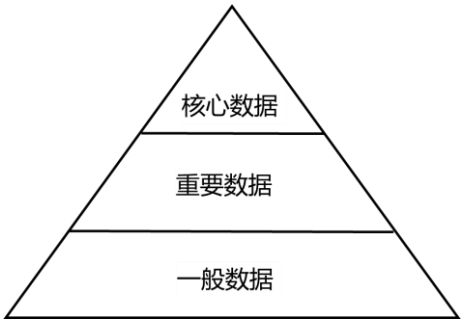
师，中国贸促委深圳委员会合规专家，深圳市法治营商环境企业合规专家，在深圳法治先行示范和合规试点工作中承担多项政府研究课题。

表 1 数据级别确定规则表

影响对象	影响程度		
	特别严重危害	严重危害	一般危害
国家安全	核心数据	核心数据	重要数据
经济运行	核心数据	重要数据	一般数据
社会秩序	核心数据	重要数据	一般数据
公共利益	核心数据	重要数据	一般数据
组织权益、个人权益	一般数据	一般数据	一般数据
注：如果影响大规模的个人或组织权益，影响对象可能不只包括个人权益或组织权益，也可能对国家安全、经济运行、社会秩序或公共利益造成影响。			

(来源:《数据分类分级规则》表 1 数据级别确定规则表)

一般数据的范围很大，除了核心数据、重要数据之外，一般企业在日常经营管理中接触和使用的数据，大部分都可以归类为“一般数据”(包括个人信息)。下图可以直观反映一般数据的范围，供企业参考和便于理解:



（二）常见的一般数据类型

鉴于本章其他部分已详细讨论个人信息和公共数据，本节聚焦于**其他类型的一般数据**，即不涉及国家安全、公共利益或重大社会影响的企业内部数据。以下列举的数据类型基于行业实践整理，**仅作参考**。企业需注意: 同一数据可能因使用场景不同而改变性质(如生产日志在制造业属一般数据，但若涉及关键基础设施则可

能升级为重要数据）；部分数据可能同时涉及多个分类维度（如客户服务录音既属"经营管理数据"，若含个人信息则会受到《个保法》的约束）。

（三）一般数据的重点合规要求

一般数据的使用和处理总体上需要遵守《数安法》的基本要求和规定。基于当前企业使用和处理的数据以网络电子数据为主的实际，企业仍然需要重点关注《网安法》以及《网数条例》下的重点规定和合规要求。对于上述法律法规中企业一般数据应当开展的合规管理要求，我们按照管控要点总结如下：

1.总体原则：合法合规

企业在收集一般数据时，应当采取合法、正当的方式，不得进行窃取或者以其他非法方式获取、非法出售或者非法向他人提供一般数据等非法处理活动。

此外，企业不得提供专门用于从事前款非法活动的程序、工具；明知他人从事前款非法活动的，不得为其提供互联网接入、服务器托管、网络存储、通讯传输等技术支持，或者提供广告推广、支付结算等帮助。

企业应当进行合作方与业务合规性评估，包括：建立全面的数据治理体系，严格防范参与任何违反数据安全法规的操作，重点监控非法获取、交易或披露数据资源等违规行为；同步开展合作方尽职调查，对存在信用瑕疵或经营异常的市场主体，系统化终止网络基础设施服务、云计算资源供给、数据存储空间租赁、信息传输通道开放、数字营销支持及金融支付接口对接等协同合作。

2.网络安全与技术措施

《网安法》第二十一条规定，网络运营者应当按照网络安全等级保护制度的要求，履行相关的安全保护义务。

根据《网安法》，“网络”是指由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换处理的系统。

实务中，很多企业简单地把“网络”理解为限于网站运营、App运营等直接的线上业务系统。但是，“网络”运营者的范围包括互联网、专用网、云计算平台/系统、物联网、工业控制系统和移动互联技术系统等（个人或家庭自用网络除外）。具体而言，如果企业开展的业务中包含有云平台、物联网系统、SasS 系统（Soft warea sa Service，“软件运营服务”）或者其他具备联网功能的产品或服务的，该企业便属于“网络运营者”，需要遵守网络安全的有关合规要求。

利用互联网等信息网络开展数据处理活动的企业，应当在网络安全等级保护制度的基础上，履行数据安全保护义务。具体而言，企业需要加强网络数据安全防护，建立健全网络数据安全管理制度，采取加密、备份、访问控制、安全认证等技术措施和其他必要措施，保护网络数据免遭篡改、破坏、泄露或者非法获取、非法利用，处置网络数据安全事件，防范针对和利用网络数据实施的违法犯罪活动，并对所处理网络数据的安全承担主体责任。

3.风险防控与应急响应

企业开展数据处理活动应当加强风险监测，发现数据安全缺

陷、漏洞等风险时，应当立即采取补救措施，履行报告义务。

其一，企业应当建立覆盖数据处理全周期的动态风险监测机制，通过部署自动化审计工具与人工巡检结合的方式，及时识别数据存储异常、API 接口漏洞等安全隐患，建立风险修复闭环机制。

其二，建议企业建立安全事件分级处置机制。例如，对于初级风险（如单点系统漏洞），由技术团队在 48 小时内完成补丁升级并留存修复日志；对于中级风险（如局部数据泄露），立即启动业务连续性预案，同步进行影响范围评估；对于高级风险（如大规模数据遭篡改），应当 30 分钟内组建跨部门应急响应小组，实施系统熔断并报决策层。

其三，建立双通知报告机制，向用户和监管部门通知报告安全事件。关于用户侧，可以根据数据类型采用差异化告知和通知的方式（个人信息需在确认泄露后 72 小时内通过注册邮箱/短信触达）；关于监管侧，根据《网安法》第四十二条要求，应当通过省级监管平台提交结构化事件报告（含受影响数据类型/数量、已采取措施、联系人信息）。

4.合作与第三方风险管理

企业在经营过程中可能存在向外提供或者委托处理一般数据等合作场景，例如企业将研发系统中的部分功能模块外包，进行研发、测试、运维和售后等工作。

实务中，企业与第三方的合同多为“委托开发协议”，其中包含有通用的知识产权条款、保密条款等内容，但是在数据安全方面的权利义务约定很少，或者只有简单的概括性条款（如“应当遵守

数据安全网络安全的有关要求”)。虽然当前法律法规没有直接对于一般数据的合同数据合规条款作出规定，但是为了降低企业在数据流动中的风险，建议企业参照《个保法》《网数条例》中关于“对外提供、委托处理”的合同条款约定要求，在合作协议中增设数据安全条款，如以下主要条款:

数据处理情况	**处理数据的类型、数量等具体指标**
	处理目的、方式、范围
	未经同意，不得访问、获取、留存、使用、泄露或者向他人提供数据，不得对数据进行关联分析
	合同结束后的数据处理（返还/销毁）
安全管理义务	企业内部提供的合规管理措施和保障
接受监管	同意接受数据源方对于数据处理活动的询问和审查，接受监督/审计
违约责任	违约（如不按照合同约定处理数据）情况下的违约责任

5.数据资产与交易

一般数据作为企业生产经营中占比最大体量的数据类型，是企业考虑启动数据资产化和数据交易的主要标的。目前，一般数据（除了个人信息以外)在数据要素市场中的产品类型丰富，以下举例三种产品形态:

行业预测分析类产品	这类产品基于大数据分析，能够为用户提供行业趋势、市场竞争格局以及消费者行为分析等信息。以地产大数据监测系统为例，它能协助许多房地产企业或其他涉及房地产市场的行业（如金融行业）进行大

	数据决策和监测。
风险预警类模型产品	风险预警模型通常是指利用机器学习技术构建的风险评估模型，帮助企业针对特定的用户或主体进行风险识别、分析和预警，例如对特定企业资信情况进行评估。风险预警模型在金融、信贷和征信等领域的应用较为广泛。
物联网数据服务	物联网数据服务是当前兴起的一个领域，无论是医疗企业还是说通信技术和制造业企业都有对物联网需求。企业通常通过将设备连接到云端，再连接到公司内部的系统网络平台，支撑整个物联网业务形态。物联网涉及设备传感数据业务、云平台以及公司内部平台，相关数据为包括个人用户数据和企业用户数据的内部数据。

企业在启动有关数据资产化和数据交易的同时，也需要严格按照有关法律法规的要求，对于一般数据的合规性开展合规审查工作，具体可以参照深圳市地方标准 DB4403/T564—2024《数据交易合规评估规范》，从合法维度、安全维度、诚信维度、权益维度对数据标的开展合规审查。

二、重要数据※

（一）重要数据的识别与评估

※ 本章作者马楷阳，本章作者马楷阳律师，万商天勤律师事务所国际委引领人、驻港代表、律师，拥有中国及美国纽约州律师执业资格，广东省法学会信息通信法学研究会理事，深圳市法学会数字法学研究会理事，担任多家行业头部公司、数据人工智能公司合规顾问。LEGALONE“客户信赖律师 15 强：涉外争议解决”、LEGALBAND“中国律界俊杰榜 30 强”、LEGAL ONE“中国律界实力新锐 30 强”、广东省涉外律师新锐人才、深圳市优秀青年律师。

如前文所述，在华新加坡企业获取和处理数据时，应依照中国相关法律法规对所涉数据进行分级管理，过程通常包括：确定待分级的数据范围、识别分级要素、开展数据安全影响分析，并据此识别和评估是否涉及核心数据及重要数据。然而，各行业领域重要数据目录尚在陆续制定中，相关识别标准在实践中仍然存在一定的模糊性，在此背景下，地方性规范及行业指引在重要数据识别和评估过程中，具有较强的补充性和参考价值，有助于企业更准确地理解和履行数据合规义务。

1.重要数据的识别方法

具体到重要数据而言，满足以下任一条件的数据，企业即应识别为重要数据：

（1）数据一旦遭到泄露、篡改、损毁或者非法获取、非法使用、非法共享，直接对国家安全、经济运行、社会秩序和公共利益造成一般危害的[15]；

（2）数据直接关系国家安全、经济运行、社会稳定、公共健康和安全的特定领域、特定群体或特定区域；

（3）数据达到一定精度、规模、深度或重要性，直接影响国家安全、经济运行、社会稳定、公共健康和安全；

（4）经行业领域主管（监管）部门评估确定的重要数据。

在根据以上方法完成数据项级别识别以后，如果分级对象是数据集或者衍生数据的，企业仍然需要注意根据就高从严原则、点

15 国家安全、经济运营、社会秩序和公共利益的具体考虑因素，可见《数据分类分级规则》附录 E 及附录 G。

面结合原则再综合确定级别:

（1）如分级对象为数据集的，则数据集级别可在数据项级别的基础上，按照就高从严的原则，将数据集包含数据项的最高级别作为数据集默认级别，同时需考虑分级要素（如数据规模）变化可能需要调高级别。

（2）如分级对象为衍生数据（包含脱敏数据、标签数据、统计数据、融合数据）的，则衍生数据级别在原始数据级别的基础上，综合考虑加工后的数据深度等分级要素对国家安全、经济运行、社会秩序、公共利益、组织权益、个人权益的影响进行确定。

2.各地方出台的识别规则

与此同时，各地方层面亦已开始出台识别规则，可以为在华新加坡企业识别和评估重要数据提供便捷的参考依据。天津、北京、海南、上海、浙江等地相继制定并发布自贸试验区数据出境负面清单，涵盖汽车、医药、零售、民航、再保险、深海业、种业等 17 个领域，旨在为相关数据跨境流动提供更明确的合规路径，创造更便利的条件[16]。

3.各行业出台的识别规则

除以上普适性规定及地方制定的规则外，各行业主管部门亦针对特定行业出台了数据分类分级细化标准。因篇幅所限，此处仅就金融行业、医疗健康领域、科技行业进行简单列举。

（1）金融行业

16 微信公众号 合规小叨客 《我国自贸区相继发布数据出境负面清单，企业重要数据管理影响几何？》

2024 年 12 月 28 日，中国国家金融监管总局发布并实施《银行保险机构数据安全管理办法》。针对银行业保险业数据处理活动，该办法针对数据安全治理、数据分类分级、数据安全管理、数据安全技术保护、个人信息保护、数据安全风险监测与处置作出了具体规定。

2020 年 9 月 23 日，中国人民银行发布并实施了《金融数据安全数据安全分级指南》（JR/T0197-2020），该指南主要对以下内容作出详细指引：（1）金融数据安全分级的目标、原则、范围；（2）数据安全定级的要素、规则、定级过程；（3）重要数据识别。该文件属于推荐性行业标准文件。

2023 年 8 月 6 日，中国人民银行发布并实施了《证券期货业数据安全风险防控数据分类分级指引》（GB/T42775-2023），该指引属于推荐性国家标准，主要对以下内容作出详细指引：（1）证券期货业数据分类分级保障措施；（2）数据分类的原则、要点和方法；（3）数据分级的原则、要点和方法；（4）数据分类分级中的关键问题处理。

（2）医疗健康行业

2021 年 7 月 1 日，市监总局、中国国家标准化管理委员会（“标委会”）联合发布的《信息安全技术健康医疗数据安全指南》（GB/T39725-2020）正式实施。该指南针对健康医疗数据的安全目标、分类体系、使用披露原则、安全措施要点、安全管理指南、安全技术指南进行了具体规定，并列举了医生调阅数据安全、患者查询数据安全等典型场景进行数据安全分析。

（3）科技行业

2025 年 1 月 24 日，市监总局、标委会联合发布并实施了《科学数据安全分类分级指南》。该指南属于推荐性国家标准。该指南针对科学数据安全分类、分级及分类分级原则进行了详细规定。

4.动态评估调整机制

在数字化浪潮与全球化竞争交织的背景下，重要数据的识别与管理不是静态任务，而是需要动态适配技术迭代、业务扩展及监管演进的系统性工程。随着数据分类分级标准的细化，企业需构建“识别-评估-调整”闭环机制，通过定期数据分类分级更新、风险场景动态监测及防护策略弹性优化，应对跨境流动、新兴技术应用等复杂挑战。当数据的业务属性、重要程度和可能造成的危害程度变化时，分级对象需进行动态更新。

在完成重要数据的识别后，如果企业遭遇以下常见情形，就需要积极推进数据的动态评估调整:

（1）数据规模变化，导致原有数据的安全级别不再适用;

（2）数据内容未发生变化，但数据时效性、数据规模、数据应用场景、数据加工处理方式等发生显著变化;

（3）多个原始数据直接合并，导致原有的安全级别不再适用合并后的数据;

（4）因对不同数据选取部分数据进行合并形成的新数据，导致原有数据的安全级别不再适用合并后的数据;

（5）不同数据类型经汇聚融合形成新的数据类别，导致原有的数据级别不再适用于汇聚融合后的数据;

（6）数据进行脱敏或删除关键字段，或者经过去标识化、匿名化处理;

（7）发生数据安全事件，导致数据敏感性发生变化;

（8）因国家或行业主管部门要求，导致原定的数据级别不再适用;

（9）需要对数据安全级别进行变更的其他情形。

（二）重要数据管理义务

1.采取技术措施及其他必要措施

作为重要数据的网络数据处理者，企业应当采取加密、备份、访问控制、安全认证等技术措施和其他必要措施保护网络数据。

此外，《网安法》《网数条例》均规定了所有数据的网络运营者/网络数据处理者应履行的安全保护义务，此处不再赘述。

2.重要数据的网络数据处理者应承担的数据安全保障义务

除一般规定外，作为为重要数据的网络数据处理者，企业应承担以下数据安全保障义务:

（1）对重要数据进行识别、申报

就申报而言，各行业及地方主管部门对报送对象、内容、方式的要求大体一致。以下行业及地方案例可供参考:

以汽车行业为例，广东省网信办已明确要求各注册地为广东且开展重要数据处理活动的汽车数据处理者报送《年度汽车数据安全管理情况报告》和《风险评估报告》、填写《开展重要数据处理活动的汽车数据处理者情况表》。各企业可选择通过纸质版或电子版报送至广东省网信办。除广东省网信办外，北京市网信办、北

京市经济和信息化局、北京市通信管理局亦联合组织开展了2024年度北京市汽车数据安全管理情况等报送工作。

以上海市为例，上海市通信管理局早在2023年即组织首批重点企业按照工业和信息化领域重要数据有关识别指南，开展重要数据识别认定及目录备案工作。在此期间，上海市通信管理局组织了数据安全工作委员会专家对各企业报送的重要数据开展两轮专题评审，并通过评审情况通报、公益培训、实地调研访谈等形式指导企业开展重要数据认定、分类分级和安全保护相关工作。

（2）明确网络数据安全负责人和网络数据安全管理机构

根据《网数条例》第三十条，重要数据的处理者应当明确网络数据安全负责人和和网络数据安全管理机构，网络数据安全负责人必须具备网络数据安全专业知识和相关管理工作经历，且由企业管理层成员担任，有权直接向有关主管部门报告网络数据安全情况。

就网络数据安全保护而言，企业所设置的网络数据安全管理机构需要履行以下义务:

- 制定实施网络数据安全管理制度、操作规程和网络数据安全事件应急预案;
- 定期组织开展网络数据安全风险监测、风险评估、应急演练、宣传教育培训等活动，及时处置网络数据安全风险和事件;
- 受理并处理网络数据安全投诉、举报。

如果企业掌握有关主管部门规定的特定种类、规模的重要数

据，还应当对网络数据安全负责人和关键岗位的人员进行安全背景审查，加强相关人员培训。审查时，可以申请公安机关、国家安全机关协助。

（3）风险评估义务

作为重要数据处理者，企业的风险评估义务存在于以下几种情形:

- 提供、委托处理、共同处理重要数据前，企业需要进行风险评估;
- 企业需每年度对网络数据处理活动开展风险评估，并将评估报告向省级以上有关主管部门进行报送。

风险评估内容及风险评估报告内容详见《网数条例》第三十一条、第三十三条之规定。除前述规定外，企业进行风险评估并报送报告仍需以各行业领域要求为准则。

仍以广东省汽车行业风险评估报告为例，该报告主要囊括以下几个方面的内容:

汽车数据安全风险评估概述: 含评估目标和范围、评估结论概要等。

- 基本情况介绍：包括单位、数据处理相关业务场景、信息系统等方面的基本情况，处理的重要数据的种类、数量、范围、保存地点与期限、使用方式，开展数据处理活动情况以及是否向第三方提供。
- 汽车数据安全风险识别: 从数据收集、存储、使用、加工、传输、提供、公开、删除、出境等环节，按照《汽车数据

安全管理若干规定（试行）》等法规标准要求识别风险点。

- 汽车数据安全风险分析及评价：结合已识别的风险点，从风险危害程度、安全事件发生可能性两个维度，综合确定数据安全风险大小。
- 评估总结及风险应对：描述针对已发现风险点采取的安全防护措施、评估防护效果，形成总结。

此外，根据《网数条例》的要求，如企业属处理重要数据的大型网络平台服务者，风险评估报告还需额外充分说明关键业务和供应链网络数据安全等情况。

（4）当出现企业合并、分立、解散、破产等可能影响重要数据安全的情形时，企业应当采取措施保障网络数据安全，并向省级以上有关主管部门报告重要数据处置方案、接收方的名称或者姓名和联系方式等；主管部门不明确的，应当向省级以上数据安全工作协调机制报告。

（5）企业向其他网络数据处理者提供、委托处理重要数据时，必须通过合同等与网络数据接收方约定处理目的、方式、范围以及安全保护义务等，并对网络数据接收方履行义务的情况进行监督，相关个人信息和重要数据的处理情况记录应当至少保存三年。

三、个人信息※

※ 本章作者李瑞，中伦律师事务所合伙人，为多家国内外企业提供中国网络安全与数据合规法律服务，在跨境传输、人工智能、数字化转型等前沿领域有丰富经验，业务覆盖日常经营、投融资、监管调查等多场景下涉及的网络安全与数据合规问题；蒲昱含，中伦律师事务所律师；徐晨，前中伦律师事务所律师。

作为一类特殊的数据，个人信息不仅关乎数据安全，更涉及自然人人格权、隐私权等更多维度的法律问题，因此整体安全保护及合规要求更为精细，实践中执法也最为活跃。对于企业而言，个人信息保护更是贯穿内部管理和外部业务开展的方方面面，包括但不限于客户个人信息保护、员工个人信息保护、上下游商业合作伙伴联系人个人信息保护等诸多议题。针对业务形态面向 C 端和/或其他以个人信息为重要生产要素（例如跨境电商、人工智能、医药研发等）的企业而言，还需综合考虑所面临的个人信息保护要求和信息系统架构搭建实际情况，在合规风险管理和商业发展之间寻求更佳的平衡。

（一）概览与导读

从立法层面来看，中国个人信息保护的要求以《个保法》中所搭建的合规体系为基础，同时也需遵循《民法典》《网安法》《数安法》等其他法律法规中有关数据安全的普适性要求。在此基础之上，监管部门还在执法过程中陆续出台了指导性文件，细化了部分合规要求，具有较强的指导意义，如《App 违法违规收集使用信息行为认定方法》等。系列国家标准及行业标准也在中国个人信息保护监管框架中起到了重要的作用，是企业开展个人信息保护合规工作的重要参考。

《个保法》及相关法规为个人信息保护确立了与欧盟 GDPR 类似的多项基本原则与核心机制，搭建了全生命周期保护要求，并对于个人信息主体权利保护、个人信息安全事件响应等重要方面做出了规定。此外，依据相关法律法规要求，个人信息处理者还需搭

建完善的内部合规体系，包括组织架构、制度及关键合规工具等方面。

结合上述的个人信息保护监管框架及合规要求脉络，在本章节，我们将首先厘清判断中国个人信息保护义务触发的一些关键概念，其次将阐释个人信息保护基石性的各项原则，逐一拆解个人信息全生命周期每一环节的合规保护要求并梳理两类特殊类型个人信息的额外保护要求。最后，本章将介绍个人信息保护要求下合规体系搭建维度而言的重点措施。

（二）个人信息保护义务触发的评估与判断

1.个人信息的定义及相关重要概念

根据《个保法》，个人信息是指以电子或其他方式记录的与已识别或可识别的自然人有关的各种信息。匿名化处理（即个人信息经过处理后无法再识别特定自然人且不能复原）后的信息则不被视为个人信息。

企业在判断是否需遵循个人信息保护要求时应当首先基于前述定义来明确自身业务流程中是否涉及处理个人信息。有关“个人信息”及“匿名化”这两个重要概念更详细的定义请见【附录 1：术语表】。

2.中国个人信息保护要求的域外效力

根据《个保法》第 3 条第 2 款，如企业在中国境外处理中国境内自然人个人信息的活动，存在以向境内自然人提供产品或者服务为目的，或分析、评估境内自然人的行为或法律、行政法规规定的其他情形的，也需遵循《个保法》的要求。由此可见，《个保

法》与 GDPR 一样具有域外效力，对于符合《个保法》第 3 条规定的个人信息处理者（即企业）而言，即便其处于中国境外，《个保法》仍然对其适用。

（三）个人信息保护要求

依据中国个人信息保护的立法监管框架，个人信息处理者处理个人信息，应当首先具备合法性基础。其次，个人信息处理者应当在个人信息全生命周期中的各个环节均有的放矢，落实个人信息保护要求。有关合法性基础的介绍请见下文第 3.1 节，有关全生命周期的各个环节及相应合规保护要求请见第 3.2 节。

1.个人信息处理的合法性基础

首先，个人信息的处理应当具备《个保法》第 13 条中明确的 7 类合法性基础之一。商业实践中，企业最为常用的合法性基础为告知个人信息主体并获取其同意（以下简称“告知-同意机制”），即企业需将其拟开展的个人信息收集行为告知个人信息主体并获取其同意，有关该机制的具体实践请见本章第 3.2 节第（1）部分。

需要特别提示的是，在以下对于个人信息主体权益造成比较大影响的场景，个人信息处理者还应当取得个人信息主体的**单独同意**（例如：触发单独弹窗，由用户勾选同意等）：

（1）处理敏感个人信息；

（2）向中国境外提供其处理的个人信息；

（3）向其他个人信息处理者提供其处理的个人信息；

（4）公开其处理的个人信息；

（5）在公共场所安装图像采集、个人身份识别设备所收集的

个人图像、身份识别信息用于维护公共安全意外的其他目的;

（6）其他法律、行政法规规定应当取得单独同意的情形。

根据《个保法》第 13 条，除告知-同意机制以外的其他个人信息处理的合法性基础还包括:

（1）为订立、履行个人作为一方当事人的合同所必需，或者按照依法制定的劳动规章制度和依法签订的集体合同实施人力资源管理所必需;

（2）为了履行法定职责或者法定义务所必需;

（3）为应对突发公共卫生事件，或者紧急情况下为保护自然人的生命健康和财产安全所必需;

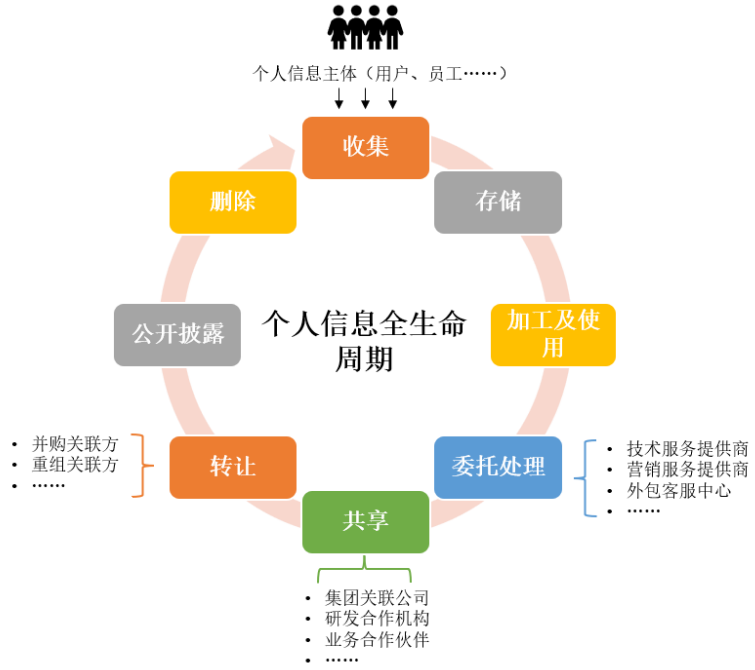
（4）为公共利益实施新闻报道、舆论监督等行为，在合理的范围内处理个人信息;

（5）在合理范围内处理个人信息主体自行公开或者其他已经合法公开的个人信息;

（6）法律法规规定的其他情形。

2.个人信息的全生命周期保护要求

个人信息的全生命周期包括收集、存储、加工与使用、委托处理、共享、转让、公开披露、删除等各个环节。



图示：个人信息全生命周期各环节

作为整体性要求，在个人信息全生命周期保护过程中，企业需要首先贯彻落实《个保法》提出的以下重要原则：

（1）合法、正当、必要原则：不得通过误导、欺诈、胁迫等方式处理个人信息；

（2）目的限制原则：处理个人信息应当具有明确、合理的目的，并应当与处理目的直接相关，采取对个人权益影响最小的方式；

（3）最小必要原则：收集个人信息，应当限于实现处理目的的最小范围，不得过度收集个人信息；

（4）公开透明原则：处理个人信息应当遵循公开、透明原则，公开个人信息处理规则，明示处理的目的、方式和范围；

（5）准确性及完整性原则：处理个人信息应当保证个人信息的质量，避免因个人信息不准确、不完整对个人权益造成不利影响。

在下文第 3. 部分中，我们将基于个人信息处理者满足告知-同意机制这一合法性基础的基础上，逐一介绍个人信息全生命周期不同环节企业需要履行的合规义务。

3.个人信息的全生命周期合规义务

（1）个人信息收集

如前所述，告知-同意机制为商业实践中最常援引的合法性基础。要落实告知-同意机制，企业应向个人信息主体明确告知收集的个人信息类型及目的，处理个人信息的规则（包括但不限于数据存放地域、存储期限、自身的数据安全能力、对外共享、转让、公开披露的有关情况等）等内容，确保个人信息主体在在充分知情的前提下，自愿、明确地表达其授权。如涉及收集未成年人个人信息，则还应注意本章第 3. 3 节第 3. 3. 1 部分的对于告知-同意机制的特殊要求。

还需特别注意的是，个人信息主体的同意需是具体、清晰的，而不能是通过默认、预选或其他不能体现个人信息主体意愿的模糊方式所获得（例如在弹窗勾选界面系统自动设置了“同意”和/或类似按键）。

从商业实践来看，企业在开展业务及运营的过程中不仅会涉及直接收集个人信息，也可能涉及频繁从第三方处收集个人信息。在前述不同的收集路径下，落实告知-同意机制的合规方案略有不同：

a)个人信息直接收集

个人信息直接收集是指企业直接从个人信息主体收集信息。

在互联网场景下，位于用户交互界面的隐私政策是落实告知-同意机制的最常用机制。

一般而言，隐私政策的内容应包括个人信息处理者的基本信息、收集和使用个人信息的目的及业务功能、个人信息处理规则（如收集方式、存储期限等）、对外共享、转让、委托处理个人信息的情况、政策变更时的告知方式等。隐私政策所告知的信息应真实、准确、完整，而且所用语言应清晰易懂。依据《网数条例》，企业还应建立并公开《个人信息收集清单》和《与第三方共享个人信息清单》作为隐私政策的配套文件。

b)个人信息间接收集

个人信息间接收集是指企业并非直接从个人信息主体处获取信息，而是通过第三方渠道获得信息。在这种场景下，企业应当注意确保第三方在提供个人信息时已履行了个人信息收集合法性要求的义务，包括获得个人信息主体的同意，并告知其个人信息将被共享的用途和范围。

（2）个人信息存储与删除

a)个人信息存储的时间期限要求

根据《个保法》第 19 条，个人信息不应无限期永久存储，保存期限应为实现目的所必需的最短时间。超出前述个人信息保存期限后，企业应对个人信息进行删除或匿名化处理，但法律法规另有规定的除外。

b)个人信息存储的安全技术与组织管理要求

存储期间的安全保障也是个人信息存储合规的重要工作。企

业应对所存储的个人信息采取加密、去标识化等的技术措施，并考虑依据内部组织架构规划设置完善访问权限管理制度，避免越级访问等带来数据泄露风险。

（3）个人信息加工与使用

在日常经营活动中，企业可能利用掌握的个人信息开展多种形式的加工处理以挖掘其商业与应用价值，如分析用户标签、构建用户画像、开展自动化决策等。在个人信息加工与使用时，企业应在遵循一般性原则的基础上，针对个人信息权益影响较大的场景有的放矢地采取风险管控措施。我们将个人信息加工处理的一般性要求及 2 个典型加工处理场景的合规要求总结如下:

a)个人信息加工使用的一般性要求

整体而言，企业在使用个人信息时应注意严格遵循个人信息主体的授权范围。若超出此前获得的授权范围，需再次征得个人信息主体的同意。

b)典型加工使用场景合规管控要求

- 用户画像及标签

涉及利用个人信息加工形成用户标签及画像的，企业应避免将违法和不良信息关键词记入用户兴趣点或者作为用户标签并据以推送信息内容，避免设置歧视性或者偏见性的用户标签，或因规则设置不当导致部分用户遭受不公平待遇。其次，用户画像中对个人信息主体的特征描述，应当杜绝包含淫秽、色情、赌博、迷信、恐怖、暴力或者对民族、种族、宗教、残疾、疾病歧视的内容。

