Data Privacy Policy - Third Parties

RECIPIENTS: Business partners (third parties) JBS and Seara.

1. GOAL

To define the necessary requirements to ensure compliance with the laws and regulations of Personal Data Privacy and Protection.

2. RESPONSIBILITY FOR COMPLIANCE

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

3. SCOPE

This policy covers all and any type of processing of personal data carried out by the Company.

4. DEFINITIONS

4.1. The following terms are considered for the purposes of this policy, both in the singular or plural:

4.1.1. Data holder: natural person whose personal data is subject to the treatment carried out by or on behalf of the Company;

4.1.2. Personal data: any information related to an identified or identifiable natural person; therefore, all the data that identifies an individual, or that, through the combination of different data, may incidentally identify them;

4.1.3. Sensitive personal data: it is a special category of personal data, due to its discriminatory potential. This is data of an individual about:

- Racial or ethnic origin;
- Political stance;
- Religious belief;
- Membership in a union or organization of a religious, philosophical, or political nature;
- Health or sexual life;
- Biometrics and
- Genetics.

4.1.4. Anonymized data: data in which the holder 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 collection to disposal;

RECIPIENTS: Business partners (third parties) JBS and Seara.

4.1.6. Third parties: all external parties that somehow represent the Company. Including, but not limited to suppliers, customers, service providers, third-party employees, partners, franchises, salespeople and others who have access to the Company's information assets, information systems or who pass on personal information;

4.1.7. Processing agents: controller and operator;

4.1.7.1 Controller: consists of the agent in charge of decisions regarding the processing of personal data;

4.1.7.2 Operator: is the agent who performs the processing of personal data on behalf of the controller;

4.1.8. National Data Protection Authority (ANPD): consists of the public administration body responsible for ensuring, implementing, and monitoring compliance with the General Data Protection Law;

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

5. GENERAL PROVISIONS

5.1. In compliance with privacy and data protection laws, the Data Privacy Program - Third Parties was created, which aims to:

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

5.1.2. Ensure that the Company's employees are fully aware of the contractual, statutory, or regulatory implications of any breaches of privacy;

5.1.3. Limit the use of personal information for the identified business purposes for which it is collected;

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

5.1.5. Make all employees aware of the processes that need to be followed for the collection, legal use, disclosure, transfer, retention, archiving, and disposal of personal information;

5.1.6. Ensure that all third parties that process personal data on behalf of the Company provide proper data protection;

RECIPIENTS: Business partners (third parties) JBS and Seara.

5.1.7. Ensure that the applicable regulations and contracts regarding the maintenance of privacy, protection, and international transfer of personal information are respected.

6. GUIDELINES AND PROCEDURES

6.1. Any and all personal data processing activities must observe good faith and the processing principles;

6.2. The Company establishes the following principles that must be followed when processing personal data:

- Minimization: when processing personal data, one should limit oneself to using the minimum data necessary for the accomplishment of one's purposes;
- Purpose: for the processing of personal data to be legitimate, the third party must inform the holder for what specific purposes it will be performed;
- Adequacy: the processing must be compatible with the purpose informed to holder;
- Need: the treatment can be carried out only when necessary for the accomplishment of the purposes;
- Free access: the holder will be entitled, in an easy and free way, to consult the third party regarding the form and duration of their personal data processing;
- Data quality: stored personal data must be kept up to date, clear, and accurate;
- Transparency: all information on how to process personal data must be clear, precise, and easily accessible. The holder must know which, and for what purpose, personal data is processed by the third party;
- Security: the third party will take all technical and administrative measures of information security, able to protect personal data from access and from accidental or unlawful situations of destruction, loss, alteration, communication, or disclosure;
- Prevention: measures will be taken to prevent the occurrence of damages due to the processing of personal data, such as periodic audits, training, etc.;
- Non-discrimination: impossibility of carrying out a processing for abusive discriminatory purposes;
- Responsibility and accountability: the adoption of effective measures will be demonstrated, capable of proving the respect for and compliance with the rules of protection of personal data and the effectiveness of those measures.

