PCPD HK
PCPD.org.hk
资料单张
香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

「自携装置」(BYOD)

摘要

「自携装置」是一项机构政策，容许雇员使用属于其个人的流动装置以查阅机构的资讯，当中包括机构所收集的个人资料。在本单张内，由机构收集所得的个人资料将统称为「机构收集的个人资料」。

机构应留意下述与个人资料私隐有关的事宜：

1. 在容许使用「自携装置」时，机构实际上是把机构收集的个人资料从具保安的企业系统转移至保安程度较低的雇员自携装置，且机构对该「自携装置」亦较难有效管控。机构必须要明白，尽管这些个人资料是储存在雇员本身所拥有的自携装置内，但就该些个人资料而言，机构仍须继续负责遵守《个人资料（私隐）条例》（「**条例**」）的规定。因此，机构应透过制定行政、实质及技术措施，来确保该些个人资料受到保障，并透过书面政策、通知及培训强化这些措施。

2. 在保护由「自携装置」器材转移或收集所得的个人资料时，机构须留意，该「自携装置」器材亦载有雇员本身、其家庭成员以至其他个别人士的私人资讯。任何机构所采取的保障措施亦应尊重这些私人资讯。

3. 为履行条例下的责任，机构应考虑：

   (a) 是否已充分提醒雇员不要滥用下载或储存于「自携装置」器材内的机构收集的个人资料；

   (b) 是否已有足够的技术措施，容许「自携装置」器材查阅或储存机构收集的个人资料的同时，亦能尊重私人资讯，例如：

      (i) 是否有其他方法代替将机构收集的个人资料直接储存到「自携装置」器材——资料可否储存于公司系统，只经由「自携装置」器材查阅（而非储存于「自携装置」器材内）？

      (ii) 是否备有有效的控制系统供查阅个人资料——雇员须以用户名称及密码登入后方可查阅机构的个人资料，使与其共用该「自携装置」器材的家人及其他人士无法查阅有关资料；及

      (iii) 是否有采取保安措施（包括独立加密），以保障经「自携装置」器材查阅或储存于「自携装置」器材的机构收集的个人资料，令未获授权人士查阅「自携装置」器材时只接触到已加密的个人资料。

4. 若机构计划容许使用「自携装置」，亦应考虑下述的良好行事方式：

   (a) 制定「自携装置」政策，详述其规管内容（例如机构与雇员的角色及责任、核准使用的程序等）；

   (b) 进行风险评估（例如决定如何落实「自携装置」政策及措施）；

   (c) 采用技术方案以减少或控制风险；及

   (d) 设立监察及检讨机制，以确保当业务上有任何改变时，「自携装置」政策仍行之有效。

引言

「自携装置」的做法在机构中越来越普遍。当雇员使用属于其个人的流动装置(例如智能电话及平板电脑)来查阅雇主的公司资讯以执行职务,这些资讯便会从具保安的企业系统转移至保安程度较低的雇员自携装置。本单张重点指出机构在制定「自携装置」政策时所须留意的个人资料私隐风险,并建议就容许雇员以「自携装置」器材查阅载有个人资料的企业系统以执行职务时的最佳行事方式。

基于「自携装置」器材的不同特点,亦涉及处理不同种类的机构资讯,加上资讯及通讯科技的急速发展,本单张所指出的议题及措施未必放诸四海皆准,因此读者须因应个别的「自携装置」器材及其使用方式来考虑本单张内容的适用性。

由于本单张主要集中于个人资料私隐范畴的保障,因此有关使用个别「自携装置」的资讯科技保安详情,读者应参阅相关的技术或业界指引。

「自携装置」与条例

除了本单张指出的具体风险及控制措施外,使用「自携装置」储存或处理个人资料的机构亦应了解六项保障资料原则[1]及其他规定。

机构可能已根据条例及六项保障资料原则的规定,就保障个人资料私隐制定一般政策;但把个人资料转移及保留于「自携装置」器材,会对有关资料构成特定的私隐风险,例如:资料由具保安的企业系统被转移至「自携装置」器材会带来资料保安的风险。儘管这些个人资料是储存于由雇员所拥有的装置内,但就该个人资料而言,机构仍有责任遵守条例的规定。如果机构要遥距管理雇员的「自携装置」器材或在器材遗失时追踪其位置,雇员储存于「自携装置」器材的私人资讯便会「反向」传到机构的系统。此举对雇员的个人资料私隐构成风险,而就这些个人资料而言,机构亦是完全有责任遵守条例的规定。

大体来说,「自携装置」的做法会对保障资料原则有下述影响:

(a) 保留及删除资料(第2原则)

机构须确定是否应该把个人资料保留在「自携装置」器材内。如要这样做,机构须确定保留及删除资料政策是否同样适用于这些保留在「自携装置」器材内的个人资料,以及这些政策如何有效地应用,例如延伸有关政策以涵盖「自携装置」器材内的资料。

