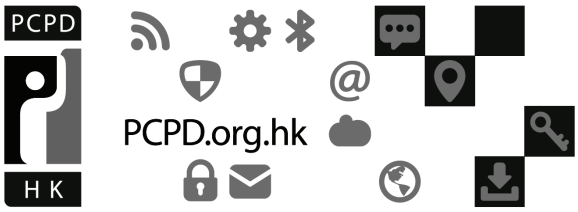

Guidance Note

香港個人資料私隱專員公署
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

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 2

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".

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 3

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.

Registers of Electors

3.7 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 and to imprisonment for 6 months.

---

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

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.

Personal Data In Other Public Domains

3.8 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[7] of the data subjects.

Option to Decline

3.9 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"

3.10 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

3.11 When conducting election activities, candidates and their Agents should take all practicable steps to protect personal data of electors against accidental or unauthorised access[8]. 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.

Case 4

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

3.12 Personal data collected for election purposes should not be retained for a period beyond completion of all the election activities[9]. 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[10] 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[11]; and (ii) unauthorised or accidental access, processing, erasure, loss or use[12].[13]

---

7 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)

8 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.

9 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.

10 "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.

11 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.

12 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.

13 Reference can be made to the information leaflet *Outsourcing the Processing of Personal Data to Data Processors* issued by the PCPD

4. Guidance for the Relevant Government Departments

Security Measures

4.1 In campaigns launched by government departments for the purpose of promotion of elector registration or the updating of electors' particulars, such activity 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[14]. 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). After the activity, the data should be returned to the office or delivered to a safe place for proper storage as soon as possible.

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[15]. 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 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 should be adopted commensurate with the quantity and sensitivity of the data 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)[16].

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.

---

[14] See footnote 8

[15] See footnote 8

[16] Reference can be made to the *Guidance on the Use of Portable Storage Devices* issued by the PCPD

Case 5

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 name 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 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) [17] of the Ordinance. An enforcement notice was served on the government department to remedy and prevent recurrence of the contravention[18].

4.5 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[19]. In making such a determination, the exemptions provided in part 8 of the Ordinance[20] 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 or mock 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[21].

Case 6

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 is 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 is to be used, whether it is obligatory or voluntary for participants to provide the data, the classes of person to whom the data may be transferred, and their right to request access to a copy of their personal data and to request correction of the data.

17 See footnote 8

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

19 See footnote 6

20 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.

21 See footnote 3

Lawful and Fair Collection

5.2 When collecting personal data in opinion or mock 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[22].

Case 7

A political body commissioned a public opinion research organisation to launch a mock poll during the election, but the website of the activity did not state clearly that the mock poll was "non-official" or "of no legal effect."

Furthermore, despite the claim on the website that the research team was commissioned by a political association to launch the activity, other parties or associations had publicly stated that they were involved in planning or participating in the activity. While the website carried the emblem of a university and a contact email with the university's domain name, there was a footnote in small print stating the activity was unrelated to the university. No clear explanation of the purpose and lawful basis for the data collection was given by the activity organiser, and the true identity of the data user was not made known. The Privacy Commissioner took the view that such a manner of collection of personal data was unfair.

After intervention by the Privacy Commissioner, the activity organiser stated on the website: the purpose of collecting the participants' personal data; made clear to the participants that the activity was initiated by community organisations; and it had no connection with the official election and the result was of no legal effect. Information related to the university, including the university's emblem and email domain name, were deleted from the website and the name of the organiser was clearly stated.

Data Security

5.3 If collection of personal data is involved, organisers of opinion or mock polls should safeguard personal data collected against accidental or unauthorised access by unrelated parties.[23] 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.

Case 7 (continued)

In this case, before casting their votes in a mock poll, participants were required to install an instant messaging programme for identity verification, and then input in the voting system their password used for the said programme. By giving away the password, participants had in effect allowed third parties to read the messages they had sent or received with the programme. A security loophole was thus created.

Subsequently, to remedy the security problem revealed in this case, the organiser replaced the voting system in question.

Data Disposal

5.4 Organisers should not retain personal data collected in opinion or mock polls after completion of these activities[24]. 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 3.12 above).

[22] See footnote 5

[23] See footnote 8

[24] See footnote 9

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.

6.6 If participants of opinion or mock 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[25]. In case of doubts, enquiries should be made to the organisers.

6.7 If personal data is collected by political bodies in their activities, participants should ascertain whether the data collected will be used in subsequent elections. If participants do not consent to such use, they should not provide their personal data.

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[26]. In the unfortunate event of a data breach, data users should consider issuing notifications to lessen the harm caused by the breach.

The office of the Privacy Commissioner for Personal Data, Hong Kong 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.

[25] See footnote 3

[26] Reference can be made to the *Guidance on Data Breach Handling and the Giving of Breach Notifications* issued by the PCPD

PCPD.org.hk

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

First published in 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)