PRIVACY POLICY

APPLICATION OF THIS PRIVACY POLICY

Credit Agricole Corporate and Investment Bank, DIFC Branch, a recognised company, regulated by the Dubai Financial Services Authority and having its principal place of business at Al Fattan Currency House, Tower 2, Level 21, Dubai International Financial Centre P.O. Box 506611, Dubai, United Arab Emirates ("**CACIB DIFC**", "**we**", "**us**" or "**our**") is committed to safeguarding the privacy of the personal information that we process in line with applicable data protection laws. This Privacy Policy ("**Policy**") describes how and why we collect, store and use personal information, and provides information about applicable rights in relation to the personal information we process. Please read the following information carefully to understand our views and practices regarding how we handle personal information.

For the purposes of applicable data protection law, CACIB DIFC may operate as either "data controller" or "data processor" of your personal information. The below information relates to CACIB DIFC's operations as a data controller.

CONSENT

By availing of our services, you consent to our collection, use, processing and disclosure of your personal information to the extent permitted by applicable laws and the terms of this Policy. We will also collect, use, process and disclose your personal data where we have legitimate reasons for such processing without seeking your consent. You may withdraw such consent at any time by contacting us at the information provided below. However, this will not affect the lawfulness of the processing, based on your consent, conducted prior to such withdrawal, or where we have other legitimate reasons for processing your personal data.

COLLECTION OF PERSONAL INFORMATION

We may collect and process the following personal information:

- **Information you give us:**
    - If you inquire about any of our services, then we may request and process your personal information, including:
        - **Personal Details**: full name, gender, nationality, date and place of birth, religion and other elements of civil status, and personal relationships;
        - **Identity Documents**: copy of passport and related documentation, copy of identity card, example of signature, Emirates ID;
        - **Contact Details**: work postal addresses, work and private email addresses, job title, contact telephone numbers and preferences regarding marketing communications;

- **Employment Details**: work title and information relating to your professional and (where relevant) financial status, background and education information prior or during employment;
- **Transaction Data**: data about your transactions, on-boarding and our products that you use, including account activity and product use and any details pertaining to payments to and from your accounts, including repayments of any loans or credit facilities or other products;
- **Payment Data**: this includes data collected for payment purposes, such as bank card number, payment amounts, etc.); and
- **Other Data**: data collection required by applicable regulations.

  - You may give us information about you by registering for any of our products or services, or by corresponding with us by phone, e-mail or other electronic means, or in writing, as well as other information you provide directly to us, including in conversation with our employees and staff.

- **Information we collect and process about you:**
  - With regard to our services, we may automatically collect the following information:
    - **During on-boarding and reviews**: credit scores, know your customer ("KYC") verification information, and other verification information;
    - **Technical information**: including the Internet protocol (IP) address used to connect your computer to the Internet, browser type and version, time zone setting, browser plug-in types and versions geolocation and behaviour data, and operating system to our website and mobile application;
    - **Cookies Data**: this includes data we collected by website logs, cookies or similar technologies;
    - **Account Data**: collected from your use of our services, websites, or mobile apps (such as cookies);
    - **Interaction Data**: This includes, records of phone calls between you and us and customer support requests and feedback that we receive from you either through our websites, mobile apps, and social media accounts, or any channels we use to communicate with our customers;
    - **Information about your visit**: including services you viewed or searched for on our website and mobile application, page response times, download errors, length of visits and page interaction information (such as scrolling, clicks, and mouse-overs); and/or
    - **Other Data**: this includes other data required by applicable regulations, identification data, geo-location data, behavioural data, personal relationship data, financial and commercial data, biometric data, health data and criminal convictions, proceedings or allegations data.

- **Information we receive from other sources:**
  - We may also receive information about you from other sources such as:
    - Our local authorised business partner, agents and service providers;

- Legal representatives and employees of companies with which we are in business, regulatory or a customer relationship or in the process of establishing such a relationship;
- Credit and government agencies;
- Surveys;
- Third party businesses or organisations, including existing corporate and business clients; and/or
- Public sources.

PURPOSES

We use your personal information, where permitted by applicable law, as follows:

- To perform our obligations under a contract with you:
  - creating your account;
  - providing our products or services to you;
  - providing you support services in relation to the products and services you avail of;
  - enhancing our products, services and your experience across our channels;
  - to inform you about key updates and changes to our channels including Privacy Policy and other terms and policies; and/or
  - for the purposes of identity management, and when you sign-in to your account.
- For purposes which are required by law, including:
  - As a regulated entity we are subject to a number of statutory and regulatory obligations that may require us to process your personal data, for example, KYC and anti-money laundering ("**AML**") purposes. We also need to process your personal data to comply with any obligations and requirements issued by governmental, legal and regulatory authorities within the United Arab Emirates, or any other jurisdiction where we conduct our business;
  - responding to requests by government or law enforcement authorities conducting an investigation; and/or
  - complying with any applicable law or regulation.
- Where this is necessary for purposes which are in our, or third parties, legitimate interests. These interests include:
  - to understand your needs as a customer and your eligibility for products and services and to understand how you use and interact with our products and services;
  - to respond to enquiries and communications and to record these interactions for the purpose of analysis and improvement;
  - to design, develop and test products, services and solutions for customers, which may include combining sources and types of your personal data across multiple legal entities and countries, subject to compliance with applicable laws;
  - to contact you for your opinions about our products and services, including through surveys and other market research.