- 自动化决策

涉及利用个人信息进行自动化决策的，企业应当保证决策的透明度和结果公平、公正，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。通过自动化决策方式向个人进行信息推送、商业营销，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。通过自动化决策方式做出对个人权益有重大影响的决定，个人有权要求个人信息处理者予以说明，并有权拒绝个人信息处理者仅通过自动化决策的方式作出决定。此外，根据《个保法》第 55 条，利用个人信息进行自动化决策的，个人信息处理者应当事先进行个人信息保护影响评估，并对处理情况进行记录，有关个人信息保护影响评估的介绍请见后文“5.个人信息保护影响评估”一节。

（4）个人信息委托处理、共享、转让及公开披露

a)个人信息的委托处理

《个保法》项下的委托处理活动是指个人信息处理者将部分个人信息处理活动委托给受托方（该角色类似于新加坡《个人数据保护法》项下的“数据中介”）的进行加工处理的行为，更为详细的定义请见本指引【附录 1：术语表】，受托方应严格遵循个人信息处理者的指示，且无权决定处理个人信息的目的、方式等。

个人信息处理者委托第三方处理个人信息时，应当事前开展个人信息保护影响评估，与受托方约定委托处理的目的、期限、处理方式、个人信息的种类、保护措施以及双方的权利和义务等，并对受托方的个人信息处理活动进行监督。受托方则应注意严格遵循相关要求。

b)个人信息的共享

个人信息共享是指个人信息处理者将其所掌握的个人信息提供给其他个人信息处理者的行为。在共享场景下，接收方应按约定目的适用数据，但能够独立决定个人信息后续处理的目的与方式。

企业向其他个人信息处理者共享个人信息的，应当事先进行个人信息保护影响评估，并在授权同意文件中向个人告知接收方的名称或者姓名、联系方式、处理目的、处理方式和个人信息的种类，取得个人的单独同意。为更好落实合规保护要求，双方还应签订数据处理协议明确各自的责任和义务。

c)个人信息的转让

根据相关国家标准，企业因合并、分立、解散、被宣告破产等原因需要转让个人信息的，应当向个人告知接相关情况，并确保变更后的个人信息处理者履行同等义务。

d)个人信息的公开披露

原则上，企业不应公开披露所处理的个人信息。经法律授权或具备合理事由确需公开披露任何个人信息时，企业应注意履行事先开展个人信息保护影响评估，向个人信息主体告知公开披露个人信息的目的、类型，获得个人的单独同意，记录和存储公开披露的情况等。生物识别信息、敏感个人信息分析结果等不应公开。

4.特殊类型个人信息的保护要求

（1）未成年人个人信息

依据《个保法》，不满 14 周岁的未成年人个人信息属于敏感个人信息，处理此类个人信息需遵循更高的个人信息保护要求。此

外，未成年人个人信息保护还需要遵守《未成年人网络保护条例》等法律法规中的相关要求。

收集不满 14 周岁的未成年人个人信息前应当取得未成年人的父母或者其他监护人的同意，并应当制定专门的个人信息处理规则。其他未成年人保护的要求还包括企业应当自行或委托专业机构，每年对其处理未成年人个人信息的合规情况进行审计，并将审计结果及时报告网信等部门等。

（2）死者个人信息

根据《个保法》第 49 条，自然人死亡的，其近亲属为了自身的合法、正当利益，有权对死者的相关个人信息行使查阅、复制、更正、删除等权利，但死者生前另有安排的除外。

5.个人信息主体权利保护

（1）个人信息主体的权利

个人信息主体权利的响应是个人信息保护及合规工作的重要方面。企业应当保障个人信息主体的行权路径有效且畅通。根据个保法，个人信息主体权利包括:

a)访问权

个人信息主体有权查阅、复制其个人信息，但法律、行政法规规定应当保密或者不能查阅、复制的情形除外，或者查阅、复制将妨碍国家机关履行法定职责的除外。

b)更正权

个人信息主体有权请求更正、补充其个人信息，个人信息处理者应当对其个人信息予以核实，并及时更正、补充。

c)删除权

有下列情形之一的，企业应当主动删除个人信息，企业未删除的，个人信息主体有权请求删除:

- 处理目的已实现、无法实现或者为实现处理目的不再必要;
- 已停止提供产品或者服务，或者保存期限已届满;
- 个人撤回同意;
- 违反法律、行政法规或者违反约定处理个人信息;
- 法律、行政法规规定的其他情形。

法律、行政法规规定的保存期限未届满，或者删除个人信息从技术上难以实现的，企业应当停止除存储和采取必要的安全保护措施之外的处理。

d)解释权

个人信息主体有权要求企业对其个人信息处理规则进行解释说明。

e)可携带权

个人信息主体有权请求将个人信息转移至其指定的个人信息处理者。对符合下列条件的个人信息转移请求，企业应当为个人信息主体指定的其他数据处理者访问、获取有关个人信息提供途径:

- 能够验证请求人的真实身份;
- 请求转移的是本人同意提供的或者基于合同收集的个人信息;
  - 转移个人信息具备技术可行性;
  - 转移个人信息不损害他人合法权益。

f)撤回同意权

基于个人同意处理个人信息的，个人信息主体有权撤回其同意，企业应当提供便捷的撤回同意的方式，不得以个人不同意处理其个人信息或者撤回同意为由，拒绝提供产品或者服务，但处理个人信息是提供产品或者服务所必需的除外。

（2）个人信息主体的请求响应

如果个人信息主体提出权利请求，企业应在验证个人信息主体身份后，及时响应个人信息主体提出的请求。根据国家网信办等部门发布的《App 违法违规收集使用个人信息行为认定方法》，APP 产品经营者响应个人信息主体权利期限以接到行权请求之日起 15 个工作日内处理并反馈为宜；如无法及时响应的，个人信息处理者应提前联系用户并说明情况和反馈时限。

对合理的行权请求原则上不收取费用，但对一定时期内多次重复的请求，可视情况收取一定成本费用。

6.个人信息保护影响评估

个人信息保护影响评估是《个保法》第 55 条所明确的重要合规机制。它是指对企业的特定个人信息处理活动，检验其合法合规程度，判断其对个人信息主体合法权益造成损害的各种风险，以及评估用于保护个人信息主体的各项措施有效性的过程。

（1）个人信息保护影响评估触发情形

根据《个保法》第 55 条，企业有下述情形之一的，应当提前开展个人信息保护影响评估，并依据评估结果考虑是否调整并完善合规措施：

- 处理敏感个人信息;
- 利用个人信息进行自动化决策;
- 委托处理个人信息、向第三方提供个人信息、公开个人信息;
- 向境外提供个人信息;
- 其他对个人权益有重大影响的个人信息处理活动。

（2）个人信息保护影响评估的核心要点

根据《个保法》第 56 条，个人信息保护影响评估应当包括个人信息的处理目的、处理方式等是否合法、正当、必要、对个人权益的影响及安全风险、所采取的保护措施是否合法、有效并与风险程度相适应。

7.个人信息保护合规审计

个人信息保护合规审计是《个保法》所明确的法定义务，是指对个人信息处理者的个人信息处理活动是否遵守法律、行政法规的情况进行审查和评价的监督活动，主要要求可参考《个保审计办法》。一般而言，企业应当依法主动定期开展审计（以下简称“企业主动审计”），但个人信息保护监管机关也有权在特定情形下要求个人信息处理者委托专业机构发起审计（以下简称“保护部门发起审计”）。相关具体情形、频次及审计要点总结如下:

（1）企业主动审计

根据《个保审计办法》，处理超过 1000 万人个人信息的企业，应每两年至少开展一次个人信息保护合规审计。其他企业可根据自身情况合理确定开展个人信息保护合规审计的频次。此外，处理

100 万人以上个人信息的企业还应当指定个人信息保护负责人，负责个人信息保护合规审计工作。

（2）保护部门发起审计

《个保审计办法》第 5 条指出，符合以下情形之一的，国家网信部门和其他履行个人信息保护职责的部门（即“保护部门”），可以要求企业委托专业机构对个人信息处理活动进行合规审计：

- 发现个人信息处理活动存在严重影响个人权益或者严重缺乏安全措施等较大风险的；
- 个人信息处理活动可能侵害众多个人的权益的；
- 发生个人信息安全事件，导致 100 万人以上个人信息或者 10 万人以上敏感个人信息泄露、篡改、丢失、毁损的。

（3）审计核心要点

依据《个保审计办法》，企业自行开展或者按照监管部门要求委托专业机构开展个人信息保护合规审计的，均应参照《个保审计办法》的附件《个人信息保护合规审计指引》开展审计，包括但不限于个人信息处理活动的合法性基础；个人信息处理规则的完整性、准确性；个人信息委托处理、共享的合规保护情况；是否保障个人信息主体权利；是否制定内部管理制度和操作规程等。

8.个人信息安全事件处置

个人信息安全事件具有隐蔽性、突发性和多样性等特点。根据个保法第 51 条，企业应制定并组织实施个人信息安全事件应急预案，并定期进行演练。一旦遭遇个人信息安全事件，企业应依据应急预案在第一时间进行响应和处置。

（1）应急响应预案及演练

企业应当结合业务实际，对面临的个人信息安全风险做出系统评估和预测，制定全面、有效和可执行的个人信息安全事件应急响应预案。企业还应当对相关人员进行应急预案培训，定期开展应急预案演练。

（2）个人信息安全事件应急响应处置

如发生个人信息安全事件，企业应按照应急预案、操作规程及时查明个人信息安全事件的影响、范围和可能造成的危害，分析、确定事件发生的原因，提出防止危害扩大的措施方案。

企业还应当建立通报渠道，在安全事件发生后按照相关规定及时通知监管部门和个人。此外，企业应当采取相应措施将个人信息安全事件可能造成的损失和可能产生的危害风险降至最低。

9.个人信息保护外部监督机构

根据《个保法》第 58 条，提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者，应当履行下列义务:

（1）按照国家规定建立健全个人信息保护合规制度体系，成立主要由外部成员组成的独立机构对个人信息保护情况进行监督;

（2）遵循公开、公平、公正的原则，制定平台规则，明确平台内产品或者服务提供者处理个人信息的规范和保护个人信息的义务;

（3）对严重违反法律、行政法规处理个人信息的平台内的产品或者服务提供者，停止提供服务;

（4）定期发布个人信息保护社会责任报告，接受社会监督。

当前，针对“主要由外部成员组成的独立机构”的配套规定尚在制定过程中。关于该机构外部成员的任职资格、提名及任免程序、履职要求、人选及任期、监督职责等具体问题，企业可参考国家标准 GB/T45404—2025《数据安全技术　大型互联网企业内设个人信息保护监督机构要求》的相关内容。

四、公共数据※

（一）公共数据开发利用的政策背景

在我国，政府部门以及承担着公共管理职能与公共服务的企事业单位规模十分庞大，并且在公共职能运转、服务提供过程中均能收集、产生大量数据。而这些数据往往涉及经济社会生活的方方面面，具有规模体量大、数据质量好、价值潜能大、带动作用强、公共属性强等特点，承担着重要的数据流通价值，对于政府治理能力的提升、公共资源的优化配置、民生服务的保障等都具有重大意义。故而如何盘活公共职能承担部门、企业的数据，充分发挥其要素作用始终是发展建设数字经济的重要命题。

早在 2015 年，《关于积极推进“互联网+”行动的指导意见》《促进大数据发展行动纲要》便已经关注到公共数据在大数据发展中的重要价值。此后，国家出台了大量政策文件以期鼓励、引导公共数据的开发利用，其中最为重要的政策文件系《数据二十条》与《关于加快公共数据资源开发利用的意见》（以下简称“《开发利用意

※ 本章作者段志超律师，汉坤律师事务所合伙人，长期专注数据合规与跨境传输，深谙中外监管框架，服务多家头部跨国企业与科技公司；王雨婷，北京市汉坤律师事务所顾问。

见》”)。

2022 年,《数据二十条》作为首部构建数据基础制度的国家级文件,不仅明确了公共数据的定义、将公共数据正式列为三大数据要素之一,并且也首次规定了公共数据的授权机制、共享开发等相关事宜。

2024 年,《开发利用意见》则从 17 个方面提出了加快公共数据开发利用的具体措施,明确了公共数据共享、开放和授权运营的三种开发利用方式,作为中央层面首次针对公共数据资源开发利用进行系统部署的政策文件,在公共数据开发利用中具有领航性作用。

(二)公共数据的界定与识别

1.国家层面的定义

“公共数据”首次在国家层面的法律法规中作为独立概念出现系《网安法》,但该法仅体现立法者对公共数据资源开放的肯定态度,并未具体界定公共数据的概念。同样地,《电子商务法》也仅提及此概念,并未规定具体定义。

早期,在国家层面的立法中并未明确区分政务数据与公共数据,对前述两个概念的使用常常相互关联,甚至可以彼此替换。例如,2021 年,《数安法》中专章规定了政务数据安全与开放,其中虽未直接规定政务数据的概念,但从第 38 条的文义解释出发[17],

17 《数安法》第 38 条:“国家机关为履行法定职责的需要收集、使用数据,应当在其履行法定职责的范围内依照法律、行政法规规定的条件和程序进行;对在履行职责中知悉的个人隐私、个人信息、商业秘密、保密商务信息

可以理解政务数据是指国家机关为履行法定职责的需要收集、使用的数据。并且，第 43 条还拓宽了政务数据的范围[18]，使政务数据的概念有了与公共数据接轨的可能性，明确了具有管理公共事务职能的组织为履行职责中处理的数据适用该专章的规定。同样，在 2022 年国务院办公厅印发的《全国一体化政务大数据体系建设指南》中，公共数据仍然作为广义的政务数据概念被使用。这种政务数据与公共数据概念的混用一直延续到了《数据二十条》的发布。

《数据二十条》首次从国家层面将公共数据定义为：**“各级党政机关、企事业单位依法履职或提供公共服务过程中产生的数据”**，正式将政务数据囊括进了公共数据的范畴之中，并且明确企事业单位也在主体之中。

2024 年 12 月 30 日，国家数据局公布的《数据领域常用名词解释（第一批）》第 15 条吸收了该种界定[19]，以期进一步统一社会对公共数据定义的认识。

2.地方层面的定义

在顶层政策支持公共数据开发利用的背景下，全国各省市诸如北京、上海、广东等地纷纷出台大量以探索推动公共数据开发利

等数据应当依法予以保密，不得泄露或者非法向他人提供。

18 《数安法》第 43 条：“法律、法规授权的具有管理公共事务职能的组织为履行法定职责开展数据处理活动，适用本章规定。

19 《数据领域常用名词解释（第一批）》第 15 条：“公共数据，是指各级党政机关、企事业单位依法履职或提供公共服务过程中产生的数据。

用为主题的法律法规，其中同样对公共数据进行了定义。总的来看，各地基本均通过“主体”+“行为”的要件模式对公共数据作出定义，行为要件均规定为“依法履行公共事务管理职责或提供公共服务过程中”，主体要件则随各地情况不同而略有差异。随着国家将公共数据相关定义、发展方向等从政策层面上升到法律层面，公共数据的定义终得以统一。

在主体要件层面，绝大多数地方法规均将国家机关和获得授权承担公共职能的组织作为公共数据主体，但在事业单位、提供公共服务的企业组织是否属于主体范围上，各地规定均考虑到了地方企业、组织的具体情况作出了差异性规定。例如，北京并未将事业单位、公共服务组织纳入主体范围[20]，上海采取具体列举的方式，明确事业单位、提供供水、供电等基础公共服务的组织为公共数据主体[21]，江苏则直接概括性地将具有公共服务职能的企事业单位均规定为公共数据主体[22]。

---

20 《北京市公共数据专区授权运营管理办法（试行）》第 2 条：“本办法所称公共数据是指本市各级国家机关、经依法授权具有管理公共事务职能的组织在履行职责和提供公共服务过程中处理的各类数据。

21 《上海市公共数据开放实施细则》第 3 条：“本细则所称公共数据，是指本市国家机关、事业单位，经依法授权具有管理公共事务职能的组织，以及供水、供电、供气、公共交通等提供公共服务的组织（以下统称公共管理和服务机构），在履行公共管理和服务职责过程中收集和产生的数据。

22 《江苏省公共数据管理办法》第 2 条：“本办法所称公共数据，是指本省各级行政机关、法律法规授权的具有管理公共事务职能的组织、公共企事业单位（以下统称公共管理和服务机构）为履行法定职责、提供公共服务收集、产生的，以电子或者其他方式对具有公共使用价值的信息的记录。

3.公共数据的识别方法

从前述政策法规的定义梳理中可以发现，公共数据的核心识别要素即“主体”、与“行为”两个要件，由于行为要素基本固定，企业在具体识别时应重点关注主体要素，最为广泛的范围包括行政机关、事业单位、公共职能组织、公共服务组织。由于各地区在主体要素上根据地区特色作了因地制宜的细化与调整，企业同样也需具体参照当地法律法规逐一判断，从而实现精准识别。

- 在识别过程中应先进行主体性质核查，若主体完全不属于地方规定的主体范围内，则应将该数据排除于公共数据之外;
- 若主体性质符合，则判定行为性质，综合考量数据生成场景是否落入前述主体日常办公、对外服务、执法监管等履行职责的范围，行为是否具备法律授权等因素;
- 最后有必要核查属地主管部门公开的公共数据目录，因为可能会出现某类数据虽不满足主体或行为要素，但被明确纳入某地方的公共数据目录之中的情况。例如在无锡市公开的公共数据中包括“二级民营医院总体概况”[23]，民营医院一般并不属于《无锡市公共数据管理办法》规定的行政机关以及履行公共管理和服务职能的企业、事业单位和社会组织，但其产生的数据仍然被纳入了公共数据目录之中。

（三）公共数据共享与开放

23 参见无锡市公共数据开放平台。

如前述，《开发利用意见》第 2 条中明确了公共数据的三种开发利用方式，包括共享、开放与授权运营。这三种方式虽然在适用对象、实施主体和应用场景上存在差异，但本质上都是我国在严格保障数据安全的基础上，通过创新公共数据开发利用路径，实现数据资源高效供给与价值释放的实践探索。准确认知、深入理解这三种方式，并切实关注、严格遵循其中的合规要点，是企业有效、合法且充分地挖掘与利用公共数据价值的关键所在。

1.公共数据共享

公共数据共享是各层级、地区政府部门之间打通数据壁垒，进行数据交换的重要方式。早在 2016 年，《政务信息资源共享管理暂行办法》便提出了政务数据“以共享为原则、不共享为例外”的原则，直至今日，公共数据共享仍然是公共数据开发利用的重要途径，可以提高政府内部协同监管能力，最终改善公共服务水平。

公共数据共享依赖政府部门编写公共数据目录并主导相关数据的归集、共享工作。以上海市公共数据共享的工作机制为例，根据《上海市公共数据共享实施办法（试行）》，公共数据共享的工作部门主要包括市政府办公厅、市大数据中心、市级责任部门与区公共数据主管部门，建立起了从上到下的部门责任体系，重点工作为编制、归集、共享公共数据目录。共享机制的实现依赖于大数据资源平台，其余各地各级行政部门需要使用共享数据的，需在该平台上提交申请并作出需求承诺，后续使用也许在限定在承诺范围内，不得应用于其他场景和目的。

2.公共数据开放

不同于公共数据共享，公共数据开放主要面对的对象是企业和社会公众，以保障企业和社会公众获取和利用公共数据的权利为目标，故而其对企业产生的积极意义也更为直接。

一般而言，公共数据开放的重点范围是与公共安全、民生保障、企业公共信用信息等相关的数据。根据敏感程度，各地法规通常将公共数据开放划分为不予开放类、有条件开放类与无条件开放类，公共数据开放主体可根据公共数据分类分级相关规则以确定开放属性。

以《广东省公共数据开放暂行办法》为例，不予开放的公共数据主要为涉及国家秘密、开放会影响国家社会安全、会侵犯商业秘密、个人隐私、知识产权等的数据；有条件开放类则主要包括数据主体同意开放的涉及商业秘密和个人隐私的数据、无条件开放会影响公共数据处理运行效率、具有显著经济效益但具有安全风险的数据；不予开放类和有条件开放类以外的数据则为无条件开放类数据。

在开放机制上，各公共数据持有主体按照法律法规规定，在该地区公共数据目录范围内编制公共数据开放清单、将公共数据录入数据开放平台后，对于无条件开放的公共数据，企业和社会公众可以通过数据下载、接口调用等法律法规规定方式查询、获取、利用开放的公共数据；对于有条件开放类的公共数据需提交申请通过审核后，与数据开放主体签订数据利用协议后方可获取使用。

此外，对于尚未开放的公共数据，企业和社会公众还可以在数据开放平台中向有关政府单位提出数据需求，例如，在深圳市政府

数据开放平台中，用户可以通过填写数据需求内容、应用场景等以提交个性化的公共数据开放需求[24]。

3.企业参与公共数据共享开放的合规要点

（1）针对拟公开数据进行脱敏脱密处理

涉及提供公共服务的国企，在接触到涉及国家秘密、商业秘密、个人信息的数据时，需进行依法脱密、脱敏处理或取得相关权利人同意才可进行开放以及加工处理。其余企业获取到的公共数据资源中涉及到相关数据的，也必须遵守商业秘密保护与个人信息保护相关的规定。

以个人信息保护为例，实践中曾出现转载包含个人信息的公开判决书而被认为侵犯个人权益的案例。在伊某与江苏苏州某公司侵犯个人信息权纠纷案中[25]，被告系向社会提供裁判文书查询的企业，运营网站中的裁判文书信息均转载自中国裁判文书网中的合法公开信息，但原告主张此种转载行为系未经其同意而对其个人信息的二次公开，侵犯了其个人信息权。法院认为此案中，个人信息主体对其已经合法公开的个人信息具有传播控制权、企业对已公开个人信息的再处理不得侵害其选择自由以及个人信息主体对信息传播控制的人格权益高于已经合法公开的个人信息流通所产生的潜在财产权益，最终判决被告企业删除相关判决文书并赔偿原告 8000 元经济损失。

---

24 参见深圳市政府数据开放平台公共数据开放需求及应用场景征集表。

25 参见江苏省苏州市中级人民法院(2019)苏 05 民终 4745 号民事判决书。

（2）以合法方式获取公共数据

在获取公共数据环节，目前，地方法规层面仅提出了不得损害国家利益、社会利益和其他主体的合法权益的原则要求，《上海市公共数据开放实施细则》第 32 条则明确禁止企业采用非法手段获取公共数据、侵犯商业秘密、个人隐私等他人合法权益或以其他违法违规开发利用公共数据[26]。

其中需要特别关注，在公共数据获取手段上，对于无条件开放的公共数据，企业并非可以以任意方式获取，需要具体参考各地有关公共数据开放法规与公共数据开放平台的规定，避免不当使用网络爬虫等自动化工具。

例如，《广东省公共数据开放暂行办法》第 22 条规定了企业获取公共数据的合法方式，包括数据下载、接口调用数据、通过数据开放平台以算法模型获取结果数据、存储介质传递数据、法律法规规章规定的其他方式。规定中并不包含目前实践中许多企业常常借助的网络爬虫等自动化手段。尽管我国法律法规中也并未一刀切地禁止网络爬虫活动，但《反不正当竞争法》《网数条例》《刑法》等法律法规均对该类活动进行了限制。如《网数条例》第 18 条要求网络数据处理者评估自动化工具对网络服务带来的影响。企业必须谨慎考虑使用此等自动化手段时可能带来的诸如不正当

26 《上海市公共数据开放实施细则》第 32 条：“（一）违反开放平台管理制度；（二）采用非法手段获取公共数据；（三）侵犯商业秘密、个人隐私等他人合法权益；（四）超出数据利用协议限制的应用场景使用公共数据；（五）违反法律、法规、规章和数据利用协议的其他行为。”

竞争、行政处罚、甚至构成非法侵入计算机信息系统罪、非法获取计算机信息系统数据罪等合规风险。

（3）采取必要措施保障数据质量

企业在开发利用公共数据的过程中，不能仅因为公共数据的公开属性而不履行合理范围内的注意义务，若无法保障所利用公共数据的准确性、时效性，不仅会导致公共数据的开发利用效益降低，而且也存在引发侵权风险的可能性。尤其当公共数据中涉及可能影响他人权益的重大负面敏感信息时，应当进行核查，以确保所开发利用的公共数据准确无误。

例如，在苏州朗动网络科技有限公司与浙江蚂蚁小微金融服务集团股份有限公司等商业诋毁及不正当竞争纠纷一案中，被告由于未核查从国家企业信用公示系统中获取到的企业清算信息时效性，在其经营的网站平台中多次向用户推送错误的原告清算变更信息通知，导致公众将原告的历史清算信息误认为 2019 年的即时信息，对原告造成了商誉损失，被法院认为构成不正当竞争，并被判处赔偿原告损失及合理费用共 60 万元[27]。

4.公共数据授权运营

授权运营作为第三种开发利用方式，通常指专业性的运营机构基于授权针对非原始公共数据进行开发利用，为市场主体提供数据产品和服务的活动。其旨在引入社会专业力量对数据资源进行加工使用，从而实现数据资源价值的充分释放。相较公共数据共

27 参见浙江省杭州市中级人民法院(2020)浙 01 民终 4847 号民事判决书。

享与开放，授权运营起步较晚，是在共享与开放基础上，作为解决部分敏感性较高的高价值公共数据价值闲置问题的补充渠道而产生。

2025 年以来，在《开发利用意见》的基础上，国家出台了《公共数据资源授权运营实施规范（试行）》（以下简称“《实施规范》”）《公共数据资源登记管理暂行办法》《关于建立公共数据资源授权运营价格形成机制的通知》，形成了“1+3”的政策规则体系，为高效合规的公共数据授权运营提供了法规基础。

（1）公共数据授权运营概述

a)参与主体

公共数据授权运营中主要涉及到三类主体，即授权主体、实施机构、运营机构。

针对授权主体，《实施规范》规定其范围主要包括县级以上地方各级人民政府、国家行业主管部门。除此以外，在附则第 25 条中说明了中央党群机关、县级以上各级地方党委、供水、供气、供热、供电、公共交通等公用企业可以参考适用。

根据《实施规范》，实施机构指由县级以上地方各级人民政府或国家行业主管部门确定的、具体负责开展授权运营活动的单位，职责主要包括编制实施方案、公平选择运营机构、签订授权运营协议、对运营机构进行内控审计等。

而运营机构则指按照《实施规范》获得授权，具体对公共数据资源进行开发运营的法人组织。换言之，私营企业通常作为运营机构参与到公共数据授权运营之中。

b)授权模式

《开发利用意见》则对授权模式进行了归纳总结，总体分为整体授权模式、分领域授权与依场景授权模式[28]。

- 整体授权模式指的是 1 对 1 授权或综合授权模式，即在地方数据主管部门统筹下，将跨部门的公共数据资源整体授权给运营机构进行开发利用，成都市的公共数据授权运营便为此模式[29]；
- 分领域授权模式则指按照行业或领域进行 1 对 N 授权，根据不同行业或领域的数据特点、应用需求情况，选择具备行业属性的运营机构进行特定领域应用场景的开发。典型如《北京市公共数据专区授权运营管理办法（试行）》中规定的授权模式[30]；

---

28 《开发利用意见》第 2 条第 3 项："（三）鼓励探索公共数据授权运营。落实数据产权结构性分置制度要求，探索建立公共数据分类分级授权机制。加强对授权运营工作的统筹管理，明确数据管理机构，探索将授权运营纳入"三重一大"决策范围，明确授权条件、运营模式、运营期限、退出机制和安全管理责任，**结合实际采用整体授权、分领域授权、依场景授权等模式**，授权符合条件的运营机构开展公共数据资源开发、产品经营和技术服务。数据管理机构要履行行业监管职责，指导监督运营机构依法依规经营。运营机构要落实授权要求，规范运营行为，面向市场公平提供服务，严禁未经授权超范围使用数据。加快形成权责清晰、部省协同的授权运营格局。适时制定公共数据资源授权运营管理规定。"

29 成都市公共数据运营服务平台官网介绍。

30 《北京市公共数据专区授权运营管理办法（试行）》第 3 条第 1 款："本办法所称公共数据专区是指针对重大领域、重点区域或特定场景，为推动公共数据的多源融合及社会化开发利用、释放数据要素价值而建设的各类专题

- 依场景授权模式即根据具体需求，由不同运营机构遵循“一场景一申请一审批”的原则开展资源的开发利用，实践中的道路信号灯优化、信用风险预警等都是典型此授权模式下的开发应用场景[31]。

需要指出，此三种授权模式并非完全独立存在，各地区往往结合不同模式的优势灵活建立运营体系。例如，南京市、济南市采取了整体授权与分领域授权并行的发展模式，以期形成良好协同合作效果。[32]

c)数据流转链路

从流转链路来看，典型的授权运营运作方式为授权主体汇聚收集产生的公共数据，并可能借由地方数据授权运营平台进行数据清洗。随后实施机构按照规定编制公共数据资源授权运营实施方案，并按照该方案通过公开招标等方式选择运营机构。经过审议后，与选定运营机构签订授权运营协议，运营机构从而可以将公共数据加工处理形成公共数据产品和服务，在各地数据交易中心上架，最终得以向数据交易相对方流通。

（2）企业参与授权运营的合规要点

《开发利用意见》中明确提出将公共数据授权运营纳入“三重

数据区域的统称，一般分为领域类、区域类及综合基础类。”

