个人数据保护与隐私亚洲指南

November 2023

MERITAS®

个人数据保护与隐私
亚洲指南

目录

Jeffrey Lim,
编辑
jeffrey@joylaw.com
Director,
Joyce A. Tan & Partners LLC

导言

世界各地的数据保护和隐私法律都在不断变化，而这还仅仅只是法律。

新的社会、技术或经济的发展每天都在影响着数据保护和隐私法律。

与时俱进至关重要。

在 Meritas® 上一次发布指南时，我们用一本书涵盖了亚太地区、欧洲以及美国的内容。现在，我们需要至少三本。

而这其中很大一部分都归功于亚洲。

自上一版本指南发布以来，中国、印度、印度尼西亚、斯里兰卡和泰国（共同拥有占全世界 40% 的人口）都分别通过了新的法律，更不必提还有其他国家的重大更新。

因此，尽管我们非常乐意与 Meritas® 在欧洲和美国的同行合作，但这一版本聚焦于亚洲这一各国都坚守其主权的复杂区域。

数字主权已然成为一个关键问题。如今，进行涉及跨境数据转移的商业活动已经变得非常微妙。

我们生活在一个非常有趣的时代。

为了找到应对这些复杂问题的方向，Meritas® 制作了本指南，通过汇集亚洲顶级律师事务所的意见，以问答形式概述了每个法域的情况，并附上了可在这一重要业务领域提供帮助的专业人士的联系方式。

鸣谢

特别鸣谢 Meritas® 的同事们，包括 Meritas 亚洲数据保护实践组的联合主席饶尧（中国）、Eliza Tan（Meritas® 亚洲区域代表）、Darcy Kishida（日本）以及所有撰稿者，本指南的完成离不开他们的辛勤工作及支持。

关于 Meritas

作为由各市场领先的独立律师事务所组成的国际网络，Meritas 的法律服务助力企业在世界各地把握机遇并应对难题。在与 Meritas 成员所的合作中，企业不仅能够获益于本地经验、集体支持，还能体验到更高效的合作模式。Meritas 在业内首创追求极致的服务质量并将客户优先置于一切之上的承诺，从而为企业带来个性化的关注和服务体验。

Meritas 于 1990 年创立，拥有覆盖全球 254 个法律市场的成员所，并拥有近 9,000 名专注业务、积极协作的律师。如需在特定领域或某个市场寻求 Meritas 支持，请访问 http://www.meritas.org 或致电+ 1 - 612 339 - 8680。

MERITAS®

中国

律所 **安杰世泽律师事务所**

www.anjielaw.com

联系人

杨洪泉
中国，北京
电话： + 86 10 8567 5988
邮箱： yanghongquan@anjielaw.com

安杰世泽是一家提供全方位服务的中国律师事务所，业务领域广泛。其 TMT 团队在技术、数据保护和网络安全领域处于领先地位。安杰世泽在该领域的业务包括个人信息和数据保护、网络安全、人工智能、媒体、电信和互联网服务。其客户不仅包括国内外众多知名电信运营商和互联网服务提供商，还包括银行、保险公司、汽车制造商和制药公司等电信和互联网服务用户。该团队在 Chambers、Legal 500、LEGALBAND 等专业法律研究公司的评级中名列前茅。

安杰世泽的 TMT 团队由前英国电信（BT）中国区总法务杨洪泉领导。他是中国数据保护法律领域的先锋，也是少数在数据保护和网络安全事务方面拥有超过 15 年经验的律师之一。Chambers 认可杨律师为“数据与隐私”以及“科技与电信”领域的第一梯队律师。

中国

律所 **汇衡律师事务所**

www.hhp.com.cn

联系人

饶尧
中国，上海
电话： + 86 21 5047 3330
邮箱： yao.rao@hhp.com.cn

汇衡是一家以向全球客户提供卓越的专业解决方案而闻名的领先律师事务所。秉承“质量优先”和“团队合作”的核心价值观，我们致力于为不同的客户实现最佳的商业和合规目标。汇衡拥有可就网络安全、数据合规和相关监管事宜提供全面咨询和专业建议的专业团队。我们的客户遍布各行各业，包括世界 500 强企业、跨国公司、大型国有和民营企业以及上市公司。

汇衡作为数据合规、公司事务、并购和争议解决领域领先的律师事务所，其声誉广受认可，长期受到 Chambers Global/Regional Guide、Legal 500、汤森路透 Asian Legal Business、Asialaw、IFLR 1000 和 Benchmark Litigation 等知名指南的推荐。

同时，作为全国信息安全标准化技术委员会（TC260）信息安全管理工作组（WG7）的正式成员，我们得以始终保持处于不断发展的法规和最佳实践的最前沿。

1. 中国主要的个人数据保护法律或法规有哪些？ 是否存在跨领域立法？ 跨领域立法与特定领域立法之间，何者将优先适用？

中华人民共和国（“**中国**”）主要通过一套围绕“个人信息”（“**个人信息**”）的规则来进行个人信息保护，包括跨领域立法和特定领域立法。

最为重要的跨领域立法是于 2021 年生效的《个人信息保护法》（“**个保法**”），该法对个人信息保护提出了全面的要求。此外，特定领域的规定则对一些领域提出了更具体的要求。举例而言，《汽车数据安全管理若干规定（试行）》即对汽车设计、生产、销售、使用和运营过程中的个人信息保护提出了详细要求。在中国，特定领域的立法通常是为进一步细化跨领域立法的规定而制定，如特定领域的法规提出了更详尽的要求，则以特定领域的法规为准。

2. 哪些监管机构负责个人信息保护法律的实施和执行？

在中国，《个保法》的实施由中国国家互联网信息办公室（“**网信办**”）牵头，但在特定领域也可能涉及该领域的主管监管部门，如工业和信息化部（IT、电信、工业等）、国家市场监督管理总局（消费者）、国家金融监督管理总局（银行、金融、保险等）、科学技术部（遗传）、公安部（犯罪）以及其它多个监管部门。

3. “个人信息”/“个人数据”是如何定义的，是否有任何类别的个人数据受到特殊或不同的保护（例如，员工、未成年人、“敏感”个人信息等）？ 如果是，这些类别是什么？ 能否简要说明适用于这些类别的特殊规则？

根据《个保法》的规定，个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。敏感个人信息是一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。

敏感个人信息受到更严格的保护,包括:

(i) 处理活动应当具有特定的目的和充分的必要性,并采取严格保护措施;

(ii) 要求特别告知并征得个人的单独同意;以及

(iii) 事先进行个人信息保护影响评估("**个保影响评估**")。

此外,针对特定领域的法规可能会在汽车数据、金融信息、医疗信息、遗传信息和其他受特殊监管的信息方面对个人信息提出更多专门要求。

4. 与个人数据相关的主要个人数据保护法律或法规的关键原则是什么?

根据《个保法》的规定,处理个人信息的基本原则包括:

- 合法;
- 正当;
- 必要;
- 诚信;
- 公开;及
- 透明。

《个保法》还提及或者可推知一些其他的原则。不过,这些原则可视为上述原则的衍生。《个保法》还明确规定,个人信息处理者不得通过任何误导、欺诈或胁迫的方式处理个人信息。

5. 是否有适用于所有企业的正式注册合规要求(例如数据保护官员的任命、数据库登记等)?

《个保法》并未设置适用于所有企业的普遍登记要求。在特定情况下,可能需要向主管部门进行备案或报告,或需要完成其他行政程序。例如:

- 个人信息保护负责人(“**个保负责人**”):如果处理的个人信息数量达到法定数量,则处理者应指定一名个保负责人,并向主管部门报告其联系方式。
- 外国处理者的本地代表:对于位于中国大陆以外,但为向中国大陆自然人提供产品或服务,或分析其行为的目的而处理其个人信息的处理者,应向主管部门报告其在中国境内负责处理个人信息保护事宜的指定代表(机构或个人)的联系方式。
- 向境外转移个人信息:请参阅第 7 问。

6. 各类组织有哪些建立与个人数据处理、使用和披露相关的合规计划(例如法律政策和运营政策、合同等)的义务?

在中国,各类组织有义务建立与其处理活动相关的合规程序。然而,此类义务是较为宽泛的,即个人信息处理者在如何履行此类义务方面有很大的自由裁量权。典型的合规程序所涉及的事项包括:收集和使用、告知和同意、委托处理、披露和转移、个人信息的保留和删除、个人信息主体权利、制定内部管理制度和操作流程、个人信息分类、访问控制、培训、技术和管理安全措施、影响评估、安全事件响应、与监管部门合作,以及更宽泛的遵守中国法律法规等内容。

7. 是否对将个人数据转移到其他法域存在限制? 各类组织通常如何应对这些限制?

在向中国大陆以外的接收方提供中国大陆境内个人的个人信息时,境内提供方应将跨境转移的情况详细告知个人。境内提供方还应征得个人的单独同意、事先进行个保影响评估并保留处理活动记录。

此外,根据境内提供方的具体情况以及所提供个人信息的性质和数量,向境外转移个人信息将适用不同的路径。

如果满足以下任一条件,则必须由网信办进行数据出境安全评估:

(i) 个人信息涉及重要数据(定义见《数据安全法》);

(ii) 提供方是关键信息基础设施运营者;

(iii) 提供方处理 100 万人以上个人的个人信息;或

(iv) 自上年 1 月 1 日起,提供方向境外提供了超过 10 万人的个人信息或超过 1 万人的敏感个人信息。

如果上述条件均不满足,则为了合法地向境外转移个人信息,提供方可以选择签署《个人信息出境标准合同》("**标准合同**")并向当地网信办备案标准合同(及个保影响评估报告),或者完成个人信息保护认证。据我们观察,除非必须进行安全评估,否则大多数境内提供方倾向于选择标准合同。

8. 是否存在对使用或重复使用个人数据进行数据分析/创新或采用人工智能或数据分析等新业务解决方案的限制? 各类组织通常如何应对这些限制?

当个人信息处理者将个人信息用于人工智能决策时,必须确保透明、公平和公正,还应进行影响评估,禁止在交易价格或其他条件方面进行不合理的差别待遇。对于商业营销或信息推送中使用的人工智能决策,必须为个人提供不针对其个人特征的选项,或者向个人提供便捷的拒绝方式。如果个人信息处理者通过自动化决策方式作出了对个人权益有重大影响的决定,个人有权要求个人信息处理者予以说明,并有权拒绝个人信息处理者仅通过自动化决策的方式作出决定。

中国有多部关于算法和人工智能的法规(例如《互联网信息服务算法推荐管理规定》),这些法规要求各类组织对特定人工智能技术进行备案或进行安全评估,对用于训练模型的数据进行筛选,确保人工智能输出的合法性,并要求在非常有限的时间内整改人工智能技术的问题。

因此,在将个人信息用于训练人工智能时,各类组织应重点聚焦如何确保在个人信息的整个生命周期中遵守隐私法律。除了应对人工智能训练在技术方面的挑战,通过定期进行数据分析算法审查、开展员工个人信息保护培训等措施来建立内部合规体系可能也非常重要。

9. 被收集个人数据的个人有哪些权利？ 他们能否撤回同意、反对保留（和/或要求删除）其个人数据？ 如果可以，应如何行使该权利？

《个保法》赋予个人信息主体以下权利：知情权、决定权、限制或拒绝他人处理的权利、撤回同意的权利、查阅和复制的权利、数据可携带权、更正或补充的权利、删除的权利以及要求就处理活动进行解释说明的权利。

如果处理是基于同意而进行的，那么个人信息主体可以撤回其同意。相应的，处理者必须为个人撤回同意提供便捷的方式，并在个人信息主体撤回同意时主动删除其个人信息。

在实践中，个人信息主体可以通过处理者提供的自动化工具或通过隐私政策或类似文件中公开披露的机制行使这些权利。

10. 如果违反任何个人信息保护法律，是否有任何处罚、责任或救济？

是的。如果处理者违反《个保法》或未履行任何个人信息保护义务，主管部门可责令改正、没收违法所得及给予警告。如拒不改正，可处以最高 100 万元人民币的罚款。对于情节严重的行为，主管部门可处以最高 5,000 万元人民币或上一年度营业额的 5% 的罚款，且可以责令停业整顿并吊销相关业务许可。

除行政处罚外，处理者还应承担损害个人信息主体权益的责任。

对于严重侵犯个人信息的行为，则可能会引发刑事责任。

11. 中国是否有强制性的数据泄露报告要求？ 如果有，请总结触发报告的阈值、报告内容、报告的对象以及需要/预期的时间表？

根据《个保法》的规定，如果发生或可能发生个人信息的泄露、篡改或丢失，处理者应立即采取补救措施，并通知主管部门以及个人信息主体。如果处理者采取的措施能有效防止由此造成的损害，则可免除

上述通知个人信息主体的义务，但主管部门仍可要求处理者履行该义务。

12. 中国近期在数据隐私/数据保护方面是否有显著的发展或可能会影响未来的案例？ 还有其他需要强调的方面吗？

在 2022 年和 2023 年，《个保法》第 38 条项下个人信息跨境转移的三条“法律路径”得到了落实，即安全评估、标准合同和个人信息保护认证，详见第 7 问。《数据出境安全评估办法》（2022 年）、《关于实施个人信息保护认证的公告》（2022 年）和《个人信息出境标准合同办法》（2023 年）共同构成了中国个人信息跨境转移的法律框架。

值得重点说明的是，中国监管部门近期在制定人工智能（“AI ”）规则方面有了重要的进展。具体而言，中国发布了关于 AI 开发者和服务提供商应如何确保输出公平、非歧视结果的官方指导意见，包括《互联网信息服务算法推荐管理规定》、《互联网信息服务深度合成管理规定》和《生成式人工智能服务管理暂行办法》。此外，中国政府正在采取专门措施推动 AI 技术的发展，如设立投资基金、为从事 AI 研发的企业提供税收减免等。随着 AI 技术日益融入企业、社会和人们的个人生活，在中国的 AI 服务提供商需要密切关注 AI 技术领域快速变化的法律环境。

中国香港

律所

何耀棣律师事务所

www.gallantho.com

联系人

黄永昌
中国香港，中环
电话： + 852 2825 2607
邮箱： philipwong@gallantho.com

我所创立于 1977 年，现有超过四十名律师，是香港一家声誉卓著并提供全方位法律服务的独立律师事务所。我所为客户提供涵盖公司、商业及房地产相关（诉讼及非诉讼）的全方位法律服务，其中包括资本市场、公司及商业、收购合并、银行及金融、中国业务、信托及私人客户、知识产权、物业发展及商业地产、租赁及楼宇买卖、遗嘱承办、保险、破产、调解、仲裁及诉讼等法律服务。

在向中国大陆进行投资及从中国大陆向境外投资方面，香港是外国和中国大陆投资者、企业最为青睐的普通法司法辖区，尤其是以香港公司载体作为募资及税务筹划的基地。

我所拥有四十余年的跨境工作经验，在为外国投资者和中国大陆企业搭建桥梁方面具有得天独厚的优势。

1. 中国香港主要个人数据保护法律或法规有哪些？ 是否有跨领域的立法，以及在跨领域立法与特定领域立法中，何者将优先适用?

在从收集到销毁的整个生命周期中，个人资料受到 1995 年制定的《香港法例》(Laws of Hong Kong)第 486 章《个人资料(私隐)条例》(Personal Data (Privacy) Ordinance)保护。该《条例》规定，资料使用者有义务遵守六项保障资料原则，并赋予资料当事人了解其个人资料的权利。

《条例》于 2012 年进行了修订，旨在加强对于公司资料使用者将客户个人资料应用于直接促销及与第三方共享的监管。2021 年，《条例》再次进行了一次重大修订，以打击侵犯个人资料私隐的起底(未经资料当事人同意披露其个人资料)的行为。专员亦有权就起底案件进行刑事调查、提出检控以及发出停止披露通知，要求移除起底内容。

《个人资料(私隐)条例》是中国香港现行主要的保障个人资料的立法，《条例》适用于所有领域，并优先于任何其他针对特定领域的立法。专员亦发布了若干实务守则，实务守则不具约束力，但如违反实务守则，在根据《条例》进行的法律程序中，将导致作出对资料使用者不利的推定。

2. 哪些监管机构负责个人信息保护法律的实施和执行?

个人资料私隐专员(Privacy Commissioner for Personal Data)是一个独立的法定机构，负责监督和执行有关立法的实施。公众如欲向专员查询或投诉，可前往专员公署(现地址为香港湾仔皇后大道东 248 号大新金融中心 13 楼 1303 室)，或发送电子邮件至 communications@pcpd.org.hk。更多详细信息，可访问专员公署网站 https://www.pcpd.org.hk。

3. “个人信息”/“个人数据”是如何定义的，是否有任何类别的个人数据受到特殊或不同的保护（例如，员工、未成年人、

“敏感”个人信息等)？ 如果是，这些类别是什么？ 能否简要说明适用于这些类别的特殊规则?

根据该《条例》,“资料”指“任何文件中资讯的任何陈述(包括意见表达),并包括个人身份标识符”。

“个人资料”是指“任何资料—

(a) 直接或间接与一名在世的个人有关的;

(b) 从该资料直接或间接地确定有关的个人的身份是切实可行的;及

(c) 该资料的存在形式使得资料的查阅及处理均是切实可行的。”

“个人身份标识符”是指“资料使用者为其作业而编配予一名个人的标识符;就该资料使用者而言,能识别该名个人的身份而不虞混淆,但用以识别该名个人的该人的姓名,则不包括在内”。

该等定义仅限于个人的个人资料,不包括识别法人实体(如公司和企业)的信息,但包括识别合伙中个人合伙人的信息。

《条例》并没有明文规定需对特定类别的个人资料予以更强的保护。但是,专员已通过发出实务守则的方式,就某些类别的个人资料设置具体规则,例如人力资源管理、监察活动及工作期间的个人资料私隐。专员还建议,可以采用网上警告的形式警示儿童需提供信息的最低限度,以及提醒年幼儿童在网上提供个人资料时需咨询家长或教师。

4. 与个人数据相关的主要个人数据保护法律或法规的关键原则是什么?

