1. Purpose

Regulate the legitimacy of the processing and use of personal data at Grupo Bimbo, in order to promote privacy goals and avoid any data breach.

2. Scope

This policy applies to all Grupo Bimbo Entities and Organizations, in connection with the processing of personal data of their candidates, collaborators, suppliers, clients and consumers.

3. Requirements

The guidelines to which the Entities and Organizations of Grupo Bimbo are subject as those responsible for the files and databases of data subjects are the following:

- The Global Legal and Compliance Director must:
  - Ensure compliance with this policy and applicable procedures.
  - Establish procedures for receiving, processing, monitoring and responding to requests from data subjects, ensuring compliance.
  - Advise the Entities and Organizations of Grupo Bimbo in their management and in the execution of the decisions of the Ethics Committee.
- The Ethics and Regulatory Compliance Committee ("Ethics Committee") is empowered to issue measures regarding the application of this policy and to approve situations that require express authorization from the Company.
- The Organization leaders and Functional VPs must:
  - Implement this policy and comply with internal procedures and other legal regulations to ensure that personal data is collected and processed lawfully, in an informed, proportionate, up-to-date and secure manner, with a legal basis, privacy notices and consent where applicable, in the countries where they operate.
  - Appoint a person to coordinate with the Global Legal Department.

Legality

- Collect and process the personal data of candidates, clients, consumers, suppliers and associates lawfully, in accordance with applicable regulations.
- Ensure that all processing of personal data has a legal basis recognized in the applicable regulatory provisions.
- Document, in each treatment, its legal basis and the controls of compliance with the principles of lawfulness, purpose, proportionality, quality and accountability.
- Refrain from obtaining data by deceptive or fraudulent means.
- Use personal data only for the purposes authorized in the privacy notice and other applicable regulations.

Proportionality

- Collect only the personal information that is necessary for the functions performed and its processing must be justified.
- Avoid processing personal data in a manner incompatible with its intended purposes.
- To support and justify the purpose and processing of the information collected, in the privacy notice.
- Before collecting data, check that:
  - Forms, systems, and processes should only request the necessary data.
  - That there are rules for conservation, blocking, secure disposal and evidence of destruction when the purpose or applicable term is concluded.

- Stipulate in contracts with suppliers the confidentiality and personal data protection clause, approved by the Global Legal Department .

Information

- Inform, through the privacy notice, of the essential characteristics of the processing of personal data.
- Standardize and ensure that privacy notices include, in accordance with local legislation, the identity of the responsible party, the purposes, the data processed, the rights of the data subject, the means of contact, the applicable transfers and the mechanisms for revoking consent.
- Inform the data subject when the purpose of the processing changes or their data is transferred to a third party of Grupo Bimbo.
- Notify the data controller, and the competent authority where applicable, of any data breach as soon as possible, indicating the data breached and the measures to mitigate the risk.
- Having a documented protocol to identify, escalate, assess, contain and report personal data violations, with responsible parties, timeframes and applicable evidence.

Quality

- Keep the personal information of candidates, clients, consumers, suppliers and associates up-to-date and correct.
- Take reasonable steps to rectify or delete without delay any inaccurate personal data.
- Generate or obtain aggregated or pseudonymized information responsibly and legally, and protect any data that may re-identify the owner.
- Limit the use of the information to the time strictly necessary. After that period, block it until its deletion, in accordance with the applicable legal or contractual statute of limitations.
- Delete data that is no longer required for the purpose for which it was collected and keep a record of this procedure.

Responsibility

- Establish administrative, technical, and physical security measures to protect personal data.
- Ensure ongoing compliance with the privacy notice.
- Safeguard the confidentiality of personal data received from owners or third parties.
- In the case of a data transfer, verify that the third party complies with a minimum level of data protection equivalent to that of Grupo Bimbo.
- Support the transfers and processing of personal data by third parties on a legal basis, with a prior assessment of privacy risks and contractual clauses with the third party, as well as monitor compliance with the monitoring and control mechanisms.
- Prior to each negotiation with third parties that process personal data, conduct an impact analysis, based on ***FGB-CP-01 Annex I. RoPA & PIA***.
- Subject high-risk processing, including sensitive data, minors, automated decisions, profiling, marketing, new technologies or cross-border transfers, to impact assessment, differentiated controls, privacy by design and legal analysis by jurisdiction, where appropriate.
- Review the privacy notice annually for each Grupo Bimbo Business Unit and entity to keep it updated in accordance with current regulations.
- When AI uses personal data, the functional area responsible for the project, in conjunction with Business Technology, must:
  - Ensure compliance with ***FGB-IT-23 Global Artificial Intelligence Policy***.
  - Document the legal basis in the Record of Processing Activities
  - Obtain approval from the Global Legal Department .
- Review AI results to prevent unintentional disclosure of personal data; if it occurs, treat it as a personal data incident and handle it in accordance with data breach procedures.

Activities and procedures in which personal data are used

- Identify the activities or processes in which databases of candidates, clients, consumers, suppliers and associates are handled.
- Clearly differentiate between databases containing personal information and those containing sensitive data.
- Have a document that identifies the databases and describes the personal and/or sensitive data they contain.