(b) 控制个人资料的转移及其后的使用(第3原则)

机构应就雇员如何查阅及使用机构收集的个人资料制定足够的控制措施。资料使用的政策应同样适用于机构的器材及个人的「自携装置」器材。如机构收集的个人资料可被转移至及/或保留于「自携装置」器材,那么相比于中央储存的资料,机构对于雇员如何查阅或使用储存于「自携装置」器材内的资料会有较少的控制。机构因而需要提醒雇员,并制定政策及控制措施(如适用),以确保雇员在未取得资料当事人的同意前不能把有关的个人资料用于新目的。

(c) 保障已转移至并保留于「自携装置」器材的个人资料(第4原则)

机构对保障所收集的个人资料的保安政策,应同样适用于转移至并保留于「自携装置」器材的资料。

鑑于「自携装置」器材在设计或使用方式上可能并不安全[2],在没有额外保障措施下使用「自携装置」器材,未必能符合第4原则下的保安规定。

若实行有关「自携装置」器材的保安措施时,没有同时考虑雇员的个人资料私隐,或会引起公司及雇员之间的衝突。例如,机构为了保障「自携装置」器材内的个人资料,或希望能遥距查阅「自携装置」器材以追踪其位置或确保器材中没有安装未

[1] 请参阅 www.pcpd.org.hk/tc_chi/data_privacy_law/6_data_protection_principles/principles.html

[2] 很多智能电话在製造时未有考虑保安问题。即使有,亦可能因被用户「越狱」而停止了保障功能。

经准许的应用程式(「**程式**」)。但这些安排让机构可查阅到雇员在「自携装置」器材储存的私人资讯,因而可能侵犯雇员的个人资料私隐。

因此,为抵御因「自携装置」器材遗失或被入侵[3]所引致的风险,机构应采取保安措施以保障「自携装置」器材内的个人资料,而不是利用现行用于保障机构中普遍使用的流动器材的工具(例如流动装置管理 Mobile Device Management)来保障或监察「自携装置」器材。因此在实际执行上,需要结合下述方法:

1. 避免在「自携装置」器材储存机构收集的个人资料;

2. 控制查阅储存于「自携装置」器材的个人资料(例如在使用屏幕锁之外,再使用专属的用户名称及密码);及

3. 把储存于「自携装置」器材的个人资料加密,但要采用非由「自携装置」随器材附属的加密方法,而且须与个人资料的敏感程度匹配。

这些方法会在本单张「最佳行事方式」部分阐述。

(d) 查阅及改正保留于「自携装置」器材的资料的权利(第6原则)

不论个人资料是保留于机构的中央系统或于「自携装置」器材内,个人查阅及改正其个人资料的权利都是一样。因此,机构需要确保在查阅及改正个人资料方面是否仍能履行其责任,尤其是在个人资料只保留于「自携装置」器材的情况下。故此,机构应考虑采取措施,把储存于「自携装置」器材的机构资料备份至由机构控制的地方储存。

最佳行事方式

机构应考虑下述做法,以确保使用「自携装置」的方式符合保障个人资料的规定。

(a) 制定「自携装置」政策

机构必须制定「自携装置」政策,详列有关:

1. 机构及雇员在「自携装置」措施上分别担当的角色、责任及职责;

2. 机构决定「自携装置」器材可查阅的资讯及程式的准则,以及决定哪类「自携装置」器材可获允许使用的准则,例如器材的种类、作业系统及其他技术标准;

3. 用以保障属于机构及雇员的个人资料的技术解决方案,例如不容许经「自携装置」器材查阅的个人资料被储存到器材中;或者当有关资料被储存到「自携装置」器材时,必须把资料与其他程式分隔(例如透过「沙盒」技术)或加密;及

4. 机构监察雇员遵从「自携装置」政策及措施的机制,及不遵从的后果。

(b) 进行风险评估

机构应进行风险评估,以确定「自携装置」器材可查阅或储存的个人资料种类,及资料遗失或被未经准许而披露所造成的伤害及可能性。机构应根据风险评估的结果及其技术能力,检讨和决定各类「自携装置」器材可查阅的个人资料种类,及制定相应的存取控制和保安措施保障资料。

由于雇员的「自携装置」器材可能载有不少有关自己、家人及其他人士的个人资料,如没有合理理由或在雇员不知情下查阅、监察或删除雇员在「自携装置」器材内的个人资料,会导致雇佣关系不和。因此,风险评估须兼顾对机构的资料(包括机构收集的个人资料)与雇员的个人资料的私隐影响。

