SECURITY & PRIVACY CHECKLIST FOR CLOUD SERVICE PROVIDERS IN HANDLING PERSONAL IDENTIFIABLE INFORMATION IN CLOUD PLATFORMS

Purpose

Cloud computing services are transforming IT by reducing costs, increasing flexibility and improving time to delivery of applications and services. These services, which could involve the collection, storage, processing or use of personal identifiable information (PII), may be exposed to security risks and privacy issues if measures are not properly in place. This document provides a security and privacy checklist for cloud service providers when handling PII in a cloud platform.

Target Audience

The key target audience of this document is cloud service providers that provide IT services to users based on cloud computing technology, where the services will involve the collection, storing and processing of PII. The service may be a solution directly provided by cloud service providers, based on SaaS (Software as a Service), PaaS (Platform as a Service) or IaaS (Infrastructure as a Service) or it may be a custom-built solution integrating various components of SaaS, PaaS and IaaS.

Scope of Discussion

In Hong Kong, the Personal Data (Privacy) Ordinance (Cap. 486) ("PD(P)O") is in place to protect the privacy interests of living individuals in relation to "personal data". Personal Data covers any data relating directly or indirectly to a living individual (data subject), from which it is practicable to ascertain the identity of the individual and which is in a form where access or processing is practicable. The PD(P)O applies to any person (data user) that controls the collection, holding, processing or use of personal data. When a data user outsources the processing of personal data to another person (data processor), there will be additional statutory obligations on the data user[1].

When a cloud service provider (the provider) collects, holds, processes or uses the personal data for the provider's own purposes, then the provider can be considered as a data user with respect to the PD(P)O. When the provider processes personal data on behalf of another person, and does not process the data for the provider's own purposes, then the provider can be considered as a data processor.

Very often, PII alone may not be sufficient to make an identification of a particular person. PII may however be combined with other information to compose personal data that could identify persons. This document intends to cover discussion beyond personal data in the strict sense, and in turn to drive sufficient data protection on PII and hence personal data. Both the terms PII and personal data will be used in the later sections of this document. When a checklist item is specifically making reference to the PD(P)O, the term "personal data" will be used.

How Does Security & Privacy Concern Cloud Service Providers?

In the cloud service business, protection of customer data and privacy is a critical function and has increasingly become a key determinant of business success. Cloud service providers that demonstrate an ability to protect the PII entrusted to them can gain the trust and confidence from their customers. Failure to do so can lead to an erosion of customer loyalty, negative publicity, loss of potential business and legal proceedings.

What Cloud Service Providers should be aware of?

Cloud service providers should take practicable steps to ensure PII entrusted to them remains at all times protected against unauthorized or accidental access, alteration, processing, erasure or other use. In many cases, protection of PII is similar to protection of other data and includes protecting the confidentiality, integrity, and availability of the information. A checklist recommending the best practices for protecting PII in cloud platforms is provided for reference by cloud service providers, based on their roles as data processors and data users respectively. The checklist is by no means exhaustive. Cloud service providers should always examine their own risk profile and implement the most appropriate security measures.

Practical Guide on PD(P)O

For more detailed guidelines in handling personal data, cloud service providers can make reference to the publication titled "A Practical Guide for IT Managers and Professionals on the Personal Data (Privacy) Ordinance"[2] published by the Hong Kong Computer Society.

Introduction to the Checklist

Cloud computing brings changes to the role and responsibilities on data governance when the data processing facilities are no longer fully owned by the data user. This checklist focuses on protection of personal identifiable information (PII) when processing PII on a cloud platform.

Using a cloud computing platform and service does not transfer the data protection responsibility to a cloud service provider. When PII data is collected, the collector is in control of the lifecycle of the PII data and responsible for meeting the obligations defined in the Personal Data (Privacy) Ordinance.

Terminology

The terminology adopted in this checklist aligns with the Personal Data (Privacy) Ordinance.

