Inspection Report

(published under Section 48(1) of
the Personal Data (Privacy) Ordinance, Chapter 486, Laws of Hong Kong)

Customers' Personal Data Systems of (1) CLP Power Hong Kong Limited and (2) The Hongkong Electric Company, Limited

Report Number： R21 - 3099

Date of Issue: 18 August 2021

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

Customers' Personal Data Systems of
(1) CLP Power Hong Kong Limited and
(2) The Hongkong Electric Company, Limited

Section 36 of the Personal Data (Privacy) Ordinance, Chapter 486, Laws of Hong Kong (the Ordinance) provides that:-

"*Without prejudice to the generality of section 38, the Commissioner may carry out an inspection of-*

(a) any personal data system used by a data user; or

(b) any personal data system used by a data user belonging to a class of data users,

for the purposes of ascertaining information to assist the Commissioner in making recommendations-

(i) to-

(A) where paragraph (a) is applicable, the relevant data user;

(B) where paragraph (b) is applicable, the class of data users to which the relevant data user belongs; and

(ii) relating to the promotion of compliance with the provisions of this Ordinance, in particular the data protection principles, by the relevant data user, or the class of data users to which the relevant data user belongs, as the case may be."

The term "personal data system" is defined in section 2(1) of the Ordinance to mean "*any system, whether or not automated, which is used, whether in whole or in part, by a data user for the collection, holding, processing or use of personal data, and includes any document and equipment forming part of the system*."

Section 48 of the Ordinance provides that:-

"*(1) ... the Commissioner may, after completing an inspection where section 36(b) is applicable, publish a report-*

(a) setting out any recommendations arising from the inspection that the Commissioner thinks fit to make relating to the promotion of compliance with the provisions of this Ordinance, in particular the data protection principles, by the class of data users to which the relevant data user belongs; and

(b) in such manner as he thinks fit."

This inspection report is hereby published in discharge of the powers under section 48(1) of the Ordinance.

Ada CHUNG Lai-ling
Privacy Commissioner for Personal Data, Hong Kong
18 August 2021

Table of Contents

Inspection Report

(published under Section 48(1) of the Personal Data (Privacy) Ordinance, Chapter 486, Laws of Hong Kong)

Customers' Personal Data Systems of
(1) CLP Power Hong Kong Limited and
(2) The Hongkong Electric Company, Limited

Executive Summary

Background

Public utility companies handle vast amounts of customers' personal data in the routine course of maintaining service accounts, processing bills and handling customer enquiries. In addition to providing reliable and high-quality services, public utilities are expected to embrace personal data privacy protection as part of their corporate governance and protect the personal data systems of their customers from unauthorised access, processing and use.

The Privacy Commissioner for Personal Data, Hong Kong (the Commissioner) considers that it is in the public interest to carry out an inspection of the customers' personal data systems of public utility companies (the Inspection) pursuant to section 36 of the Personal Data (Privacy) Ordinance (Cap. 486) (the Ordinance). CLP Power Hong Kong Limited (CLP) and The Hongkong Electric Company, Limited (HKE) were selected for the Inspection.

Key Findings

Areas of good practice

During the Inspection, the Commissioner was pleased to note that both CLP and HKE had strived to devote their efforts to protecting their customers' personal data and that they set good examples in the following areas:

(i) The two companies strived to implement a Personal Data Privacy Management Programme which incorporated a framework of accountability, embrace the protection of personal data as part of their corporate governance, and, right from the boardroom, foster a respectful culture for protecting personal data privacy.

(ii) The two companies appointed Data Protection Officers, who were senior staff members designated to oversee the compliance with the Ordinance throughout the organisations. The Data Protection Officers had clear reporting lines to senior management on data protection issues.

(iii) Data protection policies were reviewed and communicated to staff members regularly with training needs identified by the Data Protection Officers and the departmental coordinators of the two companies.

(iv) The two companies maintained their personal data inventory with a clear picture of the kinds of customers' personal data held by the companies, where the data was stored, the purposes of use, and the retention schedules of the data. The two companies would review and update their personal data inventory annually.

(v) The two companies demonstrated good practice in formulating access by staff members to customers' personal data systems based on their respective roles, with regular reviews of access rights. For example, when a staff member was

transferred to another post, his access right to the customers' personal data system would be reviewed and updated as appropriate before the effective date of the new posting.

(vi) As part of their ongoing efforts to enhance information security, the two companies strived to take security measures that were consistent with international standards for protecting the personal data systems of customers from cyberattack or hacking.

(vii) The two companies provided a series of data protection training for their staff. In particular, CLP provided specific trainings for staff members on how to set up and memorise complicated passwords (over 10 digits) without writing them down. Besides, CLP also highlighted the serious legal consequences of doxxing activities in its staff training materials.

Areas for improvement

Despite the above good practices adopted by CLP and HKE, it was found during the Inspection that there was room for improvement for both companies in the monitoring mechanism to track staff access to customers' personal data.

The personal data systems of customers of the two companies had mechanisms in place to check for any abnormalities in the log records. However, the Inspection Team found that the systems of the two companies could only track staff identity, time and duration of log-in, and events created by staff members (i.e. data input or changed by users), without recording the search activities. Under such circumstances, it would be difficult for the two companies to detect abnormal access to customers' personal data by an individual staff member, such as conducting name search or accessing the contact details of customers out of curiosity or for other purposes.

Conclusion

According to the findings of the Inspection, both CLP and HKE have been striving to implement a Personal Data Privacy Management Programme and adopting good practices. The security measures adopted by the two companies regarding the personal data systems of their customers conformed with international standards and were found to be satisfactory. The Commissioner considers that in the protection of their customers' personal data, the two companies comply with the requirements of Data Protection Principle 4 of Schedule 1 to the Ordinance as regards the security of personal data.

