Protect, Respect Personal Data

Guidance on Election Activities

PCPD
HK

PCPD.org.hk

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

For Candidates and their Affiliated Political Bodies

- Only adequate and necessary personal data for election purposes should be collected
- Ensure the individuals are informed of the purpose of collection of the data
- Inform the electors about how their personal data was obtained when being asked
- Should not collect personal data for election purposes by deceptive means or by misrepresenting the purpose of the collection
- Political bodies should give prior notification to members that their personal data will be used for election purposes when their personal data was collected
- Prior consent from the electors must be obtained if the personal data was obtained for non-election purposes
- Ensure the personal data from published registers of electors is used only for election purposes as prescribed by the relevant election legislation
- Consider carefully before using personal data obtained from the public domain
- Electors should be given an option to decline receipt of any electioneering communication from the candidates
- Maintain a list of individuals who find election-related communication objectionable, and avoid approaching them to canvass for votes
- Safeguard electors' personal data collected
- Should not retain personal data collected for election purposes for a period beyond completion of election activities

Case 1

After completing a training course organised by a political party, the complainant was asked to complete a questionnaire and provide his personal data for "communication purposes". Subsequently, the political party used the complainant's personal data in canvassing him to vote for a candidate.

In response to the complaint, the party revised the Personal Information Collection Statement in the questionnaire by explicitly stating that the personal data collected would be used for "election purposes"

Case 2

A resident of a building lodged a complaint with a political party in relation to the management of the building, and for this purpose supplied his personal data. Subsequently, the political party used his personal data in canvassing him to vote for a candidate in an election.

In response to the complaint, the political party undertook in future to obtain express and voluntary consent from any resident that had lodged a complaint with the party, before using their personal data for election purposes.

Case 3

A backup notebook computer of a government department prepared for use in an election was discovered missing at the fallback election venue. The computer stored the names of Election Committee members eligible to vote in the election, and also the personal data of all electors in Hong Kong.

The Privacy Commissioner considered that the assessment and approval of the use of an enquiry system containing the electors' data was not well thought out or adapted to the special circumstances of the case. The government department had simply followed past practices and had failed to review, update or appraise the existing mechanism in light of the circumstances, in a timely manner. The government department lacked the requisite awareness and vigilance expected of it in protecting personal data. Rules of application and implementation of various guidelines had not been clearly set out or followed, and internal communication was not sufficiently effective. An enforcement notice was served on the government department to remedy and prevent recurrence of the contravention.

For the Relevant Government Departments

Conducting Activities of Elector Registration and Updating Registration Particulars:

- Take practicable steps to safeguard personal data collected in the activity against accidental or unauthorised access
- Return data to the office or deliver it to a safe place for proper storage as soon as possible after the activity

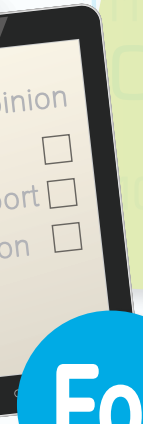
Managing Database of Electors:

- Encrypt the database
- Only keep those personal data that are necessary for access or use in portable storage devices
- Only authorised staff are able to retrieve or access personal data
- Strictly evaluate the necessity of downloading and copying electors' personal data
- Record all activity logs of the systems
- Install monitoring and alarm mechanisms for timely reporting and record tracing
- Risk assessment should be conducted before storing electors' personal data in portable storage devices.

  If it is necessary after assessment:
  - ◆ Encrypt data and adopt effective technical security measures, e.g. two-factor authentication
  - ◆ Effect adequate physical security measures to safeguard devices

Establishing Security Policies, Procedures and Practical Guidelines:

- Systematically review and update relevant policies, procedures and guidelines
- Effectively disseminate to all staff
- Set up procedures of proper recording of movements of electoral documents, retrieval systems and dossier reviews
- Formulate and review a compliance check mechanism



For Public Opinion Research Organisations

- It is generally not necessary for public opinion research organisations to indiscriminately collect the respondents' personal data
- Even when the collection of personal data is needed, organisations should not provide untrue or misleading information concerning the background and objectives of the opinion polls
- Clearly state the nature of the activities and identify the data user to the participants
- Conduct risk assessment to ensure the personal data collected is appropriately protected when employing the use of computer programmes or software developed by third parties
- Destroy the personal data collected within a reasonable time after completion of activities

