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

Inspection Report

published under Section 48(1) of the
Personal Data (Privacy) Ordinance, Chapter 486, Laws of Hong Kong

Personal Data Systems of Private Tutorial Services Industry in Hong Kong

Report Number: R18-13069

28 December 2018

This page is intentionally left blank to facilitate double-side printing

Report on the Inspection of the Personal Data Systems of Private Tutorial Services Industry in Hong Kong

This inspection report is published by the Privacy Commissioner for Personal Data, Hong Kong, pursuant to section 36 of the Personal Data (Privacy) Ordinance, Chapter 486, Laws of Hong Kong in relation to personal data systems of private tutorial services industry in the discharge of his powers and duties under section 48 of the Ordinance.

Section 36 of the Ordinance provides that:-

"*Without prejudice to the generality of section 38, the Commissioner may carry out an inspection of-*

(a) any personal data system used by a data user; or

(b) any personal data system used by a data user belonging to a class of data users,

for the purposes of ascertaining information to assist the Commissioner in making recommendations-

(i) to-

(A) where paragraph (a) is applicable, the relevant data user;

(B) where paragraph (b) is applicable, the class of data users to which the relevant data user belongs; and

(ii) relating to the promotion of compliance with the provisions of this Ordinance, in particular the data protection principles, by the relevant data user, or the class of data users to which the relevant data user belongs, as the case may be."

The term "**personal data system**" is defined in **section 2(1)** of the Ordinance to mean "*any system, whether or not automated, which is used, whether in whole or in part, by a data user for the collection, holding, processing or use of personal data, and includes any document and equipment forming part of the system*."

Section 48 of the Ordinance provides that:-

"*(1) Subject to subsection (3), the Commissioner may, after completing an inspection where section 36(b) is applicable, publish a report-*

(a) setting out any recommendations arising from the inspection that the Commissioner thinks fit to make relating to the promotion of compliance with the provisions of this Ordinance, in particular the data protection principles, by the class of data users to which the relevant data user belongs; and

(b) in such manner as he thinks fit.

……

(3) Subject to subsection (4), a report published under subsection (1)… shall be so framed as to prevent the identity of any individual being ascertained from it.

(4) Subsection (3) shall not apply to any individual who is-

(a) the Commissioner or a prescribed officer;

(b) the relevant data user."

Stephen Kai-yi WONG
Privacy Commissioner for Personal Data, Hong Kong
28 December 2018

Inspection Report
published under Section 48(1) of the
Personal Data (Privacy) Ordinance
Chapter 486, Laws of Hong Kong

Personal Data Systems of
Private Tutorial Services Industry in Hong Kong

The Executive Summary

Background

1. Hong Kong, like other major Asian jurisdictions such as mainland of China, Japan and Taiwan, places great emphasis on the academic performance and public examination results of children[1]. As a result, private tutorial services are flourishing, large-scale advertisements in private tutorial institutions abound, and such services have become major channels for children to gain academic knowledge outside conventional schools. According to the survey data, more than 76% of the children had received private tutorial services, and 22% of the children had started to receive such counselling education since Primary Four.

2. The Privacy Commissioner for Personal Data, Hong Kong (the **Commissioner**) values the privacy of personal data of children highly. As the children's awareness of privacy is relatively low, they tend to follow others' instructions and are very susceptible to peers influence. Therefore, the Commissioner believes that the institutions that serve children should give special privacy protection to the group.

3. The private tutorial services industry has a wide range of services and handles a vast quantity of personal data, including sensitive personal data. The Commissioner considered that it would be in the public interest to examine the operation of the private tutorial services industry

[1] "Children" in this report refers to persons aged under 18

in relation to the protection of personal data privacy. The Commissioner therefore carried out an inspection (the **Inspection**) of the personal data systems of three private tutorial institutions under section 36 of the Personal Data (Privacy) Ordinance (the **Ordinance**), Chapter 486 of the Laws of Hong Kong:

(i) a chain-run tutorial institution;
(ii) a tutorial institution operating on a franchise model; and
(iii) an institution that provides tutorial services using online media (mobile application).

4. The Inspection covered the entire cycles of personal data flow by private tutorial institutions of the three different business models. The Commissioner learned from the Inspection that they had had different ideas and perceptions about the handling of personal data, resulting in different strengths and weaknesses of their personal data systems. The Commissioner expected that the findings and recommendations of the Inspection would enable the industry to improve its privacy protection policies and operation practices, to nurture the culture of "protect and respect personal data privacy" and to assist them in complying with the requirements under the Ordinance and the Data Protection Principles (**DPPs**) in Schedule 1 to the Ordinance.

Findings and Recommendations

5. In the inspection, the Commissioner noted that the three institutions had taken measures to protect personal data in their operational procedures and practices. Whilst personal data protection measures are generally acceptable, inadequacies could be reflected in the functions of individual private tutorial institutions. The Commissioner was of the view that responsible organisations should formulate and maintain a comprehensive privacy management programme[2], which should serve as a strategic framework to assist them in building a robust privacy infrastructure supported by an effective ongoing review and monitoring

[2] The Commissioner published a guide entitled "*Privacy Management Programme: A Best Practice Guide*" in February 2014, which outlined the good approaches for developing a sound privacy management programme.

process to facilitate its compliance with the requirements under the Ordinance, covering business practices, operational processes, product and service design, physical architectures and network infrastructure.

6. The Inspection showed that the three institutions had committed themselves to privacy management. Their personal data systems had different strengths and weaknesses in all aspects and there was still room for improvement. In addition to the statutory compliance requirements under the Ordinance, the Commissioner also made reference to the requirements of a comprehensive privacy management programme and proposed the following recommendations to institutions in the private tutorial services industry to enhance corporate accountability and build mutual trust with customers in order to achieve a win-win situation in the process of handling personal data:

(1) Integrating the ideas of data privacy protection into corporate governance

The Commissioner noted that one selected institution did not integrate the ideas of data privacy protection into corporate governance and strongly encourages all private tutorial institutions (regardless of the mode of business or size of organisation) to do so. The Commissioner also encourage all private tutorial institutions to demonstrate organisational commitment to personal data privacy, to designate a data protection officer from top management to oversee the privacy management programme and data protection matters, and to nurture the culture of respect privacy within the organisation.

(2) Privacy by Design

Private tutorial institutions should incorporate privacy protection when designing new products and services and assess the impact of launching such products and services on personal data privacy. They could make effective use of information technology tools to provide customer-oriented services and reduce the risk of privacy leakage.

(3) Formulating a comprehensive privacy policy

The Commissioner noted that all three selected institutions had not put in place comprehensive privacy policies. Regardless of the mode of business or the size of the organisation, private tutorial institutions should develop a comprehensive privacy policy on handling personal data. The privacy policy must be applied by all departments and tutorial centres. All staff must be informed of the same in a timely manner to ensure that the organisation's system and measures for handling personal data are consistent. To cope with the social and business development, they should also review and update their privacy policies on a regular basis.

The privacy policy should cover the collection, accuracy, retention, use, security measures and destruction procedures of personal data (both physical documents and electronic records), as well as the requirements and operational procedures for handling direct marketing activities and opt-out requests.

As the current tutorial services rely heavily on information technology, a secure information technology system is of utmost importance. Private tutorial institutions should formulate relevant policies on information technology security to specify all information technology security measures and the practical policies for responding to relevant security risks.

(4) Establishing effective reporting and data breach notification mechanism

The Commissioner noted that two selected institutions did not have in place any written guidelines or procedures to regulate the handling of data loss or breach incidents. To cope with personal data privacy related matters, private tutorial institutions should establish an effective reporting and monitoring mechanism to properly respond to the problems arising from the processing of personal data and to ensure compliance of privacy policies by their staff members.

Private tutorial institutions should develop a data breach notification mechanism to stipulate the process of handling data breach incidents (including the immediate assessment and measures to be taken to

contain the breach and damage) and designate personnel from top management to handle such incidents.

(5) Enhancing employees' awareness of privacy protection through training and education

The Commissioner noted that two selected institutions would only provide personal data privacy training to new recruits. To raise employees' awareness of privacy protection and to nurture the organisational culture of respecting privacy, private tutorial institutions should provide regular education and training to all employees (including franchisees and their employees or employees of other business models). The comprehensive training and refresher courses for personal data protection should not be limited to professional training courses, practical tips through emails or corporate communications, but also be extended to provide relevant information online.

(6) Ceasing collection of unnecessary or excessive personal data

The Commissioner noted that two selected institutions involved excessive collection of personal data and one of them failed to provide Personal Information Collection Statement in application form. Private tutorial institutions should review their data collection practices taking into consideration the following factors:

(i) If it is found that the personal data collected is excessive or unnecessary, they should cease such collection, amend the relevant forms and delete/destroy those data so collected;

(ii) To provide a Personal Information Collection Statement on their registration or application forms so as to inform children and their parents of the collection purposes and other notification requirements as stipulated in DPP 1(3); and

(iii) To reduce the collection of personal data to the minimum according to the nature of the services provided.