Recommendations

Through the findings of the Inspection, the Commissioner would like to make the following recommendations to public utility companies and organisations handling vast amounts of customers' personal data:

(i) **Prepare for the unexpected**: The accelerated development of technology has brought with it unprecedented yet non-negligible risks to personal data privacy. Nowadays, many organisations have allocated substantial resources for advanced cyber security technology to protect their networks and databases from external threats. Organisations should, however, be mindful of the risks of customers' personal data being abused by malicious insiders who use the data for doxxing or other illegal purposes.

(ii) **Develop Personal Data Privacy Management Programme (PMP)**: Organisations should establish and maintain a proper system for the responsible use of personal data in compliance with the Ordinance. PMP can help organisations comply with the Ordinance, handle data breaches promptly, and gain trust from customers and other stakeholders.

(iii) **Appoint Data Protection Officers**: Designated staff members who are tasked with monitoring compliance with the Ordinance should have clear

reporting lines to senior management. Incorporating data protection issues raised by staff and lessons learnt from incidents involving customers' personal data into corporate training materials should be one of the duties of Data Protection Officers.

(iv) **Establish personal data inventory**: Organisations should establish and maintain corporate-wide personal data inventory to ensure that all relevant staff understand what personal data they are processing and what procedures are in place to protect the data.

(v) **Devise system security policies and procedures:** Organisations should devise system security policies that comply with international standards, conduct regular security risk assessments and monitor the effectiveness of the security measures in place, with a view to taking improvement measures to protect customers' personal data systems from cyberattack or hacking.

(vi) **Role-based access to customers' data**: Organisations should restrict access to customers' personal data to staff members who have a genuine need of the data to perform their respective duties. For example, a member of technical staff, regardless of his/her rank, would not need to access the contact information of customers. Granular access control could effectively avoid misuse of personal data. As some old systems may not support granular access control, organisations should consider incorporating such control functions when they update the existing system or develop a new system to manage customers' personal data.

(vii) **Implement monitoring on top of preventive measures:** Comprehensive audit logs can capture users' digital footprints. To effectively monitor all suspicious behaviours, organisations should adopt systems which are capable of tracking staff members' access to the data, including their search and modification records. Once a suspicious behaviour is detected, the organisation should consider reporting the incident to the Police and the Office of the Privacy Commissioner for Personal Data without delay.

(viii) **Protect both electronic and paper records**: Retention policies and practices should be in place for both electronic and paper records. Organisations should establish a mechanism to regularly monitor the scheduled destruction of documents containing personal data. Meanwhile, a clean desk policy can reduce the risk of unauthorised internal access to documents containing customers' personal data. It can also reduce the risk of documents being misplaced or losing personal data.

(ix) **Measures to raise staff awareness**: A comprehensive data protection training programme will help to create a culture of respecting and protecting customers' personal data across the organisation. To prevent corporate databases from becoming the source of doxxing activities, staff should be reminded that unauthorised access to customers' personal data may constitute criminal offence under the Ordinance or other laws and regulations. The court rulings on doxxing cases can be included in the training materials to remind staff of the serious legal consequences of doxxing.

Part I – Introduction

Background

1. Public utility companies handle vast amounts of customers' personal data in the routine course of maintaining service accounts, processing bills and handling customer enquiries. In addition to providing reliable and high-quality services, public utilities are expected to embrace personal data privacy protection as part of their corporate governance and protect the personal data systems of their customers from unauthorised access, processing and use.

2. The rapid development of technology and the shift from paper-based to electronic records have enhanced efficiency in data processing. However, the extensive use of computer databases or data systems allows greater complexity in how customers' personal data is stored and protected.

3. Meanwhile, work-from-home (WFH) arrangements have been implemented by both public and private organisations from time to time since early 2020 due to the COVID-19 pandemic. As a result, remote access to corporate networks may have to be granted to employees. This, coupled with the public concern about doxxing activities[1] that corporate databases may be the possible source from which doxxers obtain the information[2], indicates that enhancing access control of customers' data systems has become a pressing task for organisations handling vast amounts of customers' personal data.

[1] Doxxing involves the gathering of the personal data of a target or even his/her family members from different sources and the subsequent disclosure of such personal data on the internet, social media platforms or other open platforms without the consent of the relevant data subject.

[2] In a doxxing case sentenced in November 2020, the defendant took advantage of his work in a telecommunications company to obtain the personal data of a family member of a police officer through his office computer, and disclosed the data to a group on a social media platform for doxxing, thereby causing psychological harm to the victim.

4. The powers of the Privacy Commissioner for Personal Data, Hong Kong (the Commissioner) are conferred by the Personal Data (Privacy) Ordinance (Cap. 486) (the Ordinance). According to section 8(1) of the Ordinance, the Commissioner shall monitor and supervise compliance with the provisions of the Ordinance, and promote awareness and understanding of, and compliance with, the provisions of the Ordinance. Section 36 of the Ordinance empowers the Commissioner to carry out an inspection of any personal data system used by a data user or by a data user belonging to a class of data users.

5. The Commissioner considers that it is in the public interest to carry out an inspection of the customers' personal data systems of public utility companies (the Inspection) pursuant to section 36 of the Ordinance. CLP Power Hong Kong Limited (CLP) and The Hongkong Electric Company, Limited (HKE) were selected for the Inspection.

Scope of the Inspection

6. Before the Inspection, the Commissioner informed CLP and HKE respectively in writing of her intention to carry out the Inspection. In response, the two companies expressed their support and cooperation by furnishing the Commissioner with relevant information about the personal data systems of their customers. It was agreed that the Inspection would focus on the security measures in relation to the two companies' access control of the personal data systems of their customers.

