CORPORATE PRIVACY POLICY AND PERSONAL DATA PROTECTION

1. OBJECTIVE AND SCOPE

The purpose of this Policy is to consolidates the guidelines to be adopted by Ultra Group in the Personal Data Treatment collected in the conduct of its activities, as well as to provide guidance on Data Subjects' rights, Treatment Agents' obligations and guarantee the demonstrable responsibility, in accordance with the current legislation.

The guidelines contained herein apply to all companies comprising the Ultra Group, as well as to any and all employees, administrators, customers, suppliers of goods and services and partners who have access to Personal Data held by Ultra Group, without prejudice to additional regulations applicable to their activities.

It is responsibility of the Businesses and their employees to apply the provisions of this Policy to the Personal Data processing processes. Businesses must also define their guidelines based on the directions provided for in this Policy, considering their specific needs and the legal and regulatory aspects to which they are subject.

The Policy must be interpreted in conjunction with the Code of Ethics and other policies and rules of the Ultra Group. In case of conflict, the Risk, Integrity and Audit Executive Board shall be consulted.

All terms in capital letter used in this Policy shall have the meanings attributed thereto in the Glossary included at the end of this document or under the terms of the General Data Protection Law ("LGPD").

2. RELATED DOCUMENTS

In addition to this Policy, the Ultra Group is subject to other guidelines and rules, including:

- Ultra Group Code of Ethics
- Ultra Group Corporate Policies, where applicable
- Law No. 13,709/18, the General Data Protection Law or LGPD
- Law No. 12,965/14, the Internet Civil Civil Act
- Law No. 12,414/11, the Positive Registration Law, as amended
- Law No. 8,069/90, the Statute of the Child and the Adolescent, as applicable in the case of Processing of Personal Data of minors
- The regulations and rules published by the National Data Protection Authority ("ANPD")
- Brazilian and foreign regulations and rules in effect and/or in force in other countries where Ultra operates, as applicable.

3. GUIDING PRINCIPLES AND GUIDELINES FOR PRIVACY AND PERSONAL DATA PROTECTION

The Policy aims to ensure the privacy protection of Personal Data collected in the exercise of Ultra Group activities and to promote transparency regarding the Processing of Personal Data.

The guidelines provided wherein shall be followed from the creation of projects, products and services that involve Personal Data, until their implementation.

In this context, the Ultra Group, as well as its employees, must observe, at least, the following guidelines:

3.1 Collection and Processing of Personal Data

Personal Data shall be collected by lawful means and for legitimate purposes, protected by events set forth in the applicable legislation, particularly the LGPD, and stored in a secure environment for the time required by applicable regulations. Ultra Group companies shall follow procedures consistent with this Policy, legal requirements and risk management for the Processing of Personal Data.

3.2 Treatment of Sensitive Personal Data

The treatment of Personal Data, including Sensitive Data shall be carried out applying additional technical and administrative security measures that are reasonable and proportionate to the risk.

3.3 Children and Adolescents Personal Data Treatment

Children and adolescents Personal Data Treatment shall be performed in conformity with the relevant legislation, in compliance with the "best interests", that is, aiming to guarantee the fundamental rights of the Data Subjects involved.

3.4 Data Subject's Rights

Ultrapar and its Businesses shall adopt necessary procedures to ensure compliance with and respect for the Data Subjects rights provided for in the LGPD or other applicable rules and shall also make all reasonable efforts to respond requests filed by Data Subjects in the shortest time possible.

The Ultra Group may reject, if justified, under the terms of applicable legislation, any request from the Data Subject for legal or formal reasons.

3.5 Data Subject Consent Management

Personal Data transactions based on the Data Subject's Consent require appropriate Consent management mechanisms. Should be granted the registration and proof that it was lawful obtained and ensured the possibility of subsequent revocation by the Data Subject, as well as the guarantee that the data is used only for the necessary time and for the purposes approved by the Data Subjects. Data Treatment that does not use Consent as a legal basis must be carried out strictly through the legal bases provided for in the LGPD or applicable legislation and regulations.

3.6 Personal Data Flow Inventory

Ultrapar and its Businesses shall maintain an inventory of all Personal Data Flows, which shall contain, at least:

- Registration date of Personal Data Flow
- Responsible area and person
- Categories of Data Subjects whose Personal Data were collected
- Categories of collected Personal Data
- If Sensitive Personal Data was collected
- If Personal Data from children and adolescents were collected
- Description of purposes of use

- Storage location
- Main systems used
- Third parties which the Personal Data is shared
- Specific security measures for the Treatment
- If there is international transfer of data and, if so, the destination countries and their respective lawful applicable mechanisms for the transfer
- If there is management of the Data Subject's Consent
- Expected term for the retention and disposal of the Personal Data
- Legal basis for the Personal Data Treatment

3.7 Personal Data Flows Evaluation

Each initiative involving Personal Data Treatment shall be assessed from privacy and protection of Personal Data perspective, considering, at least:

