



Proper Handling of Data Access Request and Charging of Data Access Request Fee by Data Users

Executive Summary

This guidance note covers the following four areas:

1 What is a data access request (“DAR”)

- A DAR in general is a request made by an individual (“requestor”) to request a data user to supply him with a copy of his personal data.

2 Complying with a DAR

- When a data user receives a DAR, it should:
 - ascertain the identity of the requestor;
 - assess whether it holds the relevant personal data.
- If the data user holds the relevant personal data, it should supply a copy of the requested data in an intelligible form and within 40 calendar days after receiving the DAR.
- If the data user does not hold the requested data, it is still required to inform the requestor in writing within the 40-day time limit that it does not hold the data.

3 Charge for complying with a DAR

- A data user may impose a fee for complying with a DAR which should not be excessive. It should clearly inform the requestor what fee, if any, will be charged as soon as possible and in any event not later than 40 days after receiving the DAR.
- Fees that will be considered excessive or not directly related to and necessary for the compliance of a DAR:
 - fees that exceed the cost of compliance;
 - the costs amount to more than they would have been incurred under normal circumstances had it not been for the extraordinary situations created by the data user;
 - the costs of the data user in seeking legal advice or the costs for its consultant or staff to study the requirements under the Personal Data (Privacy) Ordinance (“Ordinance”);
 - the data user’s administrative or office overheads;
 - the redaction cost of personal data exempted from disclosure under any relevant exemption.

4 Refusing to comply with a DAR

- A data user should refuse to comply with a DAR if:
 - it is not supplied with satisfied information to identify the requestor;
 - it cannot comply with the request without disclosing the personal data of a third party;
 - where compliance with the request is for the time being prohibited under the Ordinance or any other ordinance.
- The data user is obliged to give written notice and reasons for refusal to the requestor within 40 days from receiving the DAR. It is also required to keep a log entry containing the particulars of the reasons for the refusal of the DAR for four years.

Please refer to this guideline note for more detailed information.

Introduction

The right to make a “data access request” (“**DAR**”) is an important right vested in a data subject under the Personal Data (Privacy) Ordinance, Cap. 486 (the “**Ordinance**”)¹. This right enables an individual to know whether a data user holds his personal data, and to obtain a copy of the data. It ties in with a further right under the Ordinance for a data subject to make a correction request to a data user if his personal data was found to be inaccurate.

Organisational data users who handle DARs properly will thereby demonstrate their respect for customers’ personal data privacy and gain trust from their customers. On the contrary, failure to handle a DAR in accordance with the requirements under the Ordinance without reasonable excuse may constitute an offence and render the offender liable on conviction to a fine².

Organisational data users should promulgate clear guidelines and work procedures on the handling of DARs and establish tracking procedures to monitor the progress of compliance with DARs. To this end, this guidance note provides general guidance to data users on the proper handling of DARs and the charge of DAR fees.

Individual to be informed of his right to data access

A data user who collects personal data from an individual should, *on or before the first use of such data*, explicitly provide information to the individual of his rights to request access to, and correction of, his personal data and the name or job title, and the address of the person to whom any such request may be made³.

When an individual is to be informed of his right to data access

While the information is required to be given on or before the first use of such data, generally, a data user will inform the data subject of such information in the “Personal Information Collection Statement” which is provided to the data subject on or before collection of his personal data.

What is a DAR?

A DAR is a request made by an individual to request the data user:

- (a) to inform him whether the data user holds personal data of which the individual is the data subject; and
- (b) if the data user holds such data, to supply him with a copy of such data.

A data user may refuse to comply with a DAR if the request is not made in writing with Chinese or English language.

A DAR may also be made by a “relevant person” on behalf of an individual. The “relevant person” may be a person authorised in writing by the individual to make a DAR on his behalf.

If the data subject falls within the class of minors (under the age of 18), persons incapable of managing their own affairs, or mentally incapacitated persons, the “relevant person” specified for these classes of individuals is respectively a person who has parental responsibility for the minor, a person appointed by a court to manage the data subject’s affairs, and a person appointed to be the guardian of the data subject under the Mental Health Ordinance.