7. The common features and purposes of the personal data systems of their customers of the two companies are as follows:

(i) Maintaining consumption and billing information about each customer account linked to a specific supply address;

(ii) Maintaining personal particulars (names, supply addresses, correspondence addresses, telephone numbers, email addresses, and etc) of residential account holders or contact persons of commercial accounts;

(iii) Enabling end users of the systems (designated staff of the two companies) to view and add information to the systems;

(iv) Supporting interactive customer services through the internet or by hotline, such as offering online platforms for customers to close their accounts, transfer their accounts and open new accounts for new addresses; and

(v) Providing useful and timely information to the management for planning and decision making.

8. In respect of security of personal data, Data Protection Principle (DPP) 4 of Schedule 1 to the Ordinance requires that all practicable steps shall be taken to ensure that any personal data held by a data user is protected against unauthorised or accidental access, processing, erasure, loss or use.

9. In addition to data security and access controls (DPP4), other DPPs, in particular DPP1 (data collection) and DPP2(2) (data retention), are also relevant to the protection of customers' personal data. The six DPPs are reproduced at **Appendix A** for ease of reference.

10. The Ordinance is by design principle-based and technology-neutral. DPP4 does not set out a checklist of specific requirements of data security and access control procedures to be undertaken by data users. Generally speaking, the Commissioner considers that the stringency of data security and access control

procedures should be commensurate with the risks to personal data privacy. Having regard to the amount and nature of customers' personal data handled by the two companies, the Commissioner defined the main scope of assessment on the two companies' policies and practices as follows:

Risks to personal data privacy	**Scope of assessment**
<u>Inherent corporate privacy risk</u> • If personal data not necessary for the purpose of providing services to customers is collected, there will be a greater impact to customers in case of data breach. • If an organisation fails to maintain an up-to-date personal data inventory, it cannot effectively monitor and keep track of the retention period of records that contain customers' personal data.	(1) Data governance structure (2) Personal data inventory (3) Data retention policy and practice
<u>Internal threat</u> • Inappropriate access rights to customers' personal data may make it more likely for staff to misuse the data for sales, cyberbullying or doxxing. • Accidental loss of documents or portable devices containing customers' personal data by staff.	(4) Access control of the personal data system of customers (5) Monitoring mechanism to track access (6) Work-from-Home arrangements (7) Staff training and privacy awareness program

Risks to personal data privacy	Scope of assessment
<u>External threat</u> • Cyberattack or hacking	(8) Physical and system security measures (9) Third party audit on data security system

Part II – Methodology

11. For the purpose of inspecting the customers' personal data systems of CLP and HKE and how the staff members effectively comply with the companies' data security policies and practices, the Commissioner obtained from the two companies all relevant policies, manuals, guidelines, employees' code of conduct and training materials for examination.

12. Besides, the Commissioner exercised her power of entry to premises under the Ordinance to conduct on-site visits for practical assessment. In March 2021, with the agreement of CLP and HKE, the Inspection Team[3] (the Team) conducted 7 visits to 11 departments of the two companies, including their head offices, branch offices, data centres and call centres.

13. The fieldwork of the Team included:

(i) Face-to-face interviews with responsible personnel for the management of the customers' personal data systems;

(ii) Walk-through of the various departments of the two companies to examine the actual operation of the customers' personal data systems and the relevant access control mechanisms;

(iii) More than 100 staff members of the two companies (who were selected on the basis that they had access to the customers' personal data systems) were invited to complete a questionnaire about their awareness and

[3] The Inspection Team was composed of one Chief Personal Data Officer, two Senior Personal Data Officers and four Personal Data Officers.

attitude on the protection of customers' personal data at work[4]. A copy of the questionnaire is at **Appendix B**.

14. This Inspection Report (the Report) is intended to help the two companies to recognise the areas of improvements that they can make. Meanwhile, the findings show how the two companies endeavoured to protect their customers' personal data and how they may set good examples for other data users on data protection policies and practices. The Commissioner does not consider it necessary to comment on which of the companies performs better or worse in specific areas.

[4] Due to the outbreak of COVID-19 at the material time of the Inspection, the questionnaires were completed and returned in electronic form with a view to maintaining good social distance.

Part III – Findings

15. This Report is based on the information provided by CLP and HKE and the matters that came to the Team's attention during the on-site inspection. The legal obligation to comply with the requirements under the Ordinance rests with the two companies. The findings and recommendations made in this Report do not in any way affect or prejudice the Commissioner in exercising any powers or performing any functions under the Ordinance.

(1) Data governance structure

16. In view of the ever-rising expectation of customers and stakeholders on the responsible use of personal data by companies, for organisations to gain customers' trust and enhance their corporate reputation and competitive edges, the Commissioner has been advocating the development of their own Personal Data Privacy Management Programme (PMP) and the appointment of a Data Protection Officer to institutionalise a proper system for the responsible use of personal data in compliance with the Ordinance[5]. In this regard, the adoption of a PMP by companies has been included in the Guide for Independent Non-Executive Directors published by the Hong Kong Institute of Directors, in which companies are encouraged to implement a PMP as one of the drivers for the adoption of "Environmental, Social and Governance" (ESG) management.

17. The Team noted that the top management of the two companies had attached importance and given priority to the handling of personal data privacy, and committed to fostering a culture of respecting and protecting personal data privacy among their employees. Both companies' data protection policies and procedures made it clear from the outset that customers' personal data was

[5] For examples and practical guidance on how to devise and implement a comprehensive PMP, please refer to the Best Practice Guide on Privacy Management Programme: https://www.pcpd.org.hk//english/resources_centre/publications/files/PMP_guide_e.pdf

classified as "confidential" which must be treated with the highest level of precaution in terms of storage, use and disposal.