(7) Avoiding indefinite retention of personal data

Permanent retention of personal data is contrary to the requirements of section 26 and DPP 2(2) of the Ordinance. The Commissioner was disappointed that the three selected institutions had adopted a practice of retaining permanently the personal data of children and tutors albeit in different circumstances. Private tutorial institutions should establish policies on retention of personal data, taking into account different types of data, storage media, the purpose of retaining the data, how to identify the data that has exceeded the retention period as well as the procedures and methods for destroying such data.

(8) Proper use of personal data

The Commissioner noted two selected institutions involved inappropriate use of personal data in the provision of tutorial services. Private tutorial institutions should conduct a comprehensive review on the use of personal data to ensure that such use is consistent with or directly related to the purpose for which the data was originally collected, or has obtained prescribed consent from the data subject concerned.

(9) Improving personal data security mechanism

The Commissioner found inadequate security safeguards operations and systems in all three selected institutions. Private tutorial institutions are increasingly relying on information technology systems to handle tutor-related services, preserve and manage relevant records and databases. Maintaining the healthy operation of information technology systems to protect it from cyberattacks is as important as other physical security measures:

(i) Develop physical security measures including access control system, secure important documents in locked cabinets to prevent or deter unauthorised access and use of personal data;

(ii) Make use of technical measures including encryption programmes, system access management, identity

authentication system to restrict and monitor access to personal data in the information technology systems; and

(iii) Develop a comprehensive information security policy which is supplemented by regular training to strengthen staff awareness on personal data privacy.

(10) Adopting contractual means to manage data processor

The Commissioner was satisfied that all three selected institutions had engaged data processors to regulate the retention and security of personal data through contractual means. Apart from adopting contractual means to manage the personal data entrusted to data processors, private tutorial institutions should conduct regular monitoring and compliance procedures to ensure data processors' compliance with the requirements of privacy protection.

When engaging major cloud service providers, private tutorial institutions should carefully assess the reliability of those providers, contents of their services, and whether the terms and conditions set out in the standard contracts meet all requirements of data protection.

As a matter of good practice, institutions should conduct a detailed privacy impact assessment to identity any potential privacy risks before entrusting their personal data to cloud service providers.

(11) Data ethics and standards

Institutions that amass and derive benefits from personal data should not ditch their mindset of conducting their operations to meet the minimum regulatory requirements only. They should also be held to a higher ethical standard that meets stakeholders' expectation by doing what they should do. Data ethics and stewardship can therefore bridge the gap between legal requirements and stakeholders' expectation.

– End –

Personal Data Systems of
Private Tutorial Services Industry in Hong Kong

The Report

(I) Introduction

Reasons for the Inspection

1. Hong Kong, like other major Asian jurisdictions such as the mainland of China, Japan and Taiwan, places great emphasis on the academic performance and public examination results of children. As a result, private tutorial services are flourishing, large-scale advertisements in private tutorial institutions abound, and such services have become other major channels for children to gain academic knowledge outside conventional schools. According to the survey data, more than 76% of the children had received private tutorial services, and 22% of the children had started to receive such counselling education since Primary Four.

2. There are currently over 2,000 private tutorial institutions in Hong Kong, mainly serving primary and secondary school students. As children's awareness of privacy is relatively low and they tend to follow others' instructions without hesitation, special protection on data privacy should be given to them when they receive private tutorial services. In addition, the private tutorial institutions would also collect and process the personal data of parents and tutors of children when providing their services. The quantity of personal data collected and processed by them is vast, and sensitive personal data (e.g. Hong Kong Identity Card (**HKID Card**) number) may be involved. The Commissioner considered that it would be in the public interest to carry out the inspection of the personal data systems of private tutorial industry pursuant to section 36 of the Personal Data (Privacy) Ordinance (the **Ordinance**).

(II) Inspection

Private Tutorial Services Industry

3. There is a wide variety of private tutorial services in Hong Kong, from independent private tutorial centres to chain-run private tutorial institutions; from traditional face-to-face tutors to video content or online media as teaching tools.

4. The Commissioner selected one representative institution from each of the business models below as the targets of the Inspection, in relation to the collection, holding, handling and use of personal data by them as data users in the market of private tutorial services:

   (i) chain-run tutorial institutions;
   (ii) tutorial institutions running on franchise basis; and
   (iii) institutions that provide tutorial services using online media (website and mobile application).

Chain-run tutorial institutions

5. Chain-run tutorial institutions operate various tutorial centres, with vast number of students comparable to that of conventional education. In addition to the mode of face-to-face lectures conducted by tutors, there are also video classes or self-study courses through online media. The Commissioner selected an institution (**Institution A**) with relatively large market share having tutorial centres at different districts in Hong Kong for the Inspection. Institution A had more than 60,000 enroled students annually.

Tutorial institutions running on franchise basis

6. Tutorial institutions running on franchise basis are also common in Hong Kong, with relatively small class size but larger number of branches. Interested individuals or tutors could liaise with the franchiser for setting up new branches on a franchise basis. Although all centres

share the same brand name, the franchiser and individual franchisees are separate legal entities. In the perspective of personal data privacy, they would be regarded as joint data users. In the franchise arrangement, franchisees would receive unified teaching tools, operational training and support from the franchiser. The Commissioner selected a franchiser (**Institution B**) which built a large number of franchised centres across Hong Kong for the Inspection.

Institutions that provide tutorial services using online media

7. A tutorial institution (**Institution C**) developed a mobile application (the **App**) serving as an online platform for the provision of tutorial services. The App recruited both tutors and children and played the role to match the two parties for academic questions raised. Technical tools including machine learning were deployed for enhancing the matching process.

Scope of the Inspection

8. The Inspection Team (the **Team**) examined the handling of personal data of children[3] and tutors by the three institutions from data collection to data disposal, with a view to identifying good practices or inadequacies from the perspective of data privacy protection. The personal data cycles of tutorial registration and tutor engagement in all the three selected institutions were examined in details in the Inspection. Due reference to the promotion of compliance with the requirements under the Ordinance and the Data Protection Principle (**DPP**) 1 to 6 was also made.

9. DPP 1 to 6 cover the collection, accuracy, retention, use, security, transparency and access to personal data. The three institutions' compliance with the direct marketing regulations under Part 6A of the Ordinance was also examined. In addition to the requirements under the Ordinance, the Team also reviewed how the three institutions protected personal data in the perspective of corporate governance, by making

[3] In the Inspection, children's data often consists of their parents', especially when the children concerned are very young. Therefore, for the sake of simplicity, "data of children" (or similar wordings) includes the data of their parents throughout this report.

reference to the best practices in developing a privacy management programme as advocated by the Commissioner.

10. The six DPPs, the direct marking regulations under sections 35B to 35H of the Ordinance, and a summary chart of a privacy management programme are respectively reproduced at Annexes 1 to 3 for easy reference.

Methodology

11. The Inspection consisted of five major types of review work:

a) *Mystery visits*

12. The Team conducted mystery visits at selected centres of Institutions A and B for the purposes of having a thorough understanding of the workflow from applications to the delivery of classes / services, and the performance of individual centre staff, in particular the handling of personal data in daily routines. Instead of paying a physical visit to Institution C which operated the App for the provision of its services, the Team registered and examined the App for the purposes of understanding its operation.

b) *Policy review*

13. A detailed and comprehensive policy on personal data handling is essential for ensuring a good and uniform practice. The Team examined the personal data privacy policies of the three institutions as documented in their policies, guidelines, notices, forms, and training materials.

c) *Site inspections*

14. Site inspections at the head offices of the three institutions, selected centres and a warehouse of each of Institutions A and B had been conducted for the purposes of (i) understanding the physical layout and security measures of the premises of the three institutions where personal data was collected, processed and stored; (ii) examining

equipment and systems used for the collection, processing and storage of personal data; (iii) examining paper and electronic records retained in the premises and computer systems; and (iv) identifying any irregularities in terms of data protection.

d) ***Walkthrough demonstrations***

15. During the site inspections, the three institutions demonstrated to the Team their operational processes like class / service application and enquiry handling, which gave the Team an understanding on how they collected, used and safeguarded personal data.

e) ***Interviews and Enquiries***

16. The Team made verbal and written enquiries with the three institutions before, during, and after the site inspections. Verbal enquiries were made through interviews with staff members ranking from management to operational levels at the three institutions' head offices and centres of Institutions A and B, which enabled the Team to understand how the staff members handled personal data, their familiarity with internal policies and guidelines relating to personal data privacy, and the training they provided and received. The Team also held a video conference with technical staff of Institution C in Taiwan to understand the technical tools and measures deployed to safeguard the App.

17. The information sought through written enquiries assisted the Team in understanding the operation of the three institutions' personal data systems, reconciling the documentary evidence obtained with observations at the site inspections and identifying any cause for concern.