Common examples of DARs include requests by employees for copies of their performance appraisal reports, requests by patients for copies of their medical records and requests by consumers for copies of their service application forms.

Scope of DAR

A requestor is not entitled under a DAR to access data which is not personal data or personal data not belonging to him. To constitute personal data of an individual, the data must firstly relate directly or indirectly to the individual. Secondly, it must be reasonably practicable from such data to directly or indirectly ascertain the identity of the individual. Thirdly, the data must be in a form in which access to or processing of the data is reasonably practicable⁴.

¹ Section 18 and Data Protection Principle 6 of the Ordinance

² Fine at level three, currently at HK\$10,000.

³ Data Protection Principle 1(3)(b)(ii) of the Ordinance

⁴ Section 2(1) of the Ordinance

For example, in a performance appraisal report where the appraising officer states his opinion about the aptitude and performance of the appraisee, such opinion will constitute the personal data of the appraisee. On the contrary, recorded opinion about the performance of a property management company expressed by an owner during an owners' meeting will generally not constitute the personal data of that owner.

DARs should not be used to supplement or as replacement for the rights of discovery in legal proceedings⁵.

Data Access Request Form

A DAR is usually made on the Data Access Request Form (Form OPS003) (the "**DAR Form**") specified by the Privacy Commissioner for Personal Data, Hong Kong (the "**Commissioner**")⁶. The DAR Form contains an explanatory note about the rights and responsibilities of a requestor and the data user respectively.

Sometimes, a requestor may not use the DAR Form to make the DAR but will simply say in his request that he wishes to obtain his personal data, or he is making a DAR or his request is made under the Ordinance. Although compliance with such request may be refused as it is not made on the specified form⁷, data users are strongly advised to respond to the request if it substantially sets out the scope and details of the requested personal data because reliance on such ground of refusal is merely technical and the requestor may simply lodge another DAR using the DAR Form.

Normally, an individual will not simply wish a data user to confirm to him whether it holds his personal data. He will go further to ascertain what data is held, and whether the data is accurate. Hence, if an individual asks a data user whether it holds his personal data, the data user may treat this as including a request to supply him with a copy of the personal data unless there is

contrary evidence that the requestor does not wish to obtain a copy⁸.

Complying with a DAR

Check the identity of the requestor

A data user should ascertain the identity of the requestor. If in doubt, a data user may require the requestor to provide his identity proof. For a DAR made by a "relevant person", the requestor should provide the data user with sufficient information as to his identity as follows:

- Written authorisation signed by the data subject;
- Evidence showing the requestor's parental relationship if the data subject is a minor (e.g. copy of birth certificate);
- Evidence showing the requestor's appointment by the court to manage the affairs of the data subject who is incapable of managing his own affairs; or
- Evidence showing that the requestor is the appointed guardian of the data subject under the Mental Health Ordinance.

If a data user cannot reasonably ascertain the identity of the data subject or establish the relationship between the requestor and the data subject, the data user should refuse to comply with the DAR⁹.

Response to a DAR within 40 days

Except where there are valid grounds for refusal falling within section 20 of the Ordinance, a data user is required to supply a copy of the requested data to the requestor within 40 calendar (not working) days after receiving it¹⁰.

A data user should assess whether it holds the relevant personal data on receipt of the DAR. However, the copy of personal data to be supplied to the requestor may

⁵ In the case of *Wu Kit Ping v Administrative Appeals Board* [2007] 5 HKC 450 (in relation to Administrative Appeal No. 27/2006), it was held that the entitlement under section 18(1)(b) of the Ordinance is not to "see every document which refers to a data subject" and not "to supplement rights of discovery in legal proceedings, nor to add any wider action for discovery for the purpose of discovering the identity of a wrongdoer".