- maintain the safety and security of our systems and customers, including for the purposes of detecting, investigating, mitigating or preventing risks;
- delivering and improving our products and services to our customers, or process your transactions;
- auditing usage of our products and services;
- processing and responding to inquiries, and providing our products and services;
- administering promotions and events that you take part in;
- ensure security and business continuity;
- to keep you and our staff safe;
- to detect, investigate and prevent financial crimes;
- to operate our business;
- protect our legal rights; and/or
- prevent any data leakage through our Data Leakage Prevention ("**DLP**") tools and policies.

- For the purposes of enforcing our right or initiating or defending a claim, including:
  - preparing for and managing legal proceedings, including court actions and arbitration;
  - gathering and maintaining documentation and evidence necessary for legal claims;
  - enforcing the terms of contracts with customers, employees, or third parties;
  - handling customer complaints, disputes, and grievances through judicial actions; and/or
  - evaluating claims for damages or losses to determine validity and potential compensation.

SHARING YOUR PERSONAL INFORMATION

We may also share your personal information with third parties including certain service providers we have retained in connection with our business activity, such as those listed below, or other necessary entities:

- Authorized third parties (including legal representatives, guarantors, trustees, transferees, and the clients' authorized persons);
- Third parties that can verify information (such as credit bureaus, credit reference agencies, credit protection providers, rating agencies, debt collection agencies, and fraud prevention agencies);
- Our service partners (including professional advisers, insurers, service providers, social media platform providers, and advertisers);
- Strategic referral partners (such as business alliances or charitable and non-profit organizations);
- Other financial services regulators (including without limitation, market infrastructure providers and correspondent banks);
- Any other party involved in a dispute over a transaction; and/or

- Auditors, regulators, or dispute resolution bodies for compliance with their requests.

Moreover, we may disclose your personal information to third parties:

- If we sell or buy any business or assets, in which case we may disclose your personal information to the prospective seller or buyer of such business or assets;
- If CACIB DIFC, its business, or its assets are acquired by a third party, in which case personal information held by us about our customer, employees, suppliers, or others will be one of the transferred assets;
- If we are under a duty to disclose or share your personal information in order to comply with any legal obligation, if we reasonably consider this necessary, or to protect the rights, property, or safety of CBCIA, our customer, employees, suppliers, or others; and/or
- For the purposes of crime prevention and fraud protection.

We may also disclose your personal information to law enforcement authorities or other government officials.

We may also disclose your personal information to any competent administrative or judicial authority in prevention of money laundering and terrorist financing in compliance with the applicable know your customer KYC and AML regulations, for the purposes of preventing any operation related to money laundering or terrorism financing.

USE OF AI SYSTEMS

We are committed to ensuring transparency in the processing of your personal data, particularly when using AI and automated or semi-automated systems ("**AI Systems**"). AI Systems may utilise advanced machine-based technologies, including AI and automated or semi-automated systems, to process your personal data. AI Systems are designed to operate autonomously or semi-autonomously, capable of processing data for human-defined purposes or purposes that the system itself defines, or both. The technology includes, but is not limited to, machine learning algorithms, natural language processing, and predictive analytics.

The personal data processed by AI Systems is used for specified, explicit, and legitimate purposes, including but not limited to:

- enhancing customer service and support;
- personalising and improving our products and services;
- conducting risk assessments and fraud detection;
- complying with regulatory and legal obligations; and
- conducting market research and analysis.

The output generated by AI Systems, which may include insights, predictions, and recommendations, is used to:

- improve decision-making processes;
- provide tailored services and products to our customers;
- enhance operational efficiency and effectiveness; and
- ensure compliance with legal and regulatory requirements.

We have implemented comprehensive safeguards to ensure that the processing of personal data by AI Systems we use complies with applicable data protection laws and regulations. These safeguards include:

- conducting regular risk and impact assessments to evaluate potential risks associated with data processing;
- implementing technical and organizational measures to protect personal data against unauthorized or unlawful processing and accidental loss, destruction, or damage;
- ensuring transparency by providing clear and explicit notice to users about the use of AI Systems;
- relying on a lawful basis for processing personal data; and
- appointing an Autonomous Systems Officer (ASO) for high-risk processing activities to oversee compliance and governance.

