Data Protection Information Notice

Table of Contents

1. Who are we?

We are **China Construction Bank (Europe) S.A.**, a public limited liability company (*société anonyme*) organised and established under the laws of the Grand Duchy of Luxembourg with registered office at 1, Boulevard Royal, L-2449 Luxembourg and registered with the Trade and Companies Register (RCS) under number B 176131 ("**CCBEU**").

China Construction Bank (Europe) S.A. operates in Luxembourg and have **branches in other European Union countries** in view to deliver the best service to our clients. The branches' offices are located in Paris, Barcelona, Amsterdam, Milan, Warsaw and Budapest.

In case one of the branch carries out different activities than described in the present notice and/or needs to provide you with additional or divergent local information, you will find it under the **Schedule** dedicated to such branch. The branch Schedules are part of, and must be read together with the present notice.

We also are **China Construction Bank Corporation, Luxembourg Branch**, a Luxembourg public limited liability company (*Société Anonyme*) having its registered office at 1 Boulevard Royal, L-2449 Luxembourg, Grand-Duchy of Luxembourg and registered under the law of Luxembourg with R.C.S. number B 179518. China Construction Bank Corporation, Luxembourg Branch, is a branch of China Construction Bank Corporation, a joint stock limited company, incorporated and existing under the laws of the People's Republic of China, registered with the Beijing Administration for Industry and Commerce under number 911100001000044477 ("**CCBLU**").

China Construction Bank (Europe) S.A. and China Construction Bank Corporation, Luxembourg Branch are established at the same address, carry out the same business, and share together the same premises, IT systems and infrastructure, and human resources.

The entity with which you enter into a relationship:

- China Construction Bank (Europe) S.A. or one of its branches; or
- China Construction Bank Corporation, Luxembourg Branch,

is the **controller** of the processing of the individuals' personal data processed in accordance with this notice (the "**Bank**", "**we**", "**us**", "**our**").

2. Why do we make this notice?

We provide you with this Data Protection Information Notice to inform you about:

We are required to provide you with all those information according to Article 13 and Article 14 of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data (the "**GDPR"**).

The GDPR became applicable on 25 May 2018 and significantly enhanced the protection and rights of individuals as to the processing of their personal data. It applies to companies in the European Economic Area ("**EEA"**) as well as to companies outside of the EEA when they offer goods and services to individuals in the EEA or when they monitor their behaviour.

The GDPR aims at ensuring **fair, transparent and lawful processing** (e.g. the collection, use, rectification, storage, erasure) of personal data by both the public and private sectors. As a Luxembourg bank with branches in the European Union, we are also subject to many legal and regulatory obligations and supervised by the Luxembourg banking and financial regulatory authority: the "*Commission de Surveillance du Secteur Financier" or* "CSSF"). In particular, we are bound by the **banking secrecy rules** under the Luxembourg law of 5 April 1993 on the financial sector, as amended, the Luxembourg Criminal Code, and any similar local law to which our branches are subject.

We take the security and protection of personal data seriously and responsibly and care about the related rights of every individuals. Therefore, we have implemented **internal policies and procedures** together with other necessary technical and organisational measures to ensure the proper handling of personal data through its entire lifecycle.

3. Who is concerned by this notice?

As we normally do not enter into business relationships with natural persons, the present notice (the "**Data Protection Information Notice"**) is addressed to the individuals (i.e. natural persons) connected to the legal persons listed below and whose personal data is processed by us:

- clients and prospects;
- beneficiaries of payment instruments;
- financial security providers;
- business partners and other counterparties;
- agents and other intermediaries;
- other service providers and vendors, auditors, consultants and lawyers;
- governmental, public, judicial and regulatory authorities;
- any third party contact person of our Bank.

Where the parties above are legal persons, we refer to them as the "**Related Entities**".

Depending on the circumstances, the **individuals connected** to our Related Entities may be their employees, trainees, consultants, managers, directors, officers, agents, shareholders, beneficial owners, and other staff or representatives or other connected persons (e.g. their own Related Entities). If one of the persons listed in this paragraph is also a legal person (e.g. a shareholder), this Data Protection Information Notice applies as well to the individuals connected to such legal person ("**you**", "**your**").

We may also process the personal data of the **family members and/or close associates** of the individuals listed above to the extent required by laws and regulations to which we are subject (see **Section 5B.**).

When you provide us with personal data of others (e.g. your directors, employees, representatives, beneficial owners, shareholders and their family members), you must first inform them and make sure that you can provide us with such personal data in accordance with the legal obligations to which your Related Entity is subject, including its own GDPR obligations. In particular, **you must provide or make available** the present **Data Protection Information Notice** to those persons to inform them about our processing of their personal data.

4. Contact for data protection matters

We have appointed a person to monitor that our Bank complies with the GDPR and more specifically respect the rights of the individuals concerned: our internal **Data Protection Officer** or "**DPO"**, who is notified to the Luxembourg Data Protection Supervisory Authority (i.e. the "*Commission Nationale pour la Protection des Données*"

or the "**CNPD**") and to the other data protection supervisory authorities located in the countries where our branches are established (see **Appendix I**).

