Data Privacy Policy - Third Parties

RECIPIENTS: JBS's and Seara's business partners (third parties).

1. PURPOSE

Define the necessary requirements to ensure compliance with Privacy and Personal Data Protection laws and regulations.

2. RESPONSIBILITY FOR COMPLIANCE

This policy applies to all third parties processing personal data on behalf of the Company. Compliance with this policy is mandatory and reflects corporate governance regarding personal data protection issues.

3. COVERAGE

This policy covers all types of Personal Data Processing carried out by third parties on behalf of the Company.

4. DEFINITIONS

4.1. For the purposes of this Policy, the following terms listed below, when used in the singular or plural forms, shall have the following meanings:

4.1.1. Data subject: a natural person to whom the personal data are the subject of processing carried out by the Company or on its behalf;

4.1.2. Personal data: any information related to an identified or identifiable natural person, thus any data that identifies a natural person or that, through the combination of some data, may identify them;

4.1.3. Sensitive personal data: a special category of personal data, due to its discriminatory potential. Data about a natural person are as follows:

- Racial or ethnic origin;
- Political opinions;
- Religious beliefs;
- Membership of a trade union or organization of a religious, philosophical, or political nature;
- Health or sex life;
- Biometrics and
- Genetics.

4.1.4. Anonymized data: data in which the data subject cannot be identified, considering the technical means used at the time of processing. Anonymized data is not considered personal data;

4.1.5. Processing: corresponds to any activity carried out with personal data, from its collection to its elimination;

4.1.6. Third parties: all external parties that in any way represent the Company, including, but not limited to suppliers, customers, service providers, third-party employees, partners, franchises, vendors, and other individuals who have access to the Company's information assets, and information systems, or who provide personal information;

4.1.7. Data processing agents: controller and processor;

4.1.7.1. Controller: the agent responsible for decisions regarding the processing of personal data;

4.1.7.2. Processor: the agent who processes personal data on behalf of the controller.

4.1.8. National Data Protection Authority (ANPD): the government body responsible for overseeing, implementing, and enforcing compliance with the General Data Protection Law (LGPD);

4.1.9. Information security: protection of a set of information, aiming to preserve its confidentiality, integrity, availability, authenticity, and legality;

4.1.10. Data protection officer: a person appointed by the controller and processor to act as a communication channel between the controller, data subjects, and the National Data Protection Authority (ANPD).

5. GENERAL PROVISIONS

5.1. Third parties must commit to complying with the following aspects:

5.1.1. Ensure that all personal information of the Company is adequately protected against threats, keeping it secure;

5.1.2. Ensure that their employees and subcontractors are aware of the LGPD and comply, at least, with the Company's recommendations regarding privacy, personal data protection, and information security, ensuring that there is an adequate training program under current legislation and JBS's LGPD Compliance Program;

5.1.3. Limit the use of personal information to identified commercial purposes for which they are collected;

5.1.4. Raise awareness of privacy requirements as an integral part of each employee's daily operation and ensure that everyone understands the importance of privacy practices and their responsibilities;

5.1.5. Limit the number of people processing personal data to the minimum necessary;

5.1.6. Follow market best practices regarding information security;

5.1.7. Ensure that applicable regulations and contracts regarding privacy maintenance, protection, and international transfer of personal information are respected and accepted by JBS's Privacy Office;

5.1.8. Ensure that all processing of personal data, including sensitive data, is carried out based on valid and appropriate legal grounds under the LGPD;

5.1.9. Ensure that all aspects of personal data processing are expressly endorsed by JBS's Privacy Office.

6. GUIDELINES E PROCEDURES

6.1. All personal data processing activities carried out by the third party on behalf of the Company must necessarily follow all principles listed by the LGPD, applying them in good faith, in other words, using personal data honestly, sincerely, ethically, and within moral limits;