(III) Personal Data Systems and Data Flow

The Personal Data Systems

18. The personal data systems that were inspected in the Inspection not only covered the computer systems used to process personal data, but also the systematic operation of different departments and relevant tutorial centres in the collection, holding, processing or use of personal data of children and tutors.

19. There were some differences among the personal data systems of the three institutions:

    (i) Institution A - there were several computer systems for handling children registration, course information, attendance arrangement and course allocation, among which a centralised enrolment system (the **Enrolment System**) was used to record and process children's registration of tutorial classes;

    (ii) Institution B – their franchised tutorial centres used a standard enrolment form to collect children data, the head office would input the data into their computer systems when they received the forms from centres;

    (iii) Institution C - personal data of children and tutors was collected through the App. The data collected was maintained at the institution's database for internal processing.

20. The details of the types of children's data[4] collected by and maintained in the personal data systems of the three institutions are listed below:

[4] Although there was no indication in the institutions' application forms on whether the items requested were compulsory, the institutions (except Institution C) explained that some items could be provided on a voluntarily basis.

Type of personal data	**Institution A**	**Institution B**	**Institution C**
(1) Chinese and English name	√	√	
(2) Gender	√	√	
(3) Nationality		√	
(4) HKID Card number	√		
(5) Date of birth	√	√	
(6) Class level/grade	√	√	
(7) Contact number	√	√	√
(8) Email address	√	√	√
(9) Social media account	√		
(10) Address	√	√	
(11) Name of parent/guardian	√	√	
(12) Relationship between parent/guardian	√		
(13) Contact number of parent/guardian	√	√	
(14) Email address of parent/guardian		√	
(15) School name	√	√	√

Table 1

21. In addition to the name and contact details, other kinds of personal data of tutors maintained in the personal data systems of the three institutions are listed below:

Type of personal data	**Institution A**	**Institution B**	**Institution C**
(1) HKID Card number	√	√	
(2) HKID Card copy	√	√	
(3) Marital status	√	√	
(4) Date of birth	√	√	
(5) Education background	√	√	
(6) Work experience	√	√	
(7) Professional qualifications	√	√	
(8) Name and contact details of referee	√	√	
(9) Name and contact details for emergency	√	√	
(10) Bank account number	√		√
(11) Sex offences conviction record	√		
(12) Social media account			√
(13) Public exam certificate copy			√
(14) University student identity card copy			√

Table 2

An Overview of Personal Data Flow

a) Institution A

i) Collection of personal data

22. Institution A handled children's registrations for tutorial classes at branches. Children's personal data flow started with children's completion of a course application form which involved the collection of personal data as listed in Table 1 above. Afterwards, branch staff would input the personal data in the form into the Enrolment System and print a payment receipt.

23. Regarding the personal data flow of tutors, Institution A received job applications from tutors through its website, where it requested applicants to input certain information like contact details, education background and work experience. Suitable applicants would be invited to attend an interview and requested to complete a job application form where the personal data as listed in Table 2 above would be required.

ii) Use of personal data

24. Children's personal data was used by Institution A in the course of providing tutorial services and internal administration to:

- record attendance;
- inform students of any special arrangement of their classes;
- contact parents in case of emergency;
- handle enquiries and requests from students;
- reconcile transaction records; and
- offer marketing materials.

25. Tutors' personal data was mainly used for the purpose of recruitment process and personnel management.

iii) Retention of personal data

Paper records

26. At centres, the course application forms were stored in cabinets at restricted areas. Thereafter, the forms were transported to the head office where the data was checked against that of the Enrolment System, and would then be passed to a warehouse for retention of 10 years.

27. When providing tutorial services, handling internal administrative matters and conducting direct marketing activities, the head office and centres of Institution A generated various reports, lists and records containing children's data from computer systems, with retention periods ranged from a day to seven years. Institution A formulated policies to specify the retention period of different types of documents.

28. All paper records of tutors were kept by the Human Resource Department which operated in a locked room at the head office. Records of unsuccessful applicants would be kept for four months, while those of previous employees for three years. Records of current staff members were locked in cabinet, access to which had to be marked in a log record maintained by the department head.

Computer records

29. Apart from the Enrolment System which was used to process and store children's data, Institution A had an attendance system (the **Attendance System**) for taking student attendance, and an administration system (the **Administration System**) for handling certain requests of children. Both the Attendance System and the Administration System obtained children records from the Enrolment System. Besides, individual departments and staff members may maintain working files containing children's data based on operational needs.

30. Although there was no retention policy governing children's data stored in the Enrolment System and held by individual staff members, it was the institution's practice to purge children's data in the Enrolment

System which had been inactive for seven years. The data in the Enrolment System was backed up with encryption protection and stored in the cloud.

31. Institution A did not have a specific computer system to store or manage tutors' records.

32. The retention periods of various paper and computer records of personal data held by Institution A are summarised as follows:

Type of record	**Retention period**
Course application forms	10 years
Reports, lists and records containing children's data	1 day to 7 years
Records of unsuccessful job applicants	4 months
Records of previous employees	3 years
Electronic records of inactive students	7 years

iv) Destruction of personal data

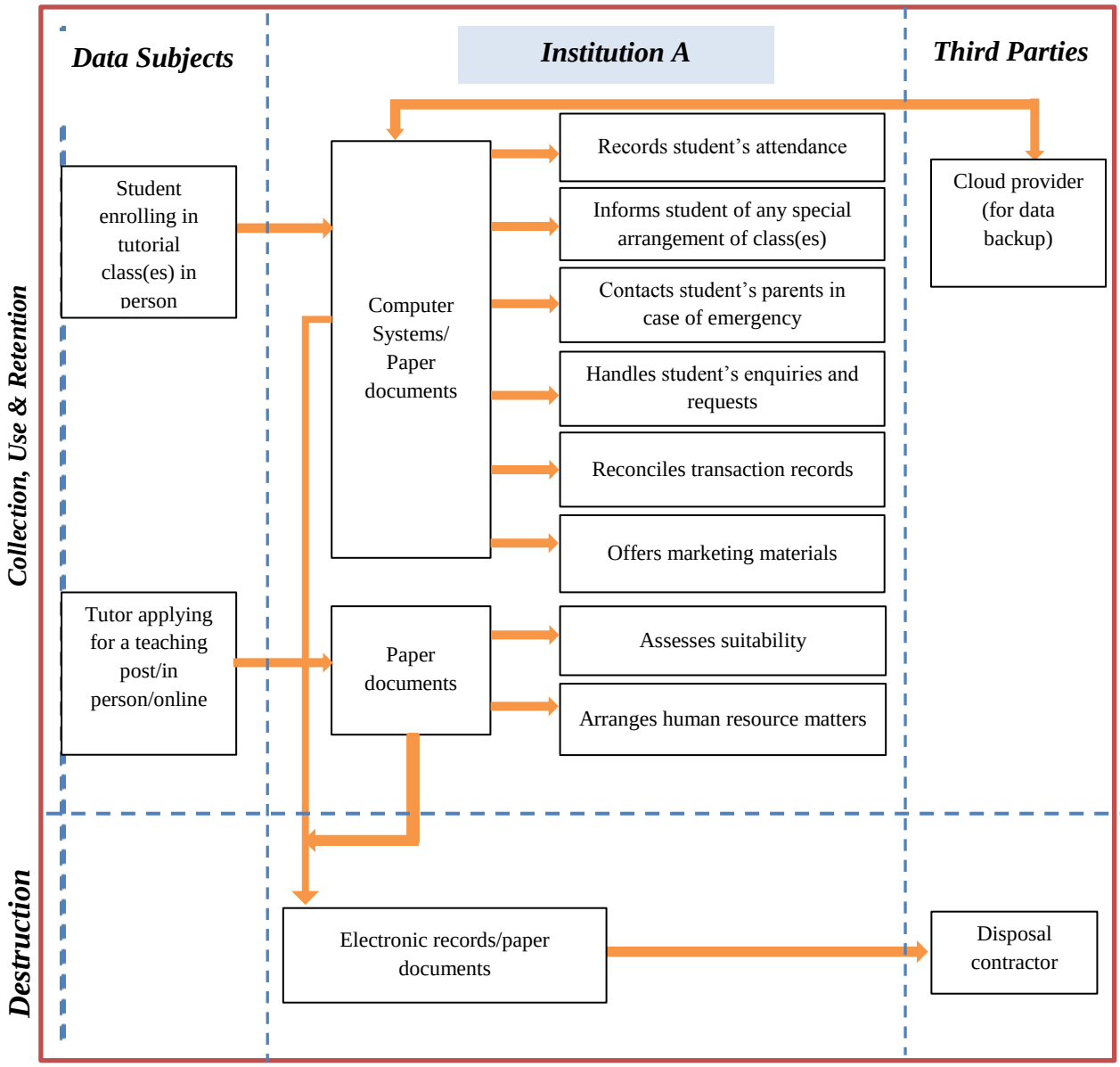
Paper records

33. According to Institution A's usual practice, when departments did not have enough space to store the children's records and documents, they would ship the documents to their warehouse for storage. The records that were stored in the warehouse would be marked with the date and file type. The warehouse clerk would deliver the documents to the designated document destruction service contractor for destruction according to the applicable retention periods of the documents. Documents that were not delivered to the warehouse would be destroyed by departments themselves.

