君合专题研究报告 JUNHE

2024 年 8 月 21 日

中国企业出海之数据合规——东南亚系列（一）：泰国、越南

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。本文将首先聚焦于**泰国**和**越南**。

一、概述

泰国有关个人数据保护的综合性法律是于 2019 年 5 月颁布，2022 年 6 月 1 日才正式全面生效的《个人数据保护法》（Personal Data Protection Act，简称“**泰国 PDPA**”）。随后，泰国的个人数据保护监管机构——泰国个人数据保护委员会（Personal Data Protection Committee，简称“**泰国 PDPC**”）又陆续发布了相关的通知、指南文件，就个人数据保护方面的规定进行了补充，构成了泰国个人数据保护方面的规则体系。从内容上看，泰国 PDPA 广泛参考了欧盟《通用数据保护条例》（General Data Protection Regulation，简称“**GDPR**”），借鉴了 GDPR 的许多重要概念。尽管如此，泰国 PDPA 也有区别于 GDPR 的特殊方面。

越南关于个人数据保护的综合性法律是 2023 年 7 月 1 日正式生效的《个人数据保护法令》（Decree on the Protection of Personal Data，简称“**越南 PDPD**”），在此之前有关个人数据保护的规定散落在不同的法律法规中，例如网络安全法、消费者权利保护法、网络信息安全法、IT 法案、电子交易法等。除越南 PDPD 外，越南也颁布过一些法令，对网络安全法的解读、互联网服务及在线信息的管理、提供和使用等方面做出补充规定。其中，部分法令曾引起广泛讨论，例如《第 53/2022/ND-CP 号法令》（Decree No. 53/2022/ND-CP of the Government dated 15 August 2022 elaborating a number of articles of the Law on Cybersecurity of Vietnam，简称“**《第 53 号法令》**”）对特定数据与实体提出了数据本地

[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

化要求，引起企业广泛关注。2024 年 2 月 29 日，越南公安部宣布计划制定新的《个人数据保护法》（Law on Personal Data Protection），旨在建立更强大的个人数据保护框架和法规，保证个人数据的安全管理、处理和使用，也承诺将解决越南 PDPD 等现行法规与其他有关个人数据保护的法律之间的冲突。但相关方也表示新的《个人数据保护法》的起草和发布可能是一个漫长的过程，需要至少两到三年的时间。

除了上述提及的有关个人数据保护的主要法律法规，与其他大多数国家/地区的数据保护立法体系类似，泰国和越南在各个领域/行业（例如医疗、金融、科技等）也会发布与该领域/行业相关的个人数据保护的特殊规则。企业在评估个人数据合规要求时也需要审慎考虑其所在领域/行业的特殊要求，特别是隶属于监管相对严格的行业，或其处理的数据相对敏感时，需特别注意。

为帮助企业更系统地理解泰国、越南在个人数据保护方面的重要规则，下文我们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权利义务、数据本地化及跨境转移规则、数据保护影响评估（简称“**DPIA**”）、数据保护官的任命要求，这几大方面对泰国、越南的法律要求进行对比分析，并为中国企业在泰国、越南经营活动中涉及的个人数据处理活动，提供初步的指引和提示。

二、个人数据保护法的适用范围

(一) 泰国 PDPA 的适用范围

根据泰国 PDPA 第 5 条规定，在泰国境内的任何自然人或法人的收集、使用或披露个人数据的行为，无论该行为本身是否发生在泰国境内，都需要遵守 PDPA。除此之外，泰国 PDPA 还存在一定的域外效力。即，如果自然人或法人位于泰国境外，但是存在以下两类活动，则仍然受到泰国 PDPA 的约束：（1）向位于泰国境内的数据主体提供商品或服务（无论数据主体是否支付对价）；或（2）对数据主体发生在泰国境内的行为进行监控。

泰国 PDPA 的第 4 条也明确了不适用该法案的特定情形，例如，某自然人为了个人的利益或家庭活动而收集、使用或披露个人数据；自然人或法人使用或披露个人数据仅用于大众媒体、艺术或文学活动且符合专业道德或公共利益；负有维护国家安全职责的公共机构、众议院、参议院、议会及其任命的其他委员会或组织为履职而收集、使用或披露个人数据；法院的审判及裁判工作或相关官员在诉讼、执行、财产保存等工作操作；征信机构及其成员依法运营数据。该排除适用条款较为特别，无论是 GDPR 还是我国的《个人信息保护法》，均未明确排除上述情形的适用。

