HKGCC Manpower Committee Meeting (Virtual)

Working from Home: Safeguarding Personal Data Privacy

2 December 2020

Tony Lam
Deputy Privacy Commissioner for Personal Data, Hong Kong

Work-from-home (WFH) arrangements

- More prevalent since COVID-19
- A new normal?
- Home as workplace: Implications on personal data privacy

6 保障資料原則 Data Protection Principles

PCPD.org.hk

1. 收集目的及方式 Collection Purpose & Means
2. 準確性、儲存及保留 Accuracy & Retention
3. 使用 Use
4. 保安措施 Security
5. 透明度 Openness
6. 查閱及更正 Data Access & Correction

4 保安措施 Security

資料使用者須採取切實可行的步驟，保障個人資料不會未經授權或意外地被查閱、處理、刪除、喪失或使用。

A data user needs to take practicable steps to safeguard personal data from unauthorised or accidental access, processing, erasure, loss or use.

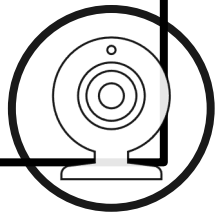
Data security risks under WFH arrangements

- Between the companies' networks and employees' home networks
- Between the corporate devices and employees' personal devices

Increase in access/transfer of data & document

- New risks to data security and personal data privacy

Increased popularity of video conferencing software



Guidance for organisations

Risk assessment

- On data security and employees' personal data privacy

Policies and guidance

- Review and adjust existing policies based on the results of risk assessment
- Provide sufficient guidance (e.g. transfer of data & remote access)

Staff training and support

- Provide sufficient training on data security
- Deploy designated staff to provide support

Device management

- If electronic devices (e.g. smartphones & notebook computers) are provided to employees, ensure the security of data (including personal data) stored in the devices

Use of VPN

- Choose the appropriate protocol and type of VPN, and keep the security setting up-to-date
- Require multi-factor authentication for connection

Best practices for employees

Device management

- Use only corporate electronic devices for work
- Secure the devices and the data therein (e.g. strong passwords & change passwords regularly)

Work environment

- Avoid working in public places
- Refrain from using public Wi-Fi

Wi-Fi connection

- Opt for wired connection
- Ensure the security protocol and firmware of Wi-Fi routers are up-to-date

Electronic communications

- Use only corporate email accounts for sending/receiving work-related documents
- Check the recipient list before sending out messages, and verify suspicious messages

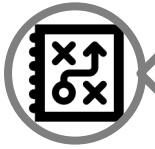
Paper document

- Avoid transferring paper documents out of office premises as far as practicable
- Enhance data security of those documents (e.g. redact or remove personal data)

Practical advice on use of video conferencing

Review and assess the policies and measures on security and protection of personal data privacy of different software

Choose a software that provides end-to-end encryption for meetings involving confidential matters



Safeguard the user accounts by setting up strong passwords, changing the passwords regularly, activating multi-factor authentication , installing latest security patches, etc.

When hosting conferences, set up unique meeting ID and strong password, use virtual waiting room to validate participants' identities, and lock the meeting when all participants are admitted

Any records of the conferences (e.g. video recordings & chat messages) be stored securely with password protection or encryption; they should not be retained for longer than necessary

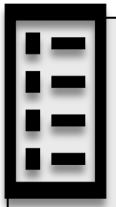
Conclusion

Digital transformation

- Data security and personal data privacy go hand-in-hand

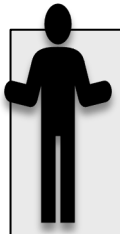
Data security and personal data privacy

- Manage both external and internal aspects



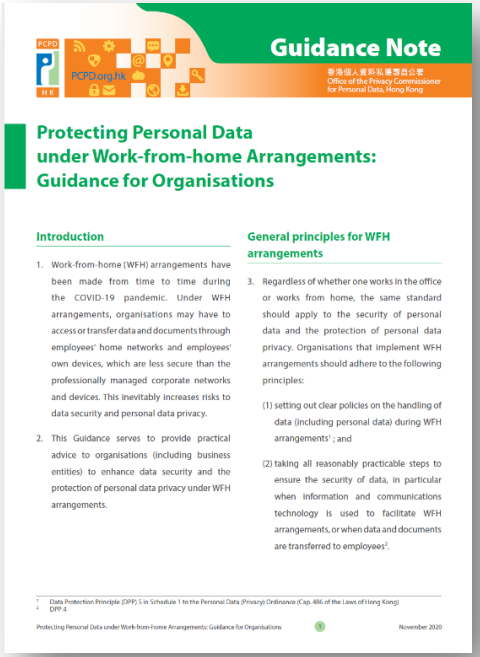
Personal data privacy and six data protection principles