Computer records

34. Institution A had no policy in relation to the purging of children's data; it was the practice of the Information Technology Department to actively purge children's records in the Enrolment System which had been inactive for seven years. For working files containing children's personal data that was saved in a staff member's own computer, he would be responsible for the deletion himself.

35. The flow of personal data of children and tutors is illustrated as follows:



b) Institution B

i) Collection of personal data

36. The franchised tutorial centres were operated by the franchisees themselves. They used a standard enrolment form provided by Institution B to collect the personal data of children as listed in Table 1 above. The enrolment form was printed in triplicate, of which the head office, the centre and child's parent would each hold a copy, and the office copy would be physically passed to the head office for data input into a computer system.

37. Those who were interested in opening a franchised tutorial centre had to submit basic personal data to Institution B via its website and join an introductory seminar. At the seminar, Institution B would require those who wished to operate a franchised centre to complete the application form, which collected the applicant's name, contact information and personal data as set out in Table 2 above.

ii) Use of personal data

38. InstitutionB and its franchised tutorial centres used children's personal data in the course of providing tutorial services and internal administration to:

- process enrolment related matters ;
- provide learning awards;
- communicate with students' parents;
- conduct internal statistical research and analysis;
- handle students or their parents' requests of changing centres or resuming classes; and
- market products, services and activities.

39. Franchisees' personal data was mainly used for matters related to the set up of franchised centres, administration of franchisees' contracts and monitoring of teaching quality, etc.

iii) Retention of personal data

Paper records

40. Apart from the enrolment forms, Institution B provided a record book to children which was marked with some basic information like name, contact number, photo and learning progress. Record books were kept at the centre for recording children's learning process. Besides, Institution B generated monthly instructor reports which showed children's learning progress for each subject at individual centres. Both the head office and centres maintained copies of enrolment forms and instructor reports.

41. At centres, record books were placed at relatively prominent areas to facilitate children's collection. Similarly, visitors could take the record books or access its contents easily. Generally speaking, individual centres would keep enrolment forms and record books of discontinued students for three to six months, but the retention period for instructor reports varied at different centres. At the head office, enrolment forms and instructor reports were stored in locked cabinets for four and six months respectively.

42. Franchisees' application forms and contracts were stored in locked cabinets at the head office. Records for unsuccessful applicants or discontinued franchisees would be kept for six months.

Computer records

43. During the Inspection, the Team noticed that some centres rarely used computers to handle children's data. Institution B stored children's data and franchisees' data in separate computer systems. Whilst records for unsuccessful applicants or discontinued franchisees would be purged after six months, there were no definite retention periods for other computer records of children and franchisees.

44. The retention periods of various paper and computer records of children and franchisees held by Institution B and its franchised centres are summarised as follows:

Type of Record	**Retainer**	**Retention Period**
Enrolment Form	Head office	4 months
	Centre	3 - 6 months
Record Book	Centre	3 - 6 months
Instructor Report	Head office	6 months
	Centre	varied
Application form and contract of unsuccessful applicant or discontinued franchisee	Head office	6 months
Electronic record of unsuccessful applicant	Head office	6 months
Electronic record of student	Head office	indefinite
Electronic record of discontinued franchisee	Head office	indefinite

iv) Destruction of personal data

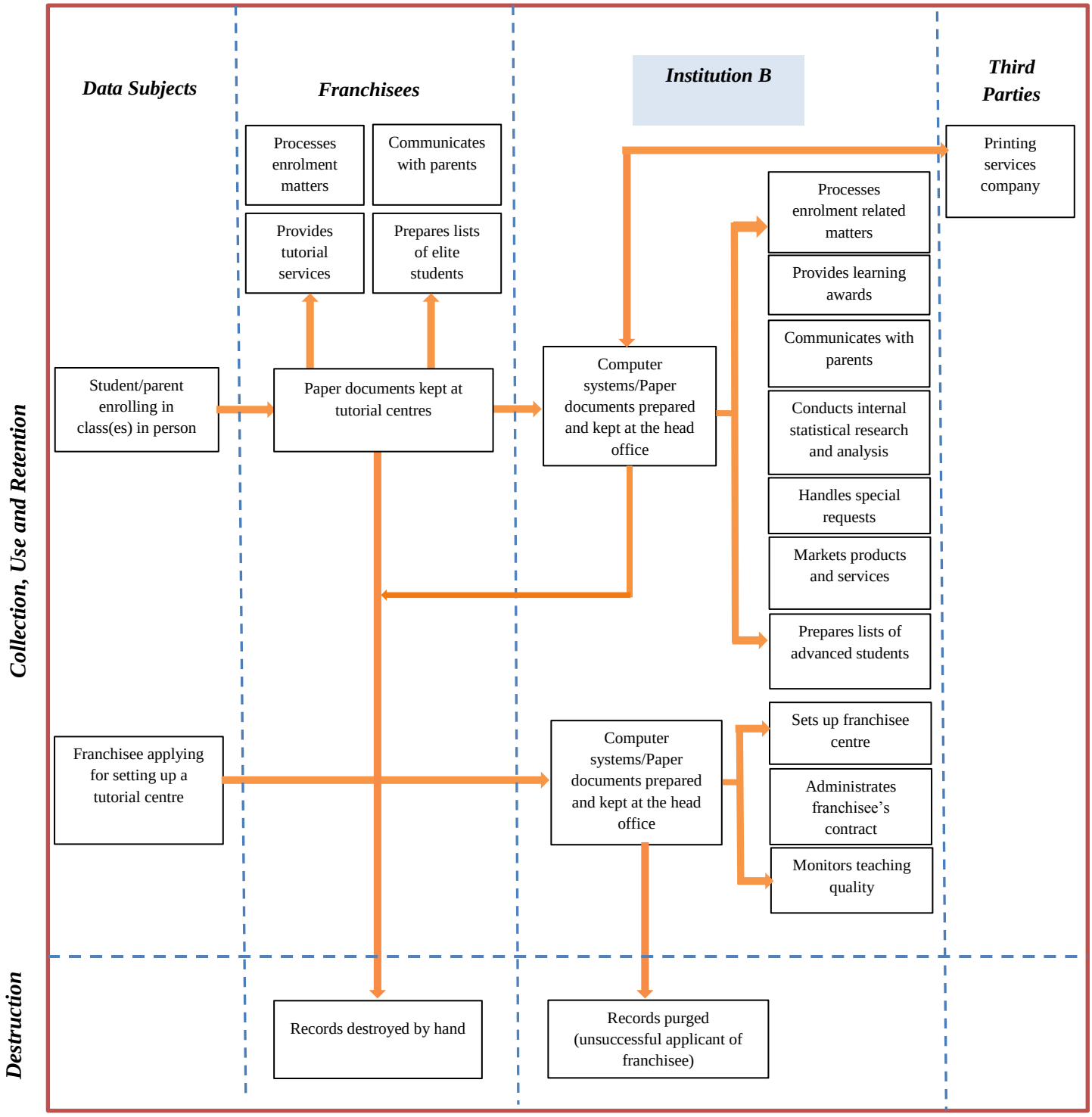
Paper records

45. Franchised centres would destroy expired records of children by hand; expired records of children and franchisees kept at the head office of Institution B would be destroyed by shredders in a designated room.

Computer records

46. As some centres rarely used computers to handle children's data, the Team did not notice any relevant computer files or records. However, except for records of unsuccessful applicants of franchisees, it appeared that Institution B did not have policy in place governing the deletion of computer files that contained personal data.

47. The flow of personal data of children and franchisee is illustrated as follows:



c) Institution C

i) Collection of personal data

48. Institution C collected personal data of children and tutors via the App when they registered themselves as users, which involved the personal data as set out in Tables 1 and 2 above.

ii) Use of personal data

49. Children could login to the App and send out questions after registration; tutors could pick up questions to answer. No personal data would be used or disclosed in the course of asking and answering questions. Nevertheless, Institution C would make use of tools like machine learning to match tutors with questions suitable for their levels and qualifications.

50. At the end of the trial period, children are required to purchase tutorial services of different value combinations to continue to ask questions through the App. The payment process was handled through a third-party payment platform. Institution C did not collect and use the credit card information provided by the children, but would give the remuneration to the designated bank account of the tutor.