6.2. The principles to be followed during the processing of personal data are:

- Minimization: when processing personal data, it must be limited to using the minimum data necessary to achieve its purposes;
- Purpose: for the processing of personal data to be legitimate, the third party must inform the data subject of the specific purposes for which it will be carried out;
- Adequacy: processing must be compatible with the purpose informed to the data subject;
- Necessity: processing may only be carried out when necessary to achieve the purposes;
- Free access: the data subject may easily and free of charge check the manner and duration of the processing of their personal data;
- Data quality: stored personal data must be kept up-to-date, clear, and accurate;
- Transparency: all information regarding the processing of personal data must be clear, accurate, and easily accessible. The data subject must know which personal data is processed and for what purposes they are kept;
- Security: the third party will take all technical and administrative information security measures capable of protecting personal data from unauthorized access and accidental or unlawful destruction, loss, alteration, communication, or dissemination;
- Prevention: measures will be taken to prevent damages resulting from the processing of personal data, such as periodic audits, training, etc.;
- Non-discrimination: the impossibility of processing for abusive discriminatory purposes;
- Accountability: effective measures will be demonstrated to prove compliance with personal data protection rules and the effectiveness of these measures.

6.3. The General Data Protection Law establishes legal hypotheses in which it is possible to process personal data. Thus, the third party may process personal data under the following hypotheses:

- Consent: the data subject, or their legal representative, must consent to the processing of personal data, specifically and distinctly, for specific purposes;
- Compliance with legal or regulatory obligations: when it is necessary to process personal data due to a legal or regulatory obligation, consent of the data subject is not required;
- Execution of public policies and studies by research agencies: processing hypotheses admitted regardless of consent, for purposes considered to be in management's interest or research purposes;
- Execution of contract or pre-contractual diligence: consent is waived when processing occurs to ensure compliance with contractual execution or pre-contractual diligences;
- Regular exercise of rights: consent is waived when processing is necessary for the regular exercise of rights in a judicial, administrative, or arbitration proceeding;
- Protection of the life of the data subject or third parties: if processing is imperative for the protection of the life or physical integrity of the data subject, it can be carried out without consent;
- Health protection: processing carried out to promote procedures by healthcare professionals or health entities will be considered a relevant public interest;

- Legitimate interest: exceptionally, the third party may rely on a legitimate interest to process personal data, such as supporting and promoting controller activities and protecting the regular exercise of the data subject's rights or providing services that benefit them;
- Credit protection: the inclusion of consumers' personal data in credit reports may be made without the express consent of the data subject.

6.4. In some cases, the third party as controller or processor of personal data may process sensitive personal data. In this case, the processing hypotheses are as follows:

- Consent: when the data subject or their legal representative expressly consents, for specific and distinct purposes;
- Compliance with legal or regulatory obligation: the data processing agent does not need the consent of the data subject when in need to process sensitive personal data due to a legal or regulatory obligation;
- Execution of public policies and studies by research agencies: hypotheses of processing admitted regardless of consent, for purposes considered to be in management's interest or research purposes;
- Regular exercise of rights, including in contracts: consent is waived when processing is necessary for the regular exercise of rights in a judicial or administrative proceeding, or even to ensure compliance with contractual execution;
- Protection of the life of the data subject or third parties: if processing is imperative for the protection of the life or physical integrity, it can be carried out without the consent of the data subject;
- Health protection: if processing is carried out to promote procedures by healthcare professionals or health entities will be considered a relevant public interest;
- Guarantee of fraud prevention and data subject security: processes of identification and authentication of registration in electronic systems are permitted without consent, except where fundamental rights and freedoms requiring the protection of personal data prevail.

6.4.1. The bases defined in the previous item must always respect the aspects introduced by the LGPD to be appropriately and legally valid and applied.

6.5. The third party may process data of children and adolescents in situations such as the hiring of apprentice minors, information about dependents and family events, among others. The processing of minors' data is the most delicate type of process, as it always requires prominent consent and must be given by at least one of their parents or legal guardians;

6.5.1. Exceptions to this legal basis require express authorization from the Privacy Office.

6.6. If the third party receives any type of request from the data subject, the Company must be immediately notified, before adopting any measures, unless expressly otherwise agreed between the parties;

6.7. Notice of personal data collection

6.7.1. Adequate notice must be provided to data subjects at the time when personal information is collected;

6.7.2. The privacy notice, policies, or other statements to which they are bound must provide complete information to demonstrate to an individual how their personal information will be used so that its use is fair and legal.