⁶ The DAR Form is available on the Office of the Privacy Commissioner for Personal Data, Hong Kong's website: www.pcpd.org.hk/english/publications/files/Dforme.pdf

⁷ Section 20(3)(e) of the Ordinance

⁸ Section 18(3) of the Ordinance provides that if a data user receives a DAR made under section 18(1)(a), the data user may, in the absence of evidence to the contrary, treat the DAR as one made under both sections 18(1)(a) and (b).

⁹ Section 20(1)(a) of the Ordinance

¹⁰ Section 19(1) of the Ordinance
Proper Handling of Data Access Request and Charging of Data Access Request Fee by Data Users

take into account any processing of such data (i) made between the time of the request and the time when the copy is supplied to the data subject; and (ii) that would have been made irrespective of the receipt of the DAR¹¹.

A data user is obliged to take all reasonably practicable steps to ascertain whether it holds and/or controls any personal data which is relevant to a DAR¹².

A copy of the requested data to be supplied to the requestor should be intelligible as far as practicable, unless the copy is a true copy of the document and is unintelligible on its face¹³. Besides, the copy of data should be readily comprehensible with the codes used by the data user adequately explained¹⁴. For instance, if an employee requests for a copy of his appraisal report, apart from the employee's name and the evaluation grading made about him, the employer should, as far as practicable, also provide to him the explanatory note (if it exists) on the grading system, so that the grading can be readily comprehensible.

The copy of the requested data to be provided to the requestor should be in the language specified in the DAR or, if no language is specified, the language in which the DAR is made. However, if the requested data is held in a different language, the data user can supply a true copy of the document which contains the requested data¹⁵.

If the data user does not hold the requested data

A data user is not obliged to provide nor to create personal data that it does not have. However, it is still required to inform the requestor in writing¹⁶ within the 40-day time limit that it does not hold the data. For example, if an individual made a DAR to his former employer for "*data concerning the reason for my dismissal*", unless the reason being sought already exists in a document, the employer has no obligation to reduce into writing the reason being sought.

However, in the case of a DAR made to the Hong Kong Police Force in respect of criminal conviction records, if the Force does not hold any criminal record of the requestor, it is not required to comply with the request in writing, though it is still required to make a verbal response within 40 days, that it does not hold such record¹⁷.

If a data user has already destroyed the requested data by reason that the purpose for which the data is to be used has been fulfilled, the data user is required to inform the requestor that it no longer holds the data. The data user may explain the reason to the requestor to ease any suspicion that the erasure is made in bad faith.

However, a data user should not deliberately destroy the requested data after receiving the DAR with a view to avoiding its statutory obligation to supply a copy of such data to the requestor.

If the requested data is "all personal data"

Where the description of the requested data is too generic, especially where there have been extensive dealings between the data user and the requestor during which a large amount of personal data has been generated, it is reasonable for the data user to seek clarification from the requestor. If the requestor fails to supply the information reasonably requested by the data user for locating the requested data, the data user is entitled to refuse to comply with the DAR¹⁸.

In some circumstances, a data user may still be able to comply with a DAR for a broad scope of the requested data, such as "all personal data". For instance, a financial institution would have a proper record keeping system for maintaining its customers' documentation and hence retrieving a customer's personal data in respect of all his accounts would be reasonably practicable by indices such as the customer's name or the account numbers.

¹¹ Section 19(3)(a) of the Ordinance

¹² According to the decision in Administrative Appeal No. 52/2011, the data user was obliged to engage in a recovery process to provide the requestor with copies of his personal data which was contained in the back-up files since the computer data had been accidentally destroyed by the data user.

¹³ Section 19(3)(c)(i) of the Ordinance

¹⁴ Section 19(3)(c)(ii) of the Ordinance

¹⁵ Section 19(3)(c)(iii) of the Ordinance

¹⁶ Section 19(1)(b) of the Ordinance

¹⁷ Section 19(1A) of the Ordinance

¹⁸ Section 20(3)(b) of the Ordinance

Another example is where a DAR is made by a current employee for all his employment-related personal data. In such circumstances, it will be reasonably practicable for the employer to retrieve all employment records about an employee from his personnel file.

