CUSTOMER PRIVACY NOTICE

BrokerCreditService (Cyprus) Limited ("**BCS**", "**we**", "**us**" or "**our**" in this privacy notice) respects your privacy and is committed to protecting your personal data. This privacy notice will inform you as to how we look after your personal data and tell you about your privacy rights and how the law protects you.

This privacy notice applies to our customers (whether prospective, current or former) who are individuals. Aside from customers, this privacy notice also applies (as the context may require) to any other individual who is not our customer but whose data is required to be collected by us by reason of, or incidental to, the provision of any services/products by us to our customers, whether the customer concerned is another individual(s) or is a company, business entity or organisation.

It is important that you read this privacy notice together with any other privacy notice or fair processing notice we may provide on specific occasions when we are collecting or processing personal data about you so that you are fully aware of how and why we are using your data. This privacy notice supplements the other notices and is not intended to override them.

1. IMPORTANT INFORMATION AND WHO WE ARE

We are a "**data controller**". This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this privacy notice.

Data Protection Officer

We have appointed a data protection officer ("**DPO**") who is responsible for overseeing questions in relation to this privacy notice. If you have any questions about this privacy notice, including any requests to exercise your legal rights, please contact the DPO using the details set out below.

Contact details

Full name of legal entity: BrokerCreditService (Cyprus) Limited
Name of DPO: Mr Alexis Zambas
E-mail address: dpo@bcscyprus.com
Postal address: Spyrou Kyprianou &1 Oktovriou, 1, VASHIOTIS KALANDE OFFICES, 2nd floor, Mesa Geitonia, 4004, Limassol, Cyprus
Telephone number: +357 25 822734
Website: www.bcscyprus.com

You have the right to make a complaint at any time to the Information Commissioner, the Cyprus supervisory authority for data protection issues (www.dataprotection.gov.cy). We would, however, appreciate the chance to deal with your concerns before you approach the Information Commissioner so please contact us in the first instance.

2. DATA PROTECTION PRINCIPLES

We comply with the requirements of the European General Data Protection Regulation ("**GDPR**") and any

associated legal documents. According to the GDPR, the principles relating to processing of personal data should be followed.

In light of this, the personal data received from you and held with us must be:

- Used lawfully, fairly and in a transparent way.
- Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
- Relevant to the purposes we have told you about and limited only to those purposes.
- Accurate and kept up to date.
- Kept only as long as necessary for the purposes we have told you about.
- Kept securely.

3. THE DATA WE COLLECT ABOUT YOU

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data). There are "**special categories**" of more sensitive personal data, which require a higher level of protection.

We may collect, use, store and transfer different kinds of personal data about you, which we have grouped together as follows:

Where you are a customer:

Identity Data: first name, maiden name, last name, username or similar identifier, title, date of birth, place of birth, nationality, passport or ID details, driving licence details, national insurance number, medical insurance number, gender, account number, photograph, video images and static pictures such as printed screen shots.

Family Data: marital status, number of dependents, personal relations with politically exposed persons and/or with individuals or entities against which the US, EU, UN, and/or UK have enacted economic sanctions;

Contact Data: residence address, mailing address, email address, telephone numbers, fax number.

Education Data: level of education, major strands, degrees, diplomas, professional qualifications, trainings, workshops and seminars.

Occupation Data: self-employed, unemployed, rentier, pensioner, employed, position held, responsibilities, employer's details, expected retirement date, appointment, election or other engagement details, disqualifications, details of any license, authorisation, registration, notification, membership or other permission granted or revoked by any governmental or statutory authority or any other regulatory or self-regulatory body, any censure, discipline, suspension, fines or investigation by any regulatory or self-regulatory body.

Financial Data: bank account and securities account details, tax residency, tax identification number, business relations with individuals or entities against which the US, EU, UN, and/or UK have enacted economic sanctions, source of funds and source of wealth, annual salary, other earned income, total annual income, cash deposits and investment portfolio details, securities and shareholdings, information about movable and immovable property, loans and other financing liabilities, bankruptcy records.

Transaction Data: trading history, details about payments and transfers, payables and receivables, cash and securities balances, records of instructions and transactions.

Technical Data: internet protocol (IP) address, login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform and other technology on the devices used to access products or services.