资料使用者必须遵守六项资料保护原则(Data Protection Principles)(“DPP”)。

DPP 1 – 个人资料必须以合法和公平的方式收集,用于与资料使用者的职能或活动直接相关的合法目的。资料当事人必须被告知收集资料的目的和资料可能转移予何种类别的人,以及资料当事人是否有

义务提供资料，以及如果有义务提供资料其拒绝提供的后果。收集的资料应是必要的，不应过度收集。

DPP 2 – 个人资料必须准确，保存时间不得超过实现收集和使用目的所必要的时间。

DPP 3 – 个人资料必须用于指定的目的或与之直接相关的目的，除非获得资料当事人自愿和明确同意的新目的。

DPP 4 – 必须采取措施防止未经授权的或非法的查阅、处理、删除、丧失或使用个人资料。

DPP 5 – 必须采取措施使得公众通过个人资料政策及实务知悉资料使用者所持有的个人资料类型及其如何使用该等资料。

DPP 6 – 必须允许资料当事人查阅其个人资料并允许其进行更正。

5. 是否有适用于所有企业的正式注册合规要求（例如数据保护官员的任命、数据库登记等）？

目前没有对有关收集或使用个人资料的数据库进行登记的法定要求。也没有任命数据保护官的法定要求，亦没有对不任命数据保护官进行处罚的规定。

6. 各类组织有哪些建立与个人数据处理、使用和披露相关的合规计划（例如法律政策和运营政策、合同等）的义务?

没有各类组织须制订合规程序的法定要求。但是，专员鼓励各类组织制定自己的隐私管理程序，并任命一名数据保护官监督组织遵守《条例》的情况。

7. 是否对将个人数据转移到其他法域存在限制？ 各类组织通常如何应对这些限制?

虽然目前从中国香港向域外转移个人资料并无限制，但专员发布了《保障个人资料：跨境资料转移指引》及《跨境资料转移指引：建议合约条文范本》，并提供两套推荐的合约条文范本，以配合跨境资料转

移的两种不同情形，即(i)由一名资料使用者转移予另一名资料使用者；及(ii)由一名资料使用者转移予资料处理者，以协助跨境转移个人资料的各方考虑《条例》的有关规定。不过，各组织仍须遵守《条例》的一般规定，以确保个人资料向中国香港域外的转移必须是为了原本收集资料之目的或直接有关的目的。

8. 是否存在对使用或重复使用个人数据进行数据分析/创新或采用人工智能或数据分析等新业务解决方案的限制？ 各类组织通常如何应对这些限制？

各类组织仅可将个人资料用于收集资料时向资料当事人披露的目的或直接有关的目的，除非该等使用属于《条例》所规定的豁免情形，例如：(1) 该资料将用于制备统计数字，而不会用于任何其他目的；以及(2) 所得到的统计数字不会以辨识资料当事人的形式提供。任何将个人资料用于新目的的行为都必须征得资料当事人的同意。各组织应采取措施，确保资料的收集是用于与资料使用者的职能或活动直接相关的合法目的、收集系必要或与该目的直接相关、资料未被过度收集并采取切实可行的措施，确保在收集资料之时或之前已通知资料当事人资料的使用目的，以及资料的保存时间不应超过必要的时间。

9. 被收集个人数据的个人有哪些权利？ 他们能否撤回同意、反对保留（和/或要求删除）其个人数据？ 如果可以，应如何行使该权利？

个人有权：

(i) 提出查阅资料的要求，并了解该要求被拒绝的理由；

(ii) 要求更正不正确的资料，并了解该要求被拒绝的理由；

(iii) 要求删除不正确的资料；

(iv) 要求不将其个人资料用于直接促销；

(v) 向专员投诉违反法律的行为；

(vi) 如个人因资料使用者未遵守法律而遭受损害,其可通过民事诉讼要求补偿,并可要求专员在诉讼中提供协助;及

(vii) 通过通知资料使用者(即收集其资料的人)的方式,撤回对第三方保留其个人资料的同意。

10. 如果违反任何个人信息保护法律,是否有任何处罚、责任或救济?

专员可发出执行通知,指令违反资料保护原则的人采取措施补救及防止再次发生违规行为。而违反执行通知,或故意作出与执行通知指明的作为或不作为相同的行为,则可能会被处以罚款和监禁。未经个人同意,披露从个人处获得的任何个人资料,意图获取金钱或其他财产得益,或使其遭受损失,均属刑事犯罪。对个人造成心理伤害的此类披露行为也属于刑事犯罪。违反前述法律的人还可能面临民事索赔。

专员可对起底案件进行刑事调查、提出检控、并要求停止披露涉及起底的内容。

11. 中国香港是否有强制性的数据泄露报告要求? 如果有,请总结触发报告的阈值、报告内容、报告的对象以及需要/预期的时间表?

目前没有关于报告数据泄露的法定要求。但是,专员发布了不具约束力的指引,鼓励资料使用者通知受影响的资料当事人、专员、相关执法机关及监管机构,以及可采取补救措施的其他各方,以保障受影响的资料当事人的个人资料私隐及权益。换言之,根据《条例》,资料使用者可能会因未能对个人资料采取适当的安全措施而承担法律责任。

12. 中国香港近期在数据隐私/数据保护方面是否有显著的发展或可能会影响未来的案例? 还有其他需要强调的方面吗?

2023 年 2 月 20 日,专员在向立法会汇报时,宣布将对《条例》作出实

质修订,包括:

(i) 设立强制性的资料外泄报告机制;

(ii) 引入对资料处理者的直接监管;

(iii) 要求制订资料保留政策;及

(iv) 赋予专员施加行政罚款的权力。

上述拟进行的修订将为《条例》带来重大改革,并将加强香港对个人资料私隐的保障。

总结

资料使用者应熟知《个人资料(私隐)条例》、六项资料保护原则、实务守则、指南及指引。实务守则不具约束力,但如违反实务守则,在根据《条例》进行的法律程序中,将导致作出对资料使用者不利的推定。专员通过指南和指引的形式说明了拟在法律框架下履行其职能或行使其权力的方式。它们代表了专员认为的最佳实践,但违反它们并不必然导致法律责任。

印度

律所

Khaitan & Co LLP

www.khaitanco.com

联系人

Harsh Walia
印度，孟买
电话： + 91 11 4151 5454
邮箱： walia@khaitanco.com

Khaitan & Co 成立于 1911 年，是印度历史最悠久、最负盛名的提供全方位服务的律师事务所之一。本所拥有 1 000 多名专业人员和 230 多名合伙人、顾问和管理人，也是规模最大的律师事务所之一。本所的团队由印度法律界经验丰富的资深律师和充满活力的后起之秀组成，能够提供最适合客户具体要求的定制化务实解决方案。本所是领先企业、跨国公司、金融机构、政府和国际律师事务所值得信赖的顾问。从并购到知识产权，从银行到税务，从资本市场到争议解决，以及白领犯罪、数据隐私和竞争法等新兴领域，本所在各个业务领域都拥有强大的专业能力和深厚的行业知识。本所在新德里、诺伊达、孟买、班加罗尔、钦奈和加尔各答设有办事处，并通过专注于各国市场的部门以及与各司法辖区顶级国际律师事务所的稳固合作关系，在海外市场同样拥有服务能力。2021 年，本所在新加坡开设了第一家国际办公室。

1. 印度的主要个人数据保护法律或法规有哪些？ 是否有跨领域的立法，以及在跨领域立法与特定领域立法中，何者将优先适用？

目前，印度还没有全面的数据保护立法。关于数据保护的条款包含在 2000 年《信息技术法案》(Information Technology Act 2000)("**IT Act**")以及根据该法案制定的规则("**SPDI Rules**")，以及与 IT Act 并存且互为补充的特定领域立法中。

一般来说，特定领域立法优先于更广泛的一般法。然而，特定领域立法可能是有限的。因此，IT Act 填补了空缺，确保了全面的数据保护。

在 2023 年 8 月 11 日，2023 年《数字个人数据保护法案》(Digital Personal Data Protection Act, 2023)("**DPDP Act**")颁布。该法案一旦正式生效，将取代 IT Act 和 SPDI Rules 建立的框架，并在与其他数据保护立法发生冲突时优先适用。

2. 哪些监管机构负责个人信息保护法律的实施和执行？

尽管目前还没有此类总体监管机构，但 DPDP Act 拟为此目的成立一个数据保护委员会(Data Protection Board)。

3. "个人信息"/"个人数据"是如何定义的，是否有任何类别的个人数据受到特殊或不同的保护（例如，员工、未成年人、"敏感"个人信息等）？ 如果是，这些类别是什么？ 能否简要说明适用于这些类别的特殊规则？

根据 SPDI Rules，"个人信息"("**个人信息**")是指与自然人相关，能够通过直接或间接地与法人团体可获得或可能获得的其他信息相结合识别个人的身份的信息。

SPDI Rules 主要为"敏感个人数据或信息"("**敏感个人信息**")提供保护，敏感个人信息指与下列事项有关的个人信息：

(i) 密码；

(ii) 财务信息，例如银行账户、信用卡、借记卡或其他支付工具的详细信息；

(iii) 身体、生理和精神健康状况;

(iv) 性取向;

(v) 医疗记录和病史;

(vi) 生物识别信息等。

敏感个人信息不包括在公共领域公开可得或可访问的信息,也不包括根据 2005 年《信息权法案》(Right to Information Act, 2005)或任何其他法律提供的信息。

一旦生效,DPDP Act 将为所有数字形式的"个人数据"提供保护,但个人为个人或家庭目的处理的个人数据以及已公开或导致被公开的个人数据除外。

4. 与个人数据相关的主要个人数据保护法律或法规的关键原则是什么?

虽然 IT Act 和 SPDI Rules 并未明确规定数据保护的主要原则,但可以注意以下几点:

(a) 同意是收集个人信息的唯一合法依据:书面同意(包括通过电子方式)是收集敏感个人信息的唯一依据。

(b) 透明:收集敏感个人信息的实体必须确保敏感个人信息的提供者知悉:(i) 信息被收集;(ii) 收集的目的;(iii) 信息的预期接收者;(iv) 收集信息的机构的名称和地址,以及该机构将保留这些信息。

(c) 目的限制:除非出于与该实体职能相关的合法目的,否则不得收集敏感个人信息。

(d) 数据最小化:除非收集敏感个人信息是目的所必要的,否则不得收集。

(e) 储存限制:除非其他法律另有规定,持有敏感个人信息的实体保留敏感个人信息的时间不应超过合法使用该等信息的目的所必需的时间。

DPDP Act 还以其他原则为基础，例如以合法方式使用个人数据、仅将数据用于收集目的、个人数据的准确性、实施合理的保障措施以及数据受托人的责任。

5. 是否有适用于所有企业的正式注册合规要求（例如数据保护官员的任命、数据库登记等）？

目前没有明确的登记合规要求。不过，收集或处理敏感个人信息的实体负有的一般义务包括：指定一名申诉专员并公布其联系信息、实施合理的安全措施和程序（“**安全程序**”）以及进行定期审计。DPDP Act 还拟定了“重要数据受托人”（尚未分类）的数据保护官和独立审计师。

6. 各类组织有哪些建立与个人数据处理、使用和披露相关的合规计划（例如法律政策和运营政策、合同等）的义务？

收集和处理敏感个人信息的实体必须向数据主体提供隐私政策，并确保其“*可供查看*”。SPDI Rules 规定，隐私政策应在该实体的网站上发布，且需告知信息提供者：

（a）有关收集的个人信息和敏感个人信息类型的信息；

（b）该实体的措施与政策；

（c）任何向第三方的披露；以及

（d）该实体采取的安全程序。

对于安全程序，SPDI Rules 认可 IS/ISO/IEC 27001 国际标准“信息技术—安全技术—信息安全管理体系— 要求”的实施。SPDI Rules 要求实体必须制定并实施全面的、记录在案的信息安全程序和政策，其中需包含与受保护信息资产相适应的管理、技术、经营和物理安全控制措施。该等措施应由独立审计员每年至少审计一次，或需在实体对其流程和基础设施进行重大升级时进行审计。

相较之下，DPDP Act 根据各类组织所承担的角色规定了更强有力的义务。然而，仍有许多方面尚未明确，预计政府将发布进一步的规则/通知。

7. 是否对将个人数据转移到其他法域存在限制？ 各类组织通常如何应对这些限制？

根据 SPDI Rules，在下列情形中，可披露和转移（包括跨境转移）敏感个人信息：

（a）敏感个人信息是根据合法的合同而收集，且敏感个人信息的提供者已允许向任何第三方披露；或

（b）披露为遵守法律义务所必需。

接收敏感个人信息的第三方不得进一步披露该等信息。

此外，在以下情况下允许转移（包括跨境转移）敏感个人信息：

（a）为履行该实体与敏感个人信息提供者之间的合法合同所必需，或敏感个人信息提供者已同意进行此类转移；以及

（b）转移方实体/接收方实体确保提供与 SPDI Rules 规定相同水平的数据保护。

为免疑义，尽管 IT Act 中没有普遍的限制，但某些部门法可能有数据本地化的要求。

实践中，各组织应确保共享敏感个人信息前事先获得用户的许可，并在披露/转移之前采取适当的保护措施。各组织还可通过签订合同的方式，确保接收被转移信息的任何实体/个人提供与 SPDI Rules 所规定的相同水平的数据保护。

目前，DPDP Act 允许在印度境外处理个人数据（除非政府以通知形式加以限制），但仍须遵守 DPDP Act 规定的一般义务。

8. 是否存在对使用或重复使用个人数据进行数据分析/创新或采用人工智能或数据分析等新业务解决方案的限制？ 各类组织通常如何应对这些限制？

对于为数据分析或其他类似目的重复使用个人数据没有具体限制。但是，SPDI Rules 规定，收集敏感个人信息必须出于与公司职能或活

动相关的合法目的，且收集必须是该目的所必要的。此外，收集敏感个人信息的实体需要将收集目的告知敏感个人信息的提供者。DPDP Act 也就个人数据的处理规定了类似的原则。

因此，各类组织如果有意重复使用个人数据，应告知信息提供者其可能使用数据的不同目的，并征得适当的同意。

9. 被收集个人数据的个人有哪些权利？ 他们能否撤回同意、反对保留（和/或要求删除）其个人数据？ 如果可以，应如何行使该权利？

SPDI Rules 规定了敏感个人信息提供者的权利。值得注意的是，任何收集/处理敏感个人信息的实体（或代表其收集/处理敏感个人信息的其他实体）都需要特别向信息提供者提供以下选项：

（a）不提供所要收集的信息；以及

（b）撤回先前给予的（书面形式）同意。

根据 SPDI Rules，信息提供者可以要求审查其所提供的信息，如有不准确或有缺陷的个人信息、敏感个人信息，应在可行的情况下予以更正或修改。

尽管 SPDI Rules 并未规定敏感个人信息提供者行使其权利的正式机制，但提供者通常可通过向该实体指定的申诉专员提交书面申诉来行使其权利。

SPDI Rules 没有明确规定删除权/被遗忘权，而印度各邦的高等法院对此采取了不同的意见。部分高等法院认可被遗忘权是个人隐私权的一部分，但也有部分高等法院（除有特定情形外）拒绝执行该权利。因此，删除权/被遗忘权的地位尚未得到确定。

另外，DPDP Act 为数据委托人规定了广泛的权利，包括访问个人数据相关信息的权利、更正和删除个人数据的权利、申诉补救权和提名权。如果个人数据处理系基于同意的，则数据委托人有权随时撤回其同意。

10. 如果违反任何个人信息保护法律，是否有任何处罚、责任或救济?

根据 IT Act，对于持有、交易或处理任何敏感个人信息的实体，如果在实施和维护安全程序方面存在疏忽，并因此对任何人造成不当损失或不当收益的，将承担向受影响者支付损害赔偿的责任。

此外，IT Act 规定，未经授权披露个人信息、意图造成或明知可能造成不当损失或不当收益的，将被处以监禁和罚款。

然而，前述规定的实际执行情况却不尽如人意。

作为对比，DPDP Act 根据违反/不遵守行为的性质规定了严格的处罚，并建立了更加全面的争议解决和执行机制。

11. 印度是否有强制性的数据泄露报告要求？ 如果有，请总结触发报告的阈值、报告内容、报告的对象以及需要/预期的时间表?

IT Act 和 SPDI Rules 并未规定数据泄露报告要求。

不过，印度计算机应急响应小组（Indian Computer Emergency Response Team）根据 IT Act 发布的指令中有此类要求。所有实体都被强制要求在发现此类事件或收到此类事件通知后的六小时内，按照规定的方式，向印度计算机应急响应小组报告特定类型的网络事件和网络安全事件。此外，在金融和保险等专门领域的法规中也存在泄漏报告要求，并规定了不同的泄漏报告时限和阈值。

此外，根据 DPDP Act，任何“个人数据泄露”都必须按照政府规定的方式通知数据保护委员会（Data Protection Board）和每个受影响的数据委托人。

12. 印度近期在数据隐私/数据保护方面是否有显著的发展或可能会影响未来的案例？ 还有其他需要强调的方面吗?