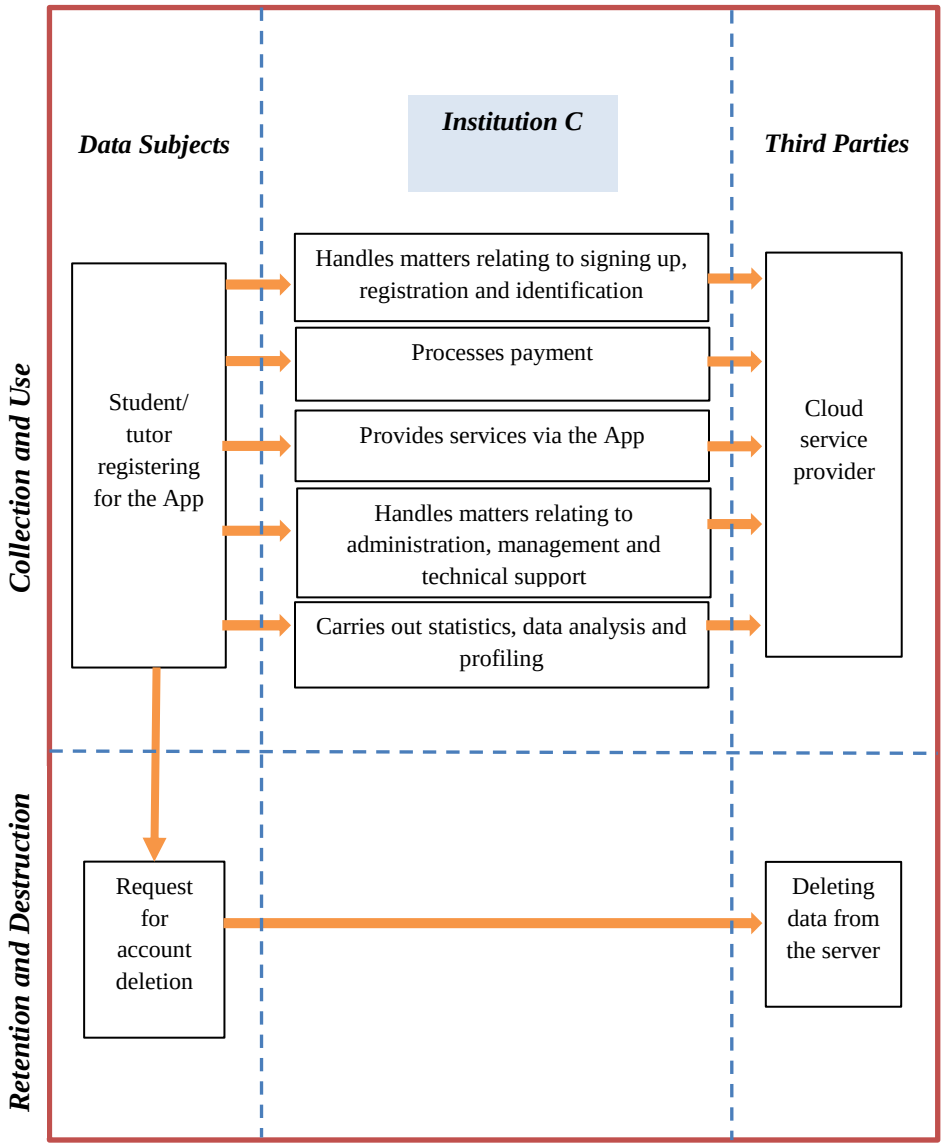
51. The personal data collected by Institution C would be used to:-

- handle matters relating to signing up, registration and identification;
- provide services via the App;
- handle matters relating to administration, management and technical support;
- process payment; and
- carry out statistics, data analysis and profiling.

iii) Retention and destruction of personal data

52. Institution C did not keep documentary form of personal data. The electronic form of users' personal data was stored in an external server operated by a cloud service provider. Users' data would be deleted if users submitted request of account deletion.

53. The flow of personal data of student and tutor is illustrated as follows:



(IV) Findings and Recommendations

Preliminaries

54. Findings and recommendations made in this Report are based on the information provided by the three institutions and the Team's on-site observations, which may not be exhaustive. They should be regarded only as a reflection of the compliance level of the matters in the Inspection.

55. In the Inspection, the Commissioner appreciated that the three institutions generally viewed the personal data of children, parents and tutors as important assets. They would not, as a matter of principle, handle or use the data indiscriminately. They were also committed to ensuring that the data was properly managed. However, institutions of different business models had different perceptions about the handling of personal data, resulting in different approaches to privacy protection measures. The institution which used the App as a platform to provide tutorial services relied on its own advantages by making use of information technology tools to carefully segment and monitor access rights to its computer systems so as to reduce the risk of unauthorised or disclosure of personal data. The Commissioner was pleased to see that the institution effectively used information technology tools to provide customer-oriented services, integrate privacy protection into product and service design and reduce the risk of privacy leakage.

56. The Commissioner noted that the three institutions had taken measures to protect personal data in their operational procedures and practices. However, only fragmented measures could be reflected, and data privacy protection was not included as part of their corporate governance. The Commissioner was of the view that responsible organisations should formulate and maintain a comprehensive privacy management programme as a matter of best practice.

Implementing the Privacy Management Programme to protect personal data privacy

57. Privacy Management Programme advocates that organisational data users should embrace personal data privacy protection as part of their corporate governance responsibilities and apply them as a business imperative throughout the organisation, covering business practices, operational processes, product and service design, physical architectures and network infrastructure, supported by an effective on-going review and monitoring process. Constructing a privacy management programme within an organisation takes careful planning and consideration across disciplines and job functions. Employees should be aware of and understand the applicability of the organisations' privacy management programme so as to add value to compliance with the requirements under the Ordinance.

a) Integrating the ideas of data privacy protection into corporate governance

	Institution A	Institution B	Institution C
Business model	Chain-run	Franchise	Online platform
No. of employees	About 300	About 200	About 15
Number of students/ tutors	About 279,000 students and 70 tutors	About 30,000 students and 150 tutors	About 103,000 students and 9,000 tutors
Staff who took up the data protection officer's role	No	Deputy General Manager	Operations Manager

58. Having top-level management to assume the role of data protection officer could lead the organisation to effectively manage and enforce personal data protection where, in particular, the three institutions were required to handle vast amount of personal data of children (and tutors).

It is worth noting that, Institutions B and C each appointed a designated staff from management to oversee privacy matters. The Commissioner particularly appreciated that Institution C, even as a start-up, had positively demonstrated commitment to privacy protection. Regardless of the size of the organsiation, the Commissioner strongly encouraged other private tutorial institutions to undertake the same organisational commitment.

Recommendation

1. The Commissioner highly encourages all private tutorial institutions (regardless of the mode of business or size of organisation) to integrate the ideas of data privacy protection into corporate governance; to demonstrate organisational commitment to personal data privacy; to designate a data protection officer from top management to oversee the privacy management programme and data protection matters, and to nurture the culture of respect privacy within the organisation.

b) Privacy by Design

59. To enhance the competitiveness and respond to the change of education needs in Hong Kong, private tutorial institutions continuously developed new services and marketing strategies. From the perspective of personal data protection, organisations should adopt "privacy by design" strategy to integrate privacy protection policy as a blueprint in the development of products or services and to define the corresponding privacy data type, processing method and risk control procedures based on its service type.

60. In the Inspection, the Commissioner noted impacts on private tutorial institutions operating in different business models varied. The App of Institution C was an online platform that heavily relied on information technology and network tools. Effective use of information technology tools appeared to have been utilized to serve its customers when designing new products and services which helped reduce the risk of data leakage. On the other hand, Institution A failed to access the

genuine needs when developing marketing events but collected children's social media accounts which were not functionally required. Besides, lack of review process of the relevant registration form led to unnecessary or excessive collection of personal data.

Recommendation

2. Private tutorial institutions should incorporate privacy protection when designing new products and services and assess the impact of launching such products and services on personal data privacy. They are encouraged to make effective use of information technology tools to provide customer-oriented services and reduce the risk of privacy leakage.

c) Formulating a comprehensive privacy policy and information security policy

61. Regardless of the business model or the size of the organisation, a comprehensive privacy policy would enable private tutorial institutions to implement and manage the process of collection, holding, processing, security, destruction and access to personal data throughout various departments. Regular review and update of the relevant policies should be carried out in response to the change of their operations or services.

	Institution A	**Institution B**	**Institution C**
Business model	Chain-run	Franchise	Online platform
Whether privacy policies or related guidelines were devised	Limited	For head office only	No
Whether information security policies were devised	Limited	No	For technical staff in Taiwan only

62. Based on the information obtained from the Inspection, the Commissioner considered that all three institutions had not put in place comprehensive privacy policies, as only fragmented measures could be reflected and data privacy management was not included as part of their corporate governance in that it was not adopted as a top-down business imperative throughout the organisation.

63. Institution A designated Human Resources Department to issue corporate directives to staff members. For instance, the department sent reminder emails to staff members in 2016 and 2017 directing the proper use of external portable storage devices and computer security matters for the purposes of avoiding the risk of personal data leakage and cyberattack. The Commissioner considered that these measures would undoubtedly enhance employees' awareness on personal data privacy. However, the formulation of the privacy policy should be more comprehensive and the guidelines should continue to be recirculated on a regular basis.

