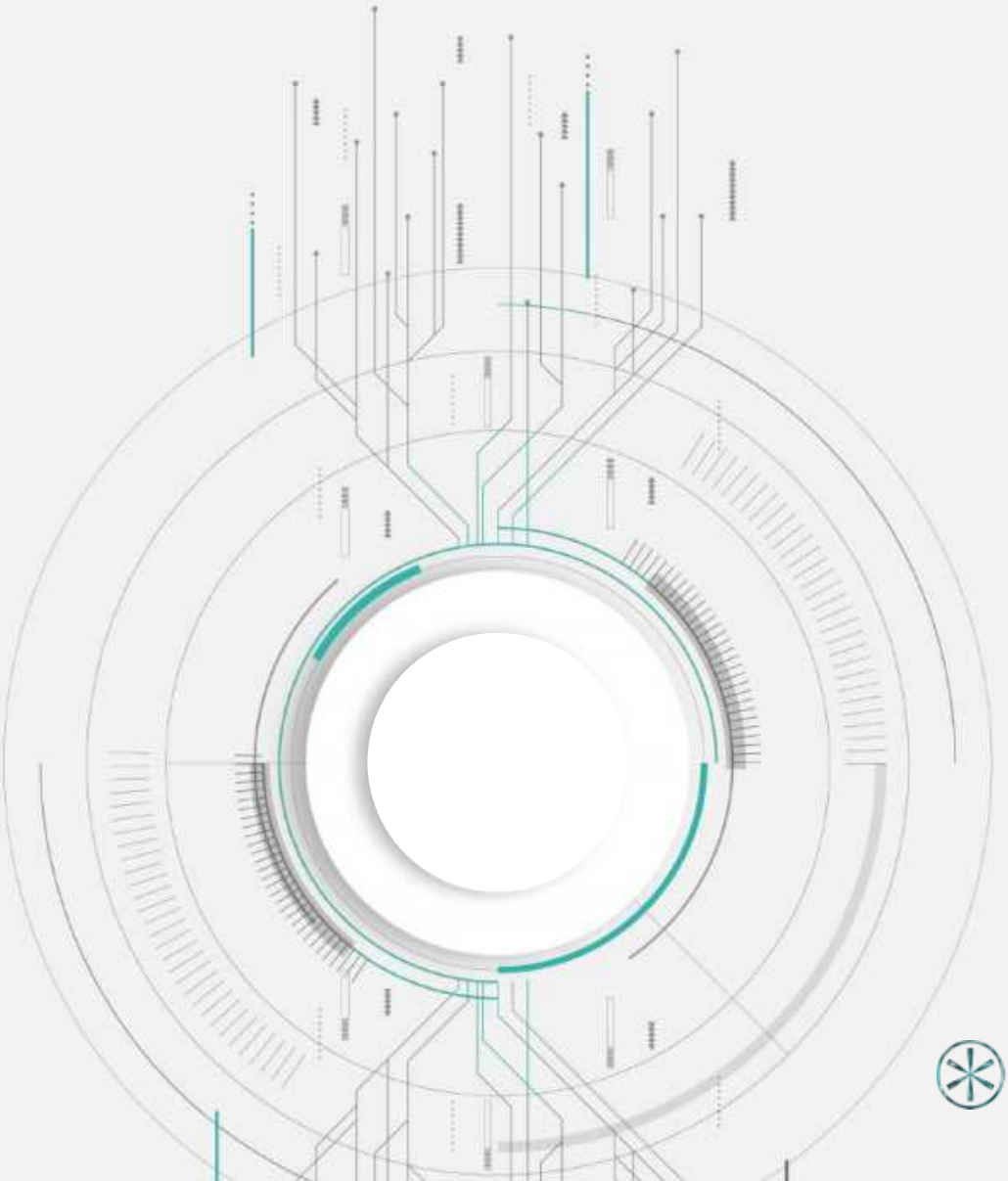
生成式人工智能-

海外合规白皮书（东南亚篇）

垦丁律师事务所

垦丁（新加坡）、 WEEE Consulting、 Boosterhub



2024年8月

KINDING 垦丁律师事务所

人工智能产业链联盟

星主： AI产业链盟主

知识星球

微信扫描预览星球详情

目　录

撰写人简介
免责声明
序言

一、新加坡 1

一）新加坡生成式人工智能产业及监管 2
1. 生成式人工智能在新加坡的发展现状和地位 2
2. 新加坡生成式人工智能监管框架 7

二）新加坡生成式人工智能合规核心问题 10
1. 基础模型和AI产品关系及定性 10
2. 大模型预训练使用公开数据合规 12
3. 数据本地化和数据跨境 15
4. 开发者安全责任 19
5. 内容安全 25
6. 生成物知识产权可版性 28
7. 大模型透明度 30
8. 用户权利保护 32

二、越南 35

一）越南生成式人工智能产业及监管 36

1. 生成式人工智能在越南的发展现状和地位 36
2. 越南生成式人工智能监管框架 39

二）越南生成式人工智能合规核心问题 41

1. 基础模型和AI产品关系及定性 41
2. 大模型预训练使用公开数据合规 43
3. 数据本地化和跨境数据 45
4. 开发者安全责任 48
5. 内容安全 50
6. 生成物知识产权可版性 52
7. 大模型透明度 53
8. 用户权利保护 53

三、泰国 55

一）泰国生成式人工智能产业及监管 56

1. 生成式人工智能在泰国的发展现状和地位 56
2. 泰国生成式人工智能监管框架 60

二）泰国生成式人工智能合规核心问题 62

1. 基础模型和AI产品关系及定性 62
2. 大模型预训练使用公开数据合规 62
3. 数据本地化和跨境数据 65
4. 开发者安全责任 68
5. 内容安全 69
6. 生成物知识产权可版性 70
7. 大模型透明度 70
8. 用户权利保护 72

四、马来西亚 73

一）马来西亚生成式人工智能产业及监管 74

1. 生成式人工智能在马来西亚的发展现状和地位 74
2. 马来西亚生成式人工智能监管框架 76

二）马来西亚生成式人工智能合规核心问题 79

1. 基础模型和AI产品关系及定性 79
2. 大模型预训练使用公开数据合规 78
3. 数据本地化和跨境数据 80
4. 开发者安全责任 83
5. 内容安全 83
6. 生成物知识产权可版性 85
7. 大模型透明度 85
8. 用户权利保护 86

五、印度尼西亚 87

一）印度尼西亚生成式人工智能产业及监管 88

1. 生成式人工智能在印度尼西亚的发展现状和地位 88
2. 印度尼西亚生成式人工智能监管框架 93

二）印度尼西亚生成式人工智能合规核心问题 95

1. 基础模型和AI产品关系及定性 95
2. 大模型预训练使用公开数据合规 96
3. 数据本地化和跨境数据 96
4. 开发者安全责任 98
5. 内容安全 98
6. 生成物知识产权可版性 100
7. 大模型透明度 100
8. 用户权利保护 100

六、菲律宾 102

一）菲律宾生成式人工智能产业及监管 103

1. 生成式人工智能在菲律宾的发展现状和地位 103

2. 菲律宾生成式人工智能监管框架 105

二）菲律宾生成式人工智能合规核心问题 107

1. 基础模型和AI产品关系及定性 107

2. 大模型预训练使用公开数据合规 107

3. 数据本地化和跨境数据 108

4. 开发者安全责任 109

5. 内容安全 110

6. 生成物知识产权可版性 111

7. 大模型透明度 111

8. 用户权利保护 112

联系我们 114

撰写人简介

垦丁律师事务所

垦丁律师事务所是由一群在网络法实务领域有丰富经验的律师，于2017年7月共同创设，是一家完全专注于提供“ 网络法 ”法律服务的专业律师机构。垦丁律师正在服务或曾经服务的客户包括： 腾讯、小米、蚂蚁国际、天猫人工智能、百度、360、星际魅族、虎牙、唯品会、焦点科技等综合和细分市场头部互联网企业。也包括强生、耐克、松下、特斯拉（中国）、smart、上汽大众、OPPO、日立（中国）、传音控股、鹏成新能源等智能制造和新兴产品市场。
垦丁所的业务范围涉及平台治理、产品合规、投资并购、数据合规、知识产权、跨境争议解决等等，行业领域涉及综合网络平台、AIGC、NFT/区块链、数字娱乐、智能终端等。

未一咨询

专注于帮助出海企业解决全球化拓展中的跨文化挑战。创立于2022年，未一咨询提供海外市场调研、品牌建设、市场营销、公共关系、跨文化管理培训等专业服务。创始团队均曾供职于大型跨国科技企业，拥有深耕东南亚、日韩、欧美、大中华等多个市场的经验，深入了解各国文化

和市场环境、监管政策、行业动态，服务过从大型跨国企业，到初创公司体量不等的各类客户，为客户量身定制高效的品牌营销策略、提供从高管到核心员工的跨文化培训，帮助更多具有国际化视野和雄心、有潜力领跑未来的企业在复杂多变的环境中找准锚点，扬帆远航，取得更大成功。

Booster Hub

Booster Hub全速引擎是以全球化服贸为产业核心的创新商业化园区，是中国杭州市综试区的“ 全球跨境电商DTC品牌创新中心 ”。
Booster Hub全速引擎专注于引进、孵化、服务在全球化市场方向上具备创新和产业优势的企业，围绕全球化的商流、物流、资金流、信息流四个核心服务方向，打造大中小全链路产业生态。除此之外，在垂直市场化产业基金配套、行业媒体矩阵服务、跨境服务商体系对接等方面给予支持。

起草人：

垦丁新加坡办公室
（按拼音排序）
陈梅瑜 何天伦 胡烨 黄帅 黄钰涯 姜正浩 麻策 牟若桃 束司斌 夏律
朱骏超 朱莎
顾问：姚雪 罗威

免责声明

本文章仅代表作者个人观点，仅为提供一般性信息之目的，不应用于替代专业咨询意见。尽管本文章中所包含的信息都是我们于发布之时从我们认为可靠的渠道获得，但鉴于人工智能相关的法律法规变化迅速，司法实践也会依个案实际情况处理，因此不对本文章内容、观点以及建议的准确性、可靠性、时效性以及完整性作任何明确或隐含的保证。

本文章仅供企业参考使用，企业切勿依赖，任何仅依照本文全部或者部分内容而做出的决定以及因此造成的后果由行为人自行负责，本文的机构和作者明示不予承担任何责任。在相关法律法规进行变更或更新时亦不会另行通知。

序言

随着生成式人工智能（Generative AI）技术的迅猛发展，其应用范围已经深入到社会生活的各个角落，从电商、制造、金融服务到教育和娱乐，无一不受到这一前沿技术的影响。生成式人工智能不仅带来了前所未有的创新和效率提升，同时也引发了诸多伦理、政治和经济方面的讨论和挑战。在这一背景下，法律合规的重要性尤为突出，特别是在不同国家和地区，其合规要求各有特色，需要我们深入了解并严格遵守。

东南亚作为全球经济快速发展的区域之一，人工智能行业也展现出蓬勃的发展势头。东南亚各国在政治、文化、法律制度等方面具有鲜明的区域特性，因此，在生成式人工智能的应用和发展过程中，合规问题显得尤为重要。不同国家的法律框架、AI合规相关的法规、伦理标准以及政府监管政策等方面都需要特别关注和遵守，以确保技术创新与法律规范的有机结合。东南亚地区经济快速发展，各国在科技创新方面也展现出巨大的潜力。然而，由于各国在政治、经济和文化上的差异，生成式AI的法律监管和合规要求也各不相同。这使得东南亚的AI行业在合规方面面临独特的挑战和要求。

通过对东南亚各国生成式AI产业及监管框架的深入分析，本白皮书旨在全面解析东南亚各国在生成式人工智能领域的法律合规要求，帮助企业

和从业者更好地理解和应对这一复杂多变的法律环境。我们将从各国具体的法律法规出发，结合实际案例和应用场景，深入探讨东南亚AI行业的合规特点和应对策略。希望通过本白皮书的研究和分享，能够为广大AI从业者提供有价值的指导和参考，推动生成式人工智能技术在东南亚地区的健康、可持续发展。

第一章、新加坡

一）新加坡生成式人工智能产业及监管

1. 生成式人工智能在新加坡的发展现状和地位
2. 新加坡生成式人工智能监管框架

二）新加坡生成式人工智能合规核心问题

1. 基础模型和AI产品关系及定性
2. 大模型预训练使用公开数据合规
3. 数据本地化和数据跨境
4. 开发者安全责任
5. 内容安全
6. 生成物知识产权可版性
7. 大模型透明度
8. 用户权利保护

一）新加坡生成式人工智能产业及监管

1. 生成式人工智能在新加坡的发展现状和地位

1）生成式AI产业政策

新加坡在人工智能治理方面采取了部门性的方法，即通过各个行业的监管机构来管理人工智能的使用。这些监管机构主要通过发布非约束性的指南和建议（软法手段）来进行治理，而不是通过强制性的法规（硬法手段）。

①金融领域

新加坡金融管理局是新加坡的中央银行和综合金融监管机构。金融管理局是首个在人工智能治理方面采取行动的部门监管机构。2018年，金融管理局与金融行业共同创建了一套FEAT原则（即公平性Fairness、伦理Ethics、问责Accountability和透明性Transparency），以指导人工智能的负责任使用。2019年，金融管理局宣布与金融行业合作创建Veritas框架，为金融机构提供可验证的方法，将FEAT原则纳入其人工智能和数据分析驱动的解决方案中。FEAT原则和Veritas框架是新加坡国家人工智能战略的一部分，旨在为金融部门的人工智能采用建立一个进步和可信赖的环境。

②信息通信领域

信息通信媒体发展局（IMDA）和个人数据保护委员会（PDPC）是人工智能治理中最活跃的监管机构。自2019年以来，IMDA和PDPC每年都推出了与人工智能治理相关的指南或倡议。2019年，两大机构在达沃斯世界经济论坛年会上发布了首个《人工智能治理模型框架》。该框架旨在为私营部门组织在部署人工智能解决方案时提供可实施的指导，解决关

键的伦理和治理问题。依据国际隐私专业人员协会（IAPP）的相关报告，2020年，上述两机构更新了该模型框架，发布了第二版，并推出了《组织实施和自我评估指南》，帮助组织评估其人工智能治理实践与模型框架的匹配程度，还发布了《案例汇编》，展示了组织如何实施负责任的人工智能治理实践。

③医疗卫生领域

2021年10月，新加坡卫生部发布了《医疗人工智能指南》，提高患者对人工智能在医疗中使用的信任。该指南是与卫生科学局和综合健康信息系统（现称为Synapxe）共同完成的，补充了新加坡对人工智能医疗设备监管的空白。

④生成式人工智能评估沙箱

新加坡信息通信媒体发展局在2024年2月初与新加坡企业发展局合作启动了生成式人工智能评估沙箱。生成式人工智能评估沙箱将为选中的中小企业提供AIGC解决方案，并根据中小企业提供的反馈结果评估这些解决方案，最终在本地中小企业中推广生成式人工智能应用。

2）生成式AI企业案例

①AI Rudder

AI Rudder成立于2019年，是一家领先的对话式AI平台和解决方案提供商，专注于潜在客户生成、客户服务和技术优化。其主要产品包括人工智能语音助手、AI聊天机器人、VoiceGPT等。AI Rudder的技术在金融行业中表现尤为出色，优化了自动语音识别（ASR）模型，提升了客户服务的准确性和效率。AI Rudder的模型支持新加坡当地IP访问。

②ADVANCE.AI

网址：https://www.advance.ai/

ADVANCE.AI成立于2016年，总部位于新加坡，并在全球如中国、印尼、菲律宾、马来西亚等多地设有本地客户支持团队，其母公司是东南亚独角兽Advance Intelligence Group，集团业务覆盖12个市场。该公司利用AI、大数据和云计算技术提供数字化解决方案，主要服务包括人脸识别、活体检测、OCR技术支持的数字身份验证、大数据与机器学习支持的风险管理和信贷评估、企业级数据分析等。

ADVANCE.AI 提供混合部署方案，可根据企业实际情况选择合适的方式运行应用程序（本地或云端），支持新加坡当地IP访问。 ADVANCE.AI的大模型本身不提供 Google Trends 功能。如果需要使用 Google Trends 数据，通常需要通过调用 Google Trends API 来实现。

③科大讯飞（iFLYTEK）

网址：https://www.iflytek.com/about.html

科大讯飞股份有限公司成立于1999年，是一家智能语音和人工智能上市企业，科大讯飞在中国和全球范围内提供包括智能语音、计算机视觉、自然语言处理、认知智能等产品和服务。

科大讯飞将新加坡作为其海外业务的第一站和战略中心。2024年5月，科大讯飞新加坡办公室正式开业，并宣布将在新加坡建立区域总部。为实现国际化战略布局，科大讯飞制定了“ 1+4 ”战略，即一个以新加坡为中心的讯飞开放平台国际站与四项战略投资：本地化投资、技术投资、产品创新投资、合作伙伴计划投资。

科大讯飞在新加坡推出了星火认知大模型，星火认知大模型是一个基于云服务的大模型平台，具备跨领域的知识和语言理解能力，能够基于自

然对话方式理解与执行任务。星火认知大模型支持当地IP访问，未限制其在特定国家或地区的访问权限。

星火认知大模型本身不直接提供Google Trends功能，但可以通过API集成实现对Google Trends数据的处理和分析。

④字节跳动

字节跳动成立于2012年，是一家跨国互联网技术公司，主要产品包括抖音、今日头条、西瓜视频、飞书、剪映等。

字节跳动积极拓展新加坡市场，将TikTok业务总部迁至新加坡，并在新加坡设立了SPRING公司，专注于开发和推广AI应用。2023年，字节跳动在海外上线基于云雀大语言模型（现名为“豆包大模型”）创建的AI工具平台“ChitChop”，为用户提供200余种工作、生活场景智能机器人服务。

字节跳动推出的豆包大模型支持新加坡当地IP访问。

其他国家投资该国情况：

新加坡已然成为东南亚地区最受欢迎的初创企业投资目的地，尤其在人工智能领域。新加坡的人工智能独角兽公司和人工智能初创企业吸引了来自全球各地的投资者。

美国投资者积极参与新加坡AI企业的融资活动。

- 根据新加坡《经济日报》，新加坡已与美国晶片制造商英伟达（Nvidia）达成共识，由英伟达公司帮助、支持和参与新加坡NAIS 2.0，深化双方在AI技术领域的合作，共同创建一个支持11种语言的大语言模型，以发展新加坡本土AI技术，并将在新加坡新建一台超级计算机。

- 在新加坡举行的第十届AWS东盟峰会上，亚马逊云科技（Amazon Web Services，简称AWS）宣布计划从2024年到2028年额外投资120亿新元（约合88.8 亿美元）用于扩展其在新加坡现有的云基础设施，以满足该国对云技术和服务日益增长的客户需求。AWS还宣布了一项名为AWS AI Spring的新计划，以加速AI（包括生成式人工智能）在新加坡的采用。重点将是为公共部门、当地企业、初创企业、社区、研发组织和劳动力开发这些技术。目前AWS已就该计划与新加坡资媒局IMDA签署了一份意向备忘录。

其他国家如西班牙、印度尼西亚和马来西亚也在新加坡AI领域有一定的投资活动。例如，Bolttech公司还从西班牙和新加坡EDBI获得了3000万美元的投资。此外，新加坡也吸引了来自东南亚其他国家如泰国和越南的企业前来设立研发中心或进行技术合作。