For Members of the Public - Personal Data Protection Advice

- Verify senders' identities for emails or letters in relation to election
- Exercise due care in submitting the completed elector registration form. For example, the envelope should be properly sealed and the information of recipients should be input correctly
- Indicate that emailing is preferred for receiving electioneering communications from the candidates
- Convey objection to receiving electioneering communications to the candidates and their affiliated political bodies
- Report the change of registration particulars to the relevant authority as soon as possible for record update
- Ascertain if the organisers of opinion polls have clearly stated the nature of the activities, their identities and the purpose of personal data collection, etc.
- Ascertain whether the data collected by political bodies during their activities will be used in subsequent elections
- Should not give up personal data for small gains. Before providing personal information, read the Personal Information Collection Statement and the privacy policy first, and get to know the other party's identity and background, as well as their purposes of collection, the classes of transferees, etc.
- If you believe that your personal data have been collected or used improperly, you can consider raising your queries and negotiating with the individuals or organisations concerned. If you are dissatisfied with the individuals' or organisations' response, you can complain to the PCPD.

* For details, please refer to the content of *Guidance on Election Activities for Candidates, Government Departments, Public Opinion Research Organisations and Members of the Public.*

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

PCPD website
pcpd.org.hk

Enquiry Hotline : **(852) 2827 2827**
Fax : **(852) 2877 7026**
Address : **Unit 1303, 13/F, Dah Sing Financial Centre, 248 Queen's Road East, Wanchai, Hong Kong**
Email : **communications@pcpd.org.hk**

Download this publication

First published in June 2000
April 2004 (First Revision)
February 2007 (Second Revision)
April 2010 (Third Revision)
October 2011 (Fourth Revision)
August 2015 (Fifth Revision)
December 2017 (Sixth Revision)
June 2020 (Seventh Revision)
July 2023 (Eighth Revision)

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

Guidance on Election Activities for Candidates, Government Departments, Public Opinion Research Organisations and Members of the Public

1. Introduction

Collection, retention, processing and use of personal data are usually involved in election activities (including elector registration, candidate nomination, electioneering, public opinion researching, and casting and counting of votes). This guidance note provides assistance to candidates and their affiliated political bodies, government departments and public opinion research organisations in relation to compliance with the requirements under the Personal Data (Privacy) Ordinance (the Ordinance) when carrying out election activities. It also provides members of the public with advice on personal data protection in this regard.

2. Legal Liabilities of Candidates, Government Departments and Public Opinion Research Organisations as Principals

Candidates, government departments and public opinion research organisations (the Principals) may engage election agents, campaign staff, full-time or part-time employees, contractors and volunteers (the Agents) to assist in election-related activities. In such circumstances, the Principals are liable for the acts and practices of their Agents in the course of performing actions assigned by them[1]. The Principals are responsible for supervising their Agents to ensure compliance with the requirements under the Ordinance.

3. Guidance for Candidates and their Affiliated Political Bodies

Minimum Data Collection

3.1 When candidates collect personal data directly from an individual or indirectly from a third party (e.g. trade union, professional or political body) for election purposes (such as electioneering, organising an election forum, or fund raising), only adequate, and not excessive personal data, necessary for election purposes should be collected (for example, a Hong Kong Identity Card number should not be collected)[2].

Informed Collection

3.2 When a candidate or affiliated trade union, professional or political body solicits personal data directly from an individual for election purposes, the candidate should ensure that the individual is informed of the purpose of collection of the data and other matters[3] set out in the Ordinance by, for example, providing a "Personal Information Collection Statement" (PICS) to the individual.

---

1 According to section 65(1) and (2) of the Ordinance, any act done or practice engaged in by a person in the course of his employment or as agent for another person with the authority of that other person shall be treated as done or engaged in by his employer or that other person as well as by him.

2 Data Protection Principle 1(1): Personal data shall not be collected unless the data is collected for a lawful purpose directly related to a function or activity of the data user; and the data collected is necessary, adequate but not excessive in relation to that purpose.

3 Data Protection Principle 1(3): On or before a data user collects personal data directly from a data subject, the data user shall take all reasonably practicable steps to ensure that the data subject has been informed of whether it is obligatory or voluntary for him to supply the data and the consequences for him if he fails to supply the data. The data subject shall be explicitly informed of the purpose of data collection and the classes of transferees to whom the data may be transferred as well as the name / job title and address of the individual to whom the request of access to and correction of the data subject's personal data may be made.