Term	Definition	Example*
Data Subject	Refers to a living individual, whose personal data is being processed.	The credit card applicant is the data subject.
Data User	Refers to the entity which owns the data collected from the Data Subject. This entity is responsible for the protection of the collected data throughout its entire data lifecycle.	The credit card issuing bank is the data user.
Data Processor	Refers to the entity which provides services or products to Data User when, collecting, processing or storing PII.	The data centre operator selected by the card issuing bank is the data processor.

** Using credit card application process as an example*

The Checklist

The table below provides a list of security and privacy protection best practises when PII is involved. This table provides high level guidance for cloud service providers to consider when implementing management, operational and technical measures.

Best Practises on Protecting PII	Cloud Service Provider assuming the role of Data User	Cloud Service Provider assuming the role of Data Processor
Policy Management		
Observe the Personal Data (Privacy) Ordinance, in particular the Data Protection Principles (DPP) [3].	✓	✓
Understand and comply with the privacy laws applicable under the jurisdiction of the location where the PII is collected and stored, as the cloud environment may extend beyond HKSAR.	✓	✓
Conduct a Privacy Impact Analysis (PIA)[4] which helps identify and detect any privacy risks associated with unauthorized or accidental access, alteration, processing, erasure or other use of PII collected and stored in cloud platforms.	✓	✓
Establish and enforce a clear data protection or privacy policy within the organization in compliance with the personal data privacy law in the jurisdiction of the location where the PII is collected, processed and stored.	✓	✓
Conduct a periodic risk assessment and periodic review to ensure security risks are properly managed.	✓	✓
Establish proper contractual terms (or at least evaluate the need for contractual terms) to govern conduct in protecting PII.	✓	✓
Collection (DPP1)		
Collect personal data by fair and lawful means and only for purposes that are directly related to the functions and activities of the cloud service.	✓	
Collect personal data only when there is an actual need, and such data collection should not be excessive with respect to the intended purpose.	✓	
Provide a Personal Information Collection (PIC) statement whenever PII is collected on-line from individuals.	✓	
Inform customers the purposes for which their personal data are used and to whom that data may be transferred.	✓	

Best Practises on Protecting PII	Cloud Service Provider assuming the role of Data User	Cloud Service Provider assuming the role of Data Processor
Retention & Accuracy (DPP2)		
Keep personal data accurate, up-to-date, secure and for no longer than necessary.	✓	
Retain personal data entrusted by clients no longer than is necessary.		✓
Use & Processing (DPP3)		
Ask for and obtain consent before customer's personal data are used for purposes other than the purposes for which they were collected.	✓	
Do not make use of personal data entrusted by client for any of the purposes not consented by the client.		✓
Security Protection - Processes and Procedures (DPP4)		
Keep records of what type of PII is stored in the cloud.	✓	
Compile a list of applications and locations in which PII will be stored to facilitate effective monitoring.	✓	
Avoid storing PII in too many different applications and locations which may increase the risk of security exposures as well as efforts in monitoring and detection of unauthorized access.	✓	✓
Define a list of authorized computer equipment including mobile devices that can be used for administering cloud operations and their corresponding security requirements.	✓	✓
Establish a formal process and step-by-step procedures for requesting and approving access rights.	✓	✓
Establish rapid response protocols to deal with security incidents including suspicion of intrusion.	✓	✓
Review logs and audit trails on computer / network equipment for anomalies and possible attacks periodically.	✓	✓
Keep continuous improvement in data protection through ongoing monitoring and assurance reviews.	✓	✓