2. 新加坡生成式人工智能监管框架

1）新加坡政府部门治理总框架

新加坡在其国家人工智能战略（NAIS）中宣布了一个宏伟的目标，就是要走在开发和部署具有可扩展性和影响力的人工智能解决方案的前沿，成为全球人工智能解决方案的开发、测试、部署和扩展的中心。该战略提出了五个“ 生态系统促进因素 ”，旨在推动人工智能的应用，其中一个就是为人工智能创造一个“ 进步和可信 ”的环境，即在创新和社会风险之间找到平衡点的环境。为了建立这样一个“ 进步和可信 ”的环境，新加坡目前对人工智能的监管采用了一种较为宽松和自主的方式。这种方式反映了新加坡对人工智能的两个现实考量。一方面，新加坡政府把人工智能视为促进经济发展和提升国民生活水平的重要战略手段。这就说明了为什么新加坡在监管人工智能方面没有采取过于严厉的措施，以免抑制创新和投资。另一方面，考虑到自身的规模，新加坡意识到，在全球人工智能治理的讨论、框架和法规不断发展的情况下，它可能只能是价格的接受者，而不是价格的制定者。因此，新加坡没有重新制定新的人工智能原则，而是选择“ 顺应世界的现状，而不是期待世界成为什么样 ”。

①《用于生成式人工智能模型的治理框架》

(Model AI Governance Framework for Generative AI，以下简称为“ MGF for GenAI ”）。

②人工智能治理示范框架

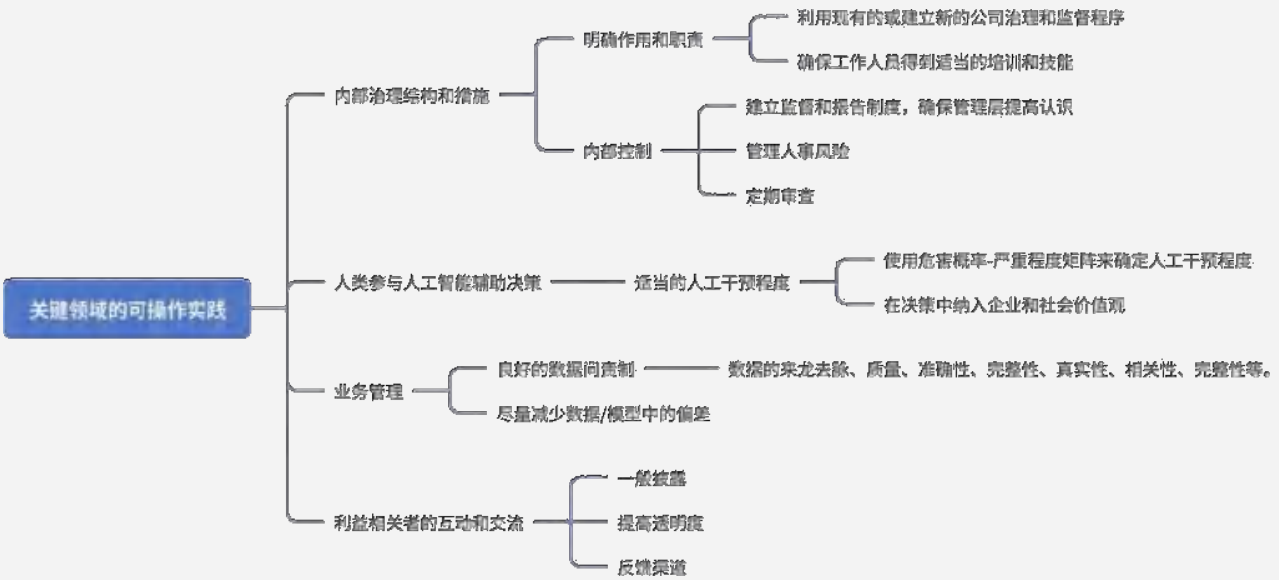
示范框架（Model Framework）是新加坡在2019年世界经济论坛年会（WEF）上推出的亚洲首个人工智能治理示范框架，作为一个自愿的、非强制性的框架，示范框架旨在指导各组织在大规模部署人工智能解决

方案时做到负责任，而不涉及技术的开发阶段。因为公共部门的人工智能使用受到内部指导方针和人工智能与数据治理工具包的约束，示范框架这一指南主要面向私营部门提供人工智能部署的实用建议。示范框架是一个“活的文档”，会根据技术和社会的变化在未来的版本中不断更新。示范框架也不受技术、行业、规模和业务模式的限制。从内容上看，示范框架遵循两个基本原则，以增强对人工智能的信任和理解：第一，使用人工智能进行决策的组织应该保证决策过程具有可解释性、透明性和公平性；第二，人工智能系统应该以人为本：在设计、开发和使用人工智能时，应该优先考虑保护人类的福祉和安全。

该框架把这些指导原则具体化为四个关键领域的可操作实践，这些领域涉及组织的决策和技术的开发过程：

(a) 内部治理的结构和措施；
(b) 确定人类在人工智能辅助决策中的参与程度；
(c) 业务管理；
(d) 利益相关方的交流和沟通。

下图列出了属于每个关键领域的一些建议考虑因素、做法和措施的摘要。



2）AI领域主要监管机构及其职责（包括网址、联系方式等）

① 信息通信媒体发展局（Infocomm Media Development Authority，IMDA）
网址： https://www.imda.gov.sg
联系方式：+65 6377 3800
② 个人数据保护委员会（Personal Data Protection Commission，PDPC）
网址：https://www.pdpc.gov.sg
联系方式：+65 6377 3131
③ 金融管理局（Monetary Authority of Singapore，MAS）
网址：https://www.mas.gov.sg
联系方式：+65 6225 5577
④ 网络安全局（Cyber Security Agency of Singapore, CSA）
网址：https://www.csa.gov.sg
联系方式：1800 2550 000（提供犯罪信息）
⑤ 卫生部（Ministry of Health, MOH）
网址：https://www.moh.gov.sg
联系方式：+65 6325 9220

二）新加坡生成式人工智能合规核心问题

1. 基础模型和AI产品关系及定性

在新加坡的监管框架中，并没有明确针对不同AI产品进行分类并区别监管，但是，我们仍可从新加坡目前的相关法律法规中梳理不同产品类型需侧重满足的监管重点。整体而言，在任何情况下AI产品都应注意遵守新加坡《个人数据保护法》（PDPA）。此外，对于基础大模型、通用大模型，应侧重于遵守MGF for GenAI中对AI产品的宏观、基础的要求，包括透明度、偏见、问责制等问题。具体到模型应用时，应同时重点关注数据保护问题。对于大模型周边服务，如果为网络安全产品的，应注意新加坡《网络安全法》的要求。

- 基础大模型是广泛训练的通用AI模型，能够执行多种任务，但并不特定于某一行业或应用场景。这类模型的监管重点在于透明度、数据质量、偏见和歧视以及算法透明度。根据MGF for GenAI的内容，透明度是监管的关键，以确保这些模型的训练数据和算法设计不会导致不公平或歧视性的结果。数据质量同样重要，因为不准确或偏见的数据会导致模型产生错误或有害的决策。为了应对这些挑战，新加坡在MGF for GenAI中强调了透明度和问责制的重要性。

- 通用大模型与基础模型类似，但这些模型经过特定领域的微调，应用于更具体的任务或行业。例如，在医疗领域，通用大模型可以用于诊断疾病或预测患者的治疗效果。在金融领域，这些模型可以用于信用评估或风险管理。通用大模型一方面同样适用基础大模型的监管重点；另一方面，还有通用大模型所在领域特定的应用合规性、隐私保护和数据管理。例如，医疗应用中，监管机构会特别关注模型是否符合医疗法规

和患者隐私保护的要求；在金融应用中，重点则是模型是否遵守金融监管政策并有效管理风险。另外，数据安全保护为该等产品的监管重点，应确保对相关数据的处理符合PDPA。

- 模型应用是指具体行业或任务的应用，如医疗诊断AI、金融风险评估AI等。这些应用的监管重点在于安全性、有效性、责任归属以及用户同意和透明度。例如，在医疗诊断中，AI模型的安全性和有效性直接影响到患者的健康和生命，因此监管机构要求这些模型经过严格的测试和验证，确保其诊断结果的准确性和可靠性。同时，明确的责任归属也是监管的重要方面，以确保在出现问题时可以迅速找到责任方并采取相应措施。就此，同样应该重点关注MGF for GenAI中问责制的内容。同样，数据安全保护为该等产品的监管重点，应确保对相关数据的处理符合PDPA。

- 大模型周边服务，如AI安全等，涉及提供安全保障、监控和优化AI系统等服务。网络安全局 (CSA) 助理首席执行官 Dan Yock Hau于2024年7月4日表示，人工智能 (AI) 越来越多地嵌入网络安全解决方案中，以应对不断演变的威胁。新加坡通讯及新闻部高级政务部长 Janil Puthucheary 博士强调了在网络安全工具中带头使用AI的作用。对于该等网络产品，应重点确保遵守新加坡《网络安全法》的要求（例如，第五部分针对网络安全服务提供商的要求，未经许可，任何人不得提供渗透测试和托管安全运营中心（SOC）监控服务）。

2. 大模型预训练使用公开数据合规

1）个人信息

在构建、训练与评估人工智能系统的过程中，个人数据扮演着至关重要的角色，其目的是使人工智能模型能够从这些数据中汲取用户的行为模式，提炼洞察用户的需求，进而做出精准的推断。根据PDPA对个人信息的保护有较为全面的保护，其规范不仅局限于企业对个人数据的初步采集与使用，更延伸至整个生命周期。因此，如果训练语料中含有新加坡或涉及新加坡居民的个人数据的大模型，使用该等模型的企业务必确保遵守PDPA的规定。

2024年3月1日，新加坡个人数据保护委员会（PDPC）发布了《关于在人工智能推荐和决策系统中使用个人数据的咨询指南》（以下简称《指南》）。该指南基于PDPA起草发布，虽大部分个人信息使用的要求与PDPA一脉相承，但其强调了在人工智能系统中保护个人隐私和数据安全的重要性，同时确保AI系统的透明度、公平性和可问责性。

该指南要求企业在使用人工智能系统的组织应当保持公开透明，并在其书面政策中纳入相关做法和保障措施，以实现公平合理，政策内容提供的详细程度应与风险相称，一般鼓励企业提供更多信息，说明在人工智能系统开发过程中的数据质量和为了保障个人信息安全所采取的管理措施，具体可以包括披露以下信息。

a) 数据质量：确保训练数据集中个人信息的质量（例如，数据集在市场中的代表性和最近的编制时间），以提高模型的准确性和性能而采取的措施；

b) 数据匿名化及访问限制：是否使用匿化数据进行模型开发，如果不是，采取了哪些流程或技术保障措施以限制只有开发人员才能访问个人

信息。另外，值得一提的是新加坡牵头发起的《东盟数据匿名化指南》（ASEAN Guide on Data Anonymisation）将在2025年发布；

c) 偏见性评估：在进行偏见性评估时，是否有必要使用个人信息来检查特殊信息(如种族信息或宗教信息)在预训练过程是否被使用，或评估训练数据集的偏见情况；

d) 测试环境安全及访问限制：如果模型预训练使用了个人信息，企业采取了哪些程序或技术保障措施来确保测试环境的安全并限制测试人员的访问权限；

e) 数据最小化原则：是否在人工智能系统开发和测试的所有阶段都遵守数据最小化原则等。

2）开源数据集

除了使用个人信息进行模型训练外，更多的企业会使用市面上已有的开源数据集作为模型训练的主要数据来源，一方面使用开源数据集的可以一定程度上规避知识产权、版权、个人信息等带来的风险，另一方面许多数据集有适用的针对性场景，可能会更加适配所需调试的模型。当人工智能系统训练使用开源数据集时，企业应检查数据集的许可证，确保数据的使用行为遵守其条款和条件。一些开源许可证可能要求数据使用者在再分发数据时保留版权声明，共享相同许可，或在某些情况下提供源代码。

目前在训练大模型时较常用到的开源数据集有综合性的数据集，如UCI Machine Learning Repository，该公开数据集包含了数百个数据集，适用于各种机器学习任务，如分类、回归和聚类，还有Kaggle

Datasets，这一数据集提供了丰富的数据集，涵盖了从图像识别到文本分析等多个领域。也有偏向某一使用场景的开源数据集，如适用于图像处理类大模型的数据集COCO，这一数据集提供了日常物体的图像和详细的注释以及自动驾驶领域常用的开源数据集Waymo Open Dataset用于自动驾驶技术的研究）。还有像Reddit这样与谷歌达成 6000万美元协议，允许其利用其线上讨论帖子训练人工智能模型，形成的数据集Reddit Comments，其中包含了Reddit网站上的评论数据，主要用于文本分析和社交网络研究。

3. 数据本地化和数据跨境

《指南》明确了PDPA如何适用于AI系统。《指南》建议企业在AI系统开发、测试和监控中使用个人数据时，考虑有效性、效益性、合规性和市场性。

新加坡的AI数据保护政策：

- 人工智能监管模式框架：新加坡早在2019年便推出了人工智能监管模式框架（Model AI Governance Framework），旨在为AI开发和部署提供指导，确保数据使用的透明度和安全性。

- AI Verify：2022年，新加坡推出了全球首个人工智能治理测试框架和工具箱AI Verify，用于测试和验证AI系统的安全性和透明度。

- 生成式AI开发安全指南：新加坡计划在2025年初推出针对生成式AI开发者的安全指南，建议开发者向用户透明公开所使用的数据来源、测试结果以及可能涉及的风险和限制，以增强用户对AI产品的信任。

- 隐私增强科技：新加坡政府还支持在AI领域使用隐私增强科技（Privacy Enhancing Technologies），包括通过资讯通信媒体发展局监管沙盒，支持与生成式AI数据使用相关的项目。

1）数据本地化

AI技术依赖于大规模的数据处理和分析，数据本地化要求可能限制数据的自由流动，影响AI模型的训练和优化。数据本地化是指在本地存储和处理数据的要求，旨在确保数据的主权、安全和隐私。随着AI技术的迅速发展，数据本地化政策对AI应用产生了重要影响。新加坡在数据本地化方面有着明确的法律和政策，以保护数据隐私和确保国家安全。

2）数据跨境

数据跨境传输要求
根据新加坡《个人信息保护法》第26条“ 个人信息跨新加坡国境传输 ”条款规定：

第一，对于跨境传输的数据，机构应当按该法律规定建立个人信息保护标准，确保被传输的数据得到与新加坡法律相等的保护，否则不得进行跨新加坡国境传输。

第二，新加坡个人信息保护委员会可以根据机构的申请，通过书面通知豁免机构前述跨境合规义务。

第三，可豁免的情形可以由个人信息保护委员会书面说明；豁免不需要在政府公报中公布，并且委员会随时可撤销豁免。

第四，新加坡个人信息保护委员会可以随时增加、改变或撤销豁免的具体适用情形。"

组织须遵守转移限制的义务：组织机构在将个人数据传输至新加坡境外任何地点时，必须遵守PDPA的相关规定。组织不得将个人数据转移到新加坡以外的国家或地区，除非按照PDPA规定的要求，确保被转移的个人数据将获得与PDPA规定的保护标准相当的保护。

要做到这一点，该组织必须：

① 确保其将遵守收集、使用和披露个人数据的义务，同时转移的个人数据仍由该组织持有或受其控制；

② 确认且保证在新加坡境外的国家或地区的接收人受到法律上可执行的义务的约束，向被转移的个人数据提供至少与PDPA下的保护标准相当的保护。

这些 "可依法执行的义务 legally enforceable obligations"包括根据法律法规、合同或具有约束力的公司规则（BCRs）或任何其他具有法律约束力的文书规定的义务。

此外，持有根据个人数据被转移到的国家或地区的法律授予或认可的"特定认证specified certification "的组织将被视为受这些可依法执行的义务约束。根据Personal Data Protection Regulations，"特定认证"是指亚太经济合作组织跨境隐私规则（“APEC CBPR”）体系和亚太经济合作组织隐私识别处理（“APEC PRP”）体系下的认证。

豁免和特殊情况

在某些情况下，如为履行合同所必需、基于个人合法利益或国家利益所需，企业可以在采取合理措施后进行数据跨境传输。此外，匿名处理后的个人数据不作为个人数据对待，可以自由流动。

国际合作

新加坡积极参与国际协调，通过双边或多边协议推动区域内形成统一的数据跨境流动制度。例如，新加坡加入了APEC主导的跨境隐私规则体系（CBPR），并着手开发与CBPR对接的认证机制

数据跨境执法案例

例如，某澳大利亚物流公司新加坡主体因未通过签署数据处理协议履行数据跨境传输义务而被处罚。此案例表明，新加坡主体在使用母公司统

一采购的境外供应商系统时，仍需确保自身履行相关义务。

总体而言，新加坡的数据跨境政策较为宽松，但监管机构执法活跃，企业需要严格遵守相关规定以避免触及监管红线。

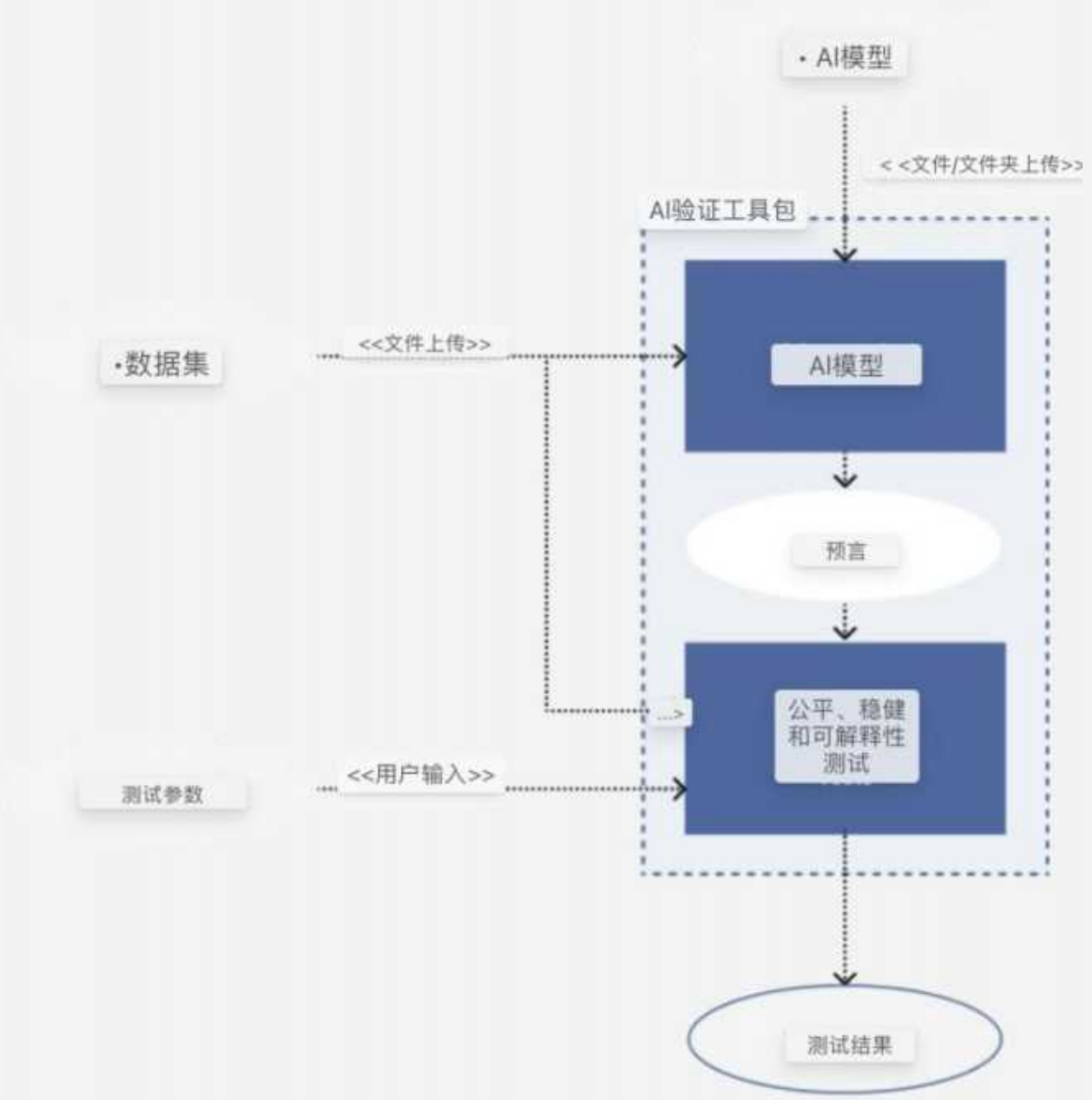
4. 开发者安全责任

新加坡《生成式人工智能治理模型框架》虽然不具有法律约束力，但它反映了政府对人工智能开发和部署的期望，并为行业参与者提供了参考标准，鼓励采用合乎道德和透明的人工智能实践。该框架建议从九个维度全面审视生成式人工智能的开发，其中就包括开发者问责制、可信开发和部署、事件报告等开发者安全责任相关的内容。