6.7.3. The following information must be considered for inclusion in a notice:

6.7.3.1. Purposes for which personal data is collected, used, and disclosed;

6.7.3.2. Options available to the individual regarding the processing of their data, whenever applicable;

6.7.3.3. Period for which personal data must be retained, according to the identified purpose or as required by law;

6.7.3.4. Methods used for the collection of personal data, including cookies and other tracking techniques, and third-party agencies;

6.7.3.5. An individual's personal data must be disclosed to third parties only for identified legal business purposes and with the individual's consent, whenever possible;

6.7.3.6. Consequences of withdrawing consent for the processing of personal data for identified purposes;

6.7.3.7. Data subjects are responsible for providing the Company with accurate and complete personal data, and may contact the company if the correction of such information is necessary;

6.7.3.8. Process for an individual to view and update their personal information records;

6.7.3.9. Process for an individual to file a complaint regarding the Company's privacy practices;

6.7.3.10. Contact information of the person in charge of privacy practices and responsible for privacy concerns.

6.7.3.11. Process for an individual to withdraw consent for the collection, use, and disclosure of their personal information for identified purposes.

6.7.4. Personal data should only be collected for legitimate, identified, and specific purposes.

6.8. Consent

6.8.1. When this is the legal basis for the processing of personal data, the third party must ensure that consent has been correctly obtained from the data subject, being able to provide evidence, if necessary;

6.8.2. Consent must be obtained freely, informed, unambiguous, and express, being obtained clearly and transparently;

6.8.3. It must be given by the data subject or their parent/legal guardian if they are under 18 years old unless there is another legal hypothesis that can be used, provided that it is expressly authorized by JBS's Privacy Office;

6.8.4. It is not allowed to collect consent after the processing of personal data.

6.9. Collection of personal data

6.9.1. Personal data should only be collected for legitimate, identified, lawful, and specific purposes;

6.9.2. Methods for collecting personal data must be reviewed by the Privacy Office to ensure that personal data is obtained:

- Appropriately, without intimidation;
- Legally, adhering to laws and regulations regarding the use of personal data;
- Validate if the privacy notice meets internal guidelines and applicable legislation;
- Authorize all aspects that process personal data from conception.

6.9.3. A privacy notice must be provided to the data subject if any new purpose is identified for processing personal data before such data is used for purposes not previously identified.

6.10. Limited use, disclosure, and retention of personal data

6.10.1. Personal data should not be used or disclosed for purposes other than those for which they were collected, except with the individual's consent or as required by law;

6.10.2. Personal data should not be retained for longer than necessary;

6.10.3. The retention period for personal data varies according to the purpose for which the data is used. Thus, retention should only be for the duration necessary to fulfill the identified purposes or as required by legal and regulatory obligations that require the data processing agent to retain the data for a certain period;

6.10.4. Guidelines and procedures must be developed for the retention and disposal of personal data. They should address minimum and maximum retention periods and storage methods;

6.10.5. After the expiration of identified purposes or the withdrawal of consent, the third party must securely delete or anonymize the personal data of the data subjects. Data is anonymized to avoid the unique identification of an individual.

6.11. Confidentiality

6.11.1. All information processed by third parties on behalf of the Company, or shared by it, must be kept in the strictest confidence, even after the termination of the relationship between the parties.

6.12. International data transfer

6.12.1. Personal data may not be transferred to a third country or international organization without the previous and express authorization of the Company;

6.12.2. For authorization of international transfer of personal data, it must be informed to which countries or international organizations the personal data will be sent, the appropriate security guarantees, and where the data will be stored.

6.13. Privacy security practices

6.13.1. The third party must commit to ensuring the security and protection of the personal data they are processing;

6.13.2. Labeling and handling guidelines for information assets should include specific controls for the storage, retention, and transfer of personal data;

6.13.3. The third party must establish procedures to ensure the protection of personal data against accidental disclosure due to natural disasters and environmental hazards;

6.13.4. Incident response protocols are established and maintained to deal with incidents related to personal data or privacy practices.

