

# PRIVACY POLICY STATEMENT

## Our Privacy Principles

Welab Bank Limited (the “**Bank**” or “**we**”) values your trust and we are committed to the full implementation and compliance with the six data protection principles and the requirements of the Personal Data (Privacy) Ordinance (Cap. 486, Laws of Hong Kong)(the “**Ordinance**”).

This Privacy Policy Statement is intended to assist you in understanding the Bank’s privacy policies and practices in relation to your personal data.

## Our Pledge

We pledge to safeguard your personal data by complying with the requirements of the Ordinance as well as the relevant codes of practice and guidance notes issued by the Office of the Privacy Commissioner for Personal Data. We will ensure that all our employees and third parties with permitted access to your personal data uphold these obligations.

## Kinds of Personal Data Held by the Bank

There are different kinds of personal data and sensitive personal data held by us. There are mainly two broad categories of personal data held by us, namely:

- (a) data of potential and existing customers; and
- (b) data of employees.

However, personal data may be provided by other individuals, including but not limited to agents and business partners.

The kinds of personal data held by us may include (but are not limited to) name, biometric data (such as facial image and finger vein), title, address, e-mail address, employment information, contact details, date of birth, nationality, financial information, credit information, marital status, identity card or passport numbers and other personal information in the public domain.

It is necessary for us to hold such data for various purposes including, without limitation, the opening or continuation of accounts, the establishment or continuation of banking/credit facilities, and the provision of insurance, securities, investment, and related services and products and facilities offered or to be offered by or through us.

## Collection and Use of Personal Data

We collect your personal data through fair and lawful means on a voluntary basis. The data is used by us for the purposes indicated in the respective screens of the Bank’s mobile application and/or website in which potential and existing customers are invited to provide personal data and in the Notice to Customers and Other Individuals relating to Personal Data (Privacy)

Ordinance (the "**Notice**"). We will provide the Notice on or before the collection of personal data in an appropriate format and manner. For details, please refer to the Notice, including the consequences of failure to provide such data.

The collection of your personal data are generally collected directly from you, but we may also collect your personal data from different sources from time to time, such as from your use of the Bank's mobile application or website, data generated or combined with other information, and other third party sources (for example, credit reference agencies).

### **Collection of Information Through Your Device**

When using the Bank's mobile application, the Bank will collect data about and/or stored in your device. This type of information includes:

- (a) Device and application information, such as the device name, device identification code (IMEI, ESN, MEID, and SN), hardware model, OS version, application version, software identification code, SIM card information, and device and application settings (such as region, language, time zone, and font size);
- (b) Mobile network information, such as network service provider the public land mobile network (PLMN) provider ID and Internet Protocol (IP) address;
- (c) Log information. When you use the Bank's mobile application, the Bank will automatically collect and log some information, such as the time of access, access count, IP address, and information about incidents (such as errors, crashes, restarts, and upgrades);
- (d) Location information. The Bank will collect, use, and process the approximate or precise location of your device when you access the mobile application. Location information can be obtained based on the GPS, WLAN, and service provider network ID. In the device settings menu, you can disable the location permissions to reject sharing your location information; and
- (e) Other data in your device. The Bank will also collect information stored on your device such as biometric data (if you have chosen to activate the feature that allows you to use your biometric credentials to log onto the Bank's mobile application), contact lists and other mobile applications of other banks you may have on your device.

### **Use of Cookies**

Cookies are small data files which that are automatically stored on your web browser in your computer, mobile phone or other device for accessing the Internet ("**device**") that can be retrieved by the Bank's mobile application and/or website when you visit certain parts of our website or click on our online advertisements. Cookies or similar technologies are used for the following purposes:

- (a) statistical analysis of your on-site behaviour such as number of visits to our mobile application and/or website and users' general usage patterns;

- (b) provide enhanced user experience, remember your preference and interests within our mobile application and/or website; and
- (c) promote personalised products and/or services to you and to make the Bank's mobile application or website more relevant to your interests.

The Bank will also use "strictly necessary cookies" which are required for the operation of the Bank's mobile application and/or website to:

- (a) allow its server to determine whether the cookies setting on your device have been enabled or disabled. This allows the Bank to know whether data can be collected from your device;
- (b) temporarily allow you to carry information between pages of the Bank's mobile application and/or website to avoid you having to re-enter that information; and
- (c) temporarily identify your device after you have logged in to the Bank's mobile application and/or website so that the Bank's server can maintain a dialogue with your device in order for you to carry out certain activities.

The above cookies may be placed on your device by the Bank or by third parties on the Bank's behalf (for example, advertising networks and providers of external services like web traffic analysis services). Information recorded through the use of cookies by third parties are aggregated and then shared with the Bank as anonymous aggregated research data. No personal contact information about you is collected or shared by third parties with the Bank as a result of the use of cookies.