2022年5月25日，新加坡IMDA和PDPC还共同推出了全球首个生成式人工智能治理测试框架和工具包：AI Verify-Project Moonshot，这款工具最初是与来自不同行业和不同规模的公司协商开发的，包括-AWS、DBS银行、谷歌、Meta、微软、新加坡航空公司、NCS（Singtel集团的一部分）/陆路运输管理局、渣打银行、UCARE.AI和X0PA.AI。

AI Verify由测试框架、AI验证工具包以及测试报告共同组成。其中测试框架与国际公认的人工智能治理原则、指导方针和框架保持一致，例如来自欧盟、经合组织和新加坡的原则、指导方针和框架，该框架由11项人工智能道德原则和相应的测试标准和测试流程组成。

AI Verify是一个人工智能治理测试框架和工具包。通过使用AI Verify，组织能够结合使用技术测试和基于流程的检查来对其AI系统进行自愿自我评估。反过来，该系统帮助公司试图客观和可验证地向利益相关者证明他们的人工智能系统是以负责任和值得信赖的方式实施的。鉴于人工智能测试方法、标准、指标和工具继续发展，人工智能验证目前也处于“ 最低可行产品 ”（MVP）阶段。这有两层含义。首先，MVP版本有几个技术限制，以及它可以测试或分析的AI模型或数据集的类型和大小限制。其次，预计AI Verify将随着人工智能测试能力的成熟而发展。



2023年10月31日，新加坡媒体发展局（IMDA）和新加坡AI验证基金会推出了首个生成式人工智能（Gen AI）的评估沙盒，该沙盒推出的测试用例将揭示当前Gen AI评估中的差距项，在特定领域（例如人力资源或安全）和目前不发达的文化特定领域，评估沙盒制定了测试基准，用于评估该特定领域的模型性能。

2023年11月，《安全人工智能系统开发指南》由英国国家网络安全中心（NCSC）和美国网络安全与基础设施安全局（CISA）发布，得到了来

自18个国家的23个国际机构的认可，这其中就包括新加坡网络安全局的参与。该指南将帮助人工智能提供商构建按预期运行的人工智能系统，在需要时可用，并在不向未经授权的方泄露敏感数据的情况下工作。新加坡网络安全局敦促所有利益相关者（包括数据科学家、开发人员、经理、决策者和风险所有者）阅读这些指南，以帮助他们就人工智能系统的设计、开发、运营做出明智的决策。

值得注意的是，为在人工智能时代更好地保障个人数据安全，也让使用者能更安心使用AI产品，新加坡在2024年7月宣布，新加坡将推出针对生成式AI开发者的安全指南，旨在将数据透明度和安全性测试，定为AI开发的优先基准和基本要求，新的安全指南也将是新加坡人工智能验证系统AI Verify框架的一部分。

2024年7月15日，PDPC还发布了《隐私增强技术（PET）：合成数据生成拟议指南》，该指南将PET定义为套件工具和技术，允许从数据中处理、分析和提取见解，而不会泄露潜在的个人或商业敏感数据，在指南中PET被分为三类，即数据混淆、加密数据处理和联合分析。数据混淆包括匿名化和假名化、合成数据生成、差异隐私和零知识证明，加密数据处理包括同态加密、多方计算和可信执行环境等技术，而联合分析包括联邦学习和分布式分析。该指南提出了生成合成数据的良好做法，以尽量减少可能的重新识别风险，最终将可能被用于为人工智能（AI）模型生成训练数据集时，用于数据分析和协作以及在软件测试中使用。通过这些应用，合成数据将为金融部门的欺诈检测训练人工智能模型，为研究人工智能偏见而训练人工智能模型，以及为数据分析保护患者数据。

安全的开发和部署责任

在开发环节，新加坡指出人工智能开发的安全措施正在迅速发展，模型开发人员和应用程序部署者最适合决定使用什么安全框架。例如，从人类反馈中强化学习（RLHF）等微调技术可以指导模型产生更符合人类偏好和价值观的“ 更安全 ”输出。检索增强生成（RAG）和几针学习等技术也通常用于减少幻觉和提高准确性。

在部署披露环节，新加坡要求应向下游用户披露相关信息，使他们能够做出更明智的决定。披露领域可能包括使用的数据、培训基础设施、评估结果、缓解措施和安全措施、风险和限制、预期用途和用户数据保护。披露的细节水平可以根据对保护专有信息的透明度进行校准。对于可能构成高风险的模型，例如具有国家安全或社会影响的高级模型，还需要提高政府的透明度。

在测试评估大模型阶段，新加坡认为，除了目前的主要基准测试方法（根据问题和答案的数据集测试模型以评估性能和安全）和红色团队（红色团队充当对手用户来“ 打破 ”模型并诱发安全、安保和其他违规行为）之外，在生成人工智能方面，需要采取更全面和系统的安全评估方法。行业和部门决策者需要共同改进评估基准和工具，同时保持基线和特定部门要求之间的一致性。

模型测试

针对模型安全测试，新加坡主要关注两个问题，一是如何标准化测试，二是测试对象的合格性。

针对如何标准化测试，新加坡认为在短期内，第三方测试将压缩开发人员自己使用的相同基准和评估集，这需要以标准化的方式进行，以使第三方检测有效，并促进模型之间的有意义的可比性。所以，应更加重视

制定共同的测试基准和方法，而对于更成熟的领域，人工智能测试可以通过ISO/IEC和IEEE等标准组织进行编码，以支持更协调、更稳健的第三方测试。

针对测试对象的独立性问题，新加坡认为独立性是确保测试结果客观性和完整性的关键，建立一个合格的第三方测试人员库至关重要，这需要行业机构和政府的共同努力。最终，新加坡可以建立一个认证机制，以确保独立性和能力。

这些模型测试的目的是让大模型适应“ 设计安全 ”，即通过在系统开发生命周期（SDLC）的每个阶段设计安全性，最大限度地减少系统漏洞，减少攻击面，SDLC的关键阶段包括开发、评估、运营和维护。鉴于生成人工智能的独特性，可能需要进行改进以制定新的安全保障措施，包括数据输入过滤器的布置，即使用输入审核工具检测不安全的提示（例如，阻止恶意代码）。同时也包括使用生成人工智能的数字取证工具，数字取证工具用于调查和分析数字数据（如文件内容），以重建网络安全事件，并帮助增强识别和提取可能隐藏在生成人工智能模型中的恶意代码的能力。

事件报告

新加坡政府在《生成式人工智能治理模型框架》中明确指出，事件报告是确保人工智能系统安全和可靠的重要机制。即使有最健全的开发过程和保障措施，人工智能系统也可能出现纰漏。因此，建立结构和流程以进行事件监控和报告是关键。事件报告机制允许及时通知和补救，支持人工智能系统的持续改进。该框架建议实施事件管理系统，以便在发生问题时能够迅速采取行动，确保问题得到及时解决，并防止类似事件再次发生。

此外，事件报告机制还包括对事件的详细记录和分析，以便从中吸取教训，改进系统设计和操作流程。这种做法不仅有助于提高系统的安全性和可靠性，还能增强公众对人工智能技术的信任。新加坡的事件报告机制强调透明度和责任制。通过建立明确的职责范围和报告流程，确保所有相关方在事件发生时能够迅速响应，并采取适当的补救措施。这种机制不仅适用于开发者，还包括使用人工智能系统的各类用户。

5. 内容安全

在新加坡，伴随生成式人工智能产品和技术的广泛应用，确保内容的安全性以及符合正确的价值观导向成为亟待解决的问题。本章节将基于新加坡的监管框架，结合本土的生成式人工智能产品案例，探讨内容安全中价值观导向等相关问题。

1）价值观导向问题

①避免歧视与偏见

新加坡《反歧视法》严禁任何基于种族、宗教、性别、年龄、国籍、婚姻状况、性取向等因素的歧视行为。在生成式人工智能的内容创作与应用中，必须严格遵循此原则。我们目前并未就新加坡当地的AIGC产品发现涉及歧视的内容安全问题，但在国际上有类似案例。

微软于2016年3月在Twitter平台上推出了人工智能聊天机器人Tay。Tay被设定为一个十九岁美国女性，主要目标受众是18岁至24岁的青少年，用户只需在推特上@TayandYou就能得到Tay的回复，而Tay也会借此和Twitter上用户的互动学习。但不到24小时，Tay就被用户“教坏”了，成为一个集反犹太、性别歧视、种族歧视于一身的“不良少女”，并发布了95000多条公然带有种族主义、厌女主义和反犹太主义的推文。微软最终终止了该服务并删除了Tay的所有不当发言。

②维护社会道德与伦理

新加坡社会高度重视道德伦理，生成式人工智能生成的内容须符合相关标准，不得生成鼓励暴力、犯罪、欺诈、淫秽、诽谤等违背公序良俗和法律规定的内容。我们目前并未就新加坡当地的AIGC产品发现涉及道德

伦理的内容安全问题，故以假设性案例进行说明。

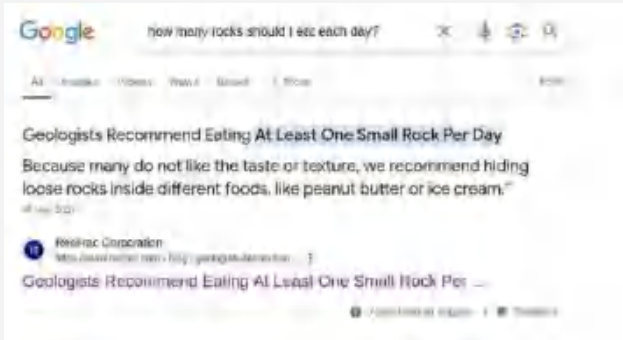
③避免内容实质错误与AI幻觉

除了歧视偏见与道德伦理问题，生成式人工智能还可能产生内容实质错误与幻觉现象，输出荒谬或有害的内容。这方面在国际有相关案例，2024年5月，谷歌宣布将其最新的AI模型植入了搜索引擎，试图一次性追赶竞争对手微软和OpenAI。然而，这项名为“AI Overview（AI概述）”的AI搜索功能一上线便遭遇了滑铁卢，“建议用户使用胶水将芝士固定在披萨上”“推荐每天至少食用一块小石头获取营养”等一连串荒谬的回答不仅让谷歌十分尴尬，也在网上掀起了轩然大波。

建议用户用胶水将芝士固定在披萨上”

推荐每天至少食用一块小石头获取营养”

建议用户用胶水将芝士固定在披萨上



推荐每天至少食用一块小石头获取营养

2）内容审核与监管机制

①企业自我监管

依据《生成式人工智能模型管理框架》，企业在开发和应用生成式人工智能技术时，需建立全面的内容管理和审核体系。

②政府监管与执法

新加坡政府相关部门依据《人工智能治理模型框架》和《组织实施和自我评估指南》等文件，积极履行监管职责，建立起全方位、多层次的监管体系。

政府部门制定了详细的生成式人工智能产品和服务的审核标准与流程，要求企业在产品上市前提交内容审核报告、风险评估报告和合规承诺书等材料。同时，政府定期组织专业人员对市场上的生成式人工智能应用进行抽查和评估，重点检查内容的合法性、公正性、道德性以及准确性，及时发现并处理存在内容实质错误与AI幻觉问题的产品和服务。

对于发现的违规行为，政府依据相关法律法规，对涉事企业处以罚款、责令整改、暂停业务甚至吊销营业执照等处罚措施。此外，政府建立了公众举报平台和奖励机制，鼓励社会公众积极参与监督，对举报属实的个人或机构给予一定的奖励和表彰。

6. 生成物知识产权可版权性

新加坡对于AI生成物可版权性的观点是，人类作者是可版权性的前提。

在Asia Pacific Publishing Pte Ltd 诉 Pioneers & Leaders (Publishers) Pte Ltd 案中，新加坡上诉法院援引了英国 1911 年版权法和 CDPA 作为暗示人类作者的版权立法的例子，因为它们为作者提供终生及 50 年的版权保护。

新加坡上诉法院在 2017 年Global Yellow Pages Ltd 诉 Promedia Directories Pte Ltd案中的一项裁决中，确认了其先前在Asia Pacific Publishing Pte Ltd 诉 Pioneers & Leaders (Publishers) Pte Ltd 案中关于“ 自然人 ”要求的意见，同一法院在该裁决中认为，任何文学作品要享有版权，作者的创作必须与“ 人类智力的运用 ”有因果联系。上诉法院随后将人类智力定义为“ 智力努力的运用……或脑力劳动的锻炼 ”，非人类作者则被视为无法提供这一点。

此外，在新加坡新的《2021 年版权法》中，一系列法定条款一起阅读时表明，只有人类个人或自然人才可以成为“ 作者 ”：（i）期限条款（第 114 条）——期限与一个人的死亡挂钩（即死后 70 年，除非是匿名/假名作品）；（ii）“ 合格个人 ”条款（第 77 条）——只有作者是合格个人，作品的版权才有效；（iii）连接因素条款（第 109、110 条），阐明了未出版和已出版的作者作品中版权存在的条件；以及（iv）道德权利条款（第 370、386、387 条）——其中提到权利本质上是个人权利，以及死亡时权利的转移。

一个相关的问题是，在参与该过程的个人中，谁应该被认定为任何人工

智能输出的人类作者——例如，编写算法的程序员、训练人工智能系统的程序员以及使用人工智能系统生成输出的程序员。根据案例权威，有两个指导原则。

只有创造性的努力才算数

首先，在决定谁是作者时，只计算作者创作的努力，不计算为其他目的而付出的努力。新加坡上诉法院最近在Global Yellow Pages Ltd v Promedia Directories Pte Ltd [2017] SGCA 28 案中重申了这一原则。因此，例如，收集训练数据或将其输入人工智能系统的努力不相关。

没有合作就没有共同作者

其次，如果要确定两个或两个以上的人是共同作者，他们需要进行过合作。Pioneers & Leaders案中强调了这一点。这一要求可能常常被忽视，类似案例是澳大利亚的Acohs Pty Ltd v Ucorp Pty Ltd [2012] FCAFC 16（“ Acohs ”）一案。在Acohs 案中，上诉人的材料安全数据表（“ MSDS ”）被发现不受版权保护。MSDS 是使用计算机程序生成的，上诉人的员工在其中输入了特定数据。然后将这些数据与计算机数据库中的信息相结合以生成 MSDS。问题在于，计算机程序是由一名顾问编写的，而他并没有与使用该程序的员工进行沟通。因此，这些人不能被称为共同作者。鉴于无法确定任何作者或共同作者，澳大利亚联邦法院裁定 MSDS 无权获得任何版权保护。 如果一家公司开发了 AI 系统，另一家公司对其进行了训练，然后提供给第三家公司使用，那么可以想象，这些不同实体的员工之间可能没有任何沟通。在这种情况下，如果参与各个阶段的两名或多名个人对最终成果做出了创造性贡献，但却是各自为政，这可能意味着最终成果将不享有任何版权保护。

7. 大模型透明度

新加坡政府认为，适当的透明度水平和清晰明确地向数据主体解释关于用于决策的数据、数据如何影响决策以及对数据主体的后果，有助于促进数据主体对公司使用人工智能的理解，也有助于确保这些系统、应用程序和算法以透明和公平的方式运行，而清晰地解释并不需要暴露知识产权或发布专有源代码。但在AIDA模型应用于某些特殊用途时，应当设定适当的透明度水平而非一味地提高，因为此时过度的透明度水平可能与使用AIDA的目的相违背。

名词及定义：人工智能与数据分析（AIDA，Artificial Intelligence and Data Analytics)

1）相关文件

新加坡金融管理局（Monetary Authority of Singapore）2018年11月12日发布了，“ 在新加坡金融业使用人工智能和数据分析时促进公平、道德、问责和透明度 “ FEAT的原则 ”。

为提供金融产品和服务的公司提供了一套关于负责任地使用人工智能和数据分析 (AIDA) 的基本原则。这些原则还有助于公司加强围绕数据管理和使用的内部治理，增强公众对使用 AIDA 的信心和信任。

《FEAT原则》专门在第八章Transparency（透明度）中就大模型透明度的相关问题提供了指导原则。

《人工智能治理模型框架》第二版在正文和附件A中也有提及提升大模型透明度的必要性。

2）基本原则

《FEAT原则》认为虽然提高AIDA公司使用AIDA的透明度可以提高公众对AIDA的理解和信心，但过度的透明度可能会造成混乱或为个人利用或操纵AIDA模型创造意想不到的机会。在确定适当的透明度水平时，必须平衡这些考虑因素。《人工智能治理模型框架》第二版同样认为，适当的互动和沟通等提高透明度和解释的行为可以在公司和数据主体(包括员工)之间建立和保持开放的关系，从而激发双方之间的信任和信心。

《FEAT原则》提到，数据主体可能会寻求关于用于决策的数据、数据如何影响决策以及对数据主体的后果的明确解释，清晰地解释并不需要暴露知识产权或发布专有源代码。相反，清晰明确的解释可以侧重于促进数据主体对公司使用AIDA的理解。在大模型透明度的体现中清晰的解释可以遵循以下基本原则：

1.为了提高公众对AIDA使用的信任感，应主动向数据主体披露AIDA的使用情况。

2.在数据主体请求时，向数据主体提供明确的解释，说明使用哪些数据来作出由AIDA驱动的有关数据主体的决策，以及这些数据如何影响决策。

3.在数据主体请求时，向数据主体提供明确的解释，说明由AIDA驱动做出的决策可能对他们产生哪些后果。

12. To increase public confidence, use of AIDA is proactively disclosed to data subjects as part of general communication.

13. Data subjects are provided, upon request, clear explanations on what data is used to make AIDA-driven decisions about the data subject and how the data affects the decision.

14. Data subjects are provided, upon request, clear explanations on the consequences that AIDA-driven decisions may have on them.

