

PRIVACY NOTICE OF SKASH LTD

Last update: January 2021

1. OVERVIEW

SKASH LTD, a company incorporated in the Republic of Cyprus under Reg. No. HE 377272 and having its registered office at Tassou Papadopoulou 6, Flat 22, Agios Dometios, 2373, Nicosia, Cyprus (“**we**,” “**our**” “**us**” or “**SKASH**”) is committed to protecting and respecting your privacy and your rights, as regards the personal data collected and processed for the provision of our products and services.

We process your personal information in accordance with the applicable legal and regulatory framework, including the *Law on the Protection of Natural Persons Against Personal Data Processing and the Free Movement of Such Data of 2018 (L. 125(I)/2018)*, as amended from time to time, and the *General Data Protection Regulation 2016/679 (“GDPR”)*, which applies as of 25 May 2018.

This notice (referred to as the “**Privacy Notice**” or “**Notice**”) provides an overview of how and why SKASH processes personal data concerning natural persons, as well as of the rights of such persons, in the context of the offering and providing a mobile wallet which operates on a smartphone through a mobile application and which may be used as a bank account and/or payment tool (“**sKash**” **Mobile Wallet Application**) for which an electronic card may be issued to its users (“**sKash**” **cards**). This Privacy Notice is directed to natural persons who are current or prospective customers of SKASH who have started but not completed for any reason their online registration to the “sKash” Mobile Wallet Application, or are authorised representatives/agents, security providers, related parties, or beneficial owners of legal entities or of natural persons which/who are current or prospective customers of SKASH (“**you**”, “**your(s)**” or “**User**”).

For the purposes of the present Privacy Notice, the terms “**personal data**”, “**data**” and “**personal information**” are used to refer to any information relating to you that identifies or may identify you, either directly or indirectly, such as your name, contact details, identification data (e.g. identity card/passport number) and authentication data (e.g. your signature). Moreover, the term “**processing**” is used herein to collectively refer to actions such as the collection, retention, use, disclosure, transfer, deletion or destruction of personal data.

Please read the following carefully in order to understand our policies and practices regarding your personal data and how we process them.

2. WHO WE ARE AND OUR CONTACT DETAILS

SKASH is a company incorporated in the Republic of Cyprus under Reg. No. HE 377272 having its registered office at Tassou Papadopoulou 6, Flat 22, Agios Dometios, 2373, Nicosia, Cyprus, telephone number 777 87 0 87 or +357 22276730.

SKASH operates under Astrobank Ltd (the “**Bank**”) and as a result SKASH is ultimately regulated by the supervision of the Central Bank of Cyprus.

Responsibility for the processing of your personal data lies with SKASH, which acts as the data controller, i.e. as the entity that, alone or jointly with others, determines the purposes and means of the processing of personal data.

You may contact our Data Protection Officer (DPO) for any matters arising out of and/or in connection with this Privacy Notice, including for the purposes of exercising your rights, at the following contact details:

Data Protection Officer of SKASH
Tel. Number: 777 87 0 87 or +357 22276730
Email: contact@skash.com

We will use reasonable endeavors, in line with the applicable legal framework, to meet, comply with and reply to your inquiries, requests and comments promptly and transparently.

3. WHAT KIND OF PERSONAL DATA WE PROCESS

SKASH LTD is 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.

This notice forms part of any contract of employment or other contract to provide services. We may update this notice at any time but if we do so, we will provide you with an updated copy of this notice as soon as reasonably practical.

It is important that you read and retain this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information and what your rights are under the data protection legislation.

The type of personal data we process, the particular processing activity we utilize, as well as the extent of such processing, depend on the services and products requested or agreed in each case.

We collect, use, consult or otherwise process personal data of:

- **prospective and current individual customers;**
- **persons connected to prospective and current customers, as applicable and/or appropriate (“connected persons”);**
 - *Where such customers are **individuals***, connected persons may include introducers, authorised representatives/agents, attorneys/administrators/executors, family members or close associates of such customers that fall under the category of politically exposed persons (PEP), past and/or current employers.
 - *Where such customers are **legal entities***, connected persons may be, *inter alia*, introducers/associates, authorised representatives/agents, officials, partners, shareholders, investors, administrators, trustees, authorised signatories, family members or close associates of such connected persons that fall under the category of politically exposed persons (PEP), ultimate beneficial owners (UBOs).
- **security providers** for credit facilities (e.g. guarantors); and
- **non-customer counterparties**, as required for the provision of our services (e.g. personal and payment information of payers or beneficiaries in payment transactions).

More analytically:

- A. Where you are a prospective customer (including an authorised representative/agent of an individual or legal entity that is a prospective customer or the ultimate beneficial owner of a legal entity that is a prospective customer); or a prospective security provider such as a guarantor of credit facilities, we collect and further process data that may include the following:**
- In particular, regarding the “sKash” Mobile Wallet Application, including the issuance of the “sKash” cards, during the registration and/or subscription process of natural persons we may collect *inter alia*, identity card numbers and copies thereof, and/or mobile phone numbers and/or email addresses and/or utility bills and/or other supporting documentation and/or all data as mentioned herein below.
 - personal identification data (e.g. name, surname, passport/identity card number, social security number);
 - personal details (e.g. gender, marital status, number of dependents, date of birth, place of birth, country of birth, citizenship, education level and other information contained in CVs, where applicable);
 - authentication information (e.g. signature);

- contact details (e.g. residence address, mailing address, phone numbers, e-mail address);
- employment data/business activities information (e.g. profession, employer's name, job title, employment address and contact data);
- financial identification data (e.g. details of income and expenses, assets and liabilities (including debts and provision of securities), past and expected financial and economic activity);
- tax information, including the US Foreign Account Tax Compliance Act (FATCA) and Common Reporting Standard (CRS) details (e.g. country of tax residence, tax identification number);
- politically exposed persons (PEP) information (where you or a family member or close associate holds/held a prominent public function);
- purposes for and nature of the intended business relationship with us;

Should we enter into a business/contractual relationship with you, we will retain and further process the aforementioned data, as explained in section 8 herein below.

B. In the course of the provision of services and products to you or the legal entity you are connected with, additional personal data may be collected, used and stored, primarily the following:

Account and payment services through "sKash" Mobile Wallet Application, the issuance of the "sKash" card"; ad hoc or standing orders/direct debits; and credit/debit cards)

Payment transaction data as well as any other data associated with the transaction. Such data includes account numbers and/or IBAN numbers and/or other unique identifiers; account(s) balance; nature and type of a payment transaction (e.g. purchase of goods, purchase of services, money transfers); data transmitted with the payment order; data about when, where and with whom you transact with, including data of third-party beneficiaries and any other processing that may arise out of our contractual obligations.

C. Regardless of whether you are a prospective or current customer (including an authorised representative/agent of such an individual or legal entity or the ultimate beneficial owner of such a legal entity); or a prospective or current security provider such as a guarantor of credit facilities, we may process the following data:

Website and electronic/digital services

When you access and use our website and the "sKash" Mobile Wallet Application), we collect data such as the internet protocol (IP) address used to connect your device to the internet, your login data, type of device you use, network/browser data, a unique device identifier (e.g your mobile phone number and/or device ID), the times you access our website and/or electronic/digital services; and geolocation data.