18. While one of the components of a PMP is the appointment of a Data Protection Officer/establishment of a Data Protection Office to oversee compliance with the Ordinance and implementation of the PMP, the Data Protection Officers of the two companies were senior executives reporting directly to the top management. Insofar as their duties in structuring, designing and managing the PMP were concerned, they involved all relevant procedures, training, monitoring or auditing, documenting, evaluating, and other follow-up actions in relation to the collection, holding, processing and use of personal data.

19. Departmental coordinators were appointed by the two companies to support the Data Protection Officers. In this regard, both companies established internal reporting mechanisms for handling staff enquiries in relation to personal data privacy and incidents of possible data breaches. Other than regular reports, the departmental coordinators and the Data Protection Officer would work together to consolidate the problems encountered by different business units, and identify the relevant areas of concerns for preparation of lessons learnt and practical tips in staff training materials.

(2) Personal data inventory

20. Documenting personal data processing is a key component of a PMP. Comprehensive and updated personal data inventory could assist an organisation to review from time to time what personal data was collected and for what purpose, as well as how the data should be protected.

21. The Team found that both companies maintained personal data inventory with information on the kinds of personal data collected (names, supply addresses,

correspondence addresses, telephone numbers, email addresses, and etc), locations of data storage, duration of retention, and how the personal data was processed. Both companies would conduct annual reviews of the personal data inventory to ensure that the collection of personal data was in line with the principle of data minimisation, and the personal data collected were necessary but not excessive.

(3) Data retention policy and practice

22. The two companies had formal retention policies in place for customers' personal data to ensure that no personal data should be kept longer than necessary for the fulfilment of the purpose for which the data is used[6].

23. The retention policies consisted of the following components:

(i) Designated staff were responsible for destroying personal data no longer required;

(ii) The retention period of personal data would depend on the type of the data;

(iii) Disposal methods and security measures were set out;

(iv) Destruction records were maintained;

(v) Both electronic and paper records were covered.

24. During the Inspection, however, the Team found that some service application forms collected by HKE from customers in 2018, which should have been destroyed within two years of receipt in accordance with the relevant retention period of physical copies of service application forms, were still kept in a

[6] Requirement under DPP2(2)

cabinet. According to HKE, some of the forms had not been destroyed yet as follow-up actions in respect of those forms were being taken at the material time of the Inspection.

25. The Commissioner recommends that HKE should store service application forms requiring no further action and service application forms pending further action separately, and that HKE should ensure the scheduled destruction of physical copies of service application forms that require no further action.

(4) Access control of customers' personal data system

26. The two companies adopted good practices in staff access to customers' personal data system as follows:

(i) **Role-based access**: Access was granted on a "need-to-know" basis commensurate with the ranks, roles and responsibilities of staff members. For example, a hotline staff member of the customer service centre was allowed to check customers' billing information for handling customers' enquiries, whereas a staff member working in the human resources department was not allowed to do so.

(ii) **Procedures for updating and removing access**: Written approval must be obtained before granting any access right to individual staff members. The access rights were reviewed and updated before any staff movement to ensure that no staff member would have unnecessary access rights. At CLP, "privileged access" was only available for a short duration and the access would be automatically removed by the system upon the expiry of a pre-determined period.

(iii) **Password management**: Staff of the two companies were assigned with unique user IDs and passwords. There were policies prohibiting any sharing of passwords and requiring passwords to be changed on a

regular basis. Passwords must fulfil the minimum length and complexity requirements. A user account would be locked after repeated incorrect login attempts.

To prevent staff members from "writing down" complicated passwords (over 10 digits), CLP provided specific trainings for staff members on how to set up and memorise complicated passwords. During the Inspection, the Team did not find any sticky notes or pieces of paper showing passwords attached to computer monitors or placed on workstations.

(5) Monitoring mechanism to track access

27. The Team noted that the two companies had maintained activity log records for all staff access to the personal data systems of their customers. There were mechanisms in place to check any abnormalities in the log records, and alert the relevant supervisory staff in case of abnormal activities (such as bulk data downloaded by an individual staff member). Both companies maintained log records for regular audit purposes.

28. Nevertheless the Team found that the systems of both companies could only track staff identity, time and duration of log-in, and events created by staff members (i.e. data input or changed by users), without recording the search activities. Under such circumstances, it would be difficult for both companies to detect abnormal access to customers' personal data by an individual staff member, such as conducting name search or accessing the contact details of customers out of curiosity or for other purposes.

29. To effectively detect any suspicious behaviours, the Commissioner recommends that both companies should consider upgrading their systems so that they could track staff members' full digital footprints, including their

search activities conducted in the systems. Once any suspicious behaviours are detected, the company concerned should consider reporting the incident to the Police and the Office of the Privacy Commissioner for Personal Data without delay.

(6) Work-from-Home arrangements

30. WFH arrangements have been implemented by organisations in Hong Kong from time to time since early 2020 due to the COVID-19 pandemic, rendering personal data more susceptible to security breach than ever before. In November 2020, the Commissioner issued three Guidance Notes under the series of "Protecting Personal Data under Work-from-Home Arrangements" as practical advice to organisations (The Guidance for Organisations is at **Appendix C**), employees, and users of video conferencing software, to enhance data security and protection of personal data.

31. The Team noted that the two companies had established policies for remote working covering the following issues:

(i) Technical controls for remote access to corporate network (e.g. deployment of multi-factor authentication); and

(ii) Procedures for authorising remote working.

32. The Commissioner recommends that the two companies should pay heed to the three Guidance Notes mentioned in paragraph 30 above when reviewing their WFH policies, and take into account their actual business situation in the future. The following practical tips should be offered to staff members:

(i) Avoid working in public places to prevent accidental disclosure of personal data or restricted information to third parties;

(ii) Use only corporate electronic devices for work as far as practicable;

(iii) Enhance the security of Wi-Fi connections and electronic communications (e.g. encryption of emails and attachments);

(iv) Ensure proper handling of data when it is necessary to take paper documents out of office premises.