8. 用户权利保护

1）用户数据权利：

新加坡生成式人工智能中的个人信息权利适用PDPA的要求。

首先，PDPA对于用户的同意权（User Consent）有着明确的规定。这种同意应当是：1.明确同意：新加坡的PDPA要求企业在收集、使用或披露个人数据之前，必须获得个人数据主体的明确同意。这种同意必须是自愿的、知情的，并且是在充分理解数据将被如何使用的基础上给出的；2.事先同意：同意必须在数据收集、使用或披露之前获得，不能是事后追认的。3.具体同意：同意应当针对特定的数据收集、使用或披露目的，不能是泛泛的、无针对性的。

生成式人工智能的“同意”弹窗则可参考新加坡PDPC发布的《ADVISORY GUIDELINES ON USE OF PERSONAL DATA IN AI RECOMMENDATION AND DECISION SYSTEMS》第9.6、9.7节：

The provision of such information could be through notification pop-ups or included in more detailed written policies that are publicly accessible or made available to end users on request. Organisations should decide the mode of providing such information, based on their own assessment of how this supports their business objectives vis-à-vis user experience.

Example: A bank uses AI to assist in credit scoring when assessing whether to approve applications for credit cards. It prepared a policy document entitled "Bank's Credit Assessment Policy Statement" which provides information about what personal data it collects from applicants and how they are processed by AI when the bank assesses applications. The policy document is provided to applicants who request for the information.

Example: An organisation provides personalised recommendations for content to an individual on its online social media platform. To provide information to individuals as to why specific content is shown to them, the organisation has provided a pop up containing a link to a page to explain why this content is shown and ranked highly on the content feed for the user. The page includes information on why that content is shown, what information has the largest influence over the order of posts in the user's content feed, such as past interactions or membership in specific groups on the platform etc.

Example: An organisation provides a video streaming service. It informs users that its service uses AI to provide recommendations. Through its notification pop-up, it informs users that it collects and analyses users' declaration of topics of interest, browsing activities and media consumption data to recommend videos that users may be interested in. Users are provided the option to consent or decline the use of this feature. The notification pop-up contains a link to its privacy policy, which contains a section that provides information about what declared topics of interest, browsing activity and media consumption data are collected and analysed. This includes the topic classification of videos that users watch, duration and proportion of the video that is played, how many times the video is played, whether the video is watched in a preview window or in actual size, etc. The organisation also explains that the topics of videos that users watch in full are most likely to influence future recommendations.

Example: A social media platform provides an AI system card to its users to explain how its AI System uses user activity data to generate recommendations for its content feed. The system card contains a step-by-step walk through on how the AI System gathers user activity data and broadly processes it in its AI System with other parameters to generate personalised output for a content feed.

此外，根据PDPA，还应确保用户访问和更正权、删除权、限制处理权、反对权、数据可携带权、投诉和寻求救济权。

2）道德和治理框架：

模型人工智能治理框架为部署人工智能解决方案时的道德和治理问题提供指导。它强调可解释性、透明度、公平性、福祉和安全等原则。

3）透明度和问责制：

新加坡金融管理局 (MAS) 已发布原则，以促进金融领域使用人工智能的公平性、道德、问责制和透明度 。

2024 年 1 月推出的生成式人工智能模型人工智能治理框架草案，该框架也解决了与生成式人工智能相关的特定风险，并提供了有关问责制、数据完整性、可信开发和部署、事件报告、测试和保证、安全、内容来源、安全和一致性研发以及公共利益人工智能的指南。

第二章、越南

一）越南生成式人工智能产业及监管

1. 生成式人工智能在越南的发展现状和地位
2. 越南生成式人工智能监管框架

二）越南生成式人工智能合规核心问题

1. 基础模型和AI产品关系及定性
2. 大模型预训练使用公开数据合规
3. 数据本地化和跨境数据
4. 开发者安全责任
5. 内容安全
6. 生成物知识产权可版性
7. 大模型透明度
8. 用户权利保护

一）越南生成式人工智能产业及监管

1. 生成式人工智能在越南的发展现状和地位

1）生成式AI产业政策

随着越南数字化转型不断深入各个领域，人工智能（AI）产品在越南的公共管理、交通、医疗、银行等行业中都拥有广泛的应用前景。越南擅长的是越南语数字助理，并在图像处理、人体和车牌识别摄像头等方面也有优势。但截至目前，越南并没有形成独立的人工智能法案。

A. 在2021年1月26日颁布的第127/QD-TTg号总理决定中，越南政府颁布了《2030年人工智能研究、发展和应用国家战略》，提出了加大人工智能研究、开发和应用力度，目标是到2030年使越南成为东盟领先国家并创立十大知名人工智能品牌，使人工智能成为越南在第四次工业革命时代的一个重要技术产业。

B. 越南科技部（MoST）提议越南政府在2030年前批准一项关于人工智能（AI）研究、开发和应用的国家战略。2024年2月2日，政府批准了一项国家数据战略，为国内人工智能产业发展奠定基础，并设定了确保全国 100% 的国家数据中心、区域数据中心和国家大数据存储与高性能计算中心成功连接的目标。为了实施到2030年的科学、技术和创新发展战略，科技部批准了到2030年的一些国家科学和技术项目。

2）生成式AI企业案例

活跃在越南的生成式AI企业：

1. FPT

网址：https://fpt.com

FPT是越南最大的私营通讯技术公司，业务涵盖人工智能、系统集成、软件开发、信息技术服务等多个领域，是越南科技领域的领军企业。

FPT AI Mentor是FPT公司推出的企业培训顾问，旨在通过虚拟助手帮助企业提升员工的各项能力。FPT AI Mentor的模型支持越南当地IP访问。其模型不直接支持Google Trends功能，但可以通过集成API或其他工具实现。

2. VinBigdata

网址：https://vinbigdata.com

VinBigData是越南领先的人工智能和大数据技术公司，隶属于Vingroup集团，公司成立于Vingroup大数据研究所的科学成果基础上，致力于提供基于大数据和人工智能的先进技术解决方案和产品，在人工智能领域，VinBigData专注于计算机视觉和智能健康领域的人工智能软件解决方案。

VinBigData开发的人工智能模型ViGPT向公众开放，支持越南本地IP访问。

其他国家投资该国情况

越南的数字化转型使其成为国际企业扩展亚洲市场的重要门户，吸引各国投资者进入。

美国英伟达（NVIDIA）在越南部署多个投资项目，并与越南与中央和地方相关机构合作进行筹备，其中包括建立人工智能研究、开发和培训中心。英伟达还与FPT集团达成全面战略合作，以促进人工智能研究，为越南和全球客户提供服务和解决方案，双方计划建设人工智能工厂，培养高素质人力资源。

2. 越南生成式人工智能监管框架

1）越南政府部门治理总框架

A. 2024年7月2日，越南发布了《数字技术产业法》（征求意见稿），该法涵盖了数字技术产业活动、数字技术产品和服务在内的数字技术产业。《数字技术产业法》（征求意见稿）中，越南第一次在法律法规中以专章方式明确了人工智能发展的合规框架。而数字技术产品和服务包括信息技术产品和新技术产品，但不限于人工智能、大数据、云计算、物联网、区块链、虚拟现实/增强现实，以数字化现实、收集、存储、传输、处理信息和数字数据。

B. 在信息和通信部的主持下，公众于 2023 年 4 月至 6 月期间就《人工智能生命周期国家标准》草案提出意见。该草案建立了人工智能开发的生命周期流程，并力求确保人工智能开发安全、合乎道德且透明。它呼吁进行基于风险的评估，以评估和减轻人工智能系统和应用程序的潜在安全风险。

C. 2022年6月，新《保险业务法》(Law on Insurance Business)获得通过，允许在保险业务活动中使用技术。越南政府鼓励保险公司使用包括AI在内的技术来销售创新型保险产品和服务。

虽然越南尚未采用全面的框架来管理和规范人工智能以及越南对生成式人工智能的监管较为粗糙奔放，但监管趋势为师欧盟，以效欧盟。如越南《数字技术产业法》根据影响组织、个人健康、合法权益、人员或财产安全的风险等级进行分类（类似于欧盟《人工智能法案》中的风险分类模式设定）；并规定国家重要信息系统、关键基础设施的安全，以及

应用管理措施和技术控制风险的范围和影响很大。再如《数字技术产业法》规定，人工智能生成的数字技术产品必须贴上标识标签，以确保人工智能系统的输出以机器可读和可检测的格式标记为人工生成或操作。上述条款由越南信息和通信部提出关于人工智能生成的数字产品标签的指导。

2）AI领域主要监管机构及其职责

1. 科学技术部

网址： http://www.most.gov.vn

联系方式：84-4 39439731

2.信息和通信部

网址： https://mic.gov.vn

联系方式：024 35563461

3.公安部

网址：http://www.mps.gov.vn

联系方式：04 38226602

二）越南生成式人工智能合规核心问题

1. 基础模型和AI产品关系及定性

如上文所述，越南尚未采用全面的框架来管理和规范人工智能以及越南对生成式人工智能的监管较为粗糙奔放，但监管趋势为师欧盟，以效欧盟。就越南目前已生效的规定而言，并未对AI产品的监管进行明确的分类规定。

- 基础大模型/通用大模型

对于大模型产品，应重点注意遵守《数字技术产业法》（征求意见稿）、《人工智能生命周期国家标准》草案中关于大模型的基础要求，如开发安全、合乎道德、透明度等。注意，越南科技部在《2030年人工智能研究、发展和应用国家战略》中指出，基础大模型必须具有高透明度和可解释性，以确保模型的训练数据和算法设计不会导致不公平或歧视性结果，数据质量是基础大模型监管的关键要素。不准确或有偏见的数据可能导致模型产生错误或有害的决策。因此，确保数据的准确性和公正性是监管的重要内容。另外，对于通用大模型，越南的信息和通信部在其《AI发展战略》中强调，这类模型的监管需要特别关注领域特定的合规性、隐私保护和数据管理。因此，始终需要关注大模型开发和运营过程中的数据保护问题。

- 模型应用

首先需要注意的是，《数字技术产业法》第83条规定了禁止研发的人工智能产品和技术，包括人工智能基于特定人群（年龄/残疾等）进行行业操控、通过个性化评估形成不利待遇、非监管领域识别或预测个人犯罪的风险、公开网络和视频中处理面部识别、医疗和安全人工智能系统以

外的情绪分析，以及基于生物特征数据对个人进行分类以推断敏感数据六类。因此，首先应确保研发的AI产品不属于禁止类产品。

此外，越南《数字技术产业法》根据影响组织、个人健康、合法权益、人员或财产安全的风险等级对AI风险进行分类。在研发AI产品时，可以初步评估产品落入何等AI风险等级，以符合相应要求。

对于特定行业，如，越南政府鼓励保险公司使用包括AI在内的技术来销售创新型保险产品和服务，鉴于保险业务可能涉及个人健康、财产安全、敏感数据等内容，需要尤为注意符合数据保护法、AI合规方面的要求。

2. 大模型预训练使用公开数据合规

1). 个人信息

2023 年 4 月 17 日越南政府颁布了第 13/2023/ND-CP 号《个人数据保护法令》（Decree Protection of Personal Data，以下简称“ PDPD ”），这部法规适用于在越南境内处理个人数据的所有组织和个人，该法令强调了数据处理的合法性、透明性和目的性，并要求数据处理者采取适当的管理和技术措施来保护个人数据的安全。其中还提到了“ 自动个人数据 ”，自动个人数据处理是通过电子手段进行个人数据处理的一种形式，用于评估、分析和预测特定人员的活动，例如：习惯、兴趣、信任水平、行为、位置、趋势、能力和其他情况。当个人信息用于大模型预训练时应当注意符合PDPD的规定，包括但不限于以下内容：

- 有效同意

在收集和使用个人数据之前，除非法律另有规定，否则必须获得数据主体的有效同意。同意必须是明确的、自愿的，并且数据主体应该能够轻松地撤销同意。将用户信息投入大模型预训练，应当获得用户的明确同意。

- 敏感个人数据处理

对于敏感个人数据（如种族、宗教信仰、政治观点、健康状况等）的处理，通常需要更严格的同意标准和保护措施。注意，若将种族、宗教信仰、政治观点、健康信息等信息数据投入算法预训练的，应当在算法研发设计中，实施词汇转移和阻止词过滤等引导解码策略，避免因个性化差别待遇、内容安全和越南当地的禁忌事项而产生相应纠纷。

- 数据保留期限

必须设定合理的数据保留期限，并在不再需要时删除或匿名化数据。若将用户的个人信息投入大模型预训练建议应当匿名化处理。

(2). 公开数据集

《数字技术产业法》中专门章节对数字技术产业法中的数字数据管理和利用进行了详细说明。该法规明确鼓励企业按照法律规定发展数字数据市场、交易所及数字数据定价活动，并支持开发样本数据集以促进数字技术产品和服务的开发活动。此外，如果国家有内部数据集成的相关政策，该法规也允许组织和个人访问国家机构的开放数据。

《数字技术产业法》还对输入数据作出了明确规定：输入的数字数据应为非个人信息，或是已按照法规标准去标识化的数字数据，或者符合数据法律规定的个人信息。未来，越南可能会对训练数据集实行统一化的交易管理，这将一定程度上保障数据集的质量与合规性，同时促进数据的合理使用和流通。

3. 数据本地化和跨境数据

越南宪法中规定了隐私权和个人秘密权（personal secrets right）。以及政府颁布的第 13/2023/ND-CP 号个人数据保护法令（PDPD），该法令已经于2023 年 7 月 1 日正式生效。

与此同时，越南关于数据保护的法律规定也散见于其他法律中，例如

- 越南第86/2015/QH13号网络信息安全法（Law on Cyber Information Security,以下简称“ LCS ”）；
- 第 24/2018/QH14 号网络安全法（以下简称“ 网络安全法 ”）

以上其他法律规定了关于个人数据保护的相关条款。LCS和网络安全法，提供了基本的数据传输原则，包括个人信息的传输需要数据主体的同意等。

此外，越南是多项国际数据传输协议的缔约方，包括APEC 隐私框架和东盟个人数据保护框架。

目前，越南的数据保护监管机构为公共安全部（Ministry of Public Security，以下简称“ MPS ”）。 国防部、信息通信部、 科技部等其他部委将对MPS的决定提出意见。

A. 数据本地化

在越南开展AI相关业务，在一定条件下可能需要遵守越南《网络安全法》等相关法律规定的数据本地化和当地机构设立义务要求。

规范数据定义：

53号令对《网络安全法》引入的“数据本地化”和“强制性物理设施”要求提供了重要指导和澄清，53号令规范以下数据（“规范数据”）：

- 越南用户的个人数据；
- 越南用户创建的数据，包括帐户名称、使用时间、信用卡信息、电子邮件地址、IP 地址、最近注销和注册电话号码；
- 与越南用户与用户的朋友或与用户互动的其他人的关系有关的数据。（《53号令》，第26.1条）

B. 数据跨境

根据越南《信息技术法》第21条的规定，可以出于以下目的传输数据：

- 签订、修改或实施网络环境中信息、产品或服务的使用合同；
- 计算在网络环境中使用信息、产品或服务的价格和费用；
- 履行《信息技术法》规定的其他义务。

2013年5月16日越南政府《关于电子商务的第52/2013/ND-CP号法令》规定，从电商平台用户收集个人数据的组织可以将此类数据传输给第三方，如果此类传输的目的是：

- 根据数据主体的要求提供服务或产品；
- 履行法律规定的其他义务。

越南2013年7月15日《关于互联网服务和在线信息的管理、提供和使用的第72/2013/ND-CP号法令》规定，提供基于互联网的服务的组织可以传输服务用户的个人数据：

- 根据与另一组织的协议，以开具发票、准备凭证或防止用户逃避合同义务；
- 应国家主管部门的要求。

但是，属于国家秘密的信息，必须经主管机关批准后，方可传输。

目前，越南数据保护法律暂时没有规定数据传输协议/标准合同条款、白名单和国际条约等跨境传输解决方案。

数据跨境传输条件：

- 数据传输方需进行个人数据跨境传输影响评估（TIA），评估内容包括传输方和接收方的详细信息、传输目的、数据类型、保护措施等。
- 评估档案需在处理个人数据之日起60天内提交给越南公安部，并接受事后监管。
- 数据输出方需在传输完成后通知公安部相关信息，并在档案内容发生变化时进行更新。
- 特殊情况下，公安部可要求停止向境外传输个人数据，如数据用于危害国家安全或未遵守评估档案更新规定等。

综上所述，越南的数据跨境传输要求较为严格，在越南进行AI相关业务可能需要进行详细的影响评估并提交给监管部门，同时，在某些特定条件下还需遵守本地化存储要求。

4. 开发者安全责任

针对人工智能系统开发者安全责任，越南目前暂未制定专门法规予以规制。在越南第 24/2018/QH14 号《网络安全法》“ 第四十一条 网络空间服务企业的责任 ” 中对在越南提供网络空间服务的企业负有的网络安全保护责任。在第 13/2023/ND-CP 号《个人数据保护法令》的第三十八、三十九条中列明的个人数据控制者的责任、个人数据处理方的责任。

为了研究并采取措施以减少在开发和使用人工智能过程中可能产生的风险，并在经济、伦理和法律因素之间取得平衡，越南科技部在2024 年 6 月 11 日签发了第 1290/QD-BKHCN 号决定，并随该决定一同发布了《负责任人工智能系统研究与开发原则指南》1.0版（“《人工智能开发指南》”），为开发者研究和开发负责任的人工智能 (AI) 系统提供一系列的原则指导。

越南科技部在《人工智能开发指南》中提出了负责任的人工智能发展的九项基本原则，包括：合作创新、透明度、可控性、安全保障、安全性、隐私保护、尊重人权、用户支持和问责制。

《人工智能开发指南》中指出，开发者针对可能影响用户或相关第三方生命、安全、隐私或财产的人工智能系统，需要注意系统输入和输出的明确性以及基于所应用技术特性和使用方式的可解释性，以确保用户在内的社会信任。开发者还需要确保人工智能系统的可控性。首先，开发者需要进行事先评估与人工智能系统控制能力相关的风险（评估系统是否满足相关技术要求和标准）。评估风险的一种方法是在实验室或已采取安全保障措施的测试环境中进行测试，然后再实际应用。此外，为确

保人工智能系统的可控性，开发者还需要注意系统监控（有评估/监控工具或根据用户反馈进行调整/更新）和应对措施（如系统断开、断网等），这些措施可以由人类或其他可靠的人工智能系统执行。

关于人工智能系统的安全保障，　开发者需要确保人工智能系统不会对用户或第三方的生命、安全或财产造成损害。对于这一问题，越南科技部原则上鼓励开发者参考相关国际标准，但同时提出了以下几点注意事项，特别是由于人工智能系统训练过程中的输出或程序变化：

1）进行事先评估，以识别和减少与系统安全相关的风险；
2）在人工智能系统开发的各个阶段，采取有效措施确保内在安全（减少风险因素，如设备的能量水平）和功能安全（通过使用附加控制设备减少风险，如发生故障时自动停止）；
3）向相关方解释系统设计者的意图和适用性；
4）对用户和第三方的生命、安全或财产进行安全评估（例如，优先考虑保护人类生命、安全、财产的设计思路）。

同时，开发者还需要注意人工智能系统的安全性。除了遵守专业机构和权威机构的相关文件、指导和信息安全措施外，开发者还需注意以下几点，特别是人工智能系统在训练过程中产生的输出或程序变更：（1）需要关注系统的可靠性（即是否能按预期运行且不被非法第三方干扰）和抵御攻击或物理事故的能力。确保人工智能系统的安全性、完整性，以及与人工智能系统信息安全性相关的必要信息的可用性；（2）进行事前评估，以识别和控制与人工智能系统安全相关的风险；（3）　在人工智能系统开发过程中，采取必要措施以保持安全性，基于所应用技术的特点（设计时的安全性）。

