Inspection Report

(Published under Section 48(1) of the Personal Data (Privacy) Ordinance)

The Customers' Personal Data System of ZA Bank Limited

Report Number： R23 - 20950

Date of Issue： 9 October 2023

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

The Customers' Personal Data System of

ZA Bank Limited

Section 36 of the Personal Data (Privacy) Ordinance, Chapter 486 of the 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 the exercise of the powers conferred under section 48(1) of the Ordinance.

Ada CHUNG Lai-ling
Privacy Commissioner for Personal Data
9 October 2023

Part I – Background

1. The rapid development of fintech in the banking industry in Hong Kong in recent years has led to the provision of a one-stop financial service to customers through digital channels. Banks should ensure that the customers' personal data systems they hold are protected to meet public expectations when delivering convenient and efficient financial services.

2. Ever since the first batch of virtual banking licences were granted by the Hong Kong Monetary Authority (HKMA) in 2019, there has been eight virtual banks[1] operating in Hong Kong. Virtual banks mainly target retail customers but would also provide commercial banking services to small- and medium-sized enterprises. Unlike traditional banks, virtual banks do not have physical branches but provide digital banking services to customers through the Internet, mobile applications or other electronic channels.

3. Virtual banks are regulated by the HKMA and are subjected to the same set of regulatory requirements as traditional banks. From opening new accounts, daily operations to system maintenance, virtual banks collect, hold, process, and use vast amounts of sensitive personal data of the customers. Together with the fact that virtual banks are highly reliant on the Internet in providing their services, the security challenges faced by the virtual banks throughout the life cycle of handling of customers' personal data cannot be underestimated in light of the increasingly complex and frequent threat to cybersecurity.

4. Having considered that virtual banks handle vast amounts of sensitive personal data on a daily basis, the Privacy Commissioner for Personal Data (the Commissioner) carried out an inspection (the Inspection) of ZA Bank Limited (ZA Bank) to review its customers' personal data system, pursuant to section 36 of the Personal Data (Privacy) Ordinance, Chapter 486 of the Laws of Hong Kong (the Ordinance).

[1] Including AIRSTAR BANK LIMITED, ANT BANK (HONG KONG) LIMITED, FUSION BANK LIMITED, LIVI BANK LIMITED, MOX BANK LIMITED, PING AN ONECONNECT BANK (HONG KONG) LIMITED, WELAB BANK LIMITED and ZA BANK LIMITED.

The Business Structure of ZA Bank

5. ZA Bank, is an integrated financial brand established by ZhongAn Technologies International Group Limited in 2019. ZA Bank was granted a virtual banking licence by the HKMA in March 2019 and became the first virtual bank in Hong Kong in March 2020. The Bank holds a virtual banking licence, a licence for Type 1 regulated activity (dealing in securities) and an insurance agency licence, and must therefore comply with the relevant regulatory requirements of the HKMA, the Securities and Futures Commission and the Insurance Authority in its operation (including the handling of personal data).

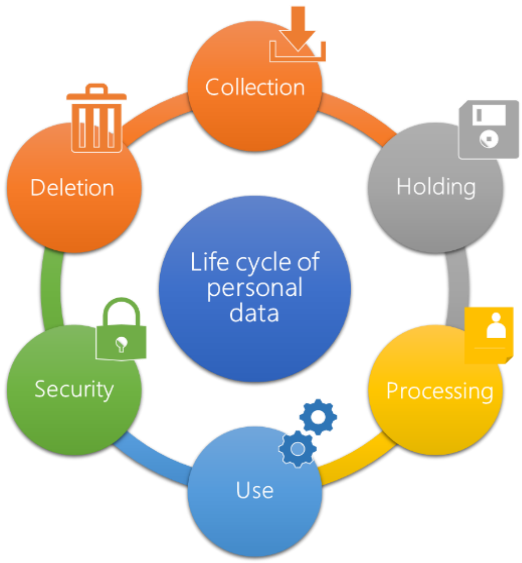
6. ZA Bank provides financial services such as savings, loans, transfers, spending, insurance, fund investments and commercial banking. As of 30 June 2023, ZA Bank had almost 700,000 retail customers with deposits and loans amounting to approximately HK$10.7 billion and HK$4.9 billion respectively[2].