(7) Staff training and privacy awareness program

33. The Team found that the two companies had provided a series of data protection training for their staff as follows:

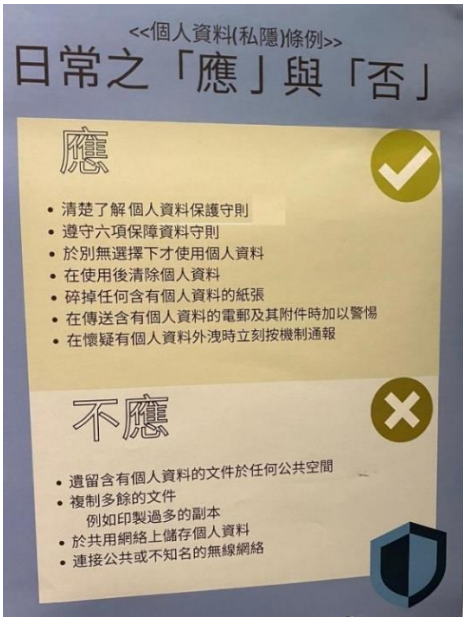
(i) Mandatory training for new recruits before they were allowed to access the customers' personal data systems;

(ii) Regular seminars or workshops as refresher training;

(iii) E-learning and videos; and

(iv) Posters were put up around the offices to raise staff awareness and enhance knowledge about data protection.

34. Below are posters found during the Inspection:



35. Apart from the introduction of the Ordinance and the DPPs, the Team noted that CLP had highlighted the serious legal consequences of doxxing activities in the training materials.

36. To prevent corporate databases from becoming the source of doxxing activities, the Commissioner recommends that staff members of the two companies should be reminded that unauthorised access to customers' personal data may constitute criminal offence under the Ordinance or other laws and regulations. The court rulings on doxxing cases can be included in the training materials to remind staff of the serious legal consequences of doxxing.

(8) Physical and system security measures

Physical Security

37. The Team noted that there were physical security measures in place in both companies to prevent unauthorised access to the workplaces, thereby reducing the risk of unauthorised access to customers' personal data. Such measures included:

(i) Visitors must be registered and escorted by staff members;

(ii) A smart card access system;

(iii) Visitors must wear badges for identification; and

(iv) A clean desk policy.

38. The clean desk policy could reduce the risk of unauthorised or accidental internal access to documents containing customers' personal data. It could also reduce the risk of documents being misplaced or losing personal data. During the site inspection, the Team found that physical files containing customers' personal data were locked up in restricted areas.

39. The Team noted that CLP would conduct regular checks in the workplaces to see whether documents containing customers' personal data would be left unattended. If non-compliance with the clean desk policy was detected, the staff member concerned would receive a warning label reminding him/her to take remedial action without delay.

40. The Commissioner recommends that the two companies should continue with their efforts to implement clean desk policy and conduct regular checks to ensure staff compliance.

System Security

41. The Team appreciated the ongoing efforts made by both CLP and HKE to enhance information security and pay heed to the international standard ISO/IEC 27002 Code of Practice for information security controls when formulating their information security policies, which covered systems protection, access control, physical security, and so on. The technical measures included firewall, data loss prevention system and end points control, and more. Owing to the confidentiality of the security technology, no details will be revealed in the Report.

(9) Third-party audit on data security system

42. The Team noted that both CLP and HKE designated an internal department to carry out periodic audits on different business operations and make recommendations on personal data protection.

43. Furthermore, CLP engaged an external consultant to examine its IT security and data security while HKE engaged an external consultant to perform an assessment on its IT systems. Both companies took corrective actions in response to the audit results.

Conclusion

44. According to the findings of the Inspection, both CLP and HKE have been striving to implement a PMP, and adopting good practices. The security measures adopted by the two companies regarding the personal data systems of their customers conformed with international standards and were found to be satisfactory. The Commissioner considers that in the protection of their customers' personal data, the two companies comply with the requirements of DPP4 of Schedule 1 to the Ordinance as regards the security of personal data.

Part IV – Recommendations

45. Through the findings of the Inspection, the Commissioner would like to make the following recommendations to public utility companies and organisations handling vast amounts of customers' personal data:

(i) **Prepare for the unexpected**: The accelerated development of technology has brought with it unprecedented yet non-negligible risks to personal data privacy. Nowadays, many organisations have allocated substantial resources for advanced cyber security technology to protect their networks and databases from external threats. Organisations should, however, be mindful of the risks of customers' personal data being abused by malicious insiders who use the data for doxxing or other illegal purposes.

(ii) **Develop Personal Data Privacy Management Programme (PMP)**: Organisations should establish and maintain a proper system for the responsible use of personal data in compliance with the Ordinance. PMP can help organisations comply with the Ordinance, handle data breaches promptly, and gain trust from customers and other stakeholders.

(iii) **Appoint Data Protection Officers**: Designated staff members who are tasked with monitoring compliance with the Ordinance should have clear reporting lines to senior management. Incorporating data protection issues raised by staff and lessons learnt from incidents involving customers' personal data into corporate training materials should be one of the duties of Data Protection Officers.

(iv) **Establish personal data inventory**: Organisations should establish and maintain corporate-wide personal data inventory to ensure that all relevant staff understand what personal data they are processing and what procedures are in place to protect the data.

(v) **Devise system security policies and procedures:** Organisations should devise system security policies that comply with international standards, conduct regular security risk assessments and monitor the effectiveness of the security measures in place, with a view to taking improvement measures to protect customers' personal data systems from cyberattack or hacking.

