Privacy Implications for Organisational Use of Social Networks

This information leaflet outlines what you need to consider to safeguard personal data privacy when using social networks or social media (collectively referred to as social networks in this leaflet) to promote your business or organisation ("organisation").

Social networks are rapidly evolving and developing, and so is the mode of engagement with social networks by organisations to advance their business interests. This leaflet outlines how personal data privacy should be respected and protected when using social networks. Commitment to personal data privacy and protection can help organisations build trust and loyalty with the public in a competitive world.

Unless otherwise stated, this leaflet provides advice on the best practices for organisations to adopt rather than prescriptive guidance for compliance with specific provisions of the Personal Data (Privacy) Ordinance ("the Ordinance").

Social Networks and the Personal Data (Privacy) Ordinance

Social networks are platforms on which users connect with friends, family and/or customers for social and/or business purposes. The Ordinance applies if organisations collect personal data as defined under the Ordinance.

What is "Personal Data"?

The Ordinance defines personal data as any data:

- relating directly or indirectly to a living individual;
- from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and
- in a form in which access to or processing of the data is practicable.

If it is practicable to ascertain, directly or indirectly, the identity of an individual from the information obtained by an organisation from the use of social networks, such information would most likely be regarded as "personal data" under the Ordinance.

In cases where the information collected from social networks does not contain unique identifiers of individuals, organisations must carefully assess if such information, taken in its totality, can be used to directly or indirectly identify an individual. Organisations should bear in mind that they may collect a complex set of such information from social networks which, when combined together, and with or without other information the organisation may hold, may be sufficient to ascertain the identity of individuals. In such circumstances, the information collected may constitute personal data and the Ordinance may apply.

Transparent Privacy Policy and Practice

Organisations are encouraged to be transparent in communicating to the public what information they collect from individuals and how organisations may use it. Even in cases where organisations do not collect or use personal data obtained from or about individuals, it is recommended that organisations make this practice known through a privacy policy statement ("PPS") to assure the public that their interactions with the organisations have no personal data privacy implications.

This is particularly important in the case of certain social network environments which require real identities of individuals to be used to create accounts, since individuals may have reason to believe or suspect that their personal data is being collected or used.

As a recommended best practice, PPS should be written in a user-friendly manner so that it is easily understandable and readable.

Organisations may refer to *Guidance on Preparing Personal Information Collection Statement and Privacy Policy Statement* issued by the Privacy Commissioner for Personal Data ("the Commissioner") for more details on making their privacy policy and practice known: www.pcpd.org.hk/english/publications/files/GN_picspps_e.pdf.

Key Principles of Data Privacy Protection

As the nature and serving functions of social networks are constantly evolving and developing, organisations should be mindful of the following principles of personal data privacy when engaging or experimenting with social networks to pursue their interests:

Appropriateness	The amount of information collected from individuals in social networks and the way in which such information is used should be relevant and proportionate in the circumstances, from the perspective of the individuals;
Transparency	Individuals should be well informed of what information about them that organisations would access, collect and/or use as part of their social network strategy;
Respect for individual rights	Individuals should be notified and given the choice to opt-out if their social network behaviour and preferences (such as "liking" a particular brand) are used for marketing purpose or being tracked;
Protection	Organisations should take reasonably practicable steps to ensure that if information about individuals is collected, transmitted, used and/or stored, it would not be subject to accidental or unauthorised access, loss or use.

Social Network Marketing

Social network marketing may be defined as a form of marketing activities conducted through the medium of social networks. It often involves producing contents that social network users are prompted to share with their friends or contacts. This sharing helps to increase brand exposure and customer reach.

This business-to-customer marketing strategy is often carried out in a one-to-many, word-of-mouth approach to spread, and in the process "validate" the marketing message to social network users.

Typically organisations (whether for-profit or non-profit-making) engaging in social network marketing do not in the process seek to identify individuals. However, organisations should be mindful that the following marketing activities may involve the collection of personal data:

- In certain social networks, such as Facebook and Google+, users are expected to use real identities to create accounts and make available personal contact information (such as Facebook account names, email addresses and contact phone numbers) to the public or to selected groups of friends. If organisations make use of such contact information for direct marketing[1] purpose, they must comply with the direct marketing requirements under the Ordinance, irrespective of whether the contact information so used is shared by the account user with the public or with the organisations specifically. Organisations are advised to read the *New Guidance on Direct Marketing* issued by the Commissioner: www.pcpd.org.hk/english/publications/files/GN_DM_e.pdf;

- One of the biggest assets of social networks is the social connection (or relationship) between members. Some businesses may make use of this relationship to boost its (or its products') reputation through recommendations by members (also known as viral marketing). Organisations engaging in such practice should ensure that any recommendations or promotions of their brands/products by members are carried out with the knowledge of the members. Where practicable, organisations should allow members to opt out of participating in such marketing process. For example, if an organisation promotes to a member's contacts that the member has shown interests in or has purchased from the organisation, the member should be made aware of this use of his/her information, and where technically feasible in the arrangement, allowed to opt out from participating in this marketing process;

