君合专题研究报告

2024 年 8 月 28 日

中国企业出海之数据合规

—— 东南亚系列（二）：马来西亚、印度尼西亚

近几年来，我国将东盟国家作为周边外交的优先方向和高质量共建“一带一路”的重点地区。中国同东盟国家在各类经济领域的多方面合作已经成为亚太地区经济区域协作的重要典范。据官方发布的文件显示，中国同东盟国家在基础设施联通、区域经济贸易、数字经济伙伴关系等多方面都正在取得积极的合作成果[1]。在此背景下，中国企业向东南亚各国开展各类出海业务的经济活动显著增多，当这些经济活动涉及开展个人数据处理活动，就不得不考虑如何遵守当地数据保护相关法律和监管的要求，规避跨国经营中的数据合规风险。鉴于此，我们初步选取东南亚地区的四个国家：泰国、越南、马来西亚和印度尼西亚进行研究，希望通过对这些国家的数据合规制度和实践的分析讨论，为中国企业开展出海业务提供数据合规指引方向。

《中国企业出海之数据合规—— 东南亚系列（一）：泰国、越南》一文主要介绍了泰国和越南的数据合规制度及实践，本文将聚焦于**马来西亚**和**印度尼西亚**。

一、概述

马来西亚在个人数据保护方面的综合性法律文件为 2010 年颁布并于 2013 年正式生效的《个人数据保护法》（Personal Data Protection Act，以下简称“**马来西亚 PDPA**”）。此外，马来西亚还陆续颁布多项配套规定，包括 2013 年颁布的《个人数据保护条例》（Personal Data Protection Regulations，以下简称“**马来西亚 PDPR**”）、《个人数据保护（数据使用者类别）指令》、《个人数据保护（数据使用者注册）条例》、《个人数据保护（费用）条例》，2015 年颁布的《个人数据保护标准》，2016 年颁布的《个人数据保护（数据使用者类别）（修订）指令》、《个人数据保护（复合犯罪）条例》，2021 年颁布的《个人数据保护（上诉仲裁庭）条例》等。这些法律法规、指南与通信、银行和金融、保险、酒店等行业的相关立法以及相应的司法判例共同构成了马来西亚的个人数据保护法律体系。

印度尼西亚在在个人数据保护方面的综合性法律文件为 2022 年颁布的《个人数据保护法》（Law No.27 of 2022 regarding Personal Data Protection，以下简称“**印尼 PDPL**”）。印尼政府也正在为该法的实施制定配套制度文件，并已于 2023 年颁布了《个

[1] 参见推进“一带一路”建设工作领导小组办公室发布的《中国—东盟国家 共建“一带一路”发展报告》，https://www.yidaiyilu.gov.cn/a/icmp/2023/12/15/20231215179983118/c720a536a9494c1bb107420dbedacb40.pdf

人数据保护法实施条例草案》（the Draft of the Government Regulation of 2023 regarding the Implementation of Law Number 27 of 2022 regarding Personal Data Protection，以下简称“**实施条例草案**”）。值得一提的是，在印尼 PDPL 颁布前，印尼主要以《电子信息及交易法》（Law No. 11 of 2008 on Electronic Information and Transactions）及其实施条例《2019 年关于实施电子信息及交易法的第 71 号政府条例》（Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions）、《2016 年关于电子系统中个人数据保护的第 29 号条例》（Regulation No. 20 of 2016 on Personal Data Protection in Electronic System）三部法律文件形成数据保护法律框架。这三部法律目前在不与印尼 PDPL 相抵触的情况下仍然有效。由于印尼 PDPL 在前述法律基础上加强了数据保护力度，保护范围也更全面，因此本文将着重围绕印尼 PDPL 展开对印尼数据保护法律制度的介绍。

下文将从个人数据保护法的适用范围和重要定义、个人数据处理的合法性基础、告知同意的要求、数据主体权利、数据控制者和处理者的义务、跨境转移规则、数据保护影响评估（简称“**DPIA**”）、数据保护官（简称“**DPO**”）的任命要求等方面对两国的法律法规要求展开对比分析，旨在回应企业出海过程中普遍关注的个人数据保护要求，对企业出海业务的开展提供指引。

