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

Guidance Note

Guidance on Use of Personal Data Obtained from the Public Domain

Purpose of this guidance

This Guidance Note is intended to assist data users to comply with the requirements under the **Personal Data (Privacy) Ordinance** (the "**Ordinance**") when collecting and using personal data from the public domain.

Personal data available in public domain

Personal data can be accessed and obtained from the public domain through different channels, e.g. a public register, a public search engine or a public directory, etc. A data user may do so for compiling information about an individual whom it targets or seeks to identify.

Below are some examples of use of personal data available in the public domain:

Examples:

1. A market research company uses personal data obtained from a public telephone directory to conduct surveys and publish reports.
2. A business entity provides its corporate customers with composite personal data of individuals aggregated from different public information sources.
3. An organisation develops a master index to facilitate the search by users of information it has compiled about an identified individual from websites, media releases, etc.

It is a misconception that publicly accessible personal data can be further used or disclosed for any purpose whatsoever without regulation. The protection afforded by the Ordinance does apply to such personal data and there is no general exemption from compliance with the requirements under the Ordinance.

The legal requirements

A data user who collects and uses personal data from the public domain must observe the requirements under the Ordinance, in particular, **Data Protection Principle ("DPP") 1(2)** and **DPP3**.

DPP1(2) requires personal data to be collected by means which are lawful and fair in the circumstances of the case. **DPP3** specifies that personal data shall not, without the prescribed consent of the data subject, be used for a new purpose. The term, "new purpose" in relation to the use of personal data, means in essence any purpose other than the one for which the personal data was originally collected or a directly related purpose. "Prescribed consent" means consent that is expressly and voluntarily given and has not been withdrawn by the data subject in writing. The term "use" in relation to personal data includes the disclosure and transfer of the data.

According to judicial authority, DPP3 "*is directed against the misuse of personal data and it matters not that the personal data involved has been published elsewhere or is publicly available. This is entirely consistent with the objective of the [Ordinance] to protect personal data*"[1].

[1] See judgment given by Hon Chu JA in *Re Hui Kee Chun, CACV 4/2012, at para 52*. The case concerns the publication on websites information regarding the full name, name of the employer and job position of a staff member in an educational institute along with a link to certain recorded conversations.

A data user who intends to use personal data obtained from the public domain for direct marketing activities has to comply with **Part VI A** of the Ordinance and obtain the consent of the data subjects[2].

Section 64 of the Ordinance stipulates that a person commits an offence if he/she discloses any personal data of a data subject which was obtained from a data user without the latter's consent and with an intent to (i) obtain gain for himself/herself or another person, or (ii) cause loss to the data subject. It is also an offence if the unauthorised disclosure causes psychological harm to the data subject[3].

Example:

A person downloads some intimate photos of a known individual from a public website. Despite his/her understanding that the photos were leaked as a result of a data breach by the data user, he/she compiles an album of these intimate photos and sells to others for profit.

Common circumstances where personal data is made available in the public domain

There are various reasons for making personal data publicly accessible. The following are some common situations:

- To comply with the statutory or legal requirement of public inspection of personal data of, for example, registered voters, registered owners of properties and company directors
- To facilitate contact and verification of the identity of professionals and officials by checking the relevant public directories
- Public records, news reporting and public announcements to serve the public interest

Collection of personal data by lawful and fair means

Data users who make personal data available in the public domain may specify the circumstances or impose restrictions under which personal data may be accessed and used. It may limit the kind of persons making access and the purposes of use of the data. A person who collects personal data from the public domain regardless of these stipulations and restrictions may contravene DPP1(2).

Example:

The Transport Department provides Certificates of Particulars of Motor Vehicle upon application. The application form stipulates that "applicants should only use personal data of the registered owner provided by the certificate for activities relating to traffic and transport matters". The Department requires the applicant to declare the purpose of requesting the Certificate by ticking the relevant checkbox provided in a declaration form before allowing access to personal data. An applicant made a false declaration by choosing one of the checkboxes, namely "for litigation purpose". His/her actual purpose was to use the personal data for direct marketing. The applicant had infringed DPP1(2)[4].

Use of personal data

Due regard must be given to the data user's original purposes of making the personal data available in the public domain. The restrictions, if any, imposed by the data users on further uses and the reasonable expectation of personal data privacy of the data subjects must be observed. The fact that a data subject's personal data can be obtained from the public domain shall not be taken to mean that the data subject has given blanket consent for use of his/her personal data for whatever purposes.

---

[2] Contraventions of the requirements under Part VI A are offences. For contraventions involving the provision of personal data for gain, the maximum penalty is a fine of HK$1 million and imprisonment for 5 years. For other contraventions, the maximum penalty is a fine of HK$500,000 and imprisonment for 3 years. See *New Guidance on Direct Marketing* issued by the Commissioner which is available at www.pcpd.org.hk/english/publications/files/GN_DM_e.pdf.