**Most web browsers are initially set up to accept cookies. If you prefer, you can, during your visit at the Bank's mobile application and/or website, you can choose to 'not accept' cookies by changing the settings on your web browser. However, if you block all cookies, including strictly necessary cookies, you may not be able to use the Bank's mobile application and/or website properly.**

For further details of our privacy policy in relation to use of cookies on our website or mobile applications, please visit our privacy policy in relation to use of our website and our privacy policy in relation to use of our mobile application.

## **CCTV**

The Bank's premises are installed with CCTV and images of yourself may be captured, collected and stored by us when you visit the Bank's premises. Information collected is mainly used for security, management and other related purposes as stated in the Notice.

## **Disclosure of Personal Data**

We follow strict privacy procedures in regard to protection of personal data. No disclosure of your personal identifiable information to third parties is allowed unless you have already been informed or have provided the consent (where required) or the disclosure is permitted or required by any law binding on the Bank. For possible transferees (whether within or outside Hong Kong), please refer to the Notice.

## **Security Measure to Safeguard Personal Data**

We provide and maintain stringent security measures to protect the Bank's system and information and personal data (including personal data at rest and in transit) retained therein, including:

- (a) use of one-time password to authenticate users or customers;
- (b) use of firewalls and network segregation to prevent unauthorized access;
- (c) use of encryption to keep your personal data private at rest and in transit;
- (d) regular review of our information collection, use, storage and processing practices;
- (e) restriction of access of personal data to relevant employees on a "need-to-know" basis;
- (f) training to employees on the proper handling of personal data; and
- (g) personal data will be encrypted by strong data encryption algorithms using encryption keys unique to us and with proper key management.

While the internet is not an inherently secure environment for communications, we continuously review and apply industry best practices to protect and secure this channel throughout our systems.

Your personal device security and general measure in handling your own personal and transactional digital data are equally important. In most cases, an imprudent transmission and handling of sensitive data such as confidential documents, password, personal identifiers etc. would facilitate unauthorized access resulting in a data breach. Hence, we remind you to be cautious when using the Bank's mobile application and/or website and handling your own sensitive documents and data.

You should be careful in handling your account details (including your username and password) and ensure that you do not knowingly or accidentally share, provide or facilitate unauthorised use of such details. Do not share your username or password or allow access or use of your username or password by others. You should safeguard your username and password and keep them secret and confidential. We will never ask you for your password given that you should be the only person who knows it. If you think your username or password has been disclosed to another person, is lost or stolen or an unauthorised transaction has been conducted, you are responsible for informing us immediately.

## **Retention of Personal Data**

The Bank retains all records of transactions for validation and auditing purposes. Appropriate retention periods apply and we will take practicable steps to ensure that your personal data will not be kept longer than necessary for the fulfilment of the intended purpose. In the majority of cases this will be for 7 years from the end of your relationship with us.

Under applicable circumstances, you may have the right to ask us to delete your personal data or not to transfer or share your personal data.

## **Outsourcing Arrangement**

If the Bank engages outsourcing service providers or data processors (whether within or outside Hong Kong), outsourcing service providers or data processors are required to adhere to specific standards, including any standards prescribed by a privacy regulator, to prevent any loss, unauthorized access, use, modification or disclosure, either by contractual provisions or other means.

## **Direct Marketing**

The Bank intends to use your personal data in direct marketing and the Bank requires your consent (which includes an indication of no objection) for that purpose. We may use your personal data to inform you of products, services and other marketing materials which we think may be of interest to you. We or our external research agencies on our behalf may also invite you to participate in market research and surveys and other similar activities.

You may refer to the Notice for details of our use of your personal data for direct marketing purposes.

**If you do not wish the Bank to use or provide to other persons your personal data for use in direct marketing as described above, you may exercise your opt-out right by notifying our Data Protection Officer at the contact details below.**

## **Data Breach Handling**

### **Access and Correction of Personal data**

As the data subject, and subject to a reasonable prescribed fee, you have a right to access your personal data or request us to correct or update your personal data.

If you have any question about our Privacy Policy Statement, or would like to request for access to data or correction of data, or for information regarding our policies and practices and kinds of data held, please contact us at:

The Data Protection Officer

Welab Bank Limited

Unit 301-6, OfficePlus@Sheung Wan, 93-103 Wing Lok Street, Sheung Wan, Hong Kong

## **Changes to Privacy Policy Statement**

This Privacy Policy Statement is subject to review and change from time to time. Please visit the Bank's mobile application or website for the Bank's latest Privacy Policy Statement.

In case of discrepancies between the English and Chinese versions of this Privacy Policy Statement, the English version shall prevail.

January 2020