64. Moreover, Institution A had a control procedures manual[5] to regulate and control its information technology systems which included system sign in, password management, maintenance and security of computer system. Apart from the existence of the manual, it was only made available to senior management through the Intranet. The contents of which were not comprehensive in addressing all major information security issues or situations on personal data handling.

65. Although Institution B developed internal guidelines for the protection of personal data in 2017, they were only applicable to staff at head office instead of franchised tutorial centres despite the fact that they handled personal data of children regularly. The Commissioner considered that privacy policy should apply across the board of the organisation. Privacy policies and practices of branches or franchised tutorial centres (or other centres under different business models) of the same organisation should not deviate.

[5] Internal Controls Procedure Manual

66. In addition, the Team noted that some tutorial centres of Institution B had installed CCTV to ensure the safety of children. However, Institution B neither had policy on the installation or use of CCTV, nor supervision of CCTV surveillance. Meanwhile, Institution B did not formulate security policy to handle information security matters.

67. Institution C emphasized that risk of personal data privacy had already been taken into account at the design stage and default setting of products and services (e.g. by implementing controls on access and modification of information in the system). It considered that formulating a privacy policy was unnecessary. That said, it nevertheless had written policies on IT security and data access handling guidelines for technical staff in Taiwan. The Commissioner appreciated that Institution C integrated privacy by design in its products and operation. Being a responsible organisation, in any event, should not regard the formulation of a privacy policy as a repetitive or unnecessary task. Rather, privacy protection and information security measures should be incorporated so as to facilitate the understanding of and compliance by its staff members. This practice would not only benefit organisation's development but also foster employees' compliance with the requirements of privacy protection.

Recommendations

3. Regardless of the mode of business or the size of the organisation, private tutorial institutions should develop a comprehensive privacy policy on handling of personal data. The privacy policy must be applied by all departments and tutorial centres. All staff must be informed of the same in a timely manner to ensure that the organisation's system and measures for handling personal data are consistent. To cope with the social and business development, they should also review and update their privacy policies on a regular basis.

   The privacy policy should cover the collection, accuracy, retention, use, security measures and destruction procedures of personal data (both physical documents and electronic records), as well as the requirements

and operational procedures for handling direct marketing activities and opt-out requests.

4. As the current tutorial services rely heavily on information technology, a secure information technology system is of utmost importance. The private tutorial institutions should formulate relevant policies on information technology security to specify all information technology security measures and the practical policies for responding to relevant security risks.

d) Establishing effective reporting and data breach notification mechanism

	Institution A	**Institution B**	**Institution C**
Business model	Chain-run	Franchise	Online platform
Whether staff was designated to handle branch matters	Yes	Yes	Not applicable
Data breach notification mechanism	Insufficient	Insufficient	Yes

68. The Commissioner was pleased to know that Institution A and B had appointed designated departments and staff to handle the administrative matters of different tutorial centres. During the Inspection, it was noted that the inspected centres were well aware of how to report a data breach. Meanwhile, both institutions monitored tutorial centre's compliance with the relevant policies and requirements through conducting regular visits.

69. Nevertheless, the two institutions did not have in place any written guidelines or procedures to regulate the handling of data loss or breach incidents. The Commissioner considered that the formulation of clear and detailed written guidelines and procedures could help respond to such incidents promptly and take remedial measures in a timely manner

so as to avoid serious loss, given that, in particular, systems are vulnerable to cyberattacks in the digital world. Therefore, prompt response could reduce the impact and loss caused by the data breach incidents.

70. Institution C, which provided tutorial services through an online platform, was well aware of the risks associated with cyberattack and had developed a set of procedures and follow-up actions to deal with data breaches. During the interview, staff members of Institution C also demonstrated good understanding of the required procedures.

Recommendations

5. To cope with personal data privacy related matters, private tutorial institutions should establish an effective monitoring and reporting mechanisms to properly respond to the problems arising from the processing of personal data and to ensure compliance of privacy policies by their staff members.

6. Private tutorial institutions should develop a data breach notification mechanism setting out the process of handling data breach incidents (including the immediate assessment and measures to be taken to contain the breach and damage) and should designate personnel from top management to handle such incidents.

e) Enhancing employees' awareness of privacy protection through training and education

71. A sound privacy management programme requires all relevant members of an organisation to be aware of, and ready to act on personal data protection obligations. In the absence of employees' compliance, a privacy management system is ineffective. Therefore, employees should be constantly reminded to the compliance of the organisation's policies and programme controls.

	Institution A	Institution B	Institution C
Business model	Chain-run	Franchise	Online platform
Whether personal data privacy training has been provided	Newly recruited staff members only	Staff members in head office and centre instructors only	Newly recruited staff members only

72. In the Inspection, the Commissioner noted that Institution A and C would only provide personal data privacy training to new recruits. In addition, Institution C tended to rely on system tools to restrict the access rights to personal data and considered that regular training were unnecessary.

73. Institution B regularly provided seminars/ workshops in relation to the handling of personal data to head office and tutorial centres running on franchise basis. It also delivered to them general data protection education through periodic circulation of newsletters. Nevertheless, communication with individual centres was limited to franchisees only, which were required to distribute information to other staff within the centre. The Commissioner considered that such communication and training were not comprehensive enough.

Recommendation

7. To raise employees' awareness of privacy protection and to nurture the organisational culture of respecting privacy, private tutorial institutions should provide regular education and training to all employees (including franchisees and their employees). The comprehensive training and refresher courses for personal data protection should not be limited to professional training courses, practical tips through emails or corporate communications; but also relevant information provided online, etc.

Findings and Recommendations specific to the provisions of the Ordinance and Data Protection Principles

74. Apart from nurturing the culture of protect personal data through corporate governance and monitoring of compliance with the provisions of the Ordinance, the Commissioner noted from the Inspection that the operation of the three private tutorial institutions involved contravention of the requirements of the Ordinance and DPPs, and made recommendations as follows.

a) Ceasing collection of unnecessary or excessive personal data

	Institution A	Institution B	Institution C
Business model	Chain-run	Franchise	Online platform
Collection of unnecessary or excessive personal data	Yes	Yes	No

75. After reviewing the course application forms of Institutions A and B, the Team found that they involved excessive collection of children's personal data, including full date of birth.

76. To tie in with the marketing initiatives, Institution A used the application form to collect children's social media account without specifying whether it was necessary or voluntary. Meanwhile, no provision of any Personal Information Collection Statement or its equivalent in the application form could be found for the purpose of complying with DPP1(3) of the Ordinance.

77. Institution A would collect a copy of the HKID Card of elite students for the provision of scholarships; whereas they would collect HKID Card number from the online registration form when a free trial course was offered. For the sole purpose of verifying their identities, the Commissioner considered that the collection of their HKID Card

numbers or copies was unnecessary. Institution A could have used other alternatives to achieve the same purpose.

78. Institution C only collected a child's contact information when he registered through the App, and an individual who registered as a tutor was required to submit his contact information, copy of university student identity card and public examination results in order to ascertain that he was competent enough to teach the relevant subjects. Nevertheless, the App did not collect their credit card information. The Commissioner was satisfied that Institution C only collected minimum amount of personal data.

Recommendation

8. Private tutorial institutions should review their data collection practices:-

(i) They should cease collecting excessive or unnecessary personal data, amend the relevant forms and delete/destroy those data so collected;

(ii) They should provide a Personal Information Collection Statement on their registration or application forms so as to inform the children and their parents of the collection purposes and other notification requirements as stipulated in DPP 1(3); and

(iii) They should reduce the collection of personal data to the minimum according to the nature of the services provided.

b) Avoiding indefinite retention of personal data

	Institution A	Institution B	Institution C
Business model	Chain-run	Franchise	Online platform
Indefinite retention of personal data	Yes	Yes	Yes

79. The Commissioner was disappointed that the three private tutorial institutions had adopted a practice of retaining permanently the personal data of children and tutors albeit in different circumstances.

80. Institution A assigned a designated email account and a social media account to handle public enquiries. However, the content of the enquiries (involving personal data) was intended to be retained indefinitely.

81. When examining the staff computer workstations and network storage devices of Institution A, the Team also found that:

(i) Institution A had no mechanisms or technical controls in place to ensure that children's information stored in their workstations or network storage devices would be deleted in a timely manner; and

(ii) Electronic documents (including documents such as class attendance certificates and certificates of achievement) were retained indefinitely in the network storage device.

82. Institution B advised that they would permanently retain the personal data of discontinued students and former tutors for internal use. In addition, the Team also noted that some tutorial centres retained the course application forms of those discontinued students longer than necessary. The Commissioner considered that retaining personal data of discontinued students and former tutors for such a long period of time was not justifiable.

83. Institution C had no personal data retention policy that specified in detail the retention period of personal data. The Team discovered that dormant accounts were retained indefinitely in the system during the Inspection. Nevertheless, Institution C advised that if a user submitted a request to remove his personal data, the personal data stored in its database would be deleted.