31 参见孟庆国、王友奎、王理达:《公共数据开放利用与授权运营——内涵、模式与机制方法》，载《中国行政管理》2024 年第 9 期。

32 参见大数据技术标准推进委员会《公共数据授权运营发展洞察（2024 年）》。

一大”决策范围[33]，这不仅体现了国家对公共数据授权运营的重视，也表明了公共数据授权运营可能影响到国家数据安全和公共利益，故而所有相关主体必须确保全过程合法合规，以保障数据安全与个人信息安全，《实施规范》第二章也对授权运营的基本要求作出了相似规定，并额外强调了开展授权运营活动不得实施垄断行为[34]。

如前所述，私营主体通常以运营机构的身份参与公共数据授权运营。对于运营机构而言，其义务主要包括符合运营主体条件、进行公共数据产品或服务登记、公开公共数据产品和服务清单与披露相关信息接受社会监督、履行数据安全主体责任、通过管理和技术措施保障数据安全、加强公共数据相关财务管理等。

故而，从《实施规范》基本要求与前述义务设置来看，需关注如下合规要点：

（3）履行个人信息保护义务

由于公共数据中可能涉及到个人信息，故而运营机构在进行开发利用时也应当注重遵守个人信息保护的相关合规要求，履行合规义务，详见前文“3.企业参与公共数据共享开放的合规要点”中“（1）针对拟公开数据进行脱敏脱密处理”。

（4）落实数据安全保护要求

33 “三重一大”：重大事项决策、重要干部任免、重大项目投资决策、大额资金使用。

34 《实施规范》第6条第1款：“开展授权运营活动，不得滥用行政权力或市场支配地位排除、限制竞争，不得利用数据和算法、技术、资本优势等从事垄断行为。”

首先在协议签订阶段，根据《实施规范》，企业应具备实施方案中要求的数据安全能力才能够被选定为运营机构，故而如果企业想要参与授权运营，需确保具备基础数据安全能力。

到了运营管理阶段，运营机构应当履行诸如加强内控管理、保障自身始终具备相关数据安全能力、按照相关法规规定与运营协议约定落实数据安全、个人信息保护要求和风险监测、应急处置措施等数据安全保护义务，并且必须在授权范围内使用公共数据资源，严格防控数据处理、运营、服务等环节的数据安全风险。

最后需强调，《实施规范》第 21 条第 2 款要求运营机构履行数据安全主体责任，该责任系一种主动合规责任，要求运营机构充分开展更为充分全面的合规自证明工作。并且，由于实施机构对运营机构具有监督审计权，从此方面而言，运营机构也需要落实数据安全保护措施以顺利配合相关审计工作。

（5）避免涉嫌构成垄断运营

《实施规范》针对公共数据运营的垄断风险特别提出了：“运营机构应当按照协议在授权范围内开展业务，不得直接或间接对相关公共数据产品服务进行再开发”。

这一规定的核心目的在于防止运营机构滥用其获得的公共数据资源，限制其他市场主体参与公共数据的开发利用，从而避免形成市场垄断。故而，为防范垄断风险，企业需确保在公共数数据运营过程中，不通过技术壁垒、排他性协议、限制再开发等手段阻碍市场竞争，维护市场公平性和开放性。

5.公共数据开发利用的未来展望

随着国家层面统一政策制度与地方具体法律规范的不断完善，我国已逐渐解决了此前无统一专门性法规、无具体配套实施规范的问题，公共数据开发利用正式迈入了“有章可循、有规可依、有据可查”的全新阶段。但也需要指出，由于目前公共数据共享、开发、授权运营的相关制度和信息披露机制仍处在初步构建阶段，具体细节与执行标准有待细化，下一步各地方各行业将根据实际情况规划实施路径、形成落地方案，并探索标准的全流程规范制度体系。

此外，尽管各地方也积极开展了诸多公共数据开发利用的具体实践探索，但目前应用场景较为集中于金融、医疗、交通等领域，公共数据产品种类不够丰富，开发利用面临着“持有数据不会用”、“想用数据找不到”的困境。未来工作将进一步优化对公共数据应用需求的判断和响应，建立良好供需对接渠道。另外，国家数据局将协同推动重点领域先行突破，打造一批有影响力的项目、形成可复制可推广的开发利用模式。

总而言之，共享、开发、授权运营有效促进了公共数据资源的开发利用，从而推进了数据要素的市场建设。未来，各地区部门的相关探索将进一步深化，并且随着更多专业、灵活、多元的企业社会力量的引入，公共数据价值潜能将得到进一步释放。

6.政策法规索引

效力范围	规范名称	公布时间	生效时间
国家	《国务院关于积极推进“互联网+”行动的指导意见》	2015.7.1	2015.7.1

效力范围	规范名称	公布时间	生效时间
	《促进大数据发展行动纲要》	2015.8.31	2015.8.31
	《政务信息资源共享管理暂行办法》	2016.9.5	2016.9.5
	《全国一体化政务大数据体系建设指南》	2022.9.13	2022.9.13
	《关于构建数据基础制度更好发挥数据要素作用的意见》	2022.12.2	2022.12.2
	《中共中央办公厅、国务院办公厅关于加快公共数据资源开发利用的意见》	2024.9.21	2024.9.21
	《数据领域常用名词解释（第一批）》	2024.12.30	2024.12.30
	《公共数据资源授权运营实施规范（试行）》	2025.1.8	2025.3.1
	《公共数据资源登记管理暂行办法》	2025.1.8	2025.3.1
	《关于建立公共数据资源授权运营价格形成机制的通知》	2025.1.16	2025.3.1
北京	《北京市公共数据专区授权运营管理办法（试行）》	2023.12.5	2023.12.5
上海	《上海市公共数据开放实施细则》	2022.12.31	2022.12.31

效力范围	规范名称	公布时间	生效时间
	《上海市公共数据共享实施办法(试行)》	2023.3.2	2023.3.2
江苏	《江苏省公共数据管理办法》	2021.12.18	2022.2.1
	《无锡市公共数据管理办法》	2020.2.26	2020.5.2
广东	《广东省公共数据开放暂行办法》	2022.11.30	2022.11.30

五、特殊行业数据※

当前，我国已构建起以《网安法》《数安法》《个保法》为核心的数据合规法律框架，确立了数据全生命周期管理、分类分级、风险评估等基础性制度。由于特殊行业数据因其承载的国家安全属性、公共利益关联度及敏感性，需在统一立法框架下特别遵循特殊的合规义务。

特殊行业数据的合规治理具有显著的溢出效应。例如，测绘地理信息数据作为国家主权的数字化映射，其精度与安全性影响国家安全；气象数据作为公共安全的核心资源，与保障防灾减灾的公益性需求密切相关；金融数据则构成金融体系的数字基础，其合规性直接关系金融稳定与金融机构的公信力；电商营销数据则涉及消费者权益保护与市场公平竞争秩序。此外，医疗健康数据因关联公民生命权与健康权，受行业主管部门和数据主管部门的双重监

※ 本章作者孟洁，北京环球律师事务所合伙人；林奕，北京环球（成都）律师事务所顾问。

管；工业制造数据关乎产业竞争力与关键基础设施安全，需依据《工业和信息化领域数据安全管理办法（试行）》实施全流程管控；应急管理数据作为公共安全应急响应的支撑，需在《中华人民共和国突发事件应对法》（以下简称“《突发事件应对法》”）框架下建立数据采集、共享与使用的特殊规则。

上述典型行业的合规需求，既体现了数据合规基础法律法规的共性要求，又凸显了差异化监管的必要性。由于测绘地理信息、气象数据、金融征信数据、电商营销数据分别对应国家安全、公共安全、金融安全、消费安全四个维度，下文将重点聚焦上述四类特殊行业数据，为相关企业的数据合规管理提供指引。

（一）测绘地理信息数据

1.测绘地理信息数据的定义

《中华人民共和国测绘法》（以下简称“《测绘法》”）未对测绘地理信息数据作出明确定义，仅在第二条规定，测绘活动是指“对自然地理要素或者地表人工设施的形状、大小、空间位置及其属性等进行测定、采集、表述，以及对获取的数据、信息、成果进行处理和提供的活动”。随着智能网联汽车的快速发展，自然资源部于 2022 年及 2024 年先后发布了《关于促进智能网联汽车发展维护测绘地理信息安全的通知》（以下简称“2022 年《通知》”）与《关于加强智能网联汽车有关测绘地理信息安全管理的通知》（以下简称“2024 年《通知》”）。2022 年《通知》首次明确“测绘地理信息数据”涵盖“车辆及周边道路设施空间坐标、影像、点云及其属性信息等”，2024 年《通知》进一步细化了实景影像数据（包含视

频和影像等环境感知数据），并扩展至道路拓扑数据，凸显智能网联场景下动态数据的监管需求。

2.数据处理活动的主体准入

（1）资质等级

我国对从事测绘活动的单位实行行政许可制度，测绘主体须具备相应测绘资质后方可开展测绘活动。根据《测绘法》第二十七条规定，从事测绘活动的单位应当具备相应条件，并依法取得测绘资质证书，方可从事测绘活动。

测绘资质的专业类别分为大地测量、测绘航空摄影、摄影测量与遥感、工程测量、海洋测绘、界线与不动产测绘、地理信息系统工程、地图编制、导航电子地图制作、互联网地图服务。自然资源部发布的《测绘资质管理办法》和《测绘资质分类分级标准》压减了资质类别等级，将测绘资质等级进行了较大幅度整合，由四级减少为甲、乙两级。

甲级测绘资质全国范围适用，由自然资源部审批；乙级测绘资质限定业务范围和区域，由省级主管部门审批，例如在相关政府部门划定的自动驾驶区域内从事导航电子地图制作等。此外，2024 年《通知》第二条强化智能网联汽车场景资质要求，明确数据收集、存储、传输等环节必须由具有导航电子地图制作等测绘资质的单位承担，第五条进一步规定，对于用于导航相关活动以及地图制作、更新的地理信息数据，应当直接传输至具备导航电子地图制作测绘资质的单位管理，无资质企业不得接触此类数据。

（2）主体类型

根据《外国的组织或者个人来华测绘管理暂行办法》，外资准入遵循“有限开放”原则，外国组织或个人须通过合资、合作形式在中国境内开展测绘活动，且不得从事导航电子地图编制、大地测量、海洋测绘、测绘航空摄影、行政区域界线测绘等关键业务。外国的组织或者个人需进行一次性测绘活动的，可不设合资、合作企业，但必须经自然资源部会同军队测绘主管部门批准，并与中国的有关部门和单位的测绘人员共同进行。同时，2022 年《通知》亦规定，内资企业则需依法取得相应测绘资质或委托具有相应测绘资质的单位开展相应测绘活动。

（3）数据处理活动的特殊合规要求

a)**本地化存储**

根据 2024 年《通知》第五条的规定，地理信息数据应当在中国境内本地化存储，不得直接将其传输至境外服务器；并且企业所使用的存储设备、网络和云服务等还须符合国家有关安全和保密要求。

b)**跨境传输**

如相关数据落入《数据分类分级规则》附录 G 中 b）款及 e[35]）款及《汽车数据安全管理若干规定（试行）》中“重要敏感区域的地理信息”“包含人脸信息、车牌信息等的车外视频、图像数据”及“其他可能危害国家安全、公共利益或者个人、组织合法权益的数据”

35 可被其他国家或组织利用发起对我国的军事打击，或反映我国战略储备、应急动员、作战等能力，如满足一定精度指标的地理数据或与战略物资产能、储备最有关的数据。

的范围内[36],则可能被认定为属于重要数据。相关企业应当依据《数据出境安全评估办法》《跨境新规》等法律法规的要求，结合行业内公开发布的重要数据目录及测绘主管部门对于重要数据的告知，同时申请向境外提供地理信息数据的，必须严格履行对外提供审批或地图审核程序，并落实数据出境安全评估等有关规定。

（4）涉密测绘数据的合规义务

根据《测绘地理信息管理工作国家秘密范围的规定》附件《测绘地理信息管理工作国家秘密目录》的规定，军事禁区以外平面精度优于（含）10 米或地物高度相对量测精度优于（含）5%、且连续覆盖范围超过 25 平方千米的三维模型、点云、倾斜影像、实景影像、导航电子地图等实测成果被认定为国家秘密。

此外，参考《测绘法》第三十四条、《中华人民共和国测绘成果管理条例》第十八条的规定，企业不得擅自向境外提供涉密测绘成果，在对外提供此类数据前，应当按照国务院和中央军事委员会规定的审批程序，报国务院测绘行政主管部门或者省、自治区、直辖市人民政府测绘行政主管部门审批；测绘行政主管部门在审批前，应当征求军队有关部门的意见。

（二）气象数据

1.数据定义及分类

---

36 反映重点目标、重要场所物理安全保护情况或未公开地理目标的位置,可被恐怖分子、犯罪分子利用实施破坏,如描述重点安保单位、重要生产企业、国家重要资产(如铁路、输油管道)的施工图、内部结构、安防情况的数据。

根据《气象数据管理办法（试行）》第三条的规定，气象数据是指通过观测监测、考察调查、收集交换、科学研究、试验开发、生产分析、授权管理等方式，获得的大气和空间天气科学技术领域的数字、文字、符号、图片和视音频等。并且，按照数据产生方式的不同，气象数据可分为原始数据和产品数据[37]。这种二分法为企业合规管理提供了基础框架，原始数据因直接反映自然现象，需重点管控采集环节；产品数据因包含加工分析内容，其使用场景与合规要求更为丰富。

2.数据处理过程中的特殊合规义务

（1）数据收集

根据《气象法》第三章的规定，气象数据采集实行严格准入制度。气象数据采集/气象资料探测须由具备相应资质的气象台站进行，且应遵守国家统一的气象技术标准、规范和规程。若企业拟通过建站方式收集气象数据，应当取得气象专用技术装备的有效许可[38]并向气象主管机构备案[39]，且不得擅自在国防及军事设施、军事敏感区域、尚未对外开放地区和其他涉及国家安全的区域设立气象探测站（点）；若企业通过气象主管机构及其下属单位或企业共享的方式获取气象数据，根据《气象数据共享服务与安全管理办

37 原始数据是指在观测监测、考察调查、科学研究、试验开发过程中得到的原始记录，以及格式改变、质量控制、数据插补、单位换算、量度变换、统计计算、汇编整编等得到的，未经加工处理的数据。

38 参照《气象专用技术装备使用许可管理办法》第五条的规定。

39 参照《气象信息服务管理办法》第十五条的规定。

法（试行）》第二章的规定，企业应当接受安全审查和监督管理、签订涉及数据共享服务的合作协议。

（2）数据存储

对于通过共享方式从各级气象主管机构处获取的气象数据，企业应遵守《气象资料共享管理办法》第十四条的要求，将该部分数据限制在内部使用。在分发数据时，可以存放在仅供本单位使用的局域网上，但不得与广域网、互联网相连接。相关企业应建立完善且严格的数据访问与存储制度，明确内部各部门及人员对气象数据的使用权限，对局域网的网络架构和安全防护措施进行定期检查与维护，防止因网络配置失误或遭受外部攻击而导致数据外流。

（3）数据使用

就各类气象数据，《气象数据管理办法（试行）》第二十条禁止任何单位和个人未经允许将所获取的气象数据以转发、转让、出售等方式对外披露，或用于气象业务、科研开发以外的其他用途。同时，根据《气象数据共享服务与安全管理办法（试行）》第三十一条以及《气象资料共享管理办法》第三章的规定，通过共享方式获得气象资料的，企业应当合法使用气象数据，落实气象数据服务协议约定的安全保障措施、不得未经同意超出气象数据服务协议约定的范围使用数据、不得出于获取国家秘密、商业秘密或者个人隐私目的，挖掘气象数据、不得危及公共气象服务安全。并且，企业仅享有气象资料有限的、不排他的使用权，不得有偿或无偿转让其从各级气象主管机构获得的气象资料。相关企业在业务开展过程

中如涉及气象数据，必须严格遵守上述规定。

（4）数据出境

根据《涉外气象探测和资料管理办法》第五条规定，任何组织和个人严禁向未经批准的外国组织或个人提供气象资料，并且不得将涉及国家秘密的气象资料以任何方式提供给外国组织或者个人。因此，在企业在与境外主体建立合作关系时，如涉及跨境传输气象数据，应履行严格的审批核查流程，确保接收方获得批准，以保证合规运营。参照《气象部门保守国家秘密实施细则》第十七条的规定，气象数据的境外传输应根据涉密级别的不同，履行分级审批手续，具体如下表所示：

级别	审批要求
绝密级	由主办单位报省（自治区、直辖市）气象局或国家气象局，经国家气象局有关职能机构审核，国家气象局保密委员会审查批准，报国家保密局备案。
机密、秘密级	由主办单位报省（自治区、直辖市）气象局或国家气象局，经国家气象局有关职能机构审核，报国家气象局保密委员会审查批准。
内部	由主办单位报省、（自治区、直辖市）气象局或国家气象局有关职能机构审查批准。
公开	由主办单位与地（市）、县气象局或国家气象局和省（自治区、直辖市）气象局处级单位协商解决。

其次，如向境外组织或个人提供的气象数据属于重要数据的，还应履行安全评估义务。需要提醒企业注意的是，《中国（天津）

自由贸易试验区数据出境管理清单（负面清单）（2024 年版）》列明，对于向境外组织或个人提供服务军事、国防科研、高科技领域的各类气象监测数据、灾害防御数据等[40]，除已由气象等相关部门公开发布的数据外，应履行数据安全评估义务。因此，建议自贸区内的企业密切关注所在自贸区最新出台的负面清单，建立清单动态跟踪机制，及时掌握政策变化要点。在开展气象数据跨境传输业务前，依据负面清单逐一核对拟传输的数据，判断是否落入受限范围。

值得注意的是，中国气象局在 2025 年 2 月 18 日表示，其将持续加强与国家数据局合作，加快出台气象数据授权运营、合规管理等数据基础制度，为气象数据的使用和流通提供保障。我们建议企业密切关注政策变化动态，从而做好合规规划，有效防范潜在的数据合规风险。

（三）金融征信数据

1.数据定义

金融数据是金融业机构开展业务、提供服务及日常经营管理的基础，涵盖银行、保险、证券、征信等多个领域[41]。其中，个人

---

40 如重大活动气象保障数据、重要敏感区数据、应对气候变化和农作物产量预报预测数据，风云卫星 L0 级数据和遥测数据、雷达基数据、人影地面作业点数据、历史气象档案及衍生数据、气象政务服务数据、气象关键信息基础设施数据等。

41 根据中国人民银行发布的《金融数据安全数据安全分级指南》（JR/T 0197－2020）（以下简称“《数据安全分级指南》”），金融数据是指“金融业机构开展金融业务、提供金融服务以及日常经营管理所需或产生的各类数据”。个

金融信息是金融业机构通过提供金融产品和服务等渠道获取、加工和保存的个人信息。此外，聚焦征信领域，根据《征信业务管理办法》的规定，信用信息被定义为“依法采集，为金融等活动提供服务，用于识别判断企业和个人信用状况的基本信息、借贷信息、其他相关信息，以及基于前述信息形成的分析评价信息”。由于金融征信数据的敏感性及特殊性，其合规管理不仅关乎个人隐私保护，还直接影响金融市场的稳定和金融机构的信誉。

2.数据处理过程中的特殊合规义务

（1）数据收集

根据《金融数据安全数据生命周期安全规范》(JR/T0223-2021)的规定，金融数据采集包括金融业机构从外部机构采集和从个人金融信息主体处采集两种方式。具体而言:

首先，在从外部机构采集数据时，金融机构需通过合同协议等方式明确双方权利义务与采集的具体内容，确保采集经过数据主体授权，避免因未经授权采集数据而引发的法律风险。在数据采集前，需开展数据安全影响评估、对数据采集过程进行日志记录，确保数据采集过程的安全性和数据来源的可追溯性。同时，金融机构要采取必要的技术措施和安全管控措施，确保数据的合规性、完整性和真实性。对于高敏感级别数据的采集，金融机构应满足更严格的加密要求，以防止数据在传输和存储过程中被泄露或篡改。

其次，从个人金融信息主体处采集数据时，除满足上述技术措

人金融信息是指“金融业机构通过提供金融产品和服务或者其他渠道获取、加工和保存的个人信息。”

施、加密要求外，金融机构不应超出用户授权范围采集数据。在停止提供金融产品或服务时，应停止数据收集和分析应用活动，避免对用户造成不必要的干扰和数据风险。

此外，聚焦征信行业，在信用信息采集方面，《征信业管理条例》第十四条要求征信机构在采集个人信用信息前，必须事先取得个人信息主体的明确同意。同时，征信机构不得采集个人的宗教信仰、基因、指纹、血型、疾病和病史信息以及法律、行政法规规定禁止采集的其他个人信息。对于一些敏感信息，如个人的收入、存款、有价证券、商业保险、不动产的信息和纳税数额信息，只有在明确告知信息主体提供这些信息可能产生的不利后果，并取得其书面同意时，方可采集。

（2）数据共享

实践中，为提升金融服务的效率和质量，帮助金融机构更有效地识别风险、评估客户信用状况，金融数据的共享较为常见。提醒金融机构注意的是，针对金融数据的外部共享，除满足《个保法》的一般要求外，还应履行必要的安全控制措施。例如定期对共享的数据进行安全审计、建立应急响应机制，对于特定级别金融数据的共享，还应进行加密处理。

此外，《征信业管理条例》第二十九条规定，从事信贷业务的机构向金融信用信息基础数据库或者其他主体提供信贷信息，应当事先取得信息主体的书面同意。由此可见，由于信贷业务涉及金融风险、资金安全等重要问题，此处的“书面同意”一方面可以让信息主体更加谨慎地对待自己的信贷信息授权，另一方面也便于从

事信贷业务的机构在后续可能出现的法律纠纷等情况中，提供明确的授权依据。

（3）数据出境

鉴于金融数据常包含客户敏感信息和行业关键数据，因此企业应特别考虑出境数据类型、敏感程度等因素，满足相应的出境合规要求。

第一，对于金融行业重要数据的出境，根据《数据安全分级指南》附录 C 中的说明，金融领域的重要数据包括宏观特征数据、海量信息汇聚得到的衍生特征数据、行业监管机构决策和执法过程中的数据，以及 CII 网络安全缺陷信息等。根据《数据出境安全评估办法》《跨境新规》等要求，在相关部门、地区告知或公开发布为重要数据的情况下，数据处理者需履行数据出境安全评估义务。值得注意的是，对于金融行业而言，若相关数据属于在我国境内产生的 5 级数据[42]，则仅能在境内存储，禁止出境。

第二，对于个人金融数据的出境，结合《数据安全分级指南》

42 重要数据，通常主要用于金融业大型或特大型机构、金融交易过程中重要核心节点类机构的关键业务使用，一般针对特定人员公开，且仅为必须知悉的对象访问或使用；数据安全性遭到破坏后，对国家安全造成影响，或对公众权益造成严重影响。

[43]《个人金融信息保护技术规范》（JR/T0171-2020）[44]的规定，在境内收集和产生的个人金融信息，原则上应在境内存储、处理和分析。如确需向境外提供的，相关企业应获得个人金融信息主体的明示同意、开展出境安全评估，并监督境外机构对数据保护的履行。

其中，针对个人信用信息这一特殊类别的数据，根据《征信业管理条例》[45]《征信业务管理办法》[46]的要求，征信机构在中国境

---

43 第 7.1.3（d）条：在中华人民共和国境内提供金融产品或服务过程中收集和产生的个人金融信息，应在境内存储、处理和分析。因业务需要，确需向境外机构（含总公司、母公司或分公司、子公司及其他为完成该业务所必需的关联机构）提供个人金融信息的，应依据国家、行业有关部门制定的办法与标准开展个人金融信息出境安全评估，确保境外机构数据安全保护能力达到国家、行业有关部门与金融业机构的安全要求；应与境外机构通过签订协议、现场核查等方式，明确并监督境外机构有效履行个人金融信息保密、数据删除、案件协查等职责义务。

44 《个人金融信息保护技术规范》第 7 条第 1 款规定，在境内提供金融产品或者服务过程中收集和产生的个人金融信息，应在境内存储、处理和分析。因业务需要，确需向境外机构（含总公司、母公司或者分公司，子公司及其他为完成该业务所必需的关联机构）提供个人金融信息的，具体要求如下：①应符合国家法律法规和行业主管部门有关规定；②应获得个人金融信息主体明示同意；③应依据国家、行业有关部门制定的办法与标准开展个人金融信息出境安全评估，确保境外机构数据安全保护能力达到国家、行业有关部门与金融业机构的安全要求；④应与境外机构通过签订协议、现场核查等方式，明确并监督境外机构有效履行个人金融信息保密、数据删除、案件协查等职责义务。

45 第二十四条　征信机构在中国境内采集的信息的整理、保存和加工，应当在中国境内进行。征信机构向境外组织或者个人提供信息，应当遵守法律、行政法规和国务院征信业监督管理部门的有关规定。

46 第三十九条　征信机构在中华人民共和国境内开展征信业务及其相关活动，采集的企业信用信息和个人信用信息应当存储在中华人民共和国境内。

内采集的信息的整理、保存和加工，原则上也应当在境内存储；如征信机构向境外信息使用者提供企业信用信息查询产品和服务，则应对信息使用者的身份、信用信息用途进行必要的审查，确保信用信息用于跨境贸易、投融资等合理用途，不得危害国家安全。

（四）电商营销数据

1.电商领域法律法规

在电子商务领域，数据合规监管呈现“上位法+专门规章+行业规范”的三维治理体系。《电子商务法》从宏观层面明确电商经营者对消费者个人信息的保护义务；《网络交易监督管理办法》则重点针对网络交易场景，细化了数据收集的原则；《规范促销行为暂行规定》《互联网直播营销信息内容服务管理规定(征求意见稿)》《互联网广告管理办法》等从促销、直播营销、广告等角度对经营者提出相应合规要求。值得注意的是，尽管现行立法未对“电商营销数据”作出明确定义，但结合《电子商务法》对于电子商务[47]概念的界定，此类数据通常包含电商企业通过互联网等信息网络销售商品、提供服务以及开展市场营销活动中收集、产生和使用的各类数据，例如消费者基本信息、消费行为数据、交易数据、商品和服务数据、平台管理数据、广告投放数据。

第四十条　征信机构向境外提供个人信用信息，应当符合法律法规的规定。

征信机构向境外信息使用者提供企业信用信息查询产品和服务，应当对信息使用者的身份、信用信息用途进行必要的审查，确保信用信息用于跨境贸易、投融资等合理用途，不得危害国家安全。

47 《电子商务法》第二条 电子商务是指通过互联网等信息网络销售商品或者提供服务的经营活动。

2.电商营销场景下处理数据的合规要点

（1）数据收集

首先，结合《电子商务法》第二十三条及《个保法》第十七条的要求，电商企业收集消费者数据时，需以清晰、易懂的方式向消费者告知收集的目的、方式、范围以及数据的使用和共享情况。具体要求包括:

a)在用户注册时提供详细的用户协议和隐私政策供用户主动勾选同意，并避免将授权条款嵌套于冗长协议中;

b)对于敏感个人信息及终端权限的调用，采用弹窗、独立页面等显著方式进行单独告知;

c)建立动态告知机制，当数据用途发生变更时需重新获取用户同意。

其次，由于电商营销数据来源广泛，企业对于从第三方合作伙伴处获取的数据，需审查第三方的数据收集和使用是否符合法律法规规定，签订合法有效的数据共享协议，明确双方的数据权利和义务，防止因数据来源问题导致法律风险。

（2）数据存储

由于电商行业涉及大量商品/服务等交易，电商平台负有合规监管义务。因此，为保障电商交易/营销行为的可追溯性，应对可能出现的纠纷、消费者权益受损或监管部门调查等情况，《电子商务法》《网络交易监督管理办法》等明确了相关数据的存储期限。例如商品和服务信息、交易信息应自交易完成之日起存储不少于三年、平台内经营者身份信息自其退出平台之日起存储不少于三

年、平台服务协议和交易规则的全部历史版本应保留修改后的版本生效之日起的前三年。电商平台应关注上述存储期限的要求，留存关键信息，这不仅有助于平台对商家的合规监管，也能在后续涉及商家资质审查、交易行为追溯等事务时，向监管部门提供准确的数据依据。

a)用户行权

《电子商务法》第二十四条规定，电子商务经营者应当明示用户行权的方式、程序，不得设置不合理条件，并应当及时响应和处理。因此，电商企业在开展营销活动时应在平台页面显著位置清晰、明确地向用户展示信息查询、更正、删除以及注销账户的方式和程序，不能以各种借口要求用户提供额外的、与行权无关的信息，也不能以拖延、推诿等方式拒绝用户合理请求。同时，还需遵循最短期限原则存储用户个人信息，在达到数据处理目的后或超出法定保存期限时，应及时删除。

此外，在电商营销场景中，个性化推荐为常见的营销方式。《电子商务法》第十八条明确，电子商务经营者根据消费者的兴趣爱好、消费习惯等特征向其提供商品或者服务的搜索结果的，应当同时向该消费者提供不针对其个人特征的选项。这一规定旨在保障用户的选择权，实践中，“拒绝个性化推送”的按钮应设置在显著位置，操作流程简洁，以确保用户能够方便地行使自身权利。

b)数据出境

为平衡数据流动便利性与安全性，《跨境新规》第五条规定，数据处理者为订立、履行个人作为一方当事人的合同而跨境提供

其个人信息的，属于免予申报安全评估、订立标准合同或通过保护认证的范围，并且，列举了如跨境购物、跨境寄递、跨境汇款、跨境支付等典型的业务场景。电商行业中，交易活动频繁且大多围绕商品或服务的买卖展开，例如在跨境购物中，消费者下单购买境外商品，与境外商家或电商平台订立了买卖合同，为了完成交易，电商平台需要将消费者的姓名、收货地址、联系方式等个人信息跨境提供给境外商家或物流承运商，因此，相关企业的数据跨境行为很可能落入这一豁免场景。

实践中，相关企业应首先判断出境数据是否属于“为订立、履行个人作为一方当事人的合同所必需”，若属于豁免范围则无需履行额外的出境要求；若不属于，则需要根据数据量级和敏感程度，判断是否属于敏感个人信息和重要数据，从而选择对应的合规出境路径。

3.人类遗传资源信息

（1）数据定义

根据《中华人民共和国生物安全法》（以下简称“《生物安全法》”）第八十五条、《中华人民共和国人类遗传资源管理条例》（以下简称“《人遗条例》”）第二条，人类遗传资源信息是指利用人类遗传资源材料产生的数据等信息资料。《人类遗传资源管理条例实施细则》（以下简称“《实施细则》”）则进一步明确，《人遗条例》第二条所称人类遗传资源信息包括利用人类遗传资源材料产生的人类基因、基因组数据等信息资料；不包括临床数据、影像数据、蛋白质数据和代谢数据。

