DATA PROTECTION POLICY

Key Terms

1. **Personal Data** – any information related to an identified or identifiable natural person (hereinafter referred to as the "Data Subject") as defined in Article 4(1) of the GDPR.
2. **GDPR** – the General Data Protection Regulation (Regulation (EU) 2016/679), which governs the processing of personal data of natural persons, ensures free data movement, and replaces Directive 95/46/EC.
3. **Data Processing** – any operations performed on personal data as defined in Article 4(2) of the GDPR.
4. **Data Processor** – a person or organization that processes personal data on behalf of the Controller, in accordance with Article 4(8) of the GDPR.
5. **Controller** – a legal entity that determines the purposes and means of personal data processing. In the context of this Policy, the Controller is Benker UAB (hereinafter referred to as "Benker," "Company," "Operator," or "Controller"), which provides payment initiation and electronic wallet account management services.
6. **Data Subject (Client)** – a natural person who intends to or has already entered into a business relationship with the Controller, such as registering on the website, applying for a loan, entering into a service agreement, or engaging in other activities. Business relationships also include cases where the contract has ended, but data processing continues on a legal basis.
7. **Platform** – a software solution developed and maintained by the Company for providing its services via a website or application.

General Provisions

8. All personal data collected by the Company is processed in accordance with the Law on Legal Protection of Personal Data of the Republic of Lithuania, the GDPR, and other applicable legal regulations. Only authorized employees and representatives of Benker with a legal basis for data processing have access to Client data. They are required to maintain confidentiality even after the termination of their employment or contractual relationships.
9. The Company implements strict measures to protect personal data from unauthorized access, loss, modification, disclosure, or destruction. Modern technical and organizational methods are employed to ensure data security.
10. This Data Protection Policy regulates the collection, processing, storage, and use of personal data, discloses processing purposes, data sources, recipient categories, and other key aspects related to confidentiality. Terms used in the singular include the plural and vice versa unless the context dictates otherwise.
11. By using the Benker UAB website, mobile application, or any services provided by the Company, you confirm that you have read this Policy, understand its terms, and consent to the processing of your personal data. The Policy also becomes an integral part of the General Payment Services Agreement once you register in the system and start using the Company's services.
12. Benker reserves the right to amend the Data Protection Policy at any time. The updated document will be published on the website, and in case of significant changes, registered

users will be notified via email or an in-app message. The new version of the Policy takes effect upon publication.

13. If a service user is a legal entity, this Data Protection Policy applies to natural persons whose data is transferred to us by that legal entity. The user, in accordance with Article 14 of the GDPR, is responsible for properly informing the Data Subject (such as executives, beneficiaries, representatives, or other relevant individuals) about the transfer of their data to Benker.

Data Providers, Recipients, Processing Purposes, and Retention Periods

14. The primary purpose of collecting personal data is to provide Benker services to Clients. As a payment service provider, Benker is legally obligated to verify and confirm your identity before entering into financial service agreements. Additionally, Benker may request and assess supplementary information during service provision and retain it for the legally required duration. Clients must provide accurate and complete information.

    Purpose: Identity verification, payment service provision (account opening, money transfers, payment collection, and other financial services), anti-money laundering (AML) and counterterrorism financing (CTF) compliance, and fulfillment of other legal obligations of a payment service provider.

15. Personal data is processed for these purposes based on Article 6(1)(b), (c), and (f) of the GDPR, ensuring compliance with legal requirements related to:

- Identity verification of Clients;
- Establishing and fulfilling contractual agreements or taking necessary pre-contractual steps at the Client's request;
- Processing financial transactions and including legally required information in payment instructions;
- Compliance with "Know Your Customer" (KYC) regulations;
- Ongoing and periodic monitoring of Client activities;
- Risk assessments and Client data updates to ensure accuracy;
- Prevention, detection, investigation, and reporting of money laundering, terrorism financing, and fraudulent activities;
- Verifying if the Client is subject to financial sanctions or engaged in politically exposed activities;
- Ensuring risk management and organizational compliance.

16. The following categories of personal data may be processed for these purposes: full name, personal identification number, address, date of birth, facial image, live video recording, nationality, identity document details (including but not limited to a copy of the document), email address, phone number, bank account number, IP address, occupation, public office held, political exposure, presence on sanction lists, data required under anti-money laundering and counter-terrorism financing laws, Client's location, intended services, purpose of account use (personal/business), expected transaction amounts, income sources, beneficial ownership details, business correspondence, transaction verification documents, tax residency, connection to the EU/EEA, taxpayer identification number, devices used, SIM card country of issuance, and transaction history.
17. These personal data are collected and processed in compliance with the legal obligations of payment service providers, including the Payment Services Act, the Electronic Money and

Electronic Money Institutions Act, the Anti-Money Laundering and Counter-Terrorism Financing Act, and other relevant regulations necessary for account opening and payment service provision.