3.3 Candidates and their Agents may lobby electors by a variety of means[4]. In certain circumstances, the electors may have no previous dealings with the candidates and their Agents, and may be concerned as to where the candidates and their Agents obtained their personal data. When asked, candidates and their Agents should inform the electors as to how their personal data was obtained.

Case 1

A candidate of the District Council election collected feedback from members of the public on community affairs by distributing flyers. In the flyer, members of the public were requested to provide their names and contact details. However, there was no PICS in the questionnaire and some members of the public were worried about how their personal data would be used.

When the candidate solicited personal data directly from individuals (such as by distributing a flyer for filling in personal data), the candidate should have provided a PICS to the individuals so that they could decide whether their personal data should be provided.

Case 2

The Election Committee members of a subsector, and Legislative Councillors of the functional constituency concerned, co-organised an election forum to provide a platform for electors of that subsector to exchange ideas on candidates' manifestoes. A complainant was dissatisfied that the organisers had failed to provide a PICS on the online registration form.

In response to the complaint, the forum organisers revised the online registration form by stating that personal data collected would be used only for enrolling participants, and the data would be destroyed after the event without it being transferred to third parties. Information on making data access and data correction requests was also made available on the registration form.

Lawful and Fair Collection

3.4 Candidates should not collect personal data for election purposes by deceptive means or by misrepresenting the purpose of the collection, for example, by collecting personal data on the pretext of assisting citizens to apply for government welfare.[5]

Collection Purpose

3.5 If a trade union, or a professional or political body intends to provide their members' personal data to candidates for election purposes, or to directly send election-related communication to their members, the proper course of action is for such bodies to determine whether this is a permitted purpose for which the personal data was collected. Prior notification to members of such use of their data, and the classes of possible transferees of the data, should be provided.

Case 3

After completing a training course organised by a political party, the complainant was asked to complete a questionnaire and provide his personal data for "communication purposes". Subsequently, the political party used the complainant's personal data in canvassing him to vote for a candidate.

In response to the complaint, the party revised the PICS in the questionnaire by explicitly stating that the personal data collected would be used for "election purposes".

Case 4

The complainant had been a member of a trade union for years. In a recent election, the complainant received a telephone call from the trade union canvassing votes for a candidate. The complainant stated that the trade union had never informed him that his personal data would be used for election purposes when he joined the union.

Upon the PCPD's enquiry, it was found that the latest version of the PICS in the membership application form had stated that the trade union would use the members' personal data for election purposes. However, the trade union did not provide the latest version of the PICS to those members who had their membership renewed. The PCPD thus requested the trade union to provide the latest version of the PICS to the members when they renewed their membership in future.

[4] Such as telephone, fax messages, SMS/MMS or emails.

[5] Data Protection Principle 1(2): Personal data must be collected by means which are lawful and fair in the circumstances of the case.

Express Consent

3.6 Personal data may have been provided to candidates and their Agents for non-election purposes, such as in connection with the handling of building management matters, or requests for assistance. Should candidates or their Agents wish to use personal data so collected for an election purpose, express consent from the data subject must be obtained beforehand[6].

Case 5

A resident of a building lodged a complaint with a political party in relation to the management of the building, and for this purpose supplied his personal data. Subsequently, the political party used his personal data in canvassing him to vote for a candidate in an election.

In response to the complaint, the political party undertook in future to obtain express and voluntary consent from any resident that had lodged a complaint with the party, before using their personal data for election purposes.

Disclosing personal data on social media

3.7 Social networks are rapidly evolving and developing. It is becoming common for political bodies, district councillors and community officers to provide information relating to the district to the residents and to stay connected with them through social media. Political bodies and district councillors must ensure that the personal data privacy of the residents is protected when sharing information that involves personal data.

Case 6

The PCPD has received complaints against councillors for not respecting the residents' privacy, for example, by uploading photos or videos which contained close-up facial images of individuals involved in disputes in the neighbourhood, or by disclosing the full addresses of patients confirmed of having contracted epidemic diseases.

The PCPD understands that councillors or political bodies may from time to time report on the local affairs in the community through social media, upload photos to reflect actual situations, or provide information to residents for combatting pandemic. However, if the information contains an individual's facial image, full address or any other personal data, councillors should take into account the data subject's wish and feeling. Individual's privacy right should be respected when sharing information on topical affairs and incidents on the social media.

