1. A. Objective This Data Privacy and Protection Policy ("Policy") aims to provide guidance on the guidelines applicable to the privacy and protection of personal data of clients, employees, third parties, service providers, suppliers, and partners to which Beephish Treinamentos e Capacitação LTDA. has access due to its activities, establishing rules for the collection, use, storage, sharing, and elimination of personal data, in accordance with laws, regulations, and good practices adopted in the market.

B. Scope All employees, including outsourced personnel, interns, and young apprentices ("employees") of Beephish Treinamentos e Capacitação LTDA., hereinafter jointly referred to as the "Company."

C. Guidelines

1. Initial Provisions

1.1. This Policy aims to demonstrate the Company's commitment to:

1.1.1. Safeguarding the privacy and protection of personal data collected from clients, employees, third parties, service providers, suppliers, and partners, in the performance of its activities.

1.1.2. Adopting guidelines that ensure comprehensive compliance with laws, regulations, and good practices related to personal data protection.

1.1.3. Promoting transparency, with personal data subjects and other stakeholders, regarding how the Company processes personal data.

1.1.4. Adopting effective and preventive measures for the protection of personal data against the risk of security incidents involving such data.

2. Information Subject to the Policy

2.1. The following are subject to this Policy:

2.1.1. All personal data provided or collected in the context of the Company's provision of services to its clients for the acceptance of electronic payment methods, including the capture, transmission, processing of information, and settlement of transactions, as well as the offering of other related services and products.

2.1.2. All personal data of employees, third parties, service providers, suppliers, and partners provided or collected in the context of a contractual, legal, or regulatory obligation, or any other personal data.

3. Personal Data Collected

3.1. The personal data collected may vary according to the relationship maintained with the Company and are classified into the following groups:

3.1.1. **Personal Data provided by the data subject:** These are data entered or submitted by the data subject or their legal representative, resulting from contact, registration, or contract with the Company, which may include, but are not limited to, the following data: full name, CPF (Brazilian individual taxpayer ID), date of birth, marital status, nationality, place of birth, parentage, beneficiaries, profession, data of the company they are a partner, owner, legal representative, or agent of, full address, bank details, email address, telephone number, and biometric data.

3.1.2. **Personal Data collected from the use of services:** These are data related to the use of electronic payment methods, captured by the Company and transmitted and/or shared with third parties within the necessary context and limits for the processing and settlement of electronic payment transactions or for the transmission of non-financial information, which is the object of the service provided by the Company.

3.1.3. **Personal Data collected from the use of websites and applications:** These are data related to access and navigation on the Company's website, pages, and applications, containing information about device identification (Date, Time, and IP). The data subject's geolocation may also be collected for fraud prevention, security, and credit protection.

3.1.4. **Personal Data collected on social media and networks:** These are data collected from interactions made by personal data subjects through the Company's social media and/or networks.

3.1.5. **Financial Personal Data:** These are data concerning the data subject's financial or credit situation, such as income, assets, negative credit status, positive credit registration, and data from the Central Bank's Credit Information System, in accordance with applicable and current legislation.

3.1.6. **Personal Data of minors under 18:** The Company will only collect and process personal data of minors under 18 years of age in accordance with Article 14 of Law 13.709/2018 and relevant legislation.

4. Form and Purpose of Collection

4.1. Personal data will be collected by ethical and legal means and stored in a secure and controlled environment, for the period required by current law or regulation. The Company undertakes to take all appropriate measures to maintain absolute secrecy and strict confidentiality of all personal data to which it has access or which it may come to know or become aware of regarding transactions, cardholders, card data, and payment methods of its clients, as well as individuals directly related to clients, to which it may have access due to the provision of services, employment relationship, contractual

relationship, or partnership, being prohibited from assigning and/or allowing third-party access to such information, except for the hypotheses described in this Policy or provided by law.

4.2. The Company uses all collected information, via registration form completion, entered by the user on its website or application, collected directly from clients, or automatically, for the following purposes: (i) service provision; (ii) expanding commercial offers and promoting products and services of interest to clients, employees, and partners; (iii) personalizing and improving offered products and services; and (iv) preventing fraud and financial losses, among other cases that may deviate from the conventional.

