BRANKAS PRIVACY POLICY

(updated May 31, 2020)

The Brankas Privacy Policy represents our commitment to treat the information of customers, stockholders, directors, officers, employees, stakeholders and other interested parties with utmost care, transparency and confidentiality. Please note that this Privacy Policy only covers the information that Brankas collects, uses, and shares. It does not explain what third parties do with any information they may collect about you separately from Brankas. This policy also does not cover any websites, products, or services provided by others. We encourage you to review the privacy policies or notices of those third parties for information about their practices and we hope you will take some time to read this Privacy Policy.

With this policy, we present transparently that we gather, store and handle the data of persons fairly and in accordance with law. As part of our drive to serve you better, we need to obtain and process your information. This includes any offline or online data that makes a person identifiable such as names, addresses, usernames and passwords, digital footprints, photographs, social security numbers, financial data, etc.

Brankas collects or processes this information only with the full knowledge, cooperation and consent of interested parties. Once this information is available to us, the following rules apply.

Your data will be kept up-to-date, collected or processed fairly and for lawful purposes only. The information you give us will be processed within legal boundaries and will be protected against any unauthorized or illegal access by internal or external parties. You are free to exercise your rights under the law as a data subject and we fully respect the same.

Your data will not be distributed to any party other than the ones consented and agreed by you or the data's owner (exempting those compellable to be disclosed by law and legitimate requests from courts of competent jurisdiction and law enforcement authorities). Without such express consent from you or the data owner, it will not be communicated or transferred, informally or in any manner, to any other person, entity, organization or country.

In addition to our methods of handling the data, Brankas has direct obligations towards people to whom the data belong. Specifically, customers, stockholders, directors, officers, employees, stakeholders and other interested parties will know which of their data is collected. We will allow people to modify, erase, reduce or correct data contained in our databases in line with their rights under the law. We will have provisions in cases of lost or corrupted data.

To practice data protection, Brankas is committed to restrict and monitor access to sensitive data. Our officers and employees will be trained in online privacy and data security and will establish data protection practices (document shredding, secure locks, data encryption, access authorization, etc.). In addition to this, security measures will be built through a secure network to protect data from cyber attacks.

We may update or change this Privacy Policy from time to time. If we make any updates or changes, we will post the new policy on the Brankas website at https://brank.as and update the effective date at the top of this Policy. In case of any inconsistency with any other policy of

Brankas regarding data, information and system security measures, this Privacy Policy will govern. For any questions on this Privacy Policy, you may email support@brank.as.

Thank you for using Brankas!

CHAPTER I
DEFINITIONS

Data Subject refers to an individual whose Personal Data is collected or processed;

Personal Data collectively refers to Personal Information, Sensitive Personal Information, and Privileged Information;

Personal Information refers to any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

Processing refers to any operation or set of operations performed upon Personal Data including, but not limited to, collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data. Processing may be performed through automated means or manual processing, if the Personal Data are contained or are intended to be contained in a filing system;

Privileged Information refers to any and all forms of Personal Data, which, under pertinent laws, constitute privileged communication;

Security Incident is an event or occurrence that affects or tends to affect data protection, or may compromise the availability, integrity and confidentiality of Personal Data. It includes incidents that would result to a personal data breach, if not for safeguards that have been put in place;

Sensitive Personal Information refers to Personal Data:

1. About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;
2. About an individual's health, education, genetic or sexual life, or to any proceeding for any offense committed or alleged to have been committed by such individual, the disposal of such proceedings, or the sentence of any court in such proceedings;
3. Issued by government agencies peculiar to an individual which includes, but is not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and
4. Specifically established by an executive order or an act of Congress to be kept classified.

CHAPTER II
PERSONAL DATA COLLECTED, USED AND SHARED

Section 2.1 Information Brankas Collects - As explained in detail below, Brankas collects your Personal Data, which, where applicable, may include login such as username and password or a security token. In some cases, we also collect your phone number, email address, security

questions and answers, and one-time password (OTP) to help verify your identity before providing you our service. When providing this information, you give Brankas the authority to act on your behalf to access, disclose and share your Personal Data from the relevant bank or other entity (i.e. financial product and service providers) with authorized persons and entities for the purpose of providing and implementing our service for you to use. You may also provide us with other information, including your name, email address, and phone number, when you contact us or enter any such information on our website.

