PERSONAL DATA PROTECTION COMMISSION SINGAPORE

# 资料保护自查核对表

贵机构在保护个人资料方面做得怎么样？该自查核对表基于2012年《个人资料保护法令》中的9项个人资料保护义务，旨在帮助贵机构审查在个人资料保护方面的相关政策，并考虑如何很好地保护现有的个人资料。

请注意，《个人资料保护法令》中的个人资料保护规定（第三章到第六章）对以下情况不具有约束力：

- 以私人或家人身份行事的个人；
- 受雇期间行事的雇员；
- 代表某家公共机构进行与个人资料收集、使用或披露相关事宜的公共机构或公司；
- 业务联系的相关资料。指本人提供的、不只是专为私人用途的相关个人信息，包括个人姓名、职位或职务、商务用途的电话号码、公司地址、公司电邮地址、公司传真号码等其他信息。

贵机构可用以下问题和现有的做法做个对比。

## I-III. 同意、目的限定及通知义务

### 个人资料的收集

是 / 否
行动计划

**1** 贵机构目前是否收集客户或员工的个人资料？例如：

- 姓名
- 身份证号码 (NRIC) 或外籍人士准证号码 (FIN)
- 护照号码
- 个人照片或视频图像
- 手机号码
- 个人电邮地址
- 拇指纹
- DNA基因图谱
- 姓名和住宅地址
- 姓名和住宅电话

*个人资料是可以用来识别个人身份的资料（无论其是真是假），或者通过这些资料和该机构拥有的或可能获取的其它信息来识别个人身份的信息。*

**2** 贵机构是否有一份关于以下内容的个人资料库导图？

- 收集了哪些个人资料以及收集的原因是什么？
- 谁负责收集个人资料？
- 收集到的个人资料保存在哪里？
- 向谁披露收集到的个人资料？

*了解收集到的个人资料可能有助于贵机构确定和实施适当的个人资料保护政策。*

是 / 否
行动计划

3 收集个人资料时，贵机构是否会明确告知资料所属人收集、使用或披露的目的并取得他或她的同意?

4 从第三方收集个人资料时，贵机构是否确保第三方已经取得资料所属人的同意，为了预期的目的向贵机构披露他们的个人资料?

*通常情况下，在收集、使用或披露个人资料前，贵机构应首先确保第三方已经取得资料所属人的同意，同意为了贵机构预期的目的收集、使用和披露他们的个人资料。*

5 当贵机构聘用某家资料处理中介机构代表贵机构收集、使用或披露个人资料时， 您是否确保该中介机构将采取必要的行动，确保贵机构遵守《个人资料保护法令》?

*虽然资料处理中介机构可能只需要遵守资料保护和保留限制义务，但委托其处理个人资料事务的机构却需要遵守《个人资料保护法令》的所有规定。*

6 是否有一套正式流程让资料所属人撤销之前所做出的同意收集、使用或披露个人资料的决定?

*一旦撤销，需确保在一段合理的撤销程序期限后，不再收集、使用或披露资料所属人的个人资料。*

7 如果贵机构想在不获得同意的情况下收集个人资料，贵机构是否查阅过《个人资料保护法令》的第二附表与其他条文，以了解在何时可以不经同意就收集个人资料?

## 个人资料的使用

8 贵机构是否将收集到的个人资料只用于已获得资料所属人同意的目的?

9 对于《个人资料保护法令》生效前收集到的个人资料，贵机构在使用这些个人资料时，是否符合其当初收集资料的目的?

*对于《个人资料保护法令》生效前收集到的个人资料，如果符合其当初收集资料的目的，贵机构可继续使用收集到的资料，除非该个人已撤回了同意。如果贵机构想将这些个人资料用于其他目的，应首先取得资料所属人的同意。对于法令生效后收集的个人资料，贵机构应该告知并取得资料所属人的同意，才能收集、使用和披露他或她的个人资料。*

是 / 否
行动计划

10 如果想不经同意就使用个人资料，贵机构是否已经查阅过《个人资料保护法令》的第三附表与其他条文，以了解在何时可以不经同意就使用个人资料?

## 个人资料的披露

11 贵机构是否只出于资料所属人同意的目的披露收集到的个人资料?

12 如果想不经同意就披露个人资料，贵机构是否已经查阅过《个人资料保护法令》的第四附表与其他条文，以了解在何时可以不经同意就披露个人资料?

## IV. 查阅与修正义务

13 贵机构是否已经建立起一套用于处理查阅个人资料申请的正式流程?

*依据《个人资料保护法令》，个人可以申请查阅自己的个人资料。但需要遵守《个人资料保护法令》的有关禁令与例外规定。*

14 贵机构是否保存有一份名单，上面记录了曾向哪些第三方机构披露过个人资料，以及这样做的目的?