The DPO is an **independent role** and is not a representative of our Bank. In case you have any question or request regarding our processing of your personal data, you can contact this person by:

- e-mail to dpo@eu.ccb.com;
- letter to the attention of the DPO at 1, Boulevard Royal, L-2449 Luxembourg;
- phone call to +352 28 66 88 00 and ask to speak to the Data Protection Officer.

To ensure an efficient communication between you and us, we also made available specific forms to be filled in by you depending on the matter, such as for reporting a data breach or sending us a request to exercise your rights. You can find those forms in the dedicated personal data protection section of our website at eu.ccb.com.

5. Why do we process personal data?

To perform our core banking activities, we need to process personal data, in particular to enter into and maintain business relationships with our Related Entities (as defined under **Section 3.**) and to comply with the laws and regulations to which we are subject.

In case we cannot obtain the personal data we need or that we are legally required to collect (e.g. during the on-boarding or ongoing due diligence), we may not be able to enter into or maintain our business relationship.

We will inform you if your refusal to provide certain personal data or your exercise of your data protection rights (see Section 11.) would result in the impossibility to enter into or in the termination of a business relationship with us.

The processing of personal data is permitted only if it relies on a specific legal basis as listed in the GDPR where it is necessary for:

A. *the performance of a contract;*
B. *compliance with a legal obligation;*
C. *our (or a third party's) legitimate interest;*
D. *the public interest; or*
E. *with your consent.*

We collect, record, use, organise, share, transmit, disclose, store, delete and otherwise process personal data for different **purposes**, each of them relying on a different **legal basis** under the GDPR as detailed below:

A. the performance of a contract

When we entered into a contract or take steps prior to entering into a contract with a Related Entities to which you are connected (see **Section 3.**), we process your personal data for concluding and performing such contract. As we deal with legal persons, it means that we process your personal data essentially for verifying that you are a person authorised by our Related Entities, for executing orders and addressing requests, and for communicating with you.

In particular, if you are an individual connected to our **clients**, we may process your personal data to perform our services as detailed in our *Standard Terms of Business* or any other agreement entered into with the Related Entities. Depending on our entity with which you enter into a relationship, our services include: the opening of accounts, execution of orders, term deposits, loans, payment services, payment transactions, M&A advisory services, and other banking, financial and investments services.

B. compliance with legal obligations

We are required to process personal data to comply with various laws and regulations to which we are subject, including:

Banking and financial law	We set up security, management and controls measures to prevent any fraud or wrongdoing in general, to identify investors profile and inform them, to conduct audits, and to otherwise protect our clients' and the public interests to the extent required by laws and regulations to which we are subject.
AML	We make on-boarding and on-going due diligence to identify our (potential) clients/counterparties, detect complex or unusually large transactions or which deviate from normal patterns and record, and assess and address risk to prevent money-laundering and financing of terrorism. We are required to disclose such information to competent regulatory and administrative authorities (see **Section 8B.**)
Anti-bribery and corruption	We control and document any monetary or non-monetary benefits received, offered, promised, or solicited by/to us or third parties in order to identify and prevent any potential bribery or corruption and ensure a fair market competition.
Conflict of interest	We take control measures to identify, prevent, manage, mitigate and disclose potential conflicts of interest we may have when third parties offer inducements to our staff.

Whistleblowing	We provide communication channels and have procedures for reporting to us any wrongdoing by members of our Bank. If you use our dedicated whistleblowing tool, our service provider processes your personal data on our behalf and makes it anonymous. We process ourselves your personal data if you contact our staff by traditional means (e.g. telephone, email, face-to-face, letter).
Voice recording (MIFID II)	We make recording of telephone conversations to keep track of all communications in relation with financial transactions with our clients and when dealing on own account.
Data breach	We take measures to prevent, detect, mitigate and notify any personal data breach to you and/or the relevant data protection supervisory authorities in accordance with the GDPR.
Data subject requests	We address requests of individuals asking us to exercise their personal data protection rights under the GDPR.
Reporting	We report to regulatory authorities, including tax authorities for FATCA and CRS purposes and related automatic exchange of information.
Authorities requests	We occasionally address requests from official public, governmental, police, judicial, supervisory or regulatory authorities, which involve disclosure of your personal data.
Complaints handling	In case you file a complaint with us or provide us not satisfying feedback on our products, services, employees, activities or relationships, we record and analyse your complaint to address it and make our own opinion on it according to our information and records in relation with the matter. We will also use your contact details to communicate with you on the handling of your complaint and its resolution.

C. our legitimate interests

When we process personal data based on our (or a third party's) legitimate interest, the GDPR requires that we make a balancing test considering your interests and fundamental rights and freedoms. We will only process your personal data to the extent your interests and fundamental rights or freedoms do not override our (or the third party's) legitimate interests, including:

Relationships management	The relationships we have together evolves. We get to know you better and learn more about your experience, position, functions, interests and preferences in our services and activities. As we care about maintaining and improving our relationships with you and deliver the best possible products and services, such information on you help us to address your requests and expectations more efficiently.
Coordination with our branches	We are established in Luxembourg with branches in Paris, Barcelona, Amsterdam, Milan, Warsaw and Budapest using the same centralised IT tools and core banking system. Therefore, we share, on a need to know basis, information concerning you between our Luxembourg entities and the branches where they are involved in business relationships with our Related Entities. Sharing such tools and system allow us to coordinate our workflow, procedures and controls, improve efficiency, and avoid discrepancies in the provision of our products and services.
Maintenance of our IT systems	We access your personal data stored in our IT systems whenever we do the maintenance and when detecting and repairing any defects or failures or when securing communication channels. When we occasionally update our systems or migrate data, we can handle your personal data to the extent required to maintain, improve or change our systems.
CCB Match + matchmaking platform	If you register to our group CCB Match + platform (https://match.ccb.com), we will collect corporate documentation and (identification) information from you only to decide whether to accept your registration or not. As the platform is operated by our parent company, China Construction Bank Corporation, we also share your personal data with them (processing your data on our behalf) to the extent necessary for providing you with effective client support services and to adequately address your claims and requests in relation with the CCB Match + platform. For more details on our personal data transfers, see **Section 9.**
Use of processors	We process personal data of persons connected to our (potential) service providers as part of the due diligence we perform on processors (i.e. processing personal data on our behalf and upon our instructions) to ensure that such processors

	implement sufficient measures to comply with the GDPR and protect the rights of the individuals concerned.
Personal data transfers	As our parent company, China Construction Bank Corporation, located in China, provides us with centralised corporate tools, including our core banking system, the personal data that is recorded in those tools are transferred to and hosted in secured servers in China (see **Section 9.**).
Dispute and litigation management	We will process your personal data in the event of a dispute or litigation we have together to the extent that we need to use documents and/or information containing your personal data to establish, exercise or defend our rights and interests.
M&A	In case we intend to merge with a third party, we will transfer documents and information, including your personal data, to such third party who will carry out a due diligence to assess risk and decide whether to conclude the deal or not.
Video-surveillance	We operate security cameras in our offices for the safety of our employees and visitors, to secure our assets, and to prevent, detect, and investigate any incident, theft, robbery, or unauthorised access to our premises. Each camera is marked with a sign describing essential information on the recording. You may obtain our **Data Protection Information Notice on Video-surveillance** containing more information by asking the local reception desk or by contacting our DPO (see **Section 4.**).

D. the public interest

We process your personal data **based on legal requirements** imposed by the banking and financial laws and regulations to which we are subject where such processing is part of a task that is carried out in the public interest and the legal requirement is proportionate to the legitimate objective pursued. The public interest includes in particular the prevention, detection and disclosure to the competent authorities of financial frauds and crimes in general, including money laundering, financing of terrorism, corruption, bribery, and market abuse.

E. with your consent

Without prejudice to our legal obligations resulting from the banking secrecy, we do not normally process your personal data on the basis of your consent, but we rely on

other legal basis (see **Section 5.**). In the event we intent to do so, we will provide you separately and in due time with all the appropriate documents and information that you will need to grant a valid consent.

When you **consent** to the processing of your personal data, it is only for one or more specific purposes that we clearly identify and for which you are informed. We only rely on **freely given** consent meaning that you have a real choice in granting your consent or not. We make sure that your possibility to refuse consent will not cause you too much detriment (e.g. in terms of services provided). When we ask your consent, we ensure to provide you with **sufficient information** for you to make a choice knowingly.

In case you give us your consent, you may **withdraw such consent** at any time. Such withdrawal will only take effect for the future and does not apply to the processing carried out prior thereto. To withdraw any consent, please use the means we provided you with when we asked for your consent or contact our DPO (see **Section 4.**).

6. What personal data do we process?

A. General information

Personal data means any information relating to an identified or identifiable natural person (i.e. you), either directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, online identifier, or other factors specific to you as a natural person.

The type and scope of personal data that we process depends on the nature of our relationships with you and the Related Entities (see **Section 3.**). In particular, it depends on the products and services provided to/by us and on our legal requirements to process specific personal data concerning you. You can contact our DPO (see **Section 4.**) or exercise your right of access (see **Section 11.**) to obtain a confirmation whether we process your personal data and, as the case may be, the list of your personal data that we have.

B. List of personal data

The personal data that we process include in particular:

Identification	names and surnames, gender, date and place of birth, ID cards or passport ID number, nationality, postal and email addresses, telephone and fax numbers, signature, tax code.
Professional	job position and history, experience, postal and email addresses, telephone and fax numbers, employer, legal capacity, power of

	representation, VAT number, registration number, association membership.
Digital	logs in our IT systems or tools, IP address.
Banking and financial	bank account number, transaction orders, compensation.
Relationships management	feedback and complaints, gifts, charity, entertainment, other monetary or non-monetary benefits or inducements causing potential bribery, corruption, or conflicts of interest, their total value and business purpose.
KYC (Know Your Customer)	sources and destination of funds and wealth, investments, financial instruments and pledge ownership, financial sanctions, politically exposed person (PEP), family and relationships, and other data needed to fight money laundering, terrorism financing, financial crime and tax fraud.
Video and voice	voice recording in relation with transactions; video recording by our security cameras in our offices.

Special categories of data: we do not request or intentionally process any special personal data, such as racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, biometrics, or sexual life. In case we incidentally access such data because you or the Related Entities provided it to us, we will not further process it and will act appropriately to protect your rights.