此外，根据国家卫生健康委员会（“国家卫健委”）相关指引[48]，人类遗传资源信息包括人类基因、基因组、转录组、表观组等核酸序列信息，以及与此关联的疾病等信息资料，不包括单纯的临床数据、影像数据、蛋白质数据和代谢数据等。

人类遗传资源信息和人类遗传资源材料同属于人类遗传资源，其采集、保藏、利用和对外提供受到一系列特殊限制。

（2）数据处理过程中的特殊合规义务

a)数据采集、存储、加工利用、对外提供的一般要求

采集、保藏、利用和对外提供人类遗传资源，需遵守以下特殊要求[49]：

- 外国组织、个人及其设立或者实际控制的机构（以下简称“外方单位”）不得在我国境内采集、保藏我国人类遗传资源，不得向境外提供我国人类遗传资源。
- 采集、保藏、利用、对外提供我国人类遗传资源，不得危害我国公众健康、国家安全和社会公共利益。
- 采集、保藏、利用、对外提供我国人类遗传资源，应当符合伦理原则，并按照国家有关规定进行伦理审查。
- 采集、保藏、利用、对外提供我国人类遗传资源，应当尊重人类遗传资源提供者的隐私权，取得其事先知情同意，

48 详见国家卫健委人类遗传资源服务系统《申报指南》：https://zwfw.nhc.gov.cn/bsp/rlyczyfwxt/202405/t20240517_2758.html

49 《人遗条例》第七条至第十条、第十二条。

并保护其合法权益。

- 其中，采集我国人类遗传资源，应当事先告知人类遗传资源提供者采集目的、采集用途、对健康可能产生的影响、个人隐私保护措施及其享有的自愿参与和随时无条件退出的权利，征得人类遗传资源提供者书面同意。在告知人类遗传资源提供者相关信息时，必须全面、完整、真实、准确，不得隐瞒、误导、欺骗。

- 采集、保藏、利用、对外提供我国人类遗传资源，应当遵守国务院卫生健康主管部门制定的技术规范。
- 禁止买卖人类遗传资源（为科学研究依法提供或者使用人类遗传资源并支付或者收取合理成本费用，不视为买卖）。

b)采集、保藏、国际合作的行政许可或备案要求

由于人类遗传资源的高度敏感性，在特定情形下，其采集、保藏与国际合作还适用专门的行政许可或备案要求[50]：

- 采集我国重要遗传家系、特定地区人类遗传资源或者采集国务院卫生健康主管部门规定种类、数量的人类遗传资源的，应当符合特定的条件，并经国务院卫生健康主管部门批准。
- 保藏我国人类遗传资源、为科学研究提供基础平台的，应当符合特定的条件，并经国务院卫生健康主管部门批准。
- 国际科学研究合作行政许可、国际合作临床试验备案应当

50 《人遗条例》第十一条、十四条、二十二条，《实施细则》第四章第一节、第二节。

由中方单位和外方单位共同申请。合作各方应当对申请材料信息的真实性、准确性、完整性作出承诺。

- 申请人类遗传资源国际科学研究合作行政许可，应当通过合作双方各自所在国（地区）的伦理审查。外方单位确无法提供所在国（地区）伦理审查证明材料的，可以提交外方单位认可中方单位伦理审查意见的证明材料。
- 为取得相关药品和医疗器械在我国上市许可，在临床医疗卫生机构利用我国人类遗传资源开展国际合作临床试验、不涉及人类遗传资源材料出境的且符合特定条件的，不需要批准，但应当完成备案。

c)对外提供我国人类遗传资源信息的要求

如上文所述，外方单位对我国人类遗传资源的采集、保藏和对外提供受到严格限制。但在科研和商业实践中，新加坡高校、科研机构、生物医药企业在合法的研究、研发活动中，确有利用人类遗传资源的正当需求。在遵守我国法律法规的前提下，这类需求可以通过与我国科研机构、高等学校、医疗机构、企业（简称“中方单位”[51]）合作的方式进行。

除上文提及的国际合作的行政许可和备案要求外，中方单位还须注意以下对外提供人类遗传资源信息的专门要求[52]：

- 将人类遗传资源信息向外方单位提供或者开放使用的，中

51 根据《实施细则》第十一条，设在港澳的内资实控机构视为中方单位。

52 《生物安全法》第五十七条、《人遗条例》第二十八条，《实施细则》第四章第三节。

方信息所有者应当向国务院卫生健康主管部门备案并提交信息备份。但已取得行政许可的国际科学研究合作或者已完成备案的国际合作临床试验实施过程中，中方单位向外方单位提供合作产生的人类遗传资源信息的，如国际合作协议中已约定由合作双方使用，不需要单独备案和提交信息备份。

- 将人类遗传资源信息向外方单位提供或者开放使用，不得危害我国公众健康、国家安全和社会公共利益；可能影响我国公众健康、国家安全和社会公共利益的，应当通过国务院卫生健康主管部门组织的安全审查。应当进行安全审查的情形包括:（一）重要遗传家系的人类遗传资源信息;（二）特定地区的人类遗传资源信息;（三）人数大于 500 例的外显子组测序、基因组测序信息资源;（四）可能影响我国公众健康、国家安全和社会公共利益的其他情形。

第五章数据跨境流通合规路径※

中国自 2016 年首次在《网安法》中对数据跨境流动提出规定后，不断在相关法律法规中完善数据流通规则。在《网安法》《数安法》《个保法》三部法律的基础上，国家网信办先后在 2022 年至 2024 年期间发布专门针对数据跨境流通的相关规定，包括《数据出境安全评估办法》《个人信息出境标准合同办法》和《跨境新规》等[53]，构建起具有中国特色的数据跨境流通合规体系。

一、数据出境流通的路径选择

（一）按照适用的合规路径完成数据出境安全评估申报、个人信息出境标准合同备案、PIP 认证等工作

1.数据出境安全评估

数据出境安全评估仅面向少数数据出境场景，适用于 CIIO、涉重要数据出境活动，以及涉大量个人信息主体的出境活动。根据国家网信办官方披露，截至 2024 年 12 月，国家网信办共完成安全评估项目 285 个，其中安全评估项目未通过评估的 27 个，占整

※ 本章作者王艺律师，北京市环球（深圳）律师事务所合伙人，执业 12 年，深数所认证数据交易合规师，专注于数据合规领域；史晶源，香港西盟斯律师事务所合伙人，专注于数据和科技法律，为众多国内外企业提供跨法域数据合规、监管合规、公司交易等服务。史律师及其团队被《钱伯斯亚太》及《亚太法律 500 强》评为 TMT 领域领先团队及领先律师（中国，国际律所）；刘嘉颐，北京市环球（深圳）律师事务所主办律师；赖雨晨，香港西盟斯律师事务所；赖衍禹，前西盟斯律师事务所。孟洁、马楷阳、林奕亦有贡献。

53 根据《跨境新规》第 13 条规定，若其与《数据出境安全评估办法》、《个人信息出境标准合同办法》存在不一致的，以《跨境新规》为准。

体比例不到 10%[54]。

安全评估包括企业内部材料准备、省级网信办形式审查、国家网信办实质审查、复评（如需）四个大的阶段。如果企业触发了安全评估要求，需要预留充分的时间准备申报材料以及与监管部门沟通，避免对业务运营活动带来不利影响。

国家网信办已先后发布三版《数据出境安全评估申报指南》，对具体流程和材料要求进行了详细说明，并开通了专门咨询电话为企业答疑解惑。在实践中，我们注意到以下两个方面是监管关注的重点，企业应尤为重视。

首先是个人信息出境的合法性，即是否具备适当的合法依据。根据申报指南，国家网信办要求申报单位在材料中提供履行《个保法》第 39 条的情况说明及佐证材料，包括告知义务和取得个人单独同意（例外情形除外）。因此，企业应当严格审查自身的隐私政策等是否满足了《个保法》第 39 条的披露要求、是否对取得的个人单独同意留有完整记录，以及个人同意的数据出境范围、目的、方式等是否与申报事项一致等。如果未能满足前述条件，应当及时修订隐私政策、取得有效的单独同意，并妥善留存记录。在实践不仅需要关注合规路径的形式要求，更重要的是关注前置的合法依据的构建。例如，有部分企业直到申报安全评估或备案标准合同的时候才发现自己尚未就个人信息出境活动取得相关个人的有效同意，为整体合规工作带来了不必要的波折。另外，值得跨国企业特

54 《关键信息基础设施安全保护条例》第 2 条

别注意的是，取得个人单独同意或具备其他合法依据是合法向境外提供个人信息的先决条件，与完成合规路径是平行的两项法律要求，不能互相替代。这一点也与新加坡等其他国家和地区的监管要求有所区别。

其次是数据出境的必要性。目的限制和数据最小化原则是各国数据隐私法律均秉持的基础性原则，应当贯穿数据处理活动的全生命周期。这意味着在企业运营活动中，应当避免一些仅出于习惯、可有可无的数据跨境流动，将数据出境限定在必要范围内。尤其需要注意的是，企业须在安全评估的申报材料中按字段说明数据出境的必要性，这也要求在内部进行必要性审查时采用较为严格的标准，免遭监管质疑。跨国企业面临的普遍挑战是随着云基础设施和 SaaS 服务的普及，大量企业内部管理系统在集团层面统一部署，使跨境数据流动无可避免。针对这种情况，应当在申报材料中充分说明数据出境活动在商业上的必要性（例如成本、实施集团统一管理等），以及访问权限控制等数据安全措施，以取得监管理解和认可。

此外，适用安全评估的企业应关注评估结果有效期的问题。自评估结果出具之日起计算，通过数据出境安全评估的结果有效期为 3 年。有效期届满，需要继续开展数据出境活动且未发生需要重新申报数据出境安全评估情形的，数据处理者可以在有效期届满前 60 个工作日内通过所在地省级网信部门向国家网信部门提出延长评估结果有效期申请。经国家网信部门批准，可以延长评估结

果有效期 3 年[55]。

而在评估结果有效期内出现以下情形的，数据处理者应当重新申报安全评估：向境外提供数据的目的、方式、范围、种类和境外接收方处理数据的用途、方式发生变化影响出境数据安全的，或者延长个人信息和重要数据境外保存期限的；境外接收方所在国家或者地区数据安全保护政策法规和网络安全环境发生变化以及发生其他不可抗力情形、数据处理者或者境外接收方实际控制权发生变化、数据处理者与境外接收方法律文件变更等影响出境数据安全的；出现影响出境数据安全的其他情形[56]。

企业应密切关注评估结果有效期的临近，以及重新申报评估的触发情形，提早准备申请延长有效期或重新申报，以免造成业务活动中断或其他不利影响。

2.个人信息出境标准合同

数据跨境流动标准合同条款是一种在多个国家和地区得到认可的数据出境保障措施，普遍应用于跨国企业的日常实践。中国的标准合同从欧盟标准合同条款（以下简称“SCCs”）中借鉴了一些有益经验，也同时具备一些独特性，我们以下表简单对比说明（非穷尽式列举）中国个人数据出境标准合同与欧盟 SCCs、新加坡认可且鼓励采用的东盟跨境数据传输示范合同（“MCCs”）。

55 《跨境新规》第 9 条。

56 《数据出境安全评估办法》第 14 条。

	中国个人信息出境标准合同	SCCs	MCCS
固定形式	标准合同和 SCCs 均为固定的格式合同条款，仅允许缔约方对合同内容进行有限修改（例如增加与主合同条款不存在冲突的附件安全措施等）。		CCs 为推荐使用的示范性条款，得到包括新加坡在内的东盟多国的认可。企业可酌情采用并进行适当修改（但不得与东盟的数据保护原则相冲突）。
优先适用	在其他相关合同与标准合同/SCCs 内容存在冲突的情况下，优先适用标准合同/SCCs。 例如，跨国企业的集团关联主体之间可能订立了涉及多个国家和地区的多方数据转移协议（以下简称“IGDTA”），并将标准合同和 SCCs 作为附件纳入 IGDTA。在此情况下，如果 IGDTA 的正文和附件存在冲突，标准合同（针对从中国境内转出数据）和 SCCs（针对从欧洲经济区转出数据）应分别优先适用。		无强制适用的效力，需要在 MCCs 中明确约定，存在冲突的情况下优先适用哪一份文本。

	中国个人信息出境标准合同	SCCs	MCCS
影响评估	在采用标准合同和 SCCs 作为数据出境合规路径时，需要按照中国和欧盟法律要求分别进行个人信息保护影响评估和转移风险评估（以下简称“TIA”），但评估内容有所区别。		未明确要求就数据跨境传输场景必须完成 TIA。
适用范围	非 CIIO 自当年 1 月 1 日起累计向境外提供 10 万人以上、不满 100 万人个人信息（不含敏感个人信息）或者不满 1 万人敏感个人信息。	转移目的地国家或地区未取得欧盟的“充分性认定”，而不论数据转出方的类型或数据出境规模。	自愿适用，可作为确保境外接收方能够提供等效保护标准的证明方式之一。
角色模块	标准合同不因数据转出方和接收方的角色而适用不同模块，但部分条款针对数据接收方的角色（个人信息处理者或受托方）区分了义务。	针对数据转出方和接收方的不同角色（数据控制者或数据处理者）而分别适用 4 种不同模块。	针对数据接收方不同角色（数据控制者或数据处理者）而分别适用 2 种不同模块
备案要求	个人信息处理者应当在标准合同生效之日	无备案要求。但缔约方应书面记	自愿机制，无备案要求。

	中国个人信息出境标准合同	SCCs	MCCS
	起 10 个工作日内向所在地省级网信部门备案。	录 TIA 并应要求向监管机构提供。	
适用法律与争议解决	适用中国法律。缔约方可选择以中国法院诉讼或《纽约公约》成员国仲裁机构仲裁解决争议。	在不同角色模块下，缔约方可选择适用法律，以及在特定国家法院以诉讼解决争议。	双方可自行约定适用的法律与争议解决机制

标准合同合规路径主要包括内部准备（开展评估、协商合同）和提交备案两个阶段。在准备过程中的一个难点是评估境外接收方所在国家或者地区的个人信息保护政策和法规对标准合同履行的影响，需寻求内部或外部熟悉境外政策和法律的专业人员开展具体工作。建议企业应客观评估境外政策和法规带来的可预期的风险，以及采用的保护措施是否能有效减轻这些风险，以顺利完成备案。

在标准合同有效期内如果出现下列情形，个人信息处理者应当重新开展个人信息保护影响评估，补充或者重新订立标准合同，并履行相应备案手续：向境外提供个人信息的目的、范围、种类、敏感程度、方式、保存地点或者境外接收方处理个人信息的用途、方式发生变化，或者延长个人信息境外保存期限的；境外接收方所

在国家或者地区的个人信息保护政策和法规发生变化等可能影响个人信息权益的；可能影响个人信息权益的其他情形。

截至 2024 年 12 月，网信部门共完成标准合同备案 1071 个[57]。

3.个人信息保护认证

个人信息保护认证（全文简称“PIP 认证”）是《个保法》规定的三种出境合规路径之一，但目前在实践中的应用相对较少。根据中国网络安全审查认证和市场监管大数据中心披露的信息，截至 2024 年 11 月，该中心作为 PIP 认证的支撑单位，共收到 PIP 认证申请意向 104 个，颁发 PIP 认证证书 7 张[58]。

2025 年 1 月，国家网信办发布《个人信息出境个人信息保护认证办法（征求意见稿）》（以下简称“**认证办法**”），随着该办法的后续出台，有望为市场提供更清晰的指引，促进 PIP 认证更大范围的落地。

根据《跨境新规》和认证办法，PIP 认证的适用条件与标准合同相同，即非 CIIO 自当年 1 月 1 日起累计向境外提供 10 万人以上、不满 100 万人个人信息（不含敏感个人信息）或者不满 1 万人敏感个人信息。此外，符合《个保法》第 3 条第二款规定，在境外处理境内个人信息的个人信息处理者，也可通过获得 PIP 认证

57 数据来源：2024 年 12 月 31 日，国家数据局关于推动数据产业高质量发展和促进企业数据资源开发利用专题新闻发布会文字实录：http://www.news.cn/energy/rdzt/sjyszb/index.html

58 数据来源：2024 年 11 月 28 日，中国网络安全审查认证和市场监管大数据中心新闻快讯：https://www.isccc.gov.cn/xwdt/tpxw/11/910689.shtml

来进行个人信息出境活动[59]。

PIP 认证需要重点评定的内容包括：个人信息出境的目的、范围、方式等的合法性、正当性、必要性；境外个人信息处理者、境外接收方所在国家或者地区的个人信息保护政策法律和网络和数据安全环境对出境个人信息安全的影响；境外个人信息处理者、境外接收方的个人信息保护水平是否达到中华人民共和国法律、行政法规的规定和强制性国家标准的要求；个人信息处理者与境外接收方订立的有法律约束力的协议是否约定了个人信息保护的义务；个人信息处理者、境外接收方的组织架构、管理体系、技术措施能否充分有效保障数据安全和个人信息权益；专业认证机构根据 PIP 认证相关标准认为需要评定的其他事项[60]。

与标准合同相比，PIP 认证具有市场化、社会化服务的特点，国家还将促进 PIP 认证活动的国际交流与合作，推动 PIP 认证与其他国家、地区、国际组织之间的互认。目前，新加坡认可“指定认证”作为数据跨境流通的保障措施，而“指定认证”包括“亚太经合组织跨境隐私规则”（简称“APEC CBPR”）和“亚太经合组织处理者隐私认可”（简称“APEC PRP”）两个体系下的认证。

4.豁免三种合规路径的情形

2024 年《跨境新规》的出台，使一些特定场景的数据出境活动免于以上三种合规路径的要求。我们将不同的豁免条件归类总

59 《个人信息出境个人信息保护认证办法（征求意见稿）》第 4、第 5 条

60 《个人信息出境个人信息保护认证办法（征求意见稿）》第 10 条

结如下。

小规模、非敏感个人信息出境：非 CIIO 自当年 1 月 1 日起累计向境外提供不满 10 万人个人信息（不含敏感个人信息）的，可免予申报安全评估、订立标准合同、通过 PIP 认证[61]。这项豁免对于中小企业以及 B 端业务的企业尤为重要。

基于特定业务场景的豁免，包括：

履行合同的必要：为订立、履行个人作为一方当事人的合同，如跨境购物、跨境寄递、跨境汇款、跨境支付、跨境开户、机票酒店预订、签证办理、考试服务等，确需向境外提供个人信息的，免予申报安全评估、订立标准合同、通过 PIP 认证[62]。这项豁免尤其利好前述业务领域的 C 端企业，在《跨境新规》实施之前，这类企业很可能因其用户规模达到百万级别而触发安全评估的要求，而新规的落地则使其合规负担大大减轻。

跨境人力资源管理的必要：按照依法制定的劳动规章制度和依法签订的集体合同实施跨境人力资源管理，确需向境外提供员工个人信息的，免予申报安全评估、订立标准合同、通过 PIP 认证[63]。这项豁免对跨国企业尤其有利，但需要注意的是，“依法制定的劳动规章制度”在劳动法律法规下有其特定内涵，除了规章制度的内容必需符合我国法律规定之外，规章制度的制定还应当满足法

61 《跨境新规》第 5 条第（四）项

62 《跨境新规》第 5 条第（一）项。

63 《跨境新规》第 5 条第（二）项。

律规定的程序性要求，例如完成民主协商程序。

应对紧急事件的必要：紧急情况下为保护自然人的生命健康和财产安全，确需向境外提供个人信息的，免予申报安全评估、订立标准合同、通过 PIP 认证[64]。

在适用上述基于特定业务场景的豁免时，企业应特别关注“确需”这一前提条件。仅仅是与业务场景存在联系，却并不构成履行合同、实施人力资源管理或应对紧急事件的必要性的，并不能满足“确需”的要求。

个人信息“过境”：数据处理者在境外收集和产生的个人信息传输至境内处理后向境外提供，处理过程中没有引入境内个人信息或者重要数据的，免予申报安全评估、订立标准合同、通过 PIP 认证[65]。例如，跨国企业集团的中国境内子公司为其境外关联方提供数据处理服务，在此过程中没有引入境内个人信息或重要数据，将受益于本条豁免。

自贸区负面清单外数据：自由贸易试验区在国家数据分类分级保护制度框架下，可以自行制定区内需要纳入安全评估、标准合同、PIP 认证管理范围的数据清单（简称“**负面清单**”），区内数据处理者向境外提供负面清单外的数据，可以免予申报安全评估、订立标准合同、通过 PIP 认证[66]。截至 2025 年 8 月，天津、北京、

64 《跨境新规》第 5 条第（三）项。

65 《跨境新规》第 4 条

66 《跨境新规》第 6 条

上海、海南、浙江、广西、江苏自贸区（港）已先后发布其 2024 或 2025 版负面清单，涉及的行业包括汽车、医药/医疗、零售、民航、人工智能、再保险、国际航运、餐饮住宿、深海、航天、种业、旅游、免税商品零售业、电子商务（企业对企业）、清结算、地理信息与气象服务、企业信用信息服务、直播跨境电商、海外音视频制作与传播等。

需要特别强调的是，上述新规仅豁免安全评估、标准合同和 PIP 认证三种合规路径，但不豁免针对数据出境的合法性要求（取得单独同意或具备其他合法依据）、个人信息保护影响评估或重要数据风险评估。

二、数据出境流通的数据处理者要求

在我国境内，数据出境的主体，既可能是数据处理者，也可能是受托数据处理者，还可能涉及多个数据处理者、多个受托数据处理者共同完成数据出境活动。具体还需要结合数据出境场景及其出境主体是否有权独立决定数据处理目的来进一步判断。对于数据出境流通的数据处理者的相关要求，如本指引第三部分主体合规内容所述，在此不再赘述。

三、本地化数据存储要求

数据处理者或者受托数据处理者是否有在中国境内本地化存储数据的义务也备受市场关注。

基于数据处理者所运营的信息系统的重要性及其所处行业，可能受限于不同的数据本地化存储要求。从普遍适用于各行业的规则而言，《网安法》第 37 条规定，CIIO 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应当在境内存储；因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估。而《个保法》第 40 条进一步明确，CIIO 和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，应当将在中华人民共和国境内收集和产生的个人信息存储在境内；确需向境外提供的，应当通过国家网信部门组织的安全评估。

是否被认定为 CIIO，是判断企业是否承担数据本地化存储义务的关键。CII 是指公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域的，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统等[67]。CIIO 的认定由相关主管、监管部门负责，认定结果将通知相关 CIIO 并通报国务院公安部门[68]。一旦被通知认定为 CIIO，相关企业应切实履行数据本地化存储的义务。

国家网信办目前尚未发布个人信息本地化存储的数量门槛。此外，金融、征信、保险、医疗健康、网约车等行业还曾经或正在面临特定的数据本地化存储或信息系统本地化的要求（部分可参考第三章第（六）节）。值得注意的是，一部分早于《网安法》《个保法》颁布的行业规章或规范性文件正在经历调整，以与上位法相

67 《关键信息基础设施安全保护条例》第 2 条

68 《关键信息基础设施安全保护条例》第 10 条

适应，这也相应减轻了相关企业的合规负担。

例如，发布于 2011 年的《中国人民银行关于银行业金融机构做好个人金融信息保护工作的通知》第 6 条曾明确规定，在中国境内收集的个人金融信息的储存、处理和分析应当在中国境内进行。除法律法规及中国人民银行另有规定外，银行业金融机构不得向境外提供境内个人金融信息。这一通知于 2023 年被人行正式废止，2025 年 5 月 1 日颁布、6 月 30 日起实施的《中国人民银行业务领域数据安全管理办法》则规定，数据处理者因业务等需要向境外提供数据，存在国家网信部门规定情形的，应当严格遵守其有关规定，法律、行政法规和中国人民银行相关规定有境内存储要求的，业务数据还应当同时在中华人民共和国境内存储[69]。

需要注意的是，数据的本地化存储要求并不等同于禁止出境。如上文所述，在确有业务需要且满足适用前提的情形下，相关企业仍然可以实现数据的合规出境。

（一）数据出境流通的境外接收方要求

新加坡当地企业在接受来自中国大陆境内数据之前，应向中国境内出境主体提供所属行业、数据需求内容、数据用途等信息，以确保接收数据需求真实、合法、合理，与其所在行业、业务需求相符;

新加坡当地企业应按照与中国境内企业签署数据跨境协议中的使用目的、场景和方式，并按照数据授权使用的目的、范围以及

69 《中国人民银行业务领域数据安全管理办法》第 24 条

限制，合法合规地使用数据。

（二）数据出境流通的内容限制

为符合我国《个保法》等相关法律法规的要求，跨境流通的数据在流通内容方面，不应具有以下情形:

1.可能危害国家安全、公共利益;

2.可能侵犯第三方的合法权益;

3.含有未依法获得授权的个人信息或有不借助其他数据的情况下可以识别特定自然人的数据;

4.含有未依法公开、开放的公共数据;

5.境内外法律法规规定禁止流通的其他情形。

例如卫星及其运载无线电遥控遥测编码和加密技术算法、无人机飞行控制系统算法、我国地理信息系统的关键算法、我国地理信息系统中具有比例尺＞1:100 万的地形及地理坐标数据等均被纳入《中国禁止出口限制出口技术目录》。根据《中华人民共和国出口管制法》第二条，出口管制物项相关的技术资料等数据同样视为出口管制物项，适用出口管制相关规定。

的情况进行监督，相关个人信息和重要数据的处理情况记录应当至少保存三年。

（三）重要数据跨境传输合规要求

重要数据因涉及国家安全、公共利益等核心领域，其跨境流通需遵循更严格规则：数据出境必须通过出境安全评估，其中 CIIO 在境内运营中收集和产生的重要数据原则上应本地化存储，并匹配加密、权限控制等技术措施。此外，就已出台负面清单自贸区内

数据处理者重要数据的出境，其合规路径需适配自贸区负面清单等动态政策。

1.重要数据出境安全评估

根据《数据出境安全评估办法》及《跨境新规》规定，数据处理者向境外提供重要数据的，应当通过所在地省级网信部门向国家网信部门申报数据出境安全评估。企业进行重要数据的出境安全评估大致分为以下几个步骤:

（1）申报前的数据出境风险自评估[70];

（2）订立法律文件;

（3）数据出境安全评估[71];

（4）履行完成数据出境安全评估后的义务，包括: 向境外提供重要数据应与评估时明确的数据出境目的等各项条件相符、期限届满前申请延长评估结果有效期。

有鉴于中国与新加坡两国企业间数据往来频繁，如需向境外提供重要数据，新加坡企业可按以下指引履行各项义务:

（1）与境外接收方订立法律文件，明确约定数据安全保护责任义务，法律文件须包括以下内容:

a)数据出境的目的、方式和数据范围，境外接收方处理数据的用途、方式等;

b)数据在境外保存地点、期限，以及达到保存期限、完成约定

70 详见《数据出境安全评估办法》第五条。

71 详见《数据出境安全评估办法》第八条。

目的或者法律文件终止后出境数据的处理措施;

c)对于境外接收方将出境数据再转移给其他组织、个人的约束性要求;

d)境外接收方在实际控制权或者经营范围发生实质性变化，或者所在国家、地区数据安全保护政策法规和网络安全环境发生变化以及发生其他不可抗力情形导致难以保障数据安全时，应当采取的安全措施;

e)违反法律文件约定的数据安全保护义务的补救措施、违约责任和争议解决方式;

f)出境数据遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等风险时，妥善开展应急处置的要求和保障个人维护其个人信息权益的途径和方式。

（2）进行数据出境风险自评估，具体内容包括:

a)数据出境和境外接收方处理数据的目的、范围、方式等的合法性、正当性、必要性;

b)出境数据的规模、范围、种类、敏感程度，数据出境可能对国家安全、公共利益、个人或者组织合法权益带来的风险;

c)境外接收方承诺承担的责任义务，以及履行责任义务的管理和技术措施、能力等能否保障出境数据的安全;

d)数据出境中和出境后遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等的风险，个人信息权益维护的渠道是否通畅等;

e)与境外接收方拟订立的数据出境相关合同或者其他具有法

律效力的文件等（以下统称法律文件）是否充分约定了数据安全保护责任义务；

f)其他可能影响数据出境安全的事项。

（3）向省级网信部门提交以下材料，申报数据出境安全评估：

序号	材料名称	要求	备注
1	统一社会信用代码证件	影印件加盖公章	
2	法定代表人身份证件	影印件加盖公章	
3	经办人身份证件	影印件加盖公章	
4	经办人授权委托书		
5	数据出境安全评估申报表		使用中文填写
6	与境外接收方拟订立的数据出境相关合同或者其他具有法律效力的文件		对数据出境相关约定条款作高亮、线框等显著标识。法律文件以中文版本为准，若仅有非中文版本，须同步提交准确的中文译本。
7	数据出境风险自评估报告		使用中文撰写
8	其他相关证明材料		

（来源：《数据出境安全评估申报指南（第三版）》附件1《数据出境安全评估申报材料要求》）

企业申请数据出境安全评估时，提交申报材料方式有两种方式：

a)通过数据出境申报系统提交申报材料，系统网址为https://sjcj.cac.gov.cn；

b)如企业属于CIIO或者其他不适合通过数据出境申报系统申报数据出境安全评估的，采用线下方式通过所在地省级网信办向国家网信办申报数据出境安全评估，申报方式为送达书面申报材料并附带材料电子版，书面申报材料需装订成册。

（4）履行完成数据出境安全评估后的义务，包括：向境外提供重要数据应与评估时明确的数据出境目的等各项条件相符、期限届满前申请延长评估结果有效期，如果出现以下情形，企业需要重新申报评估：

a)向境外提供数据的目的、方式、范围、种类和境外接收方处理数据的用途、方式发生变化影响出境数据安全的，或者延长个人信息和重要数据境外保存期限的；

b)境外接收方所在国家或者地区数据安全保护政策法规和网络安全环境发生变化以及发生其他不可抗力情形、数据处理者或者境外接收方实际控制权发生变化、数据处理者与境外接收方法律文件变更等影响出境数据安全的；

c)出现影响出境数据安全的其他情形。

2.自贸区负面清单

《跨境新规》第六条明确规定，自贸区可以自行制定区内需要纳入数据出境安全评估的数据清单（以下简称“负面清单”），出境数据属于负面清单所列行业领域的，但不属于负面清单内的，自贸区内注册的数据处理者可免予数据出境安全评估。该项规定是《跨境新规》一大亮点之一，企业在识别相关领域的重要数据时，只需查找数据是否属于清单所载明的重要数据，如不属于，则无需进行数据出境安全评估。