二、个人数据保护法的适用范围

(一) 马来西亚 PDPA 的适用范围

马来西亚 PDPA 第 2 条与第 3 条分别从正反两方面明确了 PDPA 的适用范围。根据马来西亚 PDPA 第 2 条，该法适用于商业交易中处理（处理包括使用、传播、收集、记录和/或存储）或控制个人数据处理的任何主体，如果（1）该主体在马来西亚设立且个人数据是由该主体或该主体雇佣、聘用的任何其他主体进行处理的；或（2）该主体并未在马来西亚设立，但使用马来西亚的设备处理个人数据且此种处理的目的并非仅从马来西亚过境。而第 3 条和第 45 条则明确马来西亚 PDPA 不适用的场景，包括不适用于（1）联邦政府和州政府；（2）在马来西亚境外处理的个人数据且该个人数据并不打算在马来西亚进一步处理；（3）出于个人、家庭或家庭事务，包括娱乐目的而处理的个人数据。

从条文的规定可以看出，马来西亚 PDPA 对适用范围规定的较为细致，在主体上排除了对联邦政府和州政府的适用，在内容方面则排除了对未在马来西亚境内设立的主体仅出于在马来西亚过境的目的而进行的个人数据处理活动、在马来西亚境外处理个人数据且该数据不会进一步在马来西亚处理以及出于个人、家庭或家庭事务处理个人数据的三种情形的适用。因此，企业出海马来西亚可以根据自身出海的模式判断是否会受到马来西亚 PDPA 的约束。

(二) 印尼 PDPL 的适用范围

印尼 PDPL 第 2 条规定其适用于在印尼境内处理个人数据的任何个人、企业、公共机构和国际组织，如果数据处理主体（1）位于印尼境内；或（2）位于印尼境外，但个人数据处理行为对印尼或位于印尼境外的印尼个人数据主体会产生法律上的效果。该条款也同时明确其不适用于个人基于个人或家庭活动而开展的个人数据处理行为。

印尼 PDPL 对于适用范围的表述采用了“产生法律上的效果”这一较为笼统的表述，扩大了其域外效力范围，为立法者与执法者留下了较大的解释空间。因此，企业出海印度尼西亚应当格外留意有关机关对于“产生法律上的效果”的解释，从而判断其业务场景是否将受到印尼 PDPL 的约束。

(三) 重要定义

个人数据保护领域有一些普遍但重要的定义，该等定义对于企业如何开展个人数据保护工作有较大的影响。据此，我们对马来西亚 PDPA 和印尼 PDPL 中重要概念/术语的定义，做了如下对比。

(1) 个人数据

在个人数据的定义方面，马来西亚 PDPA 与印尼 PDPL 的规定较为类似，均指能够直接或间接与个人相关联并识别具体个人的信息。但马来西亚 PDPA 还额外强调了个人数据必须是与商业交易相关，且通过设备自动化操作进行处理并作为相关归档系统的一部分进行记录或打算将其作为相关归档系统的一部分的信息。

(2) 敏感个人数据

在敏感个人数据的定义方面，马来西亚 PDPA 和印尼 PDPL 均采用列举方式明确其定义。马来西亚 PDPA 规定敏感个人数据是指数据主体的身体、精神健康状况信息、政治观点、宗教信仰或性质相似的其他信仰、所犯或被指控犯下的任何罪行信息的个人数据，或负责个人信息保护部门的部长通过在《政府公报》上发布的命令确定的任何其他个人数据。马来西亚 PDPA 没有对健康数据、生物识别数据进行特别说明，但通常这类数据与数据主体的身体、精神健康状况相关，因此也落入敏感个人数据的范畴。

印尼 PDPL 则采用“特定个人数据”表示敏感个人数据，并规定其包括：健康相关的数据和信息、生物识别数据、遗传数据、犯罪记录、儿童数据、个人财务数据及相关法律法规规定的任何其他数据。