[3] The maximum penalty for these two new offences is a fine of HK$1 million and imprisonment for 5 years. See *Information Leaflet: Offence for disclosing personal data obtained without consent from the data user* issued by the Commissioner which is available at www.pcpd.org.hk/english/publications/files/offence_disclosing_e.pdf.

[4] See *Investigation Report No.R12-3428* published by the Commissioner which is available at www.pcpd.org.hk/english/publications/files/R12_3428_e.pdf.

Relevant factors in assessing the permitted purposes of use

Before using personal data obtained from the public domain, it is necessary to take into account the following factors in assessing the permitted purposes of use in order not to infringe DPP3:–

I. The original purpose for which the personal data was placed in the public domain

A public register is usually established for a stated purpose. The purpose can often be ascertained from the enabling legislation, or is explicitly stated in the privacy policy statement and/or the personal information collection statement of the operator of the public register. The operator may also use administrative measures to specify the purposes of use, e.g. stating the conditions of use in a search application form or incorporating relevant terms and conditions in a contract granting bulk access to the personal data, etc.

Examples:

1. The Securities and Futures Commission maintains a register of licensed persons under the Securities and Futures Ordinance, Cap 571 *"for the purpose of enabling any member of the public to ascertain whether he is dealing with a licensed person in matter of or connected with any regulated activity and to ascertain the particulars of the licence of such person"*. The permitted purpose of use should relate to this stated purpose.

2. The Registrar of Marriage is required to exhibit the notice of intended marriage for inspection by the public under the Marriage Ordinance, Cap 181. The permitted purpose of use is to enable any person who has the right to object to raise objection to the proposed marriage.

3. A register of licensed estate agents and salespersons is established by the Estate Agents Authority and available for inspection under the Estate Agents Ordinance, Cap 511. The permitted purpose of inspecting the register is to allow a member of the public to ascertain that he/she is dealing with a licensed person in a property transaction.

4. The Medical Council is required under the Medical Registration Ordinance, Cap. 161 to maintain a General Register and a Specialist Register containing the names of medical practitioners, their addresses and qualifications. The purpose is to inform the public that each person named in the list is qualified to practise in Hong Kong.

Any use of the personal data which goes beyond the purpose for establishing the register or its directly related purpose may contravene DPP3, and in some instances, may constitute an offence under the relevant ordinance.

Example:

The use of voters' personal data kept in a register of electors for any purpose other than a purpose related to the election is an offence under the relevant Electoral Affairs Commission Regulations.

II. The restrictions, if any, imposed by the data user for further uses

In some public telephone directories maintained by organisations or professional bodies in respect of its employees or members, the permitted purpose of use may be explicitly limited to making official or business contact with these individuals only.

Example:

The names and contact details of government officials are published in the Government telephone directory which is available for public inspection. The directory contains a use restriction clause which specifies that the information is (a) provided to facilitate official communication between the Government of the HKSAR and related organisations and the public; and (b) not intended to be used for direct marketing activities and should not be transferred for commercial gain.

III. *The reasonable expectation of the personal data privacy of the data subjects*

When the original purpose of the data is not stated or is not clear, the Commissioner's stand point is that it is relevant to consider the reasonable expectation of personal data privacy of the individuals for assessing the lawful use of the personal data under DPP3.

A data subject has legitimate privacy expectation about the uses of his/her personal data. Any use that goes beyond the reasonable privacy expectation of the data subject is unlikely to be accepted as a related purpose of use under DPP3. The test is whether a reasonable person in the data subject's situation would find the re-use of the data unexpected, inappropriate or otherwise objectionable, taking into account all factors in the circumstances.

The following are factors (non-exhaustive) that affect an individual's privacy expectation:

The sensitivity of the personal data

Financial data, biometric and health data, litigation and criminal records, sexual preferences, etc. are sensitive personal data. Generally, it is reasonable for the data subject to expect that these kinds of personal data are to be used discretely and for limited purposes. The use of such data without the knowledge of the data subject and without providing the data subject with the opportunity to rectify any data inaccuracy could be a problem that needs to be addressed. In case of doubt, it is advisable to obtain the express and voluntary consent of the data subject before making further uses of the sensitive personal data.

The realistic risks of harm: identity theft, financial loss, harassment, injury to feelings

The name, date of birth and the identification document number of an individual are perfect ingredients for committing an identity crime. When they are used by ill-intentioned people with other information, such as one's credit card data, address and password, it can cause financial loss to the individual.