7. ZA Bank had over 150 staff members at the time of the Inspection. Various departments were involved in accessing and handling customers' personal data, including (i) front-line staff, responsible for vetting and approving account opening and loans, monitoring transactions and reporting unusual transactions, delivering customer services and handling complaints; (ii) the Compliance Department, responsible for supervising the compliance of different departments in accordance with the requirements of the Ordinance and its internal policies related to the handling of customers' personal data, and for implementing the Personal Data Privacy Management Programme; (iii) the Credit Risk Management Department, responsible for assessing customers' accounts and credit data, (iv) Anti-money Laundering Department, responsible for monitoring and investigating suspicious account activities as requested by the anti-money laundering and counter-terrorist financing regulations; and (iv) the Audit Department, responsible for conducting regular internal audits to assess the personal data handling practices adopted by different departments, and provide recommendations for improvement.

[2] www1.hkexnews.hk/listedco/listconews/sehk/2023/0321/2023032100383.pdf

Scope of Inspection

8. ZA Bank, as a data user under the Ordinance, is obliged to comply with the requirements under the Ordinance, which include the six data protection principles in Schedule 1 to the Ordinance[3] with respect to the collection, holding, processing and use of customers' personal data. The Inspection focused on ZA Bank's management mechanism on handling the entire life cycle of customers' personal data from collection, holding, processing, use, security to deletion.



[3] www.pcpd.org.hk/english/data_privacy_law/6_data_protection_principles/principles.html

Part II – Methodology

9. The Inspection commenced in January 2022, but due to the COVID-19 pandemic, on-site inspections were conducted between 11 and 26 July 2022. The Commissioner dispatched an Inspection Team[4] (the Team) to inspect the customers' personal data system of ZA Bank and assess the compliance with ZA Bank's security policies and practices by its employees and service providers. Through seven rounds of written enquiries (including those following on-site inspections), the Team examined a total of 104 documents with over 2,770 pages of ZA Bank's policies, manuals, guidelines, employees' code of conduct, training materials, consultancy reports and service contracts with its service providers. In the course of the Inspection, the Team also referred to 16 documents issued by the HKMA, including its supervisory policy manual and relevant circulars on the collection, processing and protection of customers' personal data by licensed banks.

10. The Commissioner also exercised her power of entry to the premises under the Ordinance to conduct on-site inspections. In July 2022, with the consent of all parties concerned, the Team made a total of seven visits to ZA Bank's offices and data centre. The Team's on-site inspection included:

(i) Face-to-face interviews with personnel responsible for the management of ZA Bank's customers' personal data system, including eight departmental heads, 10 senior staff members and 10 front-line staff members;

(ii) Visits to nine departments of ZA Bank, and carried out videoconferencing with its call centre staff members, to examine the operation of the customers' personal data system and the relevant access control mechanisms;

(iii) Observation of ZA Bank's demonstration of the operation of its customers' personal data system, the workflow for accessing personal data from the system and the staff access control procedures for personal data; and

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

(iv) Random checks of ZA Bank's paper and computer records containing customers' personal data, including the staff activity log records in the customers' personal data system.

11. The Team also registered as a mystery retail customer through the Bank's mobile application "ZA Bank"[5] (the App), to gain a comprehensive understanding of how ZA Bank handles customer applications (see Appendix 1 for details). The Team also made enquiries to ZA Bank's front-line staff through the App.

[5] The App can be downloaded from Apple and Google's App stores. ZA Bank also provides a hyperlink for Android users to download the Android Package directly from its official website.

Part III – Key Findings

12. This report is based on the information provided by ZA Bank and the issues that came to the Team's attention during the on-site inspections. In addition to highlighting possible areas for improvement, this report points out the good practices adopted by ZA Bank in managing its customers' personal data system. The findings and recommendations in this report do not in any way affect or prejudice the Commissioner in exercising any of her powers or performing any of her functions under the Ordinance.

Areas of Good Practice

13. Following the Inspection, the Commissioner is generally satisfied with ZA Bank's practices in protecting customers' personal data and noted its good practices in the following areas:

(1) *Implementation of a Personal Data Privacy Management Programme*

14. One component of the Personal Data Privacy Management Programme (PMP) is the appointment of a Data Protection Officer and/or the establishment of a Data Protection Office to oversee whether the measures on personal data protection of an organisation comply with the Ordinance. The Commissioner is pleased to note that the Bank appointed a Head of the Compliance Department and a dedicated Data Protection Officer to continuously supervise its PMP (including all relevant procedures, trainings, monitoring or auditing, documentation, evaluation and other follow-up actions in relation to the collection, holding, processing and use of personal data). The Head of the Compliance Department and the Data Protection Officer reported directly to the ZA Bank's top management.