Moreover, when you access and use our website or online services, we may place small data files on your device ("**cookies**") in order to create a safer and more efficient online environment. You can view our cookies policy at our website at <https://www.skash.com/cookies> .

We collect automatic information, as above, in order to assess, customise and improve our services and products, aiming to deliver to you the highest experience and service standards.

Kindly note that, should users of our website choose to follow the special connections (links, hyperlinks, banners) to the websites of third parties, we are not responsible for the terms of personal data processing and protection followed by these parties.

Communications with us

When you communicate with us (e.g. emails, phone or video calls, etc.), more data are created (e.g. method of communication, date and time, content and outcome of our communication). We record and retain in our records information generated by such communications and our relevant responses to you, for the following reasons:

- We record communications regarding customer service enquiries, requests and comments, to ensure that you receive optimum service levels;
- We record communications regarding applications for and provision of banking and financial transactions, in order to comply with our statutory obligations under the anti-money laundering and anti-terrorism law and relevant regulatory obligations of the Central Bank of Cyprus.

4. CHILDREN'S DATA

For the purposes of this Privacy Notice, "children" are defined as individuals under the age of eighteen (18). We understand and respect the importance of protecting the privacy of children. We may process the personal data of children only with the prior consent and/or authorization of their parents or legal guardians or as otherwise required or permitted by law as explained in our Privacy notice for additional cardholders (minors) which can be found at our website.

5. SOURCES OF PERSONAL DATA

We lawfully obtain data, as described above, *to the extent and where necessary* in order to provide our services and products, from:

- **Prospective and current customers**, either directly from them or from their authorised representatives/agents or via other communication channels (e.g. our website and the "sKash" Mobile Wallet Application);
- **Third parties**, e.g. public and/or regulatory and/or supervisory authorities (such as Department of the Registrar of Companies and Official Receiver of the Republic of Cyprus the Central Bank of Cyprus; Cyprus Clearing House, Central Information Registry and competent Land Registry Offices); credit reference bureaus such as the Data Exchange Mechanism Artemis; other non-affiliated entities with which we have a contractual relationship for the purposes of the provision of our services and products (e.g. JCC Payment Systems Ltd and the Lufthansa Group for credit and debit cards services; cards and ATM services providers; private investigators (in Cyprus and/or abroad), insurance companies for different kinds of insurance contracts e.g. life insurance, bancassurance, motor vehicle, fire or household insurances; other payment services institutions such as Banks and other third parties you transact with (e.g. merchants); natural or legal persons acting as introducers/associates; and entities providing services and products for Know-Your-Customer (KYC) and due diligence purposes;
- **Publicly available sources**, e.g. registries maintained by public and/or regulatory and/or supervisory authorities (such as the Companies' Registry, the Bankruptcies and Liquidations Registries and the Intellectual and Industrial Property Registries maintained by the Department of the Registrar of Companies and Official Receiver of the Republic of Cyprus; and competent Land Registry Offices); lists and databases maintained by other entities including international organisations (such as sanctions list and politically exposed persons (PEPs) lists); the media, the press and the internet.

6. WHY WE PROCESS YOUR PERSONAL DATA AND ON WHAT LEGAL BASIS

We collect and further process your personal information in compliance with the applicable data protection legal framework, for the following reasons:

- For the purposes of completion of registration of prospective customers or customers

We may contact you in order to assist you and/or provide further information as to how to complete your registration online successfully.

- For the performance of contractual obligations

We collect and further process data which is necessary in order to perform our contractual obligations to you for the provision of our services and products, or to take steps, at your request, prior to entering into a contract with us. The purposes of the data processing are mainly dependent on the specific service and/or product, as described in the relevant contractual terms and conditions and can include needs assessments, advice, asset management and support, as well as executing transactions.

- For compliance with our legal obligations

Since we operate under the Bank, we are subject to various legal obligations, namely statutory requirements (for example under the applicable payment services, money-laundering and terrorism financing, and tax laws); as well as requirements of supervising and/or regulatory authorities (including of the European Banking Supervisory Authority; the Central Bank of Cyprus; the Cyprus Police, including the Unit for Combating Money Laundering (MOKAS), and the Cyprus Securities and Exchange Commission).

For these reasons, data collected, as described above, is used for anti-money laundering and anti-fraud measures; credit controls; tax law controls and reporting obligations; assessment and management of risks of the Bank; for compliance with Court judgments and/or orders; e.t.c.

- For safeguarding legitimate interests

Where necessary, we collect and manage data above and beyond the performance of our contractual and/or legal obligations, where it is necessary for safeguarding legitimate interests pursued by us or by other parties, in compliance with the applicable personal data legal framework. Data and/or information are processed under this ground for reasons pertaining to business and/or commercial interests, taking into consideration the necessity of such action and your interests, fundamental rights and freedoms, as well as your reasonable expectations. Examples of such processing include the following:

- Consulting and exchanging data with credit reference agencies (e.g. the Data Exchange Mechanism Artemis) and other registries (e.g. the Companies' Registry, the Bankruptcies and Liquidations Registries and the Intellectual and Industrial Property Registries maintained by the Department of the Registrar of Companies and Official Receiver of the Republic of Cyprus; competent Land Registry Offices) to determine credit or default risks;
- Pursue and/or defense of claims in judicial and/or regulatory procedures;
- To collect and recover funds owned to the Bank;
- Consulting and exchanging data with external legal consultants/advisors for preparation for legal claims or on ad hoc basis for particular cases;
- Consulting or exchanging data with external accountants/auditors;
- Transfer, assignment and/or sale of any or all of our rights, titles or interests under any agreement between you and us;
- Reviewing and improving procedures for needs and demands assessments for the purpose of direct client discussions;
- Advertising or market and opinion research, provided that you have not objected to having your data processed for such purposes;
- Measures for further developing services and products and managing business;
- Ensuring the smooth operation of our network and IT operations and security;
- Measures and processes for IP rights protection and theft prevention;
- Crimes and fraud prevention and investigation;
- Measures and processes for security purposes and to prove availability (e.g. video surveillance (CCTVs) of our branches, offices and ATMs; admittance controls; and anti-trespassing measures); and
- Risk management and control.

- On the basis of your consent

Insofar as you have granted us explicit and specific consent to the processing of your personal data for specific purposes other than the ones described above, the lawfulness of such processing is based on your consent.

You have the right to revoke your consent at any time. Kindly be advised that any such revocation shall only have effect after it is submitted and filed by us, and that it will not affect the lawfulness of data processed prior to the revocation.

7. WHO RECEIVES YOUR PERSONAL DATA

Within SKASH, your personal information is only processed by the departments/units and/or persons that are authorised to process them, given that it is necessary to do so for the fulfillment of our contractual and legal obligations, or where you have given us your consent to process them, or where we believe that it necessary for our legitimate interests to do so, as explained by section 5 above. Kindly note that such persons are under banking secrecy and confidentiality obligations.