SECURITY

We use up to date information storage and security systems to hold your personal information securely in electronic and physical form, and to protect your personal information from unauthorised access, improper use or disclosure, unauthorised modification or unlawful destruction or accidental loss. Whilst we have put in place physical, electronic and managerial procedures to secure and safeguard your personal information, we will not be held responsible for any unauthorised access by third parties. We cannot guarantee that the personal information provided by you, or that is transmitted by you through our platforms, is totally secure and safe. You provide this information at your own risk.

CROSS-BORDER TRANSFERS

Your personal information may be transferred to and stored in servers and facilities located in your region or in another country. Some of these countries do not provide the same level of data protection as the country in which you reside and may not be recognised by the relevant authorities in your jurisdiction as providing an adequate level of protection. We only transfer personal information to these jurisdictions, with your consent or when it is necessary for the products or services we provide you, or otherwise subject to appropriate safeguards that assure the protection of your personal information, such as standard contractual clauses.

MARKETING COMMUNICATIONS

We, or trusted third parties on our behalf, may contact you by email, telephone, or post with information about our products or services or promotions that might be of interest to you. Where necessary, at the time that you provide your personal information to us, you will be given the opportunity to indicate whether you are happy for us to use your personal information in order to tell you about such products, services and promotions.

Withdrawal of consent to receive marketing communications will not affect the processing of personal information for the provision of our products and services. You may, at any time, withdraw your consent to receive commercial marketing communications by clicking on the link provided in the relevant email, or by emailing us on dpo-difc@ca-cib.com.

YOUR RIGHTS

You have the right to ask us to provide a copy of the personal information we hold about you, and to have personal information removed or any inaccurate personal information about you corrected.

You may have the right under applicable data protection laws to:

- obtain details relating to the personal information we hold and process about you (including information regarding how your information may be shared);
- obtain a copy of your personal information;
- request that we correct your personal information where it is inaccurate and/or that we complete your information where it is incomplete;
- limit or restrict the processing of your personal information in certain cases;
- request that we delete your personal information in certain cases;
- receive your personal information in a structured, commonly used and machine-readable format, and for CACIB DIFC to transmit that data to another controller (data portability) in certain cases;
- object and opt out of important decisions which were based solely on automated decision-making; and
- file a complaint with your local data protection controlling authority.

You can also limit or withdraw any consent you give to us at any time and may have the right under applicable law to object to us using your personal information for our legitimate purposes. You may ask us for further information regarding withdrawal or refusal of consent and the consequences of such refusal. If you do withdraw your consent, this will not affect the lawfulness of any processing based upon such consent, conducted prior to such withdrawal.

If you would like to exercise any of these rights in relation to the personal information we hold about you or wish to change your preferences at any time, please contact us at dpo-difc@ca-cib.com.

Please note that we may require your personal information to verify your identity in order to process a request made to exercise your rights in relation to your personal information. If we are unable to match this information, we may ask you to provide additional identifying information, such as a copy of your passport or drivers' license. You may designate a third party to act on your behalf, provided they have appropriate written authority to do so.

If you make a request to delete your personal information, note that we may not delete all of your information. We may still process your personal information if it is necessary to do so and subject to applicable law.

If you remain unhappy with a response you receive from us, you can refer the matter to your local data protection controlling authority, which for the DIFC is the Commissioner of Data Protection at commissioner@dp.difc.ae.

HOW LONG WE KEEP YOUR PERSONAL INFORMATION

We will retain your personal information for the length of time needed to fulfil the purposes outlined in this Policy, unless a longer retention period is required and permitted by law, including to respond to any queries or complaints, to protect our interests, or to comply with applicable laws and regulations.

Your personal information that is processed for marketing purposes will be stored until you exercise the right to withdraw consent. Once such right is exercised, your personal information will be kept only during the applicable statute of limitations period for any disputes or liabilities that may arise as a consequence of the processing of that information. Once potential actions are time barred we will proceed to delete the personal data. In any other circumstances, we will retain your personal information for a shorter or longer period as required by any applicable law.

LINKS TO THIRD PARTY SITES

Our website or mobile application may link to other, unaffiliated third-party websites. Please note that CACIB DIFC is not affiliated with, nor can it control or be responsible for the content or privacy and confidentiality practices of any third-party websites. You must always carefully review the privacy and confidentiality policy of any third-party website that you may visit in order to understand how the operators of that website may collect, store and use your personal information.

CHANGES TO THIS PRIVACY POLICY

We may from time to time make changes to this Policy. Please check back regularly to keep informed of updates to this Policy. These changes are effective immediately, upon being posted on this page.

CONTACT DETAILS

If you have any questions about this Policy, or our processing of your personal data, please contact us at dpo-difc@ca-cib.com or +971 04 376 1100.