(3) 其他

除了个人数据与敏感个人数据之外，值得注意的是马来西亚 PDPA 没有采用数据控制者（data controller）的概念，而是采用了数据使用者（data user）的概念，但其定义与数据控制者较为类似，为单独或与他人联合或共同处理任何个人数据或控制或授权处理任何个人数据的主体，但不包括数据处理者。下文马来西亚部分将采用“数据使用者”这一术语。

三、处理个人数据的合法性基础及告知同意的要求

(1) 合法性基础

基于对个人数据的保护，全球各国基本都规定处理个人数据必须具备合法性基础。除了“获取数据主体的同意”之外，还存在为签订和履行与数据主体的合同所必须、为履行法定职责或法定义务所必须、数据主体的切身利益等合法性基础。

马来西亚原则上要求处理个人数据必须获得数据主体的同意，但是也提供了同意之外的其他合法性基础，包括为签订和履行与数据主体的合同所必须、遵守数据使用者的法定义务、保护数据主体的切身利益、司法行政、行使法律职能。印尼原则上也要求处理个人数据必须获得数据主体的同意，但也同样提供了同意之外的其他合法性基础，包括履行与数据主体的合同所必须、遵守数据控制者的法定义务、保护数据主体的切身利益、公共利益、合法利益。

值得注意的是，虽然“数据主体的同意”并非唯一的合法性基础，但其仍然在个人数据处理过程中起到重要作用。马来西亚与印尼两国均对告知和同意提出了严格的要求。

(2) 马来西亚有关告知同意的具体要求

在告知要求方面，马来西亚 PDPA 第 7 条对告知原则作出了规定，该原则要求数据使用者向数据主体告知与其正在或即将被处理的个人数据相关的各种事项。其具体规定为，数据使用者应当通过书面形式告知数据主体：

- 数据主体的个人数据正在或即将由数据使用者或其代表处理，并应向该数据主体提供对这部分个人数据的描述；
- 收集或将要收集与进一步处理个人数据的目的；
- 数据使用者所知的该个人数据来源的任何信息；
- 数据主体请求访问和更正个人数据的权利，以及如何就个人数据向数据使用者咨询或投诉；
- 数据使用者向其披露或可能向其披露个人数据的第三方类别；
- 数据使用者提供给数据主体的限制个人数据处理的选择和手段，包括可能从中识别出的其他人的个人数据；
- 数据主体提供个人数据是强制性还是自愿性的；
- 如果数据主体提供个人数据是强制性的要求，数据主体不提供个人数据会导致的后果。

此外，马来西亚 PDPA 第 7 条还对通知的时间作出规定，即“尽快提供”。具体而言，数据使用者向数据主体提供前述通知的时间应当为：

- 当数据使用者首次要求数据主体提供其个人数据时；
- 当数据使用者首次收集数据主体的个人数据时；或
- 在任何其他情况下，在数据使用者：
  a) 将数据主体的个人数据用于与收集个人数据目的不同的其他目的之前；或
  b) 向第三方披露个人数据之前。

同时，在通知的形式上，马来西亚个人数据保护部门（Department of Personal Data Protection）2022 年发布的《准备个人数据保护通知指南》还要求数据使用者同时提供通知的马来语及英语版本，并应当向个人提供清晰且易于获取的方式行使选择权。

在同意方面，马来西亚 PDPA 第 6 条原则性地规定了除非符合其他规定，否则数据使用者必须就处理个人数据获得数据主体的同意。马来西亚 PDPR 第 3 条则进一步明确获取数据主体的同意需要满足如下要求：

- 数据使用者获取数据主体同意的形式可以是任何数据使用者能够妥善记录并保存数据主体同意的形式；
- 如果该作出同意的形式同时涉及其他事项，而非仅涉及个人数据的处理，获取同意的要求应当在其表面上能与其他事项显著区分。