Registers of Electors

3.8 When using personal data from published registers of electors, candidates should ensure that such personal data is used only for election purposes as prescribed by the relevant election legislation. Using any information on the register for a purpose other than a purpose related to an election is an offence under the current electoral legislations and is liable to a fine at level 2 (the prevailing amount is HK$5,000) and to imprisonment for 6 months.

3.9 Besides, the PCPD noted that the Court of Appeal handed down a judgment on 21 May 2020 and a decision on 27 May 2020 regarding an appeal[7] regarding the dismissal of an application for judicial review on whether the requirement of showing the names of the registered electors together with their principal residential addresses ("Linked Information") in the electoral registers for public inspection or provision to candidates is constitutional[8]. The Court of Appeal held, amongst others, that displaying the Linked Information of

---

6 Data Protection Principle 3: Personal data shall not, without the prescribed consent of the data subject, be used for a new purpose. New purpose, in relation to the use of personal data, means any purpose other than the purpose, or a directly related purpose, for which the data was to be used at the time of the collection of the data.

7 Junior Police Officers' Association of the Hong Kong Police Force and Anor (as the applicants) v Electoral Affairs Commission, Chief Electoral Officer, Electoral Registration Officer (as the respondents) Hong Kong Journalists Association (as the intervener) (CACV 73/2020, Date of Judgment: 21 May 2020).

8 In this appeal, the applicants challenged the constitutionality of section 20(3) of the Electoral Affairs Commission (Registration of Electors) (Legislative Council Geographical Constituencies) (District Council Geographical Constituencies) Regulation (Cap.541A) and Section 38(1) of the Electoral Affairs Commission (Electoral Procedure) (District Councils) Regulation (Cap.541F) (together as "Impugned Provisions"). Under the Impugned Provisions, the Linked Information of a registered elector as recorded in the Final Register would be available (1) to the public for inspection at place(s) specified by the Electoral Registration Officer and (2) to the candidate(s) for the District Council geographical constituency to which the elector belongs.

electors in the electoral registers to an individual's right to privacy and is thus protected generally under Article 14 of section 8 in Part II of the Hong Kong Bill of Rights Ordinance[9] (c.f. from Article 17(1) of the International Covenant on Civil and Political Rights). Hence, the requirement of displaying publicly the names and residential addresses of some individuals (for example victims of stalking or family violence) may cause a real risk of harm to them. As the ultimate guardian of the law, the Court of Appeal is obliged to consider if a proportionate balance is struck between the right of privacy and the right to vote (particularly the measures adopted in the current electoral system to achieve the transparent election aim)[10]. Nevertheless, the Court of Appeal also ruled that it is not its function to formulate electoral policy or to devise a particular electoral system.

3.10 In order to combat doxxing and protect citizens' personal data privacy, two offences targeting on doxxing took effect on 8 October 2021 pursuant to the Personal Data (Privacy) (Amendment) Ordinance 2021. If any person discloses any personal data of electors (as data subject) on the register without the relevant consent of the data subject, with an intent to cause specified harm[11] or being reckless as to whether specified harm would be caused to the data subject or any family member of the data subject, the discloser commits an offence under section 64(3A) of the Ordinance and is liable to a fine of HK$100,000 and imprisonment for 2 years. If such disclosure causes specified harm to the data subject or any family member of the data subject, the discloser commits an offence under section 64(3C) of the Ordinance and is liable to a fine of HK$1,000,000 and imprisonment for 5 years.

Personal Data in Other Public Domains

3.11 Other than for the register of electors, personal data available in the public domain (such as professional registers) is generally not intended to be used for election purposes. Before using personal data obtained from the public domain, candidates must take into account the original purpose for which the public register was established, the restrictions on its use, and the reasonable privacy expectation[12] of the data subjects.

Option to Decline

3.12 As a matter of good practice, when candidates and their Agents canvass for votes from individuals directly, or indirectly through a third party (such as a trade union, or a professional body or political body), the individuals should be given an option to decline receipt of any subsequent electioneering communication from the candidates in relation to the election concerned, so as to avoid receipt of unwanted electioneering communication from such candidates.