企业出海泰国需要根据自身出海的模式（例如是在当地设立相关实体运营还是在当地未设立相关实体，但会向泰国当地个人提供产品或服务），判断其多大程度上受到泰国 PDPA 的约束。

(二) 越南 PDPD 的适用范围

越南 PDPD 关于适用范围的规定相对粗略。根据越南 PDPD 第 1 条，该法令适用于（1）越南的机构、组织和个人；（2）位于越南境内的外国公共机构、实体和个人；（3）在外国运营的越南机构、组织和个人；以及（4）直接处理或参与处理越南境内个人数据的外国机构、组织和个人。

从上述规定可以看出越南 PDPD 也存在一定程度的域外效力。即使某机构、组织或个人位于越南境外，但其直接处理或参与处理越南境内的个人数据，也可能受到越南 PDPD 的约束。相比而言，泰国 PDPA 的域外效力借鉴了 GDPR 下的域外效力的

规定，相对具体。但越南 PDPD 的域外效力的范围则更为宽泛，因此具体场景（例如某面向全球用户的网站同样也可以被越南用户无差别访问和使用从而涉及对越南用户个人数据的处理）是否必然受到越南 PDPD 的域外效力约束，仍待实践检验。

(三) 有关个人数据、敏感个人数据

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，我们对泰国 PDPA 和越南 PDPD 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，泰国 PDPA 和越南 PDPD 没有太大的区别。均指与自然人相关联，能够直接或间接识别具体个人的信息。但是泰国 PDPA 明确表明，个人数据不包含死者的个人信息，而越南 PDPD 并未明确排除死者的个人信息。

(2) 敏感个人数据

对于敏感个人数据的定义，泰国 PDPA 和越南 PDPD 存在较大的区别。首先，泰国 PDPA 没有明确提出“敏感个人数据”的概念，但是其第 26 条对“与个人种族、民族、政治观点、宗教信仰、性行为、犯罪记录、健康数据、残疾、工会信息、遗传数据、生物识别数据或任何可能以个人数据保护委员会规定的方式影响数据主体的数据”的收集行为作出明确的限制。实践中普遍将其解释为对敏感个人数据的处理规则。

越南 PDPD 则采取明确列举的方式，将一般的个人数据和敏感个人数据分别进行列举。其中，敏感个人数据是指与个人隐私相关的个人数据，一旦受到侵犯，将直接影响个人的合法权益和利益，包括：（1）政治和宗教观点；（2）健康状况和健康记录中提到的个人信息，不包括血型信息；（3）关于种族或民族的信息；（4）与个人遗传或获得的遗传特征相关的遗传数据信息；（5）关于个人生物特征或生物属性的生物识别信息；（6）关于个人的性生活或性取向的信息；（7）执法机构收集和存储的犯罪和犯罪活动数据；（8）信贷机构、外国银行分行、支付服务提供商及其他获得许可的机构的客户信息，包括：依法规定的客户身份识别、账户、存款、存放的资产、交易、在信贷机构、银行分行和支付服务提供商处的担保组织和个人信息；（9）通过定位服务确定的个人位置；（10）法律特别规定需要特别保护的其他特定个人数据。对敏感个人数据进行明确列举的方式有利于企业对数据的敏感性进行判断。不过值得注意的是，越南对于敏感个人数据的定义和范围和中国不完全相同。例如，越南 PDPD 将身份证号码、护照号码、驾驶证号、纳税人识别号、社会保险号、健康保险卡号、数字账户信息、反映网络空间活动和活动历史的个人数据等认定为一般个人数据，但是该等信息在中国被视为敏感个人数据。因此，企业在对其所处理的数据的敏感性进行判断时，仍需要结合该处理活动所受的管辖法律进行判断。