如机构欠缺技术能力去妥善评估风险或确保在「自携装置」政策实行时个人资料获得足够保障,便应寻求外部协助。不过机构须谨记,承办商或许有责任就「自携装置」提供保障个人资料的设计及程序,但若然承办商导致或作出任何侵犯私隐的

[3] 被入侵的器材包括被「越狱」的智能电话或植入恶意软件的装置。

情况[4]，机构仍须为此负上责任。因此，机构须确保其承办商符合它指明的保安规定。有关详情，可参阅《外判个人资料的处理予资料处理者》[5]资料单张。

(c) 采用技术解决方案

机构可于「自携装置」器材利用控制软件或程式，保护转移至器材的个人资料及提高器材的保安。这些软件或程式可遥距清除「自携装置」器材上的资料，或将「自携装置」器材锁上，又或追踪其实际位置、侦测是否被「越狱」或植入恶意程式，甚至追查曾浏览的网站。此外，机构亦可以採取措施，使器材在连续多次被输入不正确密码后封锁登入，或自动删除器材内的资料。由于这些保障措施涉及向机构交出「自携装置」器材的某些控制功能，雇员或会担心在工作期间及下班后均被监察，以及暴露其个人资料。因此，在採取上述保障措施前，机构应非常清晰地向其雇员传达，在「自携装置」相关的保障个人资料政策中他们的权利和责任[6]。另外，机构可考虑（如适合）让其雇员控制这些措施。例如，雇员可拥有自己的帐户，以找出、清除或寻找自己的「自携装置」器材。不过，在容许这做法之前，机构必须知道，雇员可能因而成为操控著删除「自携装置」器材内的资料的人。机构因此应考虑採取适当的备份措施。

下述技术功能可保障机构及雇员的个人资料私隐。基于这些功能的技术性质，机构可能需要就是否及需如何落实这些功能向资讯科技人员徵询意见：

1. 除了「自携装置」器材的预设屏幕锁外，机构应额外加设独立的密码或存取控制，以保护储存于器材内的机构收集的个人资料。专用密码、双重认证、休眠模式及其他提升的保安控制的措施，可防止雇员的家人或其他人士（他们可能共同使用或可接触有关「自携装置」器材）查阅有关资料。此外，机构可能需要安装软件以加强雇员採用的密码，或发出指引要求雇员只可採用复杂的密码；

2. 机构收集的个人资料储存于「自携装置」器材时，应以其他方式妥善地加密，而不是採用由器材本身附属的加密方式，如此即使资料遗失或器材被入侵，取得资料的人也难以使用资料；

3. 机构收集的个人资料在传出及传入「自携装置」器材时，应妥善地验证及加密，令其不能被未获授权人士截取，例如当「自携装置」器材连接上不安全的Wi-Fi网络，可能会把通讯内容转移至假冒的伺服器；及

4. 如机构收集的个人资料敏感程度高并且已经备份，机构可在「自携装置」器材安装自动删除资料功能，作为预防措施。例如当「自携装置」器材因遗失而没有在预定时间内连接机构的伺服器，或出现多次尝试登入器材的情况，器材的自动删除资料功能可防止资料外洩。

(d) 监察及检讨

由于资讯及通讯科技器材面对很多威胁，亦会有漏洞，因此容许「自携装置」的机构必须定期检讨和更新其政策及措施，监察其符规情况。机构应因应科技发展或业务改变而完善及修订其保障政策，亦应定期评估储存于「自携装置」器材内个人资料的性质及/或敏感程度的转变，从而对政策作出相应修订。

---

[4] 根据条例第65(2)条，任何作为另一人的代理人并获该另一人授权的人所作出的任何作为或所从事的任何行为，须视为亦是由该另一人作出或从事的。

[5] 请参阅 www.pcpd.org.hk/tc_chi/resources_centre/publications/files/dataprocessors_c.pdf

[6] 关于电子监察雇员的详情，机构应参阅《保障个人资料私隐指引：雇主监察雇员工作须知》www.pcpd.org.hk/tc_chi/data_privacy_law/code_of_practices/files/Monitoring_and_Personal_Data_Privacy_At_Work_revis_Chi.pdf

PCPD.org.hk

查询热线 ： (852) 2827 2827
传真 ： (852) 2877 7026
地址 ： 香港湾仔皇后大道东248号阳光中心12楼
电邮 ： enquiry@pcpd.org.hk

免责声明

本刊物所载的资讯和建议只作一般参考用途，并非为《个人资料（私隐）条例》（下称「条例」）的应用提供详尽指引。有关法例的详细及明确内容，请直接参阅条例的本文。个人资料私隐专员（下称「私隐专员」）并没有就本刊物内所载的资讯和建议的准确性或个别目的或使用的适用性作出明示或隐含保证。相关资讯和建议不会影响私隐专员在条例下获赋予的职能及权力。

二零一六年八月初版