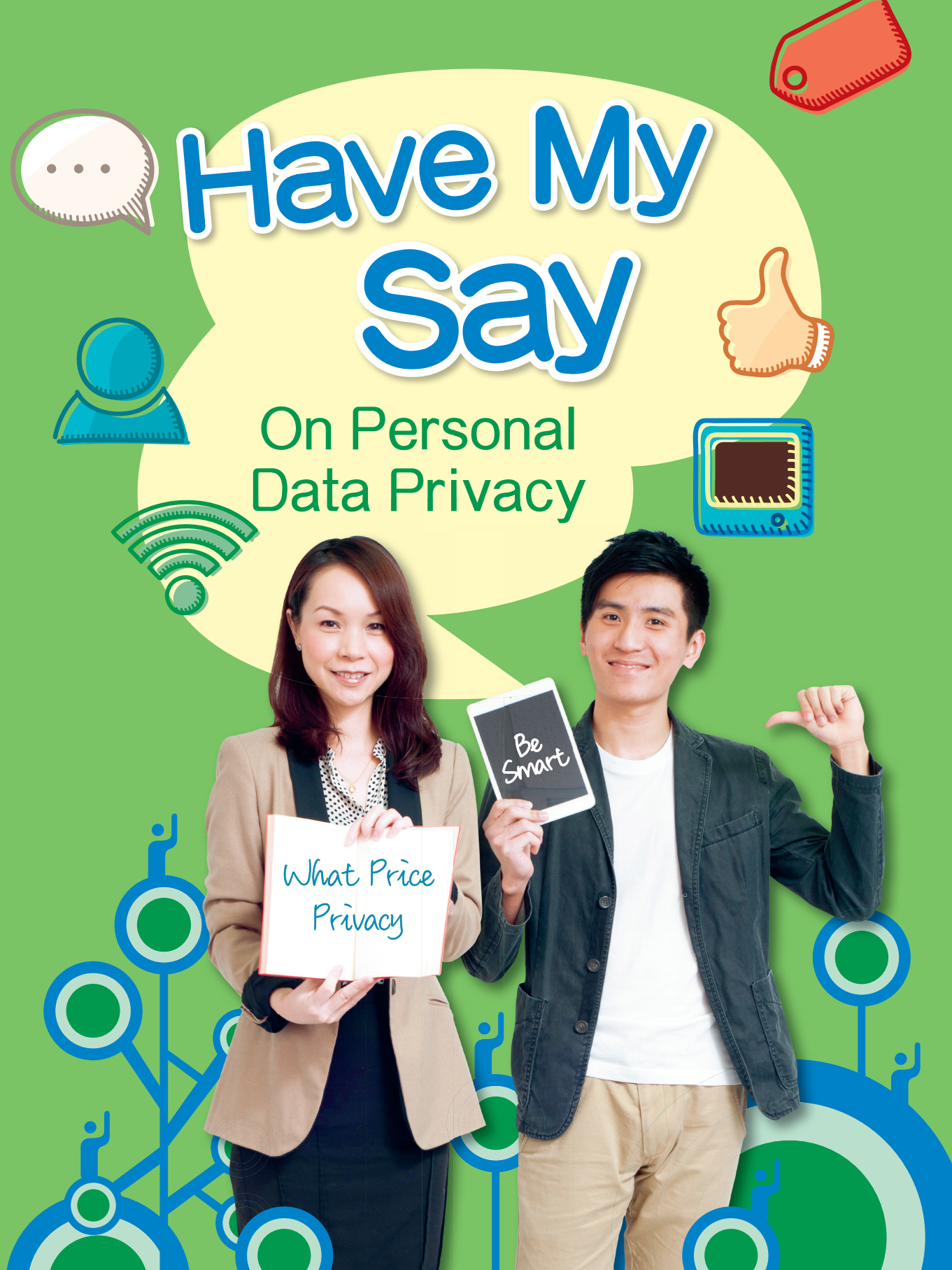
Have My Say

On Personal Data Privacy



Protect Your Personal Data

Your personal data may be disclosed when you are applying for a job, shopping, using social networking sites, or even using a smartphone. Personal data privacy is a fundamental right. You have the right to protect your privacy and actively control the use of your personal data by others to avoid any possible privacy traps in daily life.

What is personal data privacy?

