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

Information Leaflet

Outsourcing the Processing of Personal Data to Data Processors

Introduction

The trend of outsourcing and entrusting personal data processing work by data users to their agents is increasingly common. Personal data leakage incidents sometimes occur due to insufficient steps being taken by the data processors to protect the personal data entrusted to them. This may cause substantial and irrecoverable damage to the affected data subjects. The Personal Data (Privacy) Ordinance requires a data user to take all reasonably practicable steps to safeguard the security of personal data held by it and where personal data is entrusted to a data processor, a data user is responsible for any act done by the data processor.

The Personal Data (Privacy) (Amendment) Ordinance 2012 provides enhanced protection in this respect by introducing, with effect from 1 October 2012, additional obligations on data users to use contractual or other means to monitor their data processors' compliance with data protection requirements. This information leaflet provides information on the data users' new obligations and the recommended means of compliance with the requirements.

The meaning of "data processor"

The statutory obligations of data users arise when they engage data processors to process personal data on their behalf, whether within or outside Hong Kong. The term "data processor" is defined to mean *"a person who (a) processes personal data on behalf of another person; and (b) does not process the data for any of the person's own purposes"*.

With the wide meaning of the term, the scope of coverage of data processor is not limited to providers of IT processing. It also includes other contractors engaged to process personal data on behalf of the data user. For example, where an organization engages a business services company to administer its employee payroll function, the business services company will be processing information about the organization's employees on its behalf, and hence is a data processor. Where an organization engages a marketing company to carry out customer opinion survey, the marketing company will be processing customers' information on behalf of the organization, and hence is also a data processor. Other examples of data processors include service providers engaged to input personal data to computer systems and contractors engaged to shred confidential documents which contain personal data.

Obligations of data users

If a data user engages a data processor, whether within or outside Hong Kong, to process personal data on the data user's behalf, the data user must adopt contractual or other means to prevent any personal data transferred to the data processor from being kept longer than is necessary for processing of the data (**DPP 2(3)**).

If a data user engages a data processor, whether within or outside Hong Kong, to process personal data on the data user's behalf, the data user must adopt contractual or other means to prevent unauthorized or accidental access, processing, erasure, loss or use of the data transferred to the data processor for processing (**DPP4(2)**).

How to comply with the requirements

Through contractual means

The primary means by which a data user may protect personal data entrusted to its data processor is through a contract. In practice, data users often enter into contracts with their data processors for the purpose of defining the respective rights and obligations of the parties to the service contract. To fulfil the new obligations under DPP2(3) and DPP4(2), data users may incorporate additional contractual clauses in the service contract or enter into a separate contract with the data processors.

The types of obligations to be imposed on data processors by contract may include the following:-

(a) security measures required to be taken by the data processor to protect the personal data entrusted to it and obligating the data processor to protect the personal data by complying with the data protection principles (The security measures that are appropriate and necessary for a data user will depend on the circumstances. Basically, the data processor should be required to take the same security measures the data user would have to take if the data user was processing the data himself);

(b) timely return, destruction or deletion of the personal data when it is no longer required for the purpose for which it is entrusted by the data user to the data processor (it is for the parties to agree the appropriate number of days);

(c) prohibition against any use or disclosure of the personal data by the data processor for a purpose other than the purpose for which the personal data is entrusted to it by the data user;

(d) absolute prohibition or qualified prohibition (e.g. unless with the consent of the data users) on the data processor against sub-contracting the service that it is engaged to provide;

(e) where sub-contracting is allowed by the data user, the data processor's agreement with the sub-contractor should impose the same obligations in relation to processing on the sub-contractor as are imposed on the data processor by the data user; where the sub-contractor fails to fulfill its obligations, the data processor shall remain fully liable to the data user for the fulfillment of its obligations;

(f) immediate reporting of any sign of abnormalities (e.g. audit trail shows unusual frequent access of the personal data entrusted to the data processor by a staff member at odd hours) or security breaches by the data processor;

(g) measures required to be taken by the data processor (such as having personal data protection policies and procedures in place and providing adequate training to its relevant staff) to ensure that its relevant staff will carry out the security measures and comply with the obligations under the contract regarding the handling of personal data;

(h) data user's right to audit and inspect how the data processor handles and stores personal data; and

(i) consequences for violation of the contract.