Recommendation

9. Indefinite retention of personal data is contrary to the requirements of section 26 and DPP 2(2) of the Ordinance. The private tutorial institutions should establish a policy on retention of personal data, taking into account different types of data, storage media, the purpose of retaining the data, how to identify the data that has exceeded the retention period as well as the procedures and methods for destroying such data.

c) Using Personal Data properly

	Institution A	Institution B	Institution C
Business model	Chain-run	Franchise	Online platform
Inappropriate use of personal data	Yes	Yes	No

84. Institution A would print out a telephone list from the Enrolment System for emergency contact purposes but the list contained the children's HKID Card numbers. They would also generate a sit-in list from their Administration System at centres for class attendance who applied for sit-in lessons. The sit-in list contained children's partial HKID Card numbers as well. The Commissioner was of the view that the printing of HKID Card numbers for the purpose of communication and class attendance was unnecessary.

85. Institution B displayed the Lists of Advanced Students at the tutorial centres, the contents of which contained the names, results and grades of the students without obtaining prior consent of the children and their parents.

86. During the Inspection, the Team found no irregularities on the use of personal data by Institution C.

Recommendation

10. Private tutorial institutions should conduct a comprehensive review on the use of personal data to ensure that such use is consistent with or directly related to the purpose for which the data was originally collected, or has obtained prescribed consent from the data subjects concerned.

d) Improving personal data security mechanism

	Institution A	Institution B	Institution C
Business model	Chain-run	Franchise	Online platform
Level of personal data security protection	Low	Low	Medium

87. In general, internal controls and data security systems were put in place by the three institutions. However, during the course of the Inspection, the Team found inadequate security safeguards in their operations and systems.

88. Institution A had the following information security risks:

(i) HKID Card numbers were preset as the default log-in passwords for students to use online services;

(ii) Children's personal data (including HKID Card numbers and photos) was displayed in the relevant systems when recording attendance. However, the computers were placed in public areas, the contents of which could inadvertently be viewable by passers-by;

(iii) No comprehensive IT security policies were in place to govern the proper use of portable storage devices, use of encryption to protect data, password management, etc.;

(iv) Widely use of network attached storages to store personal data without central governance; and

(v) Logging and reporting mechanisms were not established to track users' activities.

89. Institution B had the following information security risks:

(i) Files containing study results of students and/ or personal data of potential franchisees were not encrypted during transmission;

(ii) Students' record books were easily accessible by the public as they were prominently placed at centres;

(iii) No comprehensive IT security policy has been developed; and

(iv) Documents containing personal data could be destroyed at home by a centre tutor without approval.

90. Institution C had the following information security risks:

(i) Personal data collected through the use of iOS platform of the App was not protected during transmission; and

(ii) Personal data being stored in the cloud would have relied solely on the security measures provided by the relevant cloud service provider.

Recommendation

11. Private tutorial institutions are increasingly relying on information technology systems to handle tutor-related services, preserve and manage relevant records and databases. Therefore, to maintain a healthy and secure operation of information technology systems to protect them from cyberattacks is as important as other physical security measures. They should:

(i) Develop physical security measures such as access control system, keep important documents in locked cabinets, etc. to prevent or deter unauthorised access and use of personal data;

(ii) Make use of technical measures such as encryption programmes,

system access management, identity authentication system, etc. to restrict and monitor access to personal data in the information technology systems; and

(iii) Develop a comprehensive information security policy which is supplemented by regular training to strengthen staff awareness on personal data privacy.

e) Adopting contractual means to manage data processor

	Institution A	**Institution B**	**Institution C**
Business model	Chain-run	Franchise	Online platform
Type of data processor engaged	Document disposal	Printing	Cloud service
Use contractual means to manage data processor	Yes	Yes	Yes

91. The Commissioner was satisfied that all three institutions had engaged data processors to regulate the retention and security of personal data through contractual means.

Recommendations

12. Apart from adopting contractual means to manage personal data entrusted to data processors, the private tutorial institutions should conduct regular monitoring and compliance checks to ensure data processors' compliance with the requirements of privacy protection.

13. When engaging major cloud service providers, private tutorial institutions should carefully assess the reliability of those providers, contents of their services, and whether the terms and conditions set out in the standard contracts meet all requirements of data protection. As a

matter of best practice, institutions should conduct a detailed privacy impact assessment to identity any potential privacy risks before entrusting their personal data to cloud service providers.

(V) Conclusion

92. The Inspection covered major business models of personal data systems of private tutorial institutions in Hong Kong and the data subjects' entire personal data life cycles from collection to destruction. The Commissioner noted that different business models of private tutorial institutions had different perceptions about the handling of personal data, resulting in different strengths and weaknesses in their personal data systems. For example, a technology-oriented tutorial institution relied on the use of system tools to restrict systems access in order to protect personal data. The Inspection aimed to let the entire private tutorial industry understand the best practice of protecting personal data, learn from one another in the industry, and improve its own policies and operating practices so as to comply with the provision of the Ordinance, adopt data governance and establish a culture of "protect and respect personal data privacy".

93. The European Union General Data Protection Regulation that came into force in May 2018 and strictly requires, inter alia, data controllers to protect personal data held by them through corporate governance. Although there are no similar laws and regulations in Hong Kong currently, it is undoubtedly a growing global trend to integrate protection of personal data privacy into corporate governance. Therefore, the Commissioner strongly encourages organisations to adopt a "Privacy Management Programme", details of which can be downloaded from: https://www.pcpd.org.hk/pmp/guide.html, to enhance corporate accountability and build mutual trust with customers to achieve a win-win situation in the process of handling personal data privacy.

94. Organisations that amass and derive benefits from personal data should not ditch their mindset of conducting their operations to meet the minimum regulatory requirements only. They should also be held to a higher ethical standard that meets stakeholders' expectation by doing what they should do. Data ethics and stewardship[6] can therefore bridge the gap between legal requirements and stakeholders' expectation.

[6] In August 2018, the Commissioner commissioned a consultancy to conduct a research study – The

95. The Commissioner would like to thank the three institutions and their staff for providing the Team with the opportunity to understand their personal data systems and the rationales behind their collection, retention and processing of personal data. He fully appreciates all the assistance rendered by them beyond their normal duties.

- End –

Legitimacy of Data Processing Project, to foster a culture of ethical data governance, a report on which can be downloaded from: https://www.pcpd.org.hk/misc/files/Ethical_Accountability_Framework.pdf

Annex 1 – Data Protection Principles (Schedule 1 to the Ordinance)

1. Principle 1 – purpose and manner of collection of personal data

(1) Personal data shall not be collected unless-

(a) the data is collected for a lawful purpose directly related to a function or activity of the data user who is to use the data;

(b) subject to paragraph (c), the collection of the data is necessary for or directly related to that purpose; and

(c) the data is adequate but not excessive in relation to that purpose.

(2) Personal data shall be collected by means which are-

(a) lawful; and

(b) fair in the circumstances of the case.

(3) Where the person from whom personal data is or is to be collected is the data subject, all practicable steps shall be taken to ensure that-

(a) he is explicitly or implicitly informed, on or before collecting the data, of-

(i) whether it is obligatory or voluntary for him to supply the data; and

(ii) where it is obligatory for him to supply the data, the consequences for him if he fails to supply the data; and

(b) he is explicitly informed-

(i) on or before collecting the data, of-

(A) the purpose (in general or specific terms) for which the data is to be used; and

(B) the classes of persons to whom the data may be transferred; and

(ii) on or before first use of the data for the purpose for which it was collected, of-

(A) his rights to request access to and to request the correction of the data; and

(B) the name or job title, and address, of the individual who is to handle any such request made to the data user,

unless to comply with the provisions of this subsection would be likely to prejudice the purpose for which the data was collected and that purpose is specified in Part 8 of this Ordinance as a purpose in relation to which personal data is exempt from the provisions of data protection principle 6.

2. Principle 2 – accuracy and duration of retention of personal data

(1) All practicable steps shall be taken to ensure that-

(a) personal data is accurate having regard to the purpose (including any directly related purpose) for which the personal data is or is to be used;

(b) where there are reasonable grounds for believing that personal data is inaccurate having regard to the purpose (including any directly related purpose) for which the data is or is to be used-

(i) the data is not used for that purpose unless and until those grounds cease to be applicable to the data, whether by the rectification of the data or otherwise; or

(ii) the data is erased;

(c) where it is practicable in all the circumstances of the case to know that-

(i) personal data disclosed on or after the appointed day to a third party is materially inaccurate having regard to the purpose (including any directly related purpose) for which the data is or is to be used by the third party; and

(ii) that data was inaccurate at the time of such disclosure,

that the third party-

(A) is informed that the data is inaccurate; and

(B) is provided with such particulars as will enable the third party to rectify the data having regard to that purpose.

(2) All practicable steps must be taken to ensure that personal data is not kept longer than is necessary for the fulfilment of the purpose (including any directly related purpose) for which the data is or is to be used.

(3) Without limiting subsection (2), 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.

(4) In subsection (3)—

data processor (資料處理者) means 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.

