CORPORATE POLICY

Global Privacy & Data Protection Policy

1. OBJECTIVE

This Policy establishes the general guidelines for data protection within the corporate environment of Braskem S.A., all its subsidiaries, and Controlled Companies ("Braskem" or "Company"). In carrying out its operations, Braskem collects, handles and stores information, some of which directly or indirectly relates to identifiable individuals (referred to as "Personal Data"), and aims to:

- comply with applicable Data Protection laws and regulations and follow best practices;
- protect the rights of Team Members, customers, suppliers and Partners from the risks of data breaches;
- be transparent about how Braskem processes Personal Data;
- promote the awareness throughout the entire Company related to Data Protection and privacy concerns;

2. SCOPE

This Policy is applicable to Braskem S.A. and all of its Controlled Companies, both in Brazil and abroad and all Team Members who have access to any Personal Data held by or on behalf of Braskem. Additional Procedures can be created in alignment with the Corporate Privacy Officer if required by local law.

All relevant national laws will take precedence in the event that they come into conflict with this Policy.

3. REFERENCES

- Braskem Code of Conduct
- PE 1050-00020 - Global Compliance System Policy
- DE 1090-00001 - Information Security Directive
- DE 1050-00006 - Internal Audit Directive
- General Data Protection Regulation ("GDPR") in Europe
- *Lei Geral de Proteção de Dados ("LGPD") in Brazil*
- *Lei Federal de Proteção de Dados Pessoais em Posse de Particulares ("LFPDPPP") in Mexico.*

4. DUTIES AND RESPONSIBILITIES

Board of Directors ("BD")

- Approve this Policy and updates; and
- To be accountable for the proper use of Personal Data Processing in their activities.

Compliance Committee ("CC")

- Review and recommend approval of this Policy and future updates to the CA;
- Be accountable for the proper use of Personal Data Processing in their activities;
- Define and approve the governance structure for Data Protection and Privacy matters;
- Continuously and effectively monitor the implementation of Privacy initiatives, including events related to Personal Data leakage and the decisions of the Privacy Committee;
- Ensure that the Compliance budget, to be approved annually by the CA, provides the necessary resources for the implementation and management of privacy initiatives;
- Propose to the Privacy Committee the resolution of matters relating to high risk events that are forwarded by it to the CC; and
- Report to the CA about events related to Personal Data leakage and Privacy Committee decisions.

Leaders

- Use properly the Personal Data Processing in the activities of their respective areas;
- Ensure that the requirements of applicable laws and regulations in the country of operation are met, as well as that Team Members adhere to this Policy; and
- Review and update the data mapping, at least once per year, as well as reviewing all substantial changes, with the assistance of the responsible Compliance Area;
- Ensure that when using Consent for the Processing of Personal Data, it is collected and managed in such a way that the option given by the Data Subject is respected and that it provides evidence necessary for submission to the authorities or the Data Subject himself / herself, when necessary.

Corporate Privacy Officer

- Propose to the CC the review and update of this Policy;
- Ensure that Braskem complies with Data Protection laws and regulations, as well as its internal policies and procedures related to the subject;
- Lead and oversee the Privacy and Data Protection strategy and advise during the implementation of adequacy measures to comply with requirements of applicable Data Protection laws and regulation;

- Participate and advise, from a privacy perspective, on global corporate projects that involve Personal Data Processing in order to be in compliance with the requirements of applicable laws and regulations, as well as to ensure privacy by default and design;
- Perform training, awareness and communication programs related to Privacy and Data Protection throughout the Company;
- Develop and maintain Normative Documentation related to Privacy and Data Protection that is within their competence;
- Monitor compliance with internal privacy rules;
- Develop, with the support of the Legal Area, International Data Transfer Agreements, as well as update Personal Data that is transferred between different regions;
- Coordinate the execution of Data Protection Impact Analysis (DPIA);
- Align the definitions and criteria with Data Protection Experts (DPEs) and Local Privacy Influencers periodically;
- Define, review and update privacy notices;
- Perform the privacy program's maturity assessment periodically, identifying improvement opportunities as well as its evolution;
- Follow-up and support the implementation of action plans for correcting gaps of the Privacy Program initiatives;
- Monitor requests from Data Subjects to ensure that they are answered on time and in accordance with the laws and regulations in force in each country and the Company's Normative Documentation;
- Cooperate and communicate with the National Authority for the Protection of Personal Data (Brazil); and
- Ensure that evidence of execution and implementation of privacy initiatives is maintained in accordance with the principle of accountability.