Your data may also be received by various service providers and suppliers with whom we have contractual agreements, pursuant to which they are bound by the confidentiality and data protection obligations according to the applicable data protection legal framework.

We may also disclose your personal information to other individuals and/or entities for any of the reasons described above, where and to the extent we are legally obligated or otherwise authorised to do so, or where you have given us your explicit consent.

We will **not** disclose and/or transfer your personal information to any third parties for their own direct marketing purposes, unless you have explicitly authorised us to do so.

Under the aforementioned conditions, recipients of your personal data may include:

- Public and/or regulatory and/or supervisory authorities and other public institutions, to the extent that we are under a statutory or regulatory obligation to do so, such as the Central Bank of Cyprus (e.g. data that we disclose and/or disclose to the Central Information Registry (CIR) maintained by the Central Bank of Cyprus that includes information about dishonoured cheques), the European Central Bank, the Cyprus Securities Exchange Commission, tax authorities, law enforcement authorities (e.g. police, including the Unit for Combating Money Laundering (MOKAS)); courts and tribunals;
- Other public authorities, where we are authorised by you to do so (e.g. the Ministry of Labour, Welfare and Social Insurance in respect of applications for benefits; the Ministry of Finance in respect of applications for exemptions);
- Other banking and financial institutions or electronic institutions or similar institutions to which we transfer your data in order to perform our contractual obligations (e.g. corresponding banks; custodian banks; brokers; stock exchanges; share and stock investment and management companies; the European Investment Fund);
- Entities we work with for the provision of credit/debit card services (e.g. VISA, MASTERCARD, and JCC Payment Systems Ltd.) including the entities with which the Bank cooperates for the issuance of the “sKash” cards;
- The Cyprus Clearing House, for the exchange and clearance of cheques;
- Direct debit service providers;
- Entities offering technological expertise, solutions and support, such as the Wallet service providers;
- Credit reference agencies such as the Data Exchange Mechanism Artemis;
- Valuers and surveyors;
- Insurance companies;
- External legal consultants, auditors and accountants; financial and business advisors;

- Marketing, market research and advertising companies;
- File storage, archiving, records management companies and cloud storage companies;
- Prospective and actual purchasers, assignees, transferees and chargees of our rights, titles, titles or interests under any agreement between you and us;
- Your own legal representatives/agents.

8. DATA TRANSFERS TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS

Personal data will only be transferred to third countries, namely countries outside the European Economic Area where:

- it is necessary to do so in order to carry out your payment orders. In particular for international credit transfers and separately requested express credit transfers executed through SWIFT, personal data may be transferred to SWIFT's operating centers in the US;
- where we are legally obliged to do so (e.g. the Bank is obliged to disclose information to the Cyprus Ministry of Finance which may in turn disclose it to the US authorities pursuant to the legal framework implementing the US Foreign Account Tax Compliance Act (FATCA) and the OECD Common Reporting Standards (CRS Law); and
- or where you have given us your consent to do so.

Service providers, members of our Group of Companies and other entities that process your personal data on our behalf are under the obligation to comply with the same personal data protection standards and safeguards as we do, on the basis of either an adequacy decision issued by the European Commission pursuant to Article 45 of the GDPR (in particular, to Switzerland regarding services being rendered in respect of private banking customers) or contractual clauses between us and them or other appropriate safeguards pursuant to Article 46 of the GDPR including, inter alia, the implementation of binding corporate rules in accordance with Article 47 of the GDPR.

9. RETENTION PERIOD

As a general rule, we only retain your personal data for as long as it strictly necessary for the purposes they were initially collected, in accordance with the applicable statutory and regulatory framework, including the relevant Directives issued by the Office of the Data Protection Commissioner of the Republic of Cyprus, which are available at the Commissioner's website:

http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/page3f_gr/page3f_gr?opendocument

1. Pursuant to the above Directives, we shall retain your personal data as follows:

- **Personal data of current customers; persons connected to current customers (as above); and current security providers (e.g. guarantors):**
We shall retain personal data of such persons throughout our business/contractual relationship with you.
- **Personal data of former customers; persons connected to former customers (as above); and former security providers (e.g. guarantors):**
We will delete and destroy or anonymize the personal data of such persons on or about the (10) ten years anniversary of when the contractual relationship between such persons and us is terminated in its totality, either by the Company's request or the Customer's request, whatever the cause of termination may be, and/or the accounts of such persons are closed and/or an individual transaction taking place outside the context of a business/contractual relationship is executed. The aforesaid will not apply and we retain such data for longer where there are any pending legal proceedings and/or investigations by public authorities/bodies and/or other disputes/differences in relation to such data.

- **Personal data of prospective customers; persons connected to prospective customers (as above); prospective security providers (e.g. guarantors) and customers with dormant accounts (dormant accounts for this policy shall mean accounts which have been created by customers but have never been used):**

We will delete and destroy or anonymize the personal data of such persons within six (6) months after the relevant notification for the rejection of applications or the withdrawal of interest by the prospective customer.

2. Pursuant to the **Prevention and Suppression of Money Laundering Activities Law of 2007**, we will retain the following information and documentation for a period of five (5) years after the end of our business relationship with the customer or after the date of a single transaction:

(a) a copy of the documents and information required for compliance with customer due diligence requirements as defined in the aforementioned Law;

(b) the relevant evidence and records of transactions which are necessary for the identification of transactions;

(c) relevant correspondence documents with customers and other persons with whom a business relationship is maintained.

- At the end of the five year period referred to above, we shall delete the above specified personal data unless otherwise provided by other legislation.
- It is provided that we retain the above information/documentation for five (5) additional years where the further retaining of such information/documentation is reasonably justifiable for the purposes of preventing, identifying and investigating money laundering activities and the financing of terrorism, without prejudice to the provisions relating to criminal proceedings concerning evidence in connection with ongoing criminal investigations and proceedings.

10. WHETHER WE CARRY OUT AUTOMATED DECISION MAKING (INCLUDING PROFILING)

We may process and/or use some of your data collected through the “sKash” Mobile Wallet Application which are necessary in order to create and or update your respective SKASH account and/or profile, including by automatic means and in order to evaluate certain of your personal aspects (**profiling**), in the following cases:

- We carry out data evaluations (including on payment transactions) in the context of our anti-money laundering, anti-terrorism financing and anti-fraud measures. Such assessments may also serve to protect your interests (e.g. where we become aware of any unusual activity of your accounts);
- We employ credit scoring to assess your creditworthiness, so that we can evaluate whether Users will meet their contractual payment obligations and to make fair and responsible decisions regarding the provision of our services and products.
- We review the frequency and/or volume of your payment transactions, so that we can evaluate whether Users may be eligible for credit vouchers with such specific merchants.

You always have the right to object to this kind of profiling activities performed from exercising your rights, as those are described under clause 13 of this Privacy Notice.

Automated decision-making means that a decision which is likely to have legal effects or similarly significant effects on you, is taken solely by technological means, without any human intervention. SKASH may use your personal data to make decisions entirely or partially based on automated processes according to the purposes outlined in this document. SKASH adopts automated decision-making processes as far as necessary to enter into or perform a contract between you and SKASH, or on the basis of your explicit consent when this is required by the law.