Hence, depending on the specific circumstances of individual cases, a data user may not simply rely on the ground that the request is made in generic terms to refuse to comply with a DAR. If the data user is aware of and can reasonably locate the requested data without any further specification from the requestor, the data user should comply with the DAR.

If the requested data comprises personal data of another individual

A data user should erase any personal data relating to a third party from the copy of the requested data unless the data user is satisfied that the third party has consented to the disclosure. If the DAR can be complied with by redacting the data relating to the third parties (e.g. names or other identifying particulars), there is no valid reason for a data user to refuse to comply with such a DAR¹⁹.

On the other hand, even though it is possible for the identity of the third party to be ascertained by deduction or inference despite the redaction of his name and other identifying particulars, it is not a valid justification to refuse compliance with the DAR.

If a data user is unable to comply with the DAR within 40 days

If a data user is unable to comply with a DAR within 40 days (e.g. the requested data is voluminous or if the DAR fee was received close to the expiry of the 40 days so that more time is required for the data user to comply with the DAR), the data user should give the requestor a written notification of the situation with reasons within the 40-day period and comply with the DAR to the extent, if any, that the data user is able to comply with

the DAR²⁰. The data user is required to comply fully with the DAR as soon as practicable thereafter²¹.

Charge for complying with a DAR

A data user may impose a fee for complying with a DAR which should not be excessive²². The data user should clearly inform the requestor what fee, if any, will be charged as soon as possible and in any event not later than 40 days after receiving the DAR. A data user is entitled to refuse to comply with a DAR unless and until the fee imposed has been paid²³.

Calculation of DAR fee

A data user should not charge a fee on a commercial basis. Any fee that exceeds the costs of compliance will be considered excessive²⁴. A data user should refrain from imposing an excessive fee to deter an individual from making a DAR so as to avoid its statutory obligation to comply with the DAR.

The costs of compliance may vary with the scope and complexity of the DAR in question. In most circumstances, the costs of compliance will be nominal. However, where the DAR is extensive (e.g. the requested data involves voluminous documents and covers a long period of time requiring extensive search), the costs can be substantial.

Not all the costs actually incurred by a data user in complying with a DAR will be considered "direct and necessary costs". "Direct and necessary" is not the same as "reasonable". A data user should consider whether it is possible to comply with the DAR without incurring the individual item of cost. If the answer is "yes", the data user should not include in the charge the cost incurred for that particular item.

The costs will be considered excessive if they amount to more than they would have been incurred under normal circumstances had it not been for the extraordinary situations created by the data user²⁵.

¹⁹ Section 20(1)(b) and 20(2) of the Ordinance

²⁰ Section 19(2)(a) of the Ordinance

²¹ Section 19(2)(b) of the Ordinance

²² Section 28(3) of the Ordinance

²³ Section 28(5) of the Ordinance

²⁴ According to the decision of Administrative Appeal No. 37/2009, a data user is allowed to charge the requestor only for the costs which are "directly related to and necessary for" complying with a DAR.

²⁵ In Administrative Appeal No. 52/2011, the personal data requested was held in a laptop which was crashed due to the fault of the data user and this made it necessary for huge and exorbitant fees to be directly incurred to recover the data lost as a result of the crash. However, it was held that such fees should not be borne by the requestor.

The burden lies with a data user to explain the fee imposed and how it is cost-related as the matter of costs is known only to the data user. If the fee is substantial, a data user should provide a written explanation on its calculation to the requestor to facilitate better understanding.

Seeking legal advice or professional service

A data user should not charge a data subject for its costs in seeking legal advice or the costs for its consultant or staff to study the requirements under the Ordinance. While it may be reasonable for the data user to seek legal advice to ensure proper discharge and compliance of its obligations under the Ordinance, such costs are incurred for the data user's own protection and are not strictly necessary for compliance with a DAR. For instance, a data user may seek legal advice on whether to supply the data under request which may be subject to legal professional privilege, as a data user is not obliged to rely on an exemption from disclosure even if the exemption applies, and as such, the cost incurred for such legal advice should not be borne by the data subject.