15. According to the data policy of ZA Bank, customers' personal data was classified as "confidential" and must be treated with caution in terms of storage, use and disposal. The Bank maintained a personal data inventory for its customers' personal data system, which included information on the types of personal data collected, retention period and procedures for

handling the data. ZA Bank would also review the personal data inventory on a regular basis to ensure that only necessary but not excessive personal data was collected, and adhered to the principle of data minimisation.

16. The Data Protection Officer of ZA Bank also prepared a privacy risk assessment questionnaire as a risk assessment tool. Before making changes to a project or launching a new project involving customers' personal data, the Operations Department was required to assess the impact of the process upon personal data privacy and to develop solutions for the various potential risks, including a data breach response plan and notification mechanism.

17. In the course of examining the documents, the Team noted that ZA Bank had established policies and guidelines[6] for various areas and would review and revise them regularly or on a needs basis. To ensure the continuous compliance of the relevant policies and guidelines with the requirements of the Ordinance, ZA Bank designated an internal audit department to conduct regular audits on various business units and provide recommendations on their handling of customers' personal data. ZA Bank had also engaged an external consultant to audit its information technology security system, and had taken remedial actions in response to the audit findings.

18. Considering the large volumes of customers' personal data and the sensitivity of these data it holds, the Commissioner is satisfied with ZA Bank's responsible handling of these data and its compliance with the requirements of the Ordinance.

(2) *Implementation of a paperless office*

19. As virtual banks provide banking services to retail customers solely through designated mobile applications, paper records of operations have been considerably reduced, which in turn lowered the risks of data breaches due to the misplacement or accidental loss of paper records.

[6] This includes data retention and deletion, personal data security, network security, patch management, account and password management, and so on.

20. The Commissioner is pleased to note that ZA Bank has generally implemented paperless operations. Except for handling data access requests from regulators, law enforcement agencies and government departments, as well as employment-related matters, most of ZA Bank's work was completed via its intranet without the need for printouts or compilation of a physical archive.

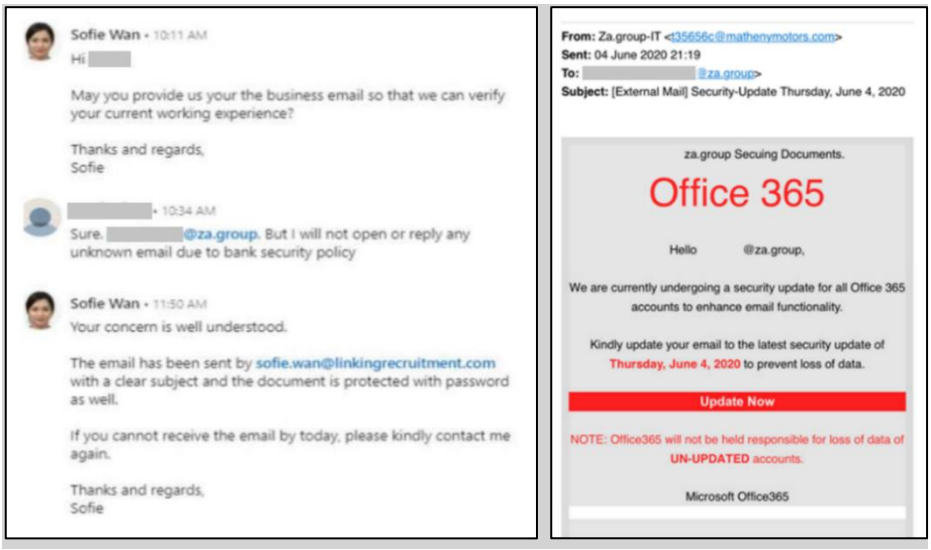
21. ZA Bank stored all paper documents relating to data access requests from regulators, law enforcement agencies and government departments in separate rooms with CCTV cameras and smart card access systems to prevent unauthorised access. ZA Bank has also placed a locked disposal bin in its office so staff members could properly dispose of documents containing personal or sensitive data.

22. In general, the Commissioner considers that ZA Bank had taken adequate security measures to protect physical documents containing customers' personal data against unauthorised or accidental access, processing, erasure, loss or use.

(3) *Prevention of the threat of phishing attacks*

23. Hackers often carry out phishing attacks on organisations that hold large volumes of personal data. These attacks may interfere with the organisations' normal operations, more seriously by hacking into administrator accounts or, in the worst case, maliciously encrypting files in their systems. Effective measures to identify phishing attacks and eliminate the risk of these attacks at an early stage are therefore required.