Chief Compliance Officer (CCO) / Regional Compliance Officers (CO)

- Use properly the Personal Data Processing in their activities;
- Administrative support to DPEs and Corporate Privacy Officer with the trainings, awareness campaigns, internal communication, etc.;
- Contract outsourced local Data Protection Officers ("DPOs") and establish the corresponding budgets to carry out their activities, being responsible for the management of such contracts and budgets;
- Approve Local Data Protection Normative Documentation that is within their competence, aligned with this Policy; and
- Report to the CC concerns regarding the implementation of privacy initiatives.

Privacy Committee

- Use properly the Personal Data Processing in their activities;
- Promote adequate knowledge of key stakeholders regarding the importance of Data Protection and internal activities inherent in privacy initiatives;
- Review annually, or in a shorter period when necessary, the privacy initiatives adopted by the Company;
- Discuss and make technical decisions about new Personal Data Processing activities, based on impact reports on Data Protection;
- Decide on technical measures to be applied for high risk events, as well as disciplinary measures;
- Submit to the CC a resolution on technical measures relating to high-risk events that cannot be decided by this Committee; and
- Report to CC about events related to Personal Data leakage and its decisions.

Data Protection Expert (DPE)

- Use properly the Personal Data Processing in their activities;
- Participate and advise, from a privacy perspective, on regional projects that involve Personal Data Processing in order to comply with the requirements of applicable laws and regulations, as well as to ensure privacy by default and design;
- Operationally assist in monitoring compliance with internal rules and maintaining Key Performance Indicators (KPIs) related to Data Protection and Privacy;
- Assist in periodic regional program maturity assessments, identifying improvement opportunities and remaining and/or new gaps;
- Support the regional follow-up and implementation of action plans to correct the Privacy and Data Protection gaps;
- Support the preparation of Data Protection Impact Assessment (DPIA) reports on Data Processing activities within their respective regions, ensuring alignment with the requirements of this Policy;
- Monitor regional requests from Data Subjects to ensure they are answered on time;
- Ensure that evidence of implementation and execution of privacy initiatives is maintained at the regional level (principle of accountability); and
- Coordinate activities and consultations with the DPO that supports the region.

Privacy Influencers

- Use properly the Personal Data Processing in their activities;
- Provide support to the specific Privacy area, based on training received from the Corporate Privacy Officer / DPE;

- Facilitate the collection of evidence on the application of internal rules of privacy and protection of Personal Data; and
- Disseminate the culture of privacy and protection of Personal Data in the respective areas.

Information Security

- Use properly the Personal Data Processing in their activities;
- Analyze data breaches and collect technical evidence;
- Monitor and implement security measures to ensure compliance with applicable laws and regulations;
- Publish privacy notices on Braskem websites and external programs;
- Review and update the Normative Documentation related to Information Security that is within its competence;
- Define and implement Personal Data Breach Incident Procedure and templates;
- Implement technical measures designed to ensure Data Subjects' rights;
- Technical support and analyze new tools and systems focusing on Personal Data exposure; and
- Ensure the application of security measures proportional to the risk generated by the Processing of Personal Data and in line with the expectation of protection of the Data Subject, ensuring the integrity, availability and confidentiality of this information.

Legal

- Use properly the Personal Data Processing in their activities;
- Ensure that contracts that provide services involving the Processing of Personal Data contain privacy clauses appropriate to applicable laws and regulations;
- Legal support in the occurrence of Personal Data breaches;
- Provide legal support and advice in the interpretation of legislation and regulations regarding the Data Protection;
- Assist in the renegotiation of contracts / addendum with suppliers and customers who perform Personal Data Processing; and
- Support interface with National Data Protection Authorities.

All Team Members, including Leaders

- Use properly the Personal Data in their activities;
- Comply with applicable laws and regulations, as well as Braskem Normative Documentation regarding the Data Protection and the application of appropriate IT security measures;

- Report to the Corporate Privacy Officer or their regional representatives the occurrence of any Personal Data or data security incidents, as well as any identified related deficiencies or possible privacy risks; and
- Participate in data protection training activities as directed.

Internal Audit

- Be responsible for the proper use of Personal Data in their activities; and
- Include assessment of compliance with Normative Documentation on Personal Data protection in audit projects and report to the Corporate Privacy Officer and to the "CC" the outcome of these assessments.

5. POLICY

5.1 Data Protection Principles

This section describes the principles of how Personal Data must be collected, handled, stored, disclosed and otherwise processed to meet Braskem's data protection standards and to comply with all applicable laws and regulations in all countries in which Braskem has operations or commercial activities.

5.1.1 Lawfulness, fairness and transparency

The Company processes Personal Data fairly, transparently and according to applicable laws and regulations.

Braskem will only process Personal Data if the purpose of the Processing satisfies one of the permitted lawful grounds, listed below, and the Data Subjects must be informed as to how and why their Personal Data is being processed either upon or before collecting it:

- necessary for the performance of a contract to which a Data Subject is a party;
- required by law or any other regulation to which Braskem is subject to;
- where Braskem has a legitimate interest, in which case such legitimate interest outweighs the rights of the Data Subject and can be communicated by Braskem beforehand;
- necessary for the Data Subject with the regular exercise of rights in judicial, administrative or arbitrary proceedings.