7. Where do we obtain your personal data?

We obtain your personal data **directly from you**, from the Related Entities to which you are connected e.g. during on-boarding process and on-going relationships (see **Section 3.**), from other credit and financial institutions, or from our service providers acting on our behalf e.g. if you use our whistleblowing tool. In some cases, you are priory informed that we record it (e.g. telephone recording or video-surveillance).

We collect personal data from **public sources**, such as national trade and company registers, registers of beneficial owners, company public reports containing data on their shareholders, directors and management.

We also collect personal data from professional and reliable **data providers** and aggregators such as *Dow Jones*, *Thomson Reuters* and *Bloomberg* to the extent required by laws and regulations to which we are subject, in particular on the fight

against money laundering and terrorist financing.

We do not source our personal data from social networks, press or any unreliable sources.

8. Do we share your data with others?

A. General information

We are required to disclose and transmit your personal data to the competent authorities or agencies in accordance with the obligations imposed by laws and regulations to which we are subject (see **Section 5B.**).

We also need to disclose your personal data to agents, business partners, other counterparties and service providers to the extent necessary to provide our services and perform our contractual obligations with the Related Entities (see **Section 5A.**) or for our legitimate interests as described above (see **Section 5C.**).

The GDPR allows us to disclose your personal data to selected recipients provided that we comply with all the GDPR related requirements and principles, including carrying out a fair, transparent and lawful processing, and minimizing the personal data to the strict necessary to achieve the purposes for which it is shared or disclosed.

As a credit institution, we (including our branches) are also subject to the **banking secrecy** obligation under the law of 5 April 1993 on the financial sector, as amended, the Luxembourg Criminal Code, and any similar local law to which our branches are subject. In this context, we are only allowed to disclose your personal data in accordance with the specific exceptions under such laws or with your consent.

B. List of recipients

Considering the above, and depending on the relationships we have together or with the Related Entities to which you are connected, we share, disclose, communicate and transmit your personal data the recipients listed below:

Public, administrative, judicial, or regulatory authorities	For our reporting and other legal or regulatory obligations, we disclose your personal data to competent authorities, including tax authorities, banking and financial regulators, financial intelligence units, ultimate beneficial owner registers, credit registers, police, public prosecutors, courts, and central banks, in Luxembourg or in the European Union. Our *Standard Terms of Business* (or any other agreement we entered into with the Related Entities) provide details on disclosure of information

	concerning our clients. Your personal data can then be transferred by those entities to other competent authorities outside of the European Union based on international agreements with third countries (e.g. by tax authorities for FATCA and CRS purposes).
Agents, market participants, business partners and other counterparties	Credit and financial institutions, other persons whom we enter into any participation or transaction in relation to any credit facilities, stock exchanges, central depositories, trade repositories, (sub-) custodians, brokers, issuers, clearing agencies, and securities commissions, as described in more details for our clients in our *Standard Terms of Business* (or any other agreement we entered into with the Related Entities).
Professionals of the financial sector (PFS) and other service providers	Auditors, consultants, lawyers, other legal or financial advisors, document and data destruction services, providers of IT services including hosting, infrastructure, application, platforms, data rooms, whistleblowing, telephone recording and other tools. They occasionally have access to or host your personal data when performing their tasks. All of them are subject to professional secrecy obligations and/or binding confidentiality or non-disclosure agreements or process your personal data as our processors (i.e. on our behalf and upon our instructions) subject to a binding data processing agreement.
Our parent company, our branches and our group entities	- **Our European branches** (see **Section 1.**) - **China Construction Bank Corporation**, located in China, which provides us with centralised corporate tools, including our core banking system and to which we make reporting; and - **China Construction Bank Corporation Luxembourg Branch**, which is established at and share the same address and premises with us, IT systems and tools, and human resources.
M&A candidates	any third party involved in a project to merge with us or to acquire our Bank. We (may potentially) assign or transfer all or any of our rights and obligations, including your personal data to such parties, including to their auditors, lawyers or other legal or financial advisors.

9. Do we transfer your personal data outside of the EU?

As we generally make business with legal entities located in the European Union, and not with natural persons, we process a limited amount of personal data and normally do not transfer them outside of the European Union. However, there are some exceptions where we transfer personal data outside of the European Union with appropriate safeguards or as otherwise required by international agreements with third countries and permitted by the GDPR and laws and regulations applicable to us, as described below**.**

According to **Points A. to F.** below, such personal data transfers may take place to jurisdictions not having a similar level of protection of personal data as within the European Union (e.g. in terms of legislation, data protection supervisory authority, exercise of individuals' rights). Such jurisdictions may also not be covered by an adequacy decision under which the European Commission decided that personal data protection is in essence equivalent to that guaranteed in the European Union.

A. Disclosure to market participants

In case a Related Entity places an order with us to transfer, store or process funds or financial instruments (including when we receive funds in a client's account), we may have to disclose identification data concerning its representatives / beneficiaries / holders of financial instruments (including any information regarding the economic reason for a transaction or the holding of the financial instruments) to third parties involved in such transfer, storage or processing, such as:

- credit and financial institutions;
- international payment systems;
- stock exchanges;
- central depositories, trade repositories, (sub-) custodians;
- brokers, issuers, clearing agencies, securities commissions; and
- other market participants

Non-compliance with such disclosure request by the above listed recipients may lead to the blocking of the financial instruments (in the sense that voting rights may not be exercised, dividends or other rights may not be received, and the financial instruments cannot be sold or disposed of in any other manner).