Profile Data: username and password, trading strategy, information about selected products and services, investment objectives, investment horizon, risk appetite, product testing scores.
Marketing and Communications Data: preferences in receiving marketing material and communication preferences.
Criminal Convictions: details of criminal convictions and offences of fraud, theft, false accounting, serious tax offences (including without limitation tax evasion or the facilitation of tax evasion offences), market manipulations or insider dealing.
Special categories of personal data: personal data related to the physical or mental health, specimen signature.

Where you are an underlying client or principal of any of our customers:
Identity Data: first name, maiden name, last name, username or similar identifier, title, date of birth, place of birth, nationality, passport or ID details, driving licence details, national insurance number, photograph, gender, account number.
Family Data: personal relations with politically exposed persons and/or with individuals or entities against which the US, EU, UN, and/or UK have enacted economic sanctions.
Contact Data: residence address, mailing address, email address, telephone numbers, fax number.
Occupation Data: self-employed, unemployed, rentier, pensioner, employed, position held, responsibilities, employer's details, expected retirement date, appointment, election or other engagement details, disqualifications, details of any license, authorisation, registration, notification, membership or other permission granted or revoked by any governmental or statutory authority or any other regulatory or self-regulatory body, any censure, discipline, suspension, fines or investigation by any regulatory or self-regulatory body.
Financial Data: bank account and securities account details, tax residency, tax identification number, business relations with individuals or entities against which the US, EU, UN, and/or UK have enacted economic sanctions, source of funds and source of wealth, annual salary, other earned income, total annual income, cash deposits and investment portfolio details, securities and shareholdings, information about movable and immovable property, loans and other financing liabilities, bankruptcy records.
Transaction Data: trading history, details about payments and transfers, payables and receivables, cash and securities balances, records of transactions.
Technical Data: internet protocol (IP) address, login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform and other technology on the devices used to access products or services.
Profile Data: username and password, information about selected products and services.
Criminal Convictions: details of criminal convictions and offences of fraud, theft, false accounting, serious tax offences (including without limitation tax evasion or the facilitation of tax evasion offences), market manipulations or insider dealing.

Where you are an individual representative of any of our customers:
Identity Data: first name, maiden name, last name, username or similar identifier, title, date of birth, place of birth, nationality, passport or ID details, gender, driving licence details, national insurance number, medical insurance number, photograph, video images and static pictures such as printed screen shots.
Family Data: personal relations with politically exposed persons and/or with individuals or entities against which the US, EU, UN, and/or UK have enacted economic sanctions.
Contact Data: residence address, mailing address, email address, telephone numbers, fax number.
Education Data: level of education, major strands, degrees and diplomas, professional qualifications.

Occupation Data: position held, responsibilities, powers and limitations, employer's or principal's details, expected retirement date, appointment, election or other engagement details, disqualifications, details of any license, authorisation, registration, notification, membership or other permission granted or revoked by any governmental or statutory authority or any other regulatory or self-regulatory body, any censure, discipline, suspension, fines or investigation by any regulatory or self-regulatory body.
Financial Data: business relations with individuals or entities against which the US, EU, UN, and/or UK have enacted economic sanctions, bankruptcy records.
Transaction Data: trading history, details about payments and transfers, records of instructions and transactions, statements of cash and securities balances.
Technical Data: internet protocol (IP) address, login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform and other technology on the devices used to access products or services.
Profile Data: username and password, trading strategy, information about selected products and services, product testing scores.
Marketing and Communications Data: preferences in receiving marketing material and communication preferences.
Criminal Convictions: details of criminal convictions and offences of fraud, theft, false accounting, serious tax offences (including without limitation tax evasion or the facilitation of tax evasion offences), market manipulations or insider dealing.
Special categories of personal data: personal data related to the physical or mental health, specimen signature.

Where you act as a representative of a customer's underlying client or principal:
Identity Data: first name, maiden name, last name, username or similar identifier, title, date of birth, place of birth, nationality, passport or ID details, gender, driving licence details, national insurance number, photographs.
Family Data: personal relations with politically exposed persons and/or with individuals or entities against which the US, EU, UN, and/or UK have enacted economic sanctions.
Contact Data: residence address, mailing address, email address, telephone numbers, fax number.
Occupation Data: position held, responsibilities, powers and limitations, employer's or principal's details, expected retirement date, appointment, election or other engagement details, disqualifications, details of any license, authorisation, registration, notification, membership or other permission granted or revoked by any governmental or statutory authority or any other regulatory or self-regulatory body, any censure, discipline, suspension, fines or investigation by any regulatory or self-regulatory body.
Financial Data: business relations with individuals or entities against which the US, EU, UN, and/or UK have enacted economic sanctions, bankruptcy records.
Transaction Data: trading history, details about payments and transfers, records of instructions and transactions, statements of cash and securities balances.
Technical Data: internet protocol (IP) address, login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform and other technology on the devices used to access products or services.
Profile Data: username and password, information about selected products and services.
Criminal Convictions: details of criminal convictions and offences of fraud, theft, false accounting, serious tax offences (including without limitation tax evasion or the facilitation of tax evasion offences), market manipulations or insider dealing.

