

Privacy Policy Statement

1. Introduction

1.1. This Statement is adopted as the Privacy Policy Statement ("Statement") of UCO Bank Limited Hong Kong Branch (the "Bank"). The purpose of this Statement is to establish the policies and practices of the Bank's commitment to protect the privacy of personal data and to act in compliance with the provisions of the Personal Data (Privacy) Ordinance (the "Ordinance") and implementation of the guidelines thereon issued by the Hong Kong Association of Banks. The provisions of this Statement are supplement to Annexure 1 Personal Data (Privacy) Ordinance ("PDPO") Notice to General Terms and Conditions Governing Accounts and Secured Loan Facilities of the Bank.

1.2. As an overseas Branch in Hong Kong, the Bank is required to establish its own policies and practices to ensure full compliance with the applicable legal and regulatory requirements in their respective jurisdictions relating to personal data protection.

2. Kinds of Personal Data Held by The Bank

2.1. There are two broad categories of personal data held in the Bank. They are personal data related to customers and (potential) employees of the Bank.

2.2. Personal data held by the Bank regarding customers may include the following:

- a. name and address, occupation, contact details, date of birth and nationality of customers and marital status of customers and their identity card and/or passport numbers and place and date of issue thereof;
- b. current employer, nature of position and annual salary of customers;
- c. information obtained by the Bank in the ordinary course of the continuation of the business relationship (for example, when customers write cheques or deposit money or generally communicate verbally or in writing with the Bank, by means of documentation or telephone recording system, as the case may be);

2.3 Personal data relating to employment held by the Bank may include the following:

- a. name and address, contact details, date of birth and nationality of employees and potential employees and their spouses and their identity card and/or passport numbers and place and date of issue thereof;
- b. additional information compiled about potential employees to assess their suitability for a job in the course of the recruitment selection process which may include references obtained from their current or former employers or other sources;
- c. additional information compiled about employees which may include records of remuneration and benefits paid to the employees, records of job postings, transfer and training, records of medical checks, sick leave and other medical claims and performance appraisal reports of the employees;
- d. relevant personal data pertaining to former employees may be required by the Bank to fulfil its obligations to the former employees and its legal obligations under certain ordinances; and

e. information which is in the public domain, if required.

2.4 The Bank may hold other kinds of personal data which it needs in the light of experience and the specific nature of its business.

3. Purposes The Personal Data Are Held

3.1 It is necessary for customers to supply the Bank with data in connection with the opening or continuation of accounts and the establishment or continuation of banking facilities or provision of banking and other financial services.

3.2 It is also the case that data are collected from customers in the ordinary course of the continuation of the banking and other financial relationship.

3.3 The purposes for which data relating to a customer may be used are as follows:

- a. the processing of applications for, and the daily operation of the services and credit facilities provided to customers;
- b. conducting credit checks (including without limitation upon an application for consumer credit and upon periodic review of the credit) and data verification;
- c. assisting other financial institutions to conduct credit checks and collect debts;
- d. ensuring ongoing creditworthiness of customers;
- e. designing financial services and/or related products for the customers' use;
- f. marketing financial services or related products to customers;
- g. determining the amount of indebtedness owed to or by customers;
- h. creating and maintaining the Bank's credit and risk related models;
- i. collection of amounts outstanding from customers and bills providing security for customers obligations;
- j. meeting the requirements to make disclosure under the requirements of any law, rule, regulation, order, ruling, judicial interpretation or directive (whether or not having the force of law) applicable to UCO Bank Limited or (any of its branches) and its agents and affiliates;
- k. enabling an actual or proposed assignee of the Bank, or participant or sub participant of the Bank's rights in respect of the customer to evaluate the transaction intended to be the subject of the assignment, participation or sub participation;
- l. any other purposes permitted by law; and
- m. purposes relating to any of the above.

3.4 The purposes for which data relating to employees and potential employees may be used are as follows:

- a. processing employment applications;
- b. determining and reviewing salaries, bonuses and other benefits;
- c. consideration for promotion, training, secondment or transfer;
- d. consideration of eligibility for and administration of staff loans and other benefits and entitlements;
- e. providing employee references;
- f. registering employees as intermediaries or licensees with statutory authorities/institutions for purposes directly related or associated to the employment;
- g. monitoring compliance with internal rules of the Bank;
- h. meeting the requirements to make disclosure under the requirements of any law binding on the Bank or under and for the purposes of any guidelines issued by regulatory or other authorities with which the Bank are expected to comply; and
- i. purposes relating thereto.

4. Security of Personal Data

It is the policy of the Bank to ensure an appropriate level of protection for personal data in order to prevent unauthorised or accidental access, processing, erasure or other use of that data, commensurate with the sensitivity of the data and the harm that would be caused by occurrence of any of the aforesaid events. It is the practice of the Bank to achieve appropriate levels of security protection by restricting physical access to data by providing secure storage facilities, and incorporating security measures into equipment in which data is held. Measures are taken to ensure the integrity, prudence, and competence of persons having access to personal data. Data is only transmitted by secure means to prevent unauthorized or accidental access. If a data user engages a data processor (whether within or outside Hong Kong Special Administrative Region) to process personal data on 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.