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

全球主要的国家/地区有关个人数据保护的立法几乎都要求处理个人数据必须具有合法性基础。并且随着立法发展，“获取数据主体的同意”在许多国家已经不是唯一的处理个人数据的合法性基础，其他常见的合法性基础还包括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、为保护自然人的生命健康所必须、公共利益等。目前，泰国和越南的立法中也都包含上述合法性基础，但泰国还特别将统计研究作为一项合法性基础，并参照 GDPR 将“合法权益”作为一项处理个人数据的合法性基础。在使用“合法利益”的合法性基础时，通常需要判断该个人数据的处理

行为是为了数据控制者或其他任何自然人或法人的合法利益所必需，且不能与数据主体的基本权利相冲突。

无论是泰国还是越南，数据主体的“同意”尽管不是唯一的处理个人数据的合法性基础，但仍然是最重要且最常被使用的合法性基础。泰国 PDPA 和越南 PDPD 均对告知和同意提出了严格的要求。

(2) 泰国有关告知同意的具体要求

根据泰国 PDPA 第 19 条的规定，在没有其他法律法规允许的情况下，除非数据主体在收集、使用或披露个人数据之前或之时已给予同意，否则数据控制者不得收集、使用和披露个人数据。同意的请求必须通过书面或电子方式明确做出，并且请求同意时，数据控制者应当告知收集、使用或披露个人数据的目的等信息。此类同意请求应使用清晰明了的语言，以易于理解的形式和陈述向数据主体告知，并且不会对数据主体造成欺骗或误导。

关于向数据主体进行告知以便获取其同意的具体程序，2022 年，泰国 PDPC 颁布了《根据 PDPA 获取数据主体同意的指南》（Guideline on Requesting Consent from the Data Subject under the Personal Data Protection Act B.E. 2562 (2019)，简称“**《同意指南》**”）、《根据 PDPA 向数据主体通知收集个人数据的目的及详情信息的程序指南》（Guideline on Procedures for Notifying the Purpose and Details relating to the Collection of Personal Data from Data Subjects under the Personal Data Protection Act. 2562 (2019)，简称“**《通知指南》**”）。

《同意指南》中包含以下要点：

第一，关于告知的形式和内容必须满足以下要求：

- 必须在收集、使用或披露个人数据之前或之时请求同意；
- 数据控制者在向数据主体进行告知时，必须说明具体的收集个人数据的目的和细节，不能只做笼统的告知，且禁止在收集、使用或披露多种类型或多个主体的个人数据时只披露某项目的，并合并获取一项同意；
- 具体设计的请求同意的表格或声明应当具有易于访问和理解的形式，语言应当易于阅读，不存在欺骗或误导数据主体的情况；
- 请求同意的声明应当与与其他声明分开，如用户协议、服务协议等。

第二，同意必须满足以下要求：

- 必须是数据主体自愿、自由地作出；
- 必须通过明确且肯定性的动作完成，如通过提交数据主体自己准备的同意书、在数据控制者准备的同意表上签字以授予同意、数据主体自己点击复选框表示同意、连续两次按下手机上的按钮或滑动屏幕以明确表示数据主体的同意。

《通知指南》则明确了在通知数据主体有关收集、使用和披露个人数据的目的和细节时应遵循公平、目的限制的原则，具体体现为：

- 数据控制者必须确保在收集个人数据之前或之时通知数据主体关于数据处理活动的目的和细节，使其能够识别使用和披露个人数据所产生的影响，并且必须确保用于通知目的和细节的语言和文本清晰易懂；
- 与收集、使用和披露个人数据有关的目的和细节必须有限且明确，数据控制者不得超出已通知数据主体的目的范围使用个

人数据。

在此基础上，《通知指南》列出了可用于通知收集个人数据的目的和细节的方法，例如书面通知、口头通知、通过短信、电子邮件、彩信、电话或任何其他电子方式的通知，为了提醒数据主体及时了解有关收集个人数据的目的和细节，可以提供专门的链接，并在相关的指引文本中设置下划线。

(3) 越南有关告知同意的要求

越南 PDPD 第 11 条和 13 条对告知和同意做出了具体要求。数据控制者在基于数据主体的同意开展个人数据处理活动之前，应向数据主体履行告知义务，并获取数据主体的同意。告知和同意应分别符合以下要求：