Automated decisions are made by technological means – mostly based on algorithms subject to predefined criteria – which may also be provided by third parties. The rationale behind automated decision making is:

- to create your SKASH account and/or perform any functions of the “sKash” Mobile Wallet Application;
- to enable or otherwise improve the decision-making process;
- to grant Users fair and unbiased treatment based on consistent and uniform criteria;
- to reduce the potential harm derived from human error, personal bias and the like which may potentially lead to discrimination or imbalance in the treatment of individuals etc;
- to reduce the risk of User's failure to meet their obligation under a contract.

As a consequence, Users subject to such processing, are entitled to exercise specific rights aimed at preventing or otherwise limiting the potential effects of the automated decisions taken. In particular, Users have the right to:

- obtain an explanation about any decision taken as a result of automated decision-making and express their point of view regarding this decision;
- challenge a decision by asking SKASH to reconsider it or take a new decision on a different basis;
- request and obtain from SKASH human intervention on such processing.

11. MARKETING

We will only use your personal information for direct marketing purposes if (a) you have given us your explicit consent to do so, in which case you may revoke such consent at any time; or (b) where we believe that such processing is necessary for pursuing our legitimate interests, in accordance with the applicable legal framework and having taken into account the considerations described in section 5 above, in which case you have the right to object to such processing, as described in section 12 below. More options on marketing notifications will be available to you for modification via your private settings inside the SKASH app.

12. WHETHER YOU HAVE AN OBLIGATION TO PROVIDE US WITH YOUR PERSONAL DATA

We will ask you to provide us with certain personal information, as described in section 2 above, when you (or the natural or legal person that you represent, or act as agent of, or the entity you are a beneficial owner of) apply to enter into a business relationship with us, as well as during the course of our business relationship (including when you apply for more services and products). The provision of such personal information is a requirement for accepting and carrying out or for continuing a business relationship with you, as they are necessary for the performance of our contractual obligations and for us to comply with our legal obligations, as described by section 5 herein. In particular, we are under legal obligations, in accordance with the applicable anti-money-laundering and anti-terrorism financing legal framework, to collect and use at least the following information and relevant documentation regarding yourself and any natural or legal person that you represent, or act as agent of, or the entity you are a beneficial owner of:

- Identification data;
- Citizenship, country and city of birth;
- Residency information, including residential address.

Moreover, during the course of our business/contractual relationship, you must be disclosing any changes to the aforementioned data, without undue delay.

If you do not provide us with the necessary information and supporting documentation, we will not be able to enter into or continue a business/contractual relationship with you (or the natural or legal person that you represent, or act as agent of, or the entity you are a beneficial owner of).

13. YOUR PERSONAL DATA RIGHTS

We respect the rights you have under the personal data legal framework, namely the following:

- **Right of access**
You have the right to obtain from us confirmation as to whether or not data concerning you are being processed and, if that is case, access to such data and further information in relation to them.
- **Right of rectification**
You have the right to request and to obtain from us rectification of inaccurate personal information concerning you.
- **Right to erasure (“right to forget”)**
You have the right to request us to erase your data, where one of the following applies:
 - Where such data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
 - Where we process such data on the basis of your consent and you refuse or withdraw such consent, provided that no other legal ground for processing applies;
 - Where we process your personal information in order to pursue our legitimate interests (e.g. for direct marketing purposes) and you object to such processing, provided that no overriding legitimate grounds for the processing apply;
 - Where such personal data have been unlawfully processed; and
 - Where such personal data have to be erased in compliance with a legal obligation of the Bank or SKASH.
- **Right to restriction of processing**
You have the right to obtain from us restriction of processing of data concerning you, where one of the following applies:
 - Where you contest the accuracy of such data, for a period that allows us to verify the accuracy of such data;
 - Where the processing is unlawful and you oppose the erasure of such data, requesting restriction of their use instead;
 - Where we no longer need to process such data, but you require their retention for the establishment, exercise or defense of legal claims; and
 - Where you have objected to us processing of your personal information on the grounds of our legitimate interests (e.g. for direct marketing purposes), until we verify whether the grounds on which we process such data override your rights and freedoms.
- **Right to object to processing**
You have the right to object, at any time, on grounds relating to your particular situation, to us processing your personal data on the basis of our legitimate interests (e.g. for profiling, including for direct marketing purposes). Should you exercise this right, we will no longer process such data unless we are able to demonstrate compelling legitimate grounds for the processing.
- **Right to withdraw consent**
Where we request your consent for processing your information, you have the right to refuse to give such consent. Moreover, where you have already given us such consent, you can revoke it at any time. Any such revocation shall only have effect after it is submitted and filed by us, and will not affect the lawfulness of data processed prior to such revocation.

- **Right to portability**

You have the right to receive a copy of the personal data that you have provided to us and to transmit those data to another organization and/or to request that we transmit such data directly to another organisation, provided that:

- we process such personal information on the basis of (a) your consent, or (b) for the performance of our contractual obligations, or (c) at your request, for the purposes of you (or natural or legal person that you represent, or act as agent of, or the entity you are a beneficial owner of) entering into a contractual relationship with us; and
- the relevant processing activities are carried out by automated means.

- **Right to lodge a complaint**

You can contact us for any personal data-related matters, as described by section 1 above.

If you are not satisfied or still concerned about any personal data-related matters, you are entitled to file a complaint with the Commissioner, as explained on the latter's website:

http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/page1i_gr/page1i_gr?opendocument

14. DATA SECURITY

We have put in place and implement security policies and procedures safeguard and to provide reasonable protection of your personal data against loss, misuse, unauthorized access, disclosure and alteration. Such measures include firewalls, digital encryption, access restriction and authorization controls. While we are dedicated to protecting your personal information, security cannot be absolutely guaranteed against threats. In the event that we become aware of a data breach which may cause you a disadvantage, we will notify you accordingly, without undue delay.

Moreover, you are responsible for protecting and maintaining protection of any identification, authentication and other security measures regarding our services and products (e.g. PIN numbers, passwords, security devices and account numbers), as described in the relevant contracts and/or terms and conditions.

15. CHANGES TO THIS PRIVACY NOTICE

We may modify this Privacy Notice from time to time in order to reflect our current practices and/or in accordance with any changes in the applicable legal framework. In such a case, we will update the revision

ASTROBANK'S PRIVACY NOTICE

Last update: June 2020

1. OVERVIEW

ASTROBANK PUBLIC COMPANY LIMITED (“we,” “our” “us” or “the Bank”) is committed to protecting and respecting your privacy and your rights, as regards the personal data collected and processed for the provision of our products and services.

We process your personal information in accordance with the applicable legal and regulatory framework, including the Law on the Protection of Natural Persons Against Personal Data Processing and the Free Movement of Such Data of 2018 (L. 125(I)/2018), as amended from time to time, and the General Data Protection Regulation 2016/679 (“GDPR”), which applies as of 25 May 2018.