If the Processing of Personal Data does not meet any of the above legal basis, the Company shall obtain the Consent of the Data Subjects for the Processing of their Personal Data, as well as ensure that the

Consent is collected only for a specific purpose and is freely given by the Data Subject in an informed and unambiguous manner. The Company must collect, store and manage all Consent responses in an organized and accessible manner so that Consent evidence can be provided if and when required.

Similarly, the Data Subjects have the right to withdraw their Consent at any time and as easily as provided in the first place.

In some circumstances the Company may also be required to process Sensitive Personal Data. This includes, but is not limited to:

- data related to health or sex life
- biometric data used for the purpose of uniquely identifying a natural person
- data concerning the sexual orientation of an individual
- data concerning the criminal convictions or offences of an individual
- data concerning the racial or ethnic origin, political opinions, religious or philosophical beliefs of an individual
- data concerning trade union membership

Processing of Sensitive Personal Data is prohibited, except in the specific cases described below, where more stringent security requirements must be observed than for other Personal Data:

- where the Processing is necessary for the purpose of, or in connection with, any legal proceedings, obtaining legal advice, or establishing, exercising or defending legal rights;
- when necessary for the regular exercise of Data Subject rights, such as the defense or proposition of legal or administrative or arbitral actions;
- where the Processing is necessary for the purposes of carrying out the obligations and exercising the specific rights of Braskem for employment, social security and social protection purposes;
- to protect the Data Subject's life or physical safety including preventative, occupational medical data or the assessment of the working capacity of an employee;
- for equal opportunity purposes on the basis of substantial public interest necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of difference racial or ethnic origins with a view to enabling such equality to be promoted or maintained;
- where the Data Subject has given their explicit Consent, to the extent permitted by law; or
- processing of Personal Data relating to criminal convictions and offences or related security measures shall be carried out only under the control of official authority or when the Processing is

authorized by local law providing for appropriate safeguards for the rights and freedoms of Data Subjects.

5.1.2 Purpose limitation

The Company shall only collect Personal Data for clearly specified and legitimate purpose(s) and Personal Data must be handled in a way that is compatible with the original purpose for which the data was collected. Personal Data cannot be collected for one reason and then used for another. Any further purposes must be compatible with the original reason for collecting the Personal Data.

5.1.3 Data minimization

The Company may only collect and process Personal Data to the extent necessary for a particular purpose, this is the principle of data minimization. Sharing Personal Data with another area or Company should consider this principle and can only be shared when they have a proper legal basis.

5.1.4 Accuracy (Data Quality)

The Company shall take reasonable steps to ensure that any Personal Data in its possession is kept accurate, up-to-date with the purposes for which it was collected, and the Data Subject must be able to request deletion or correction of any inaccurate or outdated Personal Data.

5.1.5 Storage limitation

The Company must have knowledge of its Processing activities, established retention periods and periodic review processes, and shall not keep Personal Data for longer than is needed for its intended purpose(s), but as long as it is required under applicable laws and regulations retention periods.

5.1.6 Integrity and confidentiality

The Company must ensure that appropriate technical and organizational measures are applied to Personal Data to safeguard it against unauthorized or unlawful Processing, as well as accidental loss, destruction, or damage. The obligation also entails that the Entities process Personal Data in a manner that ensures proper confidentiality. The most common security measures to this end are:

Anonymization: meaning that the Personal Data is rendered anonymous in such a way that the data no longer relates to a directly or indirectly identifiable person. The Anonymization has to be irreversible.

Pseudonymization: is a process through which data no longer directly relates to an identifiable person (e.g. by mentioning his/her name), but is not anonymous, because it is still possible with additional information that is held separately to identify a person.

5.1.7 Accountability

The Company is responsible and shall demonstrate compliance with this Policy, ensuring the implementation of several measures that include, but are not limited to:

- Ensuring that Data Subjects are able to exercise their rights as described in Section 5.5 of this Policy;
- That Braskem should have in place and maintain a number or data records, including:
  - records of Processing activities of Personal Data, including the purposes of such Processing, with whom they share the data and for how long Braskem retains the data;
  - a record of data incidents and data breaches;
- Ensuring that Third Party which are Data Processors are also acting in accordance with this Policy and applicable laws and regulations;
- Ensuring that the Company, when required, properly registers a formal DPO with the applicable Supervisory Authority;
- Ensuring that the Company is complying with all demands and inquiries from any Supervisory Authority Braskem may be subject to.