Office overheads

A data user should not charge for its administrative or office overheads. Such costs are, by their very nature, not costs directly related to and necessary for the compliance of a DAR²⁶.

Direct labour costs and necessary expenses

A data user may take into account the direct costs attributable to the time spent by its staff and the actual out-of-pocket expenses for locating, retrieving and reproducing the requested data for complying with a DAR.

For example, if a clerical assistant has spent five hours on retrieving and photocopying the requested data in the course of handling a DAR, the calculation of the labour costs incurred is the hourly rate of his remuneration (including salary and fringe benefits²⁷) multiplied by five.

The data user should consider the skills required to handle the DAR. Normally, clerical and administrative staff will be considered capable of performing the

tasks such as retrieving, photocopying and redaction of data. A data user should calculate the labour cost with reference to the staff assigned for handling the DAR. If a data user has assigned a group of staff of the same category for the task, the labour costs may be calculated by reference to the average staff cost of this staff category. Unless with valid justification, the data user should not assign a professional or managerial staff to perform the clerical and administrative tasks, otherwise the DAR fee will be jacked up unnecessarily.

A data user may charge for the labour cost attributable to the time spent on extracting or editing the requested data, provided that such tasks are directly related to and necessary for compliance with the DAR. For instance, in complying with a DAR for personal data held in a video tape, a data user may charge the costs for technical assistance in duplicating and editing the tape to remove images of other individuals. Similarly, the redaction cost of the name and other identifying particulars of individuals other than the data subject is allowed.

However, a data user should not include in its DAR fee the redaction cost of personal data exempted from disclosure under any relevant exemption. This is because the data user may still choose to comply with the DAR without invoking any exemption, and such costs are incurred for the protection of the data user's interests and hence are not directly related to and necessary for compliance with a DAR.

Photocopying

The costs of photocopying the documents containing the requested data are direct and necessary costs. Generally speaking, the photocopying charge imposed at HK\$1 per page will be considered not excessive.

Flat-rate fee

For administrative convenience, some data users who keep records in a digital format and operate standard procedures for retrieving such records may impose a flat-rate fee. Charging a flat-rate fee is permissible provided that the fee imposed is lower than the direct and necessary costs for complying with a DAR and in any event not excessive under normal circumstances. Charging at a nominal rate is also permissible.

²⁶ This issue has been decided in Administrative Appeal No. 37/2009

²⁷ It has been decided in Administrative Appeal No. 37/2009 that if the remuneration does consist of various fringe benefits, they are parts of the costs of his labour.

Special situations

In situations where the personal data may be supplied in more than one form, a data user would be able to recover only a sum not higher than the lowest fee of all alternative forms available for complying with the DAR²⁸.

Where a further copy of data is requested following a previous request, a data user is entitled to charge for the actual cost which is not more than the administrative and other costs incurred by the data user in supplying that further copy²⁹.

Refusing to comply with a DAR

Under what circumstances can a data user withhold the requested data?

A data user shall refuse to comply with a DAR under section 20(1) of the Ordinance if: (a) the data user is not supplied with information to satisfy the data user as to the identity of the requestor, (b) the data user cannot comply with the request without disclosing the personal data of a third party, (c) where compliance with the request is for the time being prohibited under the Ordinance or any other ordinance³⁰.

On the other hand, the Ordinance provides under section 20(3) various grounds upon which a data user *may* refuse to comply with a DAR. A data user *may* refuse to comply with a DAR if (a) the request is not in writing in Chinese or English, or (b) the data user is not supplied with information to locate the requested data, or (c) the DAR is not made in the DAR Form. A data user may also rely on the following grounds to refuse to comply with a DAR:

(a) the DAR follows two or more similar requests, and

it is unreasonable for the data user to comply with the DAR in the circumstances³¹;

- (b) another party controls the use of the requested data in a way that prohibits the data user from complying with the DAR³²;
- (c) the data user is entitled under the Ordinance or any other Ordinance not to comply with the DAR³³;
- (d) there is an applicable exemption provided for in the Ordinance from the requirement to comply with the DAR³⁴.