如前文所述，上海自贸区、北京自贸区、天津自贸区等自贸区均制定了各自贸区内的负面清单，可为企业识别重要数据、申报安全评估等工作提供参考及便利。以上海自贸区为例，该区负面清单

列举了再保险领域、国际航运领域两个领域的重要数据负面清单，并详细载明了场景名称、数据子类、数据基本特征与描述。其中，再保险领域里人身险再保险场景以及财产险再保险场景下的四项数据子类均属于重要数据:

a)可能会影响国家安全的承保、理赔等相关数据;

b)涉及部分敏感特殊单位及其个人的相关数据;

c)公开后可能对经济运行、社会稳定等产生严重影响的相关数据;

d)行业领域主管（监管）部门评估确定的重要数据。

换言之，在再保险领域里人身险再保险场景以及财产险再保险场景以下但不属于以上四项数据子类的数据，均无需识别为重要数据，在进行数据出境时，无需申请安全评估。

（四）跨国公司数据出境流通的合规步骤

目前，中国的数据跨境监管体系由不同的法律、行政法规、部门规章、地方法规、标准规范组成，构建了全流程监管和精准豁免的立体框架。在这一节，我们将结合跨国企业数据跨境流动的实务，提供分步骤的行动指引。

1.数据出境场景梳理

如前文所述，中国的数据跨境监管体现了与风险相适应的特点，企业因其信息系统和数据的重要性、数据出境规模、场景、敏感性等因素，可能适用不同的合规要求。因此，实现合规出境的前置条件是梳理和盘点数据出境活动，才能识别对应的合规义务。

我们建议可以建立业务场景–信息系统–数据类型的三维矩阵，

以清晰直观地反映数据出境活动，以某汽车制造企业为例（下表仅为简单示例，实践中的映射表通常远比该示例复杂）。

业务场景	信息系统/是否被认定为CII	数据类型/是否包含重要数据、敏感个人信息	个人信息主体类型/是否已取得出境同意	境外接收方和所在地
全球研发	CAD 协同平台/否	车辆测试数据（含地理位置）/否	N/A	德国总部
供应链管理	ERP 系统/否	供应商联系人信息/否	供应商联系人/是	新加坡亚太中心
客户服务	CRM 系统/否	车主身份信息、维修记录/包含敏感个人信息	个人车主/是	美国云服务商

2.数据出境合规责任识别和路径

基于已梳理的数据出境活动详情，企业应识别适用的法律要求数据出境和合规责任和路径。在这一过程中，我们建议企业按照一定的先后顺序排查合规要求，以实现精准定位适用的法律要求，做到不重不漏。

识别特殊数据监管要求：出境数据中是否包含人类遗传资源信息、出口管制物项相关数据等受到特殊限制的数据类型？对应哪些特殊的监管措施？

识别是否有任何信息系统被认定为 CII：如有，则所有未豁免的个人信息出境活动均应申报安全评估。如不存在 CII，则应盘点

未被豁免的数据出境活动涉及的个人信息主体数量（注意去重），根据《跨境新规》中的数量门槛识别适用的合规路径。

识别是否涉及重要数据出境：公司所在地区和行业是否已公布重要数据目录？如已公布，公司是否已完成重要数据的识别和申报？出境数据中是否包含重要数据？

识别个人信息出境的合规路径：

识别适用的合规路径豁免条件——逐项识别以下豁免条件的适用，并留存判断依据的书面记录。

- 是否存在个人信息“过境”处理的情形？例如中国子公司为境外关联公司提供境外数据的数据处理服务。
- 是否存在为订立、履行个人作为一方当事人的合同，确需向境外提供个人信息的情形？注意该项豁免仅适用于特定的业务领域，包括跨境购物（如跨境电商）、跨境寄递、跨境汇款、跨境支付、跨境开户（如粤港澳大湾区跨境理财通开户）、机票酒店预订、签证办理、考试服务。
- 是否存在为实施人力资源管理，确需向境外提供员工个人信息的情形？公司是否已具有依法制定的劳动规章制度？
- 是否存在紧急情况下为保护自然人的生命健康和财产安全，确需向境外提供个人信息的情形？
- 公司是否设立于自贸区？该自贸区是否已发布了数据出境负面清单、是否适用于本公司的数据出境场景？

数量	超过 100 万人的一般个人信息	10 万人至 100 万人的一	不足 10 万人的一般个	无一般个人信息

		般个人信息	人信息	
1 万人以上的敏感个人信息	安全评估	安全评估	安全评估	安全评估
不足 1 万人的敏感个人信息	安全评估	标准合同或 PIP 认证	标准合同或 PIP 认证	标准合同或 PIP 认证
无敏感个人信息	安全评估	标准合同或 PIP 认证	豁免	豁免

（注：自贸区内企业适用已出台负面清单中的规定）

3.内部评估和合规法律文件准备

在识别适用的合规路径后，公司应着手开展内部评估及准备相关法律文件，包括标准合同或其他与境外接收方之间的协议、评估报告、申报表、辅助证明公司数据保护能力的文件等。

针对跨国企业常见的集团内数据共享这一高频场景，还应充分考虑：

- 若适用人力资源管理豁免，需留存劳动合同、集体合同等证明材料，且传输范围仅限“按照依法制定的劳动规章制度和依法签订的集体合同实施跨境人力资源管理”所必需的信息。
- 境内多家子公司如同属一家集团公司且数据出境业务场景相似，可以由集团公司作为申报主体合并申报数据出境

安全评估或者备案个人信息出境标准合同，提高出境合规工作效率。

- 国家网信部门正在推动出台个人信息出境保护认证相关管理办法，指导第三方专业认证机构对个人信息出境活动进行认证，境内企业和境外接收方任意一方通过认证，企业即可在认证范围内开展个人信息出境活动，对于通过认证的跨国集团，可在集团内开展个人信息出境活动，无需分别与各国子公司单独签订个人信息出境标准合同。

内部评估和合规法律文件准备的准备工作往往涉及跨部门、跨主体的协调，建议企业内部明确牵头与支持部门、规划明确的工作周期，避免因延迟完成合规行动而导致对业务产生不利影响。

对于在内部评估过程中发现的合规差距，应及早安排整改。常见的风险点包括：

- 隐私政策未覆盖所有数据出境活动涉及的个人信息主体。例如，公司仅有面向客户的隐私政策，无法覆盖员工、应聘者、供应商等。
- 隐私政策长期未更新，其具体内容与实际数据出境活动不符。例如，随着业务发展，公司的数据出境活动与两年前相比已新增了数据类型和境外接收方，但隐私政策仍然沿用两年前的版本。
- 未取得个人的单独同意也无其他适用的合法依据。例如，仅取得了个人数据主体对一般数据处理活动的同意，而未通过勾选、弹窗等方式取得对数据出境的单独同意。

- 数据访问权限设置过宽，导致产生不必要的出境活动。例如，中国子公司的数据上传至全球系统后，所有境外关联方的对应业务部门均可查阅该数据，但实际上仅境外总部及特定直属负责人员有查阅该数据的需求和必要。

客观而言，在内部评估中能拿到“满分答卷”的企业是极少数。企业应正视评估中发现的问题，在评估报告中如实披露合规差距、整改措施和成效，确保在实施合规路径的过程中向监管部门和认证机构提交真实、完整、准确的信息。

针对跨国企业数据出境的高频场景，比如跨国企业集团内部传输员工个人信息时，若适用人力资源管理豁免，需留存劳动合同、集体合同等证明材料，且传输范围仅限与员工履职直接相关的数据（如薪酬、岗位信息）。对于跨国企业而言，在将内部评估文件转化为申报和备案材料时，还应特别注意术语等细节问题。例如在描述安全措施、内部数据保护机制、数据类型和字段等内容时，尽量采用中国法律法规、标准和指南中的标准术语；翻译外文文件时做到准确无误，避免因这类细节导致后续监管审查的延误。对于与数据出境活动关联度不高的企业内部组织架构或业务信息、内部制度文件等，还需注意在申报和备案材料中进行筛选和保密处理。

4.申报与备案

目前，国家和省级网信部门均已开通数据出境安全评估申报、个人信息出境标准合同备案的咨询渠道。我们建议企业在准备申报与备案时积极与网信部门进行预沟通，就疑难或企业难以确定的问题充分征求监管意见，以提高正式申报与备案的通过率和效

率。

在提交申报和备案材料时，应确保严格符合关于材料形式和内容的要求。对于网信部门提出的材料补正要求予以及时响应和密切配合。

此外，境内多家子公司如同属一家集团公司且数据出境业务场景相似，可以由集团公司作为申报主体合并申报数据出境安全评估或者备案个人信息出境标准合同，提高数据出境工作效率。此外，国家网信办正在推动出台个人信息出境保护认证相关管理办法，指导第三方专业认证机构对个人信息出境活动进行认证，境内企业和境外接收方任意一方通过认证，企业即可在认证范围内开展个人信息出境活动，对于通过认证的跨国集团，可在集团内开展个人信息出境活动，无需分别与各国子公司单独签订个人信息出境标准合同。

5.出境后的内部合规管理

跨国企业的数据跨境流动处在动态变化中，拓展新业务、新市场、引入新的供应商等都可能使数据出境活动产生实质变化。同时，不同国家和地区的政策法规变化也可能对数据跨境流动产生影响。

完成差距整改、走通合规路径，只说明数据出境合规管理取得了阶段性成果，但并不意味着可以从此高枕无忧。我们建议企业落实一系列“事后管理”措施，确保持续性的合规。应关注的事项包括但不限于：

适用的合规义务的变化：建议密切关注各地区、各部门后续出台的重要数据目录、负面清单等，评估对公司业务可能造成的影响。

合规路径的有效期：关注安全评估结果、PIP 认证的有效期，以及标准合同的期限，设置到期提醒，及时安排申请延长有效期、重新申报、订立备案、认证等工作。

业务发展导致的出境活动重大变化：例如新增境外接收方或原有接收方改变处理数据的目的和方式、新增数据出境的类型、新增数据出境的目的地国家或地区、延长境外保存期限、数据出境活动涉及的个人数量显著增加等。企业应评估这些变化带来的影响，评估是否需要重新申报安全评估，或补充或重新订立标准合同。

境外数据保护政策和法规的变化：需及时评估此类变化是否可能影响数据安全或个人信息主体权益。

适用的定期报告要求：例如，重要数据处理者的年度风险评估和报送要求、《银行保险机构数据安全管理办法》对银行保险机构提出的年度数据安全风险评估报告要求、《汽车数据安全管理若干规定（试行）》对汽车数据处理者的年度数据安全管理情况报送要求等。

持续落实数据出境安全保障机制：例如，在数据出境合同中明确境外接收方的数据保护责任；提供“数据出境熔断机制”，如境外接收方违反约定时的紧急召回措施；发生个人信息泄漏风险时，给予数据主体的救济方式等等。

数据跨境流动的合规管理，既是企业全球化经营的必然要求，更是参与国际数字经济合作的基础能力。当前中国构建的监管体系，既严守数据安全底线，又通过自贸区负面清单等制度创新提升政策适配性。企业需要深刻理解这一监管逻辑：在保障国家安全和

数据主体权益的前提下，推动数据要素有序流动与价值释放。新加坡企业在我国境内投资或者新设的企业，或者合作的企业，在开展上述标的数据跨境流通活动时，应注意参考上述流通合规要求，完成合规工作。

（五）数据出境违规处罚

根据《网安法》第六十六条，CIIO 违反规定，在境外存储网络数据，或者向境外提供网络数据的，由有关主管部门责令改正，给予警告，没收违法所得，处 5 万元以上 50 万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处 1 万元以上 10 万元以下罚款。

根据《数安法》第四十六条，违反规定向境外提供重要数据的，由有关主管部门责令改正，给予警告，可以并处 10 万元以上 100 万元以下罚款，对直接负责的主管人员和其他直接责任人员可以处 1 万元以上 10 万元以下罚款；情节严重的，处 100 万元以上 1000 万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处 10 万元以上 100 万元以下罚款。

根据《个保法》第六十六条，违反规定处理个人信息，或者处理个人信息未履行规定的个人信息保护义务的，可能面临责令改正，给予警告，没收违法所得，对违法处理个人信息的应用程序，责令暂停或者终止提供服务；拒不改正的，并处一百万元以下罚款；对直接负责的主管人员和其他直接责任人员处一万元以上十万元

以下罚款。有前述规定的违法行为，最高将并处五千万元以下或者上一年度营业额百分之五以下罚款，并可以责令暂停相关业务或者停业整顿、通报有关主管部门吊销相关业务许可或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款，并可以决定禁止其在一定期限内担任相关企业的董事、监事、高级管理人员和个人信息保护负责人。

《数据出境安全评估办法》未提出额外的罚则，而是规定违反该办法的，依据《网安法》《数安法》《个保法》等法律法规处理；如果构成犯罪的，将依法追究刑事责任。

（六）数据出境争议解决

《个人信息出境标准合同办法》附件中《个人信息出境标准合同》（以下简称“《标准合同》”）第九条第（四）款规定了个人信息处理者与境外接收方之间因《标准合同》产生的争议，可以通过仲裁或诉讼方式加以解决。

首先，如果选择仲裁方式，则双方仅能择一约定特定的中国内地仲裁机构（如中国国际经济贸易仲裁委员会、中国海事仲裁委员会、北京国际仲裁中心、上海国际仲裁中心）或《承认及执行外国仲裁裁决公约》（纽约公约）成员国/地区的仲裁机构。值得注意的是，目前我国境内上海仲裁委员会、武汉仲裁委员会分别发布了《数据仲裁指引》《数据争议仲裁规则》。建议如果选择武汉仲裁委员会作为争议解决机构，可以同步把《数据争议仲裁规则》也纳入

争议解决的约定条款中[72]。再有,《标准合同》排除了交叉型仲裁条款(即仲裁申请人或被申请人所在地仲裁机构管辖)以及混合仲裁条款(即仲裁机构根据非属于该仲裁机构的仲裁规则进行仲裁)的适用，进一步压缩了个人信息处理者与境外接收方的谈判与协商空间。

此外，仲裁机构的所在地并不影响仲裁地（即“在 XX 进行仲裁”）的选择。即便约定了中国内地仲裁机构，仲裁地也可以约定为境外。仲裁地的选择将影响仲裁程序的准据法以及仲裁裁决的国籍。

其次,如果选择诉讼方式,则双方仅能约定中国内地有管辖权的法院管辖，无法选择境外法院管辖。

考虑到中国内地法院的判决在域外承认/执行层面的制度性障碍,建议选择仲裁方式,将来的仲裁裁决的承认与执行会得到纽约公约的制度性保障。

72 《武汉仲裁委员会（武汉国际仲裁中心） 数据争议仲裁规则》第四条 规则的适用（一）本会受理的数据争议案件，当事人约定适用本规则的，适用本规则审理。（二）本规则与《武汉仲裁委员会（武汉国际仲裁中心）仲裁规则》不一致的，适用本规则；本规则未作规定的，适用《武汉仲裁委员会（武汉国际仲裁中心）仲裁规则》。（三）当事人约定对本规则有关内容进行变更的，从其约定，但其约定无法实施或与法律强制性规定相抵触的除外。

第六章良好合规实践指引※

案例一：外资企业的个人信息保护管理体系

在全球化运营中，外资企业面临着不同国家和地区隐私法规的差异与挑战。当将全球隐私制度与中国《个保法》要求相结合时，制定一套科学合理、切实可行的中国本地个人信息保护标准操作程序（SOP）至关重要。

某全球性企业的隐私保护团队首先对公司全球隐私制度和中国个人信息保护相关法律法规进行深入剖析，仔细梳理两者在个人信息收集、存储、使用、加工、传输、提供、公开、删除等各个环节的要求，找出异同点。例如，全球隐私制度更侧重于原则层面的隐私保护规范，而中国《个保法》对同意告知内容以及同意方式有着细致规定。通过精准对标，明确需要在 SOP 中重点完善和强化的内容，确保既符合全球统一的隐私管理框架，又充分满足中国法律要求。

在梳理清楚具体的要求后，公司隐私保护团队搭建了 SOP 框架，包括目的、适用范围、定义、角色与职责、基本原则、全生命周期合规要求、培训要求、特殊流程要求，以及监控和审计流程。具体而言，特殊流程要求包括 App 合规流程、数据出境流程、个人信息安全事件响应流程等。例如，特殊流程中的 App 合规指南等，

※ 本章作者吴涵律师，现任金杜律师事务所合规业务部合伙人，兼任北京市律师协会数字经济与人工智能领域法律专业委员会副主任，执业领域为网络安全和数据合规；姚敏侣，北京市金杜律师事务所律师。孟洁、林奕亦有贡献。

公司组建了专业的 App 合规工作组。在 App 功能需求阶段，隐私保护团队会与业务和 IT 团队深入研讨具体的个人信息需求。例如，当业务需要开发一款健康监测 App 时，隐私保护团队会与业务团队针对收集用户健康数据的需求，逐字段讨论收集的必要性以及如何以最合理的方式获取用户同意，IT 团队则会从落地可行性角度给与建议。在 App 功能上线前，隐私保护团队会进行多轮实测，模拟各种使用场景，检查个人信息处理活动是否合法、正当、必要，例如在用户注册环节，查看是否存在单独同意，告知内容是否满足《个保法》相关要求。

SOP 制定完成后，为确保全体员工理解并执行，公司开展全面的培训与宣贯活动。组织线下集中培训，邀请内部合规人员以及外部专家进行讲解。同时，通过内部邮件、公告栏等渠道持续宣传个人信息保护的重要性和 SOP 要点。此外，公司会定期对 SOP 的执行情况进行审查。通过内部审计等方式，检查各部门在个人信息处理过程中的合规性。对发现的问题及时整改，并将审查结果与员工评估挂钩，强化制度的执行力。

案例二：外资企业数据出境合规管理规则

在外资企业数据出境合规管理实践经验上，通过构建规范化、全流程的数据出境合规管理体系，紧密贴合数据出境监管流程，形成全方位、闭环式的评估与监督流程，和覆盖事前、事中、事后的流程，将数据出境合规义务切实落实至每个部门、每项业务、每个系统以及每位员工。具体来说:

其一，强化数据出境合规义务，压实主体责任。公司深刻认识

到员工合规意识是数据出境合规的第一道防线，因此大力加强数据出境合规工作的日常培训与宣导。从个人信息保护宣传日拓展至个人信息保护宣传周、宣传季，运用小游戏、视频、漫画等新颖培训方式，结合应知应会教育考核、流程规范解读以及学习考核奖励等全流程建设，充分调动员工参与培训的积极性，实现从被动知识灌输向主动提升合规意识与能力的转变，助力员工树立良好的数据出境合规理念。

其二，组建跨部门的数据出境合规工作组。公司整合多部门资源，成立了横跨合规、安全、IT、业务、法务等多个部门的数据出境管理委员会，委员会成员具备丰富的专业知识，涵盖个人信息保护评估、数据安全评估等多个领域。日常工作中，由合规团队牵头负责数据出境合规主要工作，确保各项业务活动符合法规要求。在遇到复杂的出境合规评估时，充分整合内外部资源优势，如邀请外部专家提供专业意见，与行业内其他企业交流经验，确保评估结果的准确性与权威性。

其三，融合公司隐私影响评估以及安全风险评估流程，在数据出境需求阶段，明确要求需求方必须开展内部的数据出境风险自评估，涵盖隐私评估和安全评估。隐私评估重点关注数据出境对个人信息主体权益的影响，安全评估则聚焦于数据传输过程中的安全保障措施。只有通过内部严格评估，确认风险可控后，方可进一步推进数据出境相关工作，从源头把控数据安全风险。

其四，对数据出境场景进行精细化管理，从业务模式、出境目的、数据种类、数据处理者等多个维度构建数据出境场景。依据不

同数据出境场景的风险程度、业务重要性、行业普遍性等因素，制定针对性的合规方案。例如，针对涉及人类遗传资源信息的出境，考虑到其敏感性和重要性，制定更为严格的数据出境方案；对于员工数据出境，会在结合《跨境新规》相关条件进行判断是否属于“按照依法制定的劳动规章制度和依法签订的集体合同实施跨境人力资源管理确需向境外提供员工个人信息”的情形的基础上，通过适当简化方案以实现合规平衡。运用工具提供数据出境场景体系化、结构化的视图，使管理层能够清晰了解公司数据出境的整体情况，为公司数据出境管理提供完整统一的管理视角与有力抓手。

其五，建立数据出境长期监督管理流程，对于已通过数据出境安全评估或完成个人信息出境标准合同备案的数据出境活动，借助专用追踪表单，详细记录数据出境的规模、字段、接收方等关键信息，实现对出境活动的跟踪；同时，定期开展内部审计，对数据出境活动进行全面审查，确保合规要求得到持续落实。一旦出现法定变更情形，如数据种类增加、超出预计出境规、个人信息处理目的变化、境外接收方所在国家或地区数据安全保护政策法规和网络安全环境发生变化，根据变更情形的风险程度，及时重新申报数据出境安全评估或完成个人信息出境标准合同备案。

案例三：外资企业个人信息保护影响评估体系建设

在全球化运营的背景下，数据合规为外资企业稳健发展的关键要素。从法律合规的专业视角来看，外资企业普遍致力于在全球范围内搭建整体统一的个人信息保护标准和政策框架，这套体系的核心在于贯彻个人信息影响最小化、目的限制原则以及切实保

障数据主体权利。

通常，外资企业在中国境内开展业务时，会紧密结合中国市场的本地化需求，对全球统一标准进行细致的调整与完善。比如，鉴于我国《个保法》对敏感个人信息的单独同意要求，企业会结合中国法下的数据分类分级要求，制定相适用的企业内部分类标准和处理流程。通过这种方式，既满足全球合规要求，切实履行我国本地的法律义务。这种将全球统一标准与本地化深度融合的模式，以《个保法》为核心，同时参考欧盟《通用数据保护条例》等国际通行标准，确保企业在全球范围内数据处理活动的一致性和在中国市场的合规性，有效规避法律风险。

在具体操作层面，企业针对对外业务和日常运营中的个人信息处理活动开展全面且深入的事前评估。企业将隐私设计理念贯穿于产品和服务的全生命周期，从规划阶段就开始考虑隐私保护，在开发过程中通过隐私工具，以问答形式制定《个人信息影响评估清单》。通过对清单反馈的详细分析，综合运用人工和自动化手段，精准识别潜在风险，有效提升安全影响评估的标准化程度、判断准确性以及整体工作效率。在涉及人脸识别、行踪轨迹和特定身份等敏感个人信息的特殊使用场景下，提前对个人信息的敏感程度进行专业评估，对个人信息进行分类分级管理，并提前制定应对措施以降低风险。

企业凭借其全球多层级的个人信息保护组织架构，明确各层级的职责和权限，对全球范围内的个人信息保护工作进行统筹协调。各业务部门设置专门的数据保护联络人，负责日常业务中的个

人信息保护工作。数据保护联络人不仅要确保业务流程符合合规要求，还需及时向集团隐私合规办和管理层反馈问题和提出建议，以此实现个人信息从收集、存储、使用、共享到删除的全流程标准化评估和规范化操作。

此外还值得一提的是，该企业将个人信息处理活动安全评估体系视为一个动态发展、持续改进的过程。高度重视定期对评估体系进行回顾和优化，根据法律法规的更新、业务发展的实际需求以及技术的不断进步，及时调整评估标准和操作流程，使企业的数据合规工作能够始终适应内外部环境的变化，在不断变化的法律和业务环境中保持领先地位。

案例四：外资企业业务开展个人信息处理活动合规自查策略

外资企业在个人信息处理制定行之有效的数据合规自查策略与方案，不仅是外资企业合法运营的基本前提，更是保护个人信息安全、企业长远发展的关键所在。因此，目前部分外资企业构建起一套贯穿个人信息处理全生命周期的自查体系。

具体来说，根据个人信息处理的流程，在收集环节，严格审查收集目的是否清晰合理，收集方式是否合法公开，收集范围是否恪守最小必要原则。以对外业务中基本的“用户注册”流程为例，仅收集与服务提供直接相关的信息，如姓名、联系方式等，坚决杜绝过度收集行为，从源头上保障个人信息的合规性。在存储环节，着重评估数据存储的安全性，制定是否采用加密、访问控制等技术手段，防止数据泄露与非法访问等检查方案。针对身份证号、银行卡号等潜在敏感个人信息，采用高强度加密算法，确保数据在存储过程中

的保密性与完整性。在使用环节，严格核查数据使用是否在授权范围内，防止未经授权的共享、转让或滥用。若涉及向第三方合作伙伴提供数据，企业会事先获取用户的明确同意，并签订详尽的数据处理协议，明确双方的权利义务，确保数据流转的合规性与安全性。

在保障上述自查流程的同时，该公司会同步制定自查计划，定期开展全面的数据合规审计，如依据整体业务情况每年进行至少一次内部审计，以确保各项数据处理活动严格遵循国家法律法规和企业内部规章制度。匹配组建跨部门的专业自查团队，成员涵盖法务、信息安全、数据管理等不同的业务条线。分别从不同角度审视数据处理活动的合法性，检测数据系统的安全性与稳定性，重核实数据的准确性、完整性与一致性。通过多部门协同合作，实现对数据合规风险的全面排查与有效管控。

此外，在自查过程中，该公司也同步建立自身风险预警机制，例如：借助先进的技术工具，提升数据合规自查的效率与精准度。例如，利用数据发现工具，自动识别系统中存储的各类个人信息，统计数据类型、数量及分布情况，快速定位潜在的合规风险点。及时发现并识别潜在的数据安全隐患与合规风险。一旦触发预警，立即启动应急响应程序，通知相关部门采取有效措施，降低风险损失。实施事实常态化自查机制、运用技术手段赋能自查工作以建立风险预警与整改闭环。

案例五：外资企业内部员工的个人信息合规管理方案

在全球化的商业环境下，外资企业凭借广泛的业务布局，在国际市场上发挥着重要作用。然而，其独特的运营架构也给员工个人

信息保护带来了诸多复杂挑战，这些挑战远超一般境内企业所面临的情况。众多外资企业在全球各地设有大量分支机构，员工数量相对较多，涉及全球员工招聘、个人业绩评估、薪资方案设计以及个人简历管理等业务活动，涵盖了员工管理全生命周期（招聘、入职、培训、薪酬和绩效管理和离职等环节），其中包含大量个人信息甚至敏感个人信息，这使得信息处理工作变得相较复杂。

面对这些挑战，某外资企业采取了一系列严密且细致的措施。在人力资源管理流程中，针对不同环节的特性，制定了具有针对性的知情同意书。在招聘与入职环节，企业严格界定个人信息处理的边界，以通俗易懂的语言，向员工详细说明在各个环节收集、使用、存储和共享其个人信息的目的、方式、范围和期限。比如在收集员工入职资料时，知情同意书中会明确列举所需的学历证明、身份证复印件、紧急联系人信息等具体内容，确保员工充分了解提供这些信息的用途，在此基础上获取员工的同意或单独同意（可参考本指南第三章第三节“个人信息”中对于“单独同意”的实施要求）。

为确保员工全面了解并签署知情同意书，该企业充分利用线上线下多种渠道。例如：线上，在员工入职系统中设置专门的知情同意签署模块，员工必须阅读并点击同意后，才能继续完成后续入职流程；线下，在新员工培训时，安排专业人员负责讲解知情同意书内容，并现场指导员工签署纸质文件。此外，一旦企业对个人信息处理方式进行重大调整，会及时更新知情同意书，并再次征求员工同意，以此充分保障员工的知情权和自主选择权。

在员工福利领域，该企业与保险供应商、健康管理服务商、电

商服务商等各类供应商的合作十分频繁。为切实保障员工个人信息在与供应商交互过程中的安全，企业会与供应商签订详尽的数据安全保护协议。协议中会精确界定供应商对员工个人信息的使用范围和目的，严格限定其仅能将信息用于提供服务所需的特定业务。例如，与保险供应商合作时，仅允许其在核算员工保险保费、处理理赔等业务范围内使用员工的基本信息、健康状况等个人信息。同时，要求供应商采取与企业同等严格的数据安全保护措施，包括加密存储、访问控制、定期安全审计等。协议还对个人信息泄露的责任和赔偿做出明确规定，若供应商发生数据泄露事件，必须立即通知企业，并承担相应的法律责任和赔偿损失。企业也会定期对供应商的数据安全状况进行检查和评估，一旦发现问题，则立即要求供应商整改，从而全方位保障员工个人信息的安全。

案例六：外资企业网络数据安全事件应急响应体系

外资企业通常通过全球统一的安全运营中心（Security Operation Center，SOC）负责全天候检测端点、服务器、数据库、网络应用程序、网站和其他系统的所有活动，对网络、数据安全事件进行预防、分析和响应。中国《网安法》《数安法》和《个保法》均要求企业制定安全事件应急预案、加强风险监测，并且提出了向相关监管部门报告的义务，这无疑给全球安全运营中心与中国本地团队之间的协调沟通带来了诸多挑战。

为有效应对这些挑战，某跨国公司积极构建网络数据安全事件应急响应流程，该流程涵盖内部职责、事件发现、事件信息收集、事件内部通知流程、事件处置流程、事件定级标准、事件上报要求

等关键内容，并配备了一系列实用模板，如《网络安全事件信息报告表》《个人信息主体通知表》等。

在明确内部职责方面，该公司着重厘清中国的数据保护官和信息安全官在网络数据安全事件中的关键职责。数据保护官主要从个人信息保护视角出发，全程监督数据处理活动的合规性，确保在安全事件发生时，个人信息主体的权益能得到切实保障，例如及时准确地向受影响的个人信息主体发送通知，告知事件详情及可能产生的影响。信息安全官则聚焦技术层面，在事件发生后迅速判断技术风险点，并果断采取有效应对措施，并且协助数据保护官收集相关技术背景和材料。

在事件定级标准上，该公司全面参照中国现行法律法规，从定性和定量两个维度设计定级标准。定性方面，考量事件对国家安全、社会秩序、经济建设和公众利益造成的影响；定量方面，依据数据泄露的数量、受影响用户的规模等指标进行评估。同时，充分结合自身行业特殊性，对于涉及重要敏感数据（如医疗健康数据、金融交易数据）、重点保护人群（如未成年人、老年人）的信息，给予额外的风险考量和更高的安全级别评定。

