GENERAL TERMS AND CONDITIONS FOR THE PROCESSING OF PERSONAL DATA AND INFORMATION SECURITY

1. If personal data is processed, the Parties agree to comply with specific data protection laws, such as the Federal Constitution, the Consumer Protection Code, the Civil Code, the Brazilian Framework for the Internet, and its implementing decree (Decree No. 8,771/2016), particularly the General Personal Data Protection Law No. 13,709/2018 ("LGPD").

1.1. This document should be read in conjunction with Niterra's Privacy Policy, available at: https://institucional.ngkntk.com.br/politica-de-privacidade. In the event of any conflict between the general provisions of the Privacy Policy and the specific obligations agreed upon herein, the terms set forth in these General Terms and Conditions shall prevail, as they constitute a specific agreement between the Parties.

2. To share personal data with Niterra, for the purposes of these General Terms and Conditions, and provided that such sharing is agreed upon by the Parties, the Business Partner must first obtain specific authorization from the data subject or ensure that it has a legal basis for such sharing, in accordance with the Law.

2.1. The Business Partner agrees to notify Niterra immediately if any authorization is revoked, or if the legal basis for such authorization ceases to be valid, as well as whenever any data that has been shared needs to be corrected or is no longer to be processed by Niterra on behalf of the Business Partner.

3. The Controlling Party is responsible for maintaining a channel of communication with data subjects and informing them of their rights regarding their personal data, as well as for respecting those rights, including the rights of access, erasure, restriction, portability, and deletion of data, as provided by law.

4. If the Business Partner acts as an operator of data controlled by Niterra in the performance of the contracted services, it must process Personal Data exclusively in accordance with Niterra's (the Controller) instructions.

4.1. The Business Partner shall not comply with any instructions received directly from the data subject, except in cases where authorized by the Controller and/or by applicable law.

4.2. If the Business Partner receives any direct request from the data subject regarding data controlled by Niterra, it must notify Niterra of this fact.

4.3. Any processing of Personal Data controlled by Niterra, if any, will be carried out by the Business Partner only during the relationship established between the Parties; Niterra may request, by means of an express notification to that effect, that the Business Partner cease the processing of personal data belonging to one or more data subjects, in which case the Business Partner must cease processing activities with respect to such data and may only continue to store it to comply with an applicable legal or regulatory obligation. In addition, the Business Partner, acting as a Data Processor under Niterra's control, will provide reasonable cooperation and assistance as requested by Niterra so that Niterra can respond to requests from data subjects.

4.4. The Business Partner agrees to return all Personal Data controlled by Niterra, including that related to the technology, at no cost to Niterra. This data must be returned

in a usable format, in accordance with the guidelines provided by Niterra, so as to enable the complete recovery of the information. The return must meet the following requirements:

a) The data must be returned in a usable, commonly used, and machine-readable format, ensuring that it is complete, accurate, and up-to-date at the time of return;
b) The Business Partner must return the data within fifteen (15) calendar days of Niterra's express request or upon termination of the relationship between the parties, whichever occurs first.
c) Data must be transferred securely, using encryption protocols and other appropriate security measures to protect the confidentiality and integrity of the data during transfer;
d) The Business Partner must provide Niterra with written confirmation that all personal data has been returned as requested and that it does not retain any copies of such data, except those necessary to comply with legal or regulatory obligations;
e) Any personal data that, due to a legal or regulatory obligation, cannot be returned or must be retained, must be properly identified and kept under appropriate security measures until its destruction, which must occur as soon as the legal or regulatory obligation expires. The destruction must be documented, and a destruction report must be provided to Niterra;
f) The Business Partner must cooperate with Niterra after the data has been returned to resolve any issues related to the retrieval or integrity of the returned data and provide technical assistance as needed;
g) Niterra reserves the right to conduct audits, either directly or through third parties it designates, to verify the Business Partner's compliance with the data protection and information security requirements set forth in this clause and in applicable law, without prejudice to the right to conduct general audits established in Clause 18 of these General Terms and Conditions.

5. The Business Partner ensures that its staff and/or employees are legally obligated to protect and maintain the secrecy and confidentiality of any personal data to which they have access or that they process in the course of their work.

6. If the Business Partner needs to subcontract any part of the services that involve the processing of personal data, it must obtain prior written authorization by notifying Niterra of such need, specifying the processing activities it intends to subcontract and clearly and unambiguously identifying the subcontractor and its contact information.

7. If the Business Partner needs to transfer personal data internationally to perform the contracted services, in addition to providing Niterra with prior and express notice, the Business Partner must:

a) ensure that the transferred personal data will continue to be protected in accordance with the LGPD;
b) adopt appropriate technical and organizational measures to prevent any unauthorized access, disclosure, alteration, or misuse of the transferred personal data;
c) allow Niterra to audit or request proof of compliance with the requirements of this clause, whenever necessary;

d) sign an amendment containing the standard contractual clauses for the international transfer of personal data set forth in ANPD Resolution No. 19, in the event of a direct international transfer between the Business Partner and a third party located in another country;
e) notify Niterra in advance of any international transfer of personal data carried out directly by the Business Partner to a third party located outside the country, when such data is related to the performance of the services contracted with Niterra;
f) to assume responsibility for any improper processing resulting from the international transfer, thereby releasing Niterra from any liability in this regard, without prejudice to the provisions of applicable law.

8. The Business Partner ensures that third parties it engages comply with laws related to the processing of personal data. They must follow the Business Partner's instructions and process personal data solely to fulfill the contracts entered into with the Business Partner.