List of "No"

3.13 Candidates should also maintain a list of individuals who, to their knowledge, find election-related communication, such as phone calls, mail, fax messages, emails or visits, objectionable, and avoid approaching them to canvass for their votes.

Data Security

3.14 When conducting election activities, candidates and their Agents should take all practicable steps to protect personal data of electors against accidental or unauthorised access[13]. For example, they should safeguard electors' personal data that they have obtained from the register of electors or government departments (such as a DVD of the "Candidate Mailing Label System", and mailing labels of electors). If it is absolutely necessary to access electors' information outside office premises for an election purpose, only the minimal and necessary data should be taken away from the office premises. Furthermore, the data should be encrypted and protected from unauthorised access or retrieval. After use, the data should be returned to the office, or be delivered to a safe place for proper storage as soon as possible.

---

9 Article 14 of section 8 in Part II of the Hong Kong Bill of Rights Ordinance (Cap. 383): (1) No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. (2) Everyone has the right to the protection of the law against such interference or attacks.

10 See paragraphs 95-96 of the judgment.

11 According to section 64(6) of the Ordinance, "specified harm", in relation to a person, means (a) harassment, molestation, pestering, threat or intimidation to the person; (b) bodily harm or psychological harm to the person; (c) harm causing the person reasonably to be concerned for the person's safety or well-being; or (d) damage to the property of the person.

12 Reference can be made to the *Guidance on Use of Personal Data Obtained from the Public Domain* issued by the office of the Privacy Commissioner for Personal Data, Hong Kong (PCPD).

13 Data Protection Principle 4(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 is protected against unauthorised or accidental access, processing, erasure, loss or use.

Case 7

A district councillor sent an email to a list of recipients canvassing votes for a candidate in an election without concealing the names and email addresses of the recipients. The complainant, being one of the recipients of that email, complained that his name and email address had been disclosed to all other recipients of the email.

In response to the complaint, the district councillor agreed to safeguard the security of the personal data of the electors when transmitting messages via electronic means (for example, by use of the "bcc" function).

Data Disposal

3.15 Personal data collected for election purposes should not be retained for a period beyond completion of all the election activities[14]. For example, after an election, candidates should dispose of all the electors' personal data obtained from a published register of electors, or those provided by government departments for election purposes. When data processors[15] are appointed or engaged by the candidates to destroy personal data of electors on their behalf, the candidates must use contractual or other means to prevent the personal data being transferred to data processors from: (i) being kept longer than is necessary for election purposes[16]; and (ii) unauthorised or accidental access, processing, erasure, loss or use[17].

Distributing or Providing Assistance in Purchasing Supplies

3.16 Political bodies and councillors may from time to time distribute supplies to the residents and they may collect the residents' personal data for identification purposes. Political bodies and councillors should respect the residents' privacy and comply with the Ordinance when collecting, using and retaining the residents' personal data.

Case 8

Political bodies, councillors and community officers provided assistance in purchasing anti-epidemic items through the internet or distributed anti-epidemic items to members of the public at roadside booths. This aroused a number of privacy concerns:

1) Even if there is a practical need for the organiser to collect personal data, for instance for the purposes of registration, compiling a waiting list, and collection or delivery of products, the organiser should collect the minimum amount of personal data in a lawful and fair manner[18]. As in the circumstances of shopping in the supermarket, providers of goods and services should not collect personal data that is unrelated to the transactions. Hence, the organiser should not collect data that is unrelated to and unnecessary for the transactions or delivery (for example, date of birth, income, family status, family members' personal data and identity card copy).

2) No matter whether the organiser collects personal data through paper or electronic form, the organiser should inform members of the public of the purpose of collection, the classes of transferees and whether it is obligatory or voluntary to supply the data[19]. The good practice is to provide a PICS to them.

3) The organiser should not use the personal data collected for other purposes without the data subjects' consent[20] (for example, for purposes other than the directly related purposes for which the data was collected, including marketing of commercial products or to advance political publicity)[21]. If the organiser intends to use the personal data collected for other purposes, the organiser should explain clearly to the data subject and seek the data subject's consent. The consent given by the data subject must be express and voluntary.

---

14 Data Protection Principle 2(2): Personal data shall not be kept longer than is necessary for the fulfillment of the purpose (including any directly related purpose) for which the data is or is to be used.