18. **Data Retention Period:** Personal data is retained for **ten (10) years** from the termination of the business relationship with the Client. In compliance with anti-money laundering and counter-terrorism financing laws, the data must be stored for at least **eight (8) years**. An additional **two (2) years** of retention is justified by the legitimate interest of considering the general statute of limitations for legal claims.
19. **Data Providers and Sources:** Data may be obtained from the Data Subject, financial institutions, government and private registers, identity verification databases, legal authority registers, debtor databases, sanction lists, law enforcement agencies, legal entities associated with the Client, business partners, social media accounts linked to the system, and other relevant sources. Some data may be processed using artificial intelligence.
20. **Data Recipient Groups:** Supervisory authorities, financial and payment institutions, courts, pre-trial investigative bodies, tax authorities, payment service partners, transaction recipients, payment system participants, debt collection agencies, attorneys, bailiffs, auditors, and other entities based on consent, legitimate interest, or contractual obligations with Benker UAB.

Purpose: dispute resolution and debt management.

21. Personal data is processed for the purpose of resolving disputes, managing debt and its recovery, submitting claims, demands, and lawsuits in accordance with points (c) and (f) of Article 6(1) of the GDPR.
22. The following personal data may be processed for these purposes: first name, last name, personal identification number, address, date of birth, identification document details, email address, phone number, bank account number, IP address, bank statements, and any other data related to the factual circumstances of the dispute or debt.
23. Data retention period: in the event of debt, data will be retained for 10 years from the creation of the debt (if the debt consists of several parts – from the date of creation of the last part of the debt). After the initiation of legal proceedings – until full performance of obligations by both parties. The data retention period is based on the statute of limitations set forth in the Civil Code of the Republic of Lithuania.
24. Data providers: the data subject, credit, financial, and payment institutions, electronic money institutions, state or non-governmental registers, operators of centralized debtor databases (e.g., in Lithuania, UAB "Creditinfo Lietuva"), and other parties.
25. Data recipients: operators of centralized debtor databases, credit, financial, and payment institutions, electronic money institutions, lawyers, bailiffs, courts, pre-trial investigation authorities, tax authorities, as well as other parties with a legal interest.
26. It is important to note that if you have debt to Benker and fail to fulfill your obligations within 30 days, Benker has the right to provide information about you, including your contact details and credit history (information about your financial and property obligations, as well as their fulfillment and outstanding debts) to debtor database operators (e.g., in Lithuania, to the credit bureau UAB "Creditinfo Lietuva") and debt recovery agencies. You can review your credit history by contacting the credit bureau directly.

Purpose: maintenance and administration of Client relationships, informing about available and new services, providing services, preventing disputes, and collecting evidence (e.g., recording telephone calls), business correspondence with the Client.

27. Personal data is processed for the following purposes (in accordance with points B, C, F of Article 6 (1) of the GDPR): maintaining business relationships with the Client; providing services to the Client; protecting the interests of the Client and/or Benker; preventing disputes and ensuring evidence of business communication (e.g., recording telephone calls, correspondence); verifying and maintaining the quality of services provided by Benker when necessary for the fulfillment of contractual obligations; taking actions upon the Client's request or to comply with legal obligations; informing the Client about the services provided by Benker, their prices, features, as well as changes to contracts with the Client or other significant changes; sending system and other messages related to the services provided.
28. For these purposes, the following personal data may be processed: first name, last name, address, date of birth, email address, phone number, IP address, Client's location data, bank account statements, phone call recordings, correspondence with the Client, and other data necessary to achieve the stated purposes.
29. Data retention period: 5 years after the end of the business relationship with the Client. This period may be extended by no more than 2 years upon a valid request from competent authorities. This data retention period is in accordance with regulations regarding anti-money laundering and the financing of terrorism.
30. Data providers: the data subject and telecommunications service providers.
31. Data recipients: supervisory authorities; operators of centralized debtor databases; lawyers; bailiffs; courts; pre-trial investigation authorities; organizations engaged in debt management and recovery; other parties with a legitimate interest, and other parties contracted with Benker.
32. The data subject acknowledges that they understand that such informational messages are necessary for the fulfillment of the provisions of the General Agreement on the provision of payment services and/or its annexes, and these messages are not considered direct marketing communications.

Purpose: creditworthiness assessment, credit risk management, and automated decision-making.