This notice (referred to as the “Privacy Notice”) provides an overview of how and why the Bank processes personal data concerning natural persons, as well as of the rights of such persons, in the context of the offering and provision of banking and financial services and products. It is directed to natural persons who are current or prospective customers, or are authorised representatives/agents, security providers, related parties, or beneficial owners of legal entities or of natural persons which/who are current or prospective customers of the Bank

For the purposes of the present Privacy Notice, the terms “personal data”, “data” and “personal information” are used to refer to any information relating to you that identifies or may identify you, either directly or indirectly, such as your name, contact details, identification data (e.g. identity card/passport number) and authentication data (e.g. your signature). Moreover, the term “processing” is used herein to collectively refer to actions such as the collection, retention, use, disclosure, transfer, deletion or destruction of personal data.

Please read the following carefully in order to understand our policies and practices regarding your personal data and how we process them.

2. WHO WE ARE AND OUR CONTACT DETAILS

ASTROBANK PUBLIC COMPANY LIMITED is a licensed credit institution incorporated and established in accordance with the laws and regulations of the Republic of Cyprus, with registration no. 189515, and with registered address and/or headquarters at 1 Spyrou Kyprianou Avenue, 1065 Nicosia, P.O. Box 25700, 1393 Nicosia, telephone number 22575500.

Responsibility for the processing of your personal data lies with the Bank, which acts as the data controller, i.e. as the entity that, alone or jointly with others, determines the purposes and means of the processing of personal data.

You may contact our Data Protection Officer (DPO) for any matters arising out of and/or in connection with this Privacy Notice, including for the purposes of exercising of your rights, at:

ASTROBANK PUBLIC COMPANY LIMITED

Data Protection Officer 1,

Spyrou Kyprianou Avenue, 1065, Nicosia P.O Box: 25700, 1393, Nicosia,

Cyprus Tel. Number: 22575555

Email: contact@skash.com

Additionally, the exercise of your rights may be done via any Branch and/or Unit of the Bank, which will in turn liaise with the Data Protection Officer to respond/fulfill your request, or you may also fill in the Suggestions and Complaints Form, which is available on our website at www.astrobank.com, to that effect.

We will use reasonable endeavours, in line with the applicable legal framework, to meet, comply with and reply to your inquiries, requests and comments promptly and transparently.

3. WHAT KIND OF PERSONAL DATA WE PROCESS

The type of personal data we process, the particular processing activity we utilize, as well as the extent of such processing, depend on the services and products requested or agreed in each case.

We collect, use, consult or otherwise process personal data of:

- prospective and current individual customers;
 - persons connected to prospective and current customers, as applicable and/or appropriate (“connected persons”);
- Where such customers are individuals, connected persons may include introducers, authorised representatives/agents, attorneys/administrators/executors, family members or close associates of such customers that fall under the category of politically exposed persons (PEP), past and/or current employers.
- Where such customers are legal entities, connected persons may be, inter alia, introducers/associates, authorised representatives/agents, officials, partners, shareholders, investors, administrators, trustees,

authorised signatories, family members or close associates of such connected persons that fall under the category of politically exposed persons (PEP), ultimate beneficial owners (UBOs).

- security providers for credit facilities (e.g. guarantors); and
- non-customer counterparties, as required for the provision of our services (e.g. personal and payment information of payers or beneficiaries in payment transactions).

More analytically:

A. Where you are a prospective customer (including an authorised representative/agent of an individual or legal entity that is a prospective customer or the ultimate beneficial owner of a legal entity that is a prospective customer); or a prospective security provider such as a guarantor of credit facilities, we collect and further process data that may include the following:

- personal identification data (e.g. name, surname, passport/identity card number, social security number);
- personal details (e.g. gender, marital status, number of dependents, date of birth, place of birth, country of birth, citizenship, education level and other information contained in CVs, where applicable);
- authentication information (e.g. signature);
- contact details (e.g. residence address, mailing address, phone numbers, e-mail address);
- employment data/business activities information (e.g. profession, employer's name, job title, employment address and contact data);
- financial identification data (e.g. details of income and expenses, assets and liabilities (including debts and provision of securities), past and expected financial and economic activity);
- tax information, including the US Foreign Account Tax Compliance Act (FATCA) and Common Reporting Standard (CRS) details (e.g. country of tax residence, tax identification number);
- politically exposed persons (PEP) information (where you or a family member or close associate holds/held a prominent public function);
- purposes for and nature of the intended business relationship with us;
- In particular, regarding the "sKash" Mobile Wallet Application, including the issuance of the "sKash" cards, during the registration and/or subscription process of natural persons we may collect inter alia, identity card numbers and copies thereof, and/or mobile phone numbers and/or email addresses and/or

utility bills and/or other supporting documentation and/or all data as above.

Should we enter into a business/contractual relationship with you, we will retain and further process the aforementioned data, as explained in section 8 herein below.

B. In the course of the provision of services and products to you or the legal entity you are connected with, additional personal data may be collected, used and stored, primarily the following:

Account and payment services (including WinBank and the “sKash” Mobile Wallet Application, the issuance of the “sKash” card”; ad hoc or standing orders/direct debits; and credit/debit cards) Payment transaction data as well as any other data associated with the transaction. Such data includes account numbers and/or IBAN numbers and/or other unique identifiers; account(s) balance; nature and type of payment transaction (e.g. purchase of goods, purchase of services, money transfers); data transmitted with the payment order; data about when, where and with whom you transact with, including data of third-party beneficiaries and any other processing that may arise out of our contractual obligations.

Savings and deposits: Data regarding the particular accounts and transactions (e.g. accounts numbers and/or IBAN numbers and/or other unique identifiers, account(s) balance, data transmitted with each transfer/deposit of funds, cheques’ details), withholding tax data for special contribution for defence, financial and economic information (e.g. past and expected credit turnover, source of funds and assets, source of financial possession), and data of any third-party beneficiaries.

Banking facilities (e.g. loans and overdrafts): Information and supporting documentation (that may contain personal data of the borrower(s), and other persons connected/related to the borrower(s)) regarding:

- the purpose of banking facility (e.g. for immovable property financing, we request a description of the particular property, property valuation reports, construction and municipal permits, sale agreements, title deeds etc.);

- securities for the provision of banking facilities (e.g. where an insurance policy is assigned to us, data such the particular insurance company, the policy number, current surrender values etc., or for mortgages on immovable properties, we request a description of the particular property, property valuation reports, title deeds, Land Registry reports etc.);

- where the borrower is a consumer, employment status, such as employment history and nature/term of current position; and/or financial and economic status (e.g. details and supporting documentation of current income and expenses, assets and liabilities (including debts, securities and investments) and data we obtain from the Data Exchange Mechanism Artemis and public and/or regulatory and/or supervisory authorities (such as information we obtain from the relevant registries maintained by the Department of the Registrar of Companies and Official Receiver of the Republic of Cyprus; the Central Bank of Cyprus; and competent Land Registry Offices);

- where the borrower is a self-employed person or legal entity, business profile and financial activity (e.g. cash flows and balance sheets, business management information; data regarding assets and liabilities; as well as data obtained from the Data Exchange Mechanism Artemis and public and/or regulatory and/or supervisory authorities (such as information obtained from the relevant registries maintained by the Department of the Registrar of Companies and Official Receiver of the Republic of Cyprus; the Central Bank of Cyprus; and competent Land Registry Offices)business activity information, such as expected annual turnover;
- tax status (e.g. tax identification number, tax residency status, tax declarations and proof of tax return submissions);
- personal details (e.g. where the borrower is an individual, number of dependents);
- information regarding authorized representatives/agents (e.g. identification data; authentication data; contact details); or, in the case of legal entities, identification and residency/contact information of individuals connected with the particular legal entity (directors, secretaries, shareholders, signatories and/or other authorized persons/agents, beneficial owners).