- Mapping the Personal Data Flow
- Quantification of the risk of Personal Data Flow in terms of impact and vulnerability
- Adherence and adequacy level Assessment of the Personal Data Flow to the principles and assumptions expressed in the LGPD
- Proportionality test of the Controller's legitimate interest in the Personal Data Flow as described in LGPD
- Need and suitability assessment of the Sensitive Personal Data collection to the conditions described in the LGPD
- Need and suitability assessment of children, adolescents and the elderly Personal Data collection to the conditions described in LGPD
- Need and suitability assessment of sharing Personal Data with third parties under the conditions described in LGPD
- Need and adequacy assessment of the international transfer of Personal Data to the conditions described in LGPD
- Technical and administrative measures assessment applied to the Personal Data Treatment

3.8 Disposal Management

The Ultra Group will keep Personal Data for the necessary time to fulfill the purposes for which they are processed and in accordance with applicable legislation, correctly excluding them in accordance with the law.

The Businesses or Ultrapar IT Area, as applicable, shall ensure that the disposal process is carried out with guarantees against unauthorized access or improper use.

3.9 Sharing of Personal Data

The sharing of Personal Data of the Ultra Group with third parties must be governed by agreements that ensure compliance with the LGPD, establishing responsibilities and protection measures. This sharing must follow the procedures described in this Policy and market's best practices, in addition to occur only to achieve the original purposes of the Treatment, respecting the defined legal basis.

The sharing of Personal Data with third parties must occur, as a rule, solely and exclusively: (i) to fulfill the purpose that justified the collection of Personal Data, within the limits of the legal basis defined for this purpose; and (ii) in accordance with the activity that underpins the relationship with the third party.

In the event of any sharing of Personal Data that goes beyond the conditions established above, such sharing shall be performed in conformity with any of the of the legal basis (requirements for the Personal Data Treatment) established by the LGPD. In this case, the Data Protection Officer shall analyze such sharing and define the necessary measures for the proper sharing.

The hiring instruments for external representatives shall contain provisions for compliance with the guidelines established in this Policy, the use of Personal Data to which they have access for the expressly permitted purposes and in a secure manner, as well as the duty to notify the Ultra Group of incidents.

3.10 International Transfer of Personal Data

The international transfer of Personal Data is only authorized in accordance with the LGPD and shall be supported by a valid legal mechanism, such as the transfer to countries that have been recognized by an adequacy decision issued by the ANPD or through contracts with standard contractual clauses approved by the ANPD, in order to guarantee the protection of Personal Data.

3.11 Information Security Management

All Personal Data must be treated securely, preventing:

- Improper access by unauthorized people; and
- Accidental, improper or unlawful situations of destruction, loss, alteration, communication or any form of inadequate or unlawful Personal Data Treatment.

The Ultra Group will seek to continuously improve its procedures and technological processes to ensure the integrity, confidentiality and availability of the Personal Data Processed.

3.12 Personal Data Incident Management

Ultrapar and its Business shall have process for managing incidents involving Personal Data, containing at least:

- Indication of means and tools for monitoring and detecting incidents
- Assessment and confirmation that the Personal Data under the responsibility of the Businesses has been affected
- Assessment of potential risk or damage to Data Subjects
- Identification of causes
- Definition of measures to reverse and mitigate the effects of any loss
- Definition of measures to prevent recurring incident
- If applicable, communication, to the Data Subject and the ANPD of the incident and the measures taken or to be taken in accordance with the LGPD
- Registration and documentation of incidents, observing the obligations and deadlines provided for in applicable laws and regulations.

Any incident must be immediately handled in accordance with information security incident management procedure policies, rules and procedures adopted by Ultrapar and its Businesses.

4. ROLES AND RESPONSIBILITIES

The Privacy Program ("Program") is a set of persons, processes, procedures, guidelines and culture responsible for the definition, compliance and execution of strategies and actions that lead to the adequate management of privacy controls and protection of Personal Data by the Ultra Group, ensuring the demonstration of responsibility before the ANPD and other public bodies, as well as compliance with laws and regulations on these topics.

The areas, structures and people listed below will be directly involved in the management of the Program and have the following characteristics and responsibilities with regard to the matters covered by this Policy:

4.1 Ultrapar and/or Business Executives

Ultrapar and/or each Business Executives are responsible for:

- Ensure management guidance and support for initiatives aiming to guarantee Personal Data privacy and protection in its respective Businesses
- Support its respective Officer in matters relating to compliance with this Policy
- Ensure the quality and effectiveness of the Policy, proposing revisions and updates to Ultrapar's Executives
- Suggest and monitor the implementation of policies and good practices
- Support the incident management and impact assessment process.

Ultrapar's Executives are also responsible for reporting to the Board of Directors, when necessary, events related to violations of this Policy.

4.2 Personal Data Protection Officer

Appointed by the Executives of each Business, the Officer is responsible for complying with the guidelines of this policy, as well as for maintaining the rules of privacy and protection of Personal Data in operation, taking into account their structure and the complexity of the Personal Data Treatment, in accordance with regulations in force.