33. Personal data is processed for the purpose of assessing the creditworthiness of Clients, managing credit risks, and complying with regulatory requirements related to operational risks and capital adequacy, allowing Benker to offer or provide financing (in accordance with points b, c, f of Article 6(1) of the GDPR).
34. The following personal data may be processed for these purposes: first name, last name, address, date of birth, email address, phone number, bank account number, IP address, bank account statements, current balance on the account, financial obligations, credit and payment history, credit rating, as well as data on income, assets, past debts, education, employment, position, work experience, family, and other relevant information.
35. Data retention period: 1 year after the completion of the business relationship with the Client, provided all obligations between the parties have been fulfilled. In the case of a credit refusal, the relationship is considered complete from the moment the Client is notified of the refusal.

36. Data providers: the data subject; credit and other financial institutions or their branches; law enforcement agencies; government registers and institutions; operators of centralized debtor databases (e.g., in Lithuania – UAB "Creditinfo Lietuva" and others); individuals (when they provide data about spouses, children, and other family members, as well as data about coborrowers, guarantors, providers of collateral, and other related persons); legal entities (when the Client is their representative, employee, counterparty, owner, or founder); partners or other legal entities that Benker engages for service provision.
37. Data recipients: credit, financial, and payment institutions or electronic money institutions; creditworthiness assessment service providers; operators of centralized debtor databases.
38. In the process of concluding (or offering to conclude) a financing agreement and providing services, Benker may make decisions based on the automated processing of your personal data. In such cases, the system uses an established algorithm to assess your creditworthiness and decide whether services can be provided to you. A negative decision based on automated assessment may be reconsidered if the Client provides additional information. Benker takes all necessary measures to protect your rights and interests. You have the right to request human intervention, express your opinion, and challenge the decision made automatically. If you disagree with the automated decision, you may contact Benker to review it.

Purpose: Provision of services through third parties.

39. Personal data is processed for the purpose of providing a wide range of services to Benker Clients by involving third parties for the provision of certain services.
40. For these purposes, the following personal data may be processed: first name, last name, citizenship, personal code, address, contact information.
41. In accordance with point a of part 1 of Article 6 of the GDPR, the Client must be clearly informed about any data processing for the purpose of providing services through third parties, and such processing can only occur with the Client's consent.
42. Data retention period: 1 year.
43. Data providers: the data subject, Benker, third parties providing services.
44. Data recipients: third parties providing services, Benker, data subject.

Purpose: Protection of Benker’s and Clients’ interests (video surveillance in premises).

45. Personal data is processed for the purpose of ensuring the security of Benker and/or the Client, as well as protecting their life, health, and other rights (video surveillance and video recordings in Benker’s premises), in line with the legitimate interests related to the protection of property, employees, visitors, and assets of Benker.
46. For these purposes, the following personal data may be processed: video surveillance recordings in Benker’s premises.
47. Entry to Benker’s premises where video surveillance is conducted is notified through special signs.
48. Data retention period: 1 year.
49. Data providers: the data subject, located in Benker’s premises under video surveillance and captured by the video camera; video cameras.
50. Data recipients: courts, pre-trial investigation bodies, lawyers, responsible employees of Benker.

Purpose: Direct marketing.

51. Personal data is processed for the purpose of offering services related to Benker and obtaining the Client's opinion on the services provided (in accordance with point a of part 1 of Article 6 of the GDPR).
52. For these purposes, the following personal data may be processed: first name, last name, email address, phone number.
53. For these purposes, Benker, with the Client's consent, sends informational and marketing messages. To send such messages, a third party may be involved, ensuring compliance with the GDPR data protection requirements. The Client may withdraw consent at any time by clicking on the consent withdrawal link in the message or informing Benker via email at help@benker.io
54. Data retention period: until the business relationship with the Client ends or until the Client withdraws consent for data processing for marketing purposes.
55. Data providers: the data subject.
56. Data recipients: data may be transferred to search systems or social networks (with the ability to withdraw consent for data processing on their platforms), as well as to service providers sending informational messages.

Purpose: Statistical Analysis and Service Improvement.

57. Your personal data, collected and anonymized for the purposes mentioned above, in accordance with point f of part 1 of Article 6 of the GDPR, may be processed for statistical analysis and for enhancing organizational measures, technical tools, and IT infrastructure. This includes ensuring the compatibility of services with the devices used, creating new Benker services, and improving user satisfaction with existing services by testing and upgrading technical tools and IT infrastructure. Personal data processed for statistical analysis is handled in such a way that the identity of the data subject cannot be established during the analysis. The collection of your personal data for statistical purposes is based on legitimate interests related to the analysis, enhancement, and development of the activities carried out.
58. You have the right to object to the processing of your personal data for this purpose at any time and in any form by notifying Benker of your objection or refusal. However, Benker may continue processing the data for statistical purposes if it can demonstrate that the data is being processed for compelling legitimate reasons that override the interests, rights, and freedoms of the data subject, or for the establishment or fulfillment of legal requirements.

