汉坤法律评述
2023 年 3 月 10 日

HANKUN
汉 坤 律 师 事 务 所
Han Kun Law Offices

汉坤企业出海指南：新加坡数据合规

作者：段志超 | 蔡克蒙 | 蔡诗萌

新加坡作为全球极具竞争力、开放性的经济体，已成为越来越多中国企业的出海首选。整体而言，新加坡当前已建立了较为完善的数据隐私保护法律体系，隐私保护执法也较为活跃，集中在“告知-同意”、数据跨境限制、数据安全保护等方面。中国企业出海在拓展新加坡甚至海外其他区域用户市场、部署服务器、建设数字化运营模式时，需要特别关注新加坡数据隐私合规相关要求，避免触及监管“雷区”。本文旨在简要介绍新加坡数据隐私保护法律框架，聚焦新加坡数据合规热点，以期能帮助出海企业加深对新加坡数据隐私合规要求的了解。

一、监管框架

（一）框架概览

2012 年 10 月，新加坡颁布《个人数据保护法》（Personal Data Protection Act，“**PDPA**”），该法确立了新加坡个人数据保护的基本制度。2020 年 11 月，新加坡对 PDPA 进行了修订，修订版本于 2021 年 2 月 1 日生效，系当前适用版本。《个人数据保护条例》（Personal Data Protection Regulations，“**PDPR**”）作为 PDPA 规定的实施细则，进一步细化个人数据保护的合规要求。

新加坡在 2013 年设立个人数据保护委员会（Personal Data Protection Commission，“**PDPC**”）。PDPC 隶属新加坡信息通信媒体发展局（Info-communications Media Development Authority，“**IMDA**”），负责制定 PDPA 合规指引、监督 PDPA 履行：

1. 在合规指引制定方面，PDPC 当前已颁布《关于 PDPA 关键概念的咨询指南》（Advisory Guidelines on Key Concepts in the PDPA，“**PDPA Guidelines**”）、《关于特定合规话题的 PDPA 咨询指南》（Advisory Guidelines on the Personal Data Protection Act for Selected Topics）、《拒绝来电条款咨询指南》（Advisory Guidelines on the Do Not Call Provisions）等。

2. 在监督 PDPA 履行方面，PDPA 赋予 PDPC 较大的执法权，PDPC 有权对于违反 PDPA 的行为开展执法调查、作出处罚决定，采取的处罚措施包括但不限于：（1）要求处罚对象停止收集、使用或披露违反 PDPA 的相关个人数据；（2）要求处罚对象销毁违反 PDPA 的相关个人数据；（3）对处罚对象最高处以其在新加坡年度营业额的 10%或 100 万新加坡元（以较高者为准）的罚款等。

在违反 PDPA 的责任后果方面，除前述提到行政责任外，PDPA 还规定民事责任和刑事责任。PDPA 第 480 条赋予个人向法院起诉的民事救济权利。例如，在刑事责任方面，对于未经授权故意使用、披露个人数据构成刑事犯罪的，行为人可能面临最高 2 年监禁如 PDPA 以及最高 5,000 新加坡元的罚款。企业通过故意更改、伪造、隐瞒个人数据收集、使用或披露的相关信息以逃避个人访问或更正个人数据的请求，可能面临最高 50,000 新加坡元的罚款，而行为人可能面临最高 12 个月监禁以及最高 5,000 新加坡元的罚款。

（二）适用范围

根据 PDPA 第 2 条、第 3 条，PDPA 既适用于在新加坡收集、使用和披露个人数据的组织，也适用位于新加坡境外或在新加坡境外成立的组织收集、使用和披露新加坡自然人个人数据。因此，出海企业为总部管理需要将新加坡用户个人数据传回中国统一处理，或以新加坡作为出海各国数据集中存储地，将自其他出海目的地收集用户个人数据传输至新加坡处理[1]，均应适用 PDPA。