5. 内容安全

相关法规及监管

越南政府在制定相关法律法规和指导方针时，特别强调了生成式人工智能产品的内容安全问题。具体来说：

《人工智能开发指南》 中明确要求开发者确保人工智能系统不会侵犯用户或第三方的隐私权。该指南还强调开发者在开发与人类相关的人工智能系统时应特别关注尊重相关个人的人权和尊严。此外，开发者需采取预防措施，确保人工智能系统不会违反越南基本原则中的人类价值和社会道德。

《数字技术产业法》（征求意见稿） 中提出国家鼓励企业、组织和个人开发、提供、部署和使用可靠的、以人为本的人工智能系统，并要求对人工智能系统按照对“ 组织、个人健康、合法权益、人身或者财产安全 ”影响的风险程度进行分类。该草案还规定了个人智能生成物的可识别性要求，即由人工智能创造的数字技术产品必须带有识别标签，以确保人工智能系统的输出以人工创建或操纵的机器可读和可检测的格式进行标记。

《人工智能生命周期国家标准》草案提出了人工智能开发的生命周期流程，并力求确保人工智能开发安全、合乎道德且透明。该草案呼吁进行基于风险的评估，以评估和减轻人工智能系统和应用程序的潜在安全风险。

虽然目前尚未发现具体的监管案例，但从上述法律法规和指导方针中可

以看出越南政府对于人工智能产品内容安全的高度关注。越南政府希望通过建立相应的监管框架来确保人工智能技术的健康发展，并平衡商业利益与消费者权益。

6. 生成物知识产权可版权性

越南对于AI生成物可版权性暂无定论。

根据2021年出台的《2030年人工智能研究、发展和应用国家战略》，越南计划在2030年之前制定与人工智能相关的知识产权的附加法律文件。

根据越南《知识产权法》第 143条，作品必须由作者通过智力劳动直接创作，不得抄袭他人作品。实际上，为了确保越南版权保护的质量，作品必须具有原创性(即作者自己的智力创作)和创造性(即足够的智力创造力)。版权自作品被固定在有形媒介之时起就存在(无论其内容、质量、形式、模式和语言，也无论该作品是否已出版或注册)，只要它符合独创性要求(这意味着它是独立创作的，不是抄袭别人的作品，并且表现出了一点创造力。)

暂未检索到越南关于AI生成物可版权性相关的案例及新闻。

我们认为，越南《知识产权法》也强调了作为作者的“ 人 ”的存在，以及人的原创性和创造力，可参考新加坡当前对于该问题的态度。

7. 大模型透明度

2023 年 4 月 20 日，信息和通信部 (MIC) 就《人工智能和大数据国家标准》草案征求公众意见。该草案提及了建立人工智能模块质量保证和透明度的目标，提出了人工智能安全、隐私和道德方面的质量要求。但暂时未提出为实现透明度这一目标更详细的要求。

8. 用户权利保护

越南积极制定AI指导方针和原则，并高度重视用户权利。以下是越南人工智能用户权利的要点：

1.用户数据权利及安全：

科技部（MOST）发布了优先考虑用户安全和隐私的指导方针。这些指导方针强调，人工智能系统不得直接或间接损害用户或第三方。开发人员必须确保人工智能系统的安全性、可靠性和物理完整性，同时保护用户隐私，包括保护空间隐私、个人数据和通信机密性。此外，《数据法》草案概述了禁止的人工智能行为，包括用于根据敏感标准评估或分类个人的系统。

2.生成内容安全：

越南第 24/2018/QH14 号《网络安全法》，要求平台所有者根据网络安全机构的要求预防、检测和删除有害内容。这项法律体现了针对人工智能生成内容的互联网审查法规日益增多的趋势。

3.透明度和问责制：

信息和通信部（MIC）就《人工智能和大数据国家标准》详细说明了建立人工智能模块质量保证和透明度的目标，提出了人工智能安全、隐私和道德方面的质量要求，高度强调对利益相关者的问责制和对用户的支持。

4.反歧视：

指南提倡尊重人权和尊严。开发人员应采取措施防止因训练数据存在偏见而导致的歧视或不公平。道德规范对于最大限度地发挥人工智能应用的优势和减少其危害至关重要。

第三章、泰国

一）泰国生成式人工智能产业及监管

1. 生成式人工智能在泰国的发展现状和地位
2. 泰国生成式人工智能监管框架

二）泰国生成式人工智能合规核心问题

1. 基础模型和AI产品关系及定性
2. 大模型预训练使用公开数据合规
3. 数据本地化和跨境数据
4. 开发者安全责任
5. 内容安全
6. 生成物知识产权可版性
7. 大模型透明度
8. 用户权利保护

一）泰国生成式人工智能产业及监管

1. 生成式人工智能在泰国的发展现状和地位

1）生成式AI产业政策

自2022年起，泰国高等教育与科研创新部（MHESI）启动国家人工智能发展计划，同时还打造了相关创新成果，如OpenThaiGPT这样一款泰语聊天机器人，以及编写泰国首本《人工智能伦理指南书》。

泰国高等教育与科研创新部（MHESI）联合泰国数字经济与社会部（DE）牵头启动6个项目，以推动泰国《国家人工智能发展战略》第二阶段（2024-2027）全方位落地实施。2024年开年，泰国高等教育与科研创新部（MHESI）联合泰国数字经济与社会部（DE），讨论了泰国《国家人工智能发展战略》第二阶段（2024-2027）驱动下的试点项目（草案），拟定了6个重点项目，以此来推动泰国人工智能全方位落地实施。

ETDA 关于人工智能创新测试中心（沙盒）的公告草案和ETDA 关于使用人工智能系统的风险评估的公告草案（均发布于2023 年 7 月 18 日）。除了国家行动计划外，泰国电子交易发展局就人工智能沙盒和人工智能风险评估通知草案以及促进国家人工智能创新法案草案举行了公众咨询（已于 2023 年 8 月结束）。该机构预计将继续关注人工智能，并可能提出更多法规和指导方针草案供公众咨询。在公共部门，数字政府机构已为政府服务推出了人工智能框架，并就公共部门的人工智能伦理提出了政策建议，为政府采用人工智能做好准备。然而，政府机构对在其运营中使用人工智能仍持谨慎态度。

2）生成式AI企业案例

活跃在泰国的生成式AI企业：

①Amity Solutions

网址：https://www.amitysolutions.com/

Amity Solutions是一家位于泰国曼谷的软件服务提供商。自2012年成立以来，Amity Solutions逐步发展成为泰国领先的人工智能SaaS提供商。其核心产品包括企业聊天机器人平台Amity Bots、语音机器人平台Amity Voice、以及企业员工协作平台Eko等。自2023年初以来，Amity Solutions已将其主要重心转向生成式AI应用程序和解决方案的开发和构建。

②华为云（Huawei Cloud）

华为云通过其AI原生数据库GaussDB及先锋计划，助力泰国的数字化转型。华为在曼谷举办了2024华为云数据库泰国峰会，展示了GaussDB解决方案，并推出了GaussDB先锋计划，以促进泰国数据库技术的创新应用。华为云还在泰国发布了GaussDB(DWS) 3.0，新一代云原生数据仓库，进一步推动泰国的AI和数字化基础设施发展。

③阿里云

阿里巴巴集团旗下阿里云宣布将在包括泰国在内的全球多个国家投资新建数据中心，重点布局AI基础设施。同时，阿里云AI技术将首次“出海”。阿里云宣布，大模型服务平台百炼国际版即将上线，提供一站式、全托管的大模型定制与应用服务；阿里云最新版基座模型通义千问2.5将通过百炼平台提供API。

阿里巴巴集团旗下阿里大文娱集团与泰国T&B环球媒体集团联合举办了数字人产品“ 禄小斋 ”，这是中国企业为海外市场打造的首个超写实大模型数字人。大文娱团队通过运用AI技术和数字人技术，从外形到交互都力争接近真人。在虚实互动上，禄小斋接入“ 通义星辰 ”大模型，可以开放式回答各类问题。

其他国家投资该国情况

泰国基于其高质量基础设施、极具吸引力的激励措施等优势吸引了全球多个国家前来投资。

①亚马逊网络服务（AWS）作为行业领头羊， 宣布将斥资高达 2000 亿泰铢在泰国开发数据中心，其中 250 亿泰铢将用于建设三个设施。AWS计划到2037年在泰国投资建设价值超过1900亿泰铢的数据中心，以推动泰国的数字化转型进程。AWS泰国国家总监瓦特森表示，AWS亚太（曼谷）区域将于2025年初在泰国设立，预计到2037年投资额将超过1900亿泰铢。在人工智能人才培养方面，自2017年以来，AWS已为50,000多名泰国人提供了云技能培训，计划2026年培训人数达到100,000 人。

②微软首席执行官萨蒂亚·纳德拉宣布在泰国投资创建第一个区域数据中心，以促进云端和人工智能（AI）基础设施的发展，并承诺为超过10万泰国人提供人工智能培训以开发技术。微软是继亚马逊和谷歌之后又一家在泰国建设新的云计算和人工智能基础设施的美国科技巨头。

此外，其他获得泰国投资委员会投资激励的公司也承诺在泰国进行巨额投资。澳大利亚的NextDC宣布投资预算137亿泰铢，新加坡的STT GDC

AI人工智能产业链联盟

#每日为你摘取最重要的商业新闻#

更新 · 更快 · 更精彩

Zero

AI音乐创作人
水墨动漫联盟创始人
百脑共创联合创始人
人工智能产业链联盟创始人
中关村人才协会秘书长助理
河北北大企业家分会秘书长
墨玫星辰智能科技有限公司CEO
河北清华发展研究院智能机器人中心线上负责人
中关村人才协会数字体育与电子竞技专委会秘书长助理

主要业务:AI商业化答疑及课程应用场景探索，各类AI产品学习手册，答疑及课程

欢迎扫码交流

提供：学习手册/工具/资源链接/商业化案例/行业报告/行业最新资讯及动态

人工智能产业链联盟创始人

邀请你加入星球，一起学习

人工智能产业链联盟报告库

星主：人工智能产业链联盟创始人

每天仅需0.5元，即可拥有以下福利！
每周更新各类机构的最新研究成果。立志将人工智能产业链联盟打造成市面上最全的AI研究资料库，覆盖券商、产业公司、研究院所等...

知识星球

微信扫码加入星球

承诺投资45亿泰铢，新加坡的Evolution Data Center承诺投资40亿泰铢，美国Supernap（Switch）承诺投资30亿泰铢，日本Telehouse承诺投资27亿泰铢，香港One Asia承诺投资20亿泰铢。

2. 泰国生成式人工智能监管框架

1）泰国政府部门治理总框架

泰国目前暂无AI和机器学习专项法律。泰国有意进行监管，但方式尚待确定。据曼谷邮报报道，泰国国家数字经济与社会委员会秘书长普查坦表示，该委员会已制定人工智能道德准则。数字经济促进小组将研究起草人工智能法规，对违反人工智能道德的行为者进行强制执行。2024年6月14日，泰国国家数字经济和社会委员会办公室宣布，已指示泰国电子交易发展局（ETDA）制定人工智能监管立法。在制定法规的同时，ETDA 正在审查欧盟《人工智能法案》等先例是否适用于泰国，同时考虑到欧盟和泰国之间不同的文化规范和价值观。

2022年，泰国政府部门开始研究多个司法管辖区在监管人工智能方面的监管发展和方法，结果两个不同的监管机构提出了两份不同的立法草案。 两部法律草案对人工智能监管的目标各不相同：《人工智能皇家法令草案》建议制定更严格的规则，而《人工智能法案草案》则倾向于在保护消费者的同时促进人工智能发展。然而，在人工智能立法的这些阶段，他们的立法计划仍不确定。

①《关于使用人工智能系统的商业运营的皇家法令草案》（AI 皇家法令草案）于 2022 年底由国家数字经济和社会委员会（ONDE）办公室在公开听证会上首次提出。它将根据《电子交易法》 BE 2544 (2001)（ETA）颁布，该法案赋予发布此类法令的权力。

②泰国《促进和支持人工智能创新法案》（草案）（2023年7月18日)。《泰国促进和支持人工智能创新法案草案》（AI 法案草案）于 2023 年

初由电子交易发展局 (ETDA) 首次提出，随后于 2023 年中期进行了更新并再次公开听证。与 AI 皇家法令草案不同，AI 法案草案旨在作为一项单独的法案颁布，不受 ETA 约束。

③《政府管理和服务人工智能》（2019 年 11 月）

④《人工智能政府框架》（2019 年 12 月）

2）AI领域主要监管机构及其职责

①国家数字经济和社会部（MDES）
网址：https://www.mdes.go.th/home
联系方式：02-141-6747

②泰国数字经济促进局（Digital Economy Promotion Agency，DEPA）
网址：https://www.depa.or.th/th/
联系方式：+66 2026 2333

③电子交易发展机构（Electronic Transactions Development Agency，ETDA）
网址: https://www.etda.or.th/en/
联系方式：02 123 1234

二）泰国生成式人工智能合规核心问题

1. 基础模型和AI产品关系及定性

目前，泰国暂无AI监管的具体立法，目前立法态度也仍处于不确定中。根据目前尚在讨论中的草案，就大模型而言，应当侧重于遵守《人工智能皇家法令草案》中关于大模型的基础要求，包括透明度、数据质量等方面的要求；就模型的具体应用而言，泰国就AI系统根据风险等级进行分类管理，具体的AI产品应注意明确风险定位并遵守根据该风险等级所适用的相关规定。但是具体的监管规定仍有待于泰国相关立法的出台。

2. 大模型预训练使用公开数据合规

1）泰国对于AI大模型训练数据的规定主要集中在数据保护和个人信息保护方面。泰国的个人数据保护法（PDPA）规定了收集、保护、使用、披露、转移和个人数据处理的要求。该法区分了数据管控者和数据处理者，并要求对个人数据进行合法、公平、透明的处理，具体规定如下：

①数据使用合法性：AI训练数据的收集和使用需遵循PDPA的规定，确保数据处理的合法性、正当性和透明度。

②数据主体同意：如果涉及个人数据，必须获得数据主体的有效同意才能用于训练AI模型。此外，数据主体有权知道其数据将如何被使用，并且有权撤回同意。

③数据最小化原则：仅收集实现目的所必需的数据，并且不得过度收集。

④数据准确性和更新：保持数据的准确性，并定期更新以确保数据的时效性。

⑤数据安全性：采取适当的安全措施来保护个人数据免受未经授权的访问、使用、泄露、篡改或破坏。

⑥非个人信息或去标识化数据：训练数据如果是非个人信息或已经按照法规标准去标识化的数据，则可以在一定程度上减少限制。

⑦数据集成政策：若泰国政府有内部数据集成政策，允许组织和个人访问国家机构的开放数据，这可能为AI训练提供更多的数据资源。

2）根据《资本市场中人工智能（Artificial Intelligence）和机器学习（Machine Learning）的使用监管框架》的规定，在资本市场的领域中使用的AI预训练数据做出了明确的要求，由于AI大模型在工作中需要使用数据来学习和处理，因此企业以及业务人员应该做好数据准备，对于数据准备具体包括以下基本步骤：

①确定信息的属性和质量：经营者应确定信息的属性和质量。这是为了让AI能够根据既定目标高效工作，因此需要考虑所需数据的类型、数据的大小、数据的准确性以及内部存储的信息所需的时间段（时间序列数据）等

②数据收集和集成：经营者应收集和集成不同来源的数据（数据集成），以获得完整和全面的信息。根据需要集成后并完成数据收集应准备文件以显示数据来源（数据出处），包括任何处理或更改的详细信息、数据准备过程（数据谱系），以便在AI大模型出现故障时进行追溯

检查（可追溯性）。

③识别数据类型：为模型的教学、验证和测试准备数据时，应该正确识别数据类型（Data Labelling），以便AI大模型拥有数据并能够正确识别数据的含义。

④数据质量评估：在将数据集用于模型教学、验证和测试之前，应根据组织制定的标准对数据质量进行评估和改进。

⑤个人信息保护：在使用个人信息或敏感信息（Sensitive Data）时，经营者应采取适当的个人信息保护措施，以降低个人信息泄露的风险，例如访问控制、加密和匿名化，防止信息泄露。

⑥训练、测试、验证数据集：使用验证数据集（Validation Dataset）检查模型的性能，在此阶段可以对模型进行调整（Tuning），直到给出结果。根据预期目标在实际应用前的最后阶段对模型进行测试。测试需要使用测试数据集（Testing Dataset），测试数据集与训练数据集和验证数据集不同。

上述规定为泰国企业在使用AI大模型时提供了较为清晰的数据准备指南。企业需确保数据的合法性、准确性和安全性，同时采取措施保护个人信息。数据准备过程包括确定信息属性、集成多源数据、识别数据类型、评估数据质量，并实施个人信息保护措施。最终通过训练、验证和测试数据集确保AI模型的性能达到预期目标。这些步骤有助于构建可靠且合规的AI系统，促进泰国AI行业的健康发展。

3. 数据本地化和跨境数据

在泰国，随着《个人数据保护法》（PDPA）的实施，数据保护成为各行业关注的焦点。尤其在生成式人工智能领域，数据的本地化和跨境传输要求对技术的发展和应用有着深远影响。生成式人工智能依赖于大量数据进行训练和优化，因此数据的处理和保护成为核心问题。尽管泰国目前没有强制的数据本地化要求，但跨境数据传输仍需满足严格的规定，以确保数据的安全与合规。

泰国PDPA于2019年5月17日公布，是泰国第一部提供一般数据保护的综合立法，预计2022年6月1日生效。

除此外，泰国数字经济和社会部（MDES）发布了《关于个人数据安全标准BE 2563 (2020)》（以下简称“ MDES通知 ”），提供了有关个人数据安全的规则和要求，包括维护个人数据的机密性、完整性和可用性以及防止非法丢失、访问、使用、更改、更正或披露个人数据等方面。《网络安全法案》是一系列数字相关法案之一，于2019年制定。

泰国数据保护法律主要包括：

①《个人数据保护法》（“ PDPA ”）
②《网络安全法案》
③《关于个人数据安全标准BE 2563 (2020)》（简称“ MDES通知 ”）

根据PDPA，泰国的数据监管机构是“ 个人数据保护委员会 ” The Personal Data Protection Committee (以下简称“ PDPC ”)。

1）数据本地化

目前，泰国PDPA或泰国的任何其他法律均未包含与个人数据相关的数据本地化要求。

2）数据跨境要求

-一般规定

根据PDPA第28条，只有外国或者国际组织的数据保护水平满足PDPA的要求才能进行数据传输。

但是，某些情况不受此要求的约束。并且对于个人数据的跨境传输，数据控制者必须在转移之前或转移时获得数据主体的同意。

-例外情况

根据 PDPA，在以下情况下可以将数据从泰国传输到保护水平不满足PDPC要求的外国或国际组织：

- 法律要求进行此类传输；
- 已获得数据主体的同意。如果接收国或者国际组织的数据保护水平并未达到PDPC的要求的水平，在进行传输之前，控制者需要确保将数据保护水平不满足PDPC要求的情况告知数据主体并且获得数据主体同意。
- 履行与数据主体在合同中约定的义务所必需；
- 数据控制者与其他人订立的合同约定的义务，其中受益主体是数据主体。
- 是为了防止或抑制对数据主体或其他人的生命、身体或健康造成的