该公司着力搭建本地团队和全球安全运营中心的高效沟通渠道，制定了专门的沟通规范。该规范明确了安全事件信息在公司内部汇报的详细流程和内容要求，依据不同风险等级的安全事件，设定了差异化的汇报时限、层级和具体要求。比如，对于低风险安全事件，信息安全官需在发现后的 8 小时内，以邮件形式向数据治理委员会简要汇报事件概况；而对于高风险安全事件，必须在 15

分钟内通过电话和即时通讯工具双重渠道紧急上报，并随后提交详细的书面报告。

最后，该公司定期组织应急演练，模拟不同类型和级别的安全事件，以此检验应急预案的可行性和有效性，及时发现潜在问题。在演练过程中，全面涉及本地团队、全球安全运营中心以及法务、公关等其他相关部门。例如，在一次演练中发现沟通环节存在信息传递不完整的情况，导致应对措施执行出现偏差。针对此类问题，迅速对应急预案和沟通流程进行优化，进一步明确信息传递的格式、内容要点和确认机制，确保信息的准确、完整传递。

数据保护与合规指引常见问题及解答※

1.数据出境咨询、举报联系方式有哪些？

答：（1）数据出境安全评估申报：010-55627135，sjcj@cac.gov.cn;（2）个人信息出境标准合同备案：010-55627565，bzht@cac.gov.cn；（3）PIP认证申请：010-82261100，data@isccc.gov.cn。

各地省级网信部门受理数据出境安全评估申报、个人信息出境标准合同备案工作的联系方式（办公地址、联系电话），详见各省、自治区、直辖市和新疆生产建设兵团互联网信息办公室官网、微信公众号，以及国家互联网信息办公室官网-数据治理栏目（https://www.cac.gov.cn）。

2.我国的个人信息处理者，在统计个人信息出境数量时，数据中具有去标识化后的个人信息，对于该部分数据是否应理解为是个人信息并统计在内？

答：需要。根据《个保法》第73条对匿名化和去标识化的定义[73]，匿名化是指个人信息经过处理无法识别特定自然人且不能复

※ 本章作者王艺，北京市环球（深圳）律师事务所合伙人；李瑞，中伦律师事务所合伙人；吴涵，北京市金杜律师事务所合伙人；刘嘉颐，北京市环球（深圳）律师事务所主办律师；蒲昱含，中伦律师事务所律师；徐晨，前中伦律师事务所律师；姚敏侣，北京市金杜律师事务所律师。

73 《个保法》第73条 ……（三）去标识化，是指个人信息经过处理，使其在不借助额外信息的情况下无法识别特定自然人的过程。（四）匿名化，是指个人信息经过处理无法识别特定自然人且不能复原的过程。

原的过程；去标识化是指个人信息经过处理，使其在不借助额外信息的情况下无法识别特定自然人的过程。匿名化处理和去标识化处理的区别在于：去标识化处理后的信息在借助其他信息的情况下仍能产生识别特定自然人的效果，而匿名化处理后的信息即使借助其他信息，也不能复原或再次识别特定自然人，因此，《个保法》在第 4 条对个人信息的定义中仅将匿名化处理后的信息排除在个人信息的范围之外[74]，而去标识化处理后的信息仍属于个人信息。

3.通过数据出境安全评估结果的有效期是多久？是否可以申请延期？

答:《跨境新规》将通过数据出境安全评估结果的有效期由《数据出境安全评估办法》中规定的 2 年延长至 3 年，自评估结果出具之日起计算。同时，增加数据处理者可以申请延长评估结果有效期的规定。有效期届满，需要继续开展数据出境活动且未发生需要重新申报数据出境安全评估情形的，数据处理者可以在有效期届满前60个工作日内通过所在地省级网信部门向国家网信部门提出延长评估结果有效期申请。经国家网信部门批准，可以延长评估结果有效期 3 年。

74 《个保法》第 4 条 个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。

4.《个人信息出境标准合同》及其附录是否可以留白？附录二的空白页可以约定哪些事项？

答:《标准合同》的正文部分及附录一应该填写的内容不应留白，附录二可根据需求填写，如无特别需要补充约定的事项，则可留白。《标准合同》的附录二可以约定双方在《标准合同》模板以外需要补充约定、但不与其相冲突的条款。例如:《标准合同》的有效期；如作为安全评估的法律文件，还建议对照《评估办法》第九条（四）的要求，补充约定境外接收方在实际控制权或者经营范围发生实质性变化，或者发生其他不可抗力情形导致难以保障数据安全时，应当采取的安全措施；明确约定双方的数据法角色、数据处理关系等情况；在不影响对外责任承担的情况下，约定双方内部的责任分摊等。

5.什么是敏感个人信息？

答：敏感个人信息指一旦泄露或非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。

实践中，企业想要判断其处理的信息是否涉及“敏感个人信息”时，可以结合该等信息对数据主体权益的影响程度，同时结合国家标准 GB/T45574-2025《数据安全技术敏感个人信息处理安全要求》举例表等进行综合判断。

6.什么是自动化决策？

答：根据《个保法》，自动化决策是指通过计算机程序自动分析、评估个人的行为习惯、兴趣爱好或者经济、健康、信用状况等，并进行决策的活动。自动化决策具有精准性较好、效率高等优点，常见的自动化决策应用场景包括银行信贷审批初步评估、平台内容个性化推荐、简历智能筛选、商业营销信息个性化推送等。

从实现路径来看自动化决策通常包括两个环节：

（1）特征生成，例如构建用户画像等。具体而言，个人信息处理者通过收集、汇聚、分析特定个人信息（例如：年龄、性别、行为偏好等），对某特定自然人个人特征，如职业、经济、健康、教育、个人喜好、信用、行为等方面做出分析或预测，形成其个人特征模型；

（2）利用特征生成结果做出决定，决策既可以是完全由计算机程序根据生成形成的个人特征信息而作出，也可以是由计算机程序辅助人工完成。

7.处理个人信息未达1000万人的企业是否需要开展个人信息保护合规审计？

答：就开展个人信息保护合规审计的频次而言，依据《个保审计办法》，处理超过1000万人个人信息的个人信息处理者，应当每两年至少开展一次个人信息保护合规审计。根据《个保法》第54条，个人信息处理者均应定期进行合规审计。因此，虽然《审计管理办法》并未对处理个人信息未达到1000万人的个人信息处理者

明文规定审计频次，但根据全国网络安全标准化技术委员会发布的《网络安全标准实践指南——个人信息保护合规审计要求》，处理超过100万、不超过1000万个人信息的个人信息处理者应根据个人信息合规风险、处理个人信息数量、业务规模等合理确定合规审计频率，每三年或四年至少开展一次个人信息保护合规审计，而处理不超过100万个人信息的个人信息处理者宜每5年至少开展一次个人信息保护合规审计。

8.间接收集个人信息的个人信息处理者会因为前手数据提供方未具备数据处理的合法性基础等问题而与其共同承担责任吗？

答：间接收集个人信息是指通过共享、转让、收集公开信息等渠道间接获取个人信息的行为，而非直接从个人信息主体采集信息。实践中常见的场景包括，物流公司从电商平台处获取消费者订单相关个人信息以进行发货；保险公司从医疗机构处获取诊疗记录等用于核保、理赔……

在指引正文中，我们明确了间接收集个人信息场景下的重点合规要求。需要特别提示的是，**间接收集个人信息的主体也可能因前手数据提供方本身不具备数据处理的合法性基础等原因而与其共同承担责任**。例如，未对数据来源尽审慎合理的审查义务的数据处理者可能承担责任。典型代表案例为全国首例声音侵权案。在这一案件中，原告为一名配音师，曾委托被告二录制录音制品（以下简称“音频”），后被告二将音频提供给了被告三，允许被告三开展商业和/或非商业使用。被告三以该音频为素材进行AI化处理，

生成了涉案文本转语音产品并在第三方平台上出售；该产品在售出后被被告一以应用程序接口形式调取并在其自身产品中使用。原告认为以上涉及的所有被告都侵犯了自身的原告声音权益，并提起诉讼。法院经审理认为，本案中使用原告个人声音开发的涉案文本转语音产品，AI 声音与原告音色、语调、发音风格等具有高度一致性，因此原告声音权益及于涉案 AI 声音；其次，由于被告二向被告三提供音频的行为未经过原告知情同意，因此这两家公司都构成对于原告声音权益的侵犯，应承担赔偿责任共计 25 万元。本案说明，如果前手数据提供方的数据来源不合法，或者使用超出授权，后续通过第三方采购等方式间接获取数据的企业也可能会承担责任。

但是，若个人信息处理者已履行审慎合理的数据来源合法性审查义务，则可免除相关责任。实践中，履行该审查义务的方式多样，包括合同约定、抽样核验等。例如，前文提及的物流公司从电商平台获取消费者订单信息用于发货时，可通过合同约定明确电商平台对数据的处理需具备合法基础；再如，保险公司从医疗机构获取诊疗记录时，可对医疗机构是否已获得患者同意共享数据的相关记录进行核验。这些措施能够有效降低因间接收集数据而与数据提供方承担共同责任的风险。

9.人力资源管理数据跨境场景下如何理解和适用无需开展数据出境安全评估、订立个人信息出境标准合同、通过 PIP 认证的情形？

根据《跨境新规》第五条规定，企业如拟主张豁免人力资源场

景下的个人信息出境相关义务，包括开展数据出境安全评估、订立个人信息出境标准合同、通过 PIP 认证的，应当确保满足如下条件：

（1）具备依法制定的劳动规章制度或依法签订的集体合同；

（2）劳动规章制度是保障劳动者所享有劳动权利、需要履行的劳动义务的企业规章制度文件，涉及劳动报酬、工作时间、休息休假、劳动安全卫生、保险福利、职工培训、劳动纪律以及劳动定额管理等与劳动者切身利益相关的事宜。集体合同是指用人单位与本单位职工根据法律、法规、规章的规定，就劳动报酬、工作时间、休息休假、劳动安全卫生、职业培训、保险福利等事项，通过集体协商签订的书面协议；

（3）出于跨境实施人力资源管理所必需；

（4）目前，法律层面有关何种数据对于人力资源管理涉及数据出境活动具有必需性尚无明确的规定或解释。实践中，这一问题将更多依赖于企业自身在“一事一议”的情形下对于“必要性”的认定结果与解释。对此，建议企业在主张豁免履行人力资源场景下的数据出境义务时，有必要事先在劳动规章制度或集体合同中明确数据出境的具体理由，并说明相关合理性、必要性；

（5）仅限于与企业签订劳动合同的员工的个人信息；

（6）此处的“员工”应作狭义理解，仅指与企业签署劳动合同、建立劳动法律关系的员工，不包括第三方外包员工和企业招聘过程中参与的候选人与实习生。

10.如何把握互联网广告营销中的个人信息保护义务?

与传统广告不同，互联网广告往往借助具有定向投放效果的程序化广告技术，因此通常涉及利用用户终端收集的用户信息与广告主的需求进行匹配，并由广告主结合自有的用户个人信息进行分析生成用户画像。由于涉及用户个人信息分析和处理,《个人保法》等相关法律法规对于该业务模式下的参与方提出了相应的个人信息保护义务。公司应结合实践中的商业模式,设置用户界面供用户便捷地行使其个人权利，并在隐私政策等对外文本中向用户告知法律法规所要求的相应内容。

（1）告知同意义务

在不同的商业模式下，公司需根据自身在数据处理关系中的实际角色,履行相应的告知同意义务。通常而言，通过收集用户个人信息的前端隐私政策披露个人信息的处理目的、方式、期限、范围等数据处理活动相关情况是实践中较为常见的履行告知义务的方式,以尽可能完整触达个人信息主体范围。实践中,公司需要全面梳理用于提供广告服务的个人信息字段范围，并考虑到由于业务合作方或业务开展方式的变化而可能导致的个人信息处理范围的变化,并最终以清晰易懂地方式披露在隐私政策中。此外,公司也需要根据自身的数据处理角色，以及实际业务开展过程中的触客方式，合理决策数据流转情况的披露方式及范围。

（2）自动化决策与个性化推荐相关义务

实践中，需由直接接触用户的前端渠道向用户提供关闭个性化广告或不使用个人标签推送广告的功能，且需确保关闭个性化

广告的选项易于找到且操作简单，避免设置复杂的步骤或隐藏选项，通常可在网站、App、小程序等的隐私设置或应用的设置菜单中提供便捷选项，允许用户选择退出个性化广告。一旦用户选择退出个性化广告，公司应确保系统尊重这一选择，不再使用个人信息来推送广告。此外，如可行，公司可提供技术支持，帮助用户解决在关闭个性化广告时可能遇到的问题。

11.一个相对完整的网络安全与数据合规制度体系主要包含哪些层面的制度或文件？

搭建企业的网络安全与数据合规制度体系可：1）满足现行法律法规项下的合规要求，从制度层面降低法律风险；2）可充分保护用户的个人信息；3）可及时发现和解决存在的网络安全漏洞，避免数据泄露等安全事件；4）可获得品牌声誉及市场竞争优势等。就整体制度体系框架而言，可结合企业自身管理实践基础，从三个维度进行搭建。

（1）一级文件：网络安全与数据合规系列管理政策

一级文件从公司整体层面出发，为公司构建网络安全与数据合规系列管理体系的建立和运行提供指导，为网络安全、数据安全、个人信息安全等内容提供战略规划方向，并明确相关的机构与职责等。

（2）二级文件：网络安全与数据合规系列类别划分

二级文件主要考虑并对网络安全与数据合规的类别进行进一步划分，可具体包括但不限于：信息安全管理体系类、信息安全管理组织类、人员安全管理类、资产管理类、访问控制类、密码密钥

类、物理和环境类、数据安全类、网络安全类、系统运行类、系统开发类、供应商管理类、信息安全事件类、法律法规等。

（3）三级文件：网络安全与数据合规具体规定

三级文件主要针对现行法律法规中对于网络安全与数据合规内容的具体规定进行落实以充分满足合规要求，包括但不限于：信息系统操作权限管理规定、数据分级分类制度、信息安全事件应急预案、数据全生命周期安全管理规定、个人信息全生命周期管理规定、个人信息保护影响评估制度、数据出境安全评估制度等。

12.一旦企业发生了数据泄露等安全事件，需要履行何种义务或者承担何种责任？

数据泄露是一种对数据本身的破坏，结果上表现为数据安全状态的丧失。《个保法》等法律法规规定了数据泄露等安全事件发生后的通知义务。当企业发生数据泄露事件时，按照相关法律法规和内部政策要求，及时向受影响的用户、监管机构等相关方发出通知和报告。其主要目的是保护用户的个人信息和数据安全，确保受影响的用户能够及时了解泄露事件的情况，采取必要的措施来减少损失和风险。同时，通过向监管机构报告，有助于监督机构及时了解数据泄露事件的情况，加强监管和追责。一般而言，通常包括以下内容：

（1）通知对象：包括受影响的用户、监管机构等相关方。

（2）通知内容：包括泄露事件的基本情况、发生原因、影响范围、应对措施、联系方式等。

（3）通知方式：可以通过电子邮件、短信、电话、信函等方式进行通知。

（4）通知时间：在发现数据泄露事件后，应在合理的时间内向相关方发出通知。

（5）报告要求：向监管机构报告的要求，包括报告的时间、内容、方式等。

数据泄露通知实际上是一种单独义务，它独立于数据安全保障义务。数据治理各方都不应将“数据泄露”本身视为违法行为，否则数据泄露通知制度就失去了意义，也不具备落地的可能。实践中可能出现以下四种情形：一是履行了数据泄露通知义务，也履行了数据安全保障义务，不承担相关法律责任；二是履行了数据泄露通知义务，而数据安全保障义务未履行，此时不产生泄露不通知的法律责任，但要承担未履行数据安全保障义务的法律责任；三是未履行数据泄露通知义务，而履行了数据安全保障义务，此时不承担数据安全保障义务的法律责任，但要承担不通知的法律责任；四是未履行数据泄露通知义务，也未履行数据安全保障义务，此时既要承担不通知的法律责任，也要承担未履行数据安全保障义务的法律责任。

附录 1：术语表※75

1.**数据，**是指任何以电子或其他方式对信息的记录。数据在不同视角下被称为原始数据、衍生数据、数据资源、数据产品和服务、数据资产、数据要素等。

2.**原始数据，**是指初次产生或源头收集的、未经加工处理的数据。

3.**个人信息，**是指以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息[76]。

4.**个人信息主体，**是指个人信息所识别或者关联的自然人[77]。

5.**敏感个人信息，**是指一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息[78]。

6.**匿名化，**是指个人信息经过处理无法识别特定自然人且不能复原

※ 本章作者王艺，执业 12 年，深数所认证数据交易合规师，专注于数据合规领域；刘嘉颐，北京市环球（深圳）律师事务所主办律师。

75 第 1-2 项、15-19 项、23-26 项来自国家数据局于 2024 年 12 月 30 日发布的《数据领域常用名词解释（第一批）》；第 27-38 项来自国家数据局于 2025 年 1 月 23 日发布的《数据领域常用名词解释（第二批）（征求意见稿）》；第 20-22 项来自深圳市地方标准《数据交易合规评估规范》（DB4403/T 564—2024）的规定；其它定义的来源详见对应脚注。

76 来自《个保法》第四条的规定。

77 来自《个人信息出境标准合同（第二版）》模板中第一款第（四）项的规定。

78 来自《个保法》第 28 条的规定。

的过程[79]。

7.**去标识化**，是指个人信息经过处理，使其在不借助额外信息的情况下无法识别特定自然人的过程[80]。

8.**重要数据**，是指特定领域、特定群体、特定区域或者达到一定精度和规模，一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能直接危害国家安全、经济运行、社会稳定、公共健康和安全的数据[81]。

9.**核心数据**，是指关系国家安全、国民经济命脉、重要民生、重大公共利益等数据，实行更加严格的管理制度[82]。

10.**数据分类分级**，是指国家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，对数据实行的分类分级保护[83]。

11.**数据出境**，是指（一）数据处理者将在境内运营中收集和产生的数据传输至境外;（二）数据处理者收集和产生的数据存储在境内，境外的机构、组织或者个人可以查询、调取、下载、导出；或（三）符合《个保法》第三条第二款情形，在境外处理境内自然人

79 来自《个保法》第 72 条的规定。

80 来自《个保法》第 72 条的规定。

81 来自《网数条例》第六十二条的规定。

82 来自《数安法》第二十一条第二款的规定。

83 来自《数安法》第二十一条的规定。

个人信息等其他数据处理活动[84]。

注:《个保法》第三条第二款情形包含（一）以向境内自然人提供产品或者服务为目的;（二）分析、评估境内自然人的行为;（三）法律、行政法规规定的其他情形。

12.**境外接收方**，是指在中华人民共和国境外自个人信息处理者处接收个人信息的组织、个人[85]。

13.**数据出境安全评估**，是指数据处理者向境外提供在中华人民共和国境内运营中收集和产生的数据，有下列情形之一的，应当申报的数据出境安全评估:（一）CIIO 境外提供个人信息或者重要数据;（二）CIIO 以外的数据处理者向境外提供重要数据，或者自当年 1 月 1 日起累计向境外提供 100 万人以上个人信息（不含敏感个人信息）或者 1 万人以上敏感个人信息。属于《跨境新规》第三条、第四条、第五条、第六条规定情形的，从其规定。数据处理者申报数据出境安全评估，应当通过数据出境申报系统提交申报材料，系统网址为 https://sjcj.cac.gov.cn。CIIO 或者其他不适合通过数据出境申报系统申报数据出境安全评估的，采用线下方式通过所在地省级网信办向国家网信办申报数据出境安全评估[86]。

14.**个人信息标准合同备案**，是指个人信息处理者通过订立标准合同的方式向境外提供个人信息，同时符合下列情形应当向所在地

84 来自《数据出境安全评估申报指南（第二版）》中“一、适用范围”的规定。

85 来自《个人信息出境标准合同（第二版）》模板中第一款第（二）项的规定。

86 来自《数据出境安全评估申报指南（第二版）》中“一、适用范围”及“二、申报方式及流程”的规定。

省级网信部门申报的备案:（一）CIIO 以外的数据处理者;（二）自当年 1 月 1 日起，累计向境外提供 10 万人以上、不满 100 万人个人信息（不含敏感个人信息）的;（三）自当年 1 月 1 日起，累计向境外提供不满 1 万人敏感个人信息的。属于《跨境新规》第三条、第四条、第五条、第六条规定情形的，从其规定。个人信息处理者不得采取数量拆分等手段，将依法应当通过出境安全评估的个人信息通过订立标准合同的方式向境外提供。个人信息处理者应当在标准合同生效之日起 10 个工作日内，通过数据出境申报系统备案，系统网址为 https://sjcj.cac.gov.cn[87]。

15.**个人信息出境个人信息保护认证，**是指依法设立并经国家市场监督管理部门批准取得 PIP 认证资质的专业认证机构，对个人信息处理者个人信息出境活动开展的 PIP 认证。个人信息处理者通过个人信息出境 PIP 认证方式向境外提供个人信息的，应当同时符合下列情形:（一）CIIO;（二）自当年 1 月 1 日起累计向境外提供 10 万人以上、不满 100 万人个人信息（不含敏感个人信息）或者不满 1 万人敏感个人信息。前款所称向境外提供的个人信息，不包括重要数据[88]。

16.**关键信息基础设施运营者**（全文简称“CIIO”），是指公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域的，以及其他一旦遭到破坏、丧失功

87 来自《个人信息出境标准合同备案指南（第二版）》中“一、适用范围”及“二、备案方式”的规定。

88 来自《个人信息出境个人信息保护认证办法（征求意见稿）》第三条及第四条的规定。

能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统等[89]。

17.**数据处理，**包括数据的收集、存储、使用、加工、传输、提供、公开等。

18.**委托处理，**是指网络数据处理者委托个人、组织按照约定的目的和方式开展的网络数据处理活动[90]。

19.**数据处理者，**是指在数据处理活动中自主决定处理目的和处理方式的个人或者组织。

20.**受托数据处理者，**是指接受他人委托处理数据的个人或者组织。

21.**数据流通，**是指数据在不同主体之间流动的过程，包括数据开放、共享、交易、交换等。

22.**数据交易，**是指数据供方和需方之间进行的，以特定形态数据为标的，以货币或者其他等价物作为对价的交易行为。

23.**交易主体，**是指数据交易活动中的数据卖方、数据买方和数据商。

注: **数据卖方**是指出售交易标的的法人或非法人组织。**数据买方**是指购买交易标的的法人或非法人组织。**数据商**是指从各种合法来源收集或维护数据，经汇总、加工、分析等处理转化为交易标的，向买方出售或许可；或为促成并顺利履行交易，向委托人提供交易标的发布、承销等服务，合规开展业务的企业法人。

89 来自《关键信息基础设施安全保护条例》第二条的规定。

90 《网数条例》第 62 条

24.**数据主体**，是指个人信息所标识或关联的自然人、在生产经营活动中采集加工企业数据的各类市场主体，以及在依法履职或提供公共服务过程中产生、处理公共数据的各级党政机关、企事业单位。

25.**交易标的**，是指数据卖方或数据商与数据买方交易的对象，交易标的包括数据产品、数据服务、数据工具等。

注：**数据服务**是指数据卖方或数据商提供数据处理（收集、存储、使用、加工、传输等）的服务。**数据工具**是指可实现数据服务的软硬件工具。

26.**数据治理**，是指提升数据的质量、安全、合规性，推动数据有效利用的过程，包含组织数据治理、行业数据治理、社会数据治理等。

27.**数据安全**，是指通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

28.**公共数据**，是指各级党政机关、企事业单位依法履职或提供公共服务过程中产生的数据。

29.**区块链**，是分布式网络、加密技术、智能合约等多种技术集成的新型数据库软件，具有多中心化、共识可信、不可篡改、可追溯等特性，主要用于解决数据流通过程中的信任和安全问题。

30.**数据产权**，是指权利人对特定数据享有的财产性权利，包括数据持有权、数据使用权、数据经营权等。

31.**数据产权登记**，是指数据产权登记机构按照统一的规则对数据的来源、描述、合规等情况进行审核并记载，并出具登记凭证的行

为。

32.**数据持有权**，是指权利人自行持有或委托他人代为持有合法获取的数据的权利，旨在防范他人非法违规窃取、篡改、泄露或者破坏持有权人持有的数据。

33.**数据使用权**，是指权利人通过加工、聚合、分析等方式，将数据用于优化生产经营、形成衍生数据等的权利。一般来说，使用权是权利人在不对外提供数据的前提下，将数据用于内部使用的权利。

34.**数据经营权**，是指权利人通过转让、许可、出资或者设立担保等有偿或无偿的方式对外提供数据的权利。

35.**衍生数据**，是指数据处理者对其享有使用权的数据，在保护各方合法权益前提下，通过利用专业知识加工、建模分析、关键信息提取等方式实现数据内容、形式、结构等实质改变，从而显著提升数据价值，形成的数据。

36.**企业数据**，是指企业在生产经营过程中形成或合法获取、持有的数据。

37.**数据交易机构**，是指为数据供需多方提供数据交易服务的专业机构。

38.**数据场内交易**，是指数据供需方通过数据交易机构达成数据交易的行为。

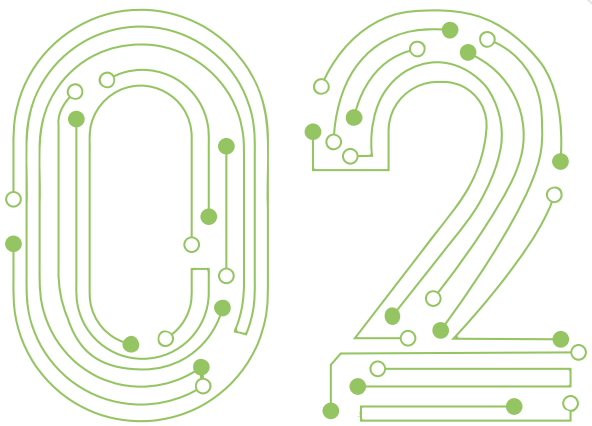
39.**数据场外交易**，数据供需方不通过数据交易机构达成数据交易的行为。

40.**数据撮合**，是指帮助数据供需方达成数据交易的行为。

41.**第三方专业服务机构**，为促进数据交易活动合规高效开展，提供数据集成、数据经纪、合规认证、安全审计、数据公证、数据保险、数据托管、资产评估、争议仲裁、风险评估、人才培训等第三方服务的专业化组织。

42.**第三方法律服务机构**，是指辅助数据交易活动有序开展，依法取得执业许可，为数据交易合规评估提供法律服务的法人或非法人组织。

新加坡章节



前言

当今世界互联互通，数据不仅催化创新，更是经济增长的关键驱动力。数据持续引领行业和市场变革，在重塑商业模式、提升效率和增强各行业生产力方面的作用日益凸显。新加坡充分认识到数据在新数字时代的重要性，对位于新加坡的亚洲商法研究所和深圳数据交易所的合作表示热烈欢迎。

由上述两家机构共同发布的《新加坡—中国联合数据合规指引》概述了新加坡和中国两大司法管辖区的相关数据保护法律法规，旨在为在两地运营的企业或与两地实体合作的企业提供实务指导。本指引通过简明易懂的方式提炼数据保护制度的基本要素，帮助企业深入理解新中两地的监管要求，为其在两地开展业务提供有力支持。

我们希望通过新中数字政策对话机制、新中（深圳）智慧城市合作倡议等重要平台，深化两国合作。同时，我们将与深圳数据交易所等机构紧密协作，引导企业在规范使用数据的基础上，充分发挥数据在创新发展中的驱动作用。展望未来数字时代，我们致力于构建更加稳固的新中跨境伙伴关系，推动两国数字经济深度融合。

作者

张汶权 新加坡立杰律师事务所合伙人兼科技、媒体与电子通讯业务部副主管

喻沛祎 新加坡立杰律师事务所高级律师

王瑞 新加坡立杰律师事务所律师

黄恺萱 新加坡立杰律师事务所律师

刘美君 新加坡立杰律师事务所见习律师

林韦良 新加坡立杰律师事务所见习律师

翁啟炫 新加坡立杰律师事务所见习律师

符淇媛

何炜俊

目录

1. 导言

1.1. 指南的目的

本指南旨在为在新加坡开展业务或有意拓展业务的中国公司提供实践性指引，并阐述新加坡数据监管制度的主要原则和要求。

1.2. 新加坡数据监管制度概览

1.2.1. 个人数据保护监管框架

新加坡的数据保护制度由《2012 年个人数据保护法》("**《个人数据保护法》**")(可在此查阅)建立，该法是新加坡数据保护的主要立法。此外，下述附属立法也对《个人数据保护法》进行了进一步的补充:

- 《2021 年个人数据保护条例》("**《个人数据保护条例》**");
- 《2021 年个人数据保护(数据泄露通知)条例》;
- 《2021 年个人数据保护(违法行为的构成)条例》;
- 《2013 年个人数据保护(谢绝来电登记)条例》;
- 《2021 年个人数据保护(执行)条例》; 以及
- 《2021 年个人数据保护(申诉)条例》。

《个人数据保护法》由新加坡个人数据保护委员会("**个人数据保护委员会**")监管和执行。

为了进一步阐释《个人数据保护法》，个人数据保护委员会发布了一系列有关解释《个人数据保护法》的建议性指

引，并会继续不时发布此类文件。

1.2.2. 影响数据保护的其他立法

除《个人数据保护法》外，还有其他地一般性法律规定了公司的数据保护义务，如:

- **《1993 年滥用计算机法》。**该法规定了涉及未经授权使用或访问计算机资料和计算机服务的各位违法行为。
- **《2018 年网络安全法》。**该法要求关键信息基础设施的所有者和运营商维护其计算机系统和服务的网络安全，并报告网络安全事件。

此外，还有其他一些影响数据保护的针对特定行业法律，如

- **《1970 年银行法》**。该法包含了保护客户数据的银行保密相关规定。
- **《2022 年电信和媒体竞争规则》(根据 《1999 年电信法》发布)。**该规则禁止电信运营商未经授权使用终端用户服务信息。
- **《2020 年医疗保健服务法》。**该法要求医疗保健服务执照持有者安全地保留医疗记录并保护医疗信息的机密性。

若出现其他成文法的规定与《个人数据保护法》不一致的情形，则以该其他成文法的规定为准。详见下文第 2.2.11(d)段。

2. 了解《个人数据保护法》框架

2.1. 范围与适用

所有在新加坡收集、使用和披露个人数据的私营组织都必须遵守《个人数据保护法》。

- **谁将被视为 "组织"?**

  《个人数据保护法》将 "组织 "定义为 "*任何个人、公司、协会或团体，无论是法人还是非法人，无论是否(a)根据新加坡法律成立或获得认可；或(b)在新加坡居住或设有办事处或营业场所*"(《个人数据保护法》第 2 条)。

