Privacy Impact Assessments (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 minimising adverse impacts. Although PIA is not expressly provided for under the Personal Data (Privacy) Ordinance ("the Ordinance"), it has become a widely accepted 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 impact on personal data privacy.

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

Why is a PIA useful

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

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

- 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; or
- 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.

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 associated with their launch and use. PIA was also undertaken for projects such as the electronic health data sharing programme that involves the collection and sharing of sensitive health records of individuals for the provision of medical services.

The PIA process

A PIA generally includes the following key components:

(i) Data processing cycle analysis;

(ii) Privacy risks analysis;

(iii) Avoiding or mitigating privacy risks; and

(iv) PIA reporting.

(i) Data processing cycle analysis

This step critically examines the purpose and rationale behind the project: 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, any less privacy intrusive alternatives should be explored and adopted.

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

Typical matters to be addressed include:

DPP1	the purpose for which and the circumstances under which the personal data is collected
DPP2	the policy regarding the retention of the personal data and the maintenance of its accuracy
DPP3	the processing (including transfer and sharing) of the personal data
DPP4	the security safeguards to prevent unauthorised or accidental access, processing, erasure, loss or use, of the data
DPP5	the privacy policy and practices to be devised
DPP6	the procedures for complying with data access and correction requests

(ii) Privacy risks analysis

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

(a) the functions and activities of the data user;

(b) the nature of the personal data involved;

(c) the number of individuals affected;

(d) the gravity of harm that may be caused to the data subjects should their personal data be improperly handled;

(e) whether a data processor[1] is appointed to carry out data processing on behalf of the data user; and

[1] "Data processor" means a person who processes personal data on behalf of another person; and does not process the data for any of the person's own purposes.

(f) the privacy standards and rules prescribed under applicable codes of practice, guidelines, policies and regulations that the data user 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, privacy risks should be avoided or mitigated to protect the personal data against indiscriminate or unauthorised access, processing, erasure, loss or use. It is highly advisable that a "privacy-by-design" approach be adopted and privacy enhancing technologies be considered and used at 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 is necessary to fulfill the objective of the project but is not excessive.
- To completely delete and erase any personal data that is no longer required for the purpose.
- Not to outsource the processing of the personal data to a data processor, whether within or outside Hong Kong, unless contractual or other means of control have been adopted to protect the personal data to be transferred to the data processor (i) from being kept longer than necessary for processing the data; and (ii) from unauthorised or accidental access, processing, erasure, loss or use.
- 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 use this role-based approach in assigning and reviewing the access right to be given to its employees, agents, and data processors.
- To incorporate an appropriate level of security measures in the personal data system so that confidentiality, integrity and accountability of the data can be achieved. It is advisable to have logging and reporting mechanisms to investigate 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 relevant stakeholders when a project of significant privacy impact is to be introduced.

(iv) PIA reporting

The above-mentioned works done in the PIA, 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 a benchmark for future audits and reviews to be carried out by the data user but can often provide useful information for the Privacy Commissioner for Personal Data ("the Commissioner")'s consideration if a complaint comes before him. Where a project carries 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:

- A description of the project;
- The data processing cycle analysis highlighting the circumstances in which the personal data is collected and processed (whether by the data user or by its data processing agent);
- Identification of the relevant privacy risks;
- The ways and means used to properly address or mitigate these risks and to explain in sufficient detail how any less privacy-intrusive alternatives have been considered and where appropriate, why they have not been adopted.

Professional assistance recommended

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

Various skills may be required to perform a PIA, and a single individual may not have all the required skills. The persons undertaking the PIA should have competent analytical skills, be familiar with the management of personal data, the assessment techniques and process as well as 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.

Comments of the Commissioner

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

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

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

Enquiry Hotline : **(852) 2827 2827**
Fax : **(852) 2877 7026**
Address : **12/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong**
Email : **enquiry@pcpd.org.hk**

First published in July 2010
October 2015 (First Revision)