(vi) **Role-based access to customers' data**: Organisations should restrict access to customers' personal data to staff members who have a genuine need of the data to perform their respective duties. For example, a technical staff, regardless of his/her rank, would not need to access the contact information of customers. Granular access control could effectively avoid misuse of personal data. As some old systems may not support granular access control, organisations should consider incorporating such control functions when they update the existing system or develop a new system to manage customers' personal data.

(vii) **Implement monitoring on top of preventive measures:** Comprehensive audit logs can capture users' digital footprints. To effectively monitor all suspicious behaviours, organisations should adopt systems which are capable of tracking staff members' access to the data, including their search and modification records. Once a suspicious behaviour is detected, the organisation should consider reporting the incident to the Police and the Office of the Privacy Commissioner for Personal Data without delay.

(viii) **Protect both electronic and paper records**: Retention policies and practices should be in place for both electronic and paper records. Organisations should establish a mechanism to regularly monitor the scheduled destruction of documents containing personal data. Meanwhile, a clean desk policy can reduce the risk of unauthorised internal access to documents containing customers' personal data. It can

also reduce the risk of documents being misplaced or losing personal data.

(ix) **Measures to raise staff awareness**: A comprehensive data protection training programme will help to create a culture of respecting and protecting customers' personal data across the organisation. To prevent corporate databases from becoming the source of doxxing activities, staff should be reminded that unauthorised access to customers' personal data may constitute criminal offence under the Ordinance or other laws and regulations. The court rulings on doxxing cases can be included in the training materials to remind staff of the serious legal consequences of doxxing.

Appendix A

Schedule 1

[ss. 2(1) & (6)]

Data Protection Principles

1. Principle 1—purpose and manner of collection of personal data

(1) Personal data shall not be collected unless—

(a) the data is collected for a lawful purpose directly related to a function or activity of the data user who is to use the data;

(b) subject to paragraph (c), the collection of the data is necessary for or directly related to that purpose; and

(c) the data is adequate but not excessive in relation to that purpose.

(2) Personal data shall be collected by means which are—

(a) lawful; and

(b) fair in the circumstances of the case.

(3) Where the person from whom personal data is or is to be collected is the data subject, all practicable steps shall be taken to ensure that— *(Amended 18 of 2012 s. 40)*

(a) he is explicitly or implicitly informed, on or before collecting the data, of—

(i) whether it is obligatory or voluntary for him to supply the data; and

(ii) where it is obligatory for him to supply the data, the consequences for him if he fails to supply the data; and

(b) he is explicitly informed—

(i) on or before collecting the data, of—

(A) the purpose (in general or specific terms) for which the data is to be used; and

(B) the classes of persons to whom the data may be transferred; and

(ii) on or before first use of the data for the purpose for which it was collected, of— *(Amended 18 of 2012 s. 40)*

(A) his rights to request access to and to request the correction of the data; and

(B) the name or job title, and address, of the individual who is to handle any such request made to the data user, *(Replaced 18 of 2012 s. 40)*

unless to comply with the provisions of this subsection would be likely to prejudice the purpose for which the data was collected and that purpose is specified in Part 8 of this Ordinance as a purpose in relation to which personal data is exempt from the provisions of data protection principle 6.

(Amended 18 of 2012 s. 40; E.R. 1 of 2013)

2. Principle 2—accuracy and duration of retention of personal data

(1) All practicable steps shall be taken to ensure that—

(a) personal data is accurate having regard to the purpose (including any directly related purpose) for which the personal data is or is to be used;

(b) where there are reasonable grounds for believing that personal data is inaccurate having regard to the purpose (including any directly related purpose) for which the data is or is to be used— *(Amended 18 of 2012 s. 40)*

(i) the data is not used for that purpose unless and until those grounds cease to be applicable to the data, whether by the rectification of the data or otherwise; or

(ii) the data is erased;

(c) where it is practicable in all the circumstances of the case to know that—

(i) personal data disclosed on or after the appointed day to a third party is materially inaccurate having regard to the purpose (including any directly related purpose) for which the data is or is to be used by the third party; and

(ii) that data was inaccurate at the time of such disclosure, that the third party—

(A) is informed that the data is inaccurate; and

(B) is provided with such particulars as will enable the third party to rectify the data having regard to that purpose. *(Amended 18 of 2012 s. 40)*

(2) All practicable steps must be taken to ensure that personal data is not kept longer than is necessary for the fulfillment of the purpose (including any directly related purpose) for which the data is or is to be used. *(Amended 18 of 2012 s. 40)*

(3) Without limiting subsection (2), if a data user engages a data processor, whether within or outside Hong Kong, to process personal data on the data user's behalf, the data user must adopt contractual or other means to prevent any personal data transferred to the

data processor from being kept longer than is necessary for processing of the data. *(Added 18 of 2012 s. 40)*

(4) In subsection (3)—

data processor (資料處理者) means a person who—

(a) processes personal data on behalf of another person; and

(b) does not process the data for any of the person's own purposes. *(Added 18 of 2012 s. 40)*

3. Principle 3—use of personal data

(1) Personal data shall not, without the prescribed consent of the data subject, be used for a new purpose. *(Amended 18 of 2012 s. 40)*

(2) A relevant person in relation to a data subject may, on his or her behalf, give the prescribed consent required for using his or her personal data for a new purpose if—

(a) the data subject is—

(i) a minor;

(ii) incapable of managing his or her own affairs; or

(iii) mentally incapacitated within the meaning of section 2 of the Mental Health Ordinance (Cap. 136);

(b) the data subject is incapable of understanding the new purpose and deciding whether to give the prescribed consent; and

(c) the relevant person has reasonable grounds for believing that the use of the data for the new purpose is clearly in the interest of the data subject. *(Added 18 of 2012 s. 40)*