Where personal guarantees by third parties are offered and/or provided, we request to collect and further process personal data of such third parties regarding their financial and economic background and circumstances, as provided directly from them or from other sources (e.g. from the Data Exchange Mechanism Artemis and the relevant registries maintained by public and/or regulatory and/or supervisory authorities (such the Department of the Registrar of Companies and Official Receiver of the Republic of Cyprus; the Central Bank of Cyprus; and the Land Registry).

Investment and interest rate and currency products and services We may collect and further process information regarding knowledge and experience with shares, funds, interest rate/currency products and financial investments (e.g. for MiFID services); investment behaviour/strategy (e.g. scope, frequency and risk policy); personal investment portfolio; income, assets and liabilities; foreseeable changes in financial circumstances.

Insurance Where you participate in our bancassurance scheme and/or assign an insurance to us for the purposes of the provision of credit facilities, we also collect information regarding existing/previous policies (e.g. policy numbers, products, premiums, properties and claims), as well as information regarding other persons that are insured under the same insurance scheme you participate in and/or assign to us.

C. Regardless of whether you are a prospective or current customer (including an authorised representative/agent of such an individual or legal entity or the ultimate beneficial owner of such a legal entity); or a prospective or current security provider such as a guarantor of credit facilities, we may process the following data: Website and electronic/digital services When you access and use our website and electronic/digital services (including the WinBank Service and the “sKash” Mobile Wallet

Application), we collect data such as the internet protocol (IP) address used to connect your device to the internet, your login data, type of device you use, network/browser data, a unique device identifier (e.g your mobile phone number and/or device ID), the times you access our website and/or electronic/digital services; and geolocation data.

Moreover, when you access and use our website or online services, we may place small data files on your device (“cookies”) in order to create a safer and more efficient online environment. You can view our cookies policy at our website at <https://www.astrobank.com>.

We collect automatic information, as above, in order to assess, customise and improve our services and products, aiming to deliver to you the highest experience and service standards.

Kindly note that, should users of our website choose to follow the special connections (links, hyperlinks, banners) to the websites of third parties, we are not responsible for the terms of personal data processing and protection followed by these parties.

Communications with us When you communicate with us (e.g. face-to-face visits to our Branches/Units and offices, or by letters, emails, faxes, phone or video calls, etc.), more data are created (e.g. method of communication, date and time, content and outcome of our communication). We record and retain in our records information generated by such communications and our relevant responses to you, for the following reasons:

- We record communications regarding customer service enquiries, requests and comments, to ensure that you receive optimum service levels;
- We record communications regarding applications for and provision of banking and financial transactions, in order to comply with our statutory obligations under the anti-money laundering and anti-terrorism law and relevant regulatory obligations of the Central Bank of Cyprus.

4. CHILDREN’S DATA

For the purposes of this Privacy Notice, “children” are defined as individuals under the age of eighteen (18). We understand and respect the importance of protecting the privacy of children. We may process the personal data of children only with the prior consent and/or authorization of their parents or legal guardians or as otherwise required or permitted by law.

5. SOURCES OF PERSONAL DATA

We lawfully obtain data, as described above, to the extent and where necessary in order to provide our services and products, from:

- Prospective and current customers, either directly from them or from their authorised representatives/agents or via other communication channels (e.g. our website, the WinBank Service and the “sKash” Mobile Wallet Application);
- Third parties, e.g. public and/or regulatory and/or supervisory authorities (such as Department of the Registrar of Companies and Official Receiver of the Republic of Cyprus the Central Bank of Cyprus; Cyprus Clearing House, Central Information Registry and competent Land Registry Offices); credit reference bureaus such as the Data Exchange Mechanism Artemis; other non-affiliated entities with which we have a contractual relationship for the purposes of the provision of our services and products (e.g. JCC Payment Systems Ltd and the Lufthansa Group for credit and debit cards services; cards and ATM services providers; private investigators (in Cyprus and/or abroad), insurance companies for different kinds of insurance contracts e.g. life insurance, bancassurance, motor vehicle, fire or household insurances; other payment services institutions such as Banks and other third parties you transact with (e.g. merchants); natural or legal persons acting as introducers/associates; and entities providing services and products for Know-Your-Customer (KYC) and due diligence purposes;
- Publicly available sources, e.g. registries maintained by public and/or regulatory and/or supervisory authorities (such as the Companies’ Registry, the Bankruptcies and Liquidations Registries and the Intellectual and Industrial Property Registries maintained by the Department of the Registrar of Companies and Official Receiver of the Republic of Cyprus; and competent Land Registry Offices); lists and databases maintained by other entities including international organisations (such as sanctions list and politically exposed persons (PEPs lists); the media, the press and the internet.

6. WHY WE PROCESS YOUR PERSONAL DATA AND ON WHAT LEGAL BASIS

We collect and further process your personal information in compliance with the applicable data protection legal framework, for the following reasons:

- For the performance of contractual obligations We collect and further process data which is necessary in order to perform our contractual obligations to you for the provision of our services and products, or to take steps, at your request, prior to entering into a contract with us. The purposes of the data processing are mainly dependent on the specific service and/or product, as described in the relevant contractual terms and conditions and can include needs assessments, advice, asset management and support, as well as executing transactions.
- For compliance with our legal obligations As a bank, we are subject to various legal obligations, namely statutory requirements (for example under the applicable payment services, money-laundering and terrorism financing, and tax laws); as well as requirements of supervising and/or regulatory authorities (including of the European Banking Supervisory Authority; the Central Bank of Cyprus; the Cyprus Police, including the Unit for Combating Money Laundering (MOKAS), and the Cyprus Securities and Exchange Commission). For these reasons, data collected, as described above, is used for anti-money laundering

and anti-fraud measures; credit controls; tax law controls and reporting obligations; assessment and management of risks of the Bank; for compliance with Court judgments and/or orders; e.t.c.