Where you are a politically exposed person with whom a customer, its underlying client, principal, or any representative of a customer, its underlying client or principal may have relations:

Identity Data: first name, maiden name, last name, title, date of birth, place of birth, nationality, passport or ID details, gender.

Family Data: personal relations with clients or client representatives.

Occupation Data: public function and period during which the function was or has been held.

Where you are a shareholder or beneficial owner of any customer or its underlying client or principal:

Identity Data: first name, maiden name, last name, username or similar identifier, title, date of birth, place of birth, nationality, passport or ID details, gender.

Family Data: personal relations with politically exposed persons and/or with individuals or entities against which the US, EU, UN, and/or UK have enacted economic sanctions.

Contact Data: residence address, mailing address, email address, telephone numbers, fax number.

Occupation Data: self-employed, unemployed, rentier, pensioner, employed, position held, responsibilities, employer's details.

Financial Data: tax residency, tax identification number, business relations with individuals or entities against which the US, EU, UN, and/or UK have enacted economic sanctions, source of wealth, securities and shareholdings.

Where you are a guarantor, collateral or security provider:

Identity Data: first name, maiden name, last name, username or similar identifier, title, date of birth, place of birth, nationality, passport or ID details, gender, photograph, video images and static pictures such as printed screen shots.

Family Data: marital status, personal relations with politically exposed persons and/or with individuals or entities against which the US, EU, UN, and/or UK have enacted economic sanctions.

Contact Data: residence address, mailing address, email address, telephone numbers, fax number.

Financial Data: bank account and securities account details, tax residency, tax identification number, business relations with individuals or entities against which the US, EU, UN, and/or UK have enacted economic sanctions, source of wealth, total annual income, cash deposits and investment portfolio details, securities and shareholdings, information about movable and immovable property, loans and other financing liabilities.

Transaction Data: details about payables and receivables, cash and securities balances.

Criminal Convictions: details of criminal convictions and offences of fraud, theft, false accounting, serious tax offences (including without limitation tax evasion or the facilitation of tax evasion offences), market manipulations or insider dealing.

Special categories of personal data: personal data related to the physical or mental health, specimen signature.

Where you act as a representative of any guarantor, collateral or security provider:

Identity Data: first name, maiden name, last name, username or similar identifier, title, date of birth, place of birth, nationality, passport or ID details, gender, photograph, video images and static pictures such as printed screen shots.

Contact Data: mailing address, email address, telephone numbers, fax number.

Occupation Data: position held, powers and limitations, employer's or principal's details.

Criminal Convictions: details of criminal convictions and offences of fraud, theft, false accounting, serious tax offences (including without limitation tax evasion or the facilitation of tax evasion offences), market manipulations or insider dealing.
Special categories of personal data: personal data related to the physical or mental health, specimen signature.

Where you act as a representative of a market counterparty:
Identity Data: first name, maiden name, last name, username or similar identifier, title, gender, photograph, video images and static pictures such as printed screen shots;
Contact Data: mailing address, email address, telephone numbers, fax number;
Occupation Data: position held, powers and limitations, employer's or principal's details.

Where you are an heir, successor or assignee of any customer, guarantor, collateral or security provider or market counterparty:
Identity Data: first name, maiden name, last name, username or similar identifier, title, date of birth, place of birth, nationality, passport or ID details, gender.
Family Data: personal relations with a client, counterparty, vendor, supplier, guarantor, collateral or security provider.
Contact Data: residence address, mailing address, email address, telephone numbers, fax number.
Financial Data: bank account and securities account details, tax residency, tax identification number, business relations with a client, counterparty, vendor, supplier, guarantor, collateral or security provider, information about movable and immovable property.