In general, we collect the following types of Personal Data from your financial product and service providers:

1. Account information, including financial institution name, account name, account type, account ownership, branch number, and account and routing number;
2. Information about an account balance, including current and available balance;
3. Information about credit accounts, including due dates, balances owed, payment amounts and dates, transaction history, credit limit, repayment status, and interest rate;
4. Information about loan accounts, including due dates, repayment status, balances, payment amounts and dates, interest rate, guarantor, loan type, payment plan, and terms;
5. Information about investment accounts, including transaction information, type of asset, identifying details about the asset, quantity, price, fees, and cost basis;
6. Information about the account owner(s), including name, email address, phone number, date of birth, and address information;
7. Information about account transactions, including amount, date, payee, type, quantity, price, location, involved securities, and a description of the transaction; and
8. Professional information, including information about your employer, in limited cases where you've connected your payroll accounts.

When you use your device to connect to our services, we receive identifiers and electronic network activity information about that device, including IP address, device type, country where the device is located, which features within our services you access, and other technical information about the device. We also use cookies or similar tracking technologies to collect usage statistics and to help us provide and improve our services.

Section 2.2 How Brankas Uses Your Personal Data – We use your Personal Data for a number of business and commercial purposes, including to operate, improve, and protect the services we provide, and to develop new services. More specifically, we use your Personal Data:

1. To provide, operate, and maintain our services;
2. To improve, modify, add to, and further develop our services;
3. To develop new services;
4. To protect you, our partners, us, and others from fraud, malicious activity, and other privacy and security-related concerns;
5. To provide customer support to you, including to help respond to your inquiries related to our service;

6. To investigate any misuse of our service, criminal activity, or other unauthorized access to our services; and
7. For other notified purposes with your consent.

Section 2.3 How Brankas Shares Your Personal Data – We share your Personal Data for a number of business purposes:

1. To enforce any contract with you;
2. With our data processors and other service providers, partners, or contractors in connection with the services they perform for us;
3. If, in good faith, disclosure is appropriate to comply with applicable law or legal process;
4. In connection with a change in ownership or control of all or a part of our business (e.g. merger, reorganization, bankruptcy, etc.);
5. Between and among Brankas affiliated entities such as parents, affiliates, subsidiaries and other companies under common control or ownership;
6. To reasonably protect the rights, privacy, safety, or property of Data Subjects such as you, plus us, our partners, and other; or
7. For any other notified purpose with your consent.

Section 2.4 Others – We may collect, use, and share your Personal Data in an aggregated or anonymized manner (without identifying you personally) for any purpose permitted under law. This includes creating or using aggregated or anonymized data based on the collected Personal Data to develop new services and to facilitate research.

We do not sell or rent Personal Data or any information that we collect.

CHAPTER III
ORGANIZATIONAL SECURITY MEASURES

Section 3.1 Data Privacy Principles - All Processing of Personal Data within Brankas will be conducted in compliance with the following data privacy principles:

1. Transparency – You will be made aware of the nature, purpose and extent of the Processing of your Personal Data by Brankas, including the risks and safeguards involved, the identity of persons and entities involved in Processing your Personal Data, your rights as a Data Subject, and how these rights can be exercised. Any information and communication relating to the Processing of Personal Data should be easy to access and understand, using clear and plain language.
2. Legitimate purpose - The Processing of Personal Data by Brankas will be compatible with a declared and specified purpose that is not contrary to law, morals, or public policy.
3. Proportionality - The Processing of Personal Data will be adequate, relevant, suitable, necessary, and not excessive in relation to the declared purpose. We process Personal Data only if the purpose could not reasonably be fulfilled by other means.

Section 3.2 Data Processing Records – We will maintain adequate records of Personal Data Processing activities at all times. A designated person within Brankas, with the cooperation and assistance of all the concerned business and service units involved in the Processing of

Personal Data, will be responsible for ensuring that these records are kept up-to-date. These records shall include, at the minimum:

1. Information about the purpose of the Processing of Personal Data, including any intended future Processing or data sharing;
2. A description of all categories of Data Subjects, Personal Data, and recipients of such Personal Data that will be involved in the Processing;
3. General information about the data flow within Brankas, from time of collection and retention, including the time limits for disposal or erasure of Personal Data;
4. A general description of the organizational, physical, and technical security measures in place within Brankas; and
5. The name and contact details of any staff accountable for ensuring compliance with the applicable laws and regulations for the protection of data privacy and security.