危险；

- 为重大公共利益而有必要进行此类传输。

对于生成式人工智能产业而言，泰国的PDPA提供了明确的框架。虽然没有数据本地化要求，但在数据跨境传输方面，企业必须确保数据保护水平符合PDPA标准，或在特定情况下获得数据主体的明确同意。这些规定保障了数据在跨境传输过程中的安全性和合法性，促使生成式人工智能企业在泰国境内外都能合规运营，同时推动了技术创新与国际合作的发展。

4. 开发者安全责任

在《关于使用人工智能系统的商业运营的皇家法令草案》提出， 高风险的人工智能系统服务（包括可能产生不公平歧视或影响个人自由的服务）的服务开发者除履行登记要求外，还有责任确保其系统在整个服务期间内具备且遵守适当的风险管理措施，并向公众发布相关信息。无论是自建系统或引用他人提供的资料或文件，均需向公众发布。具体需发布内容包括：

1. 系统风险管理流程；
2.数据管理和数据治理流程；
3.相关技术文件；
4.系统运行记录保存流程；
5.用户信息或文件发布；
6.人工监督控制流程；
7. 系统准确性、一致性和安全控制流程。

如果人工智能系统出现不符合该法令规定的情况，开发者应立即采取包括暂停服务或召回相关产品，并通知电子交易发展办公室等措施。在国外运营但涉及向泰国用户提供服务的人工智能系统开发者需在电子交易发展办公室登记其业务，并指定在泰国的代表。

在透明度要求上，开发者针对与人类互动的人工智能系统中必须告知用户他们正在与人工智能系统互动。如涉及使用人工智能系统检测情绪或识别生物特征信息时，也需告知用户。当使用人工智能系统生成或修改图像、声音或视频时，可能导致误认为是真实或原物的，开发者也有有义务向公众披露这些内容是人工合成或被修改过的。

5. 内容安全

相关法规及监管

泰国政府在制定相关法律法规和指导方针时，特别强调了生成式人工智能产品的内容安全问题。具体来说：

《AI伦理原则及指引》将透明性和责任作为AI伦理原则之一，要求人工智能的研究、设计、开发、服务和应用应该保持透明，能够解释和预测，包括可以追溯各种活动。《关于使用人工智能系统的商业运营的皇家法令草案》提出，高风险的人工智能系统服务的服务开发者除履行登记要求外，还有责任确保其系统在整个服务期间内具备且遵守适当的风险管理措施，并向公众发布相关信息。《泰国促进和支持人工智能创新法案草案》以及两项子法规草案征求公众意见，旨在通过提供人工智能监管沙箱、要求部分最低限度的内容需要向公众披露，以确保透明度并防止不公平的歧视性合同条款，促进人工智能的发展。

虽然目前尚未发现具体的监管案例，但从上述法律法规和指导方针中可以看出泰国政府对于人工智能产品内容安全的高度关注。泰国政府希望通过建立相应的监管框架来确保人工智能技术的健康发展，并平衡商业利益与消费者权益。

6. 生成物知识产权可版权性

泰国对于AI生成物可版权性暂无定论。

根据泰国《版权法》，可以注册版权的是作者在未抄袭他人的情况下创作的原创作品。对于AI生成物在哪些条件下可以视为原创作品，AI是否可以被视作作者，或者谁应该被认定为人工智能输出的人类作者的问题均没有法律法规可以解答。

另外，暂未检索到泰国关于AI生成物可版权性相关的案例及新闻。

7. 大模型透明度

泰国《AI伦理原则及指引》将透明性和责任作为AI伦理原则之一。具体包括：

1）人工智能的研究、设计、开发、服务和应用应该保持透明，能够解释和预测，包括可以追溯各种活动。

2）人工智能应具备可追溯性（Traceability），能够监控、检查异常并诊断故障（Diagnosability）。

3）研究人员、设计师、开发者、服务提供商和用户都应对人工智能带来的影响承担相应的责任（Accountability）。

《AI伦理原则和指引》还指出，为了提高用户对产品透明度和可追溯性的满意度，确保人工智能技术的透明性和责任机制是至关重要的。

泰国于2022年发布《关于使用人工智能系统的商业运作的皇家法令草案（“ 皇家法令草案 ”）》，该皇家法令草案由国家数字经济和社会委员会办公室（“ ONDE ”）根据《电子交易法》BE 2544 (2001)（“ ETA ”）提出并发布。

皇家法令草案规定，高风险人工智能系统的提供商必须遵守或实施以下要求：

- 风险管理体系，
- 数据和数据治理，
- 技术文档，
- 保持记录中，
- 向部署者提供透明度和信息，
- 人类监督，
- 准确性、稳健性和网络安全性。

除 ONDE 的皇家法令草案下的监管方面外，电子交易发展局（“ ETDA ”）还于 2023 年 7 月就《泰国人工智能促进和支持法案草案》（“ 法案草案 ”）以及两项子法规草案征求公众意见，即（i）《ETDA 关于使用人工智能系统的风险评估通知草案》和（ii）《ETDA 关于人工智能沙盒的通知草案》。

这些草案旨在通过提供人工智能监管沙箱、要求部分最低限度的内容需要向公众披露，以确保透明度并防止不公平的歧视性合同条款； 放宽或豁免某些法律以及相关部门的支持来促进人工智能的发展。鉴于人工智能发展的快速进步，草案将如何发展仍有待观察。

8. 用户权利保护

泰国的《个人数据保护法》（PDPA）旨在保护个人数据主体的权利。虽然PDPA中没有直接提到人工智能用户的具体权利，但PDPA的相关规定同样适用于人工智能领域的数据处理。由于PDPA明确了数据主体的知情权、访问权、纠正权、删除权、更新权以及获得匿名化数据的权利，因此，这些规定一定程度上确保了用户在使用生成式AI过程中个人数据被收集、处理和使用时的透明度和安全性。

第四章、马来西亚

一）马来西亚生成式人工智能产业及监管

1. 生成式人工智能在马来西亚的发展现状和地位
2. 马来西亚生成式人工智能监管框架

二）马来西亚生成式人工智能合规核心问题

1. 基础模型和AI产品关系及定性
2. 大模型预训练使用公开数据合规
3. 数据本地化和跨境数据
4. 开发者安全责任
5. 内容安全
6. 生成物知识产权可版性
7. 大模型透明度
8. 用户权利保护

一）马来西亚生成式人工智能产业及监管

1. 生成式人工智能在马来西亚的发展现状和地位

1）生成式AI产业政策

马来西亚科技创新部 (MOSTI) 发布《2021-2025年国家人工智能路线图》(Artificial Intelligence Roadmap 2021-2025)，阐明国家促进AI发展的六项战略以及负责任AI的七项原则。

2）生成式AI企业案例

活跃在马来西亚的生成式AI企业：

①VOX

VOX是马来西亚的人工智能技术服务公司，成立于2021年。VOX公司专注于对话式AI技术，帮助企业与客户进行自动化对话服务，致力于通过生成式AI提供无缝的对话体验，为企业提供高效、智能的客户服务解决方案。其主要产品Sharly.ai能够处理上千页的上传文件，与用户进行高效互动。

VOX公司将GPT3接入到自身的自动化对话平台中，并推出一款人工智能对话助手Sharly.ai，Sharly.ai与ChatGPT类似，能够帮助用户分析文档并以对话的形式回应用户对文档内容的询问，Sharly.ai支持马来西亚IP访问，但目前仅支持英文内容。

②字节跳动

字节跳动成立于2012年，是一家跨国互联网技术公司，主要产品包括抖音、今日头条、西瓜视频、飞书、剪映等。

字节跳动投入100 亿马币（约合 21.3 亿美元）以建立一个区域人工智能中心，推动相关技术于该国发展。另外，该公司还额外投入 15 亿马币用于扩建其在当地的数据中心。

字节跳动的主要产品及其应用场景同新加坡部分。

其他国家投资该国情况

马来西亚在人工智能领域成绩瞩目，吸引大量海外投资，微软、谷歌等行业巨头均投资马来西亚人工智能建设，这些投资不仅将助力马来西亚加速数字化转型，还有望提升其在全球科技领域的地位。

微软在2024年也宣布将在未来四年内对马来西亚投资约22亿美元，用于支持该国的数字化转型及人工智能基础设施的建设。这笔投资是微软在马来西亚32年来的最大单笔投资，显示出其对马来西亚市场的重视和信心。

谷歌宣布了在马来西亚的加码计划，将投资约20亿美元建设当地首个数据中心和谷歌云区域。这笔投资将进一步提升谷歌在东南亚地区的云服务能力，满足日益增长的人工智能和云服务需求。

此外，马来西亚也吸引了英伟达和英飞凌等企业的投资，国内移动互联网的代表，阿里巴巴、蚂蚁集团等公司也通过建平台、投资、技术支持等方式开始布局马来西亚市场。

2. 马来西亚生成式人工智能监管框架

1）马来西亚政府部门治理总框架

建立人工智能治理属于科技创新部的职权范围。科技创新部启动了《2021-2025年国家人工智能路线图》。此外，科技创新部部长计划制定一项全面的人工智能法案。这项立法工作将涉及与技术专家、法律专业人士、利益相关者和公众的磋商，以确保其稳健性和相关性。然而，截至目前，马来西亚还没有专门针对人工智能治理的立法，由此产生的任何问题都将仅限于现有的法规、法规和行业行为准则作为最佳实践指南。

2）马来西亚现行的人工智能相关法律法规

① 知识产权法

与生成式人工智能相关的主要问题围绕其生成的知识产权的所有权。在马来西亚专利法的背景下，主要问题是人工智能是否可以根据 1983 年《专利法》和 1986 年《专利条例》被视为发明人。在专利申请中，申请专利的人通常会成为专利所有者，拥有发明的专有权，并可以对未经许可使用该发明的任何人采取法律行动。发明人可以与申请人/所有者相同，也可以将权利转让给其他人。在人工智能生成的发明中，人们一致认为申请人/所有者必须是人类。但是，发明人是否必须是人类仍不确定。

此外，人工智能生成的作品是否受到 1987 年《版权法》的保护也仍是一个灰色地带。在马来西亚的《版权法》中，它规定了必须有人类作者，这使得版权不太可能适用于人工智能生成的内容。然而，人工智能

创造的成果有可能获得版权保护。因此，最终产品是否有资格获得版权保护将取决于它们是否符合《版权法》第 7 条概述的标准，该标准涉及评估是否已付出足够的努力使作品具有原创性。

②个人数据保护法

2010 年《个人数据保护法》具有重要意义，因为人工智能的使用通常需要收集和处理与商业交易有关的个人数据。2010 年《个人数据保护法》规定了七项个人数据保护原则，数据用户（即处理任何个人数据的人）必须遵守这些原则。因此，数据用户使用人工智能处理的个人数据仍必须按照这些原则进行处理。

以一般原则为例，一般要求同意作为处理数据的条件。这可能意味着数据用户必须确保所使用的人工智能不会在数据主体同意范围之外处理个人数据。在使用人工智能处理个人数据时，与个人数据安全性和完整性相关的其他原则也具有直接相关性。遵守 PDPA 可能会最大限度地减少数据用户在使用人工智能处理个人数据时承担的责任。

③就业法

当使用人工智能技术裁员时，雇主必须注意，马来西亚的解雇必须有正当理由和理由，雇主需要能够解释解雇的原因，因此他们需要知道算法是如何做出决定的，为什么某些员工被选中而其他员工被留用。从本质上讲，雇主必须能够准确指出人工智能使用的确切数据点，而这几乎是不可能的，因为人工智能有复杂的算法并使用多个数据点。

在判定绩效不佳时，雇主必须证明已向员工发出足够的通知/警告，强调其绩效不佳，并向员工提供了合理的机会来改善其工作绩效。

④合同法

如果满足有效合同的构成要素（要约、承诺、对价和建立法律关系的意图），基于人工智能的合同可能根据《1950 年合同法》获得强制执行。前提是不存在导致合同无效或可撤销的因素。

3）AI领域主要监管机构及其职责

①科技创新部（Ministry of Science, Technology and Innovation，MOSTI）

网址：https://www.mosti.gov.my

联系方式：+603 8000 8000

②通讯部（Ministry of Communications）

网址： https://www.kkd.gov.my

联系方式：+603 8872 1610

③通讯及多媒体委员会（Malaysian Communications And Multimedia Commission，MCMC）

网址：https://www.mcmc.gov.my

联系方式：+603 8688 8000

④数字经济机构（Malaysia Digital Economy Corporation，MDEC）

网址：https://mdec.my

联系方式：+603 8315 3000

二）马来西亚生成式人工智能合规核心问题

1. 基础模型和AI产品关系及定性

截至目前，马来西亚还没有专门针对人工智能治理的立法，以区分基础模型和AI产品进行区别监管。在现阶段，在AI产品合规性方面，建议遵循大模型合规的一般原则，包括透明度、可解释性、数据质量等问题，同时，注意遵守马来西亚的数据管理相关规定。

2. 大模型预训练使用公开数据合规

马来西亚还没有专门针对人工智能治理的立法，未对算法预训练数据做出单独的规定。但马来西亚针对个人信息制定了《个人数据保护法》，《个人数据保护法》适用于任何处理或控制处理马来西亚个人数据的人。因此，在马来西亚使用个人信息进行AI算法训练时，必须确保遵守《个人数据保护法》及其附属法规的要求，确保数据处理的合法性、正当性和透明度。

此外，使用个人信息进行算法训练的企业还需注意数据保护的各个方面，包括数据安全、数据主体权利，以及合规性审查等。具体要求包括但不限于必须获得数据主体的有效同意才能将个人信息用于算法训练，同意必须是自愿的、明确的并且可以通过书面形式记录下来。数据主体应被告知其个人信息将如何被使用，并有权随时撤回同意。企业需要定期审查AI算法中的数据处理流程以确保持续符合《个人数据保护法》的要求。

同时，除了使用个人信息投入AI模型预训练外，马来西亚当地也有不少

公开的开源数据集，可供企业投入算法训练的使用，如Magic Data的马来语对话音频数据集，Magic Data在开源社区上传了马来语对话音频数据集，采集了近700位马来西亚人的自由对话。这个数据集包含5个小时的马来语对话音频，可用于训练对话式AI系统。如果企业在训练大模型时使用了公开的开源数据集，需参照新加坡的合规意见关注开源数据集的许可范围以及是否有特殊的要求。

3. 数据本地化和跨境数据

1）数据本地化要求

《个人数据保护法》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以外的地方，但下列情况除外：

部长根据个人数据保护专员建议指定的地区 。该地区有与《个人数据保护法》实质性相似或目的相同的法律，或者个人数据保护水平至少与马来西亚相当。由此可见，未来马来西亚的数据跨境传输条件可能会进一步放宽。但就目前而言，如果要实施数据跨境流动目前只能依据《个人数据保护法》第129条的豁免条款（建议通过在隐私政策中向用户披露个人数据出境的情况并取得用户同意，即通过数据主体同意获得豁免），即下列条款：

尽管有第一款的规定，下列情况仍可进行个人数据出境：
数据主体同意；
履行数据主体和数据使用者之间的合同所必需；
1.订立或履行数据使用者与第三方之间的合同所必需；（该合同是应数据主体要求而订立，或符合数据主体的利益）

为了法律程序或为了获得法律意见或为了确立、行使或捍卫合法权利；
2. 数据使用者有合理理由相信，跨境传输是为了避免或减轻对数据主体的不利行为，且获得数据主体书面同意是不切实际的，如果获得同意是可行的，则数据主体会给予同意；
3. 数据使用者已采取一切合理的预防措施并尽一切努力确保个人数据不会在其他地方以违反《个人数据保护法》的方式处理；
4. 为保护数据主体的切身利益所必需；
5. 为公共利益所必需。

2）数据跨境要求

A.原则上禁止数据出境，但有例外

根据《个人数据保护法》第 129(1) 条，禁止数据使用者将数据主体的个人数据转移到马来西亚以外的地方，除非根据个人数据保护专员的建议，在通信和多媒体部长（“部长”)的授权下在公报中指定并列出目的地国家/地区。

目前，尚未正式指定任何国家/地区。尽管禁止将个人数据转移出境，但《个人数据保护法》 规定了一些禁止的例外情况，例如，在获得数据主体同意的情况下进行此类转移以及转移是为了履行当事人之间的合同。当对数据传输的豁免是否适用有疑问时，谨慎的做法是就此类离开马来西亚的传输需要获得数据主体的同意。

对于外包服务而言，数据使用者不得与第三方分享资料，除非已取得个人同意。

在决定是否适合将数据传输到另一个国家时，部长必须考虑到该国的法

在决定是否适合将数据传输到另一个国家时，部长必须考虑到该国的法律是否与《个人数据保护法》是实质上相似或服务于相同的目的，以及第三国是否有足够的保护水平，或至少相当于《个人数据保护法》中规定的水平。

此外，根据《个人数据保护法》第 8 条，数据传输触发了披露原则，因此，要求数据使用者在进行跨境数据传输时通知数据主体。

B.例外规定

如前所述，《个人数据保护法》为允许数据传输到马来西亚境外提供了例外规定，根据法案第 129(3) 条，在以下情况下允许数据传输至境外：

1. 数据主体已同意转让；
2. 为履行数据主体与数据使用者之间的合同而进行的传输是必要的；
3. 数据使用者与第三方之间应数据主体要求或符合数据主体利益的合同的订立或履行所必需的传输；
4. 传输是为了任何法律程序的目的或为了获得法律建议或建立、行使或捍卫合法权利；
5. 数据使用者有合理理由相信，在所有情况下：
   - 数据的传输都是为了避免或减轻对数据主体不利的行动；
   - 获得数据主体的书面同意是不切实际的；
   - 如果获得此类同意是切实可行的，则数据主体会表示同意；
6. 数据使用者已采取一切合理的预防措施并尽一切努力确保个人信息不会以任何方式（如果该地方是马来西亚）处理，以免违反本法的规定；
7. 传输是为了保护数据主体的切身利益所必需的；
8. 在部长确定的情况下，为了公共利益，传输是必要的。

4. 开发者安全责任

马来西亚还没有专门针对人工智能治理的立法，目前马来西亚的主要数据保护法律为2010年《个人数据保护法》。根据《个人数据保护法》，开发者作为数据控制者时应当采取切实措施以保护个人数据免遭任何丢失、误用、修改、未经授权或意外访问或披露、更改或破坏。

而马来西亚科技创新部发布《2021-2025年国家人工智能路线图》，阐明国家促进AI发展的六项战略以及负责任AI的七项原则。

5. 内容安全

1）相关法律法规及监管

马来西亚政府高度重视生成式人工智能产品的内容安全问题，并通过一系列法律法规来确保内容的安全性和合规性。目前，虽然马来西亚尚未出台专门针对人工智能治理的立法，但已有的数据保护法律和其他相关政策为人工智能的内容安全提供了基础框架。

《2021-2025年国家人工智能路线图》明确了负责任AI的七项原则，其中包括透明性、公平性、可靠性和控制、隐私和安全等，这些都是内容安全的重要组成部分。路线图强调了人工智能系统必须遵守数据收集、使用和存储的隐私法律，以确保个人数据得到妥善保护。这有助于确保生成式人工智能产品在内容生成过程中遵守隐私保护的要求。科技创新部（MOSTI）正在制定的人工智能法案预计将解决与人工智能相关的透明度和问责制等问题，进一步加强对内容安全的监管。