By accepting our *Standard Terms of Business*, the Related Entity instructs us to make such disclosure under the conditions described therein.

Such disclosure is made to the extent necessary for the conclusion or the performance of the contract concluded between us and the Related Entity, in the interest of the representatives / beneficiaries / holders of financial instruments (e.g. execution of the

orders / instructions we receive from the Related Entity), or for the implementation of pre-contractual measures taken at the Related Entity's request.

B. Centralised corporate tools

As we are part of a large international banking group, our parent company, China Construction Bank Corporation, located in China, provides us with centralised corporate tools, including our core banking system. The (limited amount of) personal data that we record in such tools are transferred to, and securely hosted in, China. When processing your personal data, our parent company acts as our processor i.e. acting only on our behalf and upon our instructions.

The personal data transferred through our corporate tools include identification data such as names, surnames, professional emails and phone numbers of the contact persons connected with the Related Entities whom we entered into business with.

C. Expert reports

Where requested by our parent company, we transfer to them legal opinions, annual reports, valuation reports on real estate assets, and other documentation, which include personal data of employees or representatives of our (or our Related Entities') consultants, including lawyers, auditors and other legal or financial experts.

D. CCB Match +

If you subscribe to our group CCB Match + smart matchmaking platform (https://match.ccb.com), we will share your personal data with our parent company China Construction Bank Corporation, who is operating the platform, to the extent necessary for providing you with effective support services and to adequately address your claims and requests. The personal data that we transfer are limited to your identification data and contact details such as your name, surname, professional e-mail and postal address, professional telephone number.

E. Payment transactions

In rare occasion, we also transfer banking details (IBAN) and information on transactions (purpose and amount) to payment service providers or systems (SWIFT or CIPS) in case of payment to our Related Entities' employees or representatives (e.g. costs reimbursement). Such occasional data transfers are covered under Article 49.1 (b) or (c) of the GDPR as necessary for making the payment to the employees or representatives concerned.

F. Appropriate safeguards for data transfers

For personal data transfers covered under Points B. to D. above, please note that the People's Republic of China does not offer a similar level of protection of personal data as within the European Union (e.g. in terms of legislation, data protection supervisory authority, exercise of individuals' rights). China is also not covered by an adequacy decision under which the European Commission decided that personal data protection is in essence equivalent to that guaranteed in the European Union.

To maintain the protection of your personal data that we transfer in China, we implemented appropriate safeguards in accordance with Article 46.2 of the GDPR. We entered into standard data protection clauses with our parent company (as adopted by the European Commission) under which we impose specific contractual obligations to it in relation to their processing of your personal data.

You can access to the standard data protection clauses adopted by the European Commission at: https://commission.europa.eu/publications/standard-contractual-clauses-international-transfers_en or by contacting our DPO (see **Section 4.**)

10. Do we use any automated decision making?

We do not use any automated decision making process producing legal effect or otherwise significantly affecting you. Any decision in relation to you are made by a human being. If ever we intend to start a process involving automated decision making, we will ask for your consent for this purpose or enter into a relevant contract with you.

11. What rights do you have?

You have rights under the GDPR in relation with the processing of your personal data, and we would like to help you understand them better:

1) **Right to be informed**: You can obtain from us confirmation as to whether or not we process your personal data. If yes, you can obtain from us all relevant information on the processing of your personal data by contacting our DPO (see **Section 4.**);

2) **Right of access**: You can request us to provide you with an overview of our processing and a copy of your personal data, including the purposes of such processing, the data processed and their sources, the recipients of your data, the retention period, and the appropriate safeguards for transferring your personal data outside of the EU;

3) **Right of rectification**: If you discover that your personal data is not correct, incomplete or not up-to-date, you can ask us to rectify and/or complete it;

4) **Right to erasure (right to be forgotten)**: You can request us to erase your personal data and we have the obligation to accept such request if:

   - they are no longer necessary in relation to the purposes for which we collected and processed it;
   - you withdraw your consent;
   - you object to the processing (see Point 6) below) and we have no overriding legitimate ground to continue the processing;
   - we processed your data unlawfully; or
   - the laws and regulations to which we are subject require us to erase it.

   We are not required to erase your personal data if we still need them to comply with laws and regulations to which we are subject, or to perform a task in the public interest, or for the establishment, exercise or defence of legal claims.

5) **Right to restriction of processing**: You can ask us to restrict the processing of your personal data of your data in case:

   - you contest the accuracy your personal data and want to restrict our processing during the verification;
   - the processing is unlawful, but you oppose to the erasure and request instead the restriction of its use;
   - we do not need anymore your personal data, but you require them for the establishment, exercise or defence of a legal claim;
   - you objected to the processing (see Point 6) below) pending the verification whether our legitimate grounds to process the personal data override yours.

   When the processing is restricted, we can only continue to process your personal data with your consent, for storage, for the protection of third parties rights, or for reason of important public interest.