Brankas will, from time to time, conduct a Privacy Impact Assessment relative to all activities, projects and systems involving the Processing of Personal Data. We will review security policies, conduct vulnerability assessments and perform penetration testing, as applicable, within Brankas on a regular schedule to be prescribed by our IT Team.

Section 3.3 Personal Data Management – We will develop and implement measures to ensure that all Brankas staff who have access to Personal Data will strictly process such data in compliance with applicable laws and regulations. These measures may include drafting new or updated relevant policies of Brankas and conducting or sponsoring training programs to educate our stockholders, directors, officers, employees, agents and other interested parties on data privacy related concerns.

We will obtain your informed consent, evidenced by written, electronic or recorded means, in relation to:

1. The Processing of your Personal Data, for purposes of maintaining Brankas' records;
2. The sharing of your Personal Data with a third party, subject to the requirement that you will be provided with the following information before your Personal Data is shared:
    a. Identity of the third party that will be given access to the Personal Data;
    b. Purpose of the data sharing;
    c. Categories of Personal Data concerned;
    d. Intended recipients or categories of recipients of the Personal Data;
    e. Existence of your rights as Data Subject, including the right to access and correction, and the right to object;
    f. Other information that would sufficiently notify you of the nature and extent of data sharing and the manner of processing.
3. A continuing obligation of confidentiality is imposed on our stockholders, directors, officers, employees, agents or other interested parties in connection with the Personal Data that they may encounter during the period of which they are such with Brankas. This obligation will still apply after they cease to work with Brankas for whatever reason.

Section 3.4 Data Collection Procedures – We will document our Personal Data Processing procedures. We ensure that these procedures are updated and that your consent is properly obtained when required by law and evidenced by written, electronic or recorded means. These

procedures will also be regularly monitored, modified, and updated to ensure that your rights as a Data Subject are respected, and that we process your Personal Data according to law.

Section 3.5 Data Retention Schedule - Subject to applicable requirements of relevant laws and regulations, we will not retain Personal Data for a period longer than necessary or proportionate to the purposes for which such data was collected. Upon expiration of such period, all physical and electronic copies of the Personal Data will be destroyed and disposed of using a fully secured technology or process. We will develop measures to determine the applicable data retention schedules and procedures to allow for the withdrawal of your previously given consent, and safeguard the destruction and disposal of your Personal Data in accordance with law.

CHAPTER IV
PHYSICAL SECURITY MEASURES

Section 4.1 Storage type and location (e.g. filing cabinets, electronic storage system, personal data room/separate room or part of an existing room) - All Personal Data being processed by Brankas will be stored in a data room, where paper-based documents are kept in locked filing cabinets while digital/electronic files are stored and protected in computers or servers owned, operated or managed by Brankas. Files with Personal Data will not be kept in personal drawers or in unsecured locations unless with written approval by authorized officers of Brankas.

Section 4.2 Access procedure of and by Brankas personnel – Our IT team will develop and implement policies and procedures to monitor and limit access to activities in Brankas work stations where Personal Data is processed, including guidelines that specify the proper use of, and access to, electronic media. Other personnel may be granted access upon filing of an access request form with the approval of the IT department.

Section 4.3 Work Stations - The design and layout of the office spaces and work stations of Brankas, including the physical arrangement of any furniture and equipment, will be periodically evaluated and readjusted to provide privacy to anyone Processing Personal Data, taking into consideration the environment and accessibility to unauthorized persons. The responsibilities and schedules of individuals involved in the Processing of Personal Data will be clearly defined to ensure that only the individuals actually performing official duties will be in such rooms or work stations at any given time. Further, the work stations used in the Processing of Personal Data will be secured against natural disasters, power disturbances, external access and other similar threats.

Section 4.4 Persons involved in processing, and their duties and responsibilities - Persons involved in Processing will always maintain confidentiality and integrity of Personal Data. Copying or duplicating of forms and documents containing Personal Data will not be allowed unless these are inherent in the task and specifically required by assigned responsibilities.

Section 4.5 Modes of transfer of personal data within the organization or to third parties – For transfers of Personal Data through email, we use a secured email facility with encryption of the

data, and extending such to any and all attachments. Our IT team will ensure that all Brankas technology users are properly trained and oriented in the use of secured and authorized processing and file transfers involving Personal Data. Facsimile technology will not be used for transmitting documents containing Personal Data unless secured and authorized by our IT team.