The circumstances under which the personal data is disclosed affect the severity of the privacy risks of the personal data. For instance, if the personal data is disclosed online on a website which is accessible by any person, the privacy risk associated with such disclosure would be very high. It follows that the higher the risks of harm to the data subject, the more likely that the further use of his/her personal data is beyond the data subject's reasonable expectation, hence falling outside the permitted use under DPP3.

Example:

The unrestricted disclosure of the name and residential address of the data subject online will expose the data subject to risks to his/her personal safety, such as stalking and surveillance.

The commercial use of the personal data

A data subject may be legally required to provide his/her personal data to a data user who in turn makes the data publicly available pursuant to statutory requirements. Such arrangement is intended to attain a purpose that is beneficial to the data subject (e.g. to protect his/her proprietary interest in a land property through registering title documents with the Land Registry) and serving the public interest (e.g. prevention of fraudulent property transactions).

However, where the personal data is further used for commercial purposes which do not serve the interest of the data subject, the data subject may find it objectionable.

Examples:

1. The sales approaches to an individual using contact information published on a list of licensed professionals. As the purpose of the list is for a member of the public to ascertain that the person with whom he/she is dealing is a licensed person, the use of the data for door-to-door sale of products and services unrelated to his/her professional work is likely regarded as a new purpose.

2. A service company consolidates and collates the personal data obtained from the Transport Department's register of vehicles and provides a value-added service to enable the search of all registered vehicles owned by an individual. The use of the personal data falls outside the statutory purpose of the register of vehicles maintained by the Transport Department as well as the reasonable expectation of personal data privacy of the vehicle owners.

The combining, re-arranging and/or matching of personal data from different public sources for profiling which result in function creep and inaccurate inferences being made against the data subject

Personal data obtained from different public sources can be combined to assist the profiling of an individual or compilation of information about an individual. The act of profiling itself is not prohibited under the Ordinance. However, since the primary purpose for which the personal data is made accessible is unique for each information source, the profiling of an individual would be a new purpose which may fall outside the reasonable expectation of personal data privacy of the data subject.

The combining, re-arranging and/or matching of personal data may also increase the risks of function creep, i.e. the use of the personal data by subsequent data users for a new purpose. For example, unbeknown to the data subject, his/her personal data may be collected and relied upon by other data users in decisions that may potentially affect him/her adversely such as when being considered for a job.

Example:

Integrity checking service targeting individuals involved in bankruptcy and criminal proceedings at different times as subscribers to the service may unfairly draw an adverse inference against the individuals.

In the process of combining, re-arranging and/or matching personal data, a data user may fail to ensure the accuracy of the personal data.

Example:

Personal data of an individual may be mismatched with the information about another person who bears the same or similar name. As a result, an individual who is not a party to a legal proceeding may be mistakenly linked up.

Exemptions under the Ordinance

The Ordinance specifically provides for exemptions from the application of DPP3 under **Part VIII**. The following are some of the relevant exemptions that may be invoked by a data user when using personal data obtained from the public domain for a new purpose:

- **Section 52** (domestic purposes): where personal data is held by an individual and is (i) concerned only with the management of his/her personal, family or household affairs; or (ii) held only for recreational purposes
- **Section 58** (crime, etc.): where personal data is used for the purpose of prevention or detection of crime or for prevention, preclusion or remedying of unlawful or serious improper conduct or dishonesty or malpractice by persons, etc.
- **Section 59** (health): the disclosure of the identity, location and health data (physical or mental) of a data subject where non disclosure may likely cause serious harm to the physical or mental health of the data subject or any other individual
- **Section 60B** (legal proceedings): where the use of the personal data is required or authorised by Hong Kong law or in connection with any legal proceedings in Hong Kong or is required for establishing, exercising or defending legal rights in Hong Kong
- **Section 61** (news): The disclosure of personal data by a person to a data user whose business consists of a news activity and there is reasonable ground for that person to believe that the publication or broadcasting of the personal data is in the public interest
- **Section 62** (statistics and research): where personal data is used for preparing statistics or carrying out research and the resulting statistics or research does not identify the data subjects
- **Section 63C** (emergency situation): where the use of the personal data is to identify an individual who is reasonably suspected to be, or is involved in a life-threatening situation and to carry out emergency rescue operations or providing emergency relief services

A data user should be mindful that the burden of proof that the use of the personal data is so exempted lies on the data user who wishes to apply the exemption.

Example:

A company provides asset search service to a law firm retained by a judgment creditor to locate the assets of an individual debtor for the purpose of executing a judgment debt. The personal data provided by the company may fall within an exempted purpose under the Ordinance (e.g. section 60B, for exercising legal rights in Hong Kong) but the company must take steps to ensure that the provision of personal data is lawful under the Ordinance.