2018年通过的《反假新闻法令》规定，制造、发布或传播虚假新闻是违法行为。生成式人工智能产品在内容生成和传播过程中，应避免制造和传播虚假信息，以免触犯该法。

马来西亚政府在制定相关法律法规时，强调了透明度和责任制，要求生成式人工智能产品开发者和运营者必须公开其系统的运作和数据处理机制，并对其生成的内容负责。包括：

2）告知义务

人工智能系统在与用户互动时，必须明确告知用户他们正在与人工智能系统互动，确保用户知情权。

当使用人工智能系统生成或修改图像、声音或视频时，可能导致误认为是真实或原物的，开发者有义务向公众披露这些内容是人工合成或被修改过的。

3）内容责任

生成式人工智能产品开发者需对其生成和传播的内容负责，确保内容不包含虚假信息、不侵犯他人隐私、不具煽动性或威胁性。

在出现内容安全问题时，开发者应立即采取措施，包括暂停服务、召回相关产品，并通知相关监管机构。

6. 生成物知识产权可版权性

马来西亚对于AI生成物可版权性暂无定论。

法规可参考前面“ 马来西亚现行的人工智能相关法律法规-知识产权法 ”部分。

另外，暂未检索到马来西亚关于AI生成物可版权性相关的案例及新闻。

7. 大模型透明度

马来西亚对大模型透明度暂未出台更详细的政策与法规，在《2021-2025年国家人工智能路线图》中提到了透明度作为人工智能基本原则：

1）透明性至关重要，因为缺乏透明性往往会导致怀疑和不信任。马来西亚公众非常重视组织在处理个人数据时的透明性。与全球平均水平相比，马来西亚人更愿意让组织（无论是私人机构还是政府）使用他们的数据，但允许使用的主要条件之一是他们希望了解其中的风险。设计和部署人工智能系统的人必须对其系统的操作负责。为了建立规范和最佳实践，我们可以借鉴其他行业的经验，例如医疗保健。内部审查委员会可以提供监督和指导，确定在人工智能系统开发和部署过程中应采用哪些实践。

2）负责任的人工智能原则（公平性、可靠性和控制、隐私和安全、包容性、透明性、责任和追求人的利益与幸福）需要融入中学的科学、技术、工程、艺术和数学课程。

但马来西亚目前尚未出台针对透明度更详细的法规或要求。

8. 用户权利保护

1）用户数据权利：

根据2010年《个人数据保护法》，人工智能处理的个人数据必须遵守七项个人数据保护原则。这包括获得数据处理的同意、确保数据安全以及允许个人访问和更正其数据。

2）透明度、问责制：

科技创新部已启动《2021-2025年国家人工智能路线图》，并正在制定一项全面的人工智能法案。该法案目的包括解决与人工智能相关的透明度、问责制问题。

第五章、印度尼西亚

一）印度尼西亚生成式人工智能产业及监管

1. 生成式人工智能在印度尼西亚的发展现状和地位
2. 印度尼西亚生成式人工智能监管框架

二）印度尼西亚生成式人工智能合规核心问题

1. 基础模型和AI产品关系及定性
2. 大模型预训练使用公开数据合规
3. 数据本地化和跨境数据
4. 开发者安全责任
5. 内容安全
6. 生成物知识产权可版性
7. 大模型透明度
8. 用户权利保护

一）印度尼西亚生成式人工智能产业及监管

1. 生成式人工智能在印度尼西亚的发展现状和地位

1）生成式AI产业政策

① 印尼政府与学术界和私营部门合作伙伴起草了一份白皮书，题为“印尼 2020-2045 年人工智能国家战略”（Strategi Nasional Kecerdasan Artifisial Indonesia 2020-2045）。白皮书主要关注那些优先开发和利用人工智能的领域，其中包括健康服务，管理改革，教育和研究，粮食安全以及移动性和智慧城市。

- 健康服务

印尼政府打算实施“ 4P ”医疗服务方法，即预测性、预防性、个性化和参与性。4P 方法旨在预测疾病的体征和症状，以确定一个人需要做出哪些生活方式的改变来改善他们的整体健康状况。人工智能将用于处理从个人医疗记录收集的大数据并将其与各种医疗服务提供商共享。然后，医疗服务提供商将执行 4P 方法的预期结果，分析并确定个人应接受的最合适的医疗治疗。

- 官僚信息

人工智能旨在使政府机构开展的某些重复性活动实现自动化。印度尼西亚政府目前正在开发一款聊天机器人软件，旨在向公民提供有关政府服务的基本信息。还有一项计划，即通过自动化机器人处理行政文件和表格，以减少人工参与执行手动和重复性行政任务。另一项突破性计划涉及开发一种人工智能系统，通过审查和识别预算提案中的不一致之处，支持政府监督政府预算。

- 教育和研究

人工智能将用于开发自适应评估和智能学生分类系统，该系统评估每个学生的学业水平和偏好，为他们提供更加个性化的学习环境，希望能够让印尼教育系统摆脱目前实施的千篇一律的做法。从研究的角度来看，印尼政府打算专注于培训和提高人工智能系统的能力，为它们提供印尼多样化的文化产品，例如地方语言、书写系统和表演艺术。

- 食品安全

人工智能的设想是帮助政府机构确定最需要援助的地区，具体方法包括增加特定地区的农业用地数量，以及确定可以传授的新技能，以提高有需要的社区的福利。人工智能的其他用途包括协助确定向贫困地区或经济受到流行病、流行病和自然灾害不利影响的其他地区分发援助的适当渠道。

- 交通和智慧城市

印度尼西亚政府利用人工智能的一个值得注意的计划是通过处理通过闭路电视和其他数据传感器收集的数据来提供智能交通管理解决方案，以便向道路使用者提供实时交通信息，通过优化交通信号灯配置来改善交通拥堵并评估道路使用情况。印度尼西亚政府设想的另一个有趣的人工智能用途是管理灾害风险，其中人工智能系统将接受训练以预测潜在的地震发生，通过观察降水和洪水模拟来预测洪水，并通过学习地震数据和其他相关地质信息来预测火山爆发。

② 2023年12月，印度尼西亚发布了两套关于人工智能使用的道德指南。首先是由通信和信息部（MOCI）于2023年12月19日发布的《关于人工智能道德指南的通知第9号》（以下简称“ MOCI AI 通知 ”）。其次是金融服务局（OJK）于2023年12月4日在其网站上发布的《关于金融

科技行业中负责任和可信赖的人工智能的道德指南》（以下简称“ OJK AI 指南 ”）。

- MOCI AI 通知

MOCI AI通知强调了AI对提高生产力、优化业务流程以及为各个行业的客户提供更个性化服务的优势。这些行业包括正在接纳AI进行社交媒体内容创作的创意产业，正在将AI融入以实现更准确医疗诊断的健康行业，以及正在整合AI以支持学习和研究活动的教育行业。

MOCI AI通知规定了一些责任，包括确保AI不作为决定人类政策和/或决策的唯一决定因素，防止种族主义的发生，避免任何可能伤害人的行为。

- OJK AI 指南

OJK AI指南适用于印度尼西亚的所有金融科技参与者。它们承认人工智能和机器学习可以提高业务流程的效率和金融服务交易的速度。然而，使用AI也带来了前所未有的风险。因此，这些指南旨在作为一种行为准则，指导金融科技参与者和相关方确保他们基于AI的应用遵守以下原则：

- 基于Pancasila，即载入印度尼西亚宪法的官方哲学基础，包含五个原则：(1) 相信唯一的上帝；(2) 公正和文明的人性；(3) 印度尼西亚的统一；(4) 由智慧引导的民主生活/代表；以及 (5) 实现印度尼西亚全体人民的社会公正，例如，AI的使用应符合国家利益，并根据Pancasila价值观履行道德责任；

- 有益，例如，基于AI的应用应为业务运营增加价值并提高消费者福

利；

- 公平且有责任，例如，不因消费者对使用黑箱AI技术或不适当数据集的认知不足而产生歧视；

- 透明且可解释，例如，应用“人在循环中”的方法，确保金融科技参与者具有控制基于AI的应用程序流程的知识和能力，并能向消费者解释它们；

- 稳固性和安全性，例如，确保在发生网络攻击的情况下有恢复机制。

2）生成式AI企业案例

活跃在印度尼西亚的生成式AI企业：

①Kata.ai

Kata.ai是一家总部位于印度尼西亚的AI虚拟个人助理服务提供商，专注于增强现实和自然语言处理技术的研发与应用。公司成立于2017年，致力于通过人工智能技术改变企业与客户互动的方式。Kata.ai采用B2B模式，通过其聊天机器人帮助企业提高客户交互度。

②Mekari

Mekari是一家总部位于印度尼西亚的B2B一体化解决方案供应商，专注于通过提供财务核算、人力资源和客户关系管理等服务，帮助企业实现自动化运营。Mekari的主要产品包括Talenta、Jurnal、Qontak、Klikpajak和Flex等SaaS产品，覆盖财务核算、人力资源、客户关系管

理、薪资管理和出勤管理等多个领域。

其他国家投资该国情况：

根据Statistia的数据，相较于2020年，印尼的生成式人工智能市场2023年增长10倍，居东南亚之首。

2024年4月，英伟达宣布将与印尼第二大移动电信公司 Indosat Ooredoo Hutchison 合作在中爪哇省梭罗市建设一座人工智能开发中心，总投资额 2 亿美元。该中心包括用于进行研究的Sembrani大楼和用于容纳技术开发和创新的Gumarang大楼。此外，两家公司在巴塞罗那签署的谅解备忘录，英伟达将通过 Indosat 及其子公司 Lintasarta 向印尼提供完整的 AI 平台，使 Lintasarta 成为 Nvidia 在该国的首个云端供应商合作伙伴。

2024年4月17日，苹果CEO库克在与印尼总统佐科·维多多会晤后表示，苹果将考虑在印尼生产的可能性。在库克与佐科会晤的前一天，苹果宣布了增加在印尼投资的计划，并表示将在巴厘岛开设该国第四所苹果开发者学院，该学院旨在为日益增长的iOS应用经济培养技术人才，重点是教授编码和设计，预计总投资将达1.2万亿印尼盾。

2024年4月30日，微软公司宣布将投资17亿美元在印尼建设云计算和人工智能基础设施，这是微软在印尼29年历史上的最大单笔投资。该投资计划将在四年内完成，包括在印尼全国范围内建设新的云计算数据中心和人工智能基础设施。此外，微软还计划在东南亚地区提供人工智能技能培训，预计将有250万人受益，其中印尼将有84万人接受培训。

2. 印度尼西亚生成式人工智能监管框架

1）印度尼西亚政府部门治理总框架

目前，印尼仍然缺乏针对公共和私营部门开发和使用人工智能的明确监管框架。印尼仍然依赖现有立法来解决与新兴人工智能模型的开发和使用相关的问题，例如：

- 2008 年第 11 号《电子信息和交易法》；
- 2014 年第 28 号《版权法》；
- 2022 年第 27 号《个人数据保护法》。

不过这些法规的范围非常笼统，并未直接解决印度尼西亚人工智能系统开发和使用中可能出现的人工智能相关问题。

2023 年 12 月 19 日，通信和信息部 (MCI) 承认印度尼西亚缺乏人工智能监管框架，并发布了关于MOCI AI 通知作为该国人工智能发展的现行指南。该通函初步概述了人工智能的一般定义，以及企业和电子系统提供商 (ESP) 开展的基于人工智能的咨询、分析和编程活动的价值观、道德和控制的一般准则。

目前，印度尼西亚正在积极制定一个全面的监管框架。印度尼西亚通信和信息部副部长 Nezar Patria 于近期宣布，印尼政府与由英国前首相牵头的一家非营利组织将建立变革性合作伙伴关系。该合作伙伴关系旨在制定一个全面的监管框架，专门用于管理蓬勃发展的生成人工智能技术领域。

2）AI领域主要监管机构及其职责

① 通信和信息部（Ministry of Communications and Informatics, Kominfo）

网址：https://www.kominfo.go.id/

联系方式：(021) 3452841

② 金融服务管理局（Financial Services Authority，Otoritas Jasa Keuangan或“OJK”）

网址：Otoritas Jasa Keuangan

联系方式：(021) 296 00000

二）印度尼西亚生成式人工智能合规核心问题

1. 基础模型和AI产品关系及定性

2024年4月23日，通信和信息部（Kominfo）宣布，目前正在制定有关人工智能（AI）技术治理的法规（条例）。Kominfo 概述了制定与人工智能技术相关的法规的两种方法：(1)横向——通过《信息和电子交易法》《个人数据保护法》和 Kominfo 部长关于人工智能伦理的通函；(2)垂直——通过金融和卫生等行业。

- 基础/通用大模型

MOCI 的 AI 通函规定，AI 的实施应遵守各种道德价值观，这些价值观与其他司法管辖区的道德价值观大致相似，尽管术语略有不同，主要包括安全、责任、透明度、可信度、个人信息保护。另外，目前的合规义务应当主要参照《信息和电子交易法》、《个人数据保护法》及AI通函。

同时应当注意，Pancasila是印度尼西亚的官方哲学基础，载入印度尼西亚宪法。Pancasila包括五项原则：（i）信仰唯一的神；（ii）公正文明的人类；（iii）印度尼西亚的团结；（iv）以智慧的审议/代表为指导的民主生活；（v）为印度尼西亚全体人民实现社会正义。虽然目前该原则仅在OJK AI指南中规定，但在大模型基础原则上仍可适用。

- 模型应用

印尼针对部分特殊行业制定了相应的AI模型使用规范。例如，在金融领域，印尼的金融服务管理局（OJK）要求AI模型必须符合《金融科技监管框架》的要求，以确保金融数据的安全和金融服务的稳定。因此，金融领域的AI产品应注意遵守OJK AI指南。目前医疗卫生领域尚未发布相关

规范，但基于其为重点关注行业，应持续关注合规要求，并可暂时先参照国际主要的通行要求进行。

2. 大模型预训练使用公开数据合规

在印度尼西亚使用公开信息进行AI算法训练时，若其中包含个人信息的情况下，需要确保遵守当地的数据保护法律，确保数据处理的有合法依据，如已经过数据主体的明确授权同意。此外，还需要注意数据保护的各个方面，包括数据安全、数据主体权利、以及合规性审查等。同样，如果企业使用开源数据集用于AI算法训练时，需要注意开源数据集的许可范围。

3. 数据本地化和跨境数据

2022 年 10 月 17 日，印度尼西亚颁布了一项规范个人数据保护的具体法律，即关于个人数据保护的 2022 年第 27 号法（“ PDPL ”）。

PDPL规范了个人数据主体的权利、个人数据控制者和个人数据处理者的义务以及处理个人数据的相关原则和要求。

PDPL的实施仍需遵守尚未颁布的实施细则。

除了 PDPL 之外，还有其他专门针对电子系统领域的个人数据保护规定，与数据隐私相关的条款散见于几项不同的立法中。例如：

(1) 2008年第11号《电子信息和交易法》（EIT法），该法规于2008年发布，并在2016年第19号法律中对其进行了修订，其在电子信息、记

录、签名、电子系统和电子认证的提供、电子交易、域名、知识产权、隐私保护权等方面提出了要求;

(2) 2016年第20号关于电子系统个人数据保护的条例（“Kominfo20号法规”）：印度尼西亚通信和信息部（Kominfo）于2016年12月发布该条例，作为EIT中个人数据保护要求的实施办法，其在个人数据的获取和收集、处理和分析、留存、披露、个人数据拥有者的权利、电子系统运营者的义务等方面提出了要求。

(3) 2019年第71号政府关于电子系统和交易实施的条例中(“GR71”)：该条例于2019年10月发布，取代了《2012年关于实施<电子系统和交易法>的第82号政府条例》，其在电子系统操作、电子代理商、电子交易操作、电子认证操作、可靠性认证机构、域名管理等方面提出了要求，电子信息法的程序指南也包含在其中。

a. 数据本地化要求

根据GR71，只有公共电子系统运营商才必须将其电子系统和数据放置在印度尼西亚本地。

除非另有规定，否则私人电子系统运营商可以将其电子系统和数据放置在印度尼西亚境内或境外。

b. 数据跨境要求

根据PDPL,在满足以下任一要求时，可以进行数据传输：

- 将接收个人数据的控制者和/或处理者的居住国提供等于或高于

PDPL 规定的数据保护级别；

- 如果不满足上述条件，控制者必须确保有充分且有约束力的个人数据保护；
- 如果不满足上述两个条件，控制者必须获得数据主体的同意。

4. 开发者安全责任

在《关于人工智能道德指南的通知第9号》（以下简称“ MOCI AI 通知 ”）指出在人工智能的实施背景下，伦理方面扮演着重要角色。在印度尼西亚，对发展和应用人工智能中的伦理重要性的意识日益增强。无论是私营还是公共领域的企业和电子系统运营商，作为人工智能实施的利益相关者，都应努力规范人工智能的伦理使用，包括对广泛社会影响的决策。人工智能伦理指南的开发旨在确保这一技术的使用考虑到伦理原则、谨慎、安全并以积极影响为导向。

5. 内容安全

1) 相关法律法规及监管

印度尼西亚政府高度重视生成式人工智能产品的内容安全问题，并通过一系列法律法规来确保内容的安全性和合规性。尽管印度尼西亚尚未出台专门针对人工智能治理的综合性立法，但现有的法律法规和相关政策为人工智能的内容安全提供了基础框架。

2008年的《信息与电子交易法》（UU ITE）及其后续修订案为印度尼西亚的互联网内容监管提供了法律依据。该法定义了一系列网络犯罪，包括散布色情内容、诽谤、网络欺诈、侵犯隐私等，并规定了相应的法律

责任。《电子系统与交易条例》进一步明确了电子系统和交易中的责任分配，并要求服务提供者采取必要措施来保护用户数据，确保内容的安全性。

印度尼西亚政府还发布了《人工智能伦理准则》，该准则强调了透明性、公平性、可靠性、隐私和安全等原则，这些原则也是内容安全的重要组成部分。该准则要求人工智能系统的设计、开发和应用应遵循高标准的道德和伦理规范，确保内容不会侵犯个人权利或引起社会不安。《网络与信息空间安全法》旨在保护印度尼西亚的网络空间安全，对于生成式人工智能产品而言，意味着需要采取措施来防范网络攻击，确保数据安全。

《关于人工智能道德指南的通知第9号》（MOCI AI通知）强调了AI对提高生产力、优化业务流程以及为各个行业的客户提供更个性化服务的优势，但同时也规定了一些责任，包括确保AI不作为决定人类政策和/或决策的唯一决定因素，防止种族主义的发生，避免任何可能伤害人的行为。

《关于金融科技行业中负责任和可信赖的人工智能的道德指南》（OJK AI指南）适用于印度尼西亚的所有金融科技参与者，旨在指导金融科技参与者和相关方确保他们基于AI的应用遵守一系列原则，如基于潘查希拉（Pancasila）价值观、有益、公平且有责任、透明且可解释、稳固性和安全性等。

6. 生成物知识产权可版权性

印尼对于AI生成物可版权性暂无定论。

印尼现行的2014年第28号著作权法令（Law Number 28 of 2014 on Copyright）中并未就AI生成物的可版权性进行单独论述。列明的19个“受保护的作品类型”中也未见可适用于AI生成物的作品类型。