CHAPTER V
TECHNICAL SECURITY MEASURES

Section 5.1 General Security - Our IT team will continuously develop and evaluate this Privacy Policy, considering the following:

1. Safeguards to protect Brankas computer network and systems against accidental, unlawful, or unauthorized usage, any interference which will affect data integrity or hinder the functioning or availability of the system, and unauthorized access;
2. Our ability to ensure and maintain the confidentiality, integrity, availability, and resilience of Brankas data processing systems and services;
3. Regular monitoring for security breaches, and a process for identifying and accessing reasonably foreseeable vulnerabilities in Brankas computer network and system, and taking preventive and corrective actions against security incidents that can lead to a Personal Data breach;
4. Our ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident;
5. A process for regularly testing and evaluating effectiveness of security measures; and
6. Encryption of Personal Data during storage and while in transit, authentication process, and other technical security measures that control and limit access thereto.

Section 5.2 Monitoring for security breaches – We install updated versions of anti-virus software on electronic computing devices that access the internet or wifi connections (desktops, notebooks, smart phones, ipads and similar devices). We also use an intrusion detection system to monitor security breaches and alert us of any attempt to interrupt the system.

Section 5.3 Security features of the software/s and application/s use - All software applications are reviewed and evaluated by our IT team before installing these in Brankas computers and devices to ensure the compatibility of security features with overall operations.

Section 5.4 Encryption, authentication process, and other measures - Brankas personnel with access to Personal Data will verify his or her identity using a secure encrypted link and multi-level authentication as adopted by the IT Team.

CHAPTER VI
RIGHTS OF THE DATA SUBJECT

As Data Subjects, you have the following rights in connection with the Processing of your Personal Data: right to be informed, right to object, right to access, right to rectification, right to erasure or blocking, and right to damages. Stockholders, directors, officers, employees and agents of Brankas are required to strictly respect and obey the rights of the Data Subjects.

Section 6.1 Right to be Informed – You have the right to be informed whether Personal Data pertaining to you will be, are being, or have been processed. You will be notified and furnished with information indicated below before the entry of your Personal Data into our records:

1. Description of the Personal Data to be entered into the system;
2. Purposes for which they are being or will be processed, including Processing for direct marketing, profiling or historical, statistical or scientific purpose;
3. Basis of Processing, when Processing is not based on your consent;
4. Scope and method of Personal Data Processing;
5. The recipients to whom the Personal Data are or may be disclosed or shared;
6. Methods utilized for automated access, if you allow the same, and the extent to which such access is authorized, including meaningful information about the logic involved, as well as the significance and the envisaged consequences of such Processing for you;
7. The period for which the Personal Data will be stored; and
8. The existence of your rights as Data Subject, including the right to access, correction, and to object to the Processing.

Section 6.2 Right to Object - You have the right to object to the Processing of your Personal Data, including Processing for direct marketing, automated Processing or profiling. You will also be notified and given an opportunity to withhold consent to the Processing in case of changes to the information supplied or declared to you in the preceding section.

When you object or withhold consent, we will no longer process your Personal Data, unless:

1. The Personal Data is collected or processed pursuant to a legal process or needed to comply with a legal obligation;
2. The Processing is for obvious purposes, including when it is necessary for the performance of or in relation to a contract to which you are a party, or when necessary or desirable in the context of an employer-employee relationship between you and us; or

Section 6.3 Right to Access – You have the right to reasonable access to, upon demand, the following, if such information is available with us:

1. Contents of your Personal Data that were processed;
2. Sources from which Personal Data were obtained;
3. Names and addresses of recipients of the Personal Data;
4. Manner by which your Personal Data were processed;
5. Reasons for the disclosure of the Personal Data to recipients;
6. Information on automated processes where the Personal Data will, or is likely to, be made as the sole basis for any decision that significantly affects or will affect you;
7. Date when Personal Data concerning you were last accessed and modified; and

Section 6.4 Right to Rectification – You have the right to dispute the inaccuracy or rectify the error in your Personal Data, and we will correct it immediately and accordingly, unless the request is vexatious or otherwise unreasonable. If the Personal Data has been corrected, we will ensure accessibility of both the new and the retracted Personal Data and the simultaneous receipt of the new and the retracted Personal Data by the intended recipients. In connection

with this, recipients or third parties who have previously received such processed Personal Data will be informed of its inaccuracy and its rectification, upon reasonable request.