Exemption provisions

To cater for a variety of competing public interests, Part VIII of the Ordinance provides for the specific situations in which personal data is exempt from access by the data subject.

In particular, data users may withhold the following personal data³⁵:

- (a) personal data which consists of information relevant to staff planning proposal related to filling a series of employment positions or ceasing a group of individuals' employment³⁶;
- (b) (until a decision has been made and where the data subject has a right of appeal against the decision made³⁷) personal data being considered for (i) employment, promotion, discipline and dismissal in an employment situation; or (ii) in connection with the awarding of contracts, awards, scholarships, honours or other benefits;
- (c) personal reference given by an individual other than in the ordinary course of his occupation and relevant to another individual's suitability or otherwise to fill any position of employment or office³⁸;

²⁸ Section 28(4) of the Ordinance

²⁹ Section 28(6) of the Ordinance

³⁰ Section 20(1)(c) of the Ordinance

³¹ Section 20(3)(c) of the Ordinance

³² Section 20(3)(d) of the Ordinance. It should be noted that according to the decision in Administrative Appeal No. 26/2013, "confidentiality is not a reason stipulated in the Ordinance to permit a data user to refuse to comply with a DAR".

³³ Section 20(3)(ea) of the Ordinance

³⁴ Section 20(3)(f) of the Ordinance

³⁵ Exemption for employment-related personal data is further discussed in the *Code of Practice on Human Resource Management* issued by the Commissioner. The Code can be downloaded from www.pcpd.org.hk/english/data_privacy_law/code_of_practices/files/PCPD_HR_Booklet_Eng_AW07_Web.pdf

³⁶ Section 53 of the Ordinance

³⁷ Section 55 of the Ordinance, which concerns the determination of suitability for employment, promotion, removal from employment, the taking of disciplinary action, etc.

³⁸ Section 56 of the Ordinance

- (d) personal data in respect of which a claim of legal professional privilege could be maintained in law³⁹;
- (e) personal data held by a court, a magistrate or a judicial officer in the course of performing judicial functions⁴⁰; and
- (f) personal data the disclosure of which might incriminate the data user in any proceedings for any offence other than an offence under the Ordinance⁴¹.

A data user relying on a particular exemption to refuse to comply with a DAR should be able to show sufficient evidence to invoke the exemption.

Steps to be taken when refusing to comply with a DAR

A data user is obliged to give written notice and reasons for refusal to the requestor within 40 days from receiving the DAR⁴².

Where there is another data user that controls the use of the data in such a way as to prohibit the data user from complying with the DAR, the data user should also in its notification of refusal to comply with the DAR to the requestor, inform the requestor of the name and address of the other data user⁴³.

A data user is also required to keep a log entry containing the particulars of the reasons for the refusal of the DAR for four years⁴⁴.

³⁹ Section 60 of the Ordinance

⁴⁰ Section 51A(1) of the Ordinance

⁴¹ Section 60A(1) of the Ordinance

⁴² Section 21(1) of the Ordinance

⁴³ Section 21(1)(c) of the Ordinance

⁴⁴ Section 27 of the Ordinance



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

Copyright



This publication is licensed under a Creative Commons Attribution 4.0 International (CC BY 4.0) licence. In essence, you are free to share and adapt this publication, as long as you attribute the work to the Office of the Privacy Commissioner for Personal Data, Hong Kong. For details, please visit creativecommons.org/licenses/by/4.0.

Disclaimer

The information and suggestions provided in this publication is for general reference only. It does not provide an exhaustive guide to the application of the Personal Data (Privacy) Ordinance (the "Ordinance"). For a complete and definitive statement of law, direct reference should be made to the Ordinance itself. The Privacy Commissioner for Personal Data (the "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 Commissioner under the Ordinance.

First published in June 2012
 June 2016 (First Revision)