Other obligations under the Ordinance

A data user who intends to amass personal data obtained from the public domain for further uses must observe all the legal requirements under the Ordinance. Steps should be taken to ensure that the personal data held by it is accurate (**DPP 2(1)**) and not retained for longer than necessary for fulfilment of the purpose of use (**DPP2(2)**), that appropriate security measures are in place to protect the personal data from unauthorised or accidental access, processing, erasure, loss or use (**DPP4**), that its privacy policy and practice is transparent (**DPP5**) and that the data subject's rights of access to and correction of his/her personal data are duly observed (**DPP6**).

Recommended best practices

The following are recommended best practices for a data user to safeguard the personal data privacy of data subjects:

Data users as operators of public registers or directories

- Assess privacy risks (such as by carrying out privacy impact assessment[5]) before determining whether or not to provide online access to public registers or directories

- Avoid disclosing/displaying together the name and the personal identifier, (e.g. HKID number of an individual) in a manner that increases the risks of misuse, e.g. where such data is uploaded onto a public website for unrestricted access by members of the public
- The amount of personal data that is made publicly accessible shall be limited to what is necessary. For instance, the residential address of the individuals may not be necessary when a correspondence address is sufficient to attain the purpose. Also, the disclosure of part of a residential address and part of an identification document number may suffice in place of the full residential address and full identification document number
- Consider implementing the following administrative and technological measures to safeguard the personal data:

  (i) stating the purposes of use and restrictions on further uses of the personal data in an easily understandable and readable manner

  (ii) controlling access to personal data and limiting the disclosure of personal data on a need-to-know basis

  (iii) preventing automated programmed search of personal data

  (iv) when designing an index to facilitate search by users of the personal data, restricting massive downloads and limiting the field of the query or the query criteria so that information is provided to the extent authorised. A blanket disclosure of all available personal data may be unnecessary and excessive. Disclosure of personal data not in accordance with the original intention of the data user should be avoided (e.g. not allowing query of property transactions in the Land Registry using a person's name, otherwise all property interests of a single individual would be identified)

  (v) if bulk downloads of personal data are allowed, consider using contractual or other means to impose a clear prohibition against the manipulation of the data, such as not allowing new search keys and stating the consequences of breach (e.g. termination of contract)

  (vi) consider whether or not to exclude public search engines from indexing your public register or directory as some public search engines may only be capable of selecting and presenting partial information about an individual from your website and this lack of comprehensiveness of data could be misleading, e.g. the public search engine may only reveal information about an individual being prosecuted but it may not include any information about his/her acquittal

[5] Privacy impact assessment is generally regarded as a systematic risk assessment tool which can be usually integrated into a decision making process to evaluate a proposal in term of its impact upon personal data privacy. See *Information Leaflet on Privacy Impact Assessments* issued by the Commissioner, available at www.pcpd.org.hk/english/publications/files/PIAleaflet_e.pdf.

Data users who intend to collect and use personal data from the public domain

- Do not make further use of the sensitive personal data of the data subject in a manner that takes away or is inconsistent with the protection afforded to him/her by law. For instance, it may be inappropriate for a data user to publish the names and identifying particulars of individuals and their spent conviction records as it would affect their right of rehabilitation conferred by law[6]
- Do not combine, re-arrange or match personal data originally collected for different purposes with the result of increasing the risks of misinterpretation of the personal data and inaccurate inferences being made against the data subjects
- Consider implementing administrative and technological measures to ensure that further use of the data by third parties is consistent with or directly related to the original purpose of disclosure of data in the public domain, or in line any of with the exemptions under the Ordinance.
- Obtain the prescribed consent of the data subject for a new purpose of use of the personal data, particularly when the personal data is of a sensitive nature
- Afford the data subject the right to verify the accuracy of the personal data and insofar as it is practicable to do so, to honour the data subject's request to erase or suppress his/her personal data from a combined or linked up database built for a new purpose for safety and privacy reasons
- Do not unduly rely on information collected from the public domain about a data subject in a decision affecting him/her adversely and deprive him/her of the right to object and to correct any inaccurate data

End Note

It should be firmly borne in mind all personal is protected by the Ordinance. Just because it is readily accessible from the public domain does not make any difference. Data users should carefully handle personal data in a manner consistent with the data protection principles and other requirements under the Ordinance.

Office of the Privacy Commissioner for Personal Data, Hong Kong
Tel: (852) 2827 2827
Fax: (852) 2877 7026
Address: 12/F, 248 Queen's Road East, Wanchai, Hong Kong
Website: www.pcpd.org.hk
Email: enquiry@pcpd.org.hk

[6] Under section 2 of the Rehabilitation of Offenders Ordinance, Cap 297, the failure of a rehabilitated individual to disclose his/her conviction shall not be a ground for dismissing or excluding him/her from any office, profession, occupation or employment.