(3) 印度尼西亚有关告知同意的要求

印尼 PDPL 第 21、22 条对数据主体的同意和数据控制者的告知义务作出了规定。

在告知义务方面，印尼 PDPL 第 21 条规定，如果数据控制者处理个人数据的合法性基础为数据主体的同意，则应当向数据主体提供如下的信息：

- 处理个人数据的合法性；
- 处理个人数据的目的；
- 将被处理的个人数据的类型和相关性；
- 包含个人数据的文件的存储期限；
- 收集信息的详细情况；
- 个人数据处理的期限；

- 数据主体的权利。

同时，如果上述信息发生变化，数据控制者应当在上述信息变化之前通知数据主体。

关于数据主体的同意必须满足以下要求：

- 同意应当以书面或可记录的形式作出，包括电子与非电子的形式，且不同形式具备同等的法律效力；
- 如果该作出同意的形式同时涉及其他事项，则应当：
  a) 将获取同意的请求与其他事项进行清楚显著的区分；
  b) 采用易于理解和访问的形式；
  c) 使用简单明了的语言。

四、数据主体的权利

马来西亚 PDPA 与印尼 PDPL 赋予数据主体的个人数据权利类型均涵盖了查阅复制权、更正权、删除权、撤回同意的权利、限制处理的权利、反对权。然而印尼还规定了数据主体享有数据可携带权以及反对自动化决策权，马来西亚 PDPA 则未包含该等权利。除此之外，不同于主流体系的数据主体权利，马来西亚 PDPA 还赋予了数据主体一项独特的权利，即防止可能造成损害或困扰的处理的权利（Right to prevent processing likely to cause damage or distress），该权利允许数据主体随时以书面形式通知数据使用者，要求数据使用者在合理期限内停止或不开始为特定目的处理个人数据或以特定方式处理个人数据，如果数据主体主张（1）该个人数据的处理或为特定目的或以特定方式处理个人数据正在造成或可能造成对数据主体或另一个人的重大损害或重大困扰；且（2）该损害或困扰是或将是不合理的。该权利赋予了数据主体一定程度的反对权和限制处理权，虽然此种权利的行使存在限制，但相较于 GDPR 中限制处理权的行使条件（如个人数据不准确、数据处理是非法的等），该权利行使的条件较不明确，可能会为企业带来较多基于该权利的权利行使请求，增加一定合规负担。因此，企业应当留意该权利并对其在运营上进行针对性的准备。

在数据主体请求响应的时间要求方面，马来西亚 PDPA 要求数据使用者在收到相关权利请求的 21 天内完成响应。而印尼 PDPL 则要求数据控制者在收到相关权利请求之后的 72 小时内响应。

五、数据控制者和处理者的权利义务

企业作为数据控制者与数据处理者两种不同的数据处理角色时，需要承担的义务也是不同的。马来西亚与印尼对于两种数据处理角色所需承担义务的规定如下：

在一般义务方面，两国均规定由数据控制者（马来西亚 PDPA 下称“数据使用者”）落实告知同意的要求、确保个人数据处理存在合法性基础、处理目的合法正当、确保个人数据完整、准确、并采取适当的组织和技术措施保障个人数据的安全。而数据处理者主要是在数据安全方面履行数据保护义务并配合数据控制者履行相关法律义务。印尼 PDPL 还额外要求，无论是数据控制者还是数据处理者均应履行个人数据处理活动记录义务。

在具体义务方面，数据控制者和数据处理者承担的义务也存在显著差异：

(1) 响应数据主体的权利请求：马来西亚与印尼均规定应当由数据控制者在规定时间内响应数据主体的个人权利请求，而未对数据处理者的义务作出要求。

(2) 发生数据泄露等安全事件时的通知：马来西亚未对此种情况下的通知义务作出规定。而印尼 PDPL 则仅规定由数据控制者

在发生数据泄露时书面通知监管机构和受影响的个人，但没有明确数据处理者在此种情形下的义务。

(3) DPIA：马来西亚 PDPA 没有对开展 DPIA 作出具体要求，而印尼 PDPL 则仅要求数据控制者必须在法定情形下开展 DPIA。

(4) 数据跨境转移：两国均要求由数据控制者履行作为数据对外传输方的合规义务，而数据处理者仅可能作为数据的接收方存在。印尼 PDPL 还额外明确数据控制者同样可能作为个人数据境外接收方并应当履行相应的合规义务。

