香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

Information Leaflet

Privacy Impact Assessments (PIA)

What is a PIA?

A PIA is generally regarded as a systematic risk assessment tool that can be usefully integrated into a decision-making process. It is a systematic process that evaluates a proposal in term of its impact upon personal data privacy with the objective of avoiding or minimizing adverse impacts. Although PIA is not expressly provided for under the Personal Data (Privacy) Ordinance ("the Ordinance"), it has become a widespread privacy compliance tool and data users are advised to adopt it before the launch of any new business initiative or project that might have significant impacts on personal data privacy.

This information leaflet provides information on the PIA process and its general application for data users' reference.

Why undertake a PIA

A PIA offers data users an "early warning" in identifying and detecting any privacy problems associated with the project before it is implemented. It should be undertaken by data users in the public and the private sectors to manage the privacy risks arising from a project that involves:

- significant processing or the building up of massive personal data;
- the implementation of privacy intrusive technologies that might affect large number of individuals; or
- a major change in the organizational practices that may result in expanding the amount and scope of personal data to be collected, processed or shared

For instance, before the Hong Kong Government introduced the SMART identity cards in 2003, four PIAs were undertaken to examine and address the personal data privacy issues. PIA is also recommended for projects such as the electronic heath data sharing programme that involves the collection and sharing of sensitive health records of individuals for the provision of medical services.

A PIA is useful in :

- enabling the decision-maker to adequately consider the impact on personal data privacy before undertaking the project
- directly addressing the privacy problems identified in the process and providing solutions or safeguards at the design stage
- providing benchmarks for future privacy compliance audit and control
- being a cost-effective way of reducing privacy risks
- providing a credible source of information to allay any privacy concerns from the public and the stakeholders

The PIA process

Though by no means conclusive, a PIA will generally include the following key components:

(i) Data processing cycle analysis
(ii) Privacy risks analysis
(iii) Avoiding or mitigating measures privacy risks
(iv) PIA reporting

(i) Data processing cycle analysis

This step involves the critical examination of the purpose and the rationale behind the project in deciding whether it is necessary to collect the kind, amount and extent of personal data contemplated by the data user. Insofar as it is practicable to do so, the less privacy intrusive alternatives should be explored and adopted.

The six data protection principles ("DPPs") in the Ordinance lays down the legal requirements to be observed by data users in handling the different aspects of the data processing cycle from collection, accuracy, retention, use, security, policy transparency to the access and correction of the personal data. By examining the degree of compliance with the DPPs independently in a personal data system, data users may carry out appropriate privacy risk management.

A typical list of matters to be addressed would include :

DPP1 : the purpose for which and the circumstances in which the personal data are collected

DPP2 : the policy regarding the retention of the personal data and the maintenance of their accuracy

DPP3 : the processing (including transfer and sharing) of the personal data

DPP4 : the security safeguards to prevent unauthorized or accidental access, use, modification or loss of data

DPP5 : the privacy policy and practices to be devised

DPP6 : the procedure to comply with data access and correction requests

(ii) Privacy risks analysis

The data processing cycle analysis will enable a data user to identify the key areas of privacy concerns and focus its attention on addressing these concerns. In analyzing the privacy risks, the relevant factors that the data users should take into account include :

(a) the functions and activities of the data users;
(b) the nature of the personal data involved;
(c) the number of individuals affected;
(d) the gravity of harm that may cause the data subjects should their personal data be improperly handled; and
(e) the privacy standards and rules prescribed under applicable codes of practices, guidelines, policies and regulations that the data users shall observe, etc.

The level of data protection measures required shall as a general rule be commensurate with the privacy intrusiveness of the project.

(iii) Avoiding or mitigating privacy risks

Insofar as it is practicable to do so, the privacy risks should be avoided or appropriate mitigating measures should be adopted to protect the personal data against indiscriminate or unauthorized access, processing and use. It is highly advisable that a "privacy-by-design" approach be adopted and privacy enhancement technologies be considered and used in the design stage of the personal data system. The following are some examples of these measures :

- To reduce the amount of personal data to be collected to the extent that are necessary to fulfill the objective of the project but not excessive
- To safely delete and erase personal data when no longer required for the purpose
- To define clearly and limit the number of persons who can access and use the personal data on a "need-to-know" basis. A data user may find it justifiable to use a role-based approach in assigning and reviewing the access right to be given to its employees and agents
- To incorporate an appropriate level of security measures in the system so that confidentiality, integrity and accountability can be achieved. It is advisable to have logging and reporting mechanism to detect and notify appropriate parties in the event of a data breach
- To promulgate a clear and easy to understand privacy policy that can be effectively communicated to the data subjects and stakeholders to promote transparency
- To consult the data subjects and stakeholders when a project of significant privacy impact is to be introduced

(iv) PIA reporting

The works done in the PIA as mentioned above, including the findings, recommendations and privacy protective measures proposed to be adopted in addressing the privacy risks should

be clearly reported and documented. The PIA report records the due process undertaken by a data user to proactively manage the privacy risks. The PIA report will not only serve as benchmarks for future audits and reviews to be carried out by the data user but can often provide useful information for the Privacy Commissioner's consideration when a case of complaint comes before him. For a project that have great public concern, the data user may see fit to have the PIA report published.

The contents of a PIA report may include the following :

- Description of the project
- The data processing cycle analysis highlighting the circumstances and extent that the personal data are collected and processed
- The identification of the privacy risks
- The ways and means used to properly address these calculated risks and to explain in sufficient details how the less privacy intrusive alternatives have been considered and where appropriate, why they are adopted

Professional assistance recommended

In any project which may have a significant privacy impact on personal data, the data user should consider seeking external professional advice especially if it is planning to undertake a PIA to suit its specific needs and requirements.

A variety of skills may be required to perform a PIA and a single individual may not have all the required skills. The person undertaking the PIA should have competent analytical skills, be familiar with assessment techniques and the process and management of personal data as well as having an adequate knowledge and understanding of the Ordinance.

A data user should carefully consider the scope, scale, number and phases of the PIA to be conducted.

What happens to a PIA report if it is submitted to the Privacy Commissioner?

Upon completion of a PIA, it may be in the interests of the data user to have the benefit of the comments from the Privacy Commissioner on matters considered in the PIA report. The Privacy Commissioner can offer comments upon the privacy risk analysis undertaken by the data user. However, data users should note that the Privacy Commissioner neither endorses nor approves PIA reports because of the potential conflict with its regulatory role.

It should be noted that a PIA is not a substitute for the legal protection available to data subjects under the Ordinance. The views expressed by the Privacy Commissioner on a PIA report do not in any way prejudice the exercise of his powers or functions.

Office of the Privacy Commissioner for Personal Data, Hong Kong
Enquiry Hotline: (852) 2827 2827
Fax: (852) 2877 7026
Address: 12/F, 248 Queen's Road East, Wanchai, Hong Kong
Website: www.pcpd.org.hk
Email: enquiry@pcpd.org.hk