- Always there no matter WFH or work in office



Human factors critical to your transformation

3 Practical Guidance Notes Relating to WFH Arrangements



Guidance Note

Office of the Privacy Commissioner for Personal Data, Hong Kong

Protecting Personal Data under Work-from-home Arrangements: Guidance for Organisations

Introduction

1. Work-from-home (WFH) arrangements have been made from time to time during the COVID-19 pandemic. Under WFH arrangements, organisations may have to access or transfer data and documents through employees' home networks and employees' own devices, which are less secure than the professionally managed corporate networks and devices. This inevitably increases risks to data security and personal data privacy.
2. This Guidance serves to provide practical advice to organisations (including business entities) to enhance data security and the protection of personal data privacy under WFH arrangements.

General principles for WFH arrangements

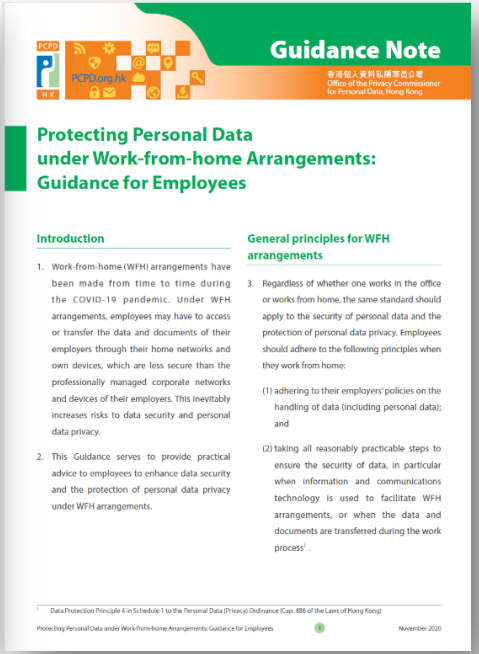
3. Regardless of whether one works in the office or works from home, the same standard should apply to the security of personal data and the protection of personal data privacy. Organisations that implement WFH arrangements should adhere to the following principles:

(1) setting out clear policies on the handling of data (including personal data) during WFH arrangements[1]; and

(2) taking all reasonably practicable steps to ensure the security of data, in particular when information and communications technology is used to facilitate WFH arrangements, or when data and documents are transferred to employees[2].

[1] Data Protection Principle (DPP) 5 in Schedule 1 to the Personal Data (Privacy) Ordinance (Cap. 486 of the Laws of Hong Kong)
[2] DPP 4

Protecting Personal Data under Work-from-home Arrangements: Guidance for Organisations 1 November 2020



Guidance Note

Office of the Privacy Commissioner for Personal Data, Hong Kong

Protecting Personal Data under Work-from-home Arrangements: Guidance for Employees

Introduction

1. Work-from-home (WFH) arrangements have been made from time to time during the COVID-19 pandemic. Under WFH arrangements, employees may have to access or transfer the data and documents of their employers through their home networks and own devices, which are less secure than the professionally managed corporate networks and devices of their employers. This inevitably increases risks to data security and personal data privacy.
2. This Guidance serves to provide practical advice to employees to enhance data security and the protection of personal data privacy under WFH arrangements.