3. Principle 3 – use of personal data

(1) Personal data shall not, without the prescribed consent of the data subject, be used for a new purpose.

(2) A relevant person in relation to a data subject may, on his or her behalf, give the prescribed consent required for using his or her personal data for a new purpose if—

(a) the data subject is—

(i) a minor;

(ii) incapable of managing his or her own affairs; or

(iii) mentally incapacitated within the meaning of section 2 of the Mental Health Ordinance (Cap 136);

(b) the data subject is incapable of understanding the new purpose and deciding whether to give the prescribed consent; and

(c) the relevant person has reasonable grounds for believing that the use of the data for the new purpose is clearly in the interest of the data subject.

(3) A data user must not use the personal data of a data subject for a new purpose even if the prescribed consent for so using that data has been given under subsection (2) by a relevant person, unless the data user has reasonable grounds for believing that the use of that data for the new purpose is clearly in the interest of the data subject.

(4) In this section—

new purpose (新目的), in relation to the use of personal data, means any purpose other than—

(a) the purpose for which the data was to be used at the time of the collection of the data; or

(b) a purpose directly related to the purpose referred to in paragraph (a).

4. Principle 4 – security of personal data

(1) All practicable steps shall be taken to ensure that personal data (including data in a form in which access to or processing of the data is not practicable) held by a data user are protected against unauthorized or accidental access, processing, erasure, loss or use having particular regard to-

(a) the kind of data and the harm that could result if any of those things should occur;

(b) the physical location where the data is stored;

(c) any security measures incorporated (whether by automated means or otherwise) into any equipment in which the data is stored;

(d) any measures taken for ensuring the integrity, prudence and competence of persons having access to the data; and

(c) any measures taken for ensuring the secure transmission of the data.

(2) Without limiting subsection (1), 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.

(3) In subsection (2)—

data processor (資料處理者) has the same meaning given by subsection (4) of data protection principle 2.

5. Principle 5 – information to be generally available

All practicable steps shall be taken to ensure that a person can-

(a) ascertain a data user's policies and practices in relation to personal data;

(b) be informed of the kind of personal data held by a data user;

(c) be informed of the main purposes for which personal data held by a data user is or is to be used.

6. Principle 6 – access to personal data

A data subject shall be entitled to-

(a) ascertain whether a data user holds personal data of which he is the data subject;

(b) request access to personal data-

(i) within a reasonable time;

(ii) at a fee, if any, that is not excessive;

(iii)in a reasonable manner; and

(iv) in a form that is intelligible;

(c) be given reasons if a request referred to in paragraph (b) is refused;

(d) object to a refusal referred to in paragraph (c);

(e) request the correction of personal data;

(f) be given reasons if a request referred to in paragraph (e) is refused; and

(g) object to a refusal referred to in paragraph (f).

<u>Annex 2</u> – Use of personal data in direct marketing (ss.35B - 35H of the Ordinance)

35B. Application

This Division does not apply in relation to the offering, or advertising of the availability, of—

(a) social services run, subvented or subsidized by the Social Welfare Department;

(b) health care services provided by the Hospital Authority or Department of Health; or

(c) any other social or health care services which, if not provided, would be likely to cause serious harm to the physical or mental health of—

(i) the individual to whom the services are intended to be provided; or

(ii) any other individual.

35C. Data user to take specified action before using personal data in direct marketing

(1) Subject to section 35D, a data user who intends to use a data subject's personal data in direct marketing must take each of the actions specified in subsection (2).

(2) The data user must—

(a) inform the data subject—

(i) that the data user intends to so use the personal data; and

(ii) that the data user may not so use the data unless the data user has received the data subject's consent to the intended use;

(b) provide the data subject with the following information in relation to the intended use—

(i) the kinds of personal data to be used; and

(ii) the classes of marketing subjects in relation to which the data is to be used; and

(c) provide the data subject with a channel through which the data subject may, without charge by the data user, communicate the data subject's consent to the intended use.

(3) Subsection (1) applies irrespective of whether the personal data is collected from the data subject by the data user.

(4) The information provided under subsection (2)(a) and (b) must be presented in a manner that is easily understandable and, if in written form, easily readable.

(5) Subject to section 35D, a data user who uses a data subject's personal data in direct marketing without taking each of the actions specified in subsection (2) commits an offence and is liable on conviction to a fine of $500000 and to imprisonment for 3 years.

(6) In any proceedings for an offence under subsection (5), it is a defence for the data user charged to prove that the data user took all reasonable precautions and exercised all due diligence to avoid the commission of the offence.

(7) In any proceedings for an offence under subsection (5), the burden of proving that this section does not apply because of section 35D lies on the data user.

35D. Circumstances under which section 35C does not apply

(1) If, before the commencement date—

(a) a data subject had been explicitly informed by a data user in an easily understandable and, if informed in writing, easily readable manner of the intended use or use of the data subject's personal data in direct marketing in relation to a class of marketing subjects;

(b) the data user had so used any of the data;

(c) the data subject had not required the data user to cease to so use any of the data; and

(d) the data user had not, in relation to the use, contravened any provision of this Ordinance as in force as at the time of the use,

then section 35C does not apply in relation to the intended use or use, on or after the commencement date, of the data subject's relevant personal data, as updated from time to time, in direct marketing in relation to the class of marketing subjects.

(2) If—

(a) a data subject's personal data is provided to a data user by a person other than the data subject (***third person***); and

(b) the third person has by notice in writing to the data user—

(i) stated that sections 35J and 35K have been complied with in relation to the provision of data; and

(ii) specified the class of marketing subjects in relation to which the data may be used in direct marketing by the data user, as consented to by the data subject,

then section 35C does not apply in relation to the intended use or use by the data user of the data in direct marketing in relation to that class of marketing subjects.

(3) In this section—

commencement date (本部生效日期) means the date on which this Part comes into operation;

relevant personal data (有關個人資料), in relation to a data subject, means any personal data of the data subject over the use of which a data user had control immediately before the commencement date.

35E. Data user must not use personal data in direct marketing without data subject's consent

(1) A data user who has complied with section 35C must not use the data subject's personal data in direct marketing unless—

(a) the data user has received the data subject's consent to the intended use of personal data, as described in the information provided by the data user under section 35C(2)(b), either generally or selectively;

(b) if the consent is given orally, the data user has, within 14 days from receiving the consent, sent a written confirmation to the data subject, confirming—

(i) the date of receipt of the consent;

(ii) the permitted kind of personal data; and

(iii) the permitted class of marketing subjects; and

(c) the use is consistent with the data subject's consent.

(2) For the purposes of subsection (1)©, the use of personal data is consistent with the data subject's consent if—

(a) the personal data falls within a permitted kind of personal data; and

(b) the marketing subject in relation to which the data is used falls within a permitted class of marketing subjects.

(3) A data subject may communicate to a data user the consent to a use of personal data either through a response channel or other means.

(4) A data user who contravenes subsection (1) commits an offence and is liable on conviction to a fine of $500000 and to imprisonment for 3 years.

(5) In any proceedings for an offence under subsection (4), it is a defence for the data user charged to prove that the data user took all reasonable precautions and exercised all due diligence to avoid the commission of the offence.

35F. Data user must notify data subject when using personal data in direct marketing for first time

(1) A data user must, when using a data subject's personal data in direct marketing for the first time, inform the data subject that the data user must, without charge to the data subject, cease to use the data in direct marketing if the data subject so requires.

(2) Subsection (1) applies irrespective of whether the personal data is collected from the data subject by the data user.

(3) A data user who contravenes subsection (1) commits an offence and is liable on conviction to a fine of $500000 and to imprisonment for 3 years.

(4) In any proceedings for an offence under subsection (3), it is a defence for the data user charged to prove that the data user took all reasonable precautions and exercised all due diligence to avoid the commission of the offence.

35G. Data subject may require data user to cease to use personal data in direct marketing

(1) A data subject may, at any time, require a data user to cease to use the data subject's personal data in direct marketing.

(2) Subsection (1) applies irrespective of whether the data subject—

(a) has received from the data user the information required to be provided in relation to the use of personal data under section 35C(2); or

(b) has earlier given consent to the data user or a third person to the use.

(3) A data user who receives a requirement from a data subject under subsection (1) must, without charge to the data subject, comply with the requirement.

(4) A data user who contravenes subsection (3) commits an offence and is liable on conviction to a fine of $500000 and to imprisonment for 3 years.

(5) In any proceedings for an offence under subsection (4), it is a defence for the data user charged to prove that the data user took all reasonable precautions and exercised all due diligence to avoid the commission of the offence.

(6) This section does not affect the operation of section 26.

35H. Prescribed consent for using personal data in direct marketing under data protection principle 3

Despite section 2(3), where a data user requires, under data protection principle 3, the prescribed consent of a data subject for using any personal data of the data subject in direct marketing, the data user is to be taken to have obtained the consent if the data user has not contravened section 35C, 35E or 35G.

Annex 3 – A summary of a privacy management programme

- End of Report -