There are many dimensions to privacy. Personal data privacy is an integral part of it and is protected by the Personal Data (Privacy) Ordinance. Personal data is recorded information relating to an identifiable living individual. Examples of personal data include identification documents, names, addresses, telephone numbers, medical and employment records, recordings, videos and photos.

Under the Ordinance, you have the following rights:

To ensure that the collection of your personal data is fair and is for a legal purpose;

To be informed of the intended use of the data;

To provide only data necessary for the prescribed purpose;

To reject any use other than the prescribed purpose;

To demand safe, accurate retention of your personal data;

To access and correct your personal data; and

To be informed of the data user's openly available privacy policy.

Job Seeking

Your Hong Kong Identity (ID) Card contains sensitive personal data. If an organisation asks for your ID card number and an ID card copy without a sound reason, you can refuse to provide it or suggest an alternative. When you prepare yourself for a job, be mindful of protecting your personal data!

tips

Recording your ID card number or taking a copy of your ID card under other circumstances

- If security guards ask for your ID card number when you enter private premises, you can suggest them to confirm your identity with the person you are visiting, or present other identification documents with your name and photo, such as your staff ID card. ID card number is not the only means.
- When you join an organisation's membership or reward programme, it is sufficient to provide your name, telephone number or email address for the company to verify your identity.
- If an organisation collects a photocopy of your ID card, the word "copy" should be marked on the image to avoid unintended use.

What is a Personal Information Collection Statement (PICS)?
An organisation collecting your personal data should provide a PICS, stating the purpose, use, possible transferees of the collected personal data, as well as the procedure for accessing and correcting the data.

Things We Can Do

When applying for a job

- Beware of anonymous advertisers, as they may collect your personal data for other undisclosed purposes. Since your résumé contains a lot of personal data, make sure you encrypt it when you submit it via electronic means, and read the PICS of the recruiter carefully to avoid any abuse or misuse of your personal data.

During interviews

- You may present your ID card for verification purposes, but you do not have to provide a copy of your ID card to a prospective employer. You can also refuse such a request.
- You can refuse to provide any data which is irrelevant to recruitment, unless an acceptable reason is given. Personal data collected during an interview should be used only for recruitment purposes.

Getting the job

- Your new employer may ask you to provide detailed personal data, so you should pay attention to the organisation's PICS before you do so.

Not getting the job

- An organisation can keep your résumé and personal data for reference or contact purposes for up to two years, and you have the right to access the collected data and demand a copy of it during that period.

Things We Can Do

Only provide the appropriate data

- There is no such thing as a free lunch. You should understand the purpose and use of the collected personal data before providing it. Do not hesitate to refuse if you do not want to provide it! You can provide personal data selectively. Sensitive data, such as your birthday, is not necessary for marketing purposes. Indicating your age group or month of birth is sufficient.

Say "no" anytime

- If a company sends you a notification stating that it wants to use your personal data for direct marketing or fundraising purposes, you do not need to respond if you want to reject these direct marketing messages. A non-response to a notification does not imply consent. It is a breach of the law if a company uses your data for direct marketing purposes without your consent.
- You can ask the marketer to stop using your personal data for direct marketing anytime, and this right to opt-out never expires. An organisation which fails to comply with your request commits a criminal offence.

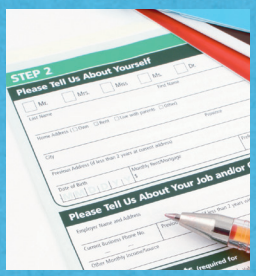
Shopping

Some merchants membership programmes offer privileges and rewards to their customers. To become a member, you usually need to complete a membership form requiring your personal data, which may be used for direct marketing. There is also a chance that your data will be transferred to other parties. Is it worth giving up your privacy for the membership benefits?

tips

How to respond to a direct marketing call or email addressing you by name?

- You can ask the callers to explain how they got hold of your personal data and tell them the following: "You may have contravened the Ordinance because you did not ask for or get my consent before using my personal data in this direct marketing message".
- You can make your opt-out request verbally, but a written request is more reliable as you can keep a copy to serve as evidence in case of miscommunication.



VIP privileges?

Using computers and the Internet

Smartphones, computers and other electronic devices enhance the convenience of everyday life, but they store a lot of sensitive data, such as photos, messages, videos and contacts, all of which are your personal data. You should handle and protect carefully to make sure these devices won't become "leakers" of your privacy.

Wi-Fi Connect Safe Surfing?