二、数据隐私合规监管热点

相较于欧盟、中国等个人数据保护规定更为严苛的国家，新加坡在“告知-同意”、“数据本地化与跨境”方面要求稍显宽松。尽管如此，PDPC“告知-同意”、“数据本地化与跨境”、“数据安全保护”、“营销监管”方面执法较为活跃，出海企业如忽视上述方面合规义务则容易触及监管红线。此外，新加坡近年来还逐步加强了信息内容合规监管。

（一）告知-同意要求

根据 PDPA 第 14 条，除 PDPA 规定的豁免同意义务情形以及其他法律要求的个人数据收集、使用和披露情形外，组织收集、使用或披露个人数据原则上应取得个人同意。但 PDPA 允许组织取得个人“视为同意”（Deemed Consent），其规定的“豁免同意义务情形”也较为宽泛，故在“告知-同意”要求方面，PDPA 的要求较 GDPR 更为宽松：

1. “视为同意”情形

根据 PDPA，构成“视为同意”的情形主要如下：

(1) 个人自愿、主动提供：个人自愿为特定目的向组织提供个人数据，且个人自愿提供该信息是合理的，该情况构成“视为同意”。（PDPA 第 15（1）条）

(2) 个人同意（包括视为同意）组织为特定目的向另一组织披露其个人数据，也视为其同意另一组织为该特定目的收集、使用或披露个人数据。（PDPA 第 15（2）条）；

(3) 履行合同所必需：为履行个人与组织之间合同的合理需要，组织可以将个人向其提供的个人数据向另一组织提供，另一组织还可以向后续其他组织进一步披露该个人数据（PDPA 第 15（3）条）；

(4) 通过“通知”：如果组织充分通知个人收集、使用或披露个人数据的目的，且个人未在合理的时间内告知组织其不同意，则也构成“视为同意”。“通知”应符合以下要求（PDPA 第 15A 条）：

[1] 对于以新加坡作为出海各国数据集中存储地，在数据跨境合规义务方面，新加坡规定数据中转行为（in transit），即来自新加坡境外的数据通过新加坡进一步转移至第三方国家或地区过程中的个人数据，该个人数据在新加坡境内未被任何组织访问、使用或披露（传输方或传输方员工访问和使用除外），该类情形被视为已履行数据传输限制义务（PDPR 第 9-10 条）。

- 根据 PDPA 第 15A（5）条和 PDPR 第 14（2）条进行评估，以识别收集、使用或披露个人数据是否会对个人造成不利影响，并采取相应缓释措施；
- 采取合理措施向个人通知该组织拟收集、使用或披露个人数据以及目的；
- 告知个人如何在合理时间内通知该组织其拒绝组织收集、使用或披露个人数据。

须注意的是，对于发送营销信息，组织不能通过“通知”方式取得同意。

2. 豁免“同意”义务

除允许为组织合法利益、个人切身利益（如为生命、健康或安全的紧急情况）、影响公共利益、满足一定条件下的商业资产交易目的等情形豁免组织取得个人的同意的义务，PDPA 允许为商业改进目的收集个人数据，包括（1）为改善、提高或开发商品或服务；（2）改善、提高或开发组织的运营方式或流程；（3）学习和了解该个人主体或其他个人对组织的商品或行为偏好；（4）确定组织提供的商品或服务是否合适该个人主体或其他个人，或为该个人主体或其他个人提供定制化商品或服务（PDPA 附录 1 第 5 部分）。须注意，组织不得以商业改进为由主张使用个人数据发送营销信息。

3. 明确同意、口头同意及告知义务

如个人数据处理活动未能构成“视为同意”、“豁免同意义务”或其他依法收集个人数据的情形，组织应取得个人同意，包括书面等可记录的同意或口头同意。但为便于日后争议举证，PDPC 在其公布的指南中建议企业在取得口头后，再以电子等其他书面方式（如补发邮件）与个人确认，或在特定情况下补充已取得个人口头同意的书面证明作为证据。须注意，对于营销活动，新加坡要求取得个人明确同意。