告知必须满足以下要求：

- 数据控制者必须在处理个人数据之前进行一次性的告知；
- 告知的内容应当包含有关个人数据处理活动的所有相关内容，包括处理目的、与处理目的相关的使用的个人数据类型、处理个人数据的方法、与处理目的相关的参与个人数据处理活动的组织及其相关信息、处理活动可能发生的不良后果和损害、处理活动开始和结束时间、数据主体的权利和义务；
- 告知应当通过电子或书面的可验证的方式进行。

同意必须满足以下要求：

- 同意必须是在知情的情况下自愿作出才有效；
- 同意必须以书面、口头、勾选同意框、发送消息、选择同意按钮等方式明确表示确认，沉默或不作响应都不应视为同意；
- 同意必须和具体的某一特定目的相关联，如果存在多个目的，数据控制者应当分别告知所有的目的，以便数据主体分别明确同意其中的某一特定目的。

四、数据主体的权利

根据对泰国 PDPA 和越南 PDPD 的内容对比，数据主体享有的个人数据权利类型相似，都涵盖了 GDPR 下数据主体享有的主要权利，包括查阅复制权、更正权、删除权、撤回同意的权利、限制处理的权利、反对权、数据可携带权。

在数据主体请求响应的时间要求方面，泰国 PDPA 规定，数据控制者必须在收到请求后最多 30 天内响应该请求，不得无故拖延，且不得延长期限。但泰国 PDPA 规定的 30 天时限仅针对查阅复制权的请求，其他类型的请求尚没有具体的时间限制。虽然没有规定其他类型请求的回复时间限制，但泰国 PDPA 规定，如果数据控制者未能回应上述任何请求，数据主体可以向相关当局提出投诉。越南 PDPD 要求数据控制者在 72 小时内完成数据主体权利请求响应。

五、数据控制者和处理者的权利义务

在个人数据处理活动中，数据控制者和数据处理者各自需要承担的义务有所不同。通观泰国和越南数据保护法律的要求，二者的区别包括：

一般情况下，数据控制者必须承担个人数据处理活动的责任，落实告知同意的要求，采取适当的组织和技术措施保障个人数据的安全，形成个人数据处理记录，并需要和监管部门保持沟通合作。而数据处理者只是根据数据控制者给出的指令或按照双方签署的协议执行个人数据处理活动，并配合数据控制者履行其法定义务。

具体的业务场景下，数据控制者和数据处理者承担的义务也存在差异：

(1) 响应数据主体的权利请求：数据控制者需要及时响应数据主体的权利请求，而数据处理者只需要在接到数据控制者的指示后配合完成个人数据更正的义务。

(2) 发生数据泄露等安全事件时的通知：由数据控制者履行向监管部门的通知义务，数据处理者只需要及时通知数据控制者即可。

(3) DPIA：泰国将义务主体限定在数据控制者，而越南要求数据控制者和数据处理者都需要履行该项义务。

(4) 数据跨境转移：泰国要求数据控制者履行作为数据对外传输方或境外接收方的合规义务，而数据处理者仅可能作为数据的接收方存在，无权主动发起将个人数据向境外传输的请求。越南则规定数据控制者、数据处理者均有权作为数据出境方开展数据跨境转移活动。

中国企业在海外开展业务时，需要先行判断在特定的个人数据处理活动中自己的角色是属于可以自主决定个人数据处理活动的数据控制者，还是代表数据控制者并接受其指令开展个人数据处理活动的数据处理者。在明确角色后，再进一步确认自身需要履行的合规义务。

六、数据跨境转移规则

(一) 泰国

泰国的数据跨境转移规则借鉴了 GDPR，要求在向泰国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) **充分保护水平的国家：**个人数据转移的目的地是被泰国认可的具有充分的数据保护标准，并按照泰国 PDPC 规定的个人数据保护规则执行的国家。目前，泰国 PDPC 目前尚未发布具有充分的数据保护标准的白名单国家列表；

(2) **采取适当保护措施：**个人数据跨境转移采取了适当的保护措施（包括签署标准合同条款、经监管部门认可的具有约束力的公司内部准则、认证以及泰国政府机构与外国政府机构之间的约束性文件）；或