Where you act as a representative of a successor or assignee of any customer, guarantor, collateral or security provider or market counterparty:
Identity Data: first name, maiden name, last name, username or similar identifier, title, gender.
Contact Data: mailing address, email address, telephone numbers, fax number.
Occupation Data: position held, powers and limitations, employer's or principal's details.

We also collect, use and share aggregated data such as statistical data for any purpose. Aggregated data may be derived from your personal data but is not considered personal data in law as this data does **not** directly or indirectly reveal your identity. For example, we may aggregate your Technical Data to calculate the percentage of users accessing a specific website feature. However, if we combine or connect aggregated data with your personal data so that it can directly or indirectly identify you, we treat the combined data as personal data, which will be used in accordance with this privacy notice.

If you fail to provide personal data
Where we need to collect personal data by law, or under the terms of a contract we have with you (or where applicable, your employer or principal) and you fail to provide that data when requested, we may not be able to perform the contract we have or are trying to enter into with you or where applicable, your employer or principal (for example, to provide you or where applicable, your employer or principal with our products or services). In this case, we may have to cancel a product or service you (or where applicable, your employer or principal) have with us but we will notify you if this is the case at the time.

4. HOW IS YOUR PERSONAL DATA COLLECTED?

We use different methods to collect data from and about you including through:

Direct interactions. You may give us your personal data by filling in forms or by corresponding with us by post, phone, e-mail or otherwise. This includes personal data you provide when you:

- Apply for our products or services, give us instructions, request marketing to be sent to you or provide us some feedback.
- Offer us to guarantee obligations or to provide security or collateral.
- Offer us your or your company's products or services or respond to our service or product requests.
- Offer or agree to execute contracts with us.

Third parties or publicly available sources. We may receive personal data about you from our outsourcers and various third parties as well as public sources as set out below:

- Personal data about customers, their underlying clients or principals, guarantors, collateral or security providers, shareholders or beneficial owners from their or clients' representatives.
- Personal data about representatives of a person from other representatives of the same person.
- Personal data about heirs, successors or permitted assignees and where applicable, their individual representatives from certifying officers, notary public, administrators, trustees or other executors of the estate of a deceased individual client, liquidators, conservators, custodians, trustees or a temporary administrators, external administrators, receivers or similar or analogous officers or bodies appointed in any bankruptcy, prevention measures, insolvency, bankruptcy, dissolution, liquidation or winding-up (or any analogous or similar proceedings).
- Criminal and employment records from the media and the criminal, bankruptcy and disqualification records bureau or agencies.
- Personal transactions records from investment firms and other financial intermediaries.
- Financial and transaction data from banking, depositary, clearing and settlement institutions, auditors, accountants, registrars, register and nominee holders, trading venues, investment firms and other financial intermediaries.
- Technical data from information technology, information security and connectivity service providers.

5. HOW WE USE YOUR PERSONAL DATA

We need all the categories of your personal data primarily to allow us to take steps at your request before we have a contract with you (**PC**), perform a contract we have with you (**C**) and to comply with our legal obligations (**O**).

In some cases, we may use your personal information to pursue legitimate interests of our own or those of third parties (**L**), provided your interests and fundamental rights do not override those interests.

The situations in which we will process your personal information are listed below. We have indicated by letters the purpose or purposes for which we are processing or will process your personal information.

- Entering into a contract and implementing pre-contractual measures: **P**, **C**.

- Fulfilling know your customer and due diligence requirements: **PC**, **C**, **O**.
- Authenticating a natural person: **C**, **O**, **L**.
- Confirming or evidencing the capacity to contract: **C**, **O**, **L**.
- Performing control and risk management functions: **C**, **O**, **L**.
- Monitoring credit exposure: **C**, **O**, **L**.
- Conducting sanctions and anti-money laundering/countering the financing of terrorism compliance processes: **O**, **L**.
- Conducting regulatory screening: **O**.
- Complying with requirements of our agents, bankers, brokers and any financial institution or intermediary with which we may have dealings, entities that are financial market infrastructure entities or trading venues, and industry bodies: **PC**, **C**, **O**, **L**.
- Carrying out financial, regulatory and tax reporting: **C**, **O**.
- Preventing, detecting and investigating a crime or other potential wrongdoing or threats to public security: **C**, **O**.
- Personal safety of staff, visitors and other members of the public and to act as a deterrent against crime – **L**.
- Protecting buildings and assets from damage, disruption, vandalism and other crime – **L**.
- Supporting law enforcement bodies in the prevention, detection and prosecution of crime – **O**, **L**.
- Auditing: **O**, **L**.
- Performing obligations to any party that may have an interest in any of our rights or obligations: **L**.
- Establishing, investigating, pursuing, exercising, defending or remedying claims, complaints, regulatory or investigative inquiries or information subpoenas: **C**, **O**, **L**.
- Taking, holding, protecting, perfecting, preserving or enforcing (or attempting to do so) any rights, powers, authorities or discretions vested in us or a third party under a contract or by law: **C**, **L**.

