

THE AMERICAN CHAMBER OF COMMERCE IN HONG KONG

Position Paper

Proposed Changes to Improve the Functionality of the PDPO

The Issue

The Personal Data (Privacy) Ordinance (“PDPO”) came into effect in 1996. The purpose of the PDPO is to protect privacy rights by regulating the use of personal data.

During the years the PDPO has been in force data users have had experience responding to many data requests. Based on this experience, data users have determined that the PDPO is being interpreted in a manner which does not sufficiently take into account: (i) the rights of individuals other than the data subject; (ii) the effect of data requests on data users and other data subjects; or (iii) the position that other data protection regulators have taken.

Position

The Office of the Privacy Commissioner for Personal Data (“PCO”) should adopt a balanced approach to enforcement of data requests so that a data user’s legal obligations cannot be exploited by disgruntled former employees or other third parties.

Recommendations

One aspect of achieving this balanced approach involves reviewing the interpretation of “personal data” and incorporating recent case law either into the PDPO or into codes of practice.

Additionally the PCO must consider the concerns specific to employment relationships in general and data access requests, in particular including confidentiality and data protection duties to data subjects. These concerns could be dealt with by the PCO interpreting “identifying particulars” at section 20(2)(b) of the PDPO to mean all statements by an individual in a staff evaluation process. Alternatively the PDPO should be amended to clarify this point.

Finally we recommend that the costs and general effect on data users of complying with data access requests be taken into account by the PCO or in the PDPO.

Rationale

Scope of Personal Data:

A data subject is entitled to request “all” his/her personal data created during a set time.

Experience indicates that the PCO interprets “personal data” without proper regard to the PDPO definition. As a consequence, in order to comply with a data request the data user is required to undertake searches of its offline email archives, current paper files and any files that have been archived in order to find all documents containing references to the data subject which may not be “personal data”.

Court decisions¹ have suggested that information must be “collected” in order for it to be subject to a data access request. Case law should be taken into account by the PCO in its interpretation of the PDPO and either referenced in PCO codes of practice or incorporated into the PDPO by amending the definition of “personal data”. The PCO stated in its May 2001 newsletter, that by the end of 2001 it would publish a booklet on the PCO’s interpretation of the PDPO in light of case law, but this has not happened.

¹ Eastweek Publisher Ltd & Anor v. Privacy Commissioner for Personal Data (Civil Appeal 331 of 1999).

The PCO should also include a “disproportionate effort test” in its codes of practice in recognition of the difficulties to which data users are subject in complying with such requests. Data protection regulators in other jurisdictions have adopted similar tests, which have proven to be an effective way to limit mischievous or malicious access requests.²

The PCO has recently suggested³ that it would require the scope of data access requests (including identification of the type of data requested) to be clearly described to enable the data user to respond. These principles should be stated clearly in PCO codes of practice.

Scope of Personal Data – Staff Evaluations:

Many data users employ ‘360 degree’ staff evaluations. Such evaluations are particularly effective as they use the opinions of a staff member’s supervisors, peers and subordinates (“evaluators”) to determine overall level of achievement and identify needs.

These ‘360 degree’ evaluations can only function where the views of evaluators are kept completely confidential. Without an assurance of confidentiality by the data user to its evaluators those evaluators may not be forthcoming.

The exemption at PDPO section 20(1)(b) is limited by PDPO section 20(2)(b) But it is vital that the PCO recognizes that simply removing evaluators’ names in this case is unlikely to protect the privacy of those evaluators. In the case of most ‘360 degree’ evaluations the identity of the evaluators - usually a small pool of people - are already known to the data subject and any comment written by the evaluator becomes an identifying particular by which the evaluator is potentially identifiable.

The PDPO’s failure to adequately deal with this issue violates the data protection and confidentiality rights of evaluators. Effectively the PDPO is putting the privacy rights of a data subject who has made a data request above the privacy rights of other data subjects.

Costs and Effect on Data User:

The PCO should balance the rights of data subjects against the impact on the data user and third parties.

Many data users are under regulatory duties to retain vast quantities of data. Without clearer guidance from the PCO on what data can be restricted from access requests, the costs to and effort required of data users in complying with access requests will be disproportionately high.

It is also not clear which costs are recoverable. The PCO has indicated that direct costs, are “reasonable” but secondary costs, such as legal fees, are not. A data user could therefore incur significant costs because it deploys staff to search for personal data and review it to confirm that (i) it is responsive to the request and (ii) it does not breach any other legal obligations.

Conclusion

The above recommendations would enhance the effectiveness of the PDPO because restricting personal data to that which is direct and relevant and discouraging malicious or mischievous requests will enable quicker responses to data requests.

The recommendations would not affect negatively the privacy rights of data subjects because they take into account the balance necessary between data subjects’ rights and data users’ duties.

The recommendations would be best implemented through a revision of the PCO’s interpretation of the PDPO and/or amendments to the PDPO which would assist the PCO in enforcing rights of data subjects whilst at the same time protecting both the rights of other data subjects and the business interests of data users.

² One of the duties of the PCO as set out on the PCO web-site is to “Liaise and cooperate with persons performing similar data protection functions in any place outside Hong Kong...”

³ For example at the Data Protection Officers’ Club meeting on 27 January 2005.