All Businesses must publicly disclose, in a clear and objective manner, on their website, the identity and contact information of their Officer.

In relation to its respective Businesses, they shall be mainly responsibilities for:

- Ensure frequent review of all procedures of Personal Data privacy and protection and related policies, submitting them for approval by the Business Executives
- Keep the Business Executives updated on responsibilities, incidents, risks and any mitigating measures related to Personal Data privacy and protection
- Submit relevant topics to the Executives of its respective company or Ultrapar
- Ensure compliance with the Businesses operational practices related to Personal Data Treatment and related procedures and policies, including the adoption of best practices
- Monitor privacy controls and Personal Data protection required by law
- Monitor the regulatory scenario
- Provide due assistance to ensure that contracts or agreements with third parties involving the Personal Data Treatment are in compliance with this Policy

- Ensure the correct preparation of the Data Protection Impact Report, as defined in the LGPD, and the Legitimate Interest Assessment Report whenever applicable
- Ensure that Data Subjects' requirements with respect to the Personal Data handled by the Businesses are answered within the term and with the qualified defined in the LGPD
- Immediately notify the Ultrapar Officer of any notification, subpoena, official letter or other documents issued by the competent authorities (including, but not limited to, the ANPD) related to the privacy and protection procedures of Personal Data and related policies of the Ultra Group or any illegal act related to the privacy and protection of Personal Data involving the Business and/or its Employees
- Cooperate with the proper authorities (including, but not limited to, the ANPD) and act as a point of contact on matters related to the Personal Data Treatment
- Monitor new requirements of conformity, expectations and good practices, submitting proposals to review and update this Policy to the Ultrapar Officer
- Provide continues training on privacy and Personal Data protection for its Business' target audience.

4.3 Ultrapar and/or its Business' IT Area

The IT Area of each Business is responsible for, together with Ultrapar's IT area, when applicable, and Ultrapar's and/or each Business Officer:

- Define minimum security information criteria for Ultrapar or for the Business, as the case may be, aiming at the privacy and protection of Personal Data
- Propose and make available security information tools for the effective privacy and protection of Personal Data for Ultrapar or for the Business, as the case may be
- Track Personal Data Flows where the application of security information techniques or tools are necessary
- Ensure the implementation of security information techniques and tools, aligned with Ultrapar's security information standards to Personal Data Flows where necessary
- Ensure the availability and maintenance of security information tools under its management
- Investigate, from a technical point of view, security incidents and propose remediation and mitigation measures together with the Business or Ultrapar, as the case may be.

5. TRAINING

All target audiences must participate in periodic training on privacy and Personal Data protection. The Officers, together with the human resources areas, must offer training to employees related to the matters covered in this Policy.

6. SANCTIONS

Any disrespect or violation of this Policy will be investigated in compliance with applicable laws, this Policy and other procedures and interests of the Ultra Group, so that appropriate measures can be taken.

To ensure its effectiveness, violations of this Policy may result in the application of disciplinary measures. The application of such measures may be combined with any applicable civil, criminal, labor and administrative fines.

7. OPEN CHANNEL

The Open Channel is available for anyone to ask questions and report on the existence or suspicion of violations of this and other internal policies of the Ultra Group or applicable legislation.

Website: canalabertoultra.com.br

Telephone: 0800 701 7172

Reports may be made anonymously. It is prohibited to engage in any act of threat, intimidation, or retaliation against anyone who [i] reports violations of this Policy and any other applicable policy or law, or [ii] expresses any questions, suspicions, or concerns regarding this matter.

The Channel is operated by an independent company and all reports are duly recorded and forwarded to investigation or supervision by the Risk, Integrity and Audit Department.

8. GLOSSARY

"Treatment Agents" – means, under the terms of the LGPD, Controller and Processor

"Data Subject's Consent" – means the free, informed, specific and unequivocal declaration of consent to the f Personal Data Treatment for any specific purpose.

"Personal Data" – information related to an identified or identifiable natural person. The expression Personal Data used in this Policy, when not explicitly mentioned, will also include Sensitive Personal Data.

"Sensitive Personal Data" – Personal Data about racial or ethnic origin, religious belief, political opinion, membership of a trade union or organization of a religious, philosophical or political nature, relating to health or sexual life, genetic or biometric data.

"Officer" – natural or legal person who, in Ultra Group companies, is responsible for coordinating and ensuring compliance with this Policy, current laws and regulations, and is also the point of contact between the Data Subject and the ANPD.

"*Personal Data Flow"* – Personal Data life cycle, which involves different stages of Personal Data Treatment by Ultrapar and/or the Businesses, such as, for example, collection, storage, sharing and disposal.

"Ultra Group" – Ultrapar Participações SA ("Ultrapar") and the companies controlled by Ultrapar, which are individually treated as "Businesses".

"Ultra Group" – Ultrapar Participações SA ("Ultrapar") and the companies controlled by Ultrapar, which are individually treated as "Businesses".

"Personal Data Treatment" - any operation carried out with Personal Data, with or without technology, including collection, use, storage, deletion, modification, transfer.