- For safeguarding legitimate interests

Where necessary, we collect and manage data above and beyond the performance of our contractual and/or legal obligations, where it is necessary for safeguarding legitimate interests pursued by us or by other parties, in compliance with the applicable personal data legal framework. Data and/or information are processed under this ground for reasons pertaining to business and/or commercial interests, taking into consideration the necessity of such action and your interests, fundamental rights and freedoms, as well as your reasonable expectations. Examples of such processing include the following:

- Consulting and exchanging data with credit reference agencies (e.g. the Data Exchange Mechanism Artemis) and other registries (e.g. the Companies' Registry, the Bankruptcies and Liquidations Registries and the Intellectual and Industrial Property Registries maintained by the Department of the Registrar of Companies and Official Receiver of the Republic of Cyprus; competent Land Registry Offices) to determine credit or default risks;
- Pursue and/or defense of claims in judicial and/or regulatory procedures;
- To collect and recover funds owned to the Bank;
- Consulting and exchanging data with external legal consultants/advisors for preparation for legal claims or on ad hoc basis for particular cases;
- Consulting or exchanging data with external accountants/auditors;
- Transfer, assignment and/or sale of any or all of our rights, titles or interests under any agreement between you and us;
- Reviewing and improving procedures for needs and demands assessments for the purpose of direct client discussions;
- Advertising or market and opinion research, provided that you have not objected to having your data processed for such purposes;
- Measures for further developing services and products and managing business;
- Ensuring the smooth operation of our network and IT operations and security;
- Measures and processes for IP rights protection and theft prevention;
- Crimes and fraud prevention and investigation;
- Measures and processes for security purposes and to prove availability (e.g. video surveillance (CCTVs) of our branches, offices and ATMs; admittance controls; and anti-trespassing measures); and

- Risk management and control.

• On the basis of your consent Insofar as you have granted us explicit and specific consent to the processing of your personal data for specific purposes other than the ones described above, the lawfulness of such processing is based on your consent. You have the right to revoke your consent at any time. Kindly be advised that any such revocation shall only have effect after it is submitted and filed by us, and that it will not affect the lawfulness of data processed prior to the revocation.

7. WHO RECEIVES YOUR PERSONAL DATA

Within the Bank, your personal information is only processed by the Departments/Units and/or persons that are authorised to process them, given that it is necessary to do so for the fulfillment of our contractual and legal obligations, or where you have given us your consent to process them, or where we believe that it necessary for our legitimate interests to do so, as explained by section 5 above. Kindly note that such persons are under banking secrecy and confidentiality obligations.

Your data may also be received by various service providers and suppliers with whom we have contractual agreements, pursuant to which they are bound by the confidentiality and data protection obligations according to the applicable data protection legal framework.

We may also disclose your personal information to other individuals and/or entities for any of the reasons described above, where and to the extent we are legally obligated or otherwise authorised to do so, or where you have given us your explicit consent.

We will not disclose and/or transfer your personal information to any third parties for their own direct marketing purposes, unless you have explicitly authorised us to do so.

Under the aforementioned conditions, recipients of your personal data may include:

- Public and/or regulatory and/or supervisory authorities and other public institutions, to the extent that we are under a statutory or regulatory obligation to do so, such as the Central Bank of Cyprus (e.g. data that we disclose and/or disclose to the Central Information Registry (CIR) maintained by the Central Bank of Cyprus that includes information about dishonoured cheques), the European Central Bank, the Cyprus Securities Exchange Commission, tax authorities, law enforcement authorities (e.g. police, including the Unit for Combating Money Laundering (MOKAS)); courts and tribunals;

- Other public authorities, where we are authorised by you to do so (e.g. the Ministry of Labour, Welfare and Social Insurance in respect of applications for benefits; the Ministry of Finance in respect of applications for exemptions);

- Other banking and financial institutions or similar institutions to which we transfer your data in order to perform our contractual obligations (e.g. corresponding banks; custodian banks; brokers; stock exchanges; share and stock investment and management companies; the European Investment Fund);
- Entities we work with for the provision of credit/debit card services (e.g. VISA, MASTERCARD, and JCC Payment Systems Ltd,) including the entities with which the Bank cooperates for the issuance of the “sKash” cards;
- The Cyprus Clearing House, for the exchange and clearance of cheques;
- Direct debit service providers;
- Entities offering technological expertise, solutions and support, such as the WinBank and Wallet service providers;
- Credit reference agencies such as the Data Exchange Mechanism Artemis;
- Valuers and surveyors;
- Insurance companies;
- External legal consultants, auditors and accountants; financial and business advisors;
- Marketing, market research and advertising companies;
- File storage, archiving, records management companies and cloud storage companies;
- Prospective and actual purchasers, assignees, transferees and chargees of our rights, titles, titles or interests under any agreement between you and us;
- Servicing Companies; and
- Your own legal representatives/agents.

8. DATA TRANSFERS TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS

Personal data will only be transferred to third countries, namely countries outside the European Economic Area where:

- it is necessary to do so in order to carry out your orders (e.g. payment or investment orders) In particular for international credit transfers and separately requested express credit transfers executed through SWIFT, personal data may be transferred to SWIFT’s operating centers in the US;
- where we are legally obliged to do so (e.g. the Bank is obliged to disclose information to the Cyprus Ministry of Finance which may in turn disclose it to the US authorities pursuant to the legal framework

implementing the US Foreign Account Tax Compliance Act (FATCA) and the OECD Common Reporting Standards (CRS Law); and

- or where you have given us your consent to do so.

Service providers and other entities that process your personal data on our behalf are under the obligation to comply with the same personal data protection standards and safeguards as we do, on the basis of either an adequacy decision issued by the European Commission pursuant to Article 45 of the GDPR (in particular, to Switzerland regarding services being rendered in respect of private banking customers) or contractual clauses between us and them or other appropriate safeguards pursuant to Article 46 of the GDPR.

9. RETENTION PERIOD

As a general rule, we only retain your personal data for as long as it strictly necessary for the purposes they were initially collected, in accordance with the applicable statutory and regulatory framework, including the relevant Directives issued by the Office of the Data Protection Commissioner of the Republic of Cyprus, which are available at the Commissioner's website:

http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/page3f_gr/page3f_gr?opendocument

1. Pursuant to the above Directives, we shall retain your personal data as follows:

- Personal data of current customers; persons connected to current customers (as above); and current security providers (e.g. guarantors): We shall retain personal data of such persons throughout our business/contractual relationship with you.
- Personal data of former customers; persons connected to former customers (as above); and former security providers (e.g. guarantors): We will delete and destroy or anonymize the personal data of such persons (10) ten years once the contractual relationship between such persons and us is terminated in its totality, and/or the accounts of such persons are closed and/or an individual transaction taking place outside the context of a business/contractual relationship is executed. The aforesaid will not apply and we retain such data for longer where there are any pending legal proceedings and/or investigations by public authorities/bodies and/or other disputes/differences in relation to such data.
- Personal data of prospective customers; persons connected to prospective customers (as above); and

prospective security providers (e.g. guarantors):

We will delete and destroy or anonymize the personal data of such persons six months after the relevant notification for the rejection of applications or the withdrawal of interest by the prospective customer.

2. Pursuant to the Prevention and Suppression of Money Laundering Activities Law of 2007, we will retain the following information and documentation for a period of five (5) years after the end of our business relationship with the customer or after the date of a single transaction:

(a) a copy of the documents and information required for compliance with customer due diligence requirements as defined in the aforementioned Law;

(b) the relevant evidence and records of transactions which are necessary for the identification of transactions;

(c) relevant correspondence documents with customers and other persons with whom a business relationship is maintained.

