# Privacy Policy

Effective date: January 20, 2022

**Company name: MBA CONSULT PTE. LTD.**

Company number: 201615276H

Legal address: #23-01, Parkview Square, 600 North Bridge Road, 188778 Singapore

Email: singapore@mbacgroup.com

**Contacts of Data Protection Officer: Evgeniya Kaspruk**

Address: #23-01, Parkview Square, 600 North Bridge Road, 188778 Singapore

Email: evgeniya.kaspruk@mbacgroup.com

## General Provisions

This Privacy Policy governs our data processing activities in case if such activities are subject to the Regulation (EU) 2016/679 (General Data Protection Regulation).

Amendments to this Policy will be posted to this URL and will be effective when posted. If we'll make any material changes to this Policy we will notify the data subjects by means of the website notice. Any data subject can choose to discontinue using of our services if the data subject does not accept the terms of this Policy, or any modified version of this Policy.

We do not knowingly collect any personal information from children under the age of 18. Our products and services are not offered to individuals under the age of 18.

We obtain the personal data as a result of interaction of the data subjects with our products. Refusal to provide the data will result in unavailability of provision of our products and services or poor user experience.

Each data subject has the right to lodge a complaint to supervisory authority in case of personal data breach, misuse or any violation of applicable law related to personal data processing. The complaint may be submitted to a supervisory authority in the EU Member State of the data subject's habitual residence, place of work or of an alleged infringement.

## Legal Basis of Processing and Categories of Data

*Entering a contract with a customer and performance of such contract.*

In case if the customer takes steps to enter information services contract with us by sending a request on our websites we need to obtain name, contact and identification details (name, email, phone number, financial operations data) as well as the customer's device and software specifications to exercise communication necessary to enter the contract and register the customer in our database, and such details will be required further to manage the data subject's loan settlement. The nature of our services requires to identify our customers by their ID (passport) and residential address as without such information we won't be able to perform the contract with a customer. In order to perform the contract with a customer we are required to set up our products and services in a manner compatible with the customer's device specifications, mobile network and internet access settings and therefore access to such data is required.

*Consent*.

We process contact details of our customers obtained from our clients or from our website request forms based on the data subject's consent. The consent may be revoken and in such case the

data processing will be ceased in case if there is no legitimate interest or any other legitimate basis for processig exist.

*Legal obligation*.

As our products operate in different countries, we have an obligation to store and provide personal data to government bodies by an authorised request.

## Period of Storage

Any data we process is stored as long as there is an unsettled loan between the data subject and our client.

## Profiling

We maintain profiles of our customers as it’s required to provide loan settlements services. No automated decision making is conducted on the basis of profile.

## Recipients of Personal Data

We share personal information with the following recipients:

- our employees;
- hosting providers;
- technical support providers;
- partners which act as our contractors for provision of our products and services;
- data management service providers;
- government bodies.

In case if the data is provided to recipients the countries outside EU and EEA we implement standard contractual clauses or other relevant terms of the data processing agreements entered with the recipients. We transfer the data outside of EU and EEA provided that the transfer is subject to model contract clauses on international transfers of personal data. Providing information to our data processors is subject to signing a data processing agreement that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller.

## Sensitive Information

We do not process the following information in any manner: racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric and health data or data concerning a person's sex life or sexual orientation.

## Rights of the Data Subjects

Each data subject has the following rights which may be exercised by contacting us by ay available means. All the rights below have specific exceptions in certain cases. The requests will be processed within 30 days.

*Right to access* allows any data subject to request the following information from us:

- if its data is processed;

- which data is processed;

- which are the recipients or categories of recipients of personal data;

- data storage period;

- existence and nature of the rights to rectification / erasure / restriction / objection,

- existence of the right to lodge a complaint to supervisory authorities;

- sources of data;

- existence of profiling and automated decision making including their logic and consequences;

- existence of safeguards of international data transfers.

*Right to rectification* is the right to correct incorrect data and the right to complete the incomplete data.

*Right to erasure ("to be forgotten")* means that the data subject may request erasure of his or her data in the following cases:

- the data is no longer needed for the purposes of processing;

- consent for processing is withdrawn and no other grounds of processing apply where such processing is based on consent;

- data subject objects to processing;

- processing is unlawful;

- the data is related to a child and was processed in the context of offering a service directly to a child.

*Right to restriction* means that processing shall be restricted if:

- the data subject claims that the data is inaccurate, and controller needs to verify if it's really inaccurate;

- processing is unlawful but the data subject wants processing to be restricted rather than the data to be erased;

- processing is no longer required for its purposes but the data subject requires it for specific purposes;

- processing is under objection but the controller needs to verify if objection is not overridden by legitimate interest of the controller.

*Right to notification* means that the data controller shall communicate the request of the data subject in exercise of his or her rights to each recipient unless it proves that it will take disproportionate effort.

*Right to data portability* means that data subject may request the data controller to provide collected data in structured and readable form.

*Right to objection* means that the data subject based on its personal circumstances may override legitimate interests of the controller which constitute the basis for processing.

The data subject has *the right not to be subject to profiling* which significantly affects his or her interests.

## Protection of Information

We take the following measures on protection of personal data to prevent the data breaches, misuse and the violation of rights of data subjects:

- Providing this Policy for review to any person or entity which is about to process the personal data.

- Keeping our officers and contractors responsible for proper data processing conducted by such officers and contractors.

- Providing advice to any officer, data subject or partner on the subject of compliance with this Policy.

- Making sure no access to personal data is provided to unauthorized parties.

- Using only reliable and tested software for processing or personal data.

- Assuming technical and organizational risks of data processing before such processing takes place.

- Ensuring that all actions in respect of the data are exercised by protected accounts to access the data and all data storages are available only to a limited number or persons on a password basis.

- Ensuring that we are able to suspend data processing or withdraw any piece of data from processing if we believe that such processing violates applicable law.

- In case of change in any business process we will determine whether such change is data-related and check if such change falls in line with this Policy.

- Providing that each location and device where personal data is stored is a safe environment.

- Utilizing firewall to minimize the risk of unauthorized access to the hosting infrastructure.

- Where necessary using third-party vendors to perform security assessments to identify issues with its data security that could result in security vulnerabilities.

- Providing encryption of most sensitive personal data.

- Ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services.

- Providing the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.

- Processing regular testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the data processing.