(3) **例外情形：**适用特定的例外情形，包括（i）为了遵守法律的要求；（ii）已获得数据主体的同意，前提是数据主体已被告知目的地国家或国际组织的个人数据保护标准不足；（iii）为了履行数据主体作为一方的合同，或者为了在签订合同前应数据主体的要求采取措施；（iv）为了遵守数据控制方与其他自然人或法人之间的合同，以维护数据主体的利益；（v）为了防止或抑制对数据主体或其他人的生命、身体或健康的危险，而数据主体当时没有能力给予同意；（vi）进行与重大公共利益相关的活动所必需；

需要注意的是，虽然泰国没有如 GDPR 体系发布专门的数据跨境转移影响评估（简称“**TIA**”）指引，但在具体执行数据出境时，作为数据出境方的数据控制者仍需根据数据跨境情况，开展 TIA。若 TIA 表明数据跨境传输活动为高风险且无法找到足够措施将风险降低至可接受水平，应在处理前向监管机构咨询并接收书面建议。同时，无论最终的评估结果显示是否需要与监管部门协商，都仍应留存数据处理活动记录、安全保护措施证明、影响评估记录等证明文件。实践中，在采取适当的保护措

施时，对于企业而言最便利的方式是签署标准合同，目前泰国允许企业选择欧盟委员会发布的标准合同条款（EU SCCs），或东盟委员会发布的数据跨境流动示范合同条款（ASEAN MCCs）。

(二) 越南

与泰国借鉴GDPR搭建数据跨境转移规则不同，越南的数据跨境规则有较大差异：

1. 数据本地化及境外企业设立分支机构或代表处的要求

越南《网络安全法》第 26 条第 3 款规定，越南本土和海外的网络服务提供商若涉及收集、处理、分析某些类型数据的活动，必须在越南境内存储数据，且海外服务提供者必须在泰国境内设立分支机构和代表处。

《第 53 号法令》将上述规则进行了细化，并对数据本地化要求进行了必要的限定，该法令自 2022 年 10 月 1 日生效，基本规则如下：

(1) 越南境内设立的网络服务提供商：无论提供何种服务类型，都必须落实数据本地化要求。

(2) 越南境外设立的网络服务提供商：在触发以下条件时，需要落实数据本地化要求，并在越南境内设立分支机构或代表处：

a) 向越南用户提供的服务落入以下范围：

- 电信服务；
- 在网络服务中存储和共享数据；
- 为越南的服务使用者提供国内或国际域名；
- 电子商务；
- 在线支付；
- 支付中介；
- 通过网络空间的交通连接服务；
- 社交网络和社交媒体；
- 在线视频游戏；
- 通过消息、语音通话、视频通话、电子邮件和在线聊天的形式在网络空间提供、管理或操作其他信息的服务。

b) 服务/在线平台被用于违反越南法律且收到监管部门（越南公安部网络安全和高科技犯罪预防局，简称“**A05**”）的书面通知。

c) 收到 A05 的书面通知后仍未能采取有效的网络安全保护措施导致违法情形未能纠正。

(3) 越南境外设立的网络服务提供商在收到 A05 的通知后有 12 个月的期限可以执行数据本地化和设立分支机构或代表处的要求。

(4) 进行本地存储的数据类型为：i）服务用户的个人信息数据、服务用户创建的数据，例如，账户名/身份、服务使用时间、信用卡信息、电子邮件、访问 IP、与账户或数据相关的注册电话号码等；ii）服务用户的网络关系数据，例如朋友关系、互动群等。

2. 数据跨境转移影响评估要求

目前，根据越南 PDPD 和《第 13/2023/ND-CP 号法令》（简称“**《第 13 号法令》**”），越南并没有像泰国一样建立类似的白名单国家制度，而是采用所有的个人数据出境都需要开展数据跨境转移影响评估的规则。根据该评估规则，越南的数据跨境转移影响评估并非只是一种自评估，而是一种在评