15 "Data processor" means a person who processes personal data on behalf of another person; and does not process the data for any of the person's own purposes. Reference can be made to the information leaflet *Outsourcing the Processing of Personal Data to Data Processors* issued by the PCPD.

16 Data Protection Principle 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 any personal data transferred to the data processor from being kept longer than is necessary for processing of the data.

17 Data Protection Principle 4(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 unauthorised or accidental access, processing, erasure, loss or use of the data transferred to the data processor for processing.

18 See footnote 2 and footnote 5.

19 See footnote 3.

20 See footnote 6.

21 Except for those scenarios that are exempted under Part 8 of the Ordinance.

Case 8 (continued)

4) For the retention period of personal data, notwithstanding that the Ordinance does not require data users to inform data subjects of the retention period of personal data, data users are required to erase personal data that is no longer needed for the purpose for which the data is used[22]. Hence, the organiser should erase the personal data collected after distributing the supplies or providing the services (in other words, after fulfilling the purpose for which the data is used), in order to avoid potential data security problem.

4. Guidance for the Relevant Government Departments

Security Measures

4.1 In campaigns launched by government departments for the purpose of promoting elector registration or updating electors' particulars, such activities may involve collection of personal data in paper form (such as collection of elector registration forms at pavement booths). Government departments should take practicable steps to safeguard personal data so collected against accidental or unauthorised access by unrelated parties[23]. For example, the responsible staff should be alert to data leakage risks in the surroundings when receiving completed forms. If notebook computers / tablets or portable storage devices are used, extra care must be taken (see paragraph 4.3 below for more details). The data should be returned to the office or delivered to a safe place for proper storage as soon as possible upon completion of the activities.

4.2 Government departments should, at all times, adopt all practicable security measures to protect the voluminous and sensitive personal data of electors held by them against unauthorised or accidental access, processing, erasure, loss or use[24]. In addition to encrypting the database, government departments should also:

- Make available the personal data for access or use only on a "need-to-know" and "need-to-use" basis, especially when portable storage devices, such as notebook computers, are involved;
- Adopt the principle of least-privileged rights, by which only staff authorised to handle identity verification are able to retrieve or access relevant personal data;
- Strictly evaluate the necessity of downloading and copying electors' personal data, and establish approval procedures and standards;
- Monitor to ascertain if any system containing electors' personal data has been downloaded or copied without authorisation. Such systems and related servers should record all activity logs in order to trace access, use, downloading, editing and / or deletion of the data by a system user; and
- Install monitoring and alarm mechanisms in all systems containing electors' personal data, and the related servers, so that if there is an irregularity (such as downloading or deletion of huge volume of personal data), timely reporting of the case, as well as tracing and reviews can be performed.

4.3 In circumstances when accessing electors' personal data outside office premises is required, a risk assessment should be conducted to ascertain the actual need of storing electors' personal data in portable storage devices (such as in USB flash cards, notebook computers / tablets, portable hard drives or optical discs). If it is necessary to store electors' personal data by such means, effective technical security measures commensurate with the quantity and sensitivity of the data should be adopted by, for example, use of two-factor authentication for data access. Adequate physical security measures should also be effected to safeguard devices (such as affixing the device with a cable lock to an appropriate fixture, or avoidance of departmental logos on the devices)[25].

4.4 Government departments should formulate, systematically review and update their current personal data security policies, procedures and practical guidelines, according to their functions and activities. Steps should be taken to effectively disseminate personal data security policies to all staff, and provide clear instructions as to how to access such policies. Government departments should also review and formulate a compliance check mechanism to ensure personal data security policies, procedures and practical guidelines are complied with.

[22] See footnote 14.

[23] See footnote 13.

[24] See footnote 13.

[25] Reference can be made to the *Guidance on the Use of Protable Storage Devices* issued by the PCPD.

4.5 The multiple transfers and storage venues for the election documents increased the risk and harm of losing the documents. For the purposes of monitoring and reviewing the implantation of the security measures, government departments should set up procedures in respect of proper recording of movements of electoral documents, retrieval systems and dossier reviews.

Case 9

A backup notebook computer of a government department prepared for use in an election was discovered missing at the fallback election venue. The computer stored the names of Election Committee members eligible to vote in the election, and also the personal data of all electors in Hong Kong.