  这意味着《个人数据保护法》具有域外效力，只要外国公司在新加坡收集、使用、披露或以其他方式处理个人数据，即使该外国公司未在新加坡注册成立，或未在新加坡设有实体机构，该法也适用于该外国公司。

- **什么是 "个人数据"?**

  根据《个人数据保护法》，"个人数据 "被定义为 "*有关个人的数据，无论其真实与否，且该个人可(a)从该数据中被识别；或(b)从该数据和该组织已获取或可能获取的其他信息中被识别*"(《个人数据保护法》第 2 条)。

  这意味着，本身就能用来单独识别个人身份的数据(如姓名、身份证号码、指纹、银行账号、照片、录像)将构成个人数据。

此外，与其他数据结合后可识别个人身份的数据(如手机号码、地址、性别、年龄)也构成个人数据。

2.2. 《个人数据保护法》的主要原则

2.2.1. 同意

组织在收集、使用或披露个人数据前，必须征得该个人的同意(《个人数据保护法》第 13 条)，除非《个人数据保护法》规定的同意例外可以适用(请参阅下文第 3.2 段(为处理和营销获取同意))。

请参阅下文第 3.2 段(为处理和营销获取同意)，了解根据《个人数据保护法》在同意处理个人数据方面的更详细的要求。

2.2.2. 目的限制

根据《个人数据保护法》，任何组织只能为一个理性的人在相关情形下认为适当之目的收集、使用或披露个人数据，且应按照《个人数据保护法》的通知要求通知有关个人(请参阅下文第 2.2.3 条(通知))(《个人数据保护法》第 18 条)。

如果一个组织拟将个人数据用于之前未经数据主体同意的新用途，除非适用法律另有规定或许可，否则必须再次取得数据主体的同意(个人数据保护委员会《个人数据保护法主要概念咨询性指引》(“**《指引》**”，可在此查阅)，第 14.22 段)。

2.2.3. 通知

在收集、使用或披露个人数据前，组织必须通知个人其拟收集、使用或披露其个人数据的目的，除非可适用同意例外情形(《个人数据保护法》第 20 条)。组织必须仅收集、使用或披露符合此类目的的个人数据。

在首次收集个人数据前，应通知收集、使用或披露个人数据的目的。

《个人数据保护法》没有明确向个人提供通知的特定形式。因此，只要足以使其了解收集、使用或披露其个人数据的目的，给予个人的通知可以通过任何方式和形式。

2.2.4. 访问和更正

(a) 访问

在个人提出要求时，组织必须在合理可能的情况下尽快向其提供以下信息：(a) 属于该个人的哪些个人数据由该组织控制，以及(b)在该个人提出要求之日前一(1)年内，该组织可能已经以何种方式使用或披露了这些个人数据(《个人数据保护法》第 21 条)。

组织必须在收到访问请求后的合理时间内尽快做出回应。如果组织无法在收到请求后 30 天内做出答复，则必须在 30 天内书面通知个人其能够做出答复的时间。

请注意，个人访问其个人数据的权利不是绝对的，《个人数据保护法》附表 5 列出了组织可以或必须拒绝遵循访问要求的各种情况。这包括遵从访问要求可能会导致以下结果的情况：

- 对提出请求的个人以外的其他个人的安全或身心健康构成威胁;

- 对提出请求的个人的安全或身心健康造成直接或严重伤害;

- 违背国家利益。

如果组织决定拒绝访问请求，则必须将该拒绝通知该个人。以防个人希望对组织的拒绝提出质疑，该组织必须保存一份该个人所请求的个人数据的副本，且保存期限不少于拒绝请求后至少 30 天。

(b) 更正

根据《个人数据保护法》，个人也有权要求组织更正其所拥有或控制的个人数据中的错误或遗漏("**更正要求**")。个人提出要求后，组织须考虑是否应进行更正(《个人数据保护法》第 22 条)。

组织一般须在提出更正要求后，在切实可行的情况下尽快更正个人数据。如果组织无法在提出要求后 30 天内更正个人数据，则必须在 30 天内书面通知个人其能够更正个人数据的时间。

- *更正个人数据*

  在更正要求被接受的情况下，更正必须在切实可行的情况下尽快进行。该组织还可能被要求将更正后的个人数据发送给在提出更正要求之日前一

年内该个人数据曾被披露的每一个其他组织，除非该其他组织为不需要更正后的个人数据以用于任何法律或商业目的。

- *拒绝更正个人数据*

  根据《个人数据保护法》，如果有合理的理由，可以拒绝更正个人数据。

  此外，某些法定类别的个人数据或包含个人数据的文件无需根据要求进行更正。

  如组织有合理理由认为不应作出更正(不论该组织是在回应更正要求或已经被通知由其他组织做出的某项更正)，该组织必须在其拥有或控制的个人数据上标注(即在数据上加上注释)，以体现已被要求但未作出的更正。较好的实操做法是由该组织同时注明拒绝更正的理由，并向个人解释为何决定不作出此类更正。

2.2.5. 准确性

如果组织收集或代表组织收集的个人数据可能会被该组织用于作出影响有关个人的决定，或被该组织披露给另一组织，则该组织必须作出合理的努力，确保该个人数据是准确和完整的(《个人数据保护法》第 23 条)。

- *个人直接提供的个人数据*

在大多数情况下，组织可以假定有关个人直接提供的个人数据是准确的。如有疑问，组织可考虑要求当事人口头或书面声明所提供的个人数据是准确和完整的(《指引》第 16.6 段)。

- ***第三方提供的个人数据***

一般而言，从第三方来源而非直接从个人本人收集个人数据时，应作出适当考虑。为此，应确保从组织的该第三方来源处获得适当的保证(即第三方来源已核实其转发给组织的个人数据的准确性和完整性)，和/或对第三方来源提供的个人数据进行进一步的独立核查(《指引》第 16.7 段)。

2.2.6. 保护

组织必须采取适当的技术和组织措施保护其拥有或控制的个人数据，防止(i)未经授权的访问、收集、使用、披露、复制、修改、处置或类似风险，以及(ii)丢失存储个人数据的任何存储介质或设备 (《个人数据保护法》第 24 条)。

个人数据保护委员会在其《指引》(第 17.2 段)中明确，组织在遵从保护义务方面并没有“一刀切”的解决方案，每个组织应综合以下因素，根据实际情况考虑采取合理和适当的安全保障措施:

(a) 个人数据的性质，

(b) 收集个人数据的形式(如实物或电子形式)，以及

(c) 如果未经授权的人获取、修改或处置个人数据，可能对当事人造成的影响。

2.2.7. 保存限制

一旦有理由认为保存个人数据不再符合收集该个人数据的目的，也不再是任何其他法律或商业目的所必需目的，则组织必须停止保存该个人数据，或必须删除该个人数据与特定个人之间的关联方式(如匿名化处理)(《个人数据保护法》第 25 条)。

文件应在各自的保留期结束后被销毁和/或处置。如果出于分析目的需要保留文件和/或数据，则必须采取措施对文件和数据进行匿名化处理。当一个组织、其代理人和数据中介不再能接触到文件及其包含的个人数据时，该组织将被视为已停止保留包含该个人数据的文件(《指引》第 18.10 段)。

但是，如果相关文件(i)与任何实际、潜在或威胁的诉讼或监管要求或调查有关，或(ii)与正在进行的内部或外部审计有关，则必须暂停在正常业务过程中销毁和处置该文件。

2.2.8. 传输限制

《个人数据保护法》没有对个人数据施加任何数据本地化要求。然而，个人数据只有在符合《个人数据保护法》规定的相关要求的情况下才能被传输到新加坡以外的国家或地区，这些要求包括确保海外接收方受可依法强制执行的义务的约束，从而能够为所传输的个人数据提供与《个人

数据保护法》规定的标准相当的保护(《个人数据保护法》第 26 条)。

有关跨境数据传输的要求和建议措施的更多信息，请参阅下文第 3.5 条(数据处理和跨境传输)。

2.2.9. 尽责

组织必须制定和实施符合《个人数据保护法》的数据保护政策和程序，包括回应公众或个人数据保护委员会的询问或投诉的程序。组织必须向公众提供有关其数据保护政策和程序的信息，这通常是通过在其网站上发布组织的隐私政策来实现的(《个人数据保护法》第 12 条)。

此外，组织必须任命一名数据保护官("DPO")，负责确保组织遵守《个人数据保护法》。数据保护官的业务联系信息也必须公开(《个人数据保护法》第 11 条)。有关数据保护官的更多信息，请参阅下文第 3.1 条(数据保护官：资格和责任)。

2.2.10. 数据泄露通知

如果某一组织有可信的理由相信发生了数据泄露事件，其必须评估该数据泄露事件是否应予以通知，并在数据泄露事件被评估为应予以通知的情况下，按照法定时限通知受影响的个人和/或个人数据保护委员会。

有关数据泄露通知的更多信息，请参阅下文第 3.4 条(数据泄露管理)。

2.2.11. 不受任何数据保护义务约束的情景

根据《个人数据保护法》，以下 4 种情况不需要履行任何

个人数据保护义务:

(a) 以个人或家庭身份行事的个人

如果个人是"为自己的目的"而不是为他人或代表某个组织开展活动，那么该个人就是以个人身份行事；如果该个人开展的活动"与其住宅或家庭有关"，比如使用家庭成员的个人数据申请入学、购买保险或开设联名银行账户或使用生物识别数据设置住宅门禁，那么该个人就是以家庭身份行事（《指引》第 6.8 至 6.10 段)。

(b) 在受雇于组织期间行事的雇员

在受雇工作期间行事的雇员，不受数据保护义务的规制，而其违反《个人数据保护法》的行为所产生的任何责任，将由其雇主承担，不论雇员的行为是否在雇主知情或批准的情况下实施或从事(《指引》第 6.11 至 6.12 段)。

应当注意的是，由于《个人数据保护法》对雇员的定义包括志愿者，因此开展工作而不期望获得报酬的个人也可能属于上述除外范围(《指引》第 6.11 段)。

(c) 公共机构或代表公共机构行事的组织

《个人数据保护法》将公共机构定义为包括(i)政府，包括任何部委、部门、机构或国家机关； (ii)根据任何成文法委任的审裁机构； 或(iii)由部长通过政府宪

报公告明确的法定机构(《2013 年个人数据保护(法定机构)公告》)。这些公共机构被排除在《个人数据保护法》规定的数据保护义务之外，因为已有更适合和更有效地管理它们活动的单独立法(《个人数据保护法》第 2 条)。

然而，为公共机构提供服务的组织，可以作为数据控制者或数据中介，承担《个人数据保护法》下的责任(《指引》第 6.14 段)。

(d) 其他成文法

《个人数据保护法》还规定，如果《个人数据保护法》的任何规定与新加坡的任何其他成文法不一致，则以其他成文法的规定为准(《个人数据保护法》第 6 条)。

但请注意，这种例外情况只适用于不一致的范围。其他成文法的规定只适用于两类规定不一致的事项。《个人数据保护法》中与其他成文法不冲突的其他条款将继续适用。

2.2.12. 仅可免除部分数据保护义务的情景

《个人数据保护法》还规定了部分除外条款，适用于下列只需履行部分个人数据义务的情形:

(a) 数据中介

《个人数据保护法》认可数据中介所承担的重要角色，

并认为有必要确保他们能有效运作。因此，《个人数据保护法》把组织与数据中介进行了区分。

- **什么是"数据中介"？**

  《个人数据保护法》第 2 条把数据中介定义为"代表另一组织处理个人数据的组织"。《个人数据保护法》第 2 条将"处理"一词定义为"*就个人数据进行的任何操作或一系列操作，并包括以下任何操作：记录、持有、组织、改编或更改、检索、组合、传输以及删除或销毁*"。

根据《个人数据保护法》，数据中介如果**根据以书面形式证明或订立的合同代表或为另一组织处理个人数据**，则其仅受保护义务、保存限制义务及数据泄露通知义务的规制。

另一方面，《个人数据保护法》第 4(3)条规定，就由数据中介代其处理的个人数据而言，组织在《个人数据保护法》下所承担的责任，如同该等个人数据是由该组织本身处理一样。个人数据保护委员会在其《指引》中进一步阐明，"*组织应就数据中介代其及为其目的处理个人数据而违反任何《个人数据保护法》的条款承担责任*"。

在这方面，个人数据保护委员会在其《指引》(第 6.20 及 6.21 段)中指出：

(a) 良好的实操做法是组织进行适当程度的尽职调查，以确保数据中介有能力遵守《个人数据保护法》。

(b) 组织应在与数据中介签订的合同中明确规定数据中介代其及为其目的履行的工作的范围。

(b) 业务联系信息

在大多数情况下，业务联系信息不受《个人数据保护法》规定的数据保护义务的约束。

- **什么被视为"业务联系信息"?**

  《个人数据保护法》第 2 条将业务联系信息定义为"*个人并非仅为其个人目的而提供的该个人的姓名、职位名称或头衔、业务电话号码、业务地址、业务电子邮件地址或业务传真号码，以及该个人的任何其他类似信息*"。

但是，如果个人仅出于个人目的提供其与工作有关的联系信息，则这些信息将不构成业务联系信息，组织对这些信息必须遵守数据保护义务。

(c) 《个人数据保护法》附表中的例外情况

《个人数据保护法》还规定了获取收集、使用和披露个人数据同意的例外情况和额外依据，这些例外情况可在《个人数据保护法》附表 1 和附表 2 中找到，包括:

(i) 个人数据已经公开;

(ii) 收集、使用或披露的目的明显符合该个人的利益，且无法及时获得同意;

(iii) 收集、使用或披露是应对威胁该个人或他人

生命、健康或安全的紧急情况所必需的;

(iv) 收集、使用或披露信息的目的是为了联系受伤、生病或死亡之个人的近亲或朋友; 以及

(v) 有合理的理由相信该个人或他人的健康或安全会受到严重影响，并且无法及时获得收集、使用或披露数据同意，但该组织应在切实可行的情况下尽快通知该个人收集、使用或披露数据的情况以及收集、使用或披露数据的目的。

《个人信息保护法》附表 1 和附表 2 列出了所有例外情况。

3. 主要合规义务

3.1. 数据保护官：资格与职责

作为《个人数据保护法》规定的尽责义务的一部分，在新加坡处理个人数据的任何组织都必须指定至少一名个人负责确保该组织遵守《个人数据保护法》(《个人数据保护法》第 11 条)。此人通常被称为数据保护官("**数据保护官**")。然而，组织应注意，指定数据保护官并不免除组织在《个人数据保护法》下的任何义务，遵守《个人数据保护法》的法律责任仍由组织承担，而不会转移给指定的个人(《指引》第 21.3 段)。

3.1.1. 数据保护官的职责

数据保护官负责确保组织遵守《个人数据保护法》。个人数据保护委员会进一步明确，数据保护官的职责通常包括

与高级管理层及组织的业务团队合作，为组织制订并实施适当的数据保护政策及做法。在这方面，数据保护官的工作可能涵盖广泛的内容，包括制作(或指导制作)个人数据清单、进行数据保护影响评估、监察和报告数据保护风险、提供有关数据保护的内部培训、就数据保护事宜与利益相关者接触，以及作为主要的内部数据保护专家开展一般工作(《指引》第 21.4 段)。

3.1.2. 数据保护官的资格

根据《指引》(第 21.5 段)，被组织指定为数据保护官的个人应具备以下条件:

(a) 有足够的技能和知识；以及

(b) 尽管他们不一定必须是组织的雇员，但他们有充分的权力履行作为数据保护官的职责。

在这方面，公司可以就遵守《个人数据保护法》对他们进行培训和/或认证来支持他们，例如，派他们参加由个人数据保护委员会和国际隐私专业人员协会联合颁发的《个人数据保护从业人员证书(新加坡)》。

另一方面，获委任的数据保护官也应参与自主学习和提高技能。例如，数据保护官可参考个人数据保护委员会的《数据保护官能力框架和培训路线图》("**路线图**")(可在此查阅))，以建立核心能力并达到一定的熟练水平。该路线图旨在提供自助指南，通过列出相关课程中关键能力的培训内容，如数据保护管理、业务风险管理、网络和数据泄

露事件管理、利益相关者管理、审计与合规以及数据治理，补充数据保护官的自主学习。

此外，数据保护官还被鼓励发展非数据保护能力，以支持人员和组织管理等关键任务。

3.1.3. 公布数据保护官的业务联系信息

由于数据保护官是公众就数据保护事宜与公司联系的主要联络人，《个人数据保护法》要求各组织公开数据保护官(或任何其他负责代表组织回答与收集、使用或披露个人数据有关的问题的个人)的业务联系信息(《个人数据保护法》第 11(5)条)。

可通过在"BizFile+"上登记在会计与企业管理局注册的公司的数据保护官信息来满足这一要求(《指引》第 21.7 段)。还可以在组织的官方网站的一个易于访问的位置公布数据保护官的信息，以满足这一要求(《指引》第 21.7 段)。

3.2. 为处理和营销获取同意

3.2.1. 针对收集、使用和/或披露个人数据的同意

(a) 明示同意和推定同意

同意可以是明示同意，也可以是推定同意。当时，在情况允许的情况下，应当尽可能取得明示同意。

明示同意

明示同意是指个人主动表示同意。不过，明示同意不必仅限于书面形式，也可以是口头形式(即个人口头同意收集、使用或披露信息)。在这种情况下，组织应保存个人口头同意的记录，作为同意的证据。记录的形式可以是录音或给个人的后续电子邮件/信件。

推定同意

推定同意是指(i)个人未主动表示同意，但自愿提供其个人资料；以及(ii)在当时的情况下，该个人这样做是合理的。

在"推定同意"的框架下，《个人数据保护法》还提供了"推定同意"的三种具体情况。

(i) 第一种情况可称为"*通过行为推定同意*"(《指引》第 12.20 和 12.21 段)。这适用于个人自愿向组织提供其个人数据的情况。收集、使用和/或披露数据的目的仅限于那些客观上显而易见的、从周围环境看合理适当的目的。

(ii) 第二种情况可称为“*因合同需要而推定同意*”(《指引》第 12.22 段)。如果个人向组织提供个人数据是为了与该组织签订合同，则该个人被推定同意将个人数据披露给下游其他组织，条件是这种披露是签订合同所合理需要的。

此外，若个人向组织提供个人数据并与该组织签订合同，则该个人被推定已同意在为下列目的合理必要的情况下向下游其他组织(包括收集和使用个人数据的下游组织)披露个人资料:

- 签订或履行该个人与该组织之间的合同；或

- 签订或履行该组织与下游组织之间应个人要求而签订的合同，或者一个合理的人会认为符合该个人利益的合同。

(iii) 第三种情况可称为"*通过通知推定同意*"(《指引》第 12.23 段)。在这种情况下，组织在以下情况下被推定获得个人的同意

- 在收集、使用或披露个人资料之前，该组织已评估拟进行的收集、使用或披露不会对该个人造成不利影响。如果发现有任何不利影响，该组织已采取措施消除、消减或减轻这些影响。如果存在任何残余的不利影响，该组织不得依靠通过通知推定同意来收集、使用或披露个人资料;

- 该组织已通知该个人收集、使用或披露其个人数据的目的，并给予其合理的时间选择退出。确定选择退出的期限是否合理的一些考虑因素包括(i) 与该个人互动的性质和频率; (ii) 所使用的通信方式和选择退出的渠道。

  在向该个人发出的通知中，该组织应提请该个人注意: (i) 该组织拟收集、使用或披露个人数据的事实; (ii) 收集、使用或披露该数据的目的; 及 (iii) 该个人选择退出

的方式，以及选择退出的期限；及

- 选择退出的期限已过，但该个人没有选择退出。

必须注意的是，通过通知推定同意不能用于为某些规定目的取得同意，包括向个人发送直接促销信息的目的。如果组织希望将个人的个人资料用于市场营销目的，则应征得该个人的明示同意。

此外，在组织根据“通过通知推定同意”收集、使用或披露个人资料期间，其必须保留其对潜在不良影响的评估副本。请在此查阅个人数据保护委员会发布的《通过通知视为同意评估清单》("**《视为同意评估清单》**")。该评估清单为组织提供有用的指引，以评估：(i)其可否依赖通过通知视为同意的方式收集、使用或披露个人数据；以及(ii)向个人发出的通知的适当性及选择退出的期限的合理性。值得注意的是，评估清单并不具有法律约束力，也没有规定组织必须使用。一般来说，组织应按以下顺序依次评估四个主要方面--(i) 目的，(ii) 通知的适当性以及选择退出的方式和期限的合理性，(iii) 对个人可能产生的任何不利影响，以及 (iv) 最终决定结果。

(b) 书面或口头同意

当组织打算收集、使用或披露个人数据时，应向个人提供明确表示同意的途径。作为最佳做法，应以书面

形式征得同意，或以将来需要参考时可以查阅的方式进行记录。在口头同意的情况下，应记录同意的事实、同意的目的以及口头同意的日期和时间。

(c) 通过虚假或误导性信息获得同意

如果通过提供虚假或误导性信息或通过欺骗或误导性做法获得同意，则该同意无效。

(d) 从第三方获取个人数据

在许多情况下，可能会从本人以外的其他方面收集个人数据。在这种情况下，除非能令人满意地证明，提供个人数据的一方已征得该个人同意，将其个人数据披露给为指定目的收集其个人数据的组织，否则不应收集个人数据(《指引》第 12.34 段)。

(e) 代表个人有效行事的人

同意也可由代表个人有效行事的人作出。这些个人可能是未成年人、已故者或缺乏作出同意的精神能力的人。在这种情况下，代表个人有效行事者的同意与个人本人的同意没有区别。

(f) 公开数据

公众可获得的数据是收集、使用或披露须征得同意的例外情况。"公众可获得的数据"是指任何公众成员都可以在很少或不受限制的情况下获得或访问的数据。

此类数据包括在个人出现的对公众开放的地点或活动中可以通过合理预期的方式观察到的个人数据。在这种情况下，个人数据可以不经该个人同意而被收集、使用或披露。

(g) 合法权益例外

如果收集、使用或披露个人数据符合组织或任何其他人的合法权益，且该组织或其他人的合法权益大于对该个人造成的任何不利影响，则该组织可在未经该个人同意的情况下收集、使用或披露个人资料(《个人数据保护法》附表 1 第 3 部分)。

"*合法权益*"一般指组织或其他人(包括其他组织)的任何合法权益。合法权益的例子包括侦查或防止非法活动(如欺诈和洗钱)，侦查或防止对人身安全和安保的威胁，确保信息技术和网络的安全，或防止滥用组织的服务，以及其他必要的尽职调查。值得注意的是，《个人数据保护法》明确规定，向个人发送宣传或营销信息不构成合法权益。

在依据合法权益例外规定收集、使用或披露个人数据之前，组织必须首先

(i) 确定并能清楚地阐明构成合法权益的情况或目的;

(ii) 评估是否可能对个人造成任何不良影响，并采取措施消除、消减或减轻这些影响。请在此查阅个人数据保护委员会公布的《合法权益例外情况评

估清单》("《合法权益例外情况**清单》**")。作为简要概述，《合法权益例外情况清单》 可作为有用的指南，供组织评估它们是否可以依赖合法权益例外情况。值得注意的是，组织可以通过证明自己符合《合法权益例外情况清单》的要求，来证明自己可以援引合法权益例外情况。另外值得注意的是，《合法权益例外清单》并不具有法律约束力，组织也没有义务使用该清单。一般来说，组织应按以下顺序依次评估四个主要方面--(i) 目的，(ii) 通知的适当性以及选择退出的方式和期限的合理性，(iii) 对个人可能产生的任何不利影响，以及 (iv) 最终决定结果。在权衡合法权益与由此对个人造成的任何不利影响时，各组织应注意，这不是一个单纯的定量工作，应适当评估这一平衡测试中的每一个反应。这意味着，即使收集、使用和/或披露的好处在数量上超过了不利影响，也并不自动意味着组织可以依赖合法权益例外;

(iii) 确保合法权益大于对个人造成的任何不利影响(如有)；以及

(iv) 通过任何合理有效的方式，例如通过组织的隐私政策，向相关个人披露其对合法权益例外的依赖。

(h) 业务改进例外

根据《个人数据保护法》附表 1 第 5 部分规定的例外情况，组织可将个人数据用于以下业务改进目的，

而无需征得该个人的同意

(i) 改进、提高或开发新的产品或服务;

(ii) 改进、提高或开发新的组织运作方法或流程;

(iii) 了解和理解个人对组织提供的商品和服务的行为和偏好(即客户偏好); 以及

(iv) 确定组织提供的可能适合于个人的商品或服务，或为个人个性化或定制任何此类商品或服务。

组织在援引此例外前，须确保只使用匿名个人数据不能合理地达到业务改进目的。在这种情况下，业务改进目的也应是适当的。

3.2.2. 撤回同意

个人如先前已同意收集、使用或披露其个人数据用于已经通知的用途，可在给予合理通知后随时撤回其同意。一旦组织收到个人撤回同意的通知，该组织应告知有关个人撤回同意可能产生的后果。

虽然个人可以撤回对收集、使用或披露其个人数据的同意，但《个人数据保护法》并不要求组织应要求删除或销毁该个人的个人数据。组织可根据保留限制义务在其文件和记录中保留个人数据。

3.2.3. 为营销目的获得同意

为营销目的收集、使用或披露个人数据是各组织的常见做法。然而，各组织应注意，在为此类目的使用个人数据时，应单独征得个人数据将被使用的个人的具体同意。此外，组织不应要求个人同意超出向其提供产品或服务的合理范围收集、使用或披露其个人数据，作为提供产品或服务的条件。

3.3. 数据管理政策

问责制要求组织展示对个人数据的妥善管理和保护，包括将法律要求调整为政策和做法，并利用监督机制和控制措施，确保这些政策和程序得到有效实施(个人数据保护委员会《制定数据保护管理计划指南》（可在此查阅)第 5 页)。这些政策应由管理层批准，传达给所有相关方，并定期审查，以确保其保持相关性。

这些政策将有助于内部利益相关者明确在日常工作中处理个人数据的相关责任和流程。此外，这些政策还将向外部各方表明责任，让他们了解组织对数据保护的重视，以及组织将如何保护所管理的个人数据(个人数据保护委员会《制定数据保护管理计划指南》第 15 页)。

3.4. 数据泄露管理

如组织有可信理由相信发生了数据泄露事件(不论是通过自我发现、公众警报或数据中介通知)，该组织必须采取合理及迅速的步骤，评估该数据泄露事件是否须予通知，如经评估后认为须予通知，则须按照法定时间表通知受影响的

个人及/或个人数据保护委员会(“**数据泄露通知责任**”)(《个人数据保护法》第 16C 条)。

3.4.1. 什么是"数据泄露"?