6) **Right to object**: You can object at any time to the processing of your personal data based on your particular situation in case we process such data for our legitimate interests (see **Section 5C.**) or for performing a task in the public interest.

   Once you objected, we shall no longer process your personal data unless we have compelling legitimate grounds to do so, which override your interests, rights and freedoms. However, even if you object, we can still process your personal data for the establishment, exercise or defence of legal claims.

7) **Right to data portability**: When you ask to receive from us your personal data that we collected from you, we are required to provide them to you in a structured and standard format (machine-readable) to the extent that the processing is made by automated means, and:

   - personal data was necessary for performing a contract; or
   - you granted your consent to the processing.

   Where technically feasible, you also have the right to have your personal data directly transmitted by us to a third party.

   You cannot pretend to your right to data portability regarding the personal data processing that we carry out for performing a task in the public interest.

8) **Right to withdraw your consent**: If you granted us your consent for processing your personal data for a specific purpose, you have the right to withdraw it at any time without prejudice to processing carried out before your withdrawal (see **Section 5E.**)

12. How long do we keep your data?

A. General information

The Bank does not keep personal data longer than needed for satisfying the purposes for which they were collected and processed (see **Section 5.**) or longer than required or allowed by European or national laws or regulations to which we are subject. However, we can be required by any order form public, administrative, judicial or regulatory authorities to keep your personal data for a longer period of time in case of investigation or litigation.

We do not keep any personal data after the legal limitation period, which is for commercial matters in principle, **10 years** starting from the end of the business relationship we have together, subject to any suspension or interruption of that period. We keep your personal data during this period to anticipate any potential litigation and establish, exercise or defend our rights and interests.

We are also required to keep your personal data for a specific period after the termination of the contractual and commercial relationships we have together. This includes the legal obligation to keep accounting and tax supporting documents or the legal obligation to keep our KYC (Know Your Customer) files for a minimum period imposed by the laws and regulations to which we are subject.

B. Specific retention periods

Depending on the purposes of the processing and the type of personal data, we apply specific retention periods, without prejudice to the general periods mentioned under point A. above, for example:

AML and KYC	5 years from the date of the termination of the business relationship as required by AML laws and regulations to which we are subject. A further period of maximum 5 years if required by the authorities or if necessary to implement internal measures for the prevention or detection of money laundering or terrorist financing.
Commercial / contractual / accounting / tax supporting documentation	Minimum 10 years from the closing of the relevant accounting year as required by commercial and accounting laws and regulations to which we are subject. Maximum 10 years from the end of the business relationship to establish, exercise or defend our rights and interests.
Business contact relationships	Maximum 3 years from the end of the business relationship with clients and counterparties.
Conflict of interests / anti-bribery and corruption	Minimum 5 years from the closing of the investigation (or 7 years if required by the authorities). Maximum 10 years from the closing of the investigation to establish, exercise or defend our rights and interests.
Whistleblowing	Minimum 5 years from the closing of the investigation. Maximum of the legal limitation period where legal proceedings or disciplinary measures are initiated, starting from the conclusion of such proceedings or measures.

Complaints	Maximum 10 years from the end of the business relationship to establish, exercise or defend our rights and interests.
Data breach and data subject request	Maximum 10 years from the date of the notification of the data breach or from the closing of the data subject's request to establish, exercise or defend our rights and interests.
CCB Match + profile	Maximum 10 years from the date of termination of the contract to establish, exercise or defend our rights and interests, or the maximum of the legal limitation period in accordance with the governing laws of the CCB Match + User Agreement, whichever is longer.
Video recording	Maximum 8 days from the recording. More in case of an incident to the extent necessary to investigate and establish, exercise or defend our rights and interests.
Telephone conversations recording	Minimum 5 years from the recording or 7 years if requested by authorities, as required by the laws and regulations to which we are subject (MIFID II). Maximum 10 years from the end of the business relationship to establish, exercise or defend our rights and interests.

13. How to complain?

In case of any question or you are not satisfied with how we process your personal data you can immediately contact our **Data Protection Officer** (see **Section 4.)**. We will do our best to address the matter in a fair and transparent manner.

In case you cannot obtain a satisfactory answer from us regarding your case or you wish to complain directly to the competent authority, you can always contact the data protection supervisory authority in the member state of your habitual residence, place of work, or of the alleged infringement of the GDPR.

As we are a Luxembourg Bank with branches located in Paris, Barcelona, Amsterdam, Milan, Warsaw and Budapest, our lead data protection supervisory authority is the Luxembourg CNPD (i.e. the *Commission Nationale pour la Protection des Données*).

You will find under **Appendix I** a list of the other data protection supervisory authorities located in the countries where we are established.

14. Update of this notice

In case we change our manner of processing your personal data or we engage into new processing activities, we are required to update this Data Protection Information Notice and inform you accordingly. We will bring this to your attention by any appropriate means such as email, letter, hyperlink to our website or otherwise.

The latest version of the present notice is always available at:
http://eu.ccb.com/europe/en/tszl/685454.html

Schedule for Amsterdam branch

The Bank's Amsterdam branch carries out different personal data processing activities than described in the Data Protection Information Notice and/or needs to provide you with additional or divergent localised information, you will find this information under the present **Schedule**.