4.3. The Company, in some cases, may also process personal data when necessary for compliance with a legal or regulatory obligation or the regular exercise of rights in judicial, administrative, or arbitration proceedings.

4.4. The Company may also process personal data based on its legitimate interest, always within the data subject's expectation, and never to the detriment of the data subject's fundamental interests, rights, and freedoms.

4.5. The Company may process sensitive personal data for fraud prevention or for conducting research, and in this case, anonymization will be guaranteed whenever possible. Furthermore, it may process this data with the data subject's consent.

4.6. The collected information may also be used for advertising purposes, such as sending communications and news that are of interest to current, potential clients, and third parties. In these cases, the objective will be to better serve the target audience by offering products suited to their needs and profile.

4.7. The collected information may also be used for profile analysis, identification, management, and treatment of potential risks in the offering and contracting of products and/or services and in other risk management activities, also aiming at the security of clients and users.

5. Relationship with Third Parties

5.1. Third-party access to information collected by the Company occurs exclusively for the purposes informed in this Policy and within the necessary limits for the performance of activities related to its business operations, and may include, but is not limited to:

5.1.1. Service providers that perform commercial operations and/or information processing for the Company and/or activities related to the Company's activities and that have been subcontracted by it;

5.1.2. Marketing partners;

5.1.3. Independent auditors;

5.1.4. Collection agencies, credit protection services, and similar; and

5.1.5. Competent regulatory bodies.

5.2. The use of information collected by the Company, in any of the hypotheses provided in item 5.1 above, is made exclusively for the purposes informed in this Policy, in the performance of the Company's activities, or in offering the client specific content based on the secure and aggregated use of information about its area of operation, whenever possible in encrypted form and, when applicable, anonymized.

5.3. The Company may share aggregated information with its partners, provided that such information is not personally identifiable. For example, it may share information to demonstrate trends in the general use of its services and/or market trends and indices.

5.4. Whenever it becomes necessary to use the collected information for purposes other than those defined in this Policy or those expressly authorized by the data subject, the Company will directly inform the data subject about this new purpose and, when necessary, will collect a new authorization.

5.5. Additionally, it is possible that some of the transfers indicated above occur outside Brazilian territory. Destinations may include: the United States and the European Union, in which case the Company undertakes to do so only to countries that provide an adequate level of protection for personal data, considered as adequate to what is provided in the applicable legislation; or through the adoption of guarantees and safeguards such as specific clauses, standard clauses, global corporate rules, among others; as well as through prior collection of consent or observance of other hypotheses authorized by law.

5.6. The Company requires all third parties to maintain the confidentiality of the information shared with them or to which they have access by virtue of their activity, as well as to use such information exclusively for the expressly permitted purposes. However, the Company will not be responsible for the improper use of such information, whether by third parties or their employees, due to non-compliance with this Policy and the contractual obligations assumed through specific instruments.

5.7. The Company also requires all third parties contracted by it to comply with all obligations contained in this Policy, and such third parties will be subject to the same obligations as the Company, for the data processing activities performed, before the data subjects.

6. Information Security

6.1. Aiming at the security of collected and/or provided information, the Company has physical, logical, technical, and administrative security processes compatible with the

sensitivity of the collected information, whose efficiency is periodically evaluated through an independent audit process.

6.2. The Company implements new procedures and continuous technological improvements to protect all collected and/or transmitted personal data.

6.3. The Company uses the latest methods and equipment available on the market to encrypt and anonymize personal data when necessary. Encryption allows us to protect data before it is transmitted over the internet. Encryption techniques make this information unreadable and prevent others from viewing it before it reaches our technological environment.

6.4. The Company only authorizes specific individuals to access the location where personal information is stored, provided that this access is essential, necessary, and indispensable for the intended activity.

6.5. The Company guarantees that employees, third parties, or partners who process personal data must commit to maintaining absolute secrecy of the accessed information, as well as adopting the best practices for handling this information, as determined in internal policies and norms.

6.6. In addition to technical efforts, the Company also adopts institutional measures aimed at protecting personal data, maintaining a privacy governance program applied to its activities and structure.