- Organisations may be interested to profile customers/potential customers based on their behaviour/preferences as social network users. This may or may not involve combining other information obtained outside of the social network. If any kind of behavioural tracking is involved, organisations should be mindful of the privacy implications. They should make the practice of tracking known to the targeted individuals and, where appropriate, allow them to opt-out. They may refer to the *Information Leaflet on Online Behavioural Tracking* issued by the Commissioner for more advice: www.pcpd.org.hk/english/publications/files/online_tracking_e.pdf;

- Organisations may conduct certain marketing campaigns (e.g. membership programme, lucky draw, photo-sharing and voting) through social networks which involve the explicit collection and use of personal data. The data of participants may be collected via a form or a web-based application developed for the social network specifically. Such collection of personal data is regulated under the Ordinance. Among other requirements under the Ordinance, data users must supply the corresponding Personal Information Collection Statement ("PICS") on or before personal data collection. Data users should also make clear in their PPS to data subjects their privacy policies and practices in relation to the personal data they handle. For more details on how to prepare PICS and PPS, organisations may refer to the *Guidance on Preparing Personal Information Collection Statement and Privacy Policy Statement* mentioned above.

[1] Under the Ordinance, direct marketing means (a) the offering, or advertising of the availability, of goods, facilities or services; or (b) the solicitation of donations or contributions for charitable, cultural, philanthropic, recreational, political or other purposes, through direct marketing means. Direct marketing means, under the Ordinance, means (a) sending information or goods, addressed to specific persons by name, by mail, fax, electronic mail or other means of communication; or (b) making telephone calls to specific persons.

Customer Services in Social Networks

Organisations may use social networks to provide customer services (including, but not limited to product/service enquiries, help desk and after-sales service) to customers (both existing and potential). In the process, organisations should take care to safeguard the personal data privacy of its customers.

Given the open nature of social networks, organisations should, at all times, remind customers not to disclose in open social networks their personal data during their interaction with the organisations. Should there be a need to establish the identity of the customer and/or to obtain personal data from customers, organisations should develop formal policies and practices in this regard, and train customer service staff to take customers off the social network to other secured communication channels.

HR Management in Social Networks

Increasingly organisations are making use of social networks as a human resource management tool. This may include brand building as an employer, recruitment (whether for paid or voluntary staff), collection of information for candidate screening and/or monitoring of employees' attitudes towards the organisations.

In each of these activities, various types of personal data may be collected by the organisations. It is important to assess whether the use of the information is proper and whether the data subjects concerned are aware of such collection.

For example, if organisations wish to use information in the Internet and/or social networks (including information posted by the candidates or their friends) to form opinions or make hiring or shortlisting decisions about candidates, they should consider whether such information is reliable, and more importantly, whether such use of the information is in line with the purposes for which they were made available in the first place.

Also, organisations may find that they would wish to take appropriate actions against employees involved in discussion of internal issues about the organisation on social networks. This may be considered an act of employee monitoring. Organisations are referred to the guidelines on employee monitoring (*Privacy Guidelines: Monitoring and Personal Data Privacy at Work* issued by the Commissioner: www.pcpd.org.hk/english/publications/files/monguide_e.pdf).

Social Network Analytics

Social network analytics may be defined as the analysis and evaluation of social network discussions for assessing customer sentiments to facilitate business decision making. Social network analytics may be used by organisations to keep track of the general consumer awareness and to gauge the reputation (both positive and negative) of their organisations or brands, to identify market demands and gaps, to detect any brewing public relation crisis, and/or to gauge the effectiveness of marketing campaigns. Often social network analytic tools would be needed to capture, correlate and analyse social network conversations over a long period and from a large number of different social networks.

While the majority of such analytics would result in aggregated information being collected and presented to organisations for decision making, sometimes organisations may be collecting personal data as a by-product. The process may involve correlation of similar views expressed in multiple social networks over a specific issue which ends up establishing the identity of an individual expressing those views. It may also be an on-purpose action to monitor or track the adverse postings of disgruntled individuals across multiple social networks with a view to containing or minimising any damage such postings may cause.

These practices may lead to the identification of individuals as a result of combining the various online identities of the individuals. As a recommended best practice, organisations should make known such use of social networks to the public. Organisations should be aware that if they collect and keep personal data, they will be obliged to observe the six Data Protection Principles stipulated under the Ordinance including the right of individuals to access and correct their personal data held by a data user. A brief description of the six Data Protection Principles can be found at: www.pcpd.org.hk/english/ordinance/ordglance.html.

Office of the Privacy Commissioner for Personal Data, Hong Kong

Enquiry Hotline : (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