另外，暂未检索到印度尼西亚关于AI生成物可版权性相关的案例及新闻。

7. 大模型透明度

印尼发布2023年第9号通函（Circular Letter No. 9 of 2023）作为政府确保人工智能发展符合道德价值观和安全的承诺。该通函强调，根据印度尼西亚标准行业分类 (KLBI) 62015 注册的商业实体有责任遵守既定的准则和道德规范。这包括在开发和实施人工智能方面的透明度、问责制和公平性等方面。鼓励商业行为者遵守责任原则，《通函》强调保护公众，防止AI成为唯一的决策者，并确保遵守法规义务。它要求在AI开发中保持透明，进行风险管理，并做好危机准备。

但印尼目前未出台针对大模型更详细的要求。

8. 用户权利保护

1） 消费者保护：

人工智能运营商必须根据适用法律法规确保消费者保护。2019 年第 71 号政府条例（关于实施电子系统和交易）（“ GR 71/2019 ”）规定了运营商在提供人工智能服务时应遵循的一般原则。

2) 人工智能的道德使用：

根据MOCI CL 9/2023 ，人工智能的实施不应导致歧视或对个人造成伤害。MOCI CL 9/2023 要求每项人工智能的实施都必须遵循以下道德规范：包容性；人性；安全；可访问性；透明度；信誉和责任；个人数据保护；可持续发展和环境；知识产权。

3) 问责制：

除非涉及用户疏忽，否则运营商应对其人工智能系统执行的操作负责，这确保用户在使用人工智能时出现问题时有补救措施。《企业所得税法》和第71/2019号政府令规定，因使用人工智能而产生的法律责任由人工智能运营者承担，但如果因用户的疏忽导致使用人工智能而产生损失，则该责任由用户承担。

第六章、菲律宾

一）菲律宾生成式人工智能产业及监管

1. 生成式人工智能在菲律宾的发展现状和地位
2. 菲律宾生成式人工智能监管框架

二）菲律宾生成式人工智能合规核心问题

1. 基础模型和AI产品关系及定性
2. 大模型预训练使用公开数据合规
3. 数据本地化和跨境数据
4. 开发者安全责任
5. 内容安全
6. 生成物知识产权可版性
7. 大模型透明度
8. 用户权利保护

一）菲律宾生成式人工智能产业及监管

1. 生成式人工智能在菲律宾的发展现状和地位

1）生成式AI产业政策

尽管菲律宾已经认识到人工智能的潜力及其在推动经济增长和创新方面的重要性，但该国仍处于人工智能采用的“早期阶段”，各行业的实施有限。政府、私营部门和学术机构正在努力推动人工智能的研究、开发和应用。

a. 教育部门方面，菲律宾大学制定了《菲律宾大学负责任和值得信赖的人工智能原则》，这是一套有助于确保人工智能在该国持续发展的指南。

b. 为了确保利用人工智能的优势，同时保护人民和国家免受潜在风险，菲律宾政府，特别是贸易工业部（DTI）推出了国家人工智能路线图，为人工智能的用户和生产者，同时还提供精确的指标来监控该技术的采用和使用方式。

2）生成式AI企业案例

活跃在菲律宾的生成式AI企业：

① Limitless Lab

Limitless Lab是一家社会创新和科技公司，成立于2018年，总部位于菲律宾。Limitless Lab致力于通过设计思维和技术来推动积极的社会变革，主要业务领域包括工具包设计、定制化工作坊、人工智能、数字化

平台开发和创新项目等。公司与多个国际组织和本地机构合作，推动公共服务设计和科技创新发展。

②ALFAFUSION

人工智能公司ALFAFUSION成立于1998年，总部位于菲律宾奎松市。ALFAFUSION 提供人工智能、电子商务开发和移动应用程序开发等产品服务，是菲律宾领先的AI聊天机器人解决方案提供商。

其他国家投资该国情况

菲律宾正日渐成为各国企业投资人工智能产业的目标地。

美国科技巨头 Supermicro宣布与菲律宾公司Converge ICT Solutions Inc合作，共同开启菲律宾人工智能 (AI) 的新时代。此次合作的重点是打造该国首个人工智能数据中心，同时推动尖端技术和环境可持续发展。

新加坡公司ADVANCE.AI与菲律宾金融科技公司FinScore签署战略合作协议，通过FinScore数字化解决方案提升 ADVANCE.AI风险管理、反欺诈解决方案的准确度与稳健性，共同帮助菲律宾及东南亚地区金融机构预防用户欺诈。

微软也宣布推出一项新计划，旨在加速在菲律宾的人工智能应用。微软希望通过这一计划，帮助菲律宾企业和机构更快地采用和利用人工智能技术，提升其在各个领域的运营效率和创新能力。

2. 菲律宾生成式人工智能监管框架

1）菲律宾政府部门治理总框架

菲律宾目前还没有人工智能的强制性标准或国家标准，也没有专门针对人工智能的法律法规。菲律宾正在寻求通过立法，成立“人工智能发展管理局”，负责制定国家AI战略和框架，指导企业在菲律宾开发和部署AI技术。几项众议院法案已经被提交，重点是确保人工智能在该国的创新和安全使用。其中之一是众议院第 7396 号法案，即《促进菲律宾人工智能发展和监管的法案》最近已提交众议院。该法案旨在创建人工智能发展局（AIDA），负责监督人工智能技术的开发和部署。关于人工智能的另一项拟议立法是众议院第10457号法案，题为《建立人工智能及相关技术发展国家战略的法案》，专门为建立国家人工智能研究中心(NCAIR)而编写。

2021年5月，菲律宾贸工部发布了该国AI发展路线图，其中包含AI涉及的四个主要方面，即：①数字化和基础设施；②研发；③劳动力发展；以及④监管。

2）AI领域主要监管机构及其职责

① 贸易和工业部（Department of Trade and Industry，DTI）
网址：https://www.dti.gov.ph
联系方式：0917 834 3330

②信息和通讯技术部（Department of Information and Communications Technology, DICT）

网址：https://dict.gov.ph
联系方式：8920 0101

③ 国家隐私委员会（National Privacy Commission，NPC）
网址：https://privacy.gov.ph
联系方式：+632 5322 1322

④ 科学技术部（Department of Science and Technology，DOST）
网址：https://www.dost.gov.ph
联系方式：+632 8837 2071

二）菲律宾生成式人工智能合规核心问题

1. 基础模型和AI产品关系及定性

截至目前，菲律宾还没有专门针对人工智能治理的立法，以区分基础模型和AI产品进行区别监管。在现阶段，在AI产品合规性方面，建议遵循大模型合规的一般原则，包括透明度、可解释性、数据质量、伦理道德等问题，同时注意遵守数据安全相关规定。

此外应注意，涉及AI合成深度伪造内容的情景，和其他地区一样，需要注意不应生成任何有害于未成年人、性虐待或性剥削的内容。

2. 大模型预训练使用公开数据合规

虽然目前菲律宾没有专门针对人工智能治理有专门的立法，但是关于菲律宾在使用公开数据进行生成式人工智能大模型预训练方面的合规问题，我们可以参考菲律宾《2012 年数据隐私法》(PDPA)（第 10173 号共和国法案）以及国际上的最佳实践，具体可以考虑以下几个方面：

数据来源合法性：AI模型预训练使用的数据必须有合法来源。这意味着数据收集过程中应遵循菲律宾当地法律法规，并且数据所有者的权益得到尊重。

知识产权保护：如果数据包含受版权保护的内容，例如书籍、文章或图像，那么在使用前需要获得适当的许可或许可协议。对于公开可用的数据集，也需要检查其许可协议，确保它们允许用于训练机器学习模型。

个人数据保护：如果预训练所使用数据集包含个人信息，必须确保按照相关隐私法规（菲律宾的《数据隐私法案》）的要求处理这些数据。必须获得个人同意，除非适用的法律允许在特定情况下无需同意即可处理数据。

3. 数据本地化和跨境数据

菲律宾的数据保护法律以2012年颁布的《数据隐私法》（第10173号共和国法）为基础，该法律一般规定了在菲律宾处理相关数据主体个人信息的要求。此后，国家隐私委员会（NPC）发布了《第10173号共和国法实施细则》，并定期发布通告以提供法律某些要求的指南。例如，NPC通告16-02、20-03、2021-01、2021-02、2021-03等，涵盖了数据共享协议、数据主体权利、公共卫生紧急情况下的个人数据处理等。

在AI行业和AI相关立法方面，数据隐私和数据保护尤为重要。随着AI技术的快速发展，AI系统需要处理大量的个人数据，这对数据隐私提出了更高的要求。菲律宾的《数据隐私法》及其相关规定为AI行业在处理个人数据时提供了法律框架，确保数据主体的隐私权利得到保护。

综上所述，菲律宾的数据保护法律为AI行业提供了明确的法律框架，确保在AI技术快速发展的同时，个人数据隐私得到有效保护。

1）数据本地化要求

菲律宾的《数据隐私法》没有规定个人数据的本地化或驻留要求。对于AI行业，这意味着企业可以将数据存储和处理在菲律宾境外。然而，企业仍需确保符合《数据隐私法》和国家隐私委员会（NPC）发布的相关

规定，特别是在数据传输和共享方面。AI系统在处理个人数据时，必须获得明确的用户同意并确保数据安全。虽然没有强制的数据本地化要求，但企业应采取适当的措施保护数据隐私，以符合菲律宾的数据保护法律框架。

2) 数据跨境要求

菲律宾《数据隐私法》要求每个实体对其控制或保管的个人信息负责，无论这些信息是国内还是国际转移，均需遵守跨境安排和合作规定。

数据跨境传输可以涉及数据共享或外包安排。“ 数据共享 ”是指将个人信息披露或转移给第三方，而这种行为必须按照相关实体的指示进行。“ 外包 ”则是指实体将个人数据披露或转移给个人信息处理者。

无论是数据共享还是外包安排，都必须符合《数据隐私法》的要求，包括签署适当的协议。国家隐私委员会也发布了关于数据共享协议的指南，规定了协议的内容。

在AI行业，数据跨境传输尤为常见。AI系统需要处理大量数据，可能涉及将数据传输到境外进行处理。虽然菲律宾没有强制的数据本地化要求，但企业在进行数据跨境传输时，必须确保符合《数据隐私法》的规定，获得用户的明确同意，并采取必要的安全措施，以保护数据隐私。

4. 开发者安全责任

AI监管在菲律宾并非一片空白。菲律宾现行的数据隐私和数据保护法在一定程度上对AI的使用作了规范。菲律宾《2012 年数据隐私法》(PDPA)（第 10173 号共和国法案）已于 2012 年 9 月 8 日生效，并且

与最终实施相关法规和规定（IRR）共同构成用于管控菲律宾数据隐私权的综合法律，它规定了数据控制方和数据处理方的义务。

5. 内容安全

相关法律法规及监管

菲律宾政府高度重视生成式人工智能产品的内容安全问题，并通过一系列法律法规来确保内容的安全性和合规性。目前，虽然菲律宾尚未出台专门针对人工智能治理的综合性立法，但已有的数据保护法律和其他相关政策为人工智能的内容安全提供了基础框架。

2012年颁布的《网络安全法》为菲律宾的网络安全和内容监管提供了法律依据。该法定义了一系列网络犯罪，包括散布色情内容、诽谤、网络欺诈等，并规定了相应的法律责任。对于生成式人工智能产品而言，这意味着产品在内容生成和传播过程中应避免触犯这些法律。《数据隐私法案》（DPA）的《实施细则和条例》（IRR）规定，未经数据主体同意，不能够仅依赖自动处理来做出任何对数据主体有法律效力的决定。对于自动化决策系统，如果它“ 完全依赖自动化处理后的数据做出对数据主体产生重大影响或将产生影响的决策 ”，那么数据主体便有权取得有关自动化决策程序的资料。

《人工智能伦理准则》强调了透明性、公平性、可靠性、隐私和安全等原则，这些原则也是内容安全的重要组成部分。该准则要求人工智能系统的设计、开发和应用应遵循高标准的道德和伦理规范，确保内容不会侵犯个人权利或引起社会不安。

2022年，菲律宾通过了第11390号共和国法案《反网络性虐待或性剥削儿童和反儿童性虐待或性剥削材料法案》。该法律认为，使用AI构建深伪（deepfake）色情视频是一种基于图像的性虐待，共享该等视频被视为对儿童实施网络性虐待或性剥削，相关行为将受到法律惩罚。这一法律体现了菲律宾对涉及人工智能生成内容的严格监管，特别是在保护儿童权益方面，明确禁止了利用AI生成有害于儿童的内容。

6. 生成物知识产权可版权性

菲律宾对于AI生成物可版权性暂无定论。

菲律宾现行的《菲律宾知识产权法典》（ Intellectual Property Code of the Philippines (Republic Act No. 8293)）中并未就AI生成物的可版权性进行单独论述。当前其他法律法规及法律性文件中未见对于AI生成物可版权性的论述。

另外，暂未检索到菲律宾关于AI生成物可版权性相关的案例及新闻。

7. 大模型透明度

菲律宾尚未颁布专门规范人工智能使用的法律，但众议院第 7396 号法案或拟议的“ 促进菲律宾人工智能发展和监管的法案 ”最近已提交众议院，寻求成立人工智能发展局（“ AIDA ”）。AIDA 应负责制定符合国家优先事项和国际标准的国家人工智能发展和监管战略，包括但不限于人工智能影响评估、数据保护和人工智能决策透明度的要求。

8. 用户权利保护

根据菲律宾2012年《数据隐私法》，数据主体拥有如下权利：

1）知情权

数据主体有权在处理其个人数据时被告知。

2）访问权

数据主体有权合理地访问与其个人数据处理有关的事项，例如，有权访问其个人数据的 PIC 或 PIP 的身份等。

3）更正权

数据主体有权在合理的时间内更正或对其个人数据的不准确或错误提出异议，并要求 PIC 予以更正。

4）删除权

数据主体有权从 PIC 归档系统中暂停、撤回或命令阻止、删除或销毁其个人数据。

5）反对/退出的权利

数据主体有权反对对其个人数据的处理，包括直接营销、自动化处理或分析的处理。

6）数据可携性权利

数据主体有权从 PIC 处获取其个人数据的副本，该副本以常用的电子或结构化格式提供，并允许数据主体进一步使用。

7）不受自动决策约束的权利

数据主体有权反对其个人数据的处理，包括自动处理。

8）其他权利

数据主体有权因个人数据不准确、不完整、过时、虚假、非法获取或未经授权使用而遭受的损害获得赔偿。此外，个人还有权向全国人大提出申诉。

AI人工智能产业链联盟

#每日为你摘取最重要的商业新闻#

更新 · 更快 · 更精彩

Zero

AI音乐创作人
水墨动漫联盟创始人
百脑共创联合创始人
人工智能产业链联盟创始人
中关村人才协会秘书长助理
河北北大企业家分会秘书长
墨玫星辰智能科技有限公司CEO
河北清华发展研究院智能机器人中心线上负责人
中关村人才协会数字体育与电子竞技专委会秘书长助理

主要业务:AI商业化答疑及课程应用场景探索，各类AI产品学习手册，答疑及课程

欢迎扫码交流

提供：学习手册/工具/资源链接/商业化案例/行业报告/行业最新资讯及动态

人工智能产业链联盟创始人

邀请你加入星球，一起学习

人工智能产业链联盟报告库

星主：人工智能产业链联盟创始人

每天仅需0.5元，即可拥有以下福利！
每周更新各类机构的最新研究成果。立志将人工智能产业链联盟打造成市面上最全的AI研究资料库，覆盖券商、产业公司、研究院所等...

知识星球

微信扫码加入星球

联系我们

垦丁新加坡

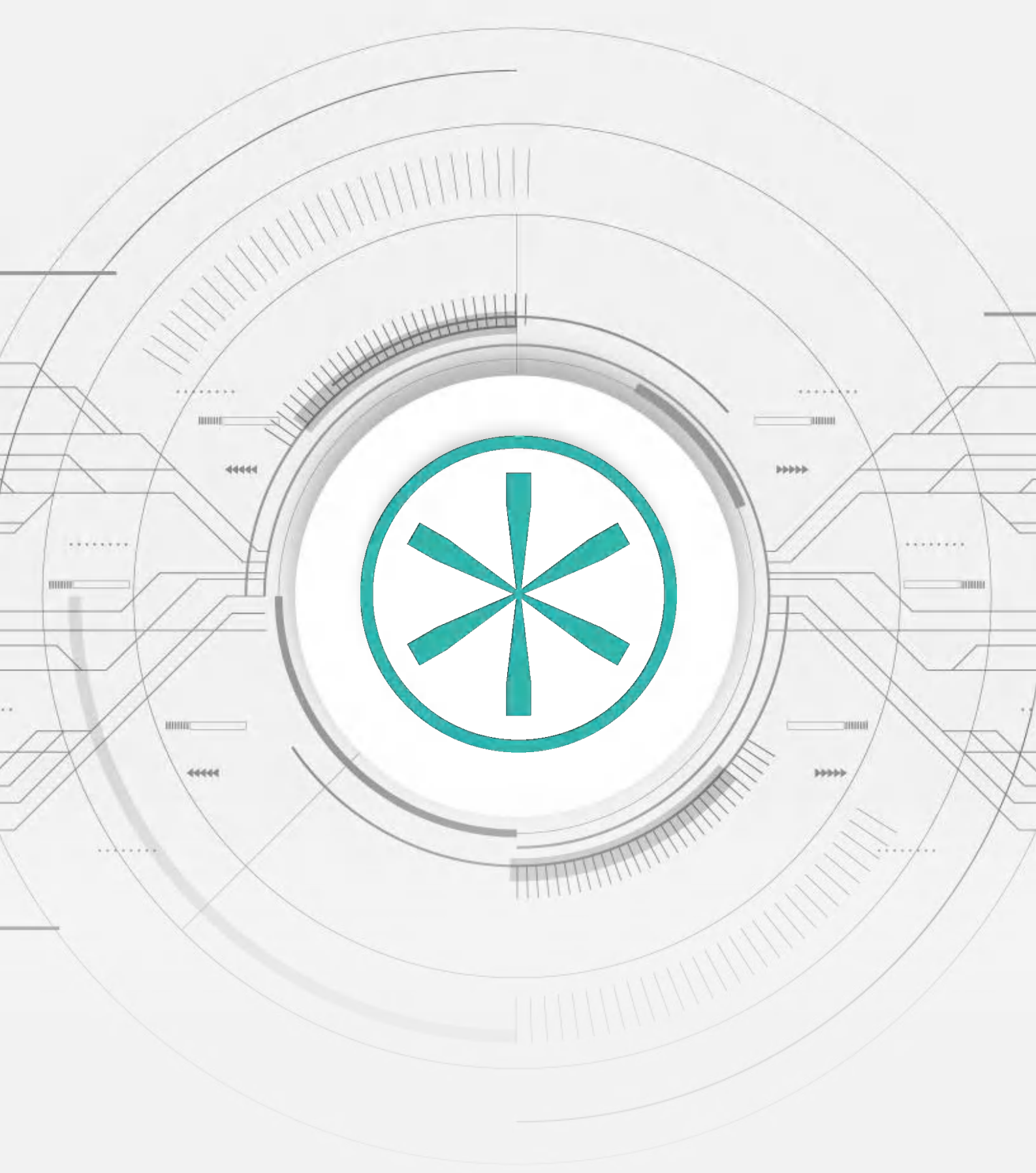
zs@kindinglaw.com； mc@kindinglaw.com；

WEEE Consulting

contact@weeeconsulting.com

Booter Hub

ljs@boosterhub.cn



垦丁律师事务所

垦丁（新加坡）、 WEEE Consulting、 Boosterhub

KINDING
垦丁律师事务所