Contact details:
Address：Claude Debussylaan 32,
1082MD Amsterdam, the Netherlands
Telephone：0031-0-205047899
Fax：0031-0-205047898
Email: info.nl@eu.ccb.com

Section 12. How long do we keep your data?

B. Specific retention periods

Video recording	Maximum 7 months from the recording. More in case of an incident to the extent necessary to investigate and establish, exercise or defend our rights and interests.

Schedule for branch in Spain

The Bank's branch in Spain carries out different personal data processing activities than described in the Data Protection Information Notice and/or needs to provide you with additional or divergent localised information, you will find this information under the present **Schedule**.

Contact details:
Address: Avenida Diagonal, 640 5a planta D,
08017, Barcelona, Spain
Telephone: 0034-935225000
Fax: 0034-935225078
Email: gdpr.es@eu.ccb.com

Section 6. What personal data do we process?

B. List of personal data

KYC	The branch in Spain does not provide investment services. Therefore, it does not process personal data relating to the provision of investment services.

Section 12. How long do we keep your data?

A. General information

In Spain, the legal limitation period is in principle 5 years for commercial matters starting from the end of the business relationship we have together, subject to any suspension or interruption of that period.

B. Specific retention periods

AML and KYC	10 years from the date of the termination of the business relationship as required by AML laws and regulations to which we are subject.
Commercial / contractual / accounting / tax supporting documentation	Minimum 6 years from the closing of the relevant accounting year as required by commercial and accounting laws and regulations to which we are subject. Maximum 5 years from the end of the business relationship to establish, exercise or defend our rights and interests.

Conflict of interests / anti-bribery and corruption	Maximum 5 years from the closing of the investigation (or 7 years if required by the authorities) to establish, exercise or defend our rights and interests.
Whistleblowing	Minimum 5 years from the closing of the investigation. Maximum of the legal limitation period where legal proceedings or disciplinary measures are initiated, starting from the conclusion of such proceedings or measures.
Complaints	Maximum 5 years from the end of the business relationship to establish, exercise or defend our rights and interests.
Data breach and data subject request	Maximum 5 years from the date of the notification of the data breach or from the closing of the data subject's request to establish, exercise or defend our rights and interests.
CCB Match + profile	Maximum 5 years from the date of termination of the contract to establish, exercise or defend our rights and interests, or for the maximum of the legal limitation period in accordance with the governing laws of the CCB Match + User Agreement, whichever is longer
Video recording	Minimum 15 days from the recording. Maximum 30 days from the recording. More in case of an incident to the extent necessary to investigate and establish, exercise or defend our rights and interests.
Telephone recording	Maximum 5 years from the end of the business relationship to establish, exercise or defend our rights and interests.

Schedule for Milan branch

The Bank's Milan branch carries out different personal data processing activities than described in the Data Protection Information Notice and/or needs to provide you with additional or divergent localised information, you will find this information under the present **Schedule**.

Contact details:
Address：Via Mike Bongiorno 13,
20124 Milan, Italy
Telephone：0039-02-32163000
Fax：0039-02-32163092
Email: marketing.it@eu.ccb.com

Sections 5. - 8. References to the *Standard Terms of Business*

Depending on the services provided by the Bank's Milan branch to the Related Entity to which you are connected, all references in the Data Protection Information Notice to the *Standard Terms of Business* must be read as a reference to:

1. The *Corporate "Multicurrency" Current Account Agreement*; and/or
2. The *Corporate Time Deposit Account Agreement*.

Section 6. *What personal data do we process?*

B. List of personal data

KYC	The Milan branch does not provide investment services. Therefore, it does not process personal data relating to the provision of investment services.

Section 9. Do we transfer your personal data outside of the EU?

B. Centralised corporate tools

In addition to the personal data listed in the Data Protection Information Notice under **Section 9B.**, the Bank's Milan branch also transfers the personal data listed below:

- place and date of birth;
- ID and tax number;

- passport;
- residence and domicile;
- job position; and
- signature.

Section 12. How long do we keep your data?

B. Specific retention periods

AML and KYC	10 years from the date of the termination of the business relationship as required by AML laws and regulations to which we are subject (or more if required by the authorities).
Commercial / contractual / accounting / tax supporting documentation	10 years from the date of the termination of the business relationship as required by laws and regulations to which we are subject and to establish, exercise or defend our rights and interests
Video recording	Maximum 72 hours from the recording. More in case of an incident to the extent necessary to investigate and establish, exercise or defend our rights and interests.

Schedule for Paris branch

The Bank's Paris branch carries out different personal data processing activities than described in the Data Protection Information Notice and/or needs to provide you with additional or divergent localised information, you will find this information under the present **Schedule**.

Contact details:
Address：86-88 bd Haussmann
75008 Paris, France
Telephone：0033-155309999
Fax：0033-155309998
Email: marketing.fr@eu.ccb.com

Section 12. How long do we keep your data?

B. Specific retention periods

Video recording	Maximum 1 month from the recording. More in case of an incident to the extent necessary to investigate and establish, exercise or defend our rights and interests.

Schedule for Hungary branch

The Bank's Hungary branch carries out different personal data processing activities than described in the Data Protection Information Notice and/or needs to provide you with additional or divergent localised information, you will find this information under the present **Schedule**.