General principles for WFH arrangements

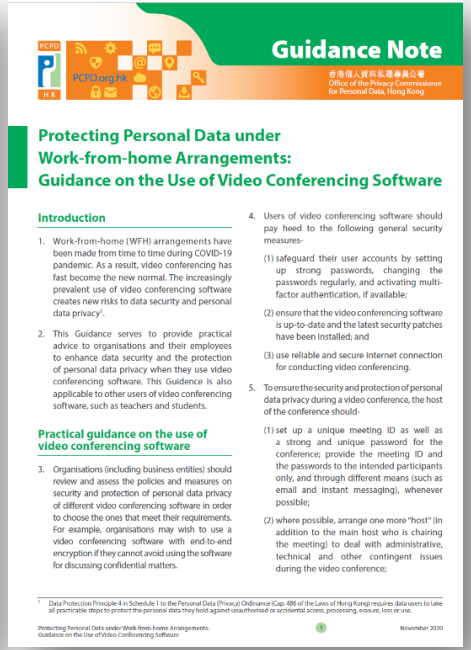
3. Regardless of whether one works in the office or works from home, the same standard should apply to the security of personal data and the protection of personal data privacy. Employees should adhere to the following principles when they work from home:

(1) adhering to their employers' policies on the handling of data (including personal data); and

(2) taking all reasonably practicable steps to ensure the security of data, in particular when information and communications technology is used to facilitate WFH arrangements, or when the data and documents are transferred during the work process[1].

[1] Data Protection Principle 4 in Schedule 1 to the Personal Data (Privacy) Ordinance (Cap. 486 of the Laws of Hong Kong)

Protecting Personal Data under Work-from-home Arrangements: Guidance for Employees 1 November 2020



Guidance Note

Office of the Privacy Commissioner for Personal Data, Hong Kong

Protecting Personal Data under Work-from-home Arrangements: Guidance on the Use of Video Conferencing Software

Introduction

1. Work-from-home (WFH) arrangements have been made from time to time during COVID-19 pandemic. As a result, video conferencing has fast become the new normal. The increasingly prevalent use of video conferencing software creates new risks to data security and personal data privacy[1].
2. This Guidance serves to provide practical advice to organisations and their employees to enhance data security and the protection of personal data privacy when they use video conferencing software. This Guidance is also applicable to other users of video conferencing software, such as teachers and students.

Practical guidance on the use of video conferencing software

3. Organisations (including business entities) should review and assess the policies and measures on security and protection of personal data privacy of different video conferencing software in order to choose the ones that meet their requirements. For example, organisations may wish to use a video conferencing software with end-to-end encryption if they cannot avoid using the software for discussing confidential matters.
4. Users of video conferencing software should pay heed to the following general security measures-

(1) safeguard their user accounts by setting up strong passwords, changing the passwords regularly, and activating multi-factor authentication, if available;

(2) ensure that the video conferencing software is up-to-date and the latest security patches have been installed; and

(3) use reliable and secure internet connection for conducting video conferencing.

5. To ensure the security and protection of personal data privacy during a video conference, the host of the conference should-

(1) set up a unique meeting ID as well as a strong and unique password for the conference; provide the meeting ID and the passwords to the intended participants only, and through different means (such as email and instant messaging), whenever possible;

(2) where possible, arrange one more "host" (in addition to the main host who is chairing the meeting) to deal with administrative, technical and other contingent issues during the video conference;

[1] Data Protection Principle 4 in Schedule 1 to the Personal Data (Privacy) Ordinance (Cap. 486 of the Laws of Hong Kong) requires data users to take all practicable steps to protect the personal data they hold against unauthorised or accidental access, processing, erasure, loss or use.

Protecting Personal Data under Work-from-home Arrangements: Guidance on the Use of Video Conferencing Software 1 November 2020

The 3 Guidance Notes can be downloaded at the PCPD's website: www.pcpd.org.hk

JOIN

Data Protection Officers' Club

(Membership Application)

保障資料主任聯會 Data Protection Officers' Club

By becoming a DPOC member, you will:

- **advance your knowledge and practice of data privacy compliance through experience sharing and training;**
- **enjoy 20% discount on the registration fee for PCPD's Professional Workshops;**
- **receive updates on the latest development in data privacy via regular e-newsletter**

As a DPOC member, your organisation's name will be published on DPOC membership list at PCPD's website, demonstrating your commitment on personal data protection to your existing and potential customers as well as your stakeholders.

Membership fee: HK$350 per year
Enquiries: dpoc@pcpd.org.hk

https://www.pcpd.org.hk/misc/dpoc/enrol.html

Contact Us

www.pcpd.org.hk

Thank You!