*贵机构在收到请求后应提供有关过去一年内实际或可能使用或披露的个人资料之使用目的与方式。*

15 如果贵机构向申请查阅个人资料的人士收取行政管理费，那么，贵机构是否已经制定好收费标准?

*请参见关于收取个人资料查阅管理费的相关规定。*

16 贵机构是否已经建立起一套用于处理个人资料修正申请的正式流程?

*资料所属人可能向贵机构提出申请，要求修正他们现有的个人资料中的错误或疏漏。收到此类申请后，贵机构应该尽快进行修正。除非《个人资料保护法令》有例外的规定或贵机构有合理的理由认定不应进行修正。*

是 / 否
行动计划

**17** 贵机构是否已经建立起一套正式流程，用于将修正后的最新个人资料发送给近一年内曾收过这些个人资料的第三方机构?

*通常情况下，如果进行了某处修正，贵机构应该将修正后的最新个人资料发送给近一年内曾接收过这些个人资料的第三方机构，除非该机构在业务和法律方面不需要这些修正后的资料。此外，在取得资料所属人同意的情况下，贵机构还可以将修正后的资料发送给指定的公司或机构（除非贵机构是一家信用局）。*

**18** 贵机构是否已经查阅过《个人资料保护法令》的S21(3)－(5)条规定及第五和第六附表，清楚在哪些情形下不需要提供个人资料的查阅及修正?

## V. 准确性义务

**19** 贵机构是否已经竭尽所能，(i)在使用资料作出任何影响个人的决定之前(ii)在披露之前，确保个人资料准确、完整?

*当个人资料可能被用于做出某项会影响到资料所属人的决定，或披露给其他机构时，贵机构有义务尽合理努力，确保收集到的个人资料准确、完整。*

## VI. 保护义务

**20** 贵机构是否已经对个人资料保护方面的内部风险进行过评估，并且已经实施了个人资料安全保护政策?

**21** 贵机构是否对收集到的个人资料进行了适当分类?

*确保员工、供应商和合作伙伴根据按需知密的原则获取信息是至关重要的。因此，应对个人资料进行适当分类并妥善保存，确保只有获得授权的人员才能查阅。*

**22** 个人资料的保存方式是否安全?

*应将个人资料（无论纸质形式还是电子形式）保存在贵机构可以安全掌控的地方，防止未经授权的人员擅自查阅、更改、披露、使用、复制、销毁或采取类似的行为。此外，贵机构还应分析安全隐患发生的可能性，并考虑可能发生的危险及漏洞。请参见我们网站上的电子平台个人资料保护指南（Guide on Securing Personal Data on Electronic Medium），了解信息与通信技术领域的常用知识，以及可以采取的相关安全措施。*

是 / 否
行动计划

**23** 外部机构是否可以轻易获得贵机构保存的个人资料?

*例如，要求客户或供应商填写的纸质记录在提交后应立即归档，以防其他人得到。有访客到访工作场所时，应安排专人陪同，并提前通知员工将个人资料收起来。*

**24** 当发生个人资料外泄事件时，是否有任何补救措施?

*应拟定一份补救方案，确定适当的措施、资源、职责和优先事项，用于应对个人资料外泄事件。请参见我们网站上的个人资料数据泄露管理指南，了解如何预防和应对个人资料外泄事件。*

**25** 贵机构是否定期在内部开展个人资料保护流程检查，或已制定个人资料保护流程定期检查计划?

**26** 当委托外包方代表贵机构处理个人资料事务时，贵机构是否与外包方签订了合同条款，以对披露给外包方的个人资料进行适当保护?

*确保外包方（资料处理中介机构）采取必要的行动，从而确保贵机构遵守《个人资料保护法令》。请参见第5条的注释。*

## VII. 保留限制义务

**27** 贵机构是否定期对个人资料进行维护?

*个人资料的保管期限不应超过业务或法律要求的必要期限。请根据业务和法律要求为各类个人资料规定明确的保管期限。*

**28** 贵机构是否会将业务或法律方面不再需要的个人资料进行删除?

*例如，应将包含个人资料的纸质记录粉碎或用其他方式安全销毁。应将电子资料彻底消除。也可以对个人资料进行匿名处理，从而确保任何人无法根据这些资料确定个人身份。*

## VIII. 传输限制义务

**29** 贵机构是否制定有适当的合同规定或企业约束规则，用于监管将个人资料传输到国外?

*禁止将任何个人资料传输到新加坡以外的国家或地区，除非贵机构可以确保这些国家或地区给予所传输资料的保护与《个人资料保护法令》提供的保护相一致。请参见将个人资料传输到国外的相关要求。*