(3) A data user must not use the personal data of a data subject for a new purpose even if the prescribed consent for so using that data has been given under subsection (2) by a relevant person, unless the data user has reasonable grounds for believing that the use of that data for the new purpose is clearly in the interest of the data subject. *(Added 18 of 2012 s. 40)*

(4) In this section—

new purpose (新目的), in relation to the use of personal data, means any purpose other than—

(a) the purpose for which the data was to be used at the time of the collection of the data; or

(b) a purpose directly related to the purpose referred to in paragraph (a). *(Added 18 of 2012 s. 40)*

4. Principle 4—security of personal data

(1) All practicable steps shall be taken to ensure that any personal data (including data in a form in which access to or processing of the data is not practicable) held by a data user is protected against unauthorized or accidental access, processing, erasure, loss or use having particular regard to— *(Amended 18 of 2012 s. 40; 17 of 2018 s. 129)*

(a) the kind of data and the harm that could result if any of those things should occur;

(b) the physical location where the data is stored; *(Amended 18 of 2012 s. 40)*

(c) any security measures incorporated (whether by automated means or otherwise) into any equipment in which the data is stored; *(Amended 18 of 2012 s. 40)*

(d) any measures taken for ensuring the integrity, prudence and competence of persons having access to the data; and

(e) any measures taken for ensuring the secure transmission of the data.

(2) Without limiting subsection (1), if a data user engages a data processor, whether within or outside Hong Kong, to process personal data on the data user's behalf, the data user must adopt contractual or other means to prevent unauthorized or accidental access, processing, erasure, loss or use of the data transferred to the data processor for processing. *(Added 18 of 2012 s. 40)*

(3) In subsection (2)—
data processor (資料處理者) has the same meaning given by subsection (4) of data protection principle 2. *(Added 18 of 2012 s. 40)*

5. Principle 5—information to be generally available

All practicable steps shall be taken to ensure that a person can—

(a) ascertain a data user's policies and practices in relation to personal data;

(b) be informed of the kind of personal data held by a data user;

(c) be informed of the main purposes for which personal data held by a data user is or is to be used. *(Amended 18 of 2012 s. 40)*

6. Principle 6—access to personal data

A data subject shall be entitled to—

(a) ascertain whether a data user holds personal data of which he is the data subject;

(b) request access to personal data—

(i) within a reasonable time;

(ii) at a fee, if any, that is not excessive;
(ii) in a reasonable manner; and

(iv) in a form that is intelligible;

(c) be given reasons if a request referred to in paragraph (b) is refused;

(d) object to a refusal referred to in paragraph (c);

(e) request the correction of personal data;

(f) be given reasons if a request referred to in paragraph (e) is refused; and

(g) object to a refusal referred to in paragraph (f).

Appendix B

Questionnaire for Employee Survey

The Privacy Commissioner for Personal Data, Hong Kong is now carrying out an inspection of the customers' personal data system of {Company Name} under section 36 of the Personal Data (Privacy) Ordinance (Ordinance). This questionnaire is a part of the inspection. It should be filled out anonymously and all information collected will only be used for integrated analysis.

This questionnaire aims to understand your awareness and attitude on the protection of customers' personal data, and the work of your employer in protecting customers' personal data. Please read the questions carefully and choose the appropriate answers. Return the questionnaire on or before _____. Thank you for your assistance.

1. Do you think that your colleagues' awareness of the protection of customers' personal data is enough?

（Scale 6 means very enough; 1 means the lowest）

Not enough	1	2	3	4	5	6	Very enough

2. Do you agree that your employer has cultivated a culture of respecting customers' personal data privacy within the governance structure of the organisation?

（Scale 6 means strongly agree; 1 means the lowest）

Not agree	1	2	3	4	5	6	Strongly agree

3. Do you think it is difficult to comply with the requirements under the Ordinance?

（Scale 1 means not difficult at all; 6 means very difficult）

Very easy	1	2	3	4	5	6	Very difficult

4. Do you consider that your employer has provided sufficient training to you on personal data privacy protection?

（Scale 6 means very sufficient; 1 means the lowest）

Not sufficient	1	2	3	4	5	6	Very sufficient

5. Do you consider that your employer has provided sufficient support to employees under Work-from-Home arrangements to ensure data security?

（Scale 6 means very enough, 1 means the lowest）

Not sufficient	1	2	3	4	5	6	Very sufficient

6. What is more important to you? completing a task as expeditiously as possible or handling personal data cautiously?

（Scale 6 means handling personal data cautiously is of extreme importance; 1 means completing a task expeditiously is of extreme importance）

Completing a task expeditiously	1	2	3	4	5	6	Handling personal data cautiously

7. Has your employer taken the following actions? If yes, please tick the appropriate box and you can choose more than one option）

- ☐ Convey to all staff of the management's support to cultivate a personal data privacy respectful culture through different channels (e.g. staff meetings or internal circulars)
- ☐ Clearly inform staff members and customers of the purposes of collecting, using and disclosing personal data and the duration of retention through the Personal Information Collection Statement and the Privacy Policy Statement
- ☐ Clearly inform staff members of the information on who to contact with questions or concerns on handling of customers' personal data
- ☐ Allocate adequate resources (including financial and manpower to implement privacy management programme
- ☐ None of the above

8. As you understand it, which of the following personal behaviours may constitute an offence under the Ordinance? (You can choose more than one option)

- ☐ Accidental erasure of a customer's account information
- ☐ Input of a customer's phone number into a personal mobile phone without authorisation for the purpose of contacting the customer during Work-from-Home arrangements
- ☐ Disclosure of a customer's name and phone number to a friend so that the friend could promote other organisation's services or products to the customer
- ☐ Disclosure of a customer's real name and the name of the customer's residential estate (without the floor or flat number) on social media platforms for doxxing purpose

9. As you understand it, doxxing acts may constitute which of the following offence(s)? (You can choose more than one option)