- At the end of the five year period referred to above, we shall delete the above specified personal data unless otherwise provided by other legislation.
- It is provided that we retain the above information/documentation for five (5) additional years where the further retaining of such information/documentation is reasonably justifiable for the purposes of preventing, identifying and investigating money laundering activities and the financing of terrorism, without prejudice to the provisions relating to criminal proceedings concerning evidence in connection with ongoing criminal investigations and proceedings.
- With regards to cases where, on the 25th of June 2015, legal proceedings were still pending relating to the prevention, detection, investigation or the initiation of criminal prosecution, and there are suspicions for money laundering activities and financing of terrorism and we have information/documentation relating to these pending proceedings, we may retain said information/documentation for a period up until 24 June 2020.
- Provided that, without prejudice to the provisions relating to criminal proceedings associated with money laundering activities and the financing of terrorism, which apply to evidence concerning criminal investigations and legal proceedings, we are obliged to retain the aforementioned information/documentation for a period up until 24 June 2025.

10. WHETHER WE CARRY OUT AUTOMATED DECISION MAKING (INCLUDING PROFILING)

We do not make decisions based solely on automated processing, including profiling.

However, we may process some of your data, including by automatic means, in order to evaluate certain of your personal aspects (profiling), in the following cases:

- We carry out data evaluations (including on payment transactions) in the context of our anti-money laundering, anti-terrorism financing and anti-fraud measures. Such assessments may also serve to protect your interests (e.g. where we become aware of any unusual activity of your accounts);
- We employ credit scoring to assess your creditworthiness, so that we can evaluate whether customers will meet their contractual payment obligations and to make fair and responsible decisions regarding the provision of our services and products, especially in the context of providing banking facilities, including loans and overdrafts.

11. MARKETING

We will only use your personal information for direct marketing purposes if:

- (a)** you have given us your explicit consent to do so, in which case you may revoke such consent at any time; or
- (b)** where we believe that such processing is necessary for pursuing our legitimate interests, in accordance with the applicable legal framework and having taken into account the considerations described in section 5 above, in which case you have the right to object to such processing, as described in section 12 below.

12. WHETHER YOU HAVE AN OBLIGATION TO PROVIDE US WITH YOUR PERSONAL DATA

We will ask you to provide us with certain personal information, as described in section 2 above, when you (or the natural or legal person that you represent, or act as agent of, or the entity you are a beneficial owner of) apply to enter into a business relationship with us, as well as during the course of our business relationship (including when you apply for more services and products). The provision of such personal information is a requirement for accepting and carrying out or for continuing a business relationship with you, as they are necessary for the performance of our contractual obligations and for us to comply with our legal obligations, as described by section 5 herein. In particular, we are under legal obligations, in accordance with the applicable anti-money-laundering and anti-terrorism financing legal framework, to collect and use at least the following information and relevant documentation regarding yourself and any natural or legal person that you represent, or act as agent of, or the entity you are a beneficial owner of:

- Identification data;
- Citizenship, country and city of birth;
- Residency information, including residential address.

Moreover, during the course of our business/contractual relationship, you must be disclosing any changes to the aforementioned data, without undue delay.

If you do not provide us with the necessary information and supporting documentation, we will not be able to enter into or continue a business/contractual relationship with you (or the natural or legal person that you represent, or act as agent of, or the entity you are a beneficial owner of).

13. YOUR PERSONAL DATA RIGHTS

We respect the rights you have under the personal data legal framework, namely the following:

- **Right of access** You have the right to obtain from us confirmation as to whether or not data concerning you are being processed and, if that is case, access to such data and further information in relation to them.
- **Right of rectification** You have the right to request and to obtain from us rectification of inaccurate personal information concerning you.
- **Right to erasure (“right to forget”)** You have the right to request us to erase your data, where one of the following applies:
 - Where such data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
 - Where we process such data on the basis of your consent and you refuse or withdraw such consent, provided that no other legal ground for processing applies;
 - Where we process your personal information in order to pursue our legitimate interests (e.g. for direct marketing purposes) and you object to such processing, provided that no overriding legitimate grounds for the processing apply;
 - Where such personal data have been unlawfully processed; and
 - Where such personal data have to be erased in compliance with a legal obligation of the Bank.
- **Right to restriction of processing** You have the right to obtain from us restriction of processing of data concerning you, where one of the following applies:

- Where you contest the accuracy of such data, for a period that allows us to verify the accuracy of such data;

- Where the processing is unlawful and you oppose the erasure of such data, requesting restriction of their use instead;

- Where we no longer need to process such data, but you require their retention for the establishment, exercise or defense of legal claims; and

- Where you have objected to us processing of your personal information on the grounds of our legitimate interests (e.g. for direct marketing purposes), until we verify whether the grounds on which we process such data override your rights and freedoms.

- **Right to object to processing** You have the right to object, at any time, on grounds relating to your particular situation, to us processing your personal data on the basis of our legitimate interests (e.g. for profiling, including for direct marketing purposes). Should you exercise this right, we will no longer process such data unless we are able to demonstrate compelling legitimate grounds for the processing.

- **Right to withdraw consent** Where we request your consent for processing your information, you have the right to refuse to give such consent. Moreover, where you have already given us such consent, you can revoke it at any time. Any such revocation shall only have effect after it is submitted and filed by us, and will not affect the lawfulness of data processed prior to such revocation.

- **Right to portability** You have the right to receive a copy of the personal data that you have provided to us and to transmit those data to another organization and/or to request that we transmit such data directly to another organisation, provided that:

- we process such personal information on the basis of:

(a) your consent, or

(b) for the performance of our contractual obligations, or

(c) at your request, for the purposes of you (or natural or legal person that you represent, or act as agent of, or the entity you are a beneficial owner of entering into a contractual relationship with us; and

- the relevant processing activities are carried out by automated means.

- **Right to lodge a complaint** You can contact us for any personal data-related matters, as described by section 1 above.

If you are not satisfied or still concerned about any personal data-related matters, you are entitled to file a complaint with the Commissioner, as explained on the latter's website:

http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/page1i_gr/page1i_gr?opendocument

14. DATA SECURITY

We have put in place and implement security policies and procedures safeguard and to provide reasonable protection of your personal data against loss, misuse, unauthorized access, disclosure and alteration. Such measures include firewalls, digital encryption, access restriction and authorization controls. While we are dedicated to protecting your personal information, security cannot be absolutely guaranteed against threats. In the event that we become aware of a data breach which may cause you a disadvantage, we will notify you accordingly, without undue delay.

Moreover, you are responsible for protecting and maintaining protection of any identification, authentication and other security measures regarding our services and products (e.g. PIN numbers, passwords, security devices and account numbers), as described in the relevant contracts and/or terms and conditions.

15. CHANGES TO THIS PRIVACY NOTICE

We may modify this Privacy Notice from time to time in order to reflect our current practices and/or in accordance with any changes in the applicable legal framework. In such a case, we will update the revision date at the top of the page and notify you accordingly, including by placing a notice to that effect on our website.