24. In addition to configuring its email system to prevent and filter out suspicious emails, the Commissioner notes that ZA Bank implemented a "Phishing Attack Drill Exercise" to simulate workplace cyber fraud and encourage staff members to report suspected scam emails, thus enhancing their levels of cybersecurity awareness. ZA Bank reported to the Team that since the Exercise was launched, no staff members had clicked on the hyperlinks contained in the simulated phishing emails.



Sample messages (left) and email (right) from the "*Phishing Attack Drill Exercise*"

25. The Commissioner considers that the abovementioned "Phishing Attack Drill Exercise" is effective in helping ZA Bank prevent cyberattacks.

(4) *Promoting a culture of privacy in the workplace*

26. A sound PMP relies on the efforts of all staff members in an organisation to protect personal data. The Commissioner is pleased to note that ZA Bank had put in place the following policies and measures to enhance staff awareness of personal data protection:

(i) Provided mandatory training on personal data protection to all new staff members (whether full-time or part-time) and required them to sign an acknowledgment that they had read the employee Code of Conduct and the relevant personal data protection manuals when onboarding;

(ii) Organised regular seminars or workshops to educate staff members about setting strong passwords for their accounts and to remind them on the compliance with the Ordinance, data protection principles, the offence of doxxing and the serious legal consequences of a contravention;

(iii) Implemented a clean desk policy and organised regular inspections of the workplace by the Data Protection Officer on whether documents containing customer personal data were stored securely

and whether staff members had fixed sticky notes or paper with passwords on screens or computers. Non-compliant staff members would receive a warning label as a reminder; and

(iv) Displayed posters and notices on information security, cyber fraud prevention and password management in the office areas, in order to enhance staff awareness of personal data protection.

Posters displayed in ZA Bank's office areas

Areas for Improvement

27. Notwithstanding the good practices described above, the Commissioner notes the following areas for improvement in the protection of customers' personal data by ZA Bank:

(1) *<u>Strengthening the management of data processors</u>*

28. The Commissioner notes that ZA Bank outsourced part of the works relating to the processing of customers' personal data to third-party service providers (i.e. data processors[7]) for services such as debit card

[7] A data processor is a person who processes personal data on behalf of another person and not for its own purposes. Data processors are not directly regulated by the Ordinance, but 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 the processing of the data (DPP 2(3)), and to prevent unauthorised or accidental access, processing, erasure, loss or use of the data transferred to the data processor for processing (DPP 4(2)).

embossing and outstanding payment recovery service. Nevertheless, ZA Bank assured the Team that all of its data processors had been vetted by the HKMA in advance to ensure that the practices involving the processing of customers' personal data were in compliance with the relevant regulatory requirements.

29. The Team made a written request to ZA Bank for the relevant service contracts and on-site audit reports related to credit card embossing and outstanding payment recovery service. The Team noted that the service contracts set out the handling procedures in case of data breaches, requiring the data processors to report any data breach incidents to ZA Bank as soon as possible, so the Bank could follow up on the incidents. The Commissioner is pleased to note that ZA Bank adopted contractual means to ensure that the personal data entrusted to its data processors was protected against unauthorised or accidental access, processing, erasure, loss or use.

30. However, the Commissioner is aware that ZA Bank did not conduct regular on-site audits to ensure that the data processor for the debit card embossing service acted in accordance with the provisions of the relevant service contract, which involved taking appropriate security measures and destroying ZA Bank's customers' personal data in a timely manner. In response to the concerns expressed by the Team, ZA Bank stated that it had assigned staff members to conduct an on-site audit in February 2023.

31. Although the Commissioner understands that ZA Bank was limited by the immigration controls and restrictions due to the outbreak of the COVID-19 pandemic and could not send its staff members for on-site audits of the data processor concerned as scheduled, she considers that ZA Bank could have hired independent auditors to complete the audits on its behalf in order to continuously monitor whether the data processor's handling of its customers' personal data complied with the requirements of the relevant service contract.

32. In addition, after reviewing ZA Bank's on-site audit reports concerning its service providers for the recovery of outstanding payments, the Commissioner finds that ZA Bank's staff members did not specify the

types of physical and system security measures that the service providers had taken. The report also did not specify whether the service providers deleted the expired customers' personal data in a timely manner. Although the Commissioner is satisfied that ZA Bank's staff members had verified each of the relevant areas, she recommends ZA Bank to list out all audit items and findings in its audit reports in order to further enhance the accountability and consistency of its on-site audits. Prior to the release of this report, ZA Bank stated that it had adopted the abovementioned recommendations of the Commissioner by revising the on-site audit form used by staff members so as to improve the relevant work records.