6.14. Quality of personal information

6.14.1. The third party may perform additional validation procedures to ensure that the collected personal data is accurate and complete for the purposes for which they are to be used;

6.14.2. The third party must ensure that the collected personal data is relevant to the purposes for which they are to be used.

6.15. Governance on the processing of personal data

6.15.1. Records of operations carried out with shared personal data as a result of the contract between the parties must be maintained;

6.15.2. An impact assessment report on data protection must be conducted and maintained, when applicable. Collaboration between the parties in the preparation of the impact report should also occur if necessary, as well as mutual collaboration in any consultation that may occur from the ANPD or the authority empowered with supervisory power, when appropriate;

6.15.3. An annual privacy compliance review must be conducted for identified business processes and their supporting applications. A record of identified non-conformities in the annual privacy reviews must be immediately informed to the Company;

6.15.4. Privacy respect must be by default, in other words, in the most protective way possible, so that from its conception, every new product or service must be carefully evaluated to reduce risks to the protection of personal data. The product/service must be validated by JBS's Privacy Office to meet this requirement;

6.15.5. All processes in which the third party processes personal data, such as security measures adopted and responses to data subjects, among others, need to be properly documented to maintain total governance over the processing of personal data;

6.15.6. Procedures must be established to monitor the effectiveness of controls over the processing of personal data and to ensure corrective actions as necessary, and such documents may be requested by the Company;

6.15.7. Any conflicts or disagreements regarding the requirements outlined in this policy or related privacy practices should be submitted to the data privacy officer for resolution.

6.16. Subcontracting

6.16.1. None of the services object of the contract that involves the processing of personal data may be subcontracted without the previous and express authorization of the Company;

6.16.2. If subcontracting is authorized, the third party must inform all subcontractors and be fully responsible for the subcontractors and, consequently, for the employees, representatives, and agents designated by the subcontractor for the execution of services, including ensuring the provision of the information established in this policy;

6.16.3. In case of non-compliance with this policy by subcontractors, the third party will remain fully responsible to the Company regarding compliance with the established obligations.

6.17. Incident management

6.17.1. In case of personal data security incidents or suspected incidents, the Company must be immediately notified, along with all relevant information for the documentation and communication of the incident, and, if available, must contain at least the following information:

- Date of discovery and occurrence;
- Means of identifying the incident;
- Description of the nature of the personal data security breach;
- The name and details of the data protection officer;
- Description of the risks related to the incident and the possible consequences of the personal data security breach;
- Indication of the technical and security measures used to protect personal data;
- Description of the measures taken or proposed to remedy the effects of the personal data security incident;
- Cause of the incident;
- Proposal for future measures to be implemented to prevent it from occurring again;
- What information and volume of people are affected;
- If the notification is partial, the information missing to conclude it.

6.17.2. If it is not possible to simultaneously provide the aforementioned information, it should be provided gradually, without undue delay;

6.17.3. The third party must provide all necessary information requested by the Company and support as necessary to notify the necessary individuals and authorities.

6.18. Audit

6.18.1. The Company reserves the right to verify, at any time, compliance with the procedures, security measures, and controls, and the procedures supporting the execution of the contract, through audits. A written request will be made at least 72 hours in advance;

6.18.2. All necessary information will be provided to show compliance with its obligations, as well as allow the adequate conduct of audits by the Company or another auditor authorized by the Company, and support any inquiries to the ANPD, when appropriate.

7. MISCELLANEOUS

7.1. Cases of violation or suspicion of violation of this policy should be directly reported to the Compliance Board through the Company's Ethics Line (www.linhaeticajbs.com.br | 0800 377-8055 (Brazil) | 0800 666 1659 (Argentina) | 000 401 90861 (Uruguay);

7.2. Violation of any guideline of this policy may result in consequences for the Company and the third party, through the application of sanctions resulting from the Code of Conduct and Ethics, internal policies, and applicable legislation.

* * *

Policy approved by the Company's Privacy Executive Committee.