对于明确同意或口头同意，组织应在取得个人关于收集、使用和对外披露个人数据的同意前向个人告知下述内容（PDPA 第 20 条）：

- 当前或之前个人数据收集、使用和对外披露的目的；
- 之前未告知的个人数据收集、使用和对外披露其他目的；
- 应个人要求，向个人告知说明个人数据收集、使用和对外披露的联系人。

在“告知-同意要求”方面，新加坡已有不少执法案例，主要集中在未经同意开展营销、出售营销线索、未经用户同意公开披露个人数据等方面，故建议企业在利用自身个人数据或自第三方获取个人数据开展营销、向第三方披露或公开披露个人数据时，应特别留意拟开展个人数据处理活动是否满足“告知-同意”要求。

（二）数据本地化与跨境

1. 数据传输限制义务要求

PDPA 未规定数据本地化存储要求，但 PDPA 第 26 条规定了数据跨境传输方面的限制，除非根据 PDPA 相关要求确保接收方对传输的个人数据提供至少与 PDPA 同等的保护，不得将任何个人数据传输到新加坡以外的国家或地区。

须注意的是，上述义务仅适用于“数据传输方”。对于数据接收方，新加坡则通过要求数据传输方确保数据接收方提供“同等保护”，通过数据传输方向数据接收方传导 PDPA 规定的数据保护义务。根据 PDPR 第 10-12 条，新加坡子公司可以通过以下方式履行该义务：

- 接收方受到与 PDPA“同等保护水平”的法律管辖（PDPR 第 11（1）（a）条）；
- 与接收方签订数据处理协议。该数据处理协议应约定接收方履行与 PDPA 同等的保护义务（PDPR 第 11（1）（b）条）；
- 集团内签订具有约束力的公司规则（Binding Corporate Rules，“**BCRs**”），要求集团内数据接收方提供不低于新加坡法的数据保护水平（PDPR 第 11（1）（c）条）；
- 取得个人关于数据跨境的同意或视为同意（PDPR 第 10（2）（a）条、第 10（2）（b）条）；
- 基于个人合法利益（为个人生命健康所必需）或国家利益所需，且传输方已采取合理措施避免该等个人数据被接收方用于其他目的（PDPR 第 10（2）（c）条）；
- 接收方取得特定的数据保护认证。当接收方为数据中介方（Data Intermediary）[2]时，接收方应取得 APEC Privacy Recognition for Processors System（APEC PRP）或 APEC Cross Border Privacy Rules System（APEC CBPR）认证；当接收方为数据中介外的其他组织（如数据控制者）时，该接收方应取得 APEC CBPR 认证（PDPR 第 12 条）。对此，数据出传输方可以登录 APEC 网站（www.cbprs.org）查询数据接收方是否已通过认证。

从实践及 PDPA Guidelines 建议看，对于持续或集团内部传输场景，企业通常采用与接收方签订数据处理协议、BCRs 的方式进行跨境传输。如传输方通过与接收方签订数据处理协议履行数据跨境传输义务，除要求接收方提供与 PDPA 相当水平的保护外，还须注意：

- 协议内容：1）数据传输目的地国/地区；2）如接收方为数据中介（数据处理者）时，该合同还应包括：安全措施、留存期限限制、数据泄漏通知相关内容；以及 3）如接收方为数据中介外的其他主体（数据控制者）时，该协议还应包括：收集、使用和披露的目的、数据准确性要求、安全措施、留存期限限制、数据保护政策、访问权、更正权以及数据泄露通知相关内容（PDPR 第 11（2）（b）条及 PDPA Guidelines）。
- 协议生效条件：该等协议经双方缔约即生效，无需再经新加坡政府审批或备案。新加坡主管部门也尚未像中国这样预先制定数据出境标准合同，因此数据传输方和接收方可自行起草该等数据处理协议。但新加坡作为东盟成员，PDPC 明确承认《东盟跨境数据流动示范合同条款》（ASEAN MCCs）可满足协议要求。因此出海企业在起草数据处理协议时可参考 ASEAN MCCs。

