Personal Data Privacy

* ***Avoid the Web facade.*** Provide web pages that make available information "About the Organization". Include the name, physical location and contact telephone/fax numbers of the organization in addition to the web address or email address. This would be a reliable channel through which a web user could contact the organization.
* ***Make the privacy policy statement easy to access.*** One possible method is to set up the privacy policy statement as a linked page accessible from the home page or other pages where personal data are collected, e.g. a registration page where registration is required for access or a customer agreement page.
* ***State the privacy policy clearly***, which should inform web users of the kinds of personal data held by the organization and the main purposes for which the personal data are used or are to be used.
* ***Provide a Personal Information Collection (PIC) statement***, to inform a person from whom personal data are requested on how these data are to be used, to whom they may be transferred, and the person's rights to request a copy of the data and correct any errors, and who should be contacted to make such requests.
* ***Collect adequate but not excessive data relevant to the purpose***, for example, if no purchase is to be made, generally it will be excessive and not relevant to request a credit card number.
* ***State whether personal data will be displayed at the time of collection.*** If personal details are collected and are later to be displayed on the Internet or elsewhere, this intention must be made clear to the individual at the time of collecting the data.
* ***Anonymise the personal data when displaying*** them on the Internet as an additional precautionary step to avoid presenting detailed information that might be excessive or abused.
* ***Use encryption when transmitting sensitive personal data*** to reduce the risk of these information being got hold of by other people.
* ***Provide a privacy warning message*** if un-encrypted data transfer is used for the transmission by users of sensitive personal data.
* ***Using "clicktrails" information.*** An ISP should not use the "clicktrails" information to do analysis on a customer's interests as the data are not provided for such purposes.
* ***Offering a secure environment that meets service commitment*** as the ISP has the liability to protect customers' sensitive information from unauthorized access or hacker attacks.

* The above information is provided by the Office of the Privacy Commissioner for Personal Data, Hong Kong. For further information, please visit web site: http://www.pco.org.hk

Published by:

Hong Kong Productivity Council 香港生產力促進局

Supported by:

消費者委員會 CONSUMER COUNCIL

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

A Guide to Personal Data Privacy and Consumer Protection on the Internet

Consumer Protection

Major Principles in Organization for Economic Cooperation Development (OECD) Guidelines for Consumer Protection in the Context of Electronic Commerce

Issue	Benefits to Achieve	Principles to Implement	Good Practices
Protection	To foster public confidence in the electronic marketplace.	Governments, businesses and consumer representatives should work together to afford a level of consumer protection that is no less transparent and effective in the cyberspace than in the real space.	Observe the existent consumer protection laws in Hong Kong. Reference: http://www.consumer.org.hk/LEGAL_E.HTM
Marketing Practices	To ensure due regard being paid to the interests of consumers in the conduct of electronic commerce.	Businesses must act in accordance with fair business, advertising and marketing practices. Regulatory framework against spamming to unsolicited parties and marketing to children must be observed.	Adopt the good advertising practices in Hong Kong. Reference: Advertising code of practices issued by OFTA http://www.ofta.gov.hk or The Association of Accredited Advertising Agents of Hong Kong.
Online Disclosures - Identification	To enhance identification of the business and the jurisdictions within which it operates.	Sufficient online disclosures must be given to enable consumers to establish the business identity and contact details, and to verify its membership in certification bodies.	Consumers must be provided with details of the retailer's identity, like business registration number, certification number, registered physical address, a phone number and an e-mail address.
Online Disclosures -Transparency	To ensure transparency of information for decision-making	Businesses should provide clear, unambiguous and easily accessible information on the goods and services so that consumers can make an informed choice before effecting a transaction.	Sites should display one overall total price to the consumer before the order is completed, which include any applicable local taxes and any delivery charges, if any. Retailers supplying to other countries can also do a lot more to assist consumers in converting prices into their own currencies. Retailers should provide information on whether an item is in stock before the order is placed.
Online Disclosures - Clarity and Comprehensiveness	To avoid unconscionable contract being entered into.	Terms, conditions and costs associated with a transaction must be clear, accurate, easily accessible, and provided in a manner that gives consumers adequate opportunity for review before entering into a transaction.	Retailers should design sites to ensure that purchasers are shown the terms and conditions (including payment terms, delivery terms, guarantees and warranties, cooling-off periods, conditions relating to returns or exchange of goods, cancellations and refunds) before confirming their orders. Terms and conditions should be provided in a manner that can be easily printed off and kept by the consumer for future reference.
Confirmation Process	To avoid ambiguity in a potential transaction.	Businesses should enable consumers to identify precisely the goods and services on offer, to correct any errors before concluding the purchase online, and to retain an accurate record of the transaction.	Site designer should use the three stage model (expression interest stage, stage of reviewing all the details of the order and final stage for confirmation of the order) and allow the consumer to have the opportunity to cancel the order.
Payment	To minimize unauthorized transactions.	Consumers should be provided with easy-to-use, secure payment and chargeback mechanisms, and information on the level of security afforded.	Sites should have easy to understand statement about their security system and the level of protection.
Dispute Resolution	To provide access to fair and timely dispute resolution mechanisms without undue cost or burden.	Businesses, consumer representatives and governments should jointly develop fair, effective and transparent dispute resolution mechanisms to resolve complaints and disputes in the context of cross-border transactions.	Sites should (1) provide a policy on returns which makes the process as simple as possible; (2) clarify within the policy what costs (if any) the consumer will incur; (3) make the policy available at the place where the purchase is made and (4) process requests for refund quickly and give targets for when consumers will receive the money.
Privacy	To advance full privacy protection.	Business-to-consumer electronic commerce should be conducted in accordance with internationally recognized privacy principles.	All sites should have a privacy policy which is easy to understand and clearly signposted. Observe the code of practices for privacy protection in Hong Kong. Reference site: http://www.pco.org.hk/
Education	To foster informed decision-making by consumers in the cyberspace.	Governments, businesses and consumer representatives should jointly promote public awareness of consumer protection framework applicable to online activities.	

*The above information is provided by the Consumer Council. For further information please visit website http:// www.consumer.org.hk