While the Privacy Commissioner for Personal Data, Hong Kong (Privacy Commissioner) considered the chance of leakage being low, as the personal data of the electors involved had already undergone multiple layers of encryption, the assessment and approval of the use of an enquiry system containing the electors' data was not well thought out or adapted to the special circumstances of the case. The data user had simply followed past practices and had failed to review, update or appraise the existing mechanism in light of the circumstances, in a timely manner. The investigation revealed that the data user lacked the requisite awareness and vigilance expected of it in protecting personal data. Rules of application and implementation of various guidelines had not been clearly set out or followed, and internal communication was not sufficiently effective. The data user failed to take all reasonably practicable steps in consideration of the actual circumstances, or to ensure that electors' personal data was protected from accidental loss, and thereby contravened Data Protection Principle 4(1)[26] of the Ordinance. An enforcement notice was served on the government department to remedy and prevent recurrence of the contravention[27].

Case 10

A government department lost a marked final register of electors after an election. The register contained the unique and sensitive information about electors' identity card numbers and their polling statuses.

The Privacy Commissioner found that there were no specific guidelines or standing procedures as security standards for managing the marked final register. Its inventory and movements were not properly and adequately documented. There were no dossier reviews, and retrieval systems for storerooms were not put in place .

In addition, human errors in handling physical and tangible records of personal data could have been caused by overly long work hours, scarce resources, inexperienced or under-trained staff, etc. The Privacy Commissioner served an Enforcement Notice to direct the government department to remedy and prevent any recurrence of the contraventions.

4.6 When handling requests for information that involve the personal data of individuals, including electors, candidates or nominees, government departments must carefully assess if the release of the requested information would amount to a breach of Data Protection Principle 3[28]. In making such a determination, the exemptions provided in Part 8 of the Ordinance[29] are applicable. If necessary, more information may be sought from the requestor to facilitate appropriate consideration.

5. Guidance for Public Opinion Research Organisations

Informed Collection

5.1 Public opinion research organisations may conduct opinion polls to gauge public views on candidates' approval ratings or electors' voting preferences. An elector's voting preference is considered to be very sensitive personal data, and organisers of these activities should exercise due care to ensure that participants are informed of the purpose of collecting the personal data, and other matters required by the Ordinance[30].

---

26 See footnote 13.

27 The investigation report (R17-6249) is available on the PCPD website.

28 See footnote 6.

29 If application of Data Protection Principle 3 is likely to prejudice security, defence and international relations; crime prevention or detection; assessment or collection of any tax or duty; news activities; health; legal proceeding; due diligence exercise; handling life-threatening emergency situation, the relevant personal data is exempt from the use limitation requirements.

30 See footnote 3.

5.2 For the purpose of gauging public views on candidates' approval ratings and the electors' voting preferences, public opinion research organisations need only the overall results of the survey and some macro parameters (for example, gender, age group, occupation categories, area of residence and income group). Hence, it is generally not necessary for the public opinion research organisations to indiscriminately collect the respondents' personal data (such as names, identity card numbers, telephone numbers and addresses). If data subjects are asked to provide these kinds of personal data for research purpose, they must check clearly the purpose of collection before considering to disclose such data, and should do so only on a well-informed and voluntary basis.

Case 11

A complainant provided his personal data in a signature campaign organised by a political body. He noticed that the purpose of collecting the personal data and data transfer arrangement was not stated on the form used for collecting personal data. According to the organiser, it had indicated on the form that "the personal data was collected solely for expressing views, and it would be destroyed afterwards".

In response to the complaint, the organiser undertook to take all practicable steps to supply relevant information to the participants in similar future events launched, including, for instance, the purpose for which the data was to be used, whether it was obligatory or voluntary for participants to provide the data, the classes of person to whom the data might be transferred, and their right to request access to a copy of their personal data and to request correction of the data.

Lawful and Fair Collection

5.3 When collecting personal data in opinion polls, organisers should carefully assess if the means of data collection could confuse or mislead the participants. Vigilance should be exercised to avoid providing untrue or misleading information concerning the background and objectives of the activities. If the organisers fail to identify themselves as the data user to the participants, or fail to state the nature of the activities clearly (e.g. whether the activities are "official" or "of legal effect"), this could amount to unfair collection of personal data[31].

Data Security

5.4 If collection of personal data is involved, organisers of opinion polls should still safeguard personal data collected against accidental or unauthorised access by unrelated parties.[32] When employing the use of computer programmes or software developed by third parties, assessment should be made to identify possible privacy risks (including, for example, the security issues related to data transmission and storage, technical safeguards of the system and network, and the restriction on data access by staff). Measures should be taken to ensure the personal data collected is appropriately protected.