(2) *Enhancing the monitoring capabilities of the data loss prevention system*

33. During the office visits, ZA Bank demonstrated its information security protection capability to the Team, covering technical aspects such as system protection, access control and physical security. The demonstrated technical measures included, among others, its data loss prevention system and endpoint security[8].

34. The Team noted that the data loss prevention system set up by ZA Bank could detect personal data contained in outgoing emails which was applicable to all staff members (not restricted by category of staff members or privileges).

35. The Commissioner is of the view that in order to effectively prevent personal data from being abused or used for illegal purposes such as "doxxing", the conditions for triggering system alerts should be role-based. Therefore, the Commissioner recommends that ZA Bank set up rules based on staff functions and privileges, or whitelist[9] the domain names of email addresses of frequently contacted regulators and law enforcement agencies. It can then carefully distinguish the requirements of different positions in its daily operations to detect suspicious behaviour as early as possible.

[8] Details have been omitted to protect sensitive and confidential information about the security of the relevant information systems.

[9] In a whitelist approach, only inputs matching pre-defined patterns are allowed through while all others are filtered out (www.infosec.gov.hk/en/best-practices/business/securing-web-application).

(3) *Limiting the time for staff members to access customers' personal data*

36. During the demonstration, the Team found that a front-line staff member responsible for approving account opening applications had access to the details of all applications he had approved over the past two years. The personal data he could access included the applicants' names, identification documents, correspondence addresses, telephone numbers, email addresses, etc.

37. In response to the Team's verbal inquiry, the Head of the Operations Department stated that the department would randomly review the applications for new accounts every month to ensure data accuracy. However, she admitted that the front-line staff member concerned had no operational need to re-access all the application details or applicants' personal data approved after completing the account opening approval process under normal circumstances.

38. The Commissioner is of the view that ZA Bank had generally adopted the "need-to-know" [10] principle in its system administration, whereby staff members were granted the least privilege to complete their work. However, ZA Bank should limit the time for staff members to access their work history in accordance to their operational needs, with a view to reducing the risk of misuse or leakage of customers' personal data. The Commissioner is delighted to know that, in response to the concerns expressed by the Team during the on-site visit, ZA Bank reviewed the system settings with its Information Technology Department to avoid unnecessary access to customers' personal data for an excessive duration by staff members.

(4) *Centralising the management of internal policies and guidelines*

39. Effective internal communication is an important factor contributing to the success of a PMP. Organisations should take all practicable steps to

[10] Before granting any access right to individual employees, the head of the department concerned must submit an application for written approval. Access rights must also be reviewed and updated by the corresponding head of department in a timely manner when employees are transferred.

inform their staff members of their personal data policies and practical guidelines in a clear and understandable manner. They should also make the relevant information easily accessible to staff members.

40. Through ZA Bank's demonstration of its systems and the Team's interviews with the personnel managing the customers' personal data system, the Team learnt that the guidelines and manuals on the employee Code of Conduct, data classification, information security and incident reporting were compiled separately by individual departments and stored in their respective common folders. Some full-time employees in certain departments could access these guidelines and manuals via the Bank's intranet. However, the intranet page was not accessible to all departments and some employees told the Team during the interviews that they were unsure how to access the guidelines and manuals.

41. The Commissioner considers that information about ZA Bank's personal data policies and practical guidelines should be made easily accessible to all staff members and centrally managed by the Data Protection Officer at the corporate level, to ensure that the relevant guidelines and manuals can be shared with staff members immediately upon future revisions or updates. The Commissioner is pleased to learn that as of 30 September 2022, ZA Bank had taken follow-up action by opening up the relevant intranet page to all staff members, followed by an internal email notifying all staff members on the same day, in order to facilitate their understanding of and compliance with ZA Bank's personal data policies and practical guidelines.

(5) *Continuous and regular review of the personal data system*

42. The Commissioner notes that ZA Bank has a designated department to conduct internal audits on different departments regularly with the aim of identifying any deficiencies in risk management and recommending corresponding improvements.