The above list is not exhaustive and data users may need to make adjustment or to include additional obligations on data processors under the contract having regard to factors such as the amount of personal data involved, the sensitivity of the personal data, the nature of the data processing service and the harm that may result from a security breach.

Through other means

Sometimes, data users may not be able to enter into a contract with its data processor to protect the personal data entrusted to it. The Ordinance provides flexibility and allows the use of "other means" of compliance. The term "other means" is not defined under DPP2(3) and DPP4(2).

Generally, data users may engage non-contractual oversight and auditing mechanisms to monitor their data processors' compliance with data protection requirements, such as through the adoption of the following measures:-

(a) Data users are expected to select reputable data processors offering sufficient guarantees in respect of the technical competence and organizational measures governing the processing to be carried out, and with a good track record on data protection.

(b) Data users must be satisfied that the data processors have robust policies and procedures in place, including adequate training for their staff and effective security measures, to ensure that the personal data in their care is properly safeguarded at all times and is not kept for longer than necessary.

(c) Data users should also have the right to audit and inspect how the data processors handle and store personal data, and exercise the right to audit and inspect when warranted.

The above measures are not exhaustive and data users may take other steps to comply with requirements. When a complaint is brought before him, the Privacy Commissioner will consider all the means engaged by a data user to protect personal data entrusted to its data processor. Therefore, it is important that effective means are selected, engaged and properly documented.

Good practice recommendations

Some further good practice recommendations are set out below when data users engage data processors to process personal data on their behalf:

(i) Data users should be transparent about their personal data handling practices and make it plain to the data subjects and in clear and understandable language when collecting their personal data that their personal data may be processed by data processors.

(ii) If the data processors are not situated in Hong Kong, the data users should make sure that their contracts are enforceable both in Hong Kong and in the countries in which the data processors are situated. The meaning of technical and legal terms such as "personal data", which may vary with the jurisdictions, should be clearly defined to suit compliance with the Hong Kong requirements.

(iii) Both data users and data processors should keep proper records of all the personal data that have been transferred for processing.

(iv) Before entrusting any personal data to data processors for system testing, data users have to consider whether the use of anonymised or dummy data by data processors can equally serve the purpose.

Redress of Data Subjects

A data processor is not directly liable to a data subject for infringement of his personal data privacy. Aggrieved data subjects may however seek recourse from the data user who engaged the data processor. The data user is liable as the principal for the wrongful act of its authorised data processor.

In case a complaint is brought by a data subject against the data user for its data processor's wrongful act or practice which infringes his personal data privacy, the contract made between the data user and the data processor incorporating specific clauses on data protection will serve as useful evidence to show the data user's compliance with the requirements under DPP2(3) and DPP4(2). If considered appropriate, a data user may bring a separate action against its data processor by relying on the contractual terms governing the data processor's obligations in data protection.

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

Copyrights

Reproduction of all or any parts of this information leaflet is permitted on condition that it is for non-profit making purposes and an acknowledgement of this work is duly made in reproduction.

Disclaimer

The information provided in this information leaflet is for general reference only. It does not provide an exhaustive guide to the Personal data (Privacy) Ordinance (the "Ordinance"). For a complete and definitive statement of law, direct reference should be made to the Ordinance itself. The Privacy Commissioner for Personal Data (the Ordinance) makes no express or implied warranties of accuracy or fitness for a particular purpose or use with respect to the above information. The above information will not affect the functions and power conferred to the Commissioner under the Ordinance.

© Office of the Privacy Commissioner for Personal Data,
Hong Kong
September 2012