In addition to the above, if you are a customer or an individual representative of a customer, we will use personal data about you for:

- Providing our products and services: **PC**, **C**.
- Account and client relationship management: **PC**, **C**.
- Conducting analysis activities: **L**.
- Ensuring and supporting network, information or physical security: **O**, **L**.

If you are a guarantor, collateral or security provider or an individual representative of any guarantor, collateral or security provider or a market counterparty, we will additionally use personal data about you for**:**

- Trading securities and other investments: **PC**, **C**, **O**, **L**.
- Obtaining guarantee, security or taking collateral: **PC**, **C**, **O**, **L**.

Where you become an heir, successor or assignee of any of our customers or any guarantor, collateral or security provider or a market counterparty or where you act as a representative of any of the foregoing, we will use personal data about you exclusively for:

- Performing our legal obligations: **O**.
- Performing obligations to any party that may have an interest in any of our rights or obligations: **L**.
- Establishing, investigating, pursuing, exercising, defending or remedying claims, complaints, regulatory or investigative inquiries or information subpoenas: **C**, **O**, **L**.

- Taking, holding, protecting, perfecting, preserving or enforcing (or attempting to do so) any rights, powers, authorities or discretions vested in us or a third party under a contract or by law: **C**, **L**.

Note that we may process your personal data for more than one lawful ground depending on the specific purpose for which we are using your data. Please contact our DPO if you need details about the specific legal ground we are relying on to process particular personal data we hold about you.

How we use particularly sensitive personal information

Special categories of particularly sensitive personal information require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal information. We have in place an appropriate policy document and safeguards, which we are required by law to maintain when processing such data.

We may process special categories of personal information in the following circumstances:

- In limited circumstances, with your explicit written consent.
- Where it is necessary for preventing, detecting and investigating a crime or other potential wrongdoing, authentication and confirmation of the capacity to contract.
- Where it is necessary for establishing, exercising or defending legal claims.

Information about criminal convictions

We will only collect information about criminal convictions where we are legally able to do so. We will use information about criminal convictions and offences to comply with requirements established by appropriate authorities for investment firms, where you have already made the information public or where it is necessary for us to establish or defend legal claims. We have in place an appropriate policy and safeguards, which we are required by law to be maintained when processing such data.

Consent

Generally, we do not rely on consent as a legal basis for processing your personal data other than in relation to sending direct marketing communications to you via e-mail or text message. We do not need your consent if we use your personal information to carry out our legal obligations or exercise specific rights afforded by law.

In limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us.

Change of purpose

We will only use your personal data for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If you wish to get an explanation as to how the processing for the new purpose is compatible with the original purpose, please, contact our DPO.

If we need to use your personal data for an unrelated purpose, we will notify you and we will explain the legal basis, which allows us to do so.

Marketing

We may use your data to form a view on what we think you may want or need, or what may be of interest to you. This is how we decide which products, services and offers may be relevant for you (we call this marketing). You will receive marketing communications from us if you have requested information from us or entered into a contract with us for the provision of financial products or services or if you provided us with your details when you registered for a promotion and, in each case, you have not opted out of receiving that marketing.

We will get your express opt-in consent before we share your personal data with any person or entity for marketing purposes.

You can ask us or third parties to stop sending you marketing messages at any time by contacting our DPO at any time. Where you opt out of receiving these marketing messages, this will not apply to personal data provided to us as a result of a product/service provision or other transactions.

Automated decision-making

You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making, unless we have a lawful basis for doing so and we have notified you.

We do not envisage that any decisions will be taken about you using automated means, however we will notify you in writing if this position changes.

6. DATA SECURITY

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed.

Specifically, we implement the following technical and organizational security measures to protect your personal data:

- Pseudonymisation of personal data.
- Encryption of personal data.
- Segregation of personal data from other networks.
- Access control and user authentication.
- Employee training on information security.
- Written information security policies and procedures.