如传输方通过签订 BCRs 履行上述义务，除要求接收方提供与 PDPA 相当水平的保护外，须注意下述事项：

- 适用范围限制：接收方与传输方须存在关联关系，包括传输方与接受方之间存在控制关系或为同一主体所控制（PDPR 第 11（3）（a）条及 PDPA Guidelines）。因此，BCRs 更适合用于集团内数据传输情况；
- BCRs 内容应包含：1）适用 BCRs 的接收方；2）适用 BCRs 的数据传输接收国；以及 3）数据保护权利及义务（PDPR 第 11（3）（b）条）。

如传输方未能与接收方签订数据处理协议或 BCRs，PDPC 在 PDPA Guidelines 中建议，企业可通过取得用户的同意或视为同意的方式履行数据跨境传输的义务。其中，“视为同意”情形包括：1）跨境传

[2] 根据 PDPA 及 PDPA Guidelines 的定义，“数据中介”为代表数据传输方并为其目的处理个人数据的主体。

输为履行合同所必需：如基于该事由跨境传输数据，接收方可基于履行合同所必需向第三方再传输数据；2）用户主动提供个人数据或虽未主动提供但允许个人数据被收集使用。无论是取得同意或“视为同意”情形，传输方均须履行以下义务：

- 告知义务：在请求个人同意前，传输方应向数据主体提供书面概要说明，告知其数据接收国对数据的保护措施，以及该保护水平不低于 PDPA（PDPR 第 10（3）（a）条）；
- 手段正当性：传输方不得以任何欺骗性或诱导性方式获得该同意（PDPR 第 10（3）（c）条）；
- 禁止捆绑同意：除非跨境传输为提供服务/产品合理所必需，传输方不得以该同意作为提供服务/产品的前提（PDPR 第 10（3）（b）条）。

2. 典型案例简介

尽管新加坡已有较为明晰的数据跨境规定，但在实操中仍存在不少模糊之处。例如，新加坡主体在使用中国境内母公司统一采购的境外供应商系统时，涉及向境外供应商跨境传输个人数据，中国境内母公司与境外供应商签订的采购协议中已约定数据跨境传输条款，能否视为新加坡主体已通过签订数据处理协议的方式履行数据跨境传输义务？PDPC 在去年做出的“某澳大利亚物流公司新加坡主体违反跨境传输限制义务案”处罚决定中对该问题作出了回答：

(1) 事实概要

2013 年 7 月，为集团员工统一管理的需要，某澳大利亚物流公司（以下简称“**T 母公司**”）采购爱尔兰的一家 HR 系统，包括其新加坡主体（以下简称“**T 新加坡主体**”）在内的全球各地子公司均将其员工个人数据上传至该系统内。该系统数据存储在欧盟境内。2020 年 11 月，因 T 母公司向 PDPC 报告集团 IT 系统（含新加坡服务器）数据泄露的情况，PDPC 随即针对 T 新加坡主体 PDPA 义务履行情况开展调查。

(2) PDPC 调查结果及处罚决定

PDPC 调查发现，T 新加坡主体在向第三方 HR 系统上传员工个人数据时违反 PDPA 第 26 条数据传输限制义务，须追究 T 新加坡主体该方面的责任。PDPC 理由为：

- T 新加坡主体作为数据传输方应履行 PDPA 第 26 条规定的数据跨境传输义务，包括但不限于通过签署数据处理协议的方式进行；
- 尽管 HR 系统采购协议已约定该系统供应商的数据保护义务，但该协议签署主体为 T 母公司和 HR 系统供应商，不包括 T 新加坡主体。因此，T 新加坡主体不能以该采购协议主张其已通过签署数据处理条款的方式履行数据跨境传输义务；
- 根据集团各主体签署的企业服务协议（“**CSAs**”），1）尽管 CSAs 约定了 T 母公司负责向集团各子公司提供 IT 政策、策略以及技术支持服务，也授权 T 母公司聘用第三方供应商，但排除 T 母公司负责 IT 设备的运营和维护工作；2）CSAs 也未约定 T 母公司代集团各子公司行使相关数据保护义务。基于上述两点安排，新加坡服务器所涉的相关数据保护义务实际仍由 T 新加坡主体自行承担。