根据《个人数据保护法》第 26A 条，与个人数据有关的"数据泄露"是指

(a) 未经授权访问、收集、使用、披露、复制、修改或处置个人数据；或

(b) 在可能发生未经授权访问、收集、使用、披露、复制、修改或处置个人数据的情况下，丢失存储个人数据的任何存储介质或设备。

3.4.2. 对数据泄露进行评估的责任

若组织有理由相信发生影响其拥有或控制的个人数据的数据泄露事件，该组织必须以合理及迅速的方式，评估该数据泄露事件是否属于须予通知的数据泄露事件(《个人数据保护法》第 26C 条)。

如不合理地延迟评估数据线泄露事件，即属违反数据泄露通知责任，个人数据保护委员会可能会采取执法行动。虽然实际上可能有不同的情况影响评估所需的时间，但个人数据保护委员会已经明确，组织一般应在 30 个历日内进行评估。若组织未能在 30 个历日内完成评估，为审慎起见，该组织应准备向个人数据保护委员会解释进行评估所需的时间(《指引》第 20.4 段)。

作为良好做法，组织应记录评估数据泄露的步骤。如数据

泄露被评估为须予通知，这亦有助通知受影响的个人及/个人数据保护委员会。

组织内部的数据泄露

数据泄露如只涉及在组织内未经授权查阅、收集、使用、披露、复制或修改个人数据，则不会被视为须予通知的数据泄露(《指引》第 20.6 段)。

举例来说，若组织的人力资源部门错误地把载有个人数据的电邮附件发送给同一组织内未获授权接收该附件的另一个部门，而数据泄露的范围限于该组织内部，则数据泄露不受数据泄露通报责任的规限(《指引》第 20.6 段)。

数据中介发现的数据泄露事件

如果数据中介有理由相信，就该数据中介代表另一组织及为该另一组织的目的而处理的个人数据而言，发生了数据泄露事件，该数据中介必须通知该另一组织发生了数据泄露事件，不得无理延误(《个人数据保护法》第 26C(3)条)。

在这种情况下，数据中介并无法定责任评估数据泄露是否须予通知，以及通知受影响个人及/或个人数据保护委员会。不过，聘用数据中介的组织在接获数据中介的通知后，必须评估数据泄露是否属于须予通知的数据泄露，即使该组织委托数据中介协助评估数据泄露或代其通知受影响个人及/或个人数据保护委员会(《指引》第 20.8 段)。

3.4.3. 通知发生应予通知的数据泄露事件的责任

(a) 须予通知的数据泄露事件

根据《个人数据保护法》第 26B 条，数据泄露事件：

- 如果有可能对受影响的个人造成重大伤害，则须同时通知个人数据保护委员会和受影响的个人，或
- 如果规模较大，则须通知个人数据保护委员会。

(i) 对受影响的个人造成重大伤害

根据《2021 年个人数据保护(数据泄露通知)条例(以下简称"**条例**")(可在此查阅)，与以下个人数据有关的数据泄露会被视为对受影响个人造成重大伤害：

个人的全名或别名或完整的国民身份号码，以及《条例》附表所列的任何个人数据，其中包括未根据任何成文法的要求公开和/或披露的以下类别的个人数据(《条例》附表；《指引》第 20.15 段)：

- 未公开披露的财务信息；
- 易受伤害的个人的身份；
- 未公开披露的人寿、意外和医疗保险信息；
- 特定医疗信息；
- 有关收养事项的信息；
- 用于验证或签署电子记录或交易的私人密钥；

以及

- 个人账户标识符和用于访问账户的数据(不含个人姓名、别名或完整身份号码)。

(ii) 大规模数据泄露

数据泄露如涉及不少于 500 名个人的个人数据，即构成大规模数据泄露事件。若组织无法确定数据泄露事件中受影响个人的实际数目，但有理由相信受影响个人的数目不少于 500 人，则须通知个人数据保护委员会(《条例》第 4 条; 《指引》第 20.21 段)。

(b) 通知时间表

根据《个人数据保护法》第 26D 条，如果组织评估认为数据泄露事件应予以通知，则必须:

(i) 在切实可行的情况下，尽快，但无论如何不得迟于该组织作出评估后的 3 个日历日，通知个人数据保护委员会; 及

(ii) 如有必要，在通知个人数据保护委员会的同时或之后，在切实可行的情况下尽快通知受数据泄露事件影响的每名受影响个人。

(c) 通知中应包括的信息

在通知受影响个人及/或个人数据保护委员会须予通知的数据泄露事件时，组织须尽其所知所信，提供有关

数据泄露的详情。根据《指引》(第 20.37 段)，通知亦应包括组织的数据泄露管理及补救计划的相关信息。

(i) 通知受影响的个人

向受影响个人发出的通知应清晰易懂，并包括受影响个人可采取的步骤指南，以便受影响个人保护自己免受数据泄露可能造成的伤害(《指引》，第 20.42 段)。

(d) 通知受影响个人的例外情况

就须通知受影响个人的数据泄露事件而言，组织在以下情况下无须通知受影响个人:

(i) 根据任何规定的要求采取任何行动，使须予通知的数据泄露事件不太可能对受影响的个人造成重大伤害；或

(ii) 在发生须予通知的数据泄露事件之前，已采取任何技术措施，使使须予通知的数据泄露事件不大可能对受影响的个人造成重大损害。

不过，组织应注意，在这种情况下，即使无须通知受影响的个人，仍须就数据泄露事件通知个人数据保护委员会。

3.5. 数据处理和跨境传输

3.5.1. 将数据传输到新加坡境外的规定

《个人数据保护法》并没有就个人数据施加任何数据本地化规定。不过，只有在采取了适当步骤，确保海外接收方受法律上可强制执行的义务约束，向被转移的个人数据提供与《个人数据保护法》规定的标准相当的保护时，组织才可将个人数据转移到海外(《个人数据保护法》第 26 条)。

在这方面，《个人数据保护条例》第 11 条规定，可根据以下文件对接受者施加可依法强制执行的义务

(a) 任何法律;

(b) 任何合同，规定了与《个人数据保护法》相当的保护标准，并载明了合同下的个人数据传输目的地国家和地区;

(c) 任何具约束力的公司规则，规定每名被传输个人数据的接收者，须为被传输的个人数据提供与《个人数据保护法》相当标准的保护，并载明(i)具约束力的公司规则可适用的被传输个人数据接收者;(ii)具约束力的公司规则下个人数据的传输目的地国家和地区;及(iii)具约束力的公司规则所规定的权利和责任; 及

(d) 任何其他具有法律约束力的文书。

此外，如数据接收组织持有个人数据传输目的地国家或地区的法律授予或认可的“指定认证”，则该数据接收组织会被视为受该等可依法强制执行的责任约束(《个人数据保

护条例》第 12 条)。根据《个人数据保护条例》，“指定认证”是指亚太经济合作组织跨境私隐规则系统及亚太经济合作组织处理者私隐规则系统下的认证(《个人数据保护条例》第 12 条)。

从实际合规的角度来看，组织可参考东盟示范合同条款("**东盟示范合同条款**")作为跨境数据传输的法律依据，以简化此类数据传输。东盟示范合同条款是合同条款，规定了各方的基本责任、所需的个人数据保护措施以及保护数据主体数据的相关义务。虽然采用东盟示范合同条款是自愿的，但各组织在跨境相互传输个人数据时，可将这些合同条款纳入其具有约束力的法律协议中，以简化起草数据传输协议的过程，减少进行广泛法律谈判的必要性，并将不遵守数据保护法规的风险降至最低。值得注意的是，个人数据保护委员会表示，东盟示范合同条款可用以履行组织载《个人数据保护法》下的传输限制义务(个人数据保护委员会《在新加坡 使用东盟示范合同条款指引》第 3 段)。此外，当组织在同一国家内或向非东盟成员国传输数据时，也可酌情采纳东盟示范合同条款(根据东盟个人数据保护框架的原则或任何东盟成员国法律的要求进行适当修改)。但是，请各组织注意，东盟示范合同条款仅是基本条款。在这方面，各组织应检查并尽最大可能遵守与数据传输有关的任何其他特定部门或特定东盟成员国的指引或规定。

4. 执行和处罚

个人数据保护委员会是负责在新加坡执行《个人数据保护法》的监管机构。个人数据保护委员会有权对投诉进行调

查，并对不遵守《个人数据保护法》的组织采取执法行动。

4.1. 个人数据保护委员会的调查权力

个人数据保护委员会可在收到个人对某组织的投诉后或自行开始调查(《个人数据保护法》第 50 条)。

如果个人数据保护委员会收到投诉或其他信息，表明某个组织已经或可能已经违反《个人数据保护法》，个人数据保护委员会将首先考虑是否可以通过解决投诉人与组织之间的潜在争议来更适当地解决该问题(个人数据保护委员会关于执行《数据保护条款》的咨询指南(“执行指南”)，第 16.2 段)。在这方面，个人数据保护委员会有权将此事提交调解或其他替代争议解决方式(《个人数据保护法》第 48G 条)。如果个人数据保护委员会根据其获得的信息(无论是通过投诉还是其他来源)认为有必要进行调查，则个人数据保护委员会可以对组织的行为展开调查。

个人数据保护委员会的调查权力包括:

(a) 要求提供文件和信息的权力(《个人数据保护法》，第九附表第 1 条);

(b) 要求有关人员出庭，并对其进行口头审查和录取供词的权力(《个人数据保护法》，第九附表第 1A 条);

(c) 无需搜查令即可进入处所的权力(《个人数据保护法》，第九附表第 2 条)；以及

(d) 有搜查令即可进入处所的权力(《个人数据保护法》，第九附表第 3 条)。

所有组织和个人都必须遵守个人数据保护委员会根据其调查权力所发出的任何通知或其他要求。任何个人妨碍或阻止个人数据保护委员会行使权力、故意或鲁莽地向个人数据保护委员会提供虚假陈述或故意试图误导个人数据保护委员会均属违反《个人数据保护法》的罪行。被定罪的个人可处以不超过 10,000 新元的罚款或不超过 12 个月的监禁，或两者并处。被认定犯有此类罪行的组织可处以不超过 100,000 新元的罚款(《个人数据保护法》第 51(3)(ba)、51(3)(bb) 和 51(6) 条)。

4.2. 为确保合规而发出指示的权力

个人数据保护委员会有权发出指示以确保组织遵守《个人数据保护法》(《个人数据保护法》第 48I 条)。个人数据保护委员会可向组织或个人(视情况而定)发出其认为适合下述情况的指示，以确保组织遵守该条款。根据 《个人数据保护法》 第 48I 条，个人数据保护委员会还可以发出以下任何或所有指示:

(a) 停止在违反《个人数据保护法》情况下收集、使用或披露个人数据的指示;

(b) 销毁在违反《个人数据保护法》的情况下收集的个人数据的指示; 或

(c) 遵守个人数据保护委员会根据《个人数据保护法》第

48H(2) 条关于个人数据保护委员会审查权力的任何指示的指示。。

如果组织不遵守《个人数据保护法》第 48I 条下的指令，则根据《个人数据保护法》第 48M 条，个人数据保护委员会有权通过在新加坡地方法院登记来执行该指示。登记的指示或书面通知在执行方面具有与在新加坡地方法院获得的庭令相同的效力。因此，可以对登记的指示采取法律诉讼来执行该指示(《个人数据保护法》第 48M 条)。

4.3. 经济处罚

个人数据保护委员会可处以最高 100 万新元或该组织在新加坡年营业额 10%(如果该组织在新加坡的年营业额超过 1000 万新元)的经济处罚，以较高者为准(《个人数据保护法》第 48J 条)。

在确定要处以的经济处罚时，个人数据保护委员会会考虑造成的损害以及该组织违反《个人数据保护法》的罪责。造成的损害程度将考虑受影响个人的数量、受影响个人数据的类别以及事件持续时间等因素。罪责是指该组织在事件中的行为。个人数据保护委员会还将考虑违反《个人数据保护法》的具体性质以及该组织对《个人数据保护法》的整体遵守情况(《执行指南》第 27.4 段)。

个人数据保护委员会将考虑的其他相关因素包括该组织是否已采取行动减轻不合规行为的影响和后果、该行动的及时性和有效性，以及该组织或个人之前是否未能遵守 《个人数据保护法》(《执行指南》第 27.4 段)。

4.4. 自愿承诺

个人数据保护委员会有权接受相关组织或个人的书面自愿承诺，而不是进行调查或发出指示(《个人数据保护法》第48L 条)。一般而言，自愿承诺流程旨在为具有良好问责做法和有效补救计划的组织提供实施补救计划的机会。在适当情况下，组织可以承诺改进其数据保护做法(《执行指南》第 25.3 段)。

个人或组织提供自愿承诺须经 个人数据保护委员会接受。例如，个人数据保护委员会不得在包括但不限于个人或组织故意或恶劣地不遵守《个人数据保护法》的情况下接受自愿承诺(《执行指南》第 25.4 段)。

如果某个组织或个人未能遵守自愿承诺中的任何承诺，个人数据保护委员会可向该组织或个人发出其认为在当时情况下合适的任何指示，以确保该组织或个人遵守该承诺(《执行指南》第 25.5 段)。

5. 合规的实际步骤

本条将指出小型和大型组织在遵守《个人数据保护法》方面通常面临的一些一般挑战，并重点介绍新加坡现有的各种可供组织利用的举措。

值得注意的是，***小型和大型组织在《个人数据保护法》下承担同样的义务***。但是，它们在遵守相同义务时所面临的挑战可能有所不同。

5.1. 小企业面临的挑战和实用解决方案

小型企业面临的挑战主要来自于它们资源有限，以及《个人数据保护法》和相关法律规定的众多义务。例如，小型企业可能并不完全了解他们在《个人数据保护法》下的义务，以及他们企业的关键业务数据基础设施和来源。

资讯通信媒体发展管理局("IMDA")为小型企业提供的实用解决方案和举措包括以下内容:

任命数据保护官并开展培训

每个组织，无论规模大小，都必须任命一名数据保护官来监督数据保护责任，以确保遵守《个人数据保护法》(《个人数据保护法》，第 11(3)节)。数据保护官也是确保企业遵守《个人数据保护法》规定义务的重要接触点(请参阅上文第 3.1 条(数据保护官：资格和责任))。

数据保护官可以接受培训，以便更好地了解组织在《个人数据保护法》下的义务，并将这些知识传授给组织的其他成员。个人数据保护委员会提供了一个 数据保护官 能力框架和培训路线图，可帮助数据保护官做好准备(有关个人数据保护委员会 的 数据保护官能力框架和培训路线图的更多信息，请参见此处)。

制定数据保护政策

企业可以而且应该制定简明扼要的数据保护政策，概述如

何收集、使用、披露和保护个人数据，并确保员工接受有关该政策的培训。这些对于确保遵守企业的责任义务(《个人数据保护法》第 12 条)非常重要。

企业可寻求法律援助，以制定合适和合规的数据保护政策。此外，个人数据保护委员会还制作了许多免费使用的指南和工具，以协助企业遵守《个人数据保护法》，并可在制定数据保护政策时用作参考。其中一些例子包括：

(a) 个人数据保护委员会关于制定数据保护管理计划的指南(请参见此处)；

(b) 个人数据保护委员会 关于数据保护影响评估指南(请参见此处)；以及

(c) 组织的 《个人数据保护法》评估工具(请参见此处)。

实施数据保护措施

公司可采取以下数据保护措施，这些措施也可在公司的数据保护政策中做出规定:

(a) 数据最小化: 只收集业务所需的个人数据(个人数据保护委员会关于《个人数据保护法》的选定主题咨询指南(“**选定主题指南**”)，第 3.11 段)

(b) 查阅控制: 限制只有获得授权的人员才能查阅个人数据，防止未经授权的查阅，并确保个人数据仅用于合法目的(《选定主题指南》，第 3.16 段)。

(c) 数据加密：在存储和传输过程中使用加密技术保护个人数据。加密可增加一层安全保护(选定主题指南，第3.7(d)段)。

框架和认证：数据保护基本计划

资讯通信媒体发展管理局认识到较小型组织所面临的特殊挑战，因此推出了数据保护基本要素("DPE")框架，该框架提供了数据保护的基本标准，中小型企业可利用该标准保护客户的个人数据，与其利益相关者建立信任，并在发生数据泄露时迅速恢复(有关 数据保护基本要素 计划的更多信息，请参见此处)。

除了通过提供实用指导帮助中小企业遵守《个人数据保护法》外，数据保护基本要素架还为其参与者提供了更多好处。满足所有要求的参与者将在 资讯通信媒体发展管理局网站上列出，并使用指定的 数据保护基本要素 徽标，以表彰他们的努力；如果发生数据泄露，数据保护基本要素 认证将被个人数据保护委员会 视为潜在的缓解因素(有关 数据保护基本要素计划益处的更多信息，请参见此处)。

为进一步帮助中小企业应用数据保护基本要素政策框架，资讯通信媒体发展管理局在其网站上提供了 "数据保护基本要素清单"等免费使用的工具，帮助用户找出与数据保护基本要素框架相关的现有数据保护措施中的差距，并就如何弥补这些差距提供实用建议(有关数据保护基本要素清单。请参见此处)。

虽然数据保护基本要素框架为中小型企业提供了一个有用的起点，使其开始遵守《个人数据保护法》，但不应将其视为包罗万象的解决方案。虽然该框架提供了结构化的途径和实用工具，帮助中小型企业建立数据保护和安全实践的基线，但要实现持续合规和建立弹性数据保护制度，中小型企业还需要采取更多措施。它们最终应超越数据保护基本要素框架中概述的基本做法，开发定制的稳健机制，以应对自身企业特有的风险、挑战和运营复杂性。

扩大计划规模：更好的数据驱动业务计划

随着中小型企业的成长和数据保护实践的不断改进，它们可以考虑参加更多的计划，以进一步加强合规性和建立信誉。这些方案可被视为中小型企业在合规过程中可以实现的实际里程碑，与数据保护基本要素方案类似。其中一个选项是由资讯通信媒体发展管理局制定的 "更好的数据驱动型业务"("BDDB")计划(有关 "更好的数据驱动型业务计划 "的更多信息，请参见此处)。

从本质上讲，更好的数据驱动型业务 使企业能够

(a) 安全收集必要的数据：确保按照相关法律和安全标准收集数据；

(b) 在得到充分保护的情况下跨系统整合数据：允许企业整合和分析各种来源的数据，同时维护安全和隐私；以及

(c) 安全地与合作伙伴和供应商共享外部数据：确保与第

三方共享数据符合《个人数据保护法》的要求。

5.2. 大型企业面临的挑战和实用解决方案

虽然大公司一般拥有更多可支配资源，但其数据量和需要遵守的法规范围往往也相应更多。此外，大型企业可能从事更复杂的商业活动，如跨司法管辖区的数据交易和数据处理，这就需要更多考虑数据传输和数据中介管理义务。总体而言，虽然大型企业要履行相同的义务，但它们也面临着有别于小型企业的一系列合规挑战。

资讯通信媒体发展局为大型企业提供的实用解决方案和倡议包括以下内容:

定期进行数据保护审计

定期进行审计，以发现并解决潜在的数据保护风险。这包括审查数据处理活动，确保遵守《个人数据保护法》。审核有助于组织识别漏洞，并在问题升级之前采取纠正措施。

制定跨境数据传输政策

个人数据不得被传输到新加坡以外的国家或地区，除非符合《个人数据保护法》规定的要求，其中包括确保海外接收方受可依法强制执行的义务的约束，为如此传输的个人数据提供与《个人数据保护法》规定的保护标准相当的保护(《个人数据保护法》第 26 条)。

大型组织如在组织内部或与其他第三方处理跨境数据传输，

应制订 跨境传输个人数据的政策及程序，确保符合《个人数据保护法》 及其他相关条例。跨境数据传输政策应包括一些机制，例如在组织内部制定具约束力的公司规则，或与第三方签订标准数据传输协议或合约条款，以确保个人数据在国际间传输时受到保护(《指南》第 19.5 段)(请参阅上 文第 3.5 条(数据处理及跨境传输))。

与数据中介打交道的免费使用指南

由于大型组织通常处理的数据量相对较大，这些组织聘请数据中介来支持其合规工作的情况并不少见。然而，重要的是要认识到，即使是由中介机构处理的个人数据，组织仍然要对所处理的个人数据负责。根据《个人数据保护法》第 4(3)条，组织被视为 "在[《个人数据保护法》]下对由数据中介机构代表其并为其目的而处理的个人数据，负有与该个人数据由该组织本身处理相同的义务"。

大型组织可以利用个人数据保护委员会公开提供的各种免费指南和工具。其中一本与大型组织特别相关的指南是《数据中介机构管理指南》("**数据中介机构指南**")(有关**《数据中介机构**管理指南》，请参见此处)。总体而言，该指南涵盖以下关键领域：(1)治理和风险评估；(2)政策和做法；(3)服务管理；及(4)退出管理。

框架和认证：数据保护信任标记

大型组织实现合规的另一种方法是参与认证计划，如资讯通信媒体发展局 提供的 "数据保护信任标志"("DPTM")。数据保护信任标志 是一项自愿性的全企业认证，使企业能够

展示其对负责任的数据保护惯例的承诺。获得 数据保护信任标志认证可增强企业的竞争优势，并有助于与客户和利益相关者建立信任关系(有关 数据保护信任标志的更多信息，请参见此处)。

数据保护信任标志认证清单是一套有价值的合规性实用指南(数据保护信任标志认证清单请参见此处)。各组织可使用该清单评估其申请认证的准备情况，并指导其加强合规工作。大体上，清单分为四个主要原则：(1) 治理和透明度；(2) 个人数据管理；(3) 个人数据保护；以及 (4) 个人权利。

6. 中国企业面临的具体挑战

随着新加坡作为全球商业中心的地位不断加强，许多中国企业将新加坡视为其全球扩张路线图的第一步。在寻求拓展新加坡业务的同时，企业必须注意遵守当地法律(包括《个人数据保护法》)所带来的挑战。我们在下文中列举了一些中国企业普遍面临的典型问题。

(a) 跨境数据传输

跨境数据传输是拥有新加坡子公司、分公司或海外总部的中国公司运营中不可或缺的一部分。许多中国公司还可能通过设在新加坡的子公司或分公司在新加坡采用云解决方案，集中管理其海外数据。

尽管《个人数据保护法》并未对个人数据提出本地化要求，但它要求转让方证明接收方的司法管辖区 提供同等水平的数据保护或实施严格的保障措施，如确保数据

保护的合同条款或公司规则。在与中国不同的标准和法规保持一致时，这一点尤其具有挑战性。

(b) 数据保护标准的差异

中国和新加坡在数据保护标准上的差异也给中国公司带来了挑战。这些公司必须提升其数据保护措施，以符合两国的标准，这可能涉及对其现有政策、培训和运营的重大调整。

同时，一些外国当局也可能要求企业广泛获取数据以进行调查，特别是在涉及国家或公共安全的情况下。因此，公司可能需要遵守监管机构和执法机构在其他司法管辖区的调查程序或信息要求，这可能会给遵守《个人数据保护法》带来问题。面对外国当局的这种访问请求，公司可能会发现很难完全履行《个人数据保护法》规定的义务。

(c) 数据保护官要求

《个人数据保护法》规定，每个组织都应任命一名数据保护官，负责遵守《个人数据保护法》。中国公司必须确保其数据保护官精通新加坡的数据保护法律，并有能力弥合中新两国在文化和运营上的差异。对于刚刚来到新加坡的中国公司，如果缺乏胜任的数据保护官人选，也可以考虑从外部聘请数据保护官，如新加坡的数据保护律师。

(d) 公众认知与信任

有效的数据管理不仅对遵守法律至关重要，而且对维护消费者的信任也至关重要。数据保护方面的失误会导致公众不信任和声誉受损，从而对企业运营造成不利影响。中国企业必须优先考虑稳健的数据保护措施，以建立和维护在新加坡的这种信任。

(e) 将合法利益作为未经同意处理数据的依据

在新加坡，合法权益是收集、使用和披露个人数据的一个明确界定的替代依据。中国的数据保护法目前还没有类似的合法权益依据。因此，如果中国公司选择以合法权益为依据，而不是征得同意，那么在遵守合法权益依据的详细要求方面可能会面临挑战。

附录

6.1. 核查清单样本

1.1 根据《个人数据保护法》合规核查清单修订，用于组织的数据保护政策和实践（个人数据保护委员会 | 组织的《个人数据保护发》评估工具）

编号	合规要点	回复
初步问题		
1	贵组织是否收集、使用或披露个人数据？ (这些数据包括员工、客户、承包商、捐赠者、志愿者等利益相关者的姓名、联系电话、地址等)。	☐是 ☐否
2	收集、使用或披露是否是根据《个人数据保护法》以外的成文法要求或授权的？ (例如《电信法》、《雇佣法》、《银行法》、《保险法》等。如果您不确定，请选择"否")。	☐是 ☐否
同意		
1	贵组织在收集、使用或披露个人数据时，会征得个人同意，或依赖于同意的例外情况。	☐已实施 ☐部分实施 ☐未实施 ☐不适用
2	贵组织通知并重新征得个人同意，将其个人数据用于新的或不同的目的。	☐已实施 ☐部分实施 ☐未实施 ☐不适用
3	贵组织有渠道处理个人提出的撤销同意请求，并作出回应。	☐已实施 ☐部分实施

		☐未实施 ☐不适用
4	贵组织确保代表个人提供同意的人是有效地代表该个人行事。	☐已实施 ☐部分实施 ☐未实施 ☐不适用
5	贵组织确保从第三方来源获取的个人数据已获得个人的有效同意。	☐已实施 ☐部分实施 ☐未实施 ☐不适用
6	贵组织已进行必要的评估，以利用视为同意的方式收集、使用或披露个人数据。	☐已实施 ☐部分实施 ☐未实施 ☐不适用
7	贵组织已制定必要流程，包括进行评估，以利用例外情况收集、使用和披露个人数据。	☐已实施 ☐部分实施 ☐未实施 ☐不适用
目的限制		
1	贵组织仅出于已告知个人并经同意的合理目的收集、使用或披露个人数据。	☐已实施 ☐部分实施 ☐未实施 ☐不适用
通知		
1	贵组织在收集个人数据时或在收集数据之前告知个人收集、使用或披露其个人数据的目的。	☐已实施 ☐部分实施 ☐未实施 ☐不适用
访问和更正		
1	贵组织有流程在拒绝查阅请求后保存一份完整准确的个人数据副本(至少 30 个日历日)。	☐已实施 ☐部分实施

		☐未实施 ☐不适用
2	贵组织已提供方法，允许个人对其在贵组织保管下的个人数据提出查阅和更正请求。	☐已实施 ☐部分实施 ☐未实施 ☐不适用
3	贵组织在合理范围内尽快回应个人的查阅请求。	☐已实施 ☐部分实施 ☐未实施 ☐不适用
4	贵组织会告知提出查阅请求的个人与处理查阅请求相关的任何费用。	☐已实施 ☐部分实施 ☐未实施 ☐不适用
5	贵组织在可行的情况下尽快回应个人提出的更正其个人数据的要求。	☐已实施 ☐部分实施 ☐未实施 ☐不适用
6	贵组织告知个人对查阅或更正请求做出回应所需的时间。	☐已实施 ☐部分实施 ☐未实施 ☐不适用
7	在回应查阅或更正请求之前，贵组织会尽职核实提出请求的个人身份，或核实第三方是否获得合法授权代表个人行事。	☐已实施 ☐部分实施 ☐未实施 ☐不适用
准确性		
1	贵组织确保从个人收集的个人数据准确完整。	☐已实施 ☐部分实施 ☐未实施 ☐不适用

2	贵组织确保从第三方来源收集的个人数据准确完整。	☐已实施 ☐部分实施 ☐未实施 ☐不适用
保护		
1	贵组织已采取适当的技术安全措施，以保护贵组织所拥有或控制的个人数据。	☐已实施 ☐部分实施 ☐未实施 ☐不适用
2	贵组织已采取适当的实体安全措施，以保护贵组织所拥有或控制的个人数据。	☐已实施 ☐部分实施 ☐未实施 ☐不适用
3	贵组织已采取适当的管理措施，保护贵组织掌握或控制的个人数据。	☐已实施 ☐部分实施 ☐未实施 ☐不适用
4	贵组织进行风险评估，以确定适当的安全措施，保护贵组织拥有或控制的个人数据。	☐已实施 ☐部分实施 ☐未实施 ☐不适用
5	贵组织已采取措施防止个人数据意外泄露。	☐已实施 ☐部分实施 ☐未实施 ☐不适用
6	贵组织确保指定的信息和通信技术("ICT")服务提供商能够提供足够的保护和安全级别，以保护贵组织所拥有或控制的个人数据。	☐已实施 ☐部分实施 ☐未实施 ☐不适用
7	贵组织确保所使用的现成软件能够满足并提供足够的安全级别，以保护贵组织所拥有或控制	☐已实施 ☐部分实施

	的个人数据。	☐未实施 ☐不适用
8	贵组织确保代表贵组织处理个人数据的第三方组织按照《个人数据保护法》保护个人数据。	☐已实施 ☐部分实施 ☐未实施 ☐不适用
保存限制		
1	在没有法律或业务理由的情况下，贵组织应停止保留个人数据。	☐已实施 ☐部分实施 ☐未实施 ☐不适用
2	贵组织已为代表贵组织处理个人数据的第三方服务提供商规定了保留期限和处置要求。	☐已实施 ☐部分实施 ☐未实施 ☐不适用
3	贵组织有处置个人数据(包括第三方持有的数据)的流程。	☐已实施 ☐部分实施 ☐未实施 ☐不适用
传输限制		
1	贵组织确保只将个人数据传输给具有与《个人数据保护法》和《个人数据保护条例》相当的数据保护标准的海外司法管辖区的组织。	☐已实施 ☐部分实施 ☐未实施 ☐不适用
尽责		
1	贵组织已任命数据保护官 (DPO) 或办公室。	☐已实施 ☐部分实施 ☐未实施 ☐不适用
2	贵组织采用问责工具，协助组织展示和实施问责制。	☐已实施 ☐部分实施

		☐未实施 ☐不适用
3	贵组织的数据保护官 业务联系信息向公众公开。	☐已实施 ☐部分实施 ☐未实施 ☐不适用
4	贵组织已制定并实施了遵守 《个人数据保护法》 的政策和做法，包括制定和实施数据保护管理计划 (DPMP)。	☐已实施 ☐部分实施 ☐未实施 ☐不适用
5	贵组织制定了政策和做法，以回应与个人数据保护有关的询问和投诉。	☐已实施 ☐部分实施 ☐未实施 ☐不适用
6	贵组织内部有明确的个人数据保护问题报告渠道。	☐已实施 ☐部分实施 ☐未实施 ☐不适用
7	贵组织对所有员工进行有关组织个人数据保护政策和做法的教育。	☐已实施 ☐部分实施 ☐未实施 ☐不适用
数据泄露通知		
1	贵组织已采取措施监控潜在的数据泄露。	☐已实施 ☐部分实施 ☐未实施 ☐不适用
2	贵组织有应对数据泄露的政策和做法。	☐已实施 ☐部分实施 ☐未实施 ☐不适用

3	贵组织已制定数据泄露管理计划，以应对与个人数据保护相关的数据泄露事件。	☐已实施 ☐部分实施 ☐未实施 ☐不适用
4	贵组织定期进行数据泄露模拟演习，为迅速有效地应对数据泄露做好准备。	☐已实施 ☐部分实施 ☐未实施 ☐不适用
谢绝来电制度		
1	贵组织在向新加坡电话号码发送电话营销信息时遵守谢绝来电(Do Not Call, “DNC”)要求。	☐已实施 ☐部分实施 ☐未实施 ☐不适用
2	贵组织在发送电话营销信息之前，会检查禁止来电 (DNC) 注册表。	☐已实施 ☐部分实施 ☐未实施 ☐不适用
3	贵组织向 禁止来电 注册中心提交检查文件。	☐已实施 ☐部分实施 ☐未实施 ☐不适用
4	贵组织已获得并记录了个人明确无误的同意，可以在不检查 禁止来电注册表的情况下向他们发送电话营销信息。	☐已实施 ☐部分实施 ☐未实施 ☐不适用
5	贵组织确保为电话营销活动聘用的第三方服务提供商遵守 禁止来电 要求。	☐已实施 ☐部分实施 ☐未实施 ☐不适用
内部合规		
1	贵组织已制定并实施了遵守《个人数据保护	☐已实施

	法》 的政策和做法，包括创建数据保护管理计划 (DPMP)。	☐部分实施 ☐未实施 ☐不适用
2	贵组织对所有员工进行个人数据保护政策和做法方面的教育。	☐已实施 ☐部分实施 ☐未实施 ☐不适用
3	贵组织定期审查和更新数据保护政策，并监控合规情况。	☐已实施 ☐部分实施 ☐未实施 ☐不适用
4	贵组织会进行风险和影响评估，以识别和应对数据保护风险。	☐已实施 ☐部分实施 ☐未实施 ☐不适用
5	贵组织将数据保护设计纳入产品、服务、系统或流程。	☐已实施 ☐部分实施 ☐未实施 ☐不适用
数据泄露		
1	贵组织已采取措施监控潜在的数据泄露。	☐已实施 ☐部分实施 ☐未实施 ☐不适用
2	贵组织有应对数据泄露的政策和做法(即人员角色、报告时限和通知流程)。	☐已实施 ☐部分实施 ☐未实施 ☐不适用
3	贵组织已制定了数据泄露管理计划，以解决与个人数据保护相关的数据泄露问题。	☐已实施 ☐部分实施 ☐未实施

		□不适用

6.2. 样本模板(如同意样本或条款样本)

(a) 发送营销材料的同意条款样本 (sampleclausesforobtainingandwithdrawingconsent8may2015.pdf)

(b) 个人数据处理协议数据保护条款指南 (Guide-on-Data-Protection-Clauses-for-Agreements-Relating to-the-Processing-of-Personal-Data-1-Feb-2021.pdf)

(c) 适用于雇员和求职者的条款样本 (Microsoft Word - Sample Clauses and Templates for Employees and Job Applicants - 171017)

请参阅 PDPC | Help and Resources ，了解个人数据保护委员会的完整资料清单。