GALL

January 2021

Employment Spotlight: Guidance for Protecting Personal Data in Work from Home (WFH) Arrangements

The Privacy Commissioner for Personal Data ("PCPD") has issued Guidance Notes for (1) organisations, (2) employees, and (3) users of video conference software, with a view to enhance measures for data security and data privacy in the use, storage and handling of personal data when employees work from home ("WFH").

In this article we have briefly summarised the three Guidance Notes ("Guidance") published by PCPD and set out key takeaways for employers.

Guidance for Organisations

Organisations, in their capacity as data users, must comply with the Data Protection Principles ("DPP") set out in Schedule 1 of Personal Data (Privacy) Ordinance (Cap 486) ("PDPO") while collecting, handling and using personal data. Briefly, the six DPP are:-

1. **Data collection:** Personal data must be collected lawfully and for a purpose that is directly related to the activity of the data user;

2. **Accuracy and retention:** Data users are required to take practicable steps to ensure that the data is accurate and is not retained for longer than necessary;

3. **Use of data:** Unless consent of the data subject is obtained, the data must be used only for the purpose for which it was obtained;

4. **Data security:** Practicable steps must be taken to prevent unauthorised access, processing, use, loss, or erasure of personal data;

5. **Openness and transparency:** Data users are required to maintain openness regarding their policies and practices for use of data and the purpose for which the data is collected; and

6. **Access and correction:** The data subjects have a right to access their personal data and request correction of personal data. Any refusal to allow access must be reasoned.

The PCPD considers employers to be primarily responsible for data security and personal data privacy. The PCPD recommends the following measures that employers may consider adopting while implementing WFH arrangements:

• Conducting a risk assessment of data security and employees' personal data privacy prior to formulating policies;

• Reviewing and revising existing policies and practices and provide sufficient guidance to the employees in each case regarding transfer of data and documents, remote access to networks and data, erasure and destruction of unnecessary data and materials, and the handling of data breaches;

• Training and providing support to employees for WFH arrangements to ensure data security with designated staff to address concerns arising during WFH;

• Providing employees with devices and including protective measures such as passwords, anti-malware software, remote access to devices, prevention of transfer of data from corporate to personal devices;

• Encouraging the use of virtual private networks to enable secured remote access to corporate networks; and

• Implementing security measures for remote access such as granting access on a need basis only and reviewing of remote access logs to track suspicious activities.

Guidance for Employees

During WFH, employees will have access to employer's data which may be processed through networks that are beyond the employer's control. As such there is a risk of the employee breaching the DPP, particularly the data security principle. Accordingly, the PCPD recommends adopting the following measures to guard against the potential risks:-

• Requiring employees to adhere to their employer's policies on handling of data;

• Suggesting the use of corporate devices during WFH for all work-related matters;

• Avoiding working in public places in order to prevent disclosure of personal data and restricted information. However, if working in a public place is unavoidable, employees should use security measures such as screen filters and mobile hotspots rather than using public Wi-Fi;

• Implementing security measures to be taken while using Wi-Fi such as strong passwords, review of devices connected to the network and use of updated security protocols;

• Requiring employees to use corporate email accounts for all work-related communications; and

• Whilst it is not advisable to carry physical documents out of office, in the event removal becomes necessary, employees should seek approval of their supervisor. Where practicable, the personal data should be redacted before removal and only necessary documents should be removed from the office. In addition, employees should have secure filing cabinets at home and should follow the employer's established shredding procedures.

Guidance for Users of Video Conferencing Software

The increased use of video conferencing software by organisations and employees in the course of WFH poses additional risks to data security and personal data privacy. To provide safeguards, the PCPD recommends the following measures:-

• Prior to opting for a particular video conferencing software, organisations are encouraged to assess the risks associated with its use;

• When using video conferencing facilities, strong passwords and a secure internet connection should be used;

• The host of the video conference should take measures such as setting up unique meeting ID, virtual waiting room to allow authorised access only and obtain consent of participants before recording and storing records; and

• The participants should also be careful that their background setting during the video conference and screen sharing functions do not lead to inadvertent disclosure of personal data and restricted information.

Key Takeaways

Although the Guidance lacks statutory force, it serves as a helpful guide for organisations to consider when implementing WFH arrangements. Employers should consider reviewing their existing policies and incorporate additional measures as appropriate to protect the personal data of individuals and other confidential information.

Employers and organisations may consider seeking legal advice to review and revise their policies relating to personal data privacy in the context of WFH. In case of employment law related queries, please get in touch with Andrea Randall (andrearandall@gallhk.com / +852 3405 7688) and Nick Dealy (ndealy@gallhk.com / +852 3405 7688).

GALL

Contacts

Nick Dealy
Partner
+852 3405 7656
ndealy@gallhk.com

Kritika Sethia
Legal Analyst
+852 3405 7654
kritikasethia@gallhk.com