Best Practises on Protecting PII	Cloud Service Provider assuming the role of Data User	Cloud Service Provider assuming the role of Data Processor
Security Protection - Technical Measures (DPP4)		
Encrypt PII or provide an encryption function for customers to encrypt their PII stored in the cloud. In all cases protect the encryption keys with great care.	✓	✓
Encrypt PII when being transmitted over an open network.	✓	✓
Apply or provide strong authentication method, such as two-factor authentication, for customers to access PII on the cloud.	✓	✓
Implement security mechanisms, such as firewall, intrusion detection/prevention systems, at the network gateway for protecting the cloud services against external attacks.		✓
Ensure that computer equipment are installed with – • anti-virus software with the latest virus definition files, real time detection feature enabled and a periodic full scan scheduled; and • latest security patches of the installed operating system and software.		✓
Conduct regular scans for system vulnerabilities and apply remedial actions as soon as practically feasible.		✓
Conduct regular backup with periodic testing of data recovery.	✓	✓
Prohibit the re-use or disposal of computer equipment without having the stored PII completely sanitized.		✓
Compliance (DPP5)		
Inform customers of the commitment and relevant measures made to the protection of their personal data. This could be in the form of a Privacy Policy Statement.	✓	✓
Access & Correction (DPP6)		
Develop and make use of a log subsystem to handle access and correction requests of personal data from clients.	✓	

Best Practises on Protecting PII	Cloud Service Provider assuming the role of Data User	Cloud Service Provider assuming the role of Data Processor
Subcontractors' Management		
Disclose PII of customers to subcontractors only for the purpose of delivering the required services. Prohibit subcontractors from using PII for any other purpose.	✓	✓
Require subcontractors or any third parties that handle PII stored in the cloud platforms to have sufficient IT security mechanisms and associated procedures.	✓	✓
Keep an inventory of and monitor all subcontractors having access to the stored PII in cloud platforms.	✓	✓
Staff Management		
Define roles and responsibilities on resource control for PII stored in the cloud platform. For example, designate an administrator responsible for implementing management decisions to grant access to PII stored in the cloud platform.	✓	✓
Assign staff for handling PII stored in the cloud platforms and also apply the principle of segregation of duties.	✓	✓
Establish strong password policy and ensure no shared account is used.	✓	✓
Conduct periodic review of staff access permissions to establish or re-establish eligibility, based on individuals' work responsibilities. For example, revoke all access and accounts of a staff that had left the organization or transferred to other unit of the organization.	✓	✓
Provide adequate education and training to staff handling PII stored in the cloud platform.	✓	✓

References

1. Refer http://www.pcpd.org.hk/english/publications/files/dataprocessors_e.pdf on the leaflet "Outsourcing the Processing of Personal Data to Data Processors" published by the Office of the Privacy Commissioner for Personal Data
2. Refer http://www.hkcs.org.hk/en_hk/home/publication/PDPO/ on the guide "A Practical Guide for IT Managers and Professionals on the Personal Data (Privacy) Ordinance" published by Hong Kong Computer Society
3. Refer http://www.pcpd.org.hk/english/ordinance/ordglance1.html#dataprotect on the data protection principles of the PDPO
4. Refer http://www.pcpd.org.hk/english/publications/files/PIAleaflet_e.pdf on the leaflet "Information Leaflet on Privacy Impact Analysis" published by the Office of the Privacy Commissioner for Personal Data

FOR FURTHER INFORMATION, PLEASE VISIT OUR WEBSITE:

www.infocloud.gov.hk

InfoCloud website is established by the Expert Group on Cloud Computing Services and Standards. It serves as a one-stop portal for the general public and enterprises (especially SMEs) to effectively access information and resources on cloud computing technologies. The website provides sample use cases, guidelines and best practices for achieving the desired benefits in adopting the cloud computing model.

The Office of the Government Chief Information Officer of the HKSAR Government established the Expert Group with an aim to draw expertise from the industry, academia, professional bodies and the Government to drive cloud computing adoption and deployment in Hong Kong, as well as facilitate exchanges among cloud experts both within Hong Kong and with the Mainland. Working Group on Cloud Security and Privacy is one of the working groups set up under the Expert Group.

This document is one of its series of best practices and guidelines on cloud security and privacy published by the Working Group on Cloud Security and Privacy. With the collaborative efforts from members of the Working Group, deliverables are developed with a view to facilitating and promoting wider adoption of cloud computing and secure use of cloud services in local industry.