T 新加坡主体作为相关数据保护义务承担者，未通过签署数据处理条款等方式履行数据跨境传输义务，违反了 PDPA 第 26 条。PDPC 考虑到违反 PDPA 的行为未造成任何实质损害，T 母公司也与新加坡主体补签《新加坡数据跨境传输协议》，故仅对 T 新加坡主体作出警告的处罚。

(3) 合规启示

从 PDPC 处罚决定看，对于向总部统一采购的供应商等第三方跨境传输数据，PDPC 并非强制要求新加坡主体与第三方另行签订数据处理协议，而是允许新加坡主体通过与母公司签订协议明确双方关于数据跨境传输、保护的权利义务，授权母公司代集团各子公司集中履行相关数据跨境传输、保护义务，以形成义务履行的链条。

因此，我们建议企业在出海过程中应特别注意，1）通过签订数据处理协议明确母公司与新加坡主体之间关于数据保护权利义务的分配。如数据跨境、数据保护义务仍由新加坡主体履行，则应由新加坡主体与个人数据接收方签署数据跨境传输协议，履行数据跨境传输限制义务。2）考虑到发生数据泄露事件很可能触发 PDPC 对组织 PDPA 义务履行情况的全面调查，母公司和新加坡主体应采取数据安全管理措施，在集团、当地主体及接收数据的供应商等第三方确保数据安全，避免数据泄露事件发生，下一节我们将就如何履行数据安全保护义务进一步展开介绍。

（三）数据安全保护

PDPA 第 24 条要求组织应采取合理措施避免 1）数据被未经授权访问、收集、使用、披露、复制、修改、处置等类似风险；2）存储个人数据的存储介质或设备丢失。根据 PDPC 发布的指引，当前没有统一的数据保护方案，每个组织应根据个人数据性质（是否为敏感个人数据）、个人数据泄露对个人的影响等因素综合制定数据保护方案。PDPC 建议组织可以采取以下措施，包括 1）综合考虑上述因素制定数据安全保护方案，包括物理措施、技术措施及管理措施；2）设置数据安全保护专业人员；3）制定内部制度和操作流程，分级保护个人数据；3）能够快速、有效应对信息安全事件；4）综合考虑组织规定、个人数据规模和类型、有权访问个人数据的内部人员、是否委托第三方处理个人数据开展风险评估，以确定相关数据保护方案是否重组。须注意，数据安全保护仍是 PDPC 执法较为活跃的领域，且可能因发生数据泄露事件而引发对其他义务履行情况的调查，建议出海企业根据自身情况采取数据安全保护措施，避免数据泄露事件发生。

如发生数据泄露事件，且相关事件根据 PDPA 第 26B 条构成应告知的信息泄露事件（Notifiable Data Breach）[3]，则组织应在发现该事件可告知后的 3 个工作日内向 PDPC 告知；如果数据泄露导致或可能导致对受影响个人的重大伤害，组织必须在通知 PDPC 时或之后通知受影响个人，以便 PDPC 在收到通知后能够协助受影响个人。

（四）营销监管

1. 取得明确同意

如“告知-同意”部分介绍，PDPA 要求利用个人数据开展营销活动应取得个人明确同意。因此，无论是利用个人电话号码开展电话营销、短信营销，或利用个人邮箱地址开展邮件营销，均需告知个人营销活动，并取得个人明确同意。

[3] PDPA 第 26B 条规定了“应告知的信息泄露事件”，包括：（1）某些类别的个人数据发生泄露，导致或可能导致受影响的个人受到重大伤害：个人的全名或别名或身份证号码，以及 PDPA 附表第 1 部分所列的与个人有关的任何个人数据或个人数据类别，以及附表第 2 部分规定了各种金融、保健、保险、儿童和残疾人以及其他数据类别（如私人加密密钥）；或（2）个人的银行或金融公司账户标识符，如账户名称或号码，与任何密码、安全代码、访问代码、对安全问题的答复、生物识别信息或个人用于访问账户的其他数据相结合。（3）影响到 500 名或更多个人的个人数据，具有或可能具有很大的规模。