5. Accuracy of Personal Data

It is the policy of the Bank to ensure accuracy of all personal data collected and processed by the Bank. Appropriate procedures are implemented to provide for all personal data to be regularly checked and updated to ensure that it is reasonably accurate having regard to the purposes for which that data is used. In so far as personal data held by the Bank consists of statements of opinion, all reasonably practicable steps are taken to ensure that any facts cited in support of such statements of opinion are correct. If a data user engages a data processor (whether within or outside Hong Kong) to process personal data on 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.

6. Collection of Personal Data

6.1 In the course of collecting personal data, the Bank will provide the individuals concerned with a Personal Data (Privacy) Ordinance Notice informing them of the purpose of collection, classes of

persons to whom the data may be transferred, their rights to access and correct the data, and other relevant information.

6.2 Prior to collect and obtain any personal data from public domain, the Bank will observe the original purposes of making the personal data available in the public domain (such as the purpose of establishing the public register in the enabling legislation) and the restrictions, if any, imposed by the original data users on further users.

6.3 In relation to the collection of personal data on-line, the following practices are adopted:

a. On-line Security

The Bank will follow strict standards of security and confidentiality to protect any information provided to the Bank online. Encryption technology is employed for sensitive data transmission on the Internet to protect individuals' privacy.

b. On-line Correction

Personal data provided to the Bank through an on-line facility, once submitted, it may not be facilitated to be deleted, corrected or updated on-line. If deletion, correction and updates are not allowed online, users should approach relevant members of the Bank.

c. On-line Retention

Personal data collected on-line will be transferred to relevant members of the Bank for processing. Personal data will be retained in the Bank's internet systems' database normally for a period of not longer than 8 years.

It has to be mentioned that no personal data (i.e. name, mobile number and personal email address) collection via on-line is shared with any third party vendor.

6.4 Use of Cookies, Tags and Web Logs etc

Cookies are small pieces of data transmitted from a web server to a web browser. Cookie data is stored on a local hard drive such that the web server can later read back the cookie data from a web browser. This is useful for allowing a website to maintain information on a particular user.

Cookies are designed to be read only by the website that provides them. Cookies cannot be used to obtain data from a user's hard drive, get a user's email address or gather a user's sensitive information.

The Bank uses cookies, tags and web tags to identify users' web browser for the following purposes:-

a. Session identifier

The Bank will not store user's sensitive information in cookies. Once a session is established, all the communications will use the cookies to identify a user.

b. Analytical Tracking

Users' visit to the Bank's websites will be recorded for analysis and information may be collected through technologies such as cookies, tags and web logs etc. The information collected is anonymous research data and no personally identifiable information is collected. The Bank mainly collects the

information to understand more about our users including user demographics, interests and usage patterns.

c. The Bank also uses Google Analytics to collect information on how visitors use our website. The cookies collect information in an anonymous form, including the number of visitors to the website, how visitors were directed to the website, and the pages they have visited.

7. Data Access Requests and Data Correction Requests

7.1 It is the policy of the Bank to comply with and process all data access and correction requests in accordance with the provisions of the Ordinance, and for all staff concerned to be familiar with the requirements for assisting individuals to make such requests.

7.2 The Bank may, subject to the Ordinance and the guidelines thereon issued by the Privacy Commissioner for Personal Data ("Privacy Commissioner"), impose a fee for complying with a data access request ("DAR"). The Bank is only allowed to charge a DAR requestor for the costs which are directly related to and necessary for complying with a DAR. If a person making a data access request requires an additional copy of the personal data that the Bank has previously supplied pursuant to an earlier data access request, the Bank may charge a fee to cover the full administrative and other costs incurred in supplying that additional copy.

7.3 Data access and correction requests to the Bank may be addressed to the Bank's Data Protection Officer ("DPO") or other person as specifically advised.

8. Retention of Personal Data

The Bank shall usually hold data relating to the customer(s) for a period of at least eight years after the business relationship is ended or such other period as prescribed by applicable laws and regulation after closure of account/termination of service.

9. Appointment of Data Protection Officer

9.1 To co-ordinate and oversee compliance with the Ordinance and the personal data protection policies of the Bank, a DPO has been appointed by the Bank.

9.2 The contact details of the DPO are as follows:

Data Protection Officer
UCO Bank, Hong Kong Branch
2/F, Astoria Building, Ashley Road,
Tsim Sha Tsui, Kowloon, Hong Kong

Telephone : (852) 2524 9240
Fax: (852) 2810 6954
Website: www.ucobankhongkong.com