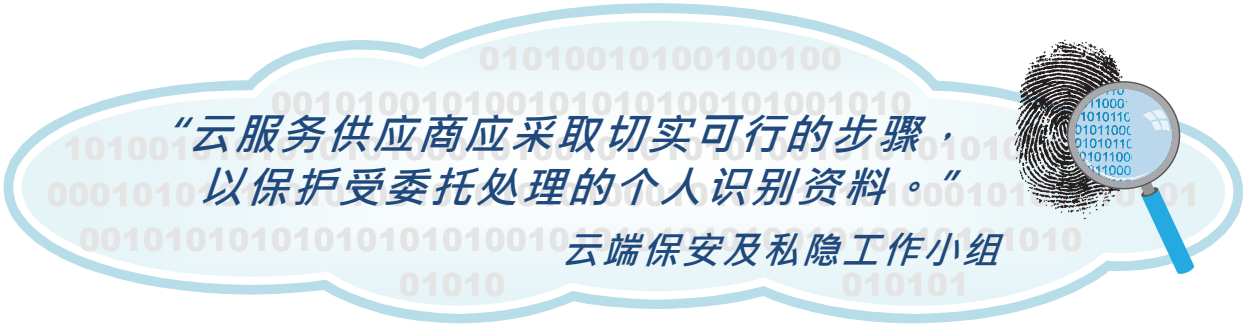
云服务供应商
在云上处理个人识别资料的信息安全及私隐保障备忘事项



目的

云计算服务透过减少成本、增加弹性及缩短推出应用程序和服务所需的时间，为信息技术带来变革。这些服务可能涉及收集、储存、处理或使用个人识别资料，一旦没有采用适当防护措施，便有可能出现安全风险及私隐问题。本文件载列了有关信息安全及私隐保障备忘事项，以供云服务供应商在云上处理个人识别资料时参考。

目标对象

本文件的主要目标对象是云服务供应商。云服务供应商以云计算技术为基础向用户提供信息技术服务，而有关服务会涉及收集、储存和处理个人识别资料。有关服务可能是由云服务供应商基于「软件即服务」、「平台即服务」或「基础设施即服务」而直接提供的解决方案，也可能是按用户需要根据以上三类服务的不同组合而建立的解决方案。

讨论范围

香港制订《个人资料（私隐）条例》（第 486 章）（下称《条例》），以保障在世人士的「个人资料」私隐。个人资料包括任何直接或间接与一名在世人士（资料当事人）有关的资料、可切实用以确定有关人士身分的资料，以及其存在形式令查阅或处理均是切实可行的资料。《条例》适用于任何控制个人资料的收集、持有、处理或使用的人士（资料使用者）。当一个资料使用者外判个人资料处理工作予另一人（资料处理者）时，该资料使用者须遵守额外的法定责任[1]。

就《条例》而言，当云服务供应商为本身的目的而收集、持有、处理或使用个人资料，便可视作资料使用者。当供应商并非为了本身的目的而代表另一人处理个人资料，便可视作资料处理者。

单凭个人识别资料很多时不足以识别某一个人的身分。但个人识别资料加上其他资料，便可组成用以识别某人身分的个人资料。本文的讨论范围并不限于个人资料的严格涵义，从而推动为个人识别资料以至个人资料提供充分保护。在下文各段，「个人识别资料」及「个人资料」两词均会使用；但在特别参照《条例》而订定的备忘事项，则使用「个人资料」一词。

云服务供应商
在云上处理个人识别资料的信息安全及私隐保障备忘事项

信息安全及私隐保障对云服务供应商有甚么影响？

在云服务的业务中，保护客户的资料及私隐是十分重要的工作，也逐渐成为企业成功的关键因素。对云服务供应商而言，显示有能力保护受委托处理的个人识别资料，便可得到客户的信任及信心。相反的话，可能削弱客户的忠诚度、产生负面的宣传效果、失去潜在商机及导致法律诉讼。

云服务供应商应该注意甚么？

云服务供应商应该采取切实可行的步骤，以确保受委托处理的个人识别资料一直受到保护，免遭在未获授权或无意的情况下被查阅、改动、处理、删除或作其他用途。很多时候，保护个人识别资料跟保护其他资料相似，包括保护资料的机密性、完整性及可用性。本文件所载的备忘事项，提供建议在云保护个人识别资料所采取的良好作业模式。云服务供应商可视乎本身作为资料处理者或资料使用者的身分以作参考。该备忘事项未必能尽錄所有项目。云服务供应商应经常检查本身的风险状况，并采取最适合的安全措施。