6.7. Access to collected information is restricted to authorized employees and individuals. Those who improperly use this information will be subject to applicable administrative, disciplinary, and legal sanctions.

6.8. Notwithstanding the security measures adopted, the Company is not responsible for damages resulting from violations and/or security incidents due to the occurrence of any fact or situation not attributable to it.

6.9. In the processing of collected information, the Company uses structured systems to meet security and transparency requirements, good practice standards, governance, and the general principles established in Law No. 13.709/2018, the General Data Protection Law ("LGPD").

7. Data Subject Rights

7.1. In compliance with applicable regulations regarding the processing of personal data, the Company respects and guarantees the data subject the possibility to submit requests based on the following rights:

- Confirmation of the existence of processing;

- Access to personal data;
- Correction of incomplete, inaccurate, or outdated data;
- Anonymization, blocking, or elimination of unnecessary, excessive, or unlawfully processed data;
- Portability of data to another service or product provider, upon express request by the user;
- Elimination of data processed with the user's consent;
- Obtaining information about public or private entities with which the Company shares its data;

- Information about the possibility of the user not providing consent, as well as being informed about the consequences in case of refusal;
- Revocation of consent; and
- Review of decisions made solely based on automated processing of personal data.

7.2. Some of the rights listed above may be exercised directly by the data subject or their legal representative, through the management of registration information available in the logged-in area of the website, while another part will depend on sending a request to the Privacy and Data Protection area, for evaluation and adoption of necessary measures. The channel for receiving requests of this nature is the email: contato@beephish.com.

7.3. For more information, questions, or requests regarding data processing, you can consult the External Privacy Notice at: beephish.com/privacidade, or contact the Data Protection Officer ("DPO") via email: contato@beephish.com.

7.4. Any request for exclusion of essential information for managing registration with the Company will imply the termination of its contractual relationship, with the consequent cancellation of the services then provided, and the data may be retained to comply with legal or regulatory determination.

8. Cooperation with Regulatory Authorities

8.1. In cases where the disclosure of personal data is necessary, whether due to compliance with law, judicial determination, or a competent regulatory body overseeing the activities developed by the Company and/or third parties, such information shall be disclosed only under the strict terms and within the limits required for its disclosure, and the data subjects of the disclosed information, whenever possible, will be notified of such disclosure, so that they can take appropriate protective or remedial measures.

9. Changes

9.1. This Policy may be modified at any time, according to the purpose or need for adaptation and compliance with legal provisions, regulations, or whenever the Company deems necessary. Changes will be disclosed through the website https://beephish.com/. The continued use of services or provision of services to the Company, as the case may

be, after the disclosure of changes will be considered acceptance by the client and third parties of the new terms and conditions.

D. Consequence Management Non-compliance with the guidelines of this Policy entails the application of accountability measures to the agents who fail to comply, according to the respective severity of the non-compliance and in accordance with internal regulations, being applicable to all persons described in the "Scope" item of this Policy.

E. Responsibilities

- **Administrators, Employees, and Service Providers:** Observe and ensure compliance with this Policy and, when necessary, contact the Data Protection Officer for consultation on situations involving conflict with this Policy or upon the occurrence of situations described therein. Act ethically and responsibly when becoming aware of any security incident involving personal data, promptly informing the responsible areas. Understand the role of information security and privacy in their daily activities and participate in awareness and education programs, as well as contribute to the implementation, maintenance, and continuous improvement of Security.
- **Suppliers:** Observe and ensure compliance with the best practices of information security and privacy, contractually required during the relationship with the Company. Act ethically and responsibly when becoming aware of any security incident involving personal data that may entail significant risks to data subjects, promptly informing the responsible areas.

F. Complementary Documentation

- Article 5 of the Federal Constitution of 1988;
- Law No. 12.965, of April 23, 2014 – Brazilian Civil Rights Framework for the Internet;
- Law No. 13.709, of August 14, 2018 - General Data Protection Law ("LGPD");
- ABNT NBR ISO 27001 - Information Security;
- ABNT NBR ISO 27701 – Information Privacy;

G. General Provisions This Policy comes into effect on the date of its publication and revokes any contrary documents.

São Paulo, August 01, 2024 Beephish Treinamentos e Capacitação LTDA.