6.3. The General Data Protection Law establishes legal cases in which it is possible to carry out the processing of personal data. Thus, the third party may process personal data in the following cases:

- Provision of consent: holders, or their legal guardian, must consent to the processing of personal data, in a specific and detached manner, for specific purposes;
- Compliance with legal obligation: when the controller needs to process personal data due to a legal or regulatory obligation, they will not need the consent of the holder;
- Performance of public policies and studies by a research body: cases of processing admitted regardless of consent, for purposes considered to be of interest to the administration or for research purposes;
- Performance of contract or pre-contractual diligence: consent is waived when processing occurs to ensure compliance with contractual performance or pre-contractual diligences;

- Regular exercise of rights: consent is waived when processing is required for the regular exercise of rights in judicial, administrative, or arbitration proceedings;
- Protection of the holder or third parties' lives: if the treatment is indispensable for the protection of the holder's life or physical safety, it may be carried out without consent;
- Health protection: treatment carried out with the purpose of promoting procedures by health professionals by health entities, will be considered relevant public interest;
- Legitimate interest: as an exception, the third party may use the legitimate interest to process personal data, as support and promotion of activities of the controller, and protection of the holder's regular exercise of rights or provision of services that benefit them;
- Credit protection: the inclusion of consumers' personal data in positive registrations may be affected, regardless of the holder's express consent.

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

- Provision of consent: when the holder or their legal guardian consents, in a specific and prominent way, for specific purposes;
- Compliance with legal obligation: when the controller needs to process sensitive personal data due to a legal or regulatory obligation, they will not need the holder's consent;
- Performance of public policies and studies by a research body: cases of processing admitted regardless of consent, for purposes considered to be of interest to the administration or for research purposes;
- Regular exercise of rights, including in contracts: consent is waived when processing is required for the regular exercise of rights in judicial, administrative, or arbitration proceedings, or even to assure the compliance with contractual performance;
- Protection of the holder or third parties' lives: if the processing is indispensable for the protection of life or physical safety, it may be carried out without the holder's consent;
- Health protection: if the processing is carried out with the purpose of promoting procedures by health professionals or by health entities, it will be considered relevant public interest;
- Guarantee of fraud prevention and security of the holder: the processes of identification and authentication of registration in electronic systems are allowed regardless of consent, except in case fundamental rights and freedoms prevail that require the protection of personal data.

6.5. The third party will be able to process data of children and adolescents, upon hiring of apprentice minors, information about dependents, and family events. The processing of the minor is the most sensitive type of personal data, as it always requires the specific consent given by at least one of the parents or guardians of the minor;

6.6. All Company's processes and procedures carried out by third parties must guarantee the rights of the data Holders:

- Confirmation of the existence of processing and access to personal data: the holder may request the third party to declare whether it processes their personal data. This right is related to the principle of free access, that is, the guarantee that the holder can consult, free of charge and easily, regarding the form and duration of the processing of their personal data, as well as the completeness of their personal data;

RECIPIENTS: Business partners (third parties) JBS and Seara.

- Data portability to another service provider or product: holders can request the personal data they have provided, so that the provider can transmit it to another provider in charge of the processing, without the Company or the third party being able to prevent it;
- Information of the entities with which the controller has carried out shared use of data: the holder may request information regarding the sharing of their personal data with third parties;
- Correction of incomplete data: the holder may ask the third party to correct or supplement their personal data;
- Information about the possibility of not providing consent: the data holder has the right to be informed about the possibility of not providing consent when processing of personal data is carried out;
- Anonymizing, blocking, or deleting unnecessary, excessive or illegally processed data: due to the principles of adequacy and need, the holder may request the anonymization, blocking, or elimination of unnecessary, excessive or illegally processed data. To the extent technically possible, the third party will anonymize the personal data of their holders and will strive to minimize the personal data processed;
- Revocation of consent: the holder may, at any time, request the revocation of the consent given for the processing of their data;
- Complaint to ANPD: the holder may file a complaint with the ANPD for occasional violations committed;
- Elimination of personal data: the holder may request the elimination of their processed personal data. In situations of legal or regulatory obligation, this data may be retained;
- Opposition to processing, if irregular: the holder may object to the processing of their personal data, if it is found that it is an irregular processing.

6.7. Notice of personal data collection

6.7.1. Proper notice must be provided to data holders when personal information is collected;

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

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

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

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

6.7.3.3. Period in which the personal data is to be maintained, according to the purpose identified or as required by legislation;

6.7.3.4. Methods employed to collect personal data, including Cookies and other tracking techniques, and third party agencies;

6.7.3.5. An individual's personal data should 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 holders are responsible for providing the Company with accurate and complete personal data, and can contact the company if correction of such information is required;

6.7.3.8. Process to enable an individual viewing and updating their personal information records;

6.7.3.9. Process to enable an individual to file a complaint or claim with respect to the Company's privacy practices;

6.7.3.10. Contact information for a person responsible for privacy practices and accountable for privacy concerns;

6.7.3.11. Process to enable 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;

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

6.8. Consent

6.8.1. Consent is the standard case for data processing, unless another case can be used, such as a law or regulation that specifically requires or permits otherwise;

6.8.2. The consent must be free, informed and express, and must be requested in a clear and transparent manner;

6.8.3. It must be given by the data holder or by their parent or legal guardian if they are under 18 years old, unless there is another legal case that can be used;

6.8.4. A record is kept of the consent obtained from data holders;

6.8.5. Appropriate consent must be obtained from data holders before their personal data is included in information processing systems;

6.8.6. Consent must be obtained from data holders before their personal data is used for purposes not previously identified.