估完成后按照法定要求提交相关评估文件到监管部门的申报备案，只有评估通过监管部门的审查，才能开展个人数据出境活动。因此，在越南开展数据出境活动，不止需要留存相关评估记录形成档案以备监管部门检查，数据出境方还需要在处理个人数据之日起 60 天内，主动依照 PDPD 附录中的官方模版表格，向 A05 提交评估档案，并在个人数据传输完成后，将数据传输内容的相关信息及负责传输的组织或个人的联系方式以书面形式通知 A05。最后，越南赋予 A05 在特定情形下暂停个人数据出境的权力，包括发现传输的个人数据被用于违反越南社会主义共和国利益和国家安全的活动；数据出境活动违反国家法律和越南签署的国际公约；数据出境活动将导致越南公民的个人数据被泄露或丢失。

七、DPIA

目前泰国对 DPIA 并没有进行直接的规定，只是在泰国 PDPA 第 37 条第 1 款指出，为了防止未经授权或非法的数据访问、使用、更改、更正或披露个人数据导致数据丢失，数据控制者必须提供适当的安全措施，且在必要时或技术发生变化时需要及时对这些措施进行审查，以确认安全保护措施的有效性。对此泰国 PDPC 发布的《通知指南》中，进一步规定数据控制者从其他来源收集、使用或披露个人数据之前，应实施 DPIA，以识别和评估可能因使用或披露个人数据而产生的风险，同时在使用人工智能等现代技术导致处理或披露大量个人数据时也应当实施 DPIA。

越南关于 DPIA 的规定更加严格，要求对所有个人数据处理活动都必须进行评估，并形成数据处理活动的记录和影响评估档案，向监管部门提交。越南 PDPD 附录中专门发布了 DPIA 报告的官方模版。

八、组织内设置 DPO 的要求

关于在企业组织内设置 DPO 的要求，泰国和越南两国的相关法律法规要求如下：

(1) 触发任命的情形：

泰国和越南均在特定的情形下要求企业内强制任命 DPO：

- 泰国法下的强制任命 DPO 的情形包括：数据控制者或数据处理者是监管机构规定和公布的公共机构；数据控制者或数据处理者拥有大量个人数据[2]且需要定期监控个人数据或系统；数据控制者或数据处理者的核心活动是处理敏感个人数据。
- 越南则仅规定当企业组织收集和处理敏感个人数据时，需要任命 DPO。

(2) 资质和岗位要求：

- 泰国和越南都要求 DPO 应当具备数据合规领域的专业知识和技能。
- 泰国允许公司内的员工或外部第三方专业服务人员担任公司的 DPO，而越南的法律实践中一般要求 DPO 是公司的内部员工。
- 泰国和越南都允许 DPO 可以是母公司或同一组织内的关联公司的员工。
- 特别的，越南 PDPD 要求如果企业内存在收集和处理敏感个人数据的情形，除了任命 DPO，企业内还需要设置专门的数据保护部门，但泰国目前没有强制性的法律要求公司内必须设立专门的数据保护委员

[2] 关于企业组织处理个人数据的规模，泰国 PDPC 曾发布指南，规定如果数据控制者或数据处理者处理超过 10 万条包含个人数据的记录，则必须任命 DPO。

会或工作机构，尽管实践中大多数企业仍然会设置该等委员会或工作机构。

(3) 职责要求：

- 泰国 PDPA 第 42 条要求 DPO 承担向企业组织提供法律咨询意见并开展调查，确保企业组织的业务活动遵守泰国数据保护法律法规的要求，并在企业内出现违规行为时，与监管部门进行协调和合作。
- 越南 PDPD 目前就 DPO 的职责内容，没有具体说明。

(4) 备案要求：

- 泰国和越南都有登记备案的要求，数据控制者和数据处理者有义务向监管机构提供 DPO 的基本信息、联系地址和联系方式。

对于打算在泰国或越南当地设立公司实体的中国企业而言，需特别注意当地关于数据合规管理人员或组织的任命要求。目前两国都规定需强制任命 DPO 的特定情形，即在该等特定情形发生时，必须任命 DPO。但实践中，即使未触发强制任命 DPO 的情形，企业出于合规需要，其最佳实践仍然是任命一名 DPO。但需要注意的是，一旦任命了 DPO，则 DPO 的相关信息需要向监管部门备案。

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
史晓宇　律　师　电话：86-21 2283 8301　邮箱地址：shixiaoyu@junhe.com