Section 6.5 Right to Erasure or Blocking - You have the right to suspend, withdraw, or order the blocking, removal, or destruction of your Personal Data from our system. This right may be exercised upon discovery and substantial proof of any of the following:

1. The Personal Data is incomplete, outdated, false, or unlawfully obtained;
2. The Personal Data is being used for purpose not authorized by you;
3. The Personal Data is no longer necessary for the purpose for which they were collected;
4. You withdraw consent or object to the Processing, and there is no other legal ground or overriding legitimate interest for us to continue the Processing;
5. The Personal Data concerns private information that is prejudicial to you or other Data Subjects, unless justified by freedom of speech, expression or authorized by law;
6. The Processing is unlawful; or
7. You or other Data Subjects' rights have been violated.

We will notify third parties who have previously received such processed Personal Data that you have withdrawn consent or objected to the Processing thereof upon reasonable request.

Section 6.6 Transmissibility of Rights of Data Subjects – Your lawful heirs and assigns may invoke your rights as the Data Subject at any time after your death, or when you become incapacitated or incapable of exercising your rights.

Section 6.7 Data Portability – Where we process your Personal Data through electronic means and in a structured and commonly used format, you will have the right to obtain a copy of such data in an electronic or structured format that is commonly used and allows for your further use. The exercise of this right will primarily take into account your right to have control over your Personal Data being processed based on consent, for commercial purpose, or through automated means.

CHAPTER VII
DATA BREACHES AND SECURITY INCIDENTS

Section 7.1 Data Breach Notification - All our stockholders, directors, officers, employees and agents involved in the Processing of Personal Data are tasked with regularly monitoring for signs of a possible data breach or Security Incident. In the event that such signs are discovered, facts and circumstances will be reported to our authorized personnel within 24 hours from for verification as to whether or not a breach requiring notification to regulators has occurred. If indeed there is a breach of such nature, we will notify any relevant government authority and affected Data Subjects pursuant to requirements and procedures prescribed by law.

The notification will at least describe the nature of the breach, the Personal Data possibly involved, and measures taken by Brankas to address the breach. The notification will also include measures taken to reduce the harm of the breach and the name and contact details of Brankas authorized personnel. The form and procedure for notification will conform with law.

Section 7.2 Breach Reports - All Security Incidents and Personal Data breaches will be documented through written reports, including those not covered by notification requirements. In the case of Personal Data breaches, a report will include the facts surrounding an incident, the effects of such incident, and the remedial actions taken by Brankas. In other security incidents not involving Personal Data, a report containing aggregated data will be sufficient.

CHAPTER VIII
OUTSOURCING AND SUBCONTRACTING

Any Personal Data Processing conducted by an external agent or entity (third-party service provider) on our behalf should be evidenced by a valid written contract with us. The contract should expressly set out the subject matter and duration of the Processing, the nature and purpose of the Processing, the type of Personal Data and categories of Data Subjects, our obligations and rights, and the geographic location of the Processing under the contract.

The fact that we entered into such an arrangement does not give the said external agent or entity the authority to subcontract to another entity the whole or part of the subject matter of said arrangement, unless expressly stipulated in writing. The subcontracting agreement will also comply with the criteria prescribed by the preceding paragraph.

In addition, both foregoing contracts described will include express stipulations requiring the external agent or entity (including the subcontractor) to:

1. Process the Personal Data only upon our documented instructions, including transfers of Personal Data to another country or an international organization, unless such transfer is required by law;
2. Ensure that an obligation of confidentiality is imposed on persons and employees authorized by the external agent/entity and subcontractor to process the Personal Data;
3. Implement appropriate security measures;
4. Comply with applicable laws and regulations, in addition to the obligations provided in the contract, or other legal act with the external party;
5. Not engage another processor without our prior instruction, and any such arrangement will ensure that the same obligations for data protection under the contract or legal act are implemented, taking into account the nature of the Processing;
6. Assist us, by appropriate technical and organizational measures, and to the extent possible, fulfill the obligation to respond to requests by Data Subjects relative to the exercise of their rights;
7. Assist us in ensuring compliance with law, taking into account the nature of Processing and the information available to the external party;
8. At our discretion, delete or return all Personal Data to us after the end of the provision of services relating to the Processing, including the deletion of existing copies unless storage is authorized by law;
9. Make available to us all information necessary to demonstrate compliance with law, and allow for and contribute to audits, including inspections, conducted by us or another auditor mandated by us; and
10. Immediately inform us if, in its opinion, an instruction violates law.