如上所述，DPDP Act 已经颁布但尚未生效。政府可能会规定在一段时间内逐步推行 DPDP Act 的条款。一旦 DPDP Act 生效，该法案将为印度数据保护提供全面的框架，并对个人数据的处理提出更严格的要求。

印度尼西亚

律所

Hutabarat Halim & Rekan（HHR Lawyers）

www.hhrlawyers.com

联系人

Milanti T. Kirana
印度尼西亚，雅加达
电话： + 6221 5091 3991
邮箱： milantikirana@hhrlawyers.com

HHR Lawyers 是印度尼西亚的顶级商事律师事务所，拥有卓越的专业声誉。自两位创始合伙人 Pheo M. Hutabarat 和 Nini N. Halim 于 1996 年创立律师事务所以来，HHR Lawyers 不断发展和展露其提供优质法律工作和客户服务的能力，这使得 HHR Lawyers 始终作为最具声誉和最为领先的印度尼西亚商业律师事务所之一，并同时具备全球影响力。HHR Lawyers 拥有超过 26 年的丰富经验，由众多经验丰富、在商业、公司、金融和商业纠纷等广泛领域拥有专业技能的印尼律师和外国法律顾问提供全面支持。

HHR Lawyers 为客户提供广泛的法律服务。HHR Lawyers 的专业知识和能力在各专业领域备受认可，包括：(i) 资本市场、银行和金融；(ii) 商业纠纷解决；(iii) 企业、投资和并购；(iv) 能源和自然资源；(v) 私有化和开发；(vi) 人力和劳资关系；(vii) 贸易和竞争；(viii) 技术和知识产权；(ix) 旅游和房地产；(x) 航空；以及 (xi) 航运。

1. 印度尼西亚的主要个人数据保护法律或法规有哪些？ 是否有跨领域的立法，以及在跨领域立法与特定领域立法中，何者将优先适用?

2022 年 10 月颁布的《印度尼西亚个人数据保护法(2022 年第 27 号)》(Indonesia Personal Data Protection Law No. 27 of 2022)("**PDP Law**"),以及通讯和信息部(Ministry of Communication and Information)《2016 年第 20 号法规》(Regulation No.20 of 2016)("**MOCI Reg No.20/2016**")是主要的个人数据保护法律和/或法规。PDP Law 涵盖电子系统和非电子系统中的保护,而 MOCI Reg No.20/2016 仅涵盖电子系统中的保护。PDP Law 作为适用于印度尼西亚各政府机构的基本法,具有跨领域的性质。但是,亦存在部分针对特定领域的要求,举例如下:(i) **银行和数字金融服务领域**:由金融服务管理局《2018 年第 12 号法规》(Financial Services Authority (*Otoritas Jasa Keuangan*) Regulation No.12 of 2018)监管;以及(ii) **健康领域**:受(i)《2009 年第 36 号健康相关法律》(Law No.36 of 2009 on Health);以及(ii)《2014 年第 46 号政府法规》(Government Regulation No.46 of 2014)("**政府法规**"简称为"**GR**")监管。印度尼西亚的 PDP Law 在各方面的实施仍有待进一步明确。因此,我们预计在不久的将来会进行数次调整。

2. 哪些监管机构负责个人信息保护法律的实施和执行?

目前,通讯和信息部("**通信部**")是个人数据("**个人数据**")保护的监管机构,有权管控印度尼西亚全国的网络活动、颁布法规并为从事信息技术行业的公司颁发许可证。

PDP Law 引入了一个新的监管机构,即"机构(institution)",其主要职责是落实个人数据保护。然而,迄今为止,有关该机构的法规尚未颁布。

3. "个人信息"/"个人数据"是如何定义的，是否有任何类别的个人数据受到特殊或不同的保护(例如，员工、未成年人、"敏感"个人信息等)？ 如果是，这些类别是什么？ 能否简要说明适用于这些类别的特殊规则?

一般而言,PDP Law 第 4 条规定了以下两种不同类别的个人数据:

a. **特定个人数据**：（i）健康数据和信息；（ii）生物识别数据；（iii）基因数据；（iv）犯罪记录；（v）儿童数据；（vi）个人财务数据；和/或（vii）法律法规规定的其他数据。

b. **一般个人数据**：（i）全名；（ii）性别；（iii）国籍；（iv）宗教信仰；（v）婚姻状况；和/或（vi）用于识别某人身份的组合性个人数据。

PDP Law 第 25 条和第 26 条还规定了特殊个人数据的处理，即：

a. **儿童个人数据处理**：应以特殊形式进行，并设置了根据法律法规征得父母和/或监护人同意的义务；以及

b. **残疾人数据处理**：应以符合法律法规的特定方法沟通的特殊形式进行，并设置了根据法律法规征得残疾人和/或监护人同意的义务。

法律法规尚未对儿童和残疾人个人数据相关“特别形式”的范围和执行进行解释。

4. 与个人数据相关的主要个人数据保护法律或法规的关键原则是什么？

PDP Law 规定了个人数据保护的原则，具体如下：

a. 在有限和特定的基础上，以合法和透明的方式收集个人数据；

b. 根据其目的处理个人数据；

c. 以保障个人数据主体权利的方式处理个人数据；

d. 应准确、完整、无误导、及时且负责地处理个人数据；

e. 以保障个人数据的安全，防止个人数据被非法访问、非法披露、非法篡改、滥用、毁坏和/或丢失的方式处理个人数据；

f. 处理个人数据的过程中，告知目的、处理活动及无法保护个人数据安全的情况；

g. 除非现行法律另有规定，在保存期限届满后或应个人数据主体的要求，应当对个人数据进行销毁和/或删除；

h. 以负责且可予明确证明的方式处理个人数据。

5. 是否有适用于所有企业的正式注册合规要求（例如数据保护官员的任命、数据库登记等）？

PDP Law 规定，只要不与 PDP Law 相抵触，所有与处理个人数据相关的现行规定仍然有效。基于此，《第 71/2019 号 GR》（GR No.71/2019）和通信部《第 5/2020 号法规》（MOCI Reg No.5/2020）设置了向主管部门登记的主要规定，其中《第 71/2019 号 GR》规定所有电子系统供应商（“**电子系统供应商**”）必须使用一站式线上提交（Online Single Submission）系统向通信部进行登记。

PDP Law 还要求任命一名“专员”以在特定情形下履行个人数据保护的职能，例如：

a. 为公共服务利益处理个人数据；

b. 个人数据控制者的核心活动的性质、范围和/或目的要求定期、系统的大规模监控个人数据；以及

c. 个人数据控制者的核心活动包含对特定个人数据和/或与刑事犯罪有关的个人数据进行大规模处理。

6. 各类组织有哪些建立与个人数据处理、使用和披露相关的合规计划（例如法律政策和运营政策、合同等）的义务？

MOCI Reg No.20/2016 规定，个人数据保护的原则之一是制定关于个人数据处理的内部制度。与此相关的是，PDP Law 第 35（a）条规定，个人数据控制者有义务通过准备和实施业务技术措施的方式，保护所处理的个人数据并确保其安全，使个人数据免于违反法律法规的个人数据处理。

7. 是否对将个人数据转移到其他法域存在限制？ 各类组织通常如何应对这些限制？

跨境数据流受到 PDP Law 第 56 条的规制，限制如下：

a. 在进行个人数据转移时，个人数据控制者应确保接收个人数据转移的个人数据控制者和/或个人数据处理者具备与 PDP Law 同等或更高的个人数据保护水平；

b. 如不满足(a)项的要求，则个人数据控制者应确保具备充分且有约束力的个人数据保护；

c. 如不满足(a)和(b)项的要求，则控制者有义务获得个人数据主体的同意。

为履行该等义务并确保遵守该等要求，相关的个人数据控制者可向通信部请求支持(MOCI Reg No.20/2016 第 23 条(2)(b)项)。

8. 是否存在对使用或重复使用个人数据进行数据分析/创新或采用人工智能或数据分析等新业务解决方案的限制？ 各类组织通常如何应对这些限制？

PDP Law 第 10 条规定，数据主体有权反对仅基于自动化处理(包括用户画像)且对数据主体产生法律后果或重大影响的决策措施。为确保符合上述规定，在征得数据主体的同意之前，个人数据控制者必须提供有关个人数据使用的详细信息(包括法律依据)。通过此种方式，数据主体将被充分告知其个人数据会被如何使用，从而最大限度地降低撤回同意的可能性。针对该事项，将会出台一部实施条例。

9. 被收集个人数据的个人有哪些权利？ 他们能否撤回同意、反对保留（和/或要求删除）其个人数据？ 如果可以，应如何行使该权利？

PDP Law 列举了数据主体的以下权利：

a. 就索取个人数据的一方，获取关于其明确身份、基础法律利益、索取和使用个人数据的目的及其责任的信息；

b. 根据个人数据处理的目的，填写、更新和/或纠正与其自身相关的个人数据的错误和/或不准确之处；

c. 根据现行法律获取与其自身相关的个人数据并获得其副本；

d. 根据现行法律终止处理、删除和/或销毁与其自身相关的个人数据；

e. 撤回对处理与其自身相关的个人数据的同意。

数据主体还有权通过向个人数据控制者提出请求，要求：(i)终止个人数据处理；(ii)删除个人数据；和/或(iii)销毁个人数据(PDP Law 第 42、43 和 44 条)。

请注意，数据主体的权利有以下几种例外情况：

a. 国防和国家安全利益；

b. 法律执行程序的利益；

c. 国家行政中的公共利益；

d. 在国家行政中对货币金融服务行业、支付系统和金融系统稳定性进行监督的利益；或

e. 统计和科学研究的利益。

10. 如果违反任何个人信息保护法律，是否有任何处罚、责任或救济?

是的，根据 PDP Law，违反和不遵守 PDP Law 规定的行为都可能面临以下处罚：

a. 行政处罚：(i) 书面通知；(ii) 暂停个人数据处理活动；(iii) 删除和/或销毁个人数据；和/或(iv) 行政罚款——最高年收入的百分之二(2)，依据违规的情节确定；

b. 刑事处罚：针对个人最高处六(6)年监禁和/或最高 60 亿印尼盾的罚金，针对公司最高处前述金额十(10)倍的罚金。

11. 印度尼西亚是否有强制性的数据泄露报告要求? 如果有，请总结触发报告的阈值、报告内容、报告的对象以及需要/预期的时间表?

是的，如果未能保护个人数据，个人数据控制者必须在不晚于 72 小

时内向个人数据主体和机构发出书面通知，通知内容应包括：(i)披露的个人数据；(ii)该等个人数据在何时通过何种方式披露；以及(iii)个人数据控制者处理和追回被披露的个人数据的措施。此外，在特定情形下，需要向公众发送该等通知。

此外，根据《第 71/2019 号 GR》，当任何人的行为导致系统故障或干扰时，电子系统供应商有义务在第一时间向执法部门和通信部报告。该法规并未规定提交报告的时限。

12. 印度尼西亚近期在数据隐私/数据保护方面是否有显著的发展或可能会影响未来的案例？ 还有其他需要强调的方面吗？

近期，在 2023 年 5 月发生了一起个人数据泄露事件。一家金融机构公司遭遇网络攻击，泄露的数据总量达 1.5TB。作为对这一事件的回应，该公司决定增加 IT 方面的资本性支出并变更董事会构成。由此可见，加快制定 PDP Law 的实施条例至关重要。

日本

律所

小岛国际法律事务所 / Kojima Law Offices

www.kojimalaw.jp/en/

联系人

Nozomi Watanabe
日本，东京
电话： + 81 3 3222 1401
邮箱： watanabe@kojimalaw.jp

小岛国际法律事务所(“KLO”)办理各类商事交易和公司法律事务,包括协助美国、欧洲及其他外国公司及个人进行对日投资。我们为客户在日本独特的法律和商业文化背景下开展业务过程中的各类错综复杂的问题提供指引。

KLO 在广泛的业务领域中为客户提供服务,包括为协助投资者对日开展外商直接投资。近四十年来,从国际饮料公司到外国政府再到初创企业,KLO 一直助力各种类型的外国客户在日本成功开展业务。20 世纪 90 年代初,KLO 成为首家建立法律机制以协助日本公司在印度投资的律师事务所。KLO 在建立合资企业、创建战略联盟以及处理并购交易方面拥有丰富的经验。我们为外国公司应对日常法律问题提供支持,包括监管合规和劳动事宜。

凭借强大的诉讼部门,KLO 曾代表外国政府在日本诉讼,并拥有在国际仲裁中代表日本及外国客户的丰富经验。

1. 日本的主要个人数据保护法律或法规有哪些？ 是否有跨领域的立法，以及在跨领域立法与特定领域立法中，何者将优先适用?

日本主要的个人信息保护法律是《个人信息保护法案》(Act on the Protection of Personal Information)("**APPI**")及其附属的通用指南和专门指南。专门指南涉及以下七项业务领域：

(i) 金融服务；

(ii) 医疗服务；

(iii) 电信；

(iv) 广播；

(v) 由日本邮政提供的邮政服务；

(vi) 信件递送服务；以及

(vii) 个人基因信息。

因此，在日本提供上述七项服务中任何一项的实体都需要遵守 APPI 本身、通用指南和专门指南。APPI 本身是一项跨领域立法，上述面向特定领域的专门指南仅是对 APPI 的解释。

2. 哪些监管机构负责个人信息保护法律的实施和执行?

个人信息保护委员会(Personal Information Protection Commission)("**个保委员会**")对于个人信息保护相关事宜拥有排他的管辖权(关于个保委员会及 APPI 的相关信息，包括上述通用指南和专门指南，请参阅 https://www.ppc.go.jp/en/)。

3. "个人信息" / "个人数据"是如何定义的，是否有任何类别的个人数据受到特殊或不同的保护（例如，员工、未成年人、"敏感"个人信息等）？ 如果是，这些类别是什么？ 能否简要说明适用于这些类别的特殊规则?

APPI 将"个人信息"定义为下列信息之一：

(i) 与一名在世个人有关的信息，包含姓名、出生日期或可识别个人的其他描述（包括可与其他单项信息共同识别个人的单项信息）；或者

(ii) 包含政府向所有日本居民发放的特有个人识别符号的信息（类似于美国的社会保障号码）。

(i)项中的“其他描述”指在文件、图像或电子形式中通过声音、动作或其他方式表述、记录或以其他方式表达的任何内容。

由于 APPI 明确适用于“在世个人”，因此并不保护死者的信息或公司的信息。另一方面，由于 APPI 涵盖了能够识别特定个人的信息，因此在特定情形下，该法案可以将指纹、虹膜和特定的 DNA 序列作为个人信息加以保护。

就单项信息如何能够与其他单项信息共同识别个人，举例而言，一些公司在产品注册过程中会为其客户分配特有的编号（例如“W2P99N”，而非以下讨论的“Yukio Nishima”）。当客户向公司注册产品时，他们通常会向该公司提供其姓名、地址和电话号码等特定信息。许多公司利用此类信息创建客户数据库，以便通知客户有关新产品或特殊优惠的信息。由于这个特有编号与客户的个人信息相关联，因此 APPI 将该编号本身视为个人信息。

APPI 认可特定类别的个人数据需受到不同的保护。其中一类即“敏感个人信息”，此类个人信息需要事先征得个人同意后才能获取。此类信息涉及个人的种族、宗教、意识形态、社会地位、病史、犯罪记录或曾是犯罪受害者的事实。“社会地位”旨在保护日本历史上曾因出生在特定阶层而面临特殊歧视的特定群体。

APPI 确认被称为“匿名化个人信息”的另一类个人数据受到不同的保护。此类信息与个人有关，但经过修改后已无法再识别该等个人（这意味着理论上它不再是个人信息）。一个例子是以下这组某公司同时使用的数据：（1）将客户的姓名更改为一串随机的字母和数字（“W2P99N”代替“Yukio Nishima”）；（2）使用年龄范围而不是客户的出生日期（“30—40 岁”代替“1989 年 4 月 11 日”）；以及（3）仅使用客

户居住的城市而不是客户的地址(“东京”代替“日本桥街 1 - 2 - 3 号”)。只要企业公开披露了匿名化个人信息中包含的个人信息类型,就可以转移匿名化个人信息。

与匿名化个人信息类似,APPI 还认可一类被称为“去标识化个人信息”的个人数据。这是与个人有关的但已被修改,使得在没有额外数据的情况下无法识别该等个人的信息。去标识化个人信息可以在各类企业内部用于改进业务运营,且各企业可以保留去标识化的个人信息以供未来分析之用。但是,根据 APPI,此类信息仍属于“个人数据”,因此法律仍然对拥有去标识化个人信息的企业施加了一系列限制。特别地,如果企业拥有的其他个人信息可以与去标识化个人信息结合以识别个人身份的,则该企业将面临更大的限制。

最后,2020 年修正案还引入了个人相关信息,其中包括 Cookie 和购买记录等数据。企业必须征得数据主体的同意(通常是通过选择性接受的弹窗),才能将此类数据转移给第三方并由第三方将此类数据与其他数据组合并转化为个人信息。若要向境外转移个人相关信息,转移者还必须向数据主体说明境外国家及数据接收方的数据保护制度。

4. 与个人数据相关的主要个人数据保护法律或法规的关键原则是什么?

APPI 的主要原则是在个人信息的显著实用性与保护个人信息的必要性之间进行平衡。这种平衡在该法案中显而易见,例如,法案认可个人信息的使用有助于为社会提供各种实用的商品和服务。同时,法案也认可,在发达的信息社会中,个人信息的不当使用存在严重侵犯人权的风险。

5. 是否有适用于所有企业的正式注册合规要求(例如数据保护官员的任命、数据库登记等)?

