Privacy Impact Assessment (PIA)

Service White Paper

PIA Introduction

Privacy Impact Assessment (PIA) is generally regarded as a systematic risk assessment tool that can be integrated into the decision-making process.This is a systematic process to assess the impact of a project on personal data privacy with a view to avoiding or minimizing adverse impacts. All departments of Hong Kong Special Administrative Region Government, enterprises and institutions in Hong Kong must comply with the Personal Data (Privacy) Ordinance (Cap. 486) and conduct PIA, when personal data is collected, stored, used and processed and when major privacy issues are involved.

Why is PIA useful?

PIA systematically identifies potential privacy risks in personal data processing, provides forward-looking guidance to organizations, and clarifies the compliance measures that need to be deployed as a priority, thereby building targeted protection mechanisms before major resource

PIA helps organizations demonstrate compliance with relevant privacy and data protection requirements during privacy audits or compliance investigations.

PIA can enhance informed decision-making, expose internal privacy management loopholes,and help customers proactively identify hidden dangers and avoid external audits or passive responses

Suggested Scenarios

A PIA offers data users an "early warning" by identifying and detecting any privacy problems associated with the project before it is implemented. Any organization, public or private sector data user concerned about privacy should conduct a PIA to manage the privacy risks arising from projects involving:

- Processing (whether by the data user itself or by an agent appointed by the data user) or the building up of a massive amount of personal data
- The implementation of privacy-intrusive technologies that might affect a large number of individuals
- A major change in the organisational practices that may result in expanding the amount and scope of personal data to be collected, processed, or shared

About 6DDP

Six data protection principles (6DDP) from PCPD is applied for data processing cycle analysis.

DPP1	Collection Purpose & Means
DPP2	Accuracy & Retention
DPP3	Use
DDP4	Security
DDP5	Openness
DDP6	Data Access & Correction

PIA service process

As a professional service team deeply engaged in the field of data compliance and cyber security in Hong Kong, we strictly abide by the Personal Data (Privacy) Ordinance (Cap. 486) and the Six Data Protection Principles to help clients reduce data compliance risks.

1 Data Processing Cycle Analysis

2 Privacy Risk Analysis

3 Avoiding or mitigating privacy risks

4 PIA Reporting

How we work?

We adopt a phased and efficient operation mode, and for customers who require the assessment timeliness, the whole process of assessment can be completed within 8 working days at the earliest.

Data collection(1-3days)

- □ Fill out the PIA Basic
- □ Sign the project

Onsite/remote assessment (3-5 days)

- □ Compliance interviews
- □ Verify actual data processing flow
- □ PIA Testing

Report delivery (4-7 days)

- □ Submitting the PIA Report

How you support us in PIA?

- Sign the project authorization agreement
- Fill out the PIA Questionnaire
- Assign a dedicated staff for contact
- Provide necessary information, i.e., data flow diagrams, privacy policy text, system architecture and technical description documents,etc.
- Related system usage support

Output

The PIA report mainly includes the following three parts

1 Recognized Risk

2 Dispose Suggestion

3 Compliance Conclusion

Shenzhen Open Source Cybersecurity Services Company Limited

Email: mareketing@scssec.com

Website: www.scssec-hk.com

Address: Room 2901, Huafeng Building, No. 6006 Shennan Road,
Futian District, Shenzhen

Copyright Statement and Confidentiality Agreement