9. The Business Partner acknowledges that it will be jointly and severally liable with any third parties it engages for any damages caused to Niterra, a data subject, a national authority, or an interested third party as a result of a violation of the law.

10. During the term of this agreement, each Party agrees to:

a) establish and follow privacy and information security policies, including guidelines on best practices and governance covering aspects such as organization, operational procedures, security standards, technical standards, obligations for those involved in data processing, educational initiatives, and mechanisms for oversight and mitigation of risks related to the processing of personal data;
b) adopt safety, technical, and administrative measures to protect personal data of non-authorized accesses and of accidental or illegal situations of destruction, loss, change, communication, or any form of inappropriate or illegal handling;
c) notify, within a reasonable time, the national authority and the data subject of any data security incident involving data under its control that could pose a significant risk or cause significant harm to data subjects;
d) comply with the principles of good faith, purpose, appropriateness, necessity, free access, data quality, transparency, security, prevention, non-discrimination, and accountability, as defined by law;
e) ensure that the data processing activities you carry out fall under one of the situations permitted by law;
f) not to retain or use personal data for longer than is necessary to fulfill the legitimate purposes for which the processing was authorized;
g) not to sell, disclose to third parties, or otherwise use personal data without the data subject's authorization or in violation of the law;
h) facilitate and cooperate with the exercise of data subjects' legal rights, in accordance with the law;
i) maintain records of the personal data processing operations they carry out, especially when based on legitimate interest;
j) whenever requested by the competent authority, conduct assessments and prepare reports on the impact on the protection of personal data, including sensitive data, related to its data processing operations, while respecting trade and industrial secrets. The reports must include, at a minimum, a description of

the types of data collected, the methodology used for data collection and to ensure information security, and the data controller's analysis of the measures, safeguards, and risk mitigation mechanisms adopted;

k) restrict access to personal data only to those who need it to fulfill the purpose disclosed to the data subject, and only to the extent necessary for the processing, while also ensuring that those who, on its behalf, have or may have access to personal data respect and maintain the confidentiality and security of such data.

11. If the relationship established between the Parties involves the processing of personal data, a Party agrees to notify the other Party within 24 (twenty-four) hours if it identifies or suspects a security incident related to the processing of personal data that could pose a significant risk or cause significant harm to the other Party or to the data subjects.

a) The notifying party must provide details of the incident, including a description of the personal data affected, information about the data subjects involved, the technical and security measures used, the risks associated with the incident, the reasons for any delay in notification (if any), and the measures taken or to be taken to mitigate or reduce the effects of the incident.
b) The Parties shall cooperate in good faith to determine responsibilities regarding the necessary notifications to regulatory authorities and data subjects, in accordance with applicable law, and to address the causes of the Security Incident, while ensuring the security of the data and its processing.
c) In the event of a Security Incident caused by an act or omission of the Business Partner, the Business Partner shall bear all reasonable and substantiated costs incurred by Niterra to remedy the incident, including, but not limited to, costs related to forensic investigations, notification to data subjects and authorities, and the provision of mitigation services to data subjects, without prejudice to any other compensation for losses and damages.

Each Party acknowledges that it will be fully and solely responsible for the data processing activities it carries out, including those performed by its employees, subcontractors, representatives, and contractors acting on its behalf.

12. This liability extends to the other Party, data subjects, the applicable regulatory and tax authorities, and any interested third parties, except in cases where the law provides for an exemption from liability, particularly with respect to activities carried out by the Operator.

13. If one Party is challenged, either administratively or judicially, regarding the legality and legitimacy of any personal data processing activity carried out under the responsibility of the other Party, the latter shall:

a) Identify yourself as the sole party responsible for the processing activity in question.
b) Take every possible measure within your power to exclude the party not responsible for the processing in question.

14. If it is not possible to exclude the party not responsible for the disputed processing, the responsible party shall provide that party with support and information so that it may

conduct its response and defense in the lawsuit, for as long as it remains a party to the lawsuit and while the lawsuit is pending, in order to safeguard its interests.

15. A Party's participation in the process or proceeding referred to in the clause above shall in no way alter the exclusive liability of the Party that was actually responsible for the data processing activity in question; the latter Party shall, even in the event of a judgment against the Party not responsible for the processing in question, be solely liable for bearing any losses, penalties, rulings, costs, and fines, and for compensating and providing redress, when necessary, and as provided by law, all damages (whether pecuniary, moral, individual, or collective), losses, restrictions, consequences, and harm caused by it, whether they were suffered:

a) by the Party that did not carry out the data processing in question, as well as its respective directors, officers, employees, contractors, representatives, and agents of any kind;
b) by the data subject; or any third parties.

Public Registry Notice and Language Prevalence: This document is an English courtesy translation of the official Portuguese version of the General Terms and Conditions for the Processing of Personal Data and Information Security (*Condições Gerais de Tratamento de Dados Pessoais e Segurança da Informação*) of Niterra do Brasil Ltda.. The official Portuguese version is duly registered for the purposes of public notice and legal effect vis-à-vis third parties at the 1st Registry of Deeds, Titles, and Documents and Civil Registry of Legal Entities of Mogi das Cruzes, São Paulo, under registration number 95514 (Book B), on February 27, 2026 (Protocol No. 79145 of February 19, 2026).

The authenticity of the Portuguese registration can be verified on the TJSP Digital Seal portal (https://selodigital.tjsp.jus.br) using seal: 1115674TISE000697693SE26A.

In the event of any conflict, discrepancy, or inconsistency between this English translation and the official Portuguese version, or in matters of legal interpretation, the Portuguese version shall prevail for all legal intents and purposes.