没有,不存在适用于所有企业的正式登记的合规要求。企业只需要

根据 APPI 采取适当的安全措施来保护个人信息，无需采取任命数据保护官、登记数据库等具体措施。

6. 各类组织有哪些建立与个人数据处理、使用和披露相关的合规计划（例如法律政策和运营政策、合同等）的义务?

APPI 要求企业建立系统性的安全控制措施、人员安全控制措施、物理安全控制措施和技术安全控制措施，以保护其处理的个人数据。

7. 是否对将个人数据转移到其他法域存在限制? 各类组织通常如何应对这些限制?

除非存在以下情形，否则各类组织在向其他法域转移数据前需征得数据主体的同意：

(i) 转移系日本法律/法规的要求；

(ii) 转移系为防止死亡、伤害或财产损失所必需，且难以征得个人同意的；

(iii) 转移系为改善公共卫生或促进儿童福利所必需，且难以征得个人同意的；或

(iv) 向个保委员会认可的法域进行转移，或者在特定情形下转移到至少与 APPI 的数据保护标准同样严格的法域，例如委托处理个人信息、个人信息作为企业收购的一部分而转移，以及在集团公司之间共享个人信息。

8. 是否存在对使用或重复使用个人数据进行数据分析/创新或采用人工智能或数据分析等新业务解决方案的限制? 各类组织通常如何应对这些限制?

对于问题 3 中讨论的去标识化处理后的信息，各类组织可将其用于内部目的，比如数据分析和开发新的计算模型。不同于其他形式的数据，企业可以超出数据主体最初同意的目的而使用去标识化处理后的信息，并可将其保留以用于未来进行数据分析。数据主体有权要求企

业在使用个人信息的业务完成后将其个人信息删除。

9. 被收集个人数据的个人有哪些权利？ 他们能否撤回同意、反对保留（和/或要求删除）其个人数据？ 如果可以，应如何行使该权利？

APPI 规定个人有权要求公司：

（1）披露公司所拥有的与之有关的任何个人信息；

（2）更正任何错误的信息；以及

（3）停止使用、删除和/或停止转移公司违法处理的个人信息或者公司不再需要使用的信息。如果企业发生数据泄露或个人数据权利受到其他威胁，个人也可以要求企业停止使用或删除其个人信息。

除了上述第(3)项(或许可被视为“撤回同意”)之外，APPI 并未明确允许个人撤回同意。

10. 如果违反任何个人信息保护法律，是否有任何处罚、责任或救济？

企业违反 APPI 的最高处罚为 1 亿日元，对个人的最高处罚为 100 万日元或一年以下监禁。然而，在实践中，罚款并不常见，宣判监禁的更是罕见，除非违法者故意且屡次拒绝遵守规定。日本政府部门一般会先向违法者(特别是首次违法者)出具“行政指导”。这种行政指导本质上是一种警告，政府部门在实施处罚前通常会先给违法者一个解决违法问题的机会。通常只有在违法者不遵守行政指导的情况下，政府部门才会施加处罚。

11. 日本是否有强制性的数据泄露报告要求？ 如果有，请总结触发报告的阈值、报告内容、报告的对象以及需要/预期的时间表？

是的，APPI 规定了特定情形下的强制性数据泄露报告制度。具体来

说，如果受影响的数据包括敏感数据且可能被非法使用并造成财务损失，或者数据泄露是恶意实施的，或者可能超过 1,000 名主体将受到数据泄露的影响，则企业必须在数据泄露后立即向个保委员会提交初步报告。APPI 还要求遭受数据泄露的企业通知受影响的个人，或者如果通知难以实现的，则应发布公告，并需建立渠道以便受影响的数据主体可与企业取得联系并解决问题。

12. 日本近期在数据隐私/数据保护方面是否有显著的发展或可能会影响未来的案例？ 还有其他需要强调的方面吗？

APPI 的最新修正案于 2022 年 4 月 1 日生效，并且该法案通常每三年审查和修订一次，以应对技术的变化。因此，我们可能在近几年中就会看到对 APPI 的修订，其中或将涉及近期热门的人工智能和大型语言模型问题。

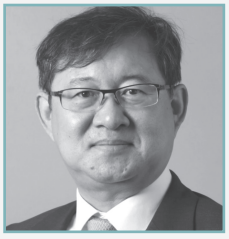
此外，欧盟委员会已经认可日本满足从欧盟向其转移个人数据所需的充分性要求，这有助于便利两地之间的个人数据转移。

韩国

律所 K1 Chamber LLP

en.k1chamber.com

联系人



Jong Jae Lee
韩国，首尔
电话： + 82 2 6956 8420
邮箱： jjlee@k1chamber.com

K1 Chamber LLP 成立于 2021 年 5 月，致力于成为一家前沿律师事务所，提供及时、创新且具有战略性的卓越服务。我们的团队由精选领域内享有盛誉的专家和行业领袖共同组成，所涉业务领域广泛，包括金融服务、知识产权/信息技术、隐私和个人信息保护、药物制造、数字经济、公司、商业、房地产和全球争议解决。在隐私和个人信息保护方面，我们的合伙人具备韩国数据隐私和数据安全法律（如《个人信息保护法案》以及与其他与信息安全和数据保护相关的法律）方面的专业知识，能够协助我们的客户更好地了解韩国复杂的隐私和个人信息保护要求。我们是 Meritas 国际律师事务所联盟的成员。K1 Chamber 承诺成为客户最值得信赖的顾问，通过与内外部专家团队的紧密协作，积极发现问题并创造性地制定战略解决方案。

1. 韩国的主要个人数据保护法律或法规有哪些？是否有跨领域的立法，以及在跨领域立法与特定领域立法中，何者将优先适用？

在韩国，主要的个人数据保护法律和法规包括《个人信息保护法案》(Personal Information Protection Act)(“**PIPA**”)和《促进信息和通信网络利用和信息保护法案》(Act on Promotion of Information and Communications Network Utilization and Information Protection)(“**Network Act**”)。这些法律旨在保护个人的隐私和个人信息权利。

PIPA 是一部适用于所有领域的综合性法律，规定了个人数据保护的一般性原则和要求。它为不同领域的个人数据保护设定了基准。作为对 PIPA 一般性规定的补充，PIPA 之外还有一些针对特定领域的法律和法规。这些特定法律适用于某些具体的行业或领域，如金融服务、医疗健康、电信和征信。虽然这些特定法律规定的额外要求面向特定领域，但仍应该与 PIPA 结合在一起理解。当出现冲突或不一致时，针对特定领域的法律必须遵守 PIPA 规定的一般性原则和要求。

2. 哪些监管机构负责个人信息保护法律的实施和执行？

在韩国，内政安全部(Ministry of the Interior and Safety)(“**MOIS**”)负责个人数据保护的整体监管和协调。韩国通信委员会(Korea Communications Commission)(“**KCC**”)负责执行 Network Act，Network Act 中包含了电子通信情形下个人信息保护的相关规定。韩国个人信息保护委员会(Korea Personal Information Protection Commission)(“**PIPC**”)是负责实施和执行 PIPA 的中央行政机构，其职能包括制定指引和法规、处理投诉和纠纷，以及对违规行为作出行政罚款和处罚。其他特定领域监管机构也可能在各自领域内负责执行个人数据保护法规。

3. “个人信息”/“个人数据”是如何定义的，是否有任何类别的个人数据受到特殊或不同的保护（例如，员工、未成年人、“敏感”个人信息等）？ 如果是，这些类别是什么？ 能否简要说明适用于这些类别的特殊规则?

在韩国，个人信息被定义为能够识别特定个人的任何信息，包括但不限于姓名、居民登记号码、照片、指纹和个人身份号码。根据 PIPA，某些类别的个人数据受到特殊保护。首先是某些敏感个人信息，其包括种族、民族、意识形态、信仰、政治倾向、工会成员身份、健康状况、性取向、从基因测试中获得的 DNA 信息、构成犯罪记录的数据，以及为唯一识别个人之目的、对与个人身体和生理或行为特征相关的数据进行特定技术处理所产生的个人信息。

此类数据需要更高水平的保护，通常需要征得明确同意才能收集、使用和披露。14 岁以下儿童的个人信息也受到额外保护，包括需要获得父母或法定监护人的同意。

4. 与个人数据相关的主要个人数据保护法律或法规的关键原则是什么?

在韩国，PIPA 和 Network Act 规定的主要原则如下：

首先，个人数据的收集和使用应仅限于特定的合法目的，并且应向个人告知数据收集的目的。

其次，一般而言，收集、使用和披露个人数据需要征得本人同意。同意应以明确和自愿的方式做出，个人有权撤回同意。

再次，应以为实现预期目的最少且必要的方式收集和处理个人数据。原则上禁止过度收集和保留个人数据。

然后，各类组织必须采取适当的技术和管理措施，以保护个人数据免受未经授权的访问、更改、披露或破坏。

最后，个人拥有各种权利，包括访问其个人数据的权利、要求更正或

删除不准确或过时数据的权利，以及在特定情形下拒绝数据处理的权利。

5. 是否有适用于所有企业的正式注册合规要求（例如数据保护官员的任命、数据库登记等）？

在韩国，存在针对企业的与个人信息相关的正式登记和合规要求。以下是部分主要的合规要求：

某些组织（例如处理大量个人信息或从事特定类型的数据处理活动的组织）必须任命一名数据保护官（Data Protection Officer）（“**DPO**”）。DPO 负责监督和确保个人信息保护的合规。根据 PIPA，在特定情形下（如处理敏感个人信息或数据主体达到一定数量），这些组织需要向 PIPC 登记其数据库。各类组织还需要采取适当的技术和管理措施，以保护个人信息免受未经授权的访问、丢失、更改或披露。

6. 各类组织有哪些建立与个人数据处理、使用和披露相关的合规计划（例如法律政策和运营政策、合同等）的义务？

各类组织必须建立并维护与个人数据的处理、使用和披露相关的合规方案。PIPA 要求企业制定并实施各类制度和规程以实现个人信息保护，包括制定隐私政策，隐私政策中应说明如何收集、使用和披露个人信息。各类组织还必须与为其处理个人信息的第三方服务供应商签订数据保护协议。这些协议必须明确规定处理的目的和范围、采取的个人信息保护措施、以及服务供应商的义务。

7. 是否对将个人数据转移到其他法域存在限制？ 各类组织通常如何应对这些限制？

韩国 PIPA 明确规定了可向域外转移个人数据的若干情形。根据 PIPA，可将个人信息转移至境外的情况包括：（1）已取得数据主体对于个人信息转移至境外的单独同意；（2）为签署和履行与数据主体之

间的协议而必需委托处理或存储个人信息;(3) 个人信息接收方已获得 PIPC 的认证;以及(4) 韩国政府认定接收个人信息的国家具有足够的数据保护水平。

8. 使用或重复使用个人数据进行数据分析/创新，或采用人工智能或数据分析等新型业务解决方案方面有哪些限制（如有）？ 各类组织一般如何应对这些限制?

在韩国,各类组织在为该等目的收集和使用个人数据的之前必须征得个人的同意。他们在处理个人数据时还必须遵守目的限制、数据最少化和去标识化等原则。

各类组织通常会采取相关措施来应对这些限制,例如同意管理、匿名化和去标识化、数据安全措施、隐私影响评估、合规框架等。

9. 被收集个人数据的个人有哪些权利？ 他们能否撤回同意、反对保留（和/或要求删除）其个人数据？ 如果可以，应如何行使该权利?

在韩国,个人就对其个人数据的收集和处理拥有相关权利。在特定情况下,他们有权撤回同意、反对保留其个人数据,以及要求删除其个人数据。为撤回同意或反对保留其个人数据,需要提交一份申请明确表示希望撤回同意、反对保留或要求删除其个人数据,并提供姓名、联系方式以及希望处理的具体个人数据等详情。

10. 如果违反任何个人信息保护法律，是否有任何处罚、责任或救济?

在韩国,如果违反个人信息保护法律,存在相关处罚、责任和救济措施。主要的处罚如下:

1. 行政处罚:PIPC 有权对违反 PIPA 的行为处以行政罚款。根据违法行为的严重程度,罚款金额在 300 万韩元(约合 2,500 美元)到违法实体年收入的 5% 之间。

2. 刑事处罚：对于严重违规、故意违法或非法转移个人信息的情况，可能会处以刑事处罚。构成犯罪的个人，可能面临最高 5 年的监禁或最高 5,000 万韩元(约合 4.2 万美元)的罚款。

3. 损害赔偿：如因侵犯个人信息权利导致个人遭受损害，可以通过民事诉讼寻求赔偿，包括对侵权行为造成的损害要求经济补偿。

4. 整改措施：PIPC 可以责令相关组织进行整改，如停止收集或使用个人信息、采取安全措施或进行内部审计以确保合规。

11. 韩国是否有强制性的数据泄露报告要求？ 如果有，请总结触发报告的阈值、报告内容、报告的对象以及需要/预期的时间表?

韩国存在强制性的数据泄露报告制度。根据 PIPA，如果数据泄露涉及 1,000 人或以上的敏感个人信息(包括居民登记号码、密码、财务信息等)，相关组织必须报告。当发生数据泄露时，相关组织必须报告以下信息：泄露的性质、为减轻损害而采取或计划采取的措施，以及为防止未来泄露而采取或计划采取的措施。应当向 PIPC 和受影响的个人报告数据泄露情况。如果泄露影响 1,000,000 人以上，可能同时需要进行公告通知。数据泄露一经确认，必须立即报告，但法律并未规定具体的时限。

12. 韩国近期在数据隐私/数据保护方面是否有显著的发展或可能会影响未来的案例？ 还有其他需要强调的方面吗?

最近一个值得注意的事件是 PIPA 的新修正案，涉及向境外转移个人信息问题。根据于 2023 年 3 月 14 日颁布并于 2023 年 9 月 15 日实施的新修正案，在未征得数据主体同意的情况下，也有可能可以将个人信息转移出境。对于获得 PIPC 认证的主体和被韩国政府认定为具有足够数据保护水平的国家，如向其跨境转移个人信息，无需征得同意。

近些年来，韩国发生了几起备受瞩目的数据泄露和隐私事件，引起了

公众对数据保护的关注和担忧。这些事件引发了关于加强立法和执法的讨论和呼吁。

此外,欧盟委员会已经认可韩国满足从欧盟向其转移个人数据所需的充分性要求,这有助于便利两地之间的个人数据转移。

总而言之,这些变化表明韩国越来越重视数据隐私和保护,我们可以预见未来在个人信息保护方面会有更多的进步和举措。

马来西亚

律所

Zul Rafique & Partners

www.zulrafique.com.my

联系人

Yit Meng Kor
马来西亚，吉隆坡
电话： + 603 - 62098247
邮箱： darren@zulrafique.com.my

Zul Rafique & Partners(ZRp)是一家总部位于吉隆坡的律师事务所,成立于 1999 年 12 月。ZRp 自成立以来取得了显着的增长,现在已成为一家大型、涉猎广泛的商业法律事务所。

我们战略性地将我们的人才集中到专门的业务团队中,以最大限度地发挥我们深厚的专业知识和经验。我们不断扩大的业务也考虑到了这一点,您会发现我们律师拥有无可挑剔的法律基础、多样化的共同经验和专业技能。

我们的业务团队包括:

- 银行与金融
- 资本市场
- 通讯与多媒体
- 建设工程争议解决
- 企业责任与风险管理
- 公司/并购
- 企业房地产
- 雇佣与劳资关系
- 能源与公用事业
- 基础设施与建设
- 知识产权
- 法律取证调查与合规
- 诉讼
- 石油和天然气
- 项目与企业咨询
- 税法

1. 马来西亚主要的个人数据保护法律或法规有哪些？ 是否存在跨领域立法？ 跨领域立法与特定领域立法之间，何者将优先适用？

在马来西亚，主要的个人数据保护立法是《2010 年个人数据保护法》(Personal Data Protection Act 2010)("**PDPA**")及其附属法规。PDPA 适用于：

(i) 处理与商业交易有关的任何个人数据的任何人；及

(ii) 控制或授权处理与商业交易有关的任何个人数据的任何人，

根据 PDPA 第 23 条，可以发布并登记业务守则来规范某类数据用户的个人数据事宜。业务守则可由个人数据保护委员(Personal Data Protection Commissioner)("**PDP 委员**")指定的数据使用者协会制定，或在某些情况下由 PDP 委员发布。业务守则在业务守则登记册中注册登记后方才生效。PDPA 第 29 条强制要求数据使用者遵守业务守则，否则可能数据使用者会被处以罚款和/或监禁。

《个人数据保护通用业务守则》(General Code of Practice of Personal Data Protection)是一项已登记的业务守则，适用于尚未准备业务守则的数据使用者及/或没有数据使用者协会为其制定特定类型业务守则的数据使用者。另外，数据使用者协会还制定了针对特定领域的业务守则，用于处理特定领域的数据保护要求。

客户数据(可能包括个人数据)的保护也受到特定领域立法的监管，并且也必须遵守 PDPA。相关领域包括银行和金融、医疗健康和电信。

2. 哪些监管机构负责个人信息保护法律的实施和执行？

通信和数字部长(Minister of Communications and Digital)("**部长**")负责监管与 PDPA 相关的事务，部长任命的 PDP 专员则履行 PDPA 授予的职能和权力。

根据 PDPA，这两个机构的职能和权力有明确的划分和界定。

3. “个人信息”/“个人数据”是如何定义的，是否有任何类别的个人数据受到特殊或不同的保护（例如，员工、未成年人、“敏感”个人信息等）？ 如果是，这些类别是什么？ 能否简要说明适用于这些类别的特殊规则?

PDPA 下的个人数据是指与商业交易有关的任何信息，且该信息：

(i) 根据上述目的下达的指示，正在被全部或部分通过自动化设备进行处理；

(ii) 被记录的目的是全部或部分通过自动化设备进行处理；或

(iii) 被记录为相关归档系统的一部分或意图使其成为相关归档系统的一部分，

直接或间接与通过该数据或数据使用者在商业交易中掌握的其他数据已识别或可识别的数据主体相关，包括任何敏感的个人数据以及对数据主体的评价，但不包括为征信机构根据《2010 征信机构法》(Credit Reporting Agencies Act 2010)开展的征信业务而处理的任何信息。

PDPA 还定义了特定的个人数据类别，即“敏感个人数据”，包括有关数据主体健康和信仰、犯罪或涉嫌犯罪的信息，或部长在《宪报》公布的其他个人数据。数据使用者不得处理“敏感个人资料”，除非：

(i) 有明确同意；

(ii) 满足明确同意的例外情况；或者

(iii) 该信息已由于数据主体故意采取的措施而被公开。

另一个子类别是与十八岁以下数据主体相关的个人数据。处理此类个人数据必须获得数据主体的父母或监护人的同意。

4. 与个人数据相关的主要个人数据保护法律或法规的关键原则是什么?

PDPA 规定了七项关键原则：

(i) 一般原则——除非豁免,在处理数据主体的个人信息之前必须获得其同意,并且处理应出于合法、充分、相关的目的且不超过目的的范围;

(ii) 通知和选择原则——告知数据主体其个人数据的处理方式;

(iii) 披露原则——不得超出收集时已公开的目的之外披露个人数据,也不得向数据保护通知以外的任何一方披露个人数据;

(iv) 安全原则——确保采取足够的安全措施,保护个人数据免遭丢失、误用、修改、未经授权或意外访问或披露、更改或破坏;

(v) 保存原则——个人数据的保存时间不得超过实现相关目的所需的时间;

(vi) 数据完整性原则——确保个人数据准确、完整和最新;及

(vii) 访问原则——数据主体有权访问和更正其个人数据。

5. 是否有适用于所有企业的正式注册合规要求(例如数据保护官员的任命、数据库登记等)?

形式上的注册要求仅适用于《2013 年个人数据保护(数据使用者类别)指令》(已修订)(Personal Data Protection (Class of Data Users) Order 2013)(as amended)中规定的数据使用者,其中该数据使用者须向 PDP 专员注册登记。

6. 各类组织有哪些建立与个人数据处理、使用和披露相关的合规计划(例如法律政策和运营政策、合同等)的义务?

每个组织都必须制定合规计划,以确保遵守七项个人数据保护原则以及相关的业务守则(如果适用)。此外,此类合规计划必须符合《2015 年个人数据保护标准》(Personal Data Protection Standard 2015)("**数据保护标准**")的要求。《数据保护标准》规定了与个人数据相关的安全、保存和数据完整性标准的最低要求。

7. 是否对将转移个人数据至其他法域存在限制？ 各类组织通常如何应对这些限制？

PDPA 第 129 条禁止数据使用者将个人数据转移到马来西亚境外，除非该国家在部长公布的《宪报》公告中（“**白名单制度**”）。尽管有一般性禁止，数据使用者仍可在符合第 129 条规定的例外情况时，将个人数据传输到马来西亚境外的地方。例外情况包括（但不限于）数据主体已同意传输，或者传输是在为订立或履行合同所必需的。

PDP 专员发布的第 01/2020 号公众咨询文件（Public Consultation Paper No.01/2020）（“**PCP No.01/2020**”）曾建议取消白名单制度，并修改 PDPA 第 129 条，明确规定允许转移个人数据至马来西亚境外的条件。PCP No.01/2020 认为这对于促进电子商务交易和自由贸易协定至关重要。

8. 是否存在对使用或重复使用个人数据进行数据分析/创新或采用人工智能或数据分析等新业务解决方案的限制？ 各类组织通常如何应对这些限制？

各类组织必须获得数据主体的适当同意才能出于此类目的处理个人数据。如果在首次要求数据主体提供其个人数据或数据使用者首次收集数据主体的个人数据时未获得该等同意，则必须取得数据主体的同意才能进一步处理该个人数据。

或者，数据使用者可以考虑匿名化数据以防止任何个人数据被处理和/或披露。

9. 被收集个人数据的个人拥有哪些权利？ 他们可否撤回同意、反对保留（和/或要求删除）其个人数据？ 以及如果可以，该如何行使？

PDPA 授予数据主体以下权利：

（i） 访问个人数据（第 30 条）；

（ii） 更正个人数据（第 34 条）；

(iii) 撤回对个人数据处理的同意(第 38 条);

(iv) 防止可能造成损害或困扰的处理(第 42 条);及

(v) 防止出于直接营销目的进行处理(第 43 条)。

数据主体可根据 PDPA 相应条款向数据使用者发出书面通知并支付规定费用,以行使其上述权利。PDPA 要求数据使用者在收到通知后遵守数据主体的要求,除非数据使用者能够提供无法履行理由。但是在 PDPA 第 43 条规定的场景中,数据使用者必须遵守数据主体的书面请求,不可拒绝。PDPA 并没有规定数据主体有权依据 PDPA 第 44 条要求删除数据使用者所保存的个人数据,该条款仅要求数据使用者保存和维护与已经或正在由数据使用者处理的个人数据相关的信息。

10. 如果违反任何个人信息保护法律,是否有任何处罚、责任或救济?

违反 PDPA(包括个人数据保护原则)将构成违法行为,可能会面临罚款和监禁。例如,如果违反 PDPA 第 5 条,一经定罪,数据使用者将被处以不超过 30 万令吉的罚款、两年以下的监禁,或两者并罚。可以通过其官网访问个人数据保护部门(Department of Personal Data Protection)列出的违法行为清单。

11. 马来西亚是否有强制性的数据泄露报告要求? 如果有,请总结触发报告的阈值、报告内容、报告的对象以及需要/预期的时间表?

PDPA 不强制要求数据使用者通知或报告任何数据泄露事件。

然而,PCP No.01/2020 建议增加此类强制报告的规定。

12. 马来西亚近期在数据隐私/数据保护方面是否有显著的发展或可能会影响未来的案例? 还有其他需要强调的方面吗?

最近的显著的发展包括 2020 年发布的 PCP No.01/2020。该文件在

征求利益相关方对 PDPA 新增的功能或条款的意见。它提供了对于马来西亚 PDPA 中个人数据保护义务的新发展与功能的政策见解。

PCP No.01/2020 建议的重点包括：

(i) 任命一名合规官员；

(ii) 被遗忘权，即获得删除个人数据的权利；

(iii) 数据可携带权，即以结构化和机器可读格式获取数据并传输给其他数据使用者的权利；

(iv) 数据保护设计，即要求采取旨在践行数据保护原则的适当技术和操作措施；

(v) 个人数据泄露通知；

(vi) 实施拒收来电的登记(Do Not Call Registry)；

(vii) 直接对数据处理者施加义务，包括要求处理者采取适当的技术和组织措施、实施数据泄露通知以及保持记录处理活动的类别；和

(viii) 将 PDPA 的适用范围扩大到联邦和州政府。

如果这些新重点被引入 PDPA，PDPA 将更加符合欧盟通用数据保护条例(General Data Protection Regulation)。然而，对于现有组织(尤其是中小型组织)来说，这将是一个巨大的转变，他们可能需要更多的时间和预算来满足这些要求。

鉴于近期马来西亚 COVID－19 追踪应用程序 MySejahtera 的数据泄露事件，通信和数字部长强调了 PDPA 的不足之处，包括数据泄露事件的罚款。部长表示，通信和数字部正在考虑修订前几届政府提出的 PDPA 修正案，并计划在 2023 年底之前向议会提交新的修正案。

菲律宾

律所 **ACCRALAW**

www.accralaw.com

联系人

John Paul M. Gaba
菲律宾，马尼拉大都会
电话： + 63 2 88308000
邮箱： jmgaba@accralaw.com

Angara Abello Concepcion Regala & Cruz Law Offices（ACCRALAW）是一家领先的律师事务所，提供全方位法律服务，拥有约 170 名律师。律所主要办公室位于马尼拉大都会新开发的博尼法西奥环球城的 ACCRALAW 大厦。同时，律所还在米沙鄢群岛的宿雾市和棉兰老岛的达沃市的繁荣商业中心设有提供全面服务的分支机构。律所在为本地和跨国客户处理多样化、重大和复杂的商业项目和交易方面拥有出色的经验，并参与了具有里程碑意义的诉讼案件。ACCRALAW 的客户不仅代表了各个商业和行业领域，还包括专业的组织和个人。律所共有七个业务部门及其两个分支机构为客户提供服务，能够提供及时、创造性和战略性的法律解决方案，并使用具有成本效益的管理和法律专家满足客户的需求。

1. 菲律宾主要的个人数据保护法律或法规有哪些？ 是否存在跨领域立法？ 跨领域立法与特定领域立法之间，何者将优先适用？

菲律宾适用的法律是 2012 年《数据隐私法》/《第 10173 号共和国法案》(Data Privacy Act of 2012 or Republic Act No.10173)("**DPA**")及其实施细则和规定(Implementing Rules and Regulations)("**IRR**")。国家隐私委员会(National Privacy Commission)("**NPC**")还会发布通告和建议,进一步完善和实施 DPA 及其 IRR 的条款。

2. 哪些监管机构负责个人信息保护法律的实施和执行？

监督菲律宾个人信息隐私法律法规实施的牵头机构是**NPC**。

3. "个人信息"/"个人数据"是如何定义的，是否有任何类别的个人数据受到特殊或不同的保护（例如，员工、未成年人、"敏感"个人信息等）？ 如果是，这些类别是什么？ 能否简要说明适用于这些类别的特殊规则？

"个人信息"被定义为持有该信息的实体可以从中明显识别出个人身份的任何信息,无论是否以实物形式记录。与法人实体(例如企业、公司和合伙)相关的信息不受 DPA 保护,虽然法人实体的记录或文件很可能包含个人信息,并且此类记录或文件的部分内容应被视为在 DPA 管辖的范围内。

菲律宾的法律规定了两组"特殊"个人信息——"敏感个人信息"(Sensitive Personal Information)和"特许保密信息"(Privileged Information)。

"特许保密信息"的定义是"根据《法院规则》(Rules of Court)和其他有关法律构成特许保密通信的任何形式的数据"。根据《法院规则》第 24 章第 130 条,以下内容构成"特许保密通信":(1) 夫妻或配偶通讯;(2) 律师与委托人的通讯;(3) 医患沟通;(4) 神父与忏悔者的通讯;(5) 公职人员的通讯。

"敏感个人信息"是指以下个人信息:

(1) 关于个人的种族、民族、婚姻状况、年龄、肤色以及宗教、哲学或政治倾向;

(2) 关于个人的健康、教育、基因或性生活,实施或被指控实施任何违法行为的任何程序、该等程序的处理结果或任何法院在该等程序中判处的刑罚;

(3) 政府机构向个人签发的特有信息,包括但不限于社会保障号码、过去或目前的健康记录、执照或其驳回、中止或或撤销信息以及税费返还;和

(4) 由行政命令或议会法案特别确定的、需要保密保管的信息。

根据 DPA,“特许保密信息”和“敏感个人信息”受到同等保护。

4. 与个人数据相关的主要个人数据保护法律或法规的关键原则是什么?

与欧盟 GDPR 的原则类似,“个人信息处理”必须遵守透明性、合法目的和相称性的一般原则。例如,如果收集个人数据用于抽奖,则必须告知数据主体,其数据的收集、处理和保存仅用于满足抽奖目的且仅在满足抽奖活动要求所需的时间内进行。数据不得用于任何其他目的或保存时间超过必要的时间。收集的数据还必须与向数据主体告知的目的相称。DPA 的透明性原则需要获得数据主体的明确且明示的同意或其他处理个人信息的有效法律依据。首先,必须告知数据主体其个人信息将如何使用或“处理”——涉及哪些主体(例如数据控制者、数据处理者、第三方)、需要此类个人信息的目的、个人信息应保存多长时间,为保护数据而采取的适当安全措施,以及数据主体在有任何疑虑时如何联系数据控制者的详细联系信息。如果不满足上述任何条件,根据 DPA,“个人信息处理”通常会被视为未经授权。

5. 是否有适用于所有企业的正式注册合规要求(例如数据保护官员的任命、数据库登记等)?

一般来说,个人信息控制者(Personal Information Controller)(“**控制**

者”)和个人信息处理者(Personal Information Processor)(“**处理者**”)需要任命一名数据保护官(Data Protection Officer)(“**DPO**”)。控制者和处理者必须向 NPC 登记它们的 DPO 以及数据处理系统(“**处理系统**”),如果它们:

(1) 雇用至少两百五十(250)名员工;或

(2) 不管雇员人数多少,从事可能对数据主体的权利和自由构成风险的操作或个人信息处理活动,或者此类处理行为不是偶然性的;或

(3) 处理至少一千(1,000)人的敏感个人信息;或

(4) 不管雇员人数或者数据主体人数多少,只要是被 NPC 列为“关键部门”的行业,如银行和非银行金融机构;医院、医疗中心和健康有关的组织;中小学校和大学;研究机构;业务流程外包公司(包括“共享服务”的提供商或拥有“垄断市场”的公司);电信公司。

6. 各类组织有哪些建立与个人数据处理、使用和披露相关的合规计划(例如法律政策和运营政策、合同等)的义务?

所有控制者和处理者必须采取适当、合理的安全措施,确保个人信息的“保密性、完整性和可用性”。措施分为三(3)组:(1) 组织性的;(2) 物理性的;(3) 技术性的安全措施。

组织性的安全措施包括:

(1) 任命 DPO;

(2) 构建能够提供组织性、物理性和技术性安全措施的数据保护策略;

(3) 保存充分描述其数据处理系统并识别有权访问个人数据的人员职责的记录;

(4) 为有权访问个人数据的员工组织关于隐私或安全政策方面的能力建设和训练或培训项目;

(5) 为数据主体行使其权利并为数据保留计划、开发并实施收集和处理个人数据、访问管理、系统监控的程序,以及发生安全性事件或技术问题时需遵循的方案;及

(6) 确保与处理者(即第三方供应商)的合同也采取 DPA 及其 IRR 要求的安全措施。

物理性的安全措施包括:

(1) 建立制度/流程以监督和限制房间、工作区域或设施的访问权限及其中的活动(包括关于使用和访问电子媒体的指南);

(2) 对办公空间和工作区域进行设计以确保个人数据处理者的隐私;

(3) 定义一个适用于个人数据处理者的职责、责任和工作时间表方面的明确描述,以确保只有实际履行职责的自然人才能够在规定的时间里处于该房间内;

(4) 实施有关电子媒体转移、删除、处理和再使用的政策和程序;及

(5) 建立预防文件和设备发生机械性损坏的政策和程序。

技术性的安全措施包括:

(1) 制定有关处理个人数据的安全政策;

(2) 建立保护计算机网络抵御未经授权的访问或确保系统的数据完整性和功能的防护措施;

(3) 确保和保持其处理系统和服务的保密性、完整性、可用性和复原能力;

(4) 定期监控安全漏洞、访问漏洞,并针对数据泄露采取预防性、纠正性和缓和性的措施;

(5) 提高以及时方式恢复个人数据可用性和可访问性的能力;

(6) 建立检测安全措施有效性的流程和规约;及

(7) 实施在存储、传输、身份验证过程中对个人数据进行加密的措施,或采取任何控制和限制访问的措施。

7. 是否对将个人数据转移到其他法域存在限制？ 各类组织通常如何应对这些限制？

菲律宾允许跨境传输，但前提是：(1)相关数据主体充分了解并同意此类传输；并且(2)第三方接收者签订包含“强制性条款”的协议，以确保接收者遵守 DPA 的要求并采取适当的安全措施。这些要求也适用于属于同一集团的附属或相关公司或实体。

8. 是否存在对使用或重复使用个人数据进行数据分析/创新或采用人工智能或数据分析等新业务解决方案的限制？ 各类组织通常如何应对这些限制？

一般而言，DPA 不会限制与此类技术相关的个人信息使用，但前提是：(1) 相关数据主体已充分了解/被告知此类个人信息的使用及使用目的，并且取得了数据主体的同意；(2) 采取合理、适当的安全措施。

9. 被收集个人数据的个人拥有哪些权利？ 他们可否撤回同意、反对保留（和/或要求删除）其个人数据？ 以及如果可以，该如何行使？

数据主体有权：(1) 被告知其数据正在被处理；(2) 了解此类数据的处理程度(例如范围、目的、数据可能向谁披露数据、存储期限)；(3) 被告知行使访问和更正数据的权利；(4) 合理访问其数据，并对数据中的不准确或错误提出异议；(5) 暂停销毁其数据；(6) 因个人信息不准确、不完整、过时、错误、或非法获取或未经授权地使用个人信息的行为而遭受的损失获得赔偿。数据主体可以撤回对第三方保存个人信息的同意，虽然 DPA 及其 IRR 中没有关于撤回同意的具体流程。

10. 如果违反任何个人信息保护法律，是否有任何处罚、责任或救济？

处罚包括十万比索至五百万比索的强制罚款，以及六(6)个月至六(6)年的监禁。此外，数据主体可以提出诉讼请求民事损害赔偿(例如，实际损害赔偿、精神损害赔偿、惩戒性损害赔偿等)。

11. 菲律宾是否有强制性的数据泄露报告要求？ 如果有，请总结触发报告的阈值、报告内容、报告的对象以及需要/预期的时间表?

是的。如果出现以下情况，则必须向 NPC 报告并通知受影响的数据主体：

（1）敏感的个人信息或任何其他信息可能被用于身份欺诈；

（2）有理由相信此类信息可能已被未经授权的人员获取；及

（3）控制者或 NPC 认为，此类未经授权的信息获取可能会给任何受影响的数据主体带来严重损害的实际风险。

控制者或处理者应在其知悉或有合理理由相信发生个人数据泄露后 72 小时内进行强制报告。这是控制者的义务。

12. 菲律宾近期在数据隐私/数据保护方面是否有显著的发展或可能会影响未来的案例？ 还有其他需要强调的方面吗?

NPC 在 2022 年 8 月 8 日发布第 2022－01 号通知（Circular No.2022－01 dated 08 August 2022）（简称“**通知**”）。《通知》在 2022 年 8 月 27 日生效，规定了 NPC 在处理违反 DPA、IRR 以及 NPC 发布的其他规定的申诉时，行使准司法职权可以处以的行政罚款的数额。该通知将所有违法行为分为三类，并规定了相应的罚款范围（按照违法行为发生时上一年度总收入的百分比计算）：

（1）严重违规，处罚 0.5% 至 3%

（2）重大违规行为，处罚 0.25% 至 2%

（3）其他违规行为，处罚 0.25% 至 2%

在任何情况下，单一行为的罚款总额不得超过五百万比索（PhP 5,000,000. 00）（或约 90,000. 00 美元）。

新加坡

律所

Joyce A. Tan & Partners LLC

www.joylaw.com

联系人

Jeffrey Lim
新加坡
电话： + 65 6333 6383
邮箱： jeffrey@joylaw.com

该事务所是一家专门的商业律师事务所，提供全方位的企业和商业法律服务，在知识产权、科技、电信、媒体和隐私方面具有独特优势。该事务所在国际舞台上为广泛的行业提供服务，并在新加坡商业的重大前沿发展开创了多种形式的合法交易。

在数据保护和隐私方面，该事务所就数据保护法律法规提供建议，并协助制定政策和流程以遵守全球法律的要求。该事务所因跨境工作和国内的工作具有声誉。该事务所的客户从全球跨国公司（包括“Big Tech”公司）到与我们合作开展关键战略项目的国内知名公司，再到成熟的初创科技企业。该事务所针对网络安全、数据分析、数据挖掘、人工智能、内容合规以及战略和政策审查等问题提供针对性的解决方案。

该事务所的服务理念是旨在为客户厘清情况，并在可能出现的各种需求之间为客户提供流畅无忧的服务体验。

1. 新加坡主要的个人数据保护法律或法规有哪些？ 是否存在跨领域立法？ 跨领域立法与特定领域立法之间，何者将优先适用？

在新加坡，个人数据受到《2012 年个人数据保护法》(Personal Data Protection Act 2012)("**PDPA**")的广泛监管。PDPA 规范私营企业对个人数据的收集、使用、披露和处理。

PDPA 还有附属立法以及个人数据保护委员会(Personal Data Protection Commission)("**PDPC**")发布的各种指南的补充。这些补充文件包括实用工具，例如关于关键概念、PDPA 应用的指南以及针对其他主题和特定领域的指南(例如，关于信息和通信技术系统、区块链设计、安全系统中的生物识别数据、数据泄露防护以及教育部门等领域的 PDPA 指南)。

各领域的监管机构还会适用包含数据保护或数据隐私内容的特定领域法律，例如《2020 年医疗保健服务法》(Healthcare Services Act 2020)或《1999 年电信法》(Telecommunications Act 1999)下的具体规则和法规。如果特定领域法律和 PDPA 之间存在任何不一致，特定领域立法规定的标准和义务优先于 PDPA。

2. 哪些监管机构负责个人信息保护法律的实施和执行？

PDPC 是负责管理和执行 PDPA 的机构。

3. "个人信息"/"个人数据"是如何定义的，是否有任何类别的个人数据受到特殊或不同的保护（例如，员工、未成年人、"敏感"个人信息等）？ 如果是，这些类别是什么？ 能否简要说明适用于这些类别的特殊规则？

个人数据被定义为与可识别的个人相关的数据，而无论数据真实与否，包括：

(i) 可通过该等数据识别；或

(ii) 可通过相关组织已经或可能获取的其他信息识别。

因此，个人数据包含直接标识符和间接标识符。

虽然 PDPA 没有具体规定“敏感”个人数据，但根据 PDPA 中有关数据泄露报告的各种规则和规定，泄露可能导致重大损害的数据，将适用更严格的标准。

此外，某些类别的个人数据在个人数据处理方面可能会受到不同的处理。例如，涉及员工个人数据时，同意义务存在某些例外情况；涉及未成年人个人数据时，存在需要采取额外保护措施的具体要求。

4. 与个人数据相关的主要个人数据保护法律或法规的关键原则是什么?

PDPA 并未阐明原则，而是规定了以下关键义务：

(1) **同意：**只有出于个人同意的目的才能收集、使用或披露个人数据，除非有其他例外情况。

(2) **通知：**各组织必须通知个人收集、使用或披露其数据的目的。

(3) **目的限制：**只能出于正常人在特定情况下认为适当的目的而收集、使用或披露个人数据，各组织不得将此类同意作为提供产品或服务的条件。

(4) **准确性：**如果个人数据可能被用于做出影响个人的决策或向其他组织披露，则相关组织应尽合理努力确保所收集的个人数据准确和完整。

(5) **保护：**各类组织应制定合理的安全规划来保护其拥有的个人数据，防止未经授权的访问、收集、使用、披露或类似风险。

(6) **保存限制：**当任何业务或法律目的不再需要个人数据时，各类组织应停止保存或以适当方式处置个人数据。

(7) **转移限制：**个人数据只能按照 PDPA 及其法规规定的要求转移到其他国家，并应确保当地拥有与 PDPA 相当的保护标准。

(8) **访问和更正：**个人有权请求访问其个人数据、有关如何使用或披露数据的其他信息，并且更正其个人数据中的任何错误或遗漏。

(9) **问责制：**各类组织对其拥有和控制的个人数据负责。因此，各类组织必须采取措施确保其能够履行 PDPA 规定的义务，并在需要时证明。

(10) **数据泄露通知：**各类组织必须评估数据泄露是否需要通报，并在需要时通知 PDPC 和受影响的个人。

5. 是否有适用于所有企业的正式注册合规要求（例如数据保护官员的任命、数据库登记等）？

虽然没有正式的登记要求，但各组织必须任命一位或多位数据保护官（“DPO”），以确保该组织遵守 PDPA。各类组织必须通过向会计与企业管制局（Accounting and Corporate Regulatory Authority）登记或在该组织网站上易于访问的部分提供信息等方式来提供 DPO 的联系信息。

6. 各类组织有哪些建立与个人数据处理、使用和披露相关的合规计划（例如法律政策和运营政策、合同等）的义务?

各类组织在建立合规计划时有四项主要义务。

首先，各类组织必须制定并实施数据保护政策和实践，履行 PDPA 规定的义务。其次，各类组织必须制定一个流程来接收和回应因实施 PDPA 而可能出现的投诉。第三，各类组织必须面向员工，告知并开展数据保护政策和实践的培训。最后，各类组织还必须根据要求提供有关其数据保护政策、实践和投诉流程的信息。

7. 是否对将个人数据转移到其他法域存在限制？ 各类组织通常如何应对这些限制?

根据《2021 年个人数据保护条例》（Personal Data Protection Regulations 2021），只有各类组织在采取适当措施，确保境外接收方受到法律强制义务或特定认证的约束，为被转移数据提供与 PDPA 规定的标准相当的保护时，各类组织才可将个人数据转移到海外。

这个问题其实是，什么样的法律强制义务有助于对个人数据的保护

能达到 PDPA 所要求的标准。PDPA 接受的解决方案包括提供方和接收方之间充分的合同约定、依赖具有约束力的公司规则、其他具有法律约束力的文书等。

8. 是否存在对使用或重复使用个人数据进行数据分析/创新或采用人工智能或数据分析等新业务解决方案的限制？ 各类组织通常如何应对这些限制？

尽管 PDPA 下的某些规则将对使用或重复使用个人数据进行分析、创新以及采用新解决方案或人工智能施加一定的限制，但新加坡希望通过例外情况的规定及向各类组织发布有关这些技术的创新和应用的指南的方式来进行解决。

例外情形包括业务改良场景可豁免同意义务，这一例外情形对于提供个性化产品或服务，或者识别新解决方案或机会而言非常有用。为了应用例外情形，各类组织必须采取特定的流程和保障措施。另一种例外情形包括研究场景可豁免同意义务，其中会适用其他标准和要求。

PDPC 还发布了关于在生物识别解决方案、区块链、匿名化等领域中使用个人数据的指南，并且截至本书发布时，PDPC 正在就即将发布的关于在人工智能推荐和决策系统中使用个人数据的指南征求意见。

9. 被收集个人数据的个人拥有哪些权利？ 他们可否撤回同意、反对保留（和/或要求删除）其个人数据？ 以及如果可以，该如何行使？

个人数据被收集的个人可以：

(a) 向各类组织发出合理通知后撤回同意，并且该各类组织（及其数据处理中介和代理人）必须停止收集、使用或披露其个人数据；

(b) 请求访问各类组织拥有或控制的个人数据，以及了解有关个人数据在此前一年内已经或可能已经使用或公开的方式；及

(c) 请求更正个人数据中的错误和遗漏。各类组织收到请求后必须更正，除非该组织确信有拒绝此类请求的合理理由，并有额外的义务将

更正后的数据发送给此前在回顾期(该期限范围是指各类组织接收到个人更正请求之日前一年之内)内收到错误数据的其他组织。

10. 如果违反任何个人信息保护法律，是否有任何处罚、责任或救济?

个人和组织都可能因违反 PDPA 而面临处罚。

11. 新加坡是否有强制性的数据泄露报告要求? 如果有，请总结触发报告的阈值、报告内容、报告的对象以及需要/预期的时间表?

是的。如果有理由相信发生了影响个人数据的数据泄露,各类组织必须评估该泄露是否需要通报。如果数据泄露对受影响的个人造成或可能造成重大损害,或者已经或可能构成重大规模,则应予以通报。重大损害的阈值与受到损害的个人数据的性质有关,而重大规模则根据受泄露影响的人数判断。

各类组织必须在评估应通报违规行为后三(3)日内发出通知。通知应包括数据泄露的事实、如何处理数据泄露的详细信息以及至少一名组织授权代表的联系方式。

除非存在例外情形或禁令,各类组织也需要向受影响的个人发出通知。在这种情况下,通知必须采用在当时情况下合理的任何方式。除了泄露事实之外,通知还应包括对受影响个人的潜在伤害、组织管理的详细信息,以及受影响个人可能采取保护自己的步骤的指导。

12. 新加坡近期在数据隐私/数据保护方面是否有显著的发展或可能会影响未来的案例? 还有其他需要强调的方面吗?

新加坡通讯及新闻部(Ministry of Communications and Information)最近宣布计划根据《个人数据保护法》发布《人工智能系统中使用个人数据的咨询指南》(Advisory Guidelines on the Use of Personal Data in AI Systems)。随着人工智能的日益普及,该指南将为如何在数据保护方面考虑人工智能领域的发展提供急需的明确指引。

斯里兰卡

律所

Neelakandan & Neelakandan

www.neelakandan.lk

联系人

Thishya Weragoda
斯里兰卡，科伦坡
电话： + 94 11 2371100
邮箱： thishya.weragoda@neelakandan.lk

Neelakandan & Neelakandan（前身为 Murugesu & Neelakandan）是斯里兰卡领先的、历史最悠久的提供全方位服务的律师事务所之一，已有 60 多年的执业历史。

该事务所受到世界多家知名品牌委托，保护其在斯里兰卡的知识产权，业务包括诉讼和起诉事项，并协助众多本地和外国客户完成大量商标、工业设计和专利的申请。该事务所还为由领先的本地和国际银行组成的银行集团提供有关各种基础设施项目融资安排的咨询服务。

该事务所的争议解决业务涵盖各领域的所有民商事诉讼和上诉程序。该事务所还精于处理国际仲裁和仲裁裁决的执行、海事和航运、诉前谈判等领域的法律事务。

该事务所就商业、公司和并购事务为国内外客户提供咨询服务。该事务所还处理一系列房地产和建筑交易工作以及国际航运事务，并拥有全面的劳动法业务。

1. 斯里兰卡主要的个人数据保护法律或法规有哪些？ 是否存在跨领域立法？ 跨领域立法与特定领域立法之间，何者将优先适用？

斯里兰卡保护个人数据的主要法律框架是 2022 年第 9 号文件《个人数据保护法》(Personal Data Protection Act, No. 9 of 2022)("**PDPA**")。该法规范了个人数据的处理、强化了个人对其个人信息的权利、建立了数据保护监管机构并完善了其他相关事项。

斯里兰卡还有专门立法为特定情形下的个人数据提供额外的保护，例如《计算机犯罪法》(2007 年第 24 号)(Computer Crime Act No.24 of 2007)、《电子交易法》(2006 年第 19 号)(Electronic Transactions Act No. 19 of 2006)、《信息权法》(2016 年第 12 号)(Right to Information Act No.12 of 2016)、《支付与结算系统法》(2005 年第 28 号)(Payment and Settlement Systems Act No.28 of 2005)、《银行法》(1988 年第 30 号)(Banking Act No.30 of 1988)、《电信法》(1991 年第 25 号)(Telecommunications Act No. 25 of 1991")和《知识产权法》(2003 年第 36 号)(Intellectual Property Act No.36 of 2003")。

尽管《计算机犯罪法》没有明确定义"数据"，但第 2 条规定了该法适用范围包括计算机、计算机系统和受此类行为影响的"信息"。此外，设施或服务，包括任何计算机存储或数据或信息处理服务，也受到该法条款的保护。

尽管斯里兰卡宪法并未明确承认隐私是一项基本权利，但第 14A 条强调了信息访问限制中的隐私问题。

此外，普通法也提供了有限的救济，因为其承认侵犯隐私是一种侵权行为。斯里兰卡法院也承认个人空间的权利。

2. 哪些监管机构负责个人信息保护法律的实施和执行？

数据保护管理局(Data Protection Authority)("**管理局**")是被授权执行 PDPA 的机构。

管理局有权自行决定在何种情况下允许对数据主体进行特定定位和监控。

《信息权法》(2016 年第 12 号)还规定了审查公共机构发布信息的框架,在该框架下信息官员有权决定是否发布或公开此类信息。该决定可由公众向指定官员(Designated Officer)提出上诉,针对该指定官员的决定又可以向信息权委员会(Right to Information Commission)提出质疑。

《支付与结算系统法》(2005 年第 28 号)还将中央银行收集的所有信息以及向其传输此类信息的任何第三方的信息列为保密信息。《银行法》(1988 年第 30 号)中也有类似的限制。

3. “个人信息”/“个人数据”是如何定义的,是否有任何类别的个人数据受到特殊或不同的保护(例如,员工、未成年人、“敏感”个人信息等)? 如果是,这些类别是什么? 能否简要说明适用于这些类别的特殊规则?

PDPA 第 56 条将“个人数据”定义为能够直接或间接识别个人身份的任何信息。这种识别可以通过姓名、身份证号码、财务细节、具体位置或在线识别符等方式确定。另外,个人数据也可以与个人的身体、生理、遗传、心理、经济、文化或社会身份等特定因素相关联。

受到特殊保护的个人数据包括披露种族或民族血统、政治观点、宗教或哲学信仰、基因数据处理、用于唯一识别个人身份的生物识别数据、健康相关信息、有关个人性生活或性取向的详细信息,有关刑事犯罪、法律诉讼和定罪的数据,以及与未成年人有关的数据。

若处理上述特殊类别的个人数据是向法院、仲裁法庭或其他司法机构提出、论证法律请求或对法律请求进行抗辩所必要的,则允许对这些特殊类别的个人数据进行合法处理。

基于罗马荷兰法原则的“妨害权利之诉”(actio injuriarum)作为普通法救济措施提供了更广泛的保护范围。在 2022 年 PDPA 颁布之前还没有任何相关法律,这一救济措施的适用在斯里兰卡还有进一步探索的空间。

4. 与个人数据相关的主要个人数据保护法律或法规的关键原则是什么?

PDPA 为政府机构、银行、电信公司和医疗机构等不同实体持有的个人数据制定了保护措施。其主要目的是在个人权利和各类组织的利

益之间取得平衡，确保数据处理程序的透明度并建立问责制。

该法将责任归于处理个人信息的个体（根据该法案分为控制者（Controllers）和处理者（Processors））。PDPA 第 5 条要求各类组织的数据处理行为具有有效的合法性基础。在合法性基础范围内，应确保数据的准确性和时效性、设置存储期限限制、保持透明度并维护个人信息的机密性。

5. 是否有适用于所有企业的正式注册合规要求（例如数据保护官员的任命、数据库登记等）？

PDPA 第 20 条要求在下列情形下，每个控制者指定或任命一名数据保护官（Data Protection Officer）（“**DPO**”）来确保其遵守 PDPA：

- 个人数据由部委、政府机构、部门或公共公司（不包括具有司法能力的司法机构）处理；或者
- 核心处理活动涉及：
  - 对数据主体进行定期和系统的监控；
  - 特殊类别的数据；
  - 有损害数据主体在 PDPA 下的权利的风险。

如果多个控制者是同一集团内的实体，则可以仅指定一个 DPO。作为控制者或处理者的公共机构可以根据机构间的层级关系为多个机构指定一个 DPO。DPO 联系方式必须公布在网站上。任命 DPO 后，必须立即告知监管机构。

6. 各类组织有哪些建立与个人数据处理、使用和披露相关的合规计划（例如法律政策和运营政策、合同等）的义务?

PDPA 第 4 条要求每个控制者或企业均应按照 PDPA 规定的义务处理个人数据。

控制者和处理者承担的义务包括：

（a）以合法方式处理个人数据（PDPA 第 5 条）；

(b) 明确个人数据处理的目的(PDPA 第 6 条);

(c) 对个人数据的处理仅限于既定目的(PDPA 第 7 条);

(d) 确保准确性(PDPA 第 8 条);

(e) 限制保存期限(PDPA 第 9 条);

(f) 保持诚信和保密(PDPA 第 10 条);

(g) 用透明的方式处理个人数据(PDPA 第 11 条);

(h) 实施内部控制和程序,以遵守 PDPA 中的义务(PDPA 第 12 条)。

PDPA 第 5 条规定了处理个人数据的合法性基础,包括获得数据主体的同意、履行合同、紧急情况、出于公共利益以及出于合法利益的需要。

7. 是否对将个人数据转移到其他法域有存在限制? 各类组织通常如何应对这些限制?

公共机构必须仅在斯里兰卡境内作为控制者或处理者处理个人数据,除非相关公共机构与所涉控制方/处理方和监管机构进行协商,根据部长做出的充分性决定,指定允许在第三国进行处理的特定类别的个人数据。

部长需要在 PDPA 相关章节的语境下评估第三国的法律和执行机制后做出充分性决定。其他的标准也可以纳入跨境数据流动的评估。充分性决定必须定期监测,并可由部长与管理局协商进行修改。

对于公共机构以外的各类组织,控制者或处理者可以在满足下列情况之一的情形下处理个人数据:

(a) 在充分性决定所指定的第三国;或

(b) 虽未被充分性决定所涵盖,但确保能够遵守 PDPA 相关章节中的义务的第三国。

为了满足上述(b)规定,控制者或处理者需要采用管理局指定的文书。此类文书须确保第三国的接收方承诺采取可执行的措施来保障数据主体依据 PDPA 享有的权利以及救济。

在缺乏充分决策和保障措施的情况下，各类组织仍然可以基于同意、合同义务、法定请求、公共利益、紧急情况或 PDPA 中提到的其他情形传输数据。

8. 是否存在对使用或重复使用个人数据进行数据分析/创新或采用人工智能或数据分析等新业务解决方案的限制？ 各类组织通常如何应对这些限制？

遵守 PDPA 第 9 条规定的限制保存期限的义务非常重要。

每个控制者只能在实现处理个人数据的目的所必需或所要求的期限内保存个人数据。PDPA 第 10 条规定，如果个人数据是出于公共利益、科学研究、历史研究或统计目的而进行存档，则控制者可以将个人数据保存更长时间。

9. 被收集个人数据的个人拥有哪些权利？ 他们可否撤回同意、反对保留（和/或要求删除）其个人数据？ 以及如果可以，该如何行使？

数据主体的以下权利受 PDPA 保护：

（a）知情权：

PDPA 第 11 条规定，控制者有义务提供 PDPA 附表 V（Schedule V）中提及的信息以及与所做的任何决定相关的信息。

（b）访问权：

PDPA 第 13 条规定，数据主体有权访问其个人数据并确认其个人数据是否已被处理。

（c）撤回同意权：

PDPA 第 14 条规定，数据主体有权随时撤回其对数据处理的同意。

（d）更正或补充权：

PDPA 第 15 条规定，数据主体有权请求控制者更正或完善其不准确或不完整的个人数据。

（e）删除权：

PDPA 第 16 条赋予数据主体删除其个人数据的权利。

(f) 不受自动化决策影响的权利：

PDPA 第 18 条赋予数据主体请求控制者审查仅基于自动化处理的决策的权利。

(g) 申诉权：

PDPA 第 19 条赋予数据主体针对控制者的某些决定向管理局提出申诉的权利。

可以。PDPA 第 14 条和第 16 条规定，数据主体有权在以下情况下通过书面请求删除其个人数据：

(a) 个人数据的处理违反了 PDPA 第 5、6、7、8、9、10 和 11 条规定的义务；

(b) 根据 PDPA 附表 I(Schedule I)的(a)项或附表 II(Schedule II)的(a)项，数据主体撤回作为处理依据的同意；

(c) 任何成文法或数据主体或控制者受到管辖的主管法院的命令要求删除个人数据。

10. 如果违反任何个人信息保护法律，是否有任何处罚、责任或救济?

是的。根据 PDPA 第 38 条，每次违规行为最高可处 1,000 万斯里兰卡卢比的罚款。屡犯者还可能需支付额外罚款，该罚款数额为第二次和随后每次违规的罚款金额的两倍。

11. 斯里兰卡是否有强制性的数据泄露报告要求? 如果有，请总结触发报告的阈值、报告内容、报告的对象以及需要/预期的时间表?

是的。根据 PDPA 第 23 条，数据控制者/处理者必须按照 PDPA 规定的形式、方式并在规定的时间内向管理局通报违规行为。

12. 斯里兰卡近期在数据隐私/数据保护方面是否有显著的发展或可能会影响未来的案例? 还有其他需要强调的方面吗?

无。

中国台湾

律所

寰瀛法律事务所

www.fblaw.com.tw/en/home

联系人

李立普
中国台湾，台北
电话： + 866 2 2705 8086
邮箱： lipolee@mail.fblaw.com.tw

寰瀛法律事务所成立于 1997 年，目前是台湾地区在知识产权法、反垄断与竞争法、数据保护、争议解决、房地产法和公司法领域的顶尖综合性法律事务所之一。我们一直本着诚信正直、专业负责、团队合作的信念与态度，为客户提供高品质的法律服务，深获客户的信任与肯定。我们的多位律师兼具台湾地区和外国司法管辖区的职业资格，深谙国际法律事务。寰瀛法律事务所与其他律师事务所，尤其是国际律师事务所的不同之处在于，我们的律师和顾问团队在了解国际法律事务的同时也接受了台湾地区的法律培训。因此，我们的团队熟悉台湾地区在文化和商业上的细微差别。我们结合国际知识和本土化理解，为跨国事务制定最合适的解决方案的业务模式深受国际客户认可。

1. 中国台湾主要的个人数据保护法律或法规有哪些？ 是否存在跨领域立法？ 跨领域立法与特定领域立法之间，何者将优先适用？

《个人资料保护法》(Personal Data Protection Act)("**PDPA**")是中国台湾主要的个人数据保护法律,该法是优先于其他本地法规和条例之上的跨领域数据保护立法。PDPA 是总体指导性的数据保护法,立法机关还授权行政部门制定不同的特定领域的数据保护规则,例如《金融监督管理委员会指定非公务机关个人资料档案安全维护办法》(Directions for Personal Data Safety Maintenance by the Financial Supervisory Commission Designated Non - Government Entity)等。

2. 哪些监管机构负责个人信息保护法律的实施和执行?

中国台湾立法机构于 2023 年 5 月通过了 PDPA 修正案,指定新的个人资料保护委员会(Personal Data Protection Commision)("**PDPC**")作为台湾地区个人数据保护的唯一主管机构。

3. "个人信息"/"个人数据"是如何定义的，是否有任何类别的个人数据受到特殊或不同的保护（例如，员工、未成年人、"敏感"个人信息等）？ 如果是，这些类别是什么？ 能否简要说明适用于这些类别的特殊规则?

根据 PDPA 第 2 条,个人信息("**个人资料**")是指"自然人之姓名、出生年月日、国民身份证统一编号、护照号码、特征、指纹、婚姻、家庭、教育、职业、病历、医疗、基因、性生活、健康检查、犯罪前科、联络方式、财务情况、社会活动及其他得以直接或间接方式识别该个人之资料"。第 6 条规定,病历、医疗、基因、性生活、健康检查及犯罪前科等属于敏感个人信息,除特殊情况外,禁止收集和处理。

4. 与个人数据相关的主要个人数据保护法律或法规的关键原则是什么?

台湾地区的 PDPA 并未详细说明合法性、公平性、合法性等关键原

则，但第五条概括性地规定“个人资料之收集、处理或利用，应尊重当事人之权益，依诚实及信用方法为之，不得逾越特定目的之必要范围，并应与收集之目的具有正当合理之关联。”

5. 是否有适用于所有企业的正式注册合规要求（例如数据保护官员的任命、数据库登记等）？

没有，台湾地区的 PDPA 目前没有适用于所有企业的形式注册合规要求。

6. 各类组织有哪些建立与个人数据处理、使用和披露相关的合规计划（例如法律政策和运营政策、合同等）的义务?

第 8 条、第 9 条规定了告知个人信息主体的义务，公务机关或非公务机关在收集个人信息时，应当明确告知信息主体下列信息：

（1）公务机关或非公务机关的名称；

（2）收集的目的；

（3）个人信息的类别；

（4）个人信息的使用期间、地区、对象和方式；

（5）个人信息主体根据 PDPA 第 3 条享有的权利以及行使此类权利的方法；以及

（6）如果个人信息主体选择不提供其个人信息，其权利和利益将受到影响。

仅在特定例外情况下才可以免除告知个人信息主体的义务，例如：

（1）法律授予豁免；

（2）公务机关执行法定职务或者非公务机关履行法定义务所必需的；

（3）告知将妨碍公务机关执行法定职务；

（4）告知将妨害公共利益；

(5) 个人信息主体明知告知内容;

(6) 收集个人信息是为了非营利目的,并且明显不会对个人信息主体产生不利影响;

(7) 个人资料已由个人信息主体自行公开或已合法公开;

(8) 不能向个人信息主体或其法定代理人进行告知;

(9) 基于公共利益为统计或学术研究所必需,但提供者处理或收集者披露的个人信息须无法识别特定数据主体;

(10) 大众传播企业为新闻报道的公共利益目的而收集的个人信息。

此外,第 5 条要求收集、处理、使用个人信息应当尊重个人信息主体权益,通过诚实信用的方式,不得超出特定目的的必要范围,并与收集目的有正当合理的关联。这些重要的一般性数据保护原应当通过准确告知数据主体并最终获得其同意的方式来落实(第 8 条)。

此外,台湾地区的 PDPA 要求持有个人信息档案的公务机关应指定专人落实安全维护措施,防止个人资料被窃取、窜改、损毁、灭失或泄露(第 18 条)。

对于非政府机构,也同样要求配备人员实施安全维护措施(第 27 条)。

7. 是否对将个人数据转移到其他法域有存在限制? 各类组织通常如何应对这些限制?

中国台湾的 PDPA 仅在四种情况下对非公务机关的跨境数据传输施加限制(第 21 条):

(1) 涉及国家重大利益的;

(2) 国际条约或协定特别规定的;

(3) 接收个人信息的国家缺乏完善的个人数据保护法规,个人信息主体的权益可能因此受到损害;

(4) 为规避 PDPA 而向第三国(地区)跨境传输个人数据的;

例如，当《苹果日报》于 2021 年年中突然宣布停刊时，台湾地区文化部依据第 21 条禁止将台湾地区《苹果日报》保留的个人信息转移至其中国香港的总部。

8. 是否存在对使用或重复使用个人数据进行数据分析/创新或采用人工智能或数据分析等新业务解决方案的限制？ 各类组织通常如何应对这些限制？

台湾地区的 PDPA 没有对将个人信息用于人工智能或创新数据分析的行为采取具体限制，但处理者必须遵循第 5 条中的一般规则。

9. 被收集个人数据的个人拥有哪些权利？ 他们可否撤回同意、反对保留（和/或要求删除）其个人数据？ 以及如果可以，该如何行使？

根据 PDPA 第 3 条，个人信息主体的权利包括：

（1）查阅和问询权（第 10 条）；

（2）数据可携权（第 14 条）；

（3）更正权（第 11 条）；

（4）限制和反对处理权（第 11 条）；

（5）删除权（第 11 条第 3、4 款）。

根据台湾地区 PDPA 第 20 条第 2 款及第 19 条第 2 款规定，信息收集者或处理者在知悉相关请求或收到个人信息主体的通知后，应主动或按照个人信息主体的要求，删除、停止处理或使用个人信息。由此可知，个人信息主体当然可以撤回其同意或反对对其个人信息进行收集或处理。

需要注意的是，就删除权而言，当收集数据的特定目的不复存在，相关存储期限已到期，或个人数据的收集、处理或使用违反 PDPA 时，公务机关或非公务机关应主动或应个人信息主体的要求，删除或停止处理或使用个人数据。

10. 如果违反任何个人信息保护法律，是否有任何处罚、责任或救济?

违反 PDPA 将导致承担民事责任(第 28 至 40 条)、刑事责任(第 41 至 46 条)和行政罚款(第 47 至 50 条)。因违反 PDPA 的行为而受害的个人信息主体还可以对侵权人提起集体诉讼(PDPA 第四章)。

我们关注到,两种最常见的违反 PDPA 的行为是:

(1) 未能进行告知或超出目的限制;

(2) 未实施合理的安全措施来保护数据。

实施这两种常见违法行为者将面临民事责任(第 28、29 条),刑事起诉(第 41 条)和行政罚款(第 47、48 条)。

例如,如一公司未经适当方式通知个人信息主体而非法收集他人病历,将违反第 6 条规定,可依据第 41 条进行起诉,处五年以下有期徒刑,并处新台币 100 万元罚金。此外,政府部门还可依据第 47 条规定处新台币 5 万元以上 50 万元以下罚款。该公司也需要承担因其违法行为造成损害的赔偿责任。

11. 中国台湾是否有强制性的数据泄露报告要求? 如果有,请总结触发报告的阈值、报告内容、报告的对象以及需要/预期的时间表?

第 12 条规定,因公务机关或非公务机关违反 PDPA 导致个人资料被窃取、泄露、篡改或以其他方式损害的,应当在查明相关事实后,通过适当方式通知个人信息主体。

12. 中国台湾近期在数据隐私/数据保护方面是否有显著的发展或可能会影响未来的案例? 还有其他需要强调的方面吗?

最近,随着欺诈行为和诈骗犯罪在台湾地区日益盛行,台湾地区公众对隐私权和数据保护的意识不断增强。台湾地区政府已采取行动,通过修订现行的 PDPA 来打击公共部门和私营公司侵犯隐私权的行为。新措施包括增加行政罚款以及设立新的 PDPC 作为台湾地区个人信息保护的唯一主管机构。

泰国

律所 **LawPlus Ltd.**

www.lawplusltd.com

联系人

Kowit Somwaiya
泰国，曼谷
电话： + 662 636 0662
邮箱： kowit.somwaiya@lawplusltd.com

LawPlus Ltd.是一家提供全方位服务的律师事务所。我们的首要目标是及时为客户提供优质、务实的法律咨询和协助，同时以合理的收费为客户的商业活动增加价值。我们利用我们的专业知识和对本地以及区域市场的了解来协助我们的本地和国际客户实现他们的业务目标。

我们的客户遍布各个行业，包括汽车、建筑、工程、食品和饮料、医疗保健、酒店、物流、信息和数字技术、电信、零售和批发、电子商务和社交媒体。

我们为客户提供国内和跨境商业交易、并购、外商直接投资、合资企业、治理和监管合规、破产和债务重组、公司注册和管理、就业和劳动保护、银行和证券、知识产权、贸易竞争、数据隐私、电信、媒体和技术、不动产、数字资产、仲裁、诉讼、继承和遗嘱认证等方面的法律服务。

LawPlus 已被 Legal 500 和许多其他法律服务排名出版物评为中高端梯队，并在多个执业领域获得推荐。

1. 泰国主要的个人数据保护法律或法规有哪些？ 是否存在跨领域立法？ 跨领域立法与特定领域立法之间，何者将优先适用？

泰国主要的个人数据保护立法是《个人数据保护法》BE.2562（2018 年）（Personal Data Protection Act B.E. 2562 (A.D. 2018)）（“**PDPA**”）以及个人数据保护委员会（Personal Data Protection Committee）（“**PDPC**”）根据 PDPA 颁布的 PDPA 实施和执行规则。PDPA 是一部跨领域立法，约束企业经营者和政府机构对个人数据的处理（包括收集、使用和披露）行为，除非存在可适用的特定领域立法，且特定领域立法的适用范围限于不与 PDPA 相冲突的部分。

2. 哪些监管机构负责个人信息保护法律的实施和执行？

PDPC 是负责实施和执行 PDPA 及其实施细则和条例的监管机构。PDPC 发布实施细则和条例，确立个人数据保护政策和方向，针对投诉进行调查，并向违反 PDPA 的数据控制者和数据处理者发出执行令。

PDPC 办公室（Office of PDPC）承担 PDPC 秘书处的职责。该办公室隶属于数字经济和社会部（Ministry of Digital Economy and Society）（“**MDES**”）。

一些特定领域的监管机构，例如与商业银行和其他金融机构有关的泰国银行（Bank of Thailand），也负责实施特定领域立法中个人数据保护相关的规定。

3. “个人信息”/“个人数据”是如何定义的，是否有任何类别的个人数据受到特殊或不同的保护（例如，员工、未成年人、“敏感”个人信息等）？ 如果是，这些类别是什么？ 能否简要说明适用于这些类别的特殊规则？

PDPA 规定，“个人数据是指与一个人有关的任何可以直接或间接地识别该人身份的信息，但不包括已故个人的信息。”

PDPA 处理两类个人数据：（1）一般个人数据，（2）敏感个人数据（“**敏感数据**”）。敏感数据是指“与种族、族裔、政治观点、迷信、宗教或哲学信仰、性行为、犯罪记录、健康数据、残疾、工会信息、遗传信息、生物识别数据或任何其他可能同等程度影响数据主体的数据。”

法律禁止在未经数据主体明确同意的情况下收集敏感数据，仅包含少数例外情况：例如在数据主体无法进行同意的情况下，为了防止或遏制对个人生命、身体或健康造成的危险而收集敏感数据，无论无法进行同意是出于何种原因。

收集 10 岁以下未成年人的个人数据需要获得对该未成年人负有监护责任者的同意。收集十周岁以上但不足法定婚龄或不具有完全民事行为能力的未成年人的个人信息，应当征得未成年人的同意，并征得对其负有监护责任者的同意。

4. 与个人数据相关的主要个人数据保护法律或法规的关键原则是什么？

（1）仅限于收集目的必需的范围收集个人数据。

（2）所收集的个人数据只能保留其使用目的所必需的期限。

（3）个人数据的处理必须通过确保个人数据的完整性和保密性的方式进行。

（4）必须充分承认数据主体对其被数据控制者或数据处理者收集的个人数据的访问权、更正权、反对处理权、删除权以及采取与被收集数据相关的其他行为的权利。

（5）个人数据泄露可能会导致行政罚款、刑事责任和民事责任。

5. 是否有适用于所有企业的正式注册合规要求（例如数据保护官员的任命、数据库登记等）？

没有适用于所有企业的正式注册合规要求。

任何处理大量敏感数据或处理大量个人数据的企业都必须任命一名

数据保护官(“**DPO**”),以确保遵守 PDPA 并充当数据主体和 PDPC 的联系人。

除非符合适用例外的情形,所有企业在收集、使用或披露个人数据之前或者将要收集、使用或披露之时,都必须获得数据主体的明确同意,并应保存获得同意的记录。

作为数据控制者或数据处理者的企业必须保留其数据处理活动的记录,以备 PDPC 检查或向 PDPC 提交。

6. 各类组织有哪些建立与个人数据处理、使用和披露相关的合规计划(例如法律政策和运营政策、合同等)的义务?

各类组织根据 PDPA 制定的关键合规计划如下:

(1) 该组织必须建立并维护完全符合 PDPA 数据处理要求的数据隐私政策。

(2) 数据控制者和数据处理者之间的数据处理协议或数据传输协议必须完全符合 PDPA 的相关要求。

(3) 当企业作为数据控制者开展任何高风险数据处理活动时,必须进行数据保护影响评估(“**DPIA**”),以识别数据隐私风险以及减轻此类风险的措施。

(4) 该组织必须建立保护和便于数据主体行使权利的机制,例如访问个人数据的权利,随时撤回同意的权利,纠正、删除、限制或反对处理个人数据的权利,数据可携权以及向 PDPC 办公室投诉的权利。

7. 是否对将个人数据转移到其他法域存在限制? 各类组织通常如何应对这些限制?

(1) 个人数据不得被传输至缺乏充分数据保护水平的法域或国际组织,除非相关数据主体在被告知目的地法域或目的地国际组织不具备充分数据保护水平后仍给予相关组织明确同意,或者传输个人数据是为履行根据传输方与目的地国家或国际组织的合同义务所必需的。

(2) 各类组织通过以下方式解决这些限制：(a) 就跨境数据传输获得数据主体的明确同意；(b) 确保在数据跨境传输时采取合同措施以维持同等数据保护标准，例如签署包含数据保护标准条款的数据传输协议。

(3) PDPC 鼓励相关组织实施一套内部约束性企业规则("**BCRs**")来管理其集团内的数据传输，以确保集团内的公司采用高标准的数据保护水平来管理其集团内的个人数据传输。

8. 是否存在对使用或重复使用个人数据进行数据分析/创新或采用人工智能或数据分析等新业务解决方案的限制？ 各类组织通常如何应对这些限制？

PDPA 不对使用自动化方式和非自动化方式处理个人数据(使用或重复使用)进行区分规制。

如果各类组织计划使用或重复使用个人数据进行数据分析、人工智能或创新，则应在收集个人数据时或之前向相关数据主体披露(在其隐私声明或同意请求中)此类处理情况。

9. 被收集个人数据的个人拥有哪些权利？ 他们可否撤回同意、反对保留（和/或要求删除）其个人数据？ 以及如果可以，该如何行使？

请参见上文第 6 问的第(4)项。数据控制者向数据主体发出的隐私声明必须列出数据主体所有的权利，并涵盖有关数据主体如何以及何时行使其权利的条款。

数据主体可以随时通过向数据控制者或数据处理者发出通知的方式行使撤回处理其个人数据同意的权利。

10. 如果违反任何个人信息保护法律，是否有任何处罚、责任或救济？

违反 PDPA 相关立法的数据控制者和数据处理者可能会：(1) 受到行政罚款，(2) 承担刑事责任，(3) 承担民事责任。

最高行政罚款额度为 500 万泰铢。

刑事处罚包括每次违规处以最高一年监禁和/或最高 100 万泰铢罚款。

民事责任是法院命令向受损害的数据主体支付的实际损害赔偿和惩罚性赔偿。

PDPC 或法院施加的处罚可能会有所不同，具体取决于违规的性质、严重程度和持续时间、受影响数据主体的数量以及违规者在违规发生时采取的补救措施。

11. 泰国是否有强制性的数据泄露报告要求？ 如果有，请总结触发报告的阈值、报告内容、报告的对象以及需要/预期的时间表？

如果发生可能对数据主体的权利和自由构成风险的数据泄露事件，数据控制者必须在发现泄露后 72 小时内向 PDPC 办公室报告泄露情况。报告必须包括数据泄露的性质、数据控制者联系人或 DPO 的详细信息、可能的后果以及为减轻潜在不利影响而已采取或将采取的措施。

如果数据泄露对数据主体的权利和自由构成高风险，数据控制者还必须立即将泄露情况通知受影响的数据主体。

12. 泰国近期在数据隐私/数据保护方面是否有显著的发展或可能会影响未来的案例？ 还有其他需要强调的方面吗？

PDPA 于 2022 年 6 月 1 日起全面生效。

截至 2023 年 6 月，PDPC 已发布 14 项有关个人数据处理（收集、使用和披露）、处理活动记录、个人数据泄露报告等的实施细则、规定和指南。

MDES、PDPC 和 PDPC 办公室以及私营部门一直在开展大量项目，以促进私营和公共部门的数字经济发展、网络安全和个人数据保护建设。

个人数据保护立法和实践是新兴的且仍在不断发展的。在泰国运营或与处理在泰国收集或从泰国传输个人数据的相关组织应密切关注泰国数据隐私立法的制定、实践和执行。

越南

律所

Russin & Vecchi

www.russinvecchi.com.vn

联系人

Viet T Le
越南，胡志明市
电话： + 84 28 3824 3026
邮箱： ltviet@russinvecchi.com.vn

50 多年前，Russin & Vecchi 律师事务所在亚洲成立，为新兴经济体提供服务。我们在俄罗斯、台湾地区、泰国、多米尼加共和国、纽约和其他地方设有多个关联但相互独立的办事处。

Russin & Vecchi 于 1966 年至 1975 年间在越南设有办事处，并于 1993 年重新开业，喜力啤酒（Heineken）是我们的第一个客户。我们在越南的历史是独一无二的。我们与越南有着紧密的联系并具备丰富的经验，自成立以来一直处在越南发展的最前沿。

我们的团队由 4 名合伙人和 20 名律师组成，在胡志明市和河内均设有办公室，多年来在浓厚的学院文化中团结在一起。作为越南历史最悠久的律师事务所，我们参与了许多开创性的交易，并出具开创性的解决方案。

1. 越南主要的个人数据保护法律或法规有哪些？ 是否存在跨领域立法？ 跨领域立法与特定领域立法之间，何者将优先适用？

在越南，隐私权和个人秘密是一项宪法权利。2023 年 7 月 1 日之前，众多立法文件中都规定了数据保护要求，包括《2015 年民法典》（2015 年 11 月 24 日）（Civil Code 2015（November 24, 2015））（“**Civil Code**”）和第 86/2015/QH13 号《网络信息安全法》（2015 年 11 月 19 日）（Law on Cyber Information Security No. 86/2015/QH13（November 19, 2015））（“**LCIS**”）。各领域立法中也包含有关数据保护的规定，例如第 51/2005/QH11 号《电子交易法》（2005 年 11 月 29 日）（Law on Electronic Transactions No.51/2005/QH11（November 29, 2005））和第 41/2009/QH12 号《电信法》（2009 年 11 月 23 日）（Law on Telecommunications No.41/2009/QH12（November 23, 2009）），以及各种其他具体领域立法。2023 年 4 月 17 日，政府颁布了关于保护个人数据的《第 13/2023/ND－CP 号法令》（Decree 13/2023/ND－CP）（“**Decree 13**”），该法令于 2023 年 7 月 1 日生效。Decree 13 是政府整合个人数据相关法规的第一步。

2. 哪些监管机构负责个人信息保护法律的实施和执行？

公安部（Ministry of Public Security）（“**MPS**”）是数据保护的监督机构。公安部网络安全和防范网络犯罪司（Department of Cybersecurity and Prevention of Cyber-Crimes under the MPS）（“**A05 Department**”）是为实施和执行包括 Decree 13 在内的数据保护法规而设立的专门工作组。

3. “个人信息”/“个人数据”是如何定义的，是否有任何类别的个人数据受到特殊或不同的保护（例如，员工、未成年人、“敏感”个人信息等）？ 如果是，这些类别是什么？ 能否简要说明适用于这些类别的特殊规则？

“个人数据”被定义为数字环境中与识别特定自然人或者与其他数据相结合时可用于识别特定自然人有关的符号、字母、数字、图形、音频或任何其他形式的信息。个人数据分为基本个人数据和敏感个人数

据。保护个人数据一般需要实施适当的技术和管理措施,以及制定和发布数据保护政策。另一方面,“敏感个人数据”的保护还需要设立数据保护部门并任命个人数据保护负责人(即数据保护官)。

4. 与个人数据相关的主要个人数据保护法律或法规的关键原则是什么?

Decree 13 规定的数据保护的主要原则可概括如下:

- 除非法律另有规定,否则必须告知数据主体处理活动的具体情况;
- 数据主体必须同意处理活动。同意必须是自愿的、具体的且可验证的。同意可以被撤回或有条件。在特定情况下,可以在未经同意的情况下处理数据。
- 必须在数据主体已被告知并同意的目的范围内处理个人数据;
- 只能在数据处理的范围和目的所必需条件下收集个人数据,除非法律另有规定,禁止以任何方式出售和购买个人数据;
- 所提供的个人数据必须准确、真实、完整,并适当更新和补充;
- 个人数据必须受到安全措施的保护;
- 个人数据仅在实现处理目的所必需的时间内保存。

5. 是否有适用于所有企业的正式注册合规要求(例如数据保护官员的任命、数据库登记等)?

根据 Decree 13,任何具备数据控制者或数据处理者资格的一方都必须准备、维护并向 A05 Department 提交个人数据处理影响评估(“**PDPIA**”)。PDPIA 不需要获得批准,但 MPS 的 A05 Department 可能会要求传输方提供额外的证明文件。数据控制者和数据处理者的 PDPIA 内容不同。PDPIA 必须在个人数据处理活动开始后 60 日内提交给 A05 Department。

PDPIA 必须包括以下内容:

- 数据控制者或数据处理者的信息和联系方式；
- 数据控制者数据保护部门和管理人员的姓名和联系方式；
- 个人数据处理活动的目的；
- 处理活动的描述(仅适用于数据处理者)和处理的个人数据类型；
- 个人数据的接收方，包括境外接收方；
- 个人数据的跨境转移(如有)；
- 数据处理活动的持续时间、删除或移除个人数据的潜在原因(如有)；
- 已实施的保护措施的描述；
- 评估个人数据处理活动的影响；以及
- 潜在的不良后果和补救措施。

6. 各类组织有哪些建立与个人数据处理、使用和披露相关的合规计划（例如法律政策和运营政策、合同等）的义务?

Decree 13 对参与处理个人数据的任何个人或实体制定和采用符合数据保护条例的个人数据保护政策提出了一般性要求。Decree 13 没有要求制定任何具体的政策或方案。另一方面，Decree 13 要求 PDPIA 涵盖对已实施的保护措施的说明，包括所有已制定和采取的政策。

7. 是否对将个人数据转移到其他法域存在限制? 各类组织通常如何应对这些限制?

根据 Decree 13，个人数据的传输被视为处理活动。因此，传输个人数据适用个人数据处理的一般要求。此外，向越南境外传输个人数据或使用离岸设施处理越南国民个人数据的实体或个人必须准备并保存一份数据传输影响评估（“**DTIA**”）。DTIA 必须在传输方开始处理个人数据后 60 日内提交给 A05 Department。传输完成后，传输方必须通知

A05 Department。DTIA 不需要获得批准,但 A05 Department 可能会要求传输方提供额外的证明文件。

DTIA 必须包括以下内容:

- 传输方和接收方的信息和联系方式;
- 直接传输和接收越南国民个人数据的实体或个人传输者的全名和联系方式;
- 传输后的处理活动的目的的描述与解释;
- 传输的数据类型的描述;
- Decree 13 合规性以及所采取的安全措施的描述;
- 数据处理活动的影响、潜在后果、补救和/或预防措施的评估;
- 数据主体的同意,包括数据主体在发生任何事件时做出回应或提出索赔的机制;
- 传输方和接收方之间具有约束力的文件,概述各方的权利、义务和责任。

8. 是否存在对使用或重复使用个人数据进行数据分析/创新或采用人工智能或数据分析等新业务解决方案的限制? 各类组织通常如何应对这些限制?

在使用或重复使用个人数据进行数据分析/创新或采用人工智能等新业务解决方案方面没有特殊限制,适用个人数据处理的一般要求。

9. 被收集个人数据的个人拥有哪些权利? 他们可否撤回同意、反对保留(和/或要求删除)其个人数据? 以及如果可以,该如何行使?

就 Decree 13 而言,被收集和处理数据的个人是数据主体。

数据主体拥有以下权利:

- 知晓收集、处理和使用其个人数据的方法、范围、地点和目的的权利；
- 访问或请求查询或编辑其个人数据的权利；
- 同意或撤回对其个人数据进行处理的同意的权利；
- 删除或要求删除其个人数据的权利；
- 反对或限制数据处理活动的权利；
- 要求数据控制者提供其个人数据的副本的权利；以及
- 要求损害赔偿、提起法律诉讼和采取自我保护措施的权利。

10. 如果违反任何个人信息保护法律，是否有任何处罚、责任或救济?

不遵守数据保护法律法规可能会导致行政处罚和刑事处罚。经第 14/2022/ND－CP 号法令（2022 年 1 月 27 日）（Decree 14/2022/ND－CP（January 27, 2022））修订的第 15/2020/ND－CP 号法令（2022 年 2 月 3 日）（Decree 15/2020/ND－CP （February 3, 2022））规定，行政处罚包括每次违规行为最高 7,000 万越南盾（约 2,961 美元）的罚款，具体数额由执法机构决定。如果违反有关个人电子邮件、信件、电话或其他形式通信的保密和安全规则，可能会受到刑事处罚。政府正在制定对违反个人数据保护规则的额外制裁措施，该措施可能将行政处罚最高值提高至违规实体在越南总收入的 5%。

11. 越南是否有强制性的数据泄露报告要求？ 如果有，请总结触发报告的阈值、报告内容、报告的对象以及需要/预期的时间表?

数据处理者在发现数据泄露后必须尽快通知数据控制者。数据处理者和控制者必须在数据泄露发生后 72 小时内通知 A05 Department。若 72 小时内未通知，必须作出解释。

通知必须包括以下内容：

- 对数据泄露的性质和范围的描述，包括但不限于发生时间、地点以及所牵涉各方的泄露数据和信息情况；
- 个人数据保护负责人的联系方式；
- 数据泄露后果或损害的描述；
- 为处理或补救数据泄露的后果或损害而采取的措施的描述。

12. 越南近期在数据隐私/数据保护方面是否有显著的发展或可能会影响未来的案例？ 还有其他需要强调的方面吗？

公安部将建立国家数据保护门户网站（National Portal on Data Protection）（“**门户网站**”），该门户网站将成为数据处理者和数据控制者提交报告、影响评估和通知的中心枢纽。该门户网站还将就当前和未来的数据保护法规提供进一步的指导。该门户网站预计将于 2023 年 7 月推出。

2022 年 8 月 15 日，政府发布了第 53/2022/ND－CP 号法令（2022 年 8 月 15 日）（（Decree 53/2022/ND－CP）（August 15, 2022））（“**Decree 53**”）。其中，Decree 53 对《网络安全法》（Law on Cybersecurity）提出的“数据本地化”和“强制性物理设施”要求提供了重要指导和阐释。

Decree 53 规定了以下“受监管数据”：

- 越南用户的个人数据；
- 越南用户创建的数据，包括账户名称、使用时间、信用卡信息、电子邮件地址、IP 地址、最近登出时间和注册电话号码；以及
- 有关越南用户与其朋友或与用户互动的其他人关系的数据。

根据 Decree 53，越南公司必须在越南存储上述受监管数据。若在越南开展业务的外国企业出现特定情况，包括其服务违反《网络安全法》，则将被要求在越南存储受监管数据并设立分支机构或代表处。

MERITAS®

www.meritas.org