Purpose: Prevention of Abuse and Criminal Activity, and Proper Provision of Services.

59. The data collected for all of the above-mentioned purposes may be used to prevent unauthorized access to personal data and its unlawful use to ensure confidentiality and information security.
60. For processing personal data, Benker may engage data processors and/or, at its discretion, hire other entities to provide specific auxiliary services on behalf of Benker (e.g., data center services, hosting, cloud hosting, system administration and/or improvement, software creation, provision, support, enhancement, and development, customer service centers, marketing, communication, consulting, temporary staffing, etc.). In these cases, Benker takes all necessary measures to ensure that personal data is processed by these processors in accordance with Benker's instructions and applicable laws, and requires them to adopt appropriate measures to safeguard the personal data. Benker also guarantees that these third

parties are bound by confidentiality obligations and may use the collected information solely for the purposes related to the performance of their assigned functions.

61. The personal data collected for the purposes stated in this Policy will not be processed in ways that are incompatible with these legitimate purposes and legal requirements.
62. The aforementioned personal data is provided and obtained through software tools used by Benker or an authorized representative appointed by Benker, as well as through other means and third parties with whom Benker has entered into a contract for data processing in accordance with applicable legislation and legal acts.

Geography of Data Processing

63. In general, personal data is processed within the European Union/European Economic Area (EU/EEA). However, in certain cases, data may be transferred outside the EU/EEA and processed there.
64. Personal data may be transferred outside the EU/EEA and processed there if it is necessary for the conclusion and performance of a contract (for example, when your payment transfer is made to a third country, or when a third-country partner (correspondent) is involved in the payment process, or when a Client is conducting business on an internet platform that requires payment service providers to comply with specific requirements concerning customer information). Data transfer may also occur if required by legal acts or if the Client has given their consent. In all such cases, Benker will take necessary technical and organizational measures to protect the data in accordance with the GDPR.

Profiling

65. The profiling carried out by Benker is related to the automated processing of personal data for purposes established by legal regulations, particularly for risk management and the continuous, periodic monitoring of transactions to prevent fraud. This profiling is based on Benker's legal obligations.
66. For direct marketing and statistical analysis purposes, profiling may be carried out using tools like Matomo, Google, Meta, OpenAI, or other similar platforms.

Processing of Personal Data of Minors

67. To access Benker's payment services, minors under the age of 14 are required to obtain written consent from their legal representative (parent or guardian) for the processing of their personal data.

Cookie Policy

68. Benker's website may use cookies. Cookies are small pieces of data sent to a user's internet browser and stored on their device. Cookies are placed on a user's computer upon their first visit to the site.
69. Typically, Benker only uses essential cookies, which are necessary for the identification and functionality of the website and for simplifying user access to the site and its content. With the user's consent, Benker may use additional cookies. Below is a brief description of each type of cookie used:

Essential Cookies: These cookies are necessary for the proper functioning of various features on the Benker website. They are required for the website to operate and cannot be disabled. These cookies are stored on your computer, mobile phone, or tablet as long as you are on the website and have a limited lifespan. They are linked to your actions on the site (e.g., changing personal settings, filling out forms).
Statistical Cookies: These cookies collect anonymous data and reports to help us understand how users engage with the site. A unique ID number is registered to gather statistical information about how users use the site.
Analytical Cookies: These cookies track the number of website users and their flow. Analytical cookies allow us to determine the most visited pages and how users interact with them, helping improve service quality. If you do not agree to the use of these cookies, your visit to the site will not be counted in our statistics.
Marketing Cookies: These cookies are used to provide you with relevant information about our services, optimize content presentation based on your online activity, and offer you more opportunities on our website. These cookies may be used to display our advertisements on third-party sites. In this case, we will also receive your activity history from the websites of our official partners where our ads are displayed. If you do not agree to these cookies, you will only see general (non-personalized) ads on Benker's websites.

70. Most browsers accept cookies by default, but users can change their browser settings to reject cookies. Please note that blocking essential cookies may negatively impact the website's functionality, and certain features may not work. When a user first visits Benker's site, a popup window appears displaying a list of specific cookies, allowing the user to select which cookies they are willing to accept. By consenting to not only essential cookies but also other cookies, the user can change their selection and withdraw consent at any time through the cookie settings link at the bottom of the website.