Contact details:
Address: Szabadság tér 7.
1054 Budapest, Hungary
Tel: +36 1 336 68 88
Fax +36 1 336 68 88
E-Mail: complaint.hu@eu.ccb.com

Section 5. Why do we process personal data?

B. compliance with legal obligations

Telephone recording	We make recording of telephone conversations when accepting client complaints via telephone as required by laws and regulations to which we are subject.

Section 6. *What personal data do we process?*

C. List of personal data

Identification	Additional personal data: clients / counterparties representatives' mother names, address card number.
KYC	The Hungary branch does not provide investment services. Therefore, it does not process personal data relating to the provision of investment services.

Section 12. *How long do we keep your data?*

A. General information

In Hungary, the legal limitation period is in principle 5 years for commercial matters starting from the end of the business relationship we have together, subject to any suspension or interruption of that period.

B. Specific retention periods

AML and KYC	Minimum 8 years and maximum 10 years from the date of the termination of the business relationship as required by AML laws and regulations to which we are subject (or more if required by the authorities).
Commercial / contractual / accounting / tax supporting documentation	Minimum 6 years from the closing of the relevant accounting year as required by commercial and accounting laws and regulations to which we are subject. Maximum 5 years from the end of the business relationship to establish, exercise or defend our rights and interests.
Complaints	Where a complaint is made by telephone, the conversation is stored for minimum 5 years from the date of the recording. Maximum 5 years from the end of the business relationship to establish, exercise or defend our rights and interests.
Data breach /data subject request	Maximum 5 years from the date of the notification of the data breach or from the closing of the data subject's request to establish, exercise or defend our rights and interests.
CCB Match + profile	Maximum 5 years from the date of termination of the contract to establish, exercise or defend our rights and interests, or for the maximum of the legal limitation period under with the governing laws of the CCB Match + User Agreement, whichever is longer
Video recording	Maximum 30 days from the recording. More in case of an incident to the extent necessary to investigate and establish, exercise or defend our rights and interests.
Telephone recording	Where a complaint is made by telephone, the conversation is stored for minimum 5 years from the date of the recording. Maximum 5 years from the end of the business relationship to establish, exercise or defend our rights and interests.

Schedule for branch in Poland

The Bank's branch in Poland carries out different personal data processing activities than described in the Data Protection Information Notice and/or needs to provide you with additional or divergent localised information, you will find this information under the present **Schedule**.

Contact details:
Address：Warsaw Financial Center, ul. Emilii Plater 53,
00-113 Warsaw, Poland
Telephone：0048-22-1666666
Fax：0048-22-1666600
Email: administration.pl@eu.ccb.com

Section 12. How long do we keep your data?

B. Specific retention periods

Commercial / contractual / accounting / tax supporting documentation	Minimum 5 years from the closing of the relevant accounting year as required by commercial and accounting laws and regulations to which we are subject (or more if required by the authorities). Maximum 10 years from the end of the business relationship to establish, exercise or defend our rights and interests.
Video recording	Maximum 30 days from the recording. More in case of an incident to the extent necessary to investigate and establish, exercise or defend our rights and interests.

Annex I: List of Data Protection Authorities

Luxembourg
Commission nationale pour la protection des données - CNPD
15, Boulevard du Jazz
L-4370 Belvaux
Tél. : (+352) 26 10 60 -1
e-mail : communication@cnpd.lu
Website : https://cnpd.public.lu
Contact form : https://cnpd.public.lu/fr/support/contact/contact-prive.html

Netherlands
Autoriteit Persoonsgegevens - AP
Hoge Nieuwstraat 8, Den Haag
P.O. Box 93374
2509 AJ Den Haag/The Hague
Tel. (+31) 70 888 8500
Fax (+31) 70 888 8501
e-mail: info@autoriteitpersoonsgegevens.nl
Website: https://autoriteitpersoonsgegevens.nl/nl

France
Commission Nationale de l'Informatique et des Libertés - CNIL
8 rue Vivienne, CS 30223
F-75002 Paris, Cedex 02
Tel. (+33) 1 53 73 22 22
Fax (+33) 1 53 73 22 00
Website: http://www.cnil.fr

Italy
Garante per la protezione dei dati personali - GPDP
Piazza Venezia 11
00187 Roma
Tel. (+39) 06 69677 1
e-mail: protocollo@gpdp.it
PEC: protocollo@pec.gpdp.it
Website: http://www.garanteprivacy.it

Spain
Agencia de Protección de Datos - AEPD
C/Jorge Juan, 6
28001 Madrid
Tel. (+34) 900 293 13

Website: https://www.aepd.es

Poland
Personal Data Protection Office - UODO
ul. Stawki 2
00-193 Warszawa
Tel. (+48) 22 53 10 300
Infoline (in Polish): 606-950-000
e-mail: kancelaria@uodo.gov.pl
Website: https://uodo.gov.pl

Hungary
Hungarian National Authority for Data Protection and Freedom of Information / Nemzeti Adatvédelmi és Információszabadság Hatóság - NAIH
Falk Miksa utca 9-11
H-1055 Budapest
Tel. (+36) 1 3911 400
e-mail: ugyfelszolgalat@naih.hu
Website: http://www.naih.hu