Flow of information

Once they have identified the activities or procedures in which personal data is safeguarded, they must have a document that supports the life cycle of this data in each of their activities, clearly identifying:

1. In what part of the activity is the data collected?
2. How they are obtained (personally or directly from the holder, or indirectly through publicly accessible sources or transfer).
3. Which departments and people within each Entity or Business Unit process personal data and for which of their functions.
4. In what internal activities and/or procedures is personal data processed?
5. If these procedures require and carry out the transfer of data to third parties of Grupo Bimbo.
6. How long is personal data kept?
7. In what geographical region were the data collected and where will they be stored?
8. What are the mechanisms for updating and deleting them?
9. What measures are used for their protection and security?
10. What types of data are collected and their purpose.
11. The applicable legal basis, the consents obtained, the transfers of personal data, the processors involved, the rights applicable to the data subject, the security measures, the response times and the minimum evidence of compliance.

Consent

- Obtain the express consent of the data subjects when the purpose of the processing changes or the data is transferred to third parties of Grupo Bimbo, through the handwritten signature, electronic signature or any authentication mechanism.
- Ensure that the consent mechanism is actionable and specific to that purpose.
- Retain physical or electronic evidence of express consent.
- When consent is required, obtain it in a prior, informed, specific and verifiable manner, with mechanisms that allow its traceability, safeguarding and revocation.
- Provide suitable means for data subjects to revoke their consent.
- Where provided for by applicable law, the data subject may request the limitation of processing or other equivalent rights.
- The guidelines must be carried out based on ***FGB-CP-01 Annex I. RoPA & PIA***.

Informed consent

- Disseminate privacy notices and inform candidates, clients, consumers, suppliers and associates what data is collected and for what purposes.
- Make the privacy notice available to the data subjects before processing their data.
- Consent to privacy notices may be express or tacit, in accordance with applicable legal provisions and this policy.
- When the data corresponds to minors, consent must be given by the person exercising parental authority or guardianship.

Non-discrimination

The exercise of any of the rights of the data subject, by the data subjects, shall in no way result in distinction or exclusion that is not objective, rational or proportionate, and that has as its purpose or result, hindering, restricting, preventing or undermining the recognition, enjoyment or exercise of their human rights.

4. Definitions

Privacy notice: Physical, electronic or any other document, generated by the Global Legal and Regulatory Compliance Department or whoever it designates, made available to the Owner prior to the processing of his/her personal data, which establishes the information that will be processed and the purposes for which it will be used.

Consent: Manifestation of the will of the Owner, legal representative or guardian (or whoever exercises parental authority, in the case of a minor) in relation to the processing of personal data.

Personal data: Any information concerning an identified or identifiable natural and/or legal person.

Sensitive personal data: Data that affects the most intimate sphere of the data subject, or whose improper use may lead to discrimination or pose a serious risk to the data subject. Sensitive data includes, for example, data that may reveal aspects such as racial or ethnic origin, financial or property data, current and future health status, genetic and biometric information, religious, philosophical and moral beliefs, union membership, political opinions or sexual preference, and personal data of minors, based on applicable local legislation.

Rights of the owner: Those protections which may be granted by applicable laws or regulations related to the processing of the Owner´s Personal Data. In particular and by way of example;

- **Access:** Data Subjects may access their Personal Data held by the Controller and request a copy of the Privacy Notice governing such data processing activity.
- **Rectification:** Data Subjects may rectify their Personal Data when it is inaccurate or incomplete.
- **Deletion:** The owner will have the ability to always require deletion of his/her personal data.
- **Opposition:** The owner may oppose the processing and sale of his/her personal data, in which prevents the Controller from using it.
- **Portability:** The owner will have the right to receive his/her personal data physically or electronically and being able to transmit it to a third party.

Pseudonymisation: Processing of personal data in such a way that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Owner: The natural and/or legal person to whom the personal data correspond.

Processing: Obtaining, using, disclosing or storing personal data, by any means. Use includes any action of access, handling, use, transfer, transformation or disposal of personal data.

Data breach: Breaches of personal data security occurring at any stage of processing that violate the confidentiality, integrity and availability of data, such as: (i) loss or unauthorized destruction; (ii) theft, misplacement or unauthorized copying; (iii) unauthorized use, access or processing; or (iv) unauthorized damage, alteration or modification.

5. Updates

Changes made between versions are described.

Review / review history				
Version	**Review date**	**Updated by:**	**Approved by:**	**Main changes**
1	October, 2017			First publication
2	June 2020	Global Compliance Director	Global Legal and Compliance Director	• The name of the responsible Directorate has been changed to the Global Legal and Compliance Directorate • The term security breach was added. • In the definition of sensitive personal data, biometric, patrimonial and financial data were added. • Addition of responsibilities of the Global Legal Compliance Directorate. • The guideline on the processing of personal data of minors was added. • Two data sources were added: candidates and consumers.
3	December 2021	Global Compliance Director	Global Legal and Compliance Director	• The definition of owner, consent, personal data and objection has been expanded. • Non-discrimination guideline was added.
4	October 2022	Head of Compliance	Global Legal and Compliance Director	• Added ***FGB-CP-01 Annex I. RoPA & PIA***
5	November 2024	Head of Compliance	Global Legal and Compliance Director	• Definitions are updated. • The responsibility of the Legal and Compliance Director is updated. • General guidelines are updated.
6	June 2026	Head of Compliance	Global Legal and Compliance VP	• Artificial Intelligence guidelines were added.
7	July 2026	Manager of Regulatory Compliance	Global Regulatory Compliance Director	• Guidelines are integrated to strengthen legal bases, privacy notices, consent, rights of the data subject, third parties, incidents, PIA, record of processing, retention, privacy by design and evidence of compliance.