Your Rights to Access, Correct, Delete, or Restrict the Processing of Your Personal Data

71. You have the following rights:
    71.1. **Right to Access Data**: You have the right to request information from Benker regarding the processing of your personal data. If your data is being processed, you can request access to the personal data that Benker holds, including the sources of the data, the purpose of the processing, and the recipients or potential recipients of your data. You are also entitled to receive a copy of your personal data, subject to legal requirements. Upon receiving your written request, Benker will provide the requested personal data within the statutory time frame, or provide reasons for refusing the request. You may request your data free of charge once per calendar year; however, in other cases, a fee may apply, which will not exceed the cost of providing the data. For more information about how to access your data and the procedure for doing so.
    71.2. **Right to Rectify Data**: If the personal data held by Benker is inaccurate, incomplete, or incorrect, you have the right to request that Benker correct or supplement your personal data by submitting a written request.
    71.3. **Right to be Forgotten**: You have the right to request that your data be deleted (i.e., the processing of your data be stopped) if your personal data is being processed based on consent, and you withdraw that consent, or if the data is no longer necessary for the purpose for which it was collected, or if it was processed unlawfully, or if there is a legal obligation to delete the data. To express your disagreement with the processing of your data,

you must submit a written request to Benker, either in person, by mail, or electronically. If your objection is legally justified, Benker will stop processing your data after reviewing your request, except in cases required by law. Please note that your right to request the immediate deletion of your data may be limited due to Benker's legal obligations as a payment service provider, which include storing data related to customer identification, payment transactions, contracts, etc., for the duration specified by law.

71.4. **Right to Restrict Data Processing**: You may request the restriction of your data processing if:

- You question the accuracy of the data, for a period allowing the controller to verify the accuracy of the data;
- The data processing is unlawful, and you oppose the deletion of the data, requesting instead that processing be restricted;
- The data is no longer needed by the controller for processing, but it is required by you for the establishment, exercise, or defense of legal claims.

The controller will notify you before lifting any restriction on the processing of your data.

71.5. **Right to Object**: You have the right to object to the processing of your personal data for direct marketing purposes.

71.6. **Right to Lodge a Complaint**: You have the right to file a complaint with the supervisory authority regarding the processing of your personal data if you believe that your legal rights and interests are being violated under applicable law.

71.7. **Right to Contact the Controller**: You may contact the controller and/or the designated data protection officer to inquire about your rights.

71.8. **Other Legal Rights**: Any additional rights provided under applicable law.

72. To submit a request regarding data access, correction, or objection to data processing, you can send an email to help@benker.io The request should clearly include your name, surname, and be signed with a qualified electronic signature.

Third-Party Websites

73. Benker is not responsible for ensuring the privacy of the Client on third-party websites, even if the Client accesses these sites through links provided on this website. Benker recommends reviewing the privacy policies of each third-party site that is not owned by Benker.

Use of Logos

74. A Client utilizing Benker's services for commercial or professional purposes agrees that their name and/or logo may be used by Benker for direct marketing purposes (for example, Benker may indicate that this Client uses Benker's services).

Information Security

75. Benker's objective is to maintain the highest possible level of security for all information received from the Client or from public databases. To protect this information from unauthorized access, use, copying, accidental or unlawful deletion, alteration, or disclosure,

as well as from any other unlawful processing, Benker implements appropriate legal, administrative, technical, and physical security measures.

Final Provisions

76. Additional information about how Benker processes personal data may be provided in contracts, other documents, on the website, in the mobile app, or through remote customer service channels (such as by phone, email, etc.).

77. Benker reserves the right to unilaterally change and/or supplement this Data Protection Policy. Any changes to the Data Protection Policy will be communicated on the Company's website. In certain cases, the Company may also inform individuals of these changes via mail, email, mobile app, or other means.

78. This Data Protection Policy is governed by the laws of the Republic of Lithuania. Any disputes arising from the provisions of this Data Protection Policy will be resolved through negotiations, and if unsuccessful, in the courts of the Republic of Lithuania.

- – UAB "Creditinfo Lietuva" (Company code: 111689163, address: Konstitucijos pr. 18B, LT-09308 Vilnius, Lithuania, www.creditinfo.lt; based on legitimate interests and purposes related to creditworthiness assessment and debt management, processes and provides your information to third parties such as financial institutions, telecommunications and insurance companies, electricity and utility suppliers, trading companies, etc.; credit history data is typically processed for up to 10 years after obligations are fulfilled).