《个人资料（私隐）条例》实用指南

如需要更多有关处理个人资料的指引，云服务供应商可参考由香港电脑学会出版的《IT管理层及专业人员「个人资料（私隐）条例」实用指南》[2]。

备忘事项的引言

在云计算上，资料处理设施不再完全由资料使用者拥有，令资料规管的角色和责任有所改变。本备忘事项阐述在云上处理个人识别资料的保护措施。

使用云计算平台及其服务并非把保护资料的责任转移给云服务供应商。当收集个人识别资料时，收集者控制了有关资料的生命周期，并须负责履行《个人资料（私隐）条例》所订明的责任。

词汇

本备忘事项所采用的词汇与《个人资料(私隐)条例》保持一致。

词汇	定义	例子*
资料当事人	指一名在世人士，其个人资料正在处理中。	信用卡申请人是资料当事人。
资料使用者	指拥有从资料当事人收集得来的资料的一个实体。该实体在数据的整个生命周期内，负责保护收集得来的资料。	发卡银行是资料使用者。
资料处理者	指在收集、处理或储存个人识别资料时向资料使用者提供服务或产品的一个实体。	发卡银行选用的数据中心营办商是资料处理者。

** 使用处理信用卡申请个案作为例子*

备忘事项

下表列出当涉及个人识别资料时，在信息安全及私隐保障方面的良好作业模式。本列表为云服务供应商提供高层次的指引，以供在推行管理、运作及技术措施时参考使用。

保护个人识别资料的良好作业模式	云服务供应商担任资料使用者的角色	云服务供应商担任资料处理者的角色
政策管理		
遵守《个人资料（私隐）条例》，特别是保障资料原则[3]。	✓	✓
了解及遵从收集和储存个人识别资料所在的司法管辖区所适用的私隐法例，因为云可能超越香港特别行政区的司法管辖权范围。	✓	✓
进行私隐影响评估[4]，以助识别及侦测任何对私隐造成的风险，包括在云上收集及储存的个人识别资料，在未获授权或无意的情况下被查阅、修改、处理、删除或作出其他用途。	✓	✓
在机构内部制订及执行清晰的保护资料或私隐保障政策，以符合收集、处理及储存个人识别资料所在的司法管辖区的个人资料私隐法例。	✓	✓
定期进行风险评估及检讨，以确保有关安全风险受到妥善管理。	✓	✓
制订妥善的合约条款(或至少评估合约条款的需要)，以规管有关保护个人识别资料的行为。	✓	✓
收集（保障资料第1原则）		
以公平和合法的方式收集个人资料，而这些资料只可作与云服务功能和活动直接相关的用途。	✓	
只可在有实际需要时收集个人资料。所收集的资料不应超越原有收集的目的。	✓	
每当在网上收集个人识别资料时，必须向有关人士提供收集个人资料声明。	✓	
通知客户有关其个人资料会作何种用途，以及该等资料可能转移予何人。	✓	

保护个人识别资料的良好作业模式	云服务供应商担任资料使用者的角色	云服务供应商担任资料处理者的角色
保留及准确性（保障资料第 2 原则）		
保持个人资料准确、适时更新和稳妥，而保留期不应超过实际需要。	✓	
客户所交托的个人资料的保留期不应超过实际需要。		✓
使用及处理（保障资料第 3 原则）		
须先征求和取得客户的同意，才可将他们的个人资料作资料收集目的以外的用途。	✓	
切勿将客户交托的个人资料作任何未经客户同意的用途。		✓
安全防护 - 程序和步骤（保障资料第 4 原则）		
记录储存于云上的个人识别资料的种类。	✓	
编制一份储存了个人识别资料的软件系统及位置清单，以助有效地进行监察。	✓	
避免把个人识别资料储存于过多不同的应用程序及位置，因此举可能增加安全风险，并会加重监察及侦测未获授权查阅资料方面的工作。	✓	✓
订出一份认可计算机设备清单，包括可用以管理云端操作的移动设备及其相应的安全要求。	✓	✓
制订有关申请及审批资料查阅权的正式程序及详细步骤。	✓	✓
制订快速应变通讯方法以处理安全事故(包括怀疑被入侵的事故)。	✓	✓
定期覆检计算机/网络设备的记录和审计追踪记录，以检查是否存在异常情况和可能出现的攻击。	✓	✓
透过持续监察及安全保证覆检，不断改善资料保护措施。	✓	✓