- ☐ Disclosing personal data obtained without consent from data users under the requirement of the Ordinance
- ☐ Criminal intimidation
- ☐ Access to computer with criminal or dishonest intent
- ☐ Contempt of court（breaching injunction order restraining doxxing）

10. To the best of your knowledge, which of the following step(s) is/are required under the Ordinance regarding security of personal data? (You can choose more than one option)

- ☐ Protection of personal data against unauthorised or accidental access, processing, erasure, loss or use
- ☐ To ensure the integrity of staff members responsible for handling personal data
- ☐ An organisation must inform the affected data subjects of any data breach incident
- ☐ To ensure an appointed data processor to comply with the data security requirements

11. How often will you change your login password for your office computer system? (You can choose more than one option)

- ☐ At least once a month
- ☐ At least once every three months
- ☐ At least once every six months
- ☐ Only when the system requests you to do so

12. Have you ever disclosed your login password to your colleague due to operational need or used your colleague's login password to perform duties? (Please choose one option)

- ☐ Yes; I did not obtain my supervisor's prior approval
- ☐ Yes; I obtained my supervisor's prior approval
- ☐ No

13. Have you ever used public computer and/ or public Wi-Fi to login to your office computer system? (Please choose one option)

- ☐ Yes
- ☐ No

14. Have you ever brought paper documents home for work? (Please choose one option)

- ☐ Yes
- ☐ No

15. Have you obtained your supervisor's approval? (Please choose one option)

- ☐ Yes
- ☐ No

16. Have you taken the following measure(s)? (You can choose more than one option)

- ☐ Redacting or removing personal data from the paper documents before leaving office
- ☐ Keeping a register of paper documents that have been taken home
- ☐ Taking extra care of the paper documents when travelling
- ☐ Locking paper documents in a secure cabinet or drawer at home to prevent unauthorised access
- ☐ None of the above

17. Will you take the following steps when you have to use portable storage device (e.g. USB flash drive, hard disk, etc.) to store customers' personal data? (You can choose more than one option)

- ☐ Obtain divisional head's prior approval
- ☐ Use approved corporate device only
- ☐ Not to save any sensitive personal data such as identity card number in the device
- ☐ Use the device in office premises only

- END -

Appendix C

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

Practical advice to organisations

4. Organisations, as data users and employers, are primarily responsible for safeguarding the security of personal data and protecting their employees' personal data privacy. The following measures should be implemented by organisations in order to give effect to the general principles for WFH arrangements.

Risk assessment

5. WFH arrangements may be unprecedented or new to many organisations. Organisations should therefore assess the risks on data security and employees' personal data privacy in order to formulate appropriate safeguards.

Policies and guidance

6. In light of the results of risk assessment, organisations should review their existing policies and practices, make necessary adjustments and provide sufficient guidance to their employees. Such policies and guidance may cover the following areas:

   (1) transfer of data and documents out of the organisations' premises and corporate networks;

   (2) remote access to the corporate networks and data;

   (3) erasure and destruction of unnecessary data and materials; and

   (4) handling of data breach incidents.

Staff training and support

7. Organisations should provide sufficient training and support to their employees for WFH arrangements to ensure data security. Training and support may cover the following areas:

   (1) data security techniques such as password management, use of encryption and secure use of Wi-Fi; and

   (2) awareness about cybersecurity threats and trends, such as phishing, malware and telephone scams.

8. Organisations should deploy designated staff to answer questions from employees and provide necessary support.

Device management

9. Organisations may provide their employees with electronic devices (such as smartphones and notebook computers) under WFH arrangements. The following steps should be taken to ensure the security of the data, including personal data, stored in the electronic devices-

(1) installing proper anti-malware software, firewalls and the latest security patches in the devices;

(2) performing regular system updates for the devices;

(3) ensuring that all work-related information in the devices are encrypted;

(4) setting up strong access controls, such as requiring the use of strong passwords (with a combination of letters, numbers, and symbols), requiring changing of passwords regularly and using multi-factor authentication; limiting the number of failed log-in attempts;

(5) preventing the transfer of data from corporate devices to personal devices;

(6) enabling remote wipe function so that information in the devices can be erased if the devices are lost; and

(7) avoid putting the names, logos and other identifiers of the organisations on the devices conspicuously to avoid unwarranted attention.

Virtual Private Network (VPN)

10. VPN is an important and popular tool for WFH arrangements because it enables employees to access corporate networks remotely and more securely via the internet. Organisations should ensure the security of VPN by, for example:

(1) using multi-factor authentication for connecting to the VPN;

(2) keeping security setting of the VPN platform up-to-date;

(3) using handshake protocol (such as Internet Protocol Security (IPSec), Secure Socket Layers (SSL), Transport Layer Security (TLS), etc.) for establishing secure communication channels between employees' devices and the corporate networks;

(4) using full-tunnel VPN where possible (using split-tunnel VPN only when necessary, such as in circumstances of insufficient bandwidth); and

(5) blocking the connection from insecure devices.

Remote access

11. In addition to using VPN, organisations should implement further security measures for remote access to their corporate networks. Practicable measures include-

    (1) implementing network segmentation to divide a network into multiple segments or subnets, thereby reducing the risk and magnitude of data breach incidents as well as enhancing the protection for critical and sensitive data;

    (2) granting assess rights to employees on a need basis, for instance, using role-based access control;

    (3) enabling account lockout function to prevent login by a user after multiple failed login attempts; and

    (4) reviewing logs of remote access to identify any suspicious activities.

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

PCPD website

Download this publication

Enquiry Hotline : **(852) 2827 2827**
Fax : **(852) 2877 7026**
Address : **Room 1303, 13/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong**
Email : **communications@pcpd.org.hk**

First published in November 2020