Data Disposal

5.5 Organisers should not retain personal data collected in opinion polls after completion of these activities[33]. If data processors are appointed or engaged by the organisers to destroy the personal data of participants on their behalf, the organisers must comply with the relevant requirements under the Ordinance (see paragraph 3.15 above).

6. Personal Data Protection Advice for Members of the Public

6.1 Upon receipt of emails or letters soliciting personal data in relation to election, members of the public must verify senders' identity to ensure there is no fraudulent collection of personal data in the name of government departments.

6.2 In submitting the completed elector registration form to the relevant authority, due care must be exercised regardless of the means of submission. For example, the envelope should be properly sealed and the information of recipients should be input correctly.

6.3 Members of the public may indicate on the elector registration form that emailing is their preference for receiving electioneering communications from the candidates. Otherwise, the email address provided would only be used by the relevant authority for communication purposes.

6.4 Electors may exercise their right to object to receipt of electioneering communications from the candidates and their affiliated political bodies.

6.5 Electors who have changed their registration particulars should report the change to the relevant authority as soon as possible for the record update.

[31] See footnote 5.

[32] See footnote 13.

[33] See footnote 14.

6.6 If participants of opinion polls need to provide personal data, they must ascertain if the organisers of these activities have clearly stated the nature of the activities (e.g. whether the activities are "official" or "of legal effect") and identified themselves. Participants are also reminded to check if the organisers have provided them with information such as the purpose of collecting the personal data, and other matters required by the Ordinance[34]. In case of doubts, enquiries should be made to the organisers.

6.7 If personal data is collected by political bodies in their activities such as distribution of or providing assistance in making purchases of supplies, the participants should ascertain whether the data collected will be used in subsequent elections. If the participants do not consent to such use, they should not provide their personal data.

6.8 Members of the public should not give up their personal data for small gains. Personal data belongs to the data subjects themselves. They are advised to be vigilant about protecting their own personal data. Before providing personal information through whatever channels, they should first read the PICS and the privacy policy, and get to know the other party's identity and background, as well as their purposes of collection, the classes of transferees and whether the other party is collecting excessive personal data, etc.

6.9 If members of the public believe that their personal data have been collected or used improperly, they can consider raising their queries and negotiating with the individuals or organisations concerned. If they are dissatisfied with the individuals' or organisations' response, they can complain to the PCPD.

7. A Final Note

In view of the huge volume and sensitive nature of the personal data collected or used in election activities, candidates, government departments, public opinion research organisations and members of the public must make the best efforts to avoid leakage.

Data users are recommended to formulate a policy on data breach handling and the giving of breach notifications[35]. In the unfortunate event of a data breach, data users should consider issuing notifications to lessen the harm caused by the breach.

The PCPD stands ready to offer assistance and respond to data breach notifications to all stakeholders. For enquiries, please visit our website from which all publications referred to in this guidance can be downloaded, or call our hotline at 2827 2827.

[34] footnote 3.

[35] Reference can be made to the *Guidance on Data Breach Handling and Data Breach Notifications* issued by the PCPD.

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

PCPD.org.hk

PCPD website
pcpd.org.hk

Download this publication

Enquiry Hotline : **(852) 2827 2827**
Fax : **(852) 2877 7026**
Address : **Unit 1303, 13/F, Dah Sing Financial Centre, 248 Queen's Road East, Wanchai, Hong Kong**
Email : **communications@pcpd.org.hk**

Disclaimer

The information and suggestions provided in this publication are for general reference only. They do not serve as an exhaustive guide to the application of the law and do not constitute legal or other professional advice. The Privacy Commissioner makes no express or implied warranties of accuracy or fitness for a particular purpose or use with respect to the information and suggestions set out in this publication. The information and suggestions provided will not affect the functions and powers conferred upon the Privacy Commissioner under the Personal Data (Privacy) Ordinance.

First published in June 2000
April 2004 (First Revision)
February 2007 (Second Revision)
April 2010 (Third Revision)
October 2011 (Fourth Revision)
August 2015 (Fifth Revision)
December 2017 (Sixth Revision)
June 2020 (Seventh Revision)
July 2023 (Eighth Revision)