RECIPIENTS: Business partners (third parties) JBS and Seara.

6.9. Collection of personal data

6.9.1. The collection of personal data should be limited to the minimum requirement for lawful and specific purposes.

6.9.2. Methods of collecting personal data should be reviewed by the Privacy Office to ensure that personal data is obtained:
- Properly, without intimidation;
- Legally, adhering to the laws and regulations regarding the use of personal data.

6.9.3. Data holders should be informed if additional data about them is developed or acquired.

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

6.10.1. Personal data must not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual, or as required by law;

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

6.10.3. The retention period for personal data varies according to the purpose for which the data is used. Therefore, the retention should only be for the duration necessary to fulfill the identified purposes, or in accordance with legal and regulatory obligations that oblige the processing agent to keep the data for a particular period of time;

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 modes;

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 holders. The data is anonymized to avoid the unique identification of an individual;

6.11. Access for review and update

6.11.1. Processes must be established for data holders to:
- Request access to their personal data or information as prescribed by law;
- Correct or update their personal data or information;
- Withdraw consent to the processing of their personal data.

6.11.2. The identity of the data holders who request access to their personal data or the identity of the data holders authorized by the holder to access the information must be appropriate before providing access to the information;

6.11.3. An answer must be given to data holders who request access to their personal information in an accessible manner, within a term defined as of the moment of the complaint or request, as prescribed by law;

6.11.4. Data holders should be notified, in writing, regarding the reason for any denial of requests for access to personal information, to the extent required by applicable law.

6.12. Disclosure to third parties and international transfers

6.12.1. Personal data will be disclosed to third parties only for the identified legal purposes and after obtaining the data holders' appropriate consent, unless a law or regulation allows or requires otherwise.

6.12.2. For third parties to be able to process data on behalf of the Company, they must have:

6.12.2.1. Agreements signed to protect personal data consistent with the Company's Data Privacy policy and information security practices, or measures implemented as prescribed by law;

6.12.2.2. Non-Disclosure agreements or confidentiality agreements that include privacy clauses in the contract;

6.12.2.3. Procedures established to comply with the terms of their agreement with the Company to protect the personal data.

6.12.3. Personal data can be transferred internationally at locations where the Company operates, for data processing, provided that:

6.12.3.1. The recipient provides a degree of protection of personal data equal to or greater than that of Brazil;

6.12.3.2. The individual has given consent to the transfer of information;

6.12.3.3. The transfer is required for the performance of a contract between the individual and the Company, or the implementation of pre-contractual measures taken in response to the individual's request;

6.12.3.4. The transfer is required for the conclusion or execution of a contract entered into in the interest of the individual, between the client and a third party;

6.12.3.5. The transfer is necessary or legally required for important reasons of public interest or for the establishment, exercise, or defense of judicial claims;

6.12.3.6. The transfer is required by law;

6.12.3.7. The transfer is required in order to protect vital interests of the individual;

6.12.3.8. The transfer is made under a data transfer contract.

6.12.4. Corrective measures must be taken in response to the misuse or unauthorized disclosure of personal data by a third party that processes personal data on behalf of the Company.

6.13. Security practices for privacy

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

6.13.2. The guidelines for labeling and handling of information assets must include specific controls on the storage, retention, and transfer of personal data;

6.13.3. The third party should establish procedures that guarantee 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 in order to deal with incidents relating 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 personal data collected is accurate and complete, for the purposes for which it is to be used;

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

6.15. Privacy monitoring and performance

6.15.1. Procedures must be established for recording and responding to claims or complaints registered by data holders;

6.15.2. Each complaint regarding privacy practices registered by data holders must be validated by the Company, the responses documented and communicated to the individual;

6.15.3. An annual privacy compliance review must be conducted for identified business processes and their supporting applications;

6.15.4. A record must be kept of non-conformities identified in the annual privacy reviews. Corrective and disciplinary measures must be initiated and controlled until completion, guided by the Company's governance;

6.15.5. Procedures should be established to monitor the effectiveness of personal data controls and to ensure corrective actions, as needed;

6.15.6. Any conflicts or disagreements regarding the requirements provided for in this policy or associated privacy practices should be referred to the data privacy officer for resolution.

7. FINAL CONSIDERATIONS

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

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

* * *

Policy approved by the Company's Executive Privacy Committee at a meeting held on January 15, 2020.