5.2 Security Policy

5.2.1 Significance of data protection

Data protection is intended to secure the fundamental right of the individual to information self-determination. The Company is committed to taking these requirements and expectations of Data Subjects seriously and to adhering to the applicable data protection laws at national and international levels.

5.2.2 Ensuring data security

The main objectives of data security are confidentiality, integrity and availability as well as authenticity, reliability / non-repudiation and accountability.

5.2.3 Data secrecy obligation

All Team Members with access to Personal Data, are bound by data secrecy/confidentiality when commencing employment with the acceptance of the Company Code of Conduct and Terms of Use.

5.2.4 Data Privacy by Design and Default

When implementing new processes, procedures or systems involving the Processing of Personal Data, Braskem should strive to embed data protection measures that include privacy by design and default.

5.3 Relationship between Controller and Data Processor

Each subsidiary or Controlled Company is the Personal Data Controller in that region or Company, and a nominee is required to ensure that the Personal Data is being treated correctly and in accordance with applicable law in that region. In certain circumstances, a subsidiary or Controlled Company may act as a Processor of another. In such cases, the Processor is required to follow the guidance of who is acting as the Controller.

5.4 Data Transfer Policy

When Personal Data is to be processed in countries other than where it was collected, the international data transfer legislation and regulations of each country must be observed. The Company must ensure the existence and validity of international data transfer agreements.

5.5 Rights of Data Subjects

The Company is committed to Data Subjects' rights, these rights include:

- to be informed, at the time the Personal Data is collect, as to how their data should be processed;
- to obtain information regarding the Processing of their Personal Data and access to the Personal Data which Braskem holds about them;
- to request that Braskem correct their Personal Data if it is inaccurate or incomplete;
- to request that Braskem erases, blocks and/or anonymizes their Personal Data in certain circumstances ('right to be forgotten'). This may include, but is not limited to circumstances in which it is no longer necessary for Braskem to retain their Personal Data for the purposes for which they were collected;
- to request that Braskem restricts the Processing of their Personal Data in certain circumstances;
- to object to the Processing, if the Processing is based on legitimate interests;
- to withdraw Consent at any time if Processing of Personal Data was based on the Consent of the individual for a specific purpose;
- to port the Personal Data to another service or product provider upon express request in certain circumstances;
- to review decisions made solely on the basis of Automated Processing of Personal Data; and
- to lodge a complaint with Braskem's Data Protection Officer or with the applicable data protection authority, if the Data Subject has reason to assume that any of their data protection rights have been infringed by Braskem.

5.6 Third Party Service Providers

Service providers who process Personal Data under the instructions of the Company, its affiliates and subsidiaries are subject to the obligations imposed on Processors in accordance with applicable data protection laws and regulations. The Company shall incorporate in writing into the service agreement the Privacy clauses governing the Processing of Personal Data with Third Parties. These clauses should specify that the Processor may process Personal Data only when requested through formal Company instructions and also require the Third Party Data Processor to implement security measures as well as appropriate technical and organizational controls to ensure the confidentiality and security of the Personal Data.

In cases where the service provider is located outside the country in which the Personal Data was collected, standard contractual clauses should be included in the Personal Data protection contract as an Annex to ensure that the necessary safeguards required by applicable laws and regulations applicable data protection measures are implemented.

5.7 Data Breach Management

All incidents and potential data breaches must be reported to the Corporate Privacy Officer and / or DPE in each region. All Members should be aware of their personal responsibility to escalate potential issues as well as suspicious or actual data breaches as soon as they identify them. The moment an actual incident or violation is discovered, it is essential that data breach incident are informed in a timely manner.

Data Breaches include, but are not limited to, any loss, deletion, theft or unauthorized access of Personal Data controlled or processed by Braskem.

5.8 Internal data protection audits

The Company shall ensure that periodic audits are in place to determine whether the initiatives, measures, processes, precautions and other activities within the Data protection management are in compliance with applicable laws and regulations, legal requirements, internal organizational Documentation and whether they are effectively implemented and maintained, meeting requirements and objectives.

At the same time, as foreseen by the Global Internal Audit Directive, the Data Subject should be evaluated at appropriate intervals and in accordance with the existing risks. If the risks are relevant the Internal Audit should include specific independent review in the annual internal audit plan.

6. MISCELLANEOUS

Team Members are responsible to know and understand all Normative Documents applicable to them. Similarly, Leaders are responsible to ensure that all of their Team Members understand and abide by the applicable Normative Documents of the Company.

Team Members who have questions or concerns about this Policy, including the scope, terms, or obligations of this Document, should contact their respective Leaders and, if necessary, Braskem's Risk Management / Compliance Area.

Violations of any of the Company's Normative Documentation can result in serious consequences to Braskem and the Team Members involved. Therefore, failure to follow this Policy or to report a known violