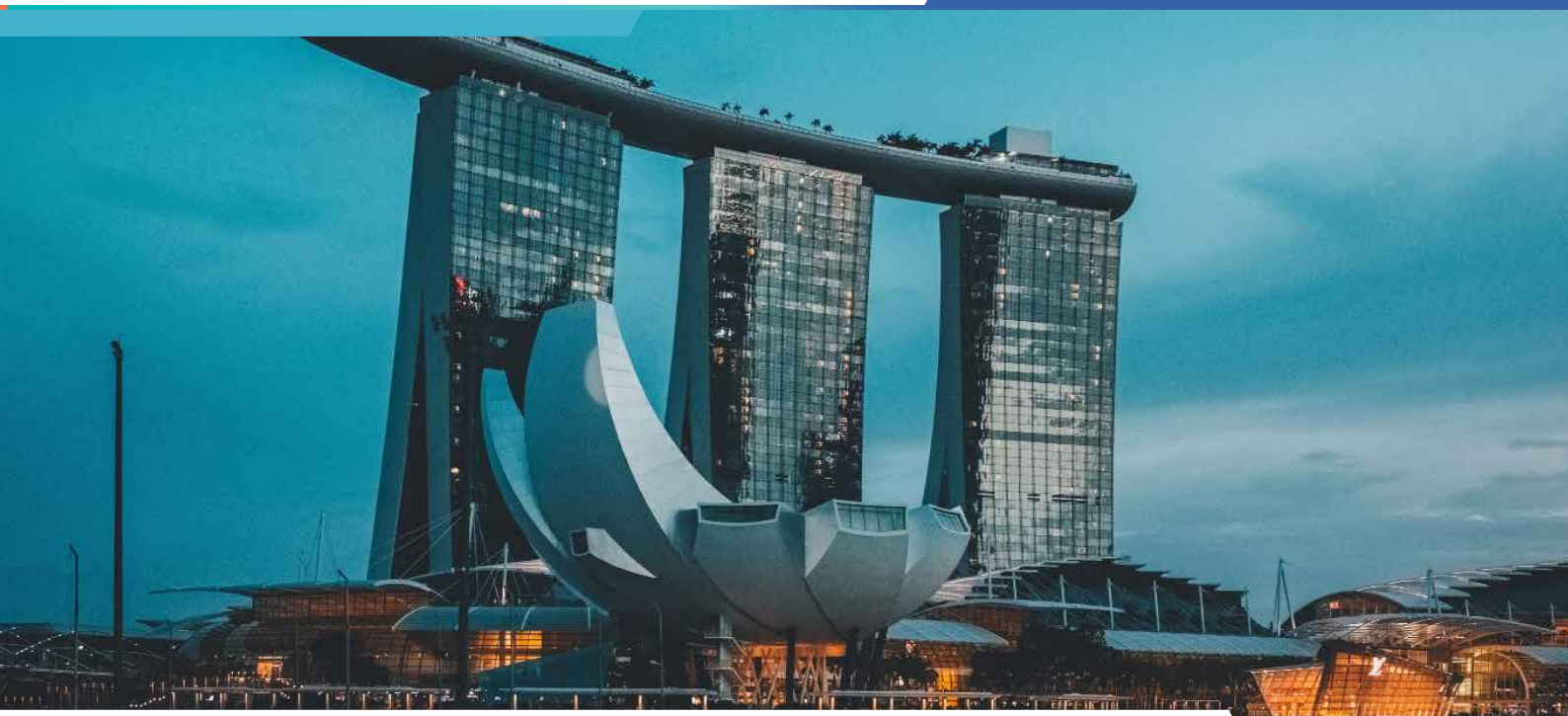
BIPO | Make Life Easier.



SINGAPORE

简述新加坡《个人资料保护法令》及其与欧盟GDPR的对比

Understanding Singapore’s Personal Data Protection Act (PDPA)

随着全球化以及电子商务和跨境贸易的兴起，大量的个人信息数据由于各种原因被第三方组织收集和使用。与世界上许多金融中心一样，新加坡也逐步采取各种保护个人信息数据的措施，承认个人保护个人信息数据的权利，包括查阅和更正个人资料的权利，以及各组织为合法和合理的目的收集、使用或披露个人信息数据的需求。

PDPA（Personal Data Protection Act）条款应运而生，此项条款详细规范了个人对于保护其个人信息数据的各项权利以及企业对于个人信息数据收集、利用或披露的规范。该法令的目的还在于加强和巩固新加坡作为可信的、世界级商业中心的竞争力和地位。以下为PDPA的详细解析：

1.新加坡《个人资料保护法令》

新加坡国民的个人信息数据受到2012年生效的PDPA的保护,此项条例分阶段生效。2013年1月2日，新加坡通讯及新闻部建立个人资料保护委员会及资料保护顾问委员会，分别负责对同一日生效的PDPA进行监管和建议。PDPA还规定建立全国性“谢绝来电”（Do Not Call “DNC”）登记处，于2014年1月2日生效。PDPA则于2014年7月2日生效。

条例承认了个人保护其个人资料的各项权利，包括个人对于其信息的获得权和修改权，同时也承认机构基于合法合理目的收集、利用或披露个人资料的需要。

大约在2018年同一时间，欧盟的《通用数据保护条例》（简称“GDPR”）也开始生效。

下表为PDPA与GDPR的对比：

概述	PDPA (新加坡)	GDPR (欧盟)
生效时间	“谢绝来电”登记处: 2014年1月2日 个人资料保护法令: 2014年7月2日	2018年5月25日

概述	PDPA (新加坡)	GDPR (欧盟)
条款的适用范围	几乎涵盖新加坡境内所有业务	适用于在欧盟境内外设立的任何组织，主要包括以下范围： - 该组织向在欧盟的个人提供货物或服务 - 对发生在欧洲范围内的数据主体的全部活动进行监控 - 本条例适用于在欧盟内部设立所有个人信息数据的行为，不论其实际数据处理行为是否在欧盟内部进行
条款简介	新加坡《个人信息保护条例（PDPA）》规定了组织在收集、使用和披露个人数据时所使用的方式需合理且恰当，同时也承认了个人有权保护其个人资料数据，且拥有对于个人数据的各项权利。	欧盟通用数据保护条例(GDPR)取代了曾经的欧盟数据保护指令（又称第95/46/EC号指令），旨在协调整个欧盟的数据保密法，保护所有欧盟公民的数据隐私并赋予其各项权利，并重塑各地区组织处理个人信息数据的方式。 更新的GDPR的目的是保护所有欧盟公民免受隐私和数据泄露的侵害，因为当今这个数据驱动的世界与1995年的指令制定时已经大不相同了。

2. 新加坡居民身份证号和其他国家身份证明信息在新加坡的使用规范

2019年9月1日起，所有组织只可在以下情况询问个人身份证明信息：

· 如有法律要求

或· 如有必要证明个人身份

其他国家身份证明信息通指出生证明号码、外国身份证号码和工作许可证号码等。

需要 使用新加坡身份证号的情况	不需使用新加坡身份证号的情况
✓新员工入职企业时	x 免费泊车赎回服务时
✓酒店入住登记时	x 加入任何零售会员俱乐部时
✓在诊所/医院求医时	x 注册任何服务或提交服务反馈时
✓申请移动电话号码套餐时	x 在线购买电影票时
✓报读私人教育机构时	x 参加抽奖活动时

3.PDPA与新加坡企业

在使用、收集或披露个人信息时，机构须遵守新加坡的《个人信息保护条例》，以下为《个人信息保护条例》下的九项义务：

1）同意义务

企业在收集、使用或披露个人信息时，必须先征得个人的同意,并且在个人给予合理的通知后，允许个人撤销同意。在撤销同意后，企业必须停止收集、使用和/或披露这些个人资料。

2）目的限制义务

企业只可收集、使用或披露个人同意的用途，这些个人数据只可被使用在适用于企业提供的产品或服务的合理范围内。

3）通知义务

企业必须在收集、使用或披露您的个人资料之前向个人解释收集个人资料的原因及使用目的和范围。

4）获取及修正义务

企业有义务要求并在合理可能的情况下尽快向个人提供关于：组织拥有或控制的个人资料详情以及在提出请求后一年内如何使用或披露这些个人资料。此外，如果个人要求企业纠正其个人资料中的任何错误或遗漏，企业必须在切实可行范围内尽快接受该要求。

5）缜密义务

企业需确保个人资料的准确性。

6) 保护义务

企业应制定必要的安全措施，以保护个人数据的拥有或控制是在安全范围内的。安全措施需要可以阻止任何未经授权的访问导致的个人数据被收集、使用和/或公开。

7) 保留限制义务

企业只可在法律或业务的所需的目的之下保留个人数据。

8) 转让限制义务

如果企业需要将个人数据转移到海外，例如将数据存储在云中，请确保将数据传送到的国家可提供与PDPA同等级别的数据保护。

9) 公开义务

企业应有权在要求个人信息数据时说明其有关数据保护的做法、政策和投诉流程的信息。例如企业的隐私政策，实体应至少委任一名数据保护专员负责确保该实体符合PDPA的相关规定，并可让希望了解更多企业的数据保护政策的个人可以与该数据保护专员进行联系，同时提供该专员的联系方式。

对于违反PDPA中的任何数据保护条款的企业，需要做到以下行为及可能受到以下处罚：

· 停止在违反该法的情况下继续收集、使用或披露个人数据；

· 销毁违反该法收集的个人数据；

· 向被侵害人提供个人数据的访问和纠正权限；

· 企业将面临最高100万新加坡元的处罚。

4. PDPA与新加坡雇员

以下列举了一些不同情况下，企业如何使用PDPA，以帮助企业和个人更好的了解PDPA如何在新加坡就业环境中的应用：

a) 企业是否需要征得求职者的同意才能收集和使用他的个人资料？

· 当个人以求职的形式自愿向某一企业提供其个人资料时，他们被视为同意该企业以评估其工作申请而收集、使用和披露这些个人资料。

· 当该个人被雇佣时，该企业继续使用工作申请表中提供的个人资料来管理与该个人的关系是合理的。

· 如果该企业希望将个人数据用于某些除上述情况以外的目的时，或在PDPA没有适用的例外情况下，则该组织须通知该个人并为此目的取得同意。

b) 企业能否保存未被雇佣的求职者的个人资料？

· 这些资料只可保存在以商业或法律为目的所需的时间内。

· 各企业还应注意到，求职者有权查阅并要求更正各企业持有的有关其的个人资料。

· 根据要求，企业还必须向个人通报过去一年内使用其个人信息数据的方式。

· 如果最终没有聘用此人，所涉个人信息数据是仅以评价为目的而保存的评论信息，则不要求各企业向个人提供此类信息。在这种情况下，企业不需要将在确定是否聘的过程中所产生的评价意见通知到个人。

c) 企业是否可以使用名片中的信息进行招聘？

· PDPA不适用于定义为个体业务联系信息的信息数据，包括：姓名、职位信息、工作电话或传真号、工作地址、工作电子邮件地址以及任何以个人目的而单独提供的有关个人的任何其他类似信息。

d) PDPA如何适用于雇员的雇佣纪录？

· 组织应告知雇员：信息收集的目的、需要使用和披露其个人资料的情况并在收集、使用和披露之前取得同意 。

· 在许多情况下，企业需要在关系开始时(任命新雇员时)获得收集、使用和披露员工的跟人信息数据的同意。在雇佣关系的不同阶段，当需要更多个人资料时，应再次取得雇员的同意。雇员可选择根据PDPA条款规定撤回他们的同意。

· 如果所收集、使用或披露的信息是以评价为目的而收集、使用或披露的，即(除其他事项外)确定个人是否适合就业、在就业中晋升或继续就业的目的、资格证书等，则无须经过个人的同意，例如：

- 从前雇主处获得一份推荐信，以确定是否合适。

- 获取业绩记录或其他相关信息，以确定雇员的业绩。

e) 以管理或终止企业与个人之间的雇佣关系为目的的收集、使用及披露个人资料的法律范围？

· 虽然雇员不需要表示同意，但雇主必须通知其雇员其收集、使用或披露个人信息数据的目的，但PDPA没有规定通知的形式和方式。

· 为避免产生疑问，企业应具备向员工提供提出收集、使用和披露数据的目的的一般通知（例如：性能评估），企业应在每次收集员工个人信息前提供相应通知。

· 属于“管理或终止雇佣关系”目的的个人信息数据范围：

- 利用雇员的银行账户信息对其发放工资
- 监察雇员在上班期间如何使用电脑网络资源及公司内部网络资源
- 管理工作人员福利计划（例如：培训/教育补贴）。

· 只要是有效或合法的目的情况下，企业可以继续保留关于前雇员的个人数据。但是，在没有明确界定的目的的情况下，不应保留个人数据信息。如果数据是在不确定的目的下和不确定的时间范围内，则会相应增加违反PDPA条例的风险。

f）如果员工不遵守PDPA，公司需要承担哪些“责任”？

· 企业对雇员在受雇期间所造成的任何违反行为负责。特别是，在该雇佣过程中由雇员从事的任何行为，不论其是否在此之前得到雇主的批准，均应由企业负责。

· PDPA对“雇员”的定义中包括志愿人员，对“雇佣”的定义中包括在无偿志愿工作关系下的工作。

5.信息储存安全与信息数据安全

PDPA也希望可以评估所有在新加坡的业务将如何存储、检索和保护个人信息数据(无论是为员工还是为其他专业目的)。

· 储存安全 — 不让未经授权的人员掌握私人信息，其中还包括保护数据免受网络攻击等。

· 数据安全 — 确保在停电、自然灾害等情况下仍有数据可用。

*这两个领域与数据保护密切相关，可能有重复部分。然而，从个别角度来看，在信息技术和网络安全生态系统中，每一种功能都是不同的。

作为一个企业，以下是一些需要考虑的领域：

· 个人数据存储是否储存在内部系统或云端（通过第三方供应商）？

· 数据存储是否在以下前提下：

(a)当前的IT基础架构是否支持

(b)有足够的安全和网络安全措施来防止数据被破坏

· 如果数据是通过第三方云端储存的，那么有什么安全措施?例如：每年进行独立渗透测试，ISO 27001 信息安全管理系统认证和其他相关认证等。

· 在停电的情况下，是否有适当的后备措施来检索和恢复“丢失的”数据。包括第三方云端提供的备份等措施。

· 在传输个人数据时，数据是否出于安全目的进行加密，它们是否符合相关的PDPA和/或GDPR策略?

· 其他内部措施：

- 进行风险评估，以确定信息安全安排是否适当
- 使用web应用防火墙
- 使用带有自动更新的反病毒软件
- 定期应用操作系统及软件的安全更新
- 定期审查用户访问情况

总之，各企业必须遵守“个人信息保护条例2012”的以下条例：

在PDPA于2014年7月2日生效之前收集的个人信息数据（原始收集的个人资料）可继续使用，除非个人已撤回同意。

如果在2014年7月2日之后获得的个人信息数据，企业须通知并获得收集、使用和披露的确认同意后方可使用个人信息数据。

关于BIPO

BIPO于2004年在上海创立，在新加坡设立亚太总部，研发中心分别设立在新加坡，上海，印度尼西亚，另外，BIPO同时也在香港、台湾、泰国、越南、印度、澳大利亚新西兰等国家和地区设立子公司，业务遍及亚太十多个国家和地区。

我们的服务产品包括人事代理、薪资外包、考勤自动化管理、劳动力精益管理、业务流程外包、差旅管理、弹性福利管理、外籍员工服务等等。除了人力资源服务，我们也提供行政和财务等相关的外包服务。

BIPO的优势在于通过BIPO HRMS“全模块”系统整合，实现云服务亚太地区“全覆盖”。

BIPO，作为亚太区服务网络最广，落地最深的一站式人力资源合作伙伴，提供创新高效的企业解决方案，助力提升企业效率，以“中国服务的探索者和实践者”为己任，致力于把“中国服务”推向世界！