企业出海拓展业务时，应当先判断在不同场景下自身的数据处理角色，即是属于能够自主决定处理个人数据的目的与方式的数据控制者（数据使用者），还是代表数据控制者根据其指令开展个人数据处理活动的数据处理者。不同角色所需要承担的法律义务与法律责任大不相同，只有明确了数据处理角色，方才能确定自身的法律义务。

六、数据跨境转移规则

(一) 马来西亚

马来西亚 PDPA 由于颁布时间较早，与目前主流的 GDPR 中的数据跨境转移规则有些许差异。马来西亚 PDPA 第 129 条规定，原则上数据使用者不得将数据主体的任何个人数据转移到马来西亚境外，除非：

（1） **发布于公报上的国家**：转移至通信与多媒体部部长根据专员的建议发布在公报上的国家（即白名单国家）。这些国家应当：

a) 存在一部与马来西亚 PDPA 在实质上相似的法律，或该法律服务于与马来西亚 PDPA 相同的目的；或

b) 在个人数据处理方面至少提供与马来西亚 PDPA 相当的充分保护。

（2） **符合法定的例外情形。**这些例外情况具体包括：（i）数据主体同意该转移；（ii）该转移对于数据主体和数据使用者之间的合同履行是必要的；（iii）该转移对于数据使用者与第三人之间的合同的订立或履行是必要的，如果该合同是应数据主体的请求而订立的或该合同是为了数据主体的利益；（iv）该转移是出于法律程序的目的，或为了获取法律意见，或为了确立、行使或维护法律权利；（v）数据使用者有合理的理由相信，该转移是为了避免或减轻对数据主体的不利行动且在事实上无法获得数据主体的书面同意，如果获取同意是可行的，数据主体一定会作出书面同意；（vi）数据使用者已经采取了所有合理的预防措施，并行使了应有的勤勉，以确保个人数据在该国的处理方式置于马来西亚也不会违反本法的要求；（vii）该转移是为了保护数据主体的切身利益；（viii）此种转移对于在通信与多媒体部部长确定的符合公共利益的情况而言是必须的。

2017 年，马来西亚个人数据保护委员发布了《个人数据保护（向马来西亚以外的地区转移个人数据）令》草案，其中规定数据使用者将无需依赖数据主体的同意或马来西亚 PDPA 规定的例外情况，即可将个人数据转移到白名单所列的地区（包含中国）。然而，该草案截至目前尚未通过。企业如果出海马来西亚，可以密切关注相关立法的进展以决定企业应当在数据跨境转移方面采取的措施。

(二) 印度尼西亚

印尼 PDPL 的数据跨境转移规则与 GDPR 较为相似，要求数据控制者在向印尼以外的国家或地区转移任何个人数据之前，应首先确保该等数据转移具有以下任一合法依据：

（1） **充分的保护水平**。接收个人数据的数据控制者和/或处理者的注册地所在国应当提供等同于或高于印尼 PDPL 规定的数据保护水平。考虑是否具有同等数据保护水平的判断标准包括：是否制定个人数据保护法、是否存在个人数据保护监管部门或机构、是否已通过国际条约或其他法律文件作出国际性承诺或约定其他义务；是否已加入相关的个人数据保护多边性或区域性的体系等。目前尚未发布被认定具有充分保护水平的国家/地区的名单。

（2） **足够且有约束力的个人数据保护**。数据控制者应当确保提供了足够且具有约束力的个人数据保障措施。此类个人数据保障措施包括：数据传输方与数据接收方之间的国际条约、个人数据保护标准合同条款、具有约束力的集团政策、个人数据保护监管机构认为是充分且具有约束力的其他文书。