In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal information on our instructions and are subject to a duty of confidentiality.

We have also put in place procedures to deal with any suspected data security breach and will notify you and the Information Commissioner of a suspected breach where we are legally required to do so. Further details of these measures may be obtained from our DPO.

7. DISCLOSURE OF YOUR PERSONAL DATA

We may share your personal data with the parties listed below for the purposes set out in section 5 above:

- Our employees.
- Our parent company, subsidiaries, and affiliated entities.

- Our business partners or intermediaries with which we may have dealings.
- Our auditors and professional advisors, such as lawyers and consultants.
- Bankers, brokers and financial market infrastructure entities.
- Trading venues.
- Governmental, regulatory or similar authorities or industry bodies.
- Courts or tribunals of competent jurisdiction.
- Law enforcement officials;
- Certifying officers, notary public, administrators, trustees or other executors.
- Liquidator, conservator, custodian, trustee or a temporary administrator, external administrator, receiver or similar or analogous officer or body appointed in any bankruptcy, prevention measures, insolvency, bankruptcy, dissolution, liquidation or winding-up (or any analogous or similar proceedings).
- Third-party service providers, such as providers of IT system management or information security.

International transfers

We may share your personal data with external third parties based outside the European Economic Area (**EEA**).

Whenever we transfer your personal data outside the EEA, we ensure a similar degree of protection is afforded to it by ensuring at least one of the following safeguards is implemented:

- We transfer your personal data to countries that have been deemed to provide an adequate level of protection for personal data by the European Commission. For further details, see European Commission: Adequacy of the protection of personal data in non-EU countries, here https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en.

- We have entered into specific contracts approved by the European Commission, which give personal data the same protection it has in Europe. For further details, see European Commission: Model contracts for the transfer of personal data to third countries, here https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en.

- The transfer is necessary to enter into or perform our contract with you or in your interest or to establish, exercise or defend legal claims or to pursue our compelling legitimate interests and we have assessed all the circumstances surrounding the transfer and have on the basis of that assessment provided suitable safeguards with regard to the protection your personal data.

Our compelling legitimate interests referred to above, may include:

- Ensuring network, information or physical security.
- Authenticating natural persons.
- Preventing, detecting and investigating a crime or other possible wrongdoing or threats to public security.
- Establishing, investigating, pursuing, exercising, defending or remedying claims, complaints, regulatory or investigative inquiries or information subpoenas.
- Managing compliance, tax, regulatory and other risks.

- Taking, holding, protecting, perfecting, preserving or enforcing (or attempting to do so) any rights, powers, authorities or discretions vested in us under a contract or by law.
- Performing obligations to any party that may have an interest in any of our rights or obligations.
- With respect to individual representatives of a business, implementing pre-contractual measures at the request of the relevant business, performing a contract between us and the business or a contract between us and a third party that is concluded in the interest of the business.

Suitable safeguard we provide for international transfers may include:

- A transfer pseudonymized or encrypted data.
- Ensuring with technical and organizational measures that the transferred data cannot be used for other purposes than those strictly foreseen by us.
- Limiting the purposes for which the data may be processed following the transfer.
- Ensuring deletion of the data as soon as possible after the transfer.
- Ensuring data recipients undertake to implement adequate technical and organizational security measures, inform us about binding requests for disclosure and any accidental or unauthorised access to personal data, respond to our enquiries and request our approval in the event of sub-processing.
- Recording all relevant aspects of data transfer.
- Advising the Information Commissioner of these transfers so that it assesses the data transfers and consider their potential impact on your rights and freedoms.

8. HOW LONG WILL WE USE YOUR PERSONAL DATA?

We will only retain your personal data for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements.

To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

We typically retain personal data for the periods set out below, subject to any exceptional circumstances or to comply with laws or regulations that require a specific retention period.

If as a result of pre-contractual negotiations we do not enter into a contract with you, we erase your personal data within 1 month following the date on which it becomes apparent to us that no contract will be made.

If we enter into a contract with or for you, we retain:

- Identity, Family, Education, Contact, Occupation, Financial, Transaction, Technical and Profile Data about you as a customer or an individual representative of a customer throughout the term of the contract and 6 years following termination thereof or 12 years following termination thereof if we provide financing on a secured basis. We retain Criminal Convictions, Marketing and Communications Data throughout the term of the contract and 5 years following termination.