2. “拒绝来电”制度

如涉及电话营销、短信营销，在询问个人是否同意接收营销信息前，出海企业还应查阅电话号码是否已在“拒绝来电”登记簿（Do Not Call Registry，以下简称“**DNC 登记簿**”）中登记。如已在“拒绝来电”登记簿中登记，组织不得向其拨打营销电话、发送营销短信。但如果构成下述情形，可豁免组织查阅 DNC 登记簿的义务，主要包括 1）为完成或确认交易所必需，且个人已事先同意该交易；2）提供产品召回信息、或与产品或服务有关的安全或保障信息；3）向个人提供事前合同约定的个人有权获得的产品和服务，包括产品更新。4）组织与用户存在持续关系（Ongoing Relationship）[4]并且发送的营销信息仅与此持续关系有关；5）为开展市场调查；6）个人以书面或其他形式明确同意公司发送营销信息；7）B2B 市场推广的目的。

3. 营销信息内容

在发送营销消息时，营销消息应提供发送或被授权发送营销信息的公司信息以及其联系方式，并同步提供退订机制。

（五）信息内容监管

在信息内容监管方面，新加坡早年发布的《互联网业务准则（Internet Code of Practice）》以及《防止网络假信息和网络操纵法案》（Protection from Online Falsehoods and Manipulation Act）、《防止骚扰法》（Protection From Harassment Act）规定互联网信息内容审查义务以及违禁内容范围，以防范违禁内容传播以及在线危害（如虚假信息的传播、人肉搜索情形）的发生。

2023 年 2 月 1 日生效的《在线安全法案（修正版）》（Online Safety （Miscellaneous Amendments）Bill）旨在进一步加强在线通信服务的信息内容监管。该法案适用于位于新加坡境内外、新加坡用户能够通过互联网访问或通过互联网向新加坡用户提供内容的任何在线通信服务。具体适用的在线通信服务类型将在该法案附录 4 中列明，当前仅社交媒体服务被列入在内，未来适用服务类型将进一步增加。该法案规定自杀或自残、身体暴力或性暴力、恐怖主义以及挑拨新加坡种族和宗教矛盾等内容属于“恶劣内容”（Egregious Content）。如发现存在恶劣内容，IMDA 作为主管部门有权要求在线通信服务提供者下架、删除内容，如在线通信服务提供者违反 IMDA 指令，可能面临最高 100 万新加坡元的罚款。此外，为配合法案落地，新加坡预计发布《在线安全业务守则》（the Code of Practice for Online Safety）、《社交媒体服务内容守则》（the Content Code for Social Media Services）两项守则，从而进一步细化信息内容审查要求及流程，建议相关出海企业关注立法进展。

三、小结

总体而言，新加坡采较为宽松的数据合规政策，为中国企业出海提供更大的便利及发展空间。在未来可预期的一段时间里，新加坡仍然是中国企业出海的热门国家。但新加坡主管部门活跃的执法也提醒出海企业严格审查自身数据合规情况。因此，我们建议出海企业对标相关规定搭建、完善数据隐私合规体系。

敬请注意，本指南中涉及境外的内容，系我们根据境外当地公开可查的法律法规、案例、文件和报道，及我们的实践经验制作，不代表我们有资质就该等资料进行审查，本指南不构成我们的任何法律意见。

[4] 根据 PDPA 附录 8 第 1（2）条持续关系指发送人与接收人之间因发送人经营或进行某项业务或活动（商业或其他）而产生的持续关系。

特别声明

汉坤律师事务所编写《汉坤法律评述》的目的仅为帮助客户及时了解中国或其他相关司法管辖区法律及实务的最新动态和发展，仅供参考，不应被视为任何意义上的法律意见或法律依据。

如您对本期《汉坤法律评述》内容有任何问题或建议，请与汉坤律师事务所以下人员联系：

段志超

电话： +86 10 8516 4123
Email： kevin.duan@hankunlaw.com

蔡克蒙

电话： +86 10 8516 4289
Email： kemeng.cai@hankunlaw.com