保护个人识别资料的良好作业模式	云服务供应商担任资料使用者的角色	云服务供应商担任资料处理者的角色
安全防护 - 技术措施（保障资料第 4 原则）		
为个人识别资料加密或提供加密功能，让客户为其储存在云上的个人识别资料加密。无论在甚么情况下加密，都要小心保护加密密钥。	✓	✓
为透过开放网络传输的个人识别资料加密。	✓	✓
应用或提供严格的认证方法，例如双重认证，确保客户通过认证才可查阅云上的个人识别资料。	✓	✓
在网络通讯闸安装保安装置，例如防火墙、入侵侦测/防御系统，以保护云服务免受外来攻击。		✓
确保计算机设备： • 已安装防病毒软件及最新的计算机病毒定义档案，启动实时侦测功能和对系统进行定期全面扫描；以及 • 使用中的操作系统及软件已安装最新安全修补程式。		✓
定期检查系统安全漏洞，在切实可行情况下尽快实行补救措施。		✓
定时进行资料备份及测试资料复原程式。	✓	✓
计算机设备内的个人识别资料未被完全删除之前，禁止重用或弃置该计算机设备。		✓
遵行规定（保障资料第 5 原则）		
可以透过私隐政策声明，告知客户在保护其个人资料上所作出的承诺及推行的相关措施。	✓	✓
查阅与改正（保障资料第 6 原则）		
开发及利用记录管理系统以处理客户查阅及改正个人资料的要求。	✓	

保护个人识别资料的良好作业模式	云服务供应商担任资料使用者的角色	云服务供应商担任资料处理者的角色
分判商的管理		
只有在提供所需服务的情况下，才可以把客户的个人识别资料向分判商披露。分判商不得使用个人识别资料作任何其他用途。	✓	✓
对于处理储存在云上的个人识别资料的分判商或任何第三方，规定他们须制订适切的信息技术安全机制及相关程序。	✓	✓
监察所有可查阅储存于云上的个人识别资料的分判商，并备存一份载列该等分判商的清单。	✓	✓
员工管理		
就储存在云上的个人识别资料而言，应订明员工在资源控制上所担任的工作和职责。例如，指定一名管理人员负责执行决策，授权查阅储存在云上的个人识别资料。	✓	✓
指派员工处理储存在云上的个人识别资料及采用职务分工原则。	✓	✓
制订严格的密码政策及确保员工没有共用帐户。	✓	✓
根据个别员工的职责，定期覆检他们的查阅权限，以确定或重新确定其是否适合进行查阅。例如，当机构内某名员工离职或调任到机构的其他单位，该员的所有查阅权限及帐户必须予以撤销。	✓	✓
向负责处理储存在云上的个人识别资料的员工提供充足的指导及培训。	✓	✓

参考资料

1. 参考 http://www.pcpd.org.hk/chinese/publications/files/dataprocessors_c.pdf
有关个人资料私隐专员公署出版的《外判个人资料的处理予资料处理者》资料单张
2. 参考 http://www.hkcs.org.hk/en_hk/home/publication/PDPO/
有关个人资料私隐专员公署出版的《IT 管理层及专业人员「个人资料（私隐）条例」实用指南》
3. 参考 http://www.pcpd.org.hk/chinese/ordinance/ordglance1.html#dataprotect
有关《个人资料(私隐)条例》的保障资料原则
4. 参考 http://www.pcpd.org.hk/chinese/publications/files/PIAleaflet_c.pdf
有关个人资料私隐专员公署出版的《私隐影响评估》资料单张

如需要进一步资料，请浏览我们的网站：
www.infocloud.gov.hk

「云资讯网」是一站式入门网站，由云端运算服务和标准专家小组建立，方便市民和企业（特别是中小企）有效取得有关云计算技术的信息和资源。該網站提供用例、相关指引和良好作业模式，让市民和企业在采用云计算模式时达到预期效益。

云端运算服务和标准专家小组由香港特区政府属下的政府资讯科技总监办公室成立，透过广纳业界、学术界、专业团体及政府的专业知识，推动香港云计算的应用和发展，以及促进本港云计算专家彼此交流及与内地专家互相交流。云端保安及私隐工作小组是一个在专家小组辖下设立的工作小组。

此文件由云端保安及私隐工作小组发表，载述了有关云安全及私隐的良好作业模式和指引。工作小组成员透过通力合作，制订有关措施，以推动并促进本地业界，更广泛应用云计算和安全使用云服务。