- Identity, Family, Education, Contact, Occupation, Financial, Transaction, Technical and Profile Data about you as a customer's underlying client or principal or their individual representative throughout the term of the contract and 6 years following termination thereof or 12 years following termination thereof if we provide financing on a secured basis. We retain Criminal Convictions Data throughout the term of the contract and 5 years following termination.

- Personal data about you as a customer's or its underlying client's or principal's shareholder, beneficial owner or a politically exposed persons with whom any customer, its underlying client or principal or any of their representatives may have relations, throughout the term of the contract and 5 years following termination of the contract.

- Identity, Contact and Transaction Data about you as a guarantor, collateral or security provider or an individual representative of a guarantor, collateral or security provider whenever secured or collateralised obligations remain outstanding and 6 years following termination of the guarantee, return of collateral or release of security, as applicable, or 12 years upon return of collateral or release of security if secured obligations relate to financing. We retain Family and Financial Data whenever secured or collateralised obligations remain outstanding and 1 month upon termination of the guarantee, return of collateral or release of security.

- Personal data about you as an individual representative of a market counterparty throughout the term of the relevant contract and 6 years following its termination.

- Personal data about you as an heir, successor or assignee of any customer, counterparty, guarantor, collateral or security provider, 12 years upon receipt.

We permanently delete video footage with your images whether live feeds from cameras and recorded images, once there is no reason to retain the recorded information. Exactly how long images are retained varies according to the purpose for which they are being recorded. For example, where images are being recorded for crime prevention purposes, we keep data long enough only for incidents to come to light. In all other cases, we keep recorded images for no longer than 40 days. We maintain a comprehensive log of when data is deleted. At the end of their useful life, we erase all images stored in whatever format permanently and securely. We dispose of any physical matter such as tapes, discs, still photographs or hard copy prints as confidential waste.

9. YOUR LEGAL RIGHTS

Under certain circumstances, you have rights under data protection laws in relation to your personal data. You have the right to:

Request access to your personal data (commonly known as a "**data subject access request**"). This enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it.

Request correction of the personal data that we hold about you. This enables you to have any incomplete or inaccurate data we hold about you corrected, though we may need to verify the accuracy of the new data you provide to us.

Request erasure of your personal data. This enables you to ask us to delete or remove personal data where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal data where you have successfully exercised your right to object to processing (see below), where we may have processed your information unlawfully or where we are required to erase your personal data to comply with local law. Note, however, that we may not always be able to comply with your request of erasure for specific legal reasons, which will be notified to you, if applicable, at the time of your request.

Object to processing of your personal data where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground as you feel it impacts on your fundamental rights and freedoms. You also have the right to object where we are processing your personal data for direct marketing purposes. In some cases, we may demonstrate that we have compelling legitimate grounds to process your information, which override your rights and freedoms.

Request restriction of processing of your personal data. This enables you to ask us to suspend the processing of your personal data in the following scenarios:

- if you want us to establish the data's accuracy;
- where our use of the data is unlawful but you do not want us to erase it;
- where you need us to hold the data even if we no longer require it as you need it to establish, exercise or defend legal claims; or
- you have objected to our use of your data but we need to verify whether we have overriding legitimate grounds to use it.

Request the transfer of your personal data to you or to a third party. We will provide to you, or a third party you have chosen, your personal data in a structured, commonly used, machine-readable format. Note that this right only applies to automated information which you initially provided consent for us to use or where we used the information to perform a contract with you.

Withdraw consent at any time where we are relying on consent to process your personal data. However, this will not affect the lawfulness of any processing carried out before you withdraw your consent. If you withdraw your consent, we may not be able to provide certain products or services to you. We will advise you if this is the case at the time you withdraw your consent.

If you wish to exercise any of the rights set out above, please, contact our DPO.

No fee usually required

You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive. Alternatively, we may refuse to comply with your request in these circumstances.

What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights). This is a security measure to ensure that

personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.

Time limit to respond

We try to respond to all legitimate requests within one month. Occasionally it may take us longer than a month if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.

10. CHANGES TO THE PRIVACY NOTICE AND YOUR DUTY TO INFORM US OF CHANGES

It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes during your relationship with us.

This version of the privacy notice was last updated on **01 October 2019** and historic versions are archived here http://bcscyprus.com/policies or can be obtained by contacting our DPO.