（3） **数据主体的同意**。数据控制者应当就该数据跨境转移获得数据主体的同意。

需要注意的是，这三种数据跨境转移的法律依据的适用存在先后顺序，只有在前一种法律依据不存在的情况下，才应当考虑是否符合后一种法律依据。

七、DPIA

在 DPIA 方面，马来西亚 PDPA 并未对其作出具体规定。

印尼 PDPL 则规定，如果个人数据处理对个人数据主体构成高潜在风险，数据控制者应当开展 DPIA。具有高潜在风险的个人数据处理行为包括：（1）对数据主体产生法律效果或重大影响的自动化决策；（2）特定个人数据的处理；（3）大规模个人数据的处理；（4）为了系统评估、打分或监控数据主体而处理个人数据；（5）为了匹配或组合一组数据的活动而处理个人数据；（6）使用新技术处理个人数据；和/或（7）限制数据主体权利行使的个人数据处理。同时，实施条例草案则进一步要求 DPIA 必须存在文件记录，且应当包含：对个人数据处理活动和处理目的进行系统性描述（包括数据控制者的利益）、对于个人数据处理活动与处理目的之间的必要性及相称性进行评估、为保护数据主体的权利而进行的风险评估、数据控制者为保护数据主体免受个人数据处理风险而采取的措施。此外，数据控制者还应当在个人数据处理风险发生变化时重新开展评估。

八、组织内设置 DPO 的要求

关于在企业组织内设置 DPO 的要求，马来西亚 PDPA 并未作出相关规定。但 2020 年马来西亚发布的 Public Consultation Paper No. 01/2020 中就是否需要引入数据使用者任命 DPO 的法律义务向社会征求意见。但截至目前，马来西亚尚未发布正式法律文件，故指定 DPO 在马来西亚并非强制义务。

印尼则对指定 DPO 的义务作出了要求，规定如下：

(1) 触发任命的情形：

印尼 PDPL 规定，在以下情况下，数据控制者和数据处理者必须指定一名 DPO：

- 为公共利益处理个人数据；

- 数据控制者主要活动的性质、范围和/或目的需要定期、系统性地监控大规模的个人数据；
- 数据控制者的核心处理活动包括进行大规模的特殊处理和/或进行与犯罪行为有关的处理。

(2) 资质和岗位要求：

指定 DPO 时，应当考虑其是否具有个人数据保护方面的专业水平、相应法律知识、个人数据保护实践经验以及履行任务的能力。DPO 可以是内部员工，也可以从外部聘任。

(3) 职责要求：

DPO 应当履行如下义务：

- 为遵守数据保护法律法规向数据控制者或数据处理者履行告知义务并提供建议；
- 监督并确保数据控制者或数据处理者遵守可适用的数据保护法律法规及相关政策；
- 就 DPIA 提供建议，并监督数据控制者和数据处理者的表现；
- 协调并担任与个人数据处理相关事宜的联络人；
- 向数据控制者负责个人数据处理安全的部门、负责人或各方提出建议和意见，以确保个人数据处理安全符合法律法规的规定；
- 作出必要努力以确保负责个人数据处理安全的部门、负责人或各方考虑到对数据主体的权利和自由而采取相关技术和实施措施；以及
- 在评估负责个人数据处理安全的部门、负责人或各方是否已经考虑到对数据主体的权利和自由而采取相关技术和实施措施后，向董事会、个人数据保护监管机构报告相关情况。

企业如希望在印度尼西亚设立公司实体，应当关注该国关于数据合规管理人员或组织的任命要求，并密切关注后续具体实施条例的发布。对于希望在马来西亚设立公司实体的中国企业而言，虽然马来西亚目前没有强制要求企业指定 DPO，但极有可能马来西亚未来对 PDPA 进行修订时便会加入相关条款。同时，从最佳实践的角度出发，我们建议企业无论是否触发强制任命 DPO 的情形，均应任命一名 DPO 以应对数据保护合规的需求。

董　潇　合伙人　电话：86-10 8519 1718　邮箱地址：dongx@junhe.com
陆斯珮　合伙人　电话：86-21 2208 6250　邮箱地址：lusp@junhe.com
沈佳旖　律　师　电话：86-21 2283 8228　邮箱地址：shenjy@junhe.com