## IX. 公开义务

是 / 否
行动计划

**30** 贵机构是否指定了一名或多名职员（可称为“资料保护负责人员”）负责确保贵机构的个人资料保护政策与实际操作符合《个人资料保护法令》的要求?

*小企业可以指定企业主或经理担任该角色。规模较大的公司机构可以指定某位管理层成员担任该角色，或专门指定一名具有必要的资历、权威和能力的资料保护负责人员。这些指定人员可以根据《个人资料保护法令》的相关规定将职责委托给公司内部的其他人员。*

**31** 贵机构的资料保护负责人员是否清楚其职责，并确保贵机构拥有或管理的个人资料得到充分保护?

**32** 贵机构指定的资料保护负责人员的业务联系信息是否对外公开?

*贵机构应该对外公开其个人资料保护政策和资料保护负责人员（或受委托负责该事宜的职员）的业务联系信息。*

**33** 贵机构是否已经制定并实施了个人资料保护政策，以遵守《个人资料保护法令》规定的义务? 贵机构的个人资料保护政策是否对外公开?

*请参见第32条的注释。*

**34** 贵机构是否已经制定了一套用于接收、调查和答复的流程来应对《个人资料保护法令》的实施而引起的投诉?

**35** 贵机构是否能应请求提供有关投诉处理流程的信息?

**36** 贵机构是否与员工沟通过关于个人资料保护政策与实际操作的信息，尤其是（但不限于）负责处理个人资料的员工?

*市场行销、电脑安全或数据库管理部门的员工可能需要接受专业培训，以确保其个人资料管理方法符合《个人资料保护法令》要求。*

**37** 贵机构的员工是否清楚，如果自己不是负责回复此类申请的人员时，应将这些申请转交给谁处理?

如果贵机构是一家资料处理中介机构*，请考虑以下问题。

## 资料处理中介机构

是 / 否
行动计划

**38** 当其他机构聘用贵机构作为资料处理中介代表其处理个人资料事务时，是否与贵机构签订了书面合同?

*按照《个人资料保护法令》中个人资料保护的相关规定，作为一家依照书面合同代表其他机构处理个人资料事务的资料处理中介，贵机构只需要遵守保护和保留限制义务。*

*资料处理中介机构是指代表其他机构处理个人资料事务的机构，但不代表其他机构中的雇员。

下面这部分内容将重点关注贵机构在“谢绝来电”条款下应遵守的义务。该 “谢绝来电”条款将与个人资料保护法令的规定同时实施。

## “谢绝来电”登记处

是 / 否
行动计划

**39** 是否贵机构促销清单上列出的个人都通过书面或其他有据可查的形式，明确表示同意贵机构可以出于电话营销的目的，通过电话、手机信息（例如短信/彩信）或传真联系他们?

*依据《个人资料保护法令》规定，“谢绝来电”条款一般禁止机构向已经注册过的新加坡电话号码（包括手机、固定电话、住宅电话和办公电话）发送特定促销信息。如果某些个人未通过书面或其他有据可查的形式，明确、清晰地表示同意贵机构向其手机发送促销信息，则贵机构在向他们发送促销信息之前，应首先核查有关“谢绝来电”登记处的信息。*

**40** 对那些未以书面或浅白易懂的语言形式，明确、清晰地表示同意贵机构向其电话号码发送促销信息的个人，贵机构是否已经建立起一套内部流程，用于在向他们发送促销信息之前，首先核查“谢绝来电”登记处号码?

*请参见第39条的注释。*

**41** 为了促销目的，从第三方购买个人联系信息数据库时，贵机构是否确保第三方已经取得必要同意，同意贵机构收集、使用和披露这些个人资料?

是 / 否
行动计划

## 42 当您拨打一个含有促销信息的语音电话时，贵机构是否会隐藏或禁止对方显示您的电话号码?

*当贵机构拨打（或委托第三方拨打）含有促销信息的语音电话时，请确保拨打者的识别信息（电话号码或能够让对方识别的其他信息）不会被隐藏。*

## 43 您的电话促销信息是否能清晰准确地来识别贵机构及联系方式?

*电话促销信息应能清楚地识别贵机构及联系方式。此外，这些信息还应在信息发出后的至少30天内有效，以使信息接收人在必要时可以联系贵机构进行确认或澄清。*

## 44 使用外包电话促销服务时，贵机构是否确保服务提供商遵守《个人资料保护法令》中关于“谢绝来电”条款的规定?

*无论是直接发送促销信息，还是委托第三方发送促销信息，贵机构均须确保不会向已经登记“谢绝来电”登记处的新加坡电话号码发送此类信息（除非该个人已通过书面或浅白易懂的语言形式，明确、清晰地表示同意贵机构向其电话号码发送促销信息）。*