43. Although ZA Bank did not conduct a separate audit of its personal data system before the Inspection, the Commissioner finds the following deficiencies in the processing of customers' personal data from its two

internal audit reports, which were respectively completed in December 2021 and January 2022:

(i) weak passwords being used by some administrator accounts;
(ii) Failure to delete the accounts of former employees who had access to customer credit data in a timely fashion;
(iii) Failure to inspect physical security measures in the office areas;
(iv) Failure to cover the procedures for disposing of endpoints/storage devices nor the registration/deregistration of portable devices in the policy on the management of endpoints and portable devices; and
(v) Failure to follow the procedures prescribed by internal policies before engaging third-party service providers or outsourcing services.

44. Nonetheless, the Commissioner is pleased to note that ZA Bank had implemented the recommendations for addressing the above deficiencies, as set out in the audit reports.

45. As a data user that hold a vast amount of customers' personal data, the Commissioner encourages ZA Bank to continuously and regularly review its personal data system (including all relevant policies, guidelines and procedures) to ensure compliance with the industry best practices or operational guidelines, thus mitigate risks to its systems in its daily operation.

Conclusion

46. The Inspection revealed that ZA Bank generally complies with the Data Protection Principles of Schedule 1 to the Ordinance in the handling of customers' personal data. The Commissioner is pleased to note that ZA Bank has established a PMP and appointed a dedicated Data Protection Officer to systematically and responsibly develop a system to comply with the requirements of the Ordinance and to manage customers' personal data. The Commissioner also recommends that ZA Bank strengthen the management of its data processors, enhance the monitoring capabilities of the data loss prevention system, limit the time for staff members to access customers' personal data, centrally manage its internal

policies and guidelines and continuously and regularly review its personal data system.

Part IV – Recommendations

47. Through this report, the Commissioner would like to remind the organisations which handle vast amounts of customers' personal data to strengthen their measures to safeguard data security, which include:-

(i) **Establish a 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, as well as establishing a personal data inventory. A PMP can help organisations comply with the Ordinance, handle data breaches promptly and gain trust from customers and other stakeholders.

(ii) **Appoint a Designated Officer as Data Protection Officer:** Organisations should appoint a designated officer as Data Protection Officer and clearly set out the roles and responsibilities of a Data Protection Officer, including overseeing the organisation's compliance with the Ordinance and reporting to senior management, as well as incorporating data protection issues raised by staff members and experiences and lessons learnt from data breach incidents involving customers' personal data into organisation's training materials.

(iii) **Formulate Comprehensive System Security Policies and Procedures:** In an era in which "data is an asset", enterprises and organisations must strengthen the protection of customers' personal data privacy and reduce the risks of personal data leakage or misuse. They should formulate system security policies and procedures in line with international standards, conduct regular and timely security risk assessments and review the effectiveness of their security measures continuously and regularly. They should also adopt timely improvement measures to protect customers' personal data system against threats such as cyberattacks or hacking.

(iv) **Devise a Role-based Access to Customer Data:** Organisations should adopt the "least privilege" principle to grant as few access rights as possible to complete a task and assign staff members to appropriate roles (i.e., adopt role-based access control, including restriction of the volume of data to be accessed and the duration of access). Organisations should also regularly review the access rights of their staff members (e.g., update access rights upon departure or redeployment of staff members) and remove unnecessary accounts and access rights in a timely manner, to prevent customers' personal data from being leaked, used for doxxing or other unlawful purposes.

(v) **Appoint and Manage Data Processors Prudently:** Organisations should conduct privacy impact assessments[8] before engaging data processors to handle personal data on their behalf. This can avoid introducing measures that have an adverse impact on personal data privacy. After the data processors are appointed, organisations should continue to monitor whether their handling of personal data complies with the mutually agreed standards as stipulated in the contract, and should formulate proper response plans with the data processors for any unforeseeable privacy risks that may arise.

- End -

[8] www.pcpd.org.hk/english/resources_centre/publications/files/InfoLeaflet_PIA_ENG_web.pdf

Appendix 1

Process of retail customers opening an account using the ZA Bank mobile application

1 Download ZA Bank mobile application. Select "CARD DETAILS" on the "ZA CARD" page

2 Enter mobile phone number, SMS verification code, invitation code (if any), and email address

3 Select document type, and take a photo of the document according to the instructions

4 Conduct facial recognition

5 After identity verification and facial recognition are successfully matched, edit the identification information accordingly

6 Fill in address, tax information, occupation and purpose of opening an account, and confirm the personal data provided

7 Read and agree to the Personal Information Collection Statement and the Terms and Conditions related to account opening

8 Customers can decide whether to activate the ZA CARD. The card number can be customised or randomly generated by the system

9 Set up login username and password

Upon completion of the account opening process, the system will automatically review the account opening information or forward it for manual review