Things We Can Do

Beware of fake Wi-Fi hotspots

- Seemingly reliable Wi-Fi hotspots in airports, coffee shops or shopping malls may be fake and your information may be intercepted when using these insecure hotspots, so it is prudent to avoid any suspicious Wi-Fi networks. In an unencrypted Wi-Fi network, the data you submit may be intercepted by other users.

Use public Wi-Fi prudently

- Do not use public Wi-Fi networks to access websites or apps for online banking or shopping.
- Home Wi-Fi networks are not entirely safe either. Enable WPA2 encryption to protect any data you transmit.

Before repairing or selling your electronic devices

- When inspecting and maintaining your electronic device, technicians can easily access your stored personal data. Before disposal, be sure you back up and delete all files and data properly and restore the factory setting.
- Avoid storing excessive amount of unencrypted sensitive information in a mobile device, such as account names, passwords, credit card information and ID card number to avoid interception of data if the device is lost.

Things We Can Do

Using social networks and apps

With a smartphone, you can surf the Internet or get in touch with friends anytime, anywhere. You may from time to time update your location, post messages or "likes" on social networks or apps, but you must consider the risk that by doing so you may unintentionally disclose your personal data or whereabouts, and may even infringe on the privacy of your friends or family members.

tips

Beware of social network traps:

- When you create a new account on a social networking site, you should read the privacy policy carefully before providing any personal data, and think carefully about the need to provide sensitive or optional information. Consider registering using different email addresses on different sites to prevent tracking of your identity.
- Once disclosed online, your personal data may be accessed, reproduced or forwarded, and you will no longer have any control over it. Make sure you understand the data-sharing mechanisms and check your privacy settings regularly.
- Synchronising your social network accounts, email accounts and smartphone may expose your personal data to others. Even if you disable a function later, personal data about you or your friends may have already been disclosed.
- Social networking sites are full of malicious links and files, so make sure your anti-virus programme is up-to-date.
- Fragmented information you provide on different sites, if consolidated, may reveal your real identity and profile. Remember to remove any accounts you no longer use and regularly clear your browser cookies to avoid being tracked online.

Understand what information will be accessed before downloading an app

- Malware is everywhere, so it is safer to download an app through official channels.
- Few people read the lengthy privacy policies, but if you do, you may be surprised to find out that many apps can freely access or upload the data stored in your smartphone, including photos, messages, contacts and account information, without your knowledge. It is important to know what data the developers will access, upload and share before downloading an app. Remove it immediately if you do not want the app to access your personal data.
- When you don't need apps or functions like geo-location tagging and location information sharing, which let others know where you have been, you should disable them.

Everyone should be privacy conscious

Our family members, especially children may be unaware of the importance of protecting their privacy. Therefore, we should explain the dangers and show them how to protect themselves against possible privacy breaches.

Things We Can Do

Remind our families :

- Do not let children play with smartphones and avoid sharing phones or computers with family members. If there is such a need, provide appropriate guidance to avoid inadvertent disclouse of data.
- Explain the data protection principles to your children, and remind them to be very careful about uploading photos or posting messages online.
- Be a good role model regarding personal data protection. Respect your children's privacy and never post their personal information or photos on the Internet without their consent.
- Remind all family members not to disclose any personal data when receiving calls from people they do not know, and to confirm the identity of callers by calling them back when in doubt.
- Protect their smartphones with a screen lock as the first line of defense against prying eyes if they leave their smartphones unattended or lost them.
- Do not write down passwords or store passwords together with the related bank cards or documents.
- Change passwords regularly. Do not use phone numbers, dates of birth or ID card numbers as passwords.
- Shred letters or documents containing personal data before disposal.

Care & Love!

Although 90% of smartphone users installed apps, only 27% of them read and considered the privacy policy before installing an app.

Some 57% of app users did not know what information their apps will access, and half of them were unaware that their contact lists may be uploaded to a central server.

Only 53% of smartphone users used screen lock and anti-virus software.

Only 30% of social apps users asked for permission before posting photos of their friends on social networking sites.

*Source: Privacy Awareness Surveys in 2012 and 2013, Office of the Privacy Commissioner for Personal Data, Hong Kong

Disclaimer: The information provided in this leaflet 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 above information. The above suggestions will not affect the functions and powers conferred upon the Commissioner under the Ordinance.

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

www.pcpd.org.hk

" Think Privacy Be Smart Online "website
www.pcpd.org.hk\besmartonline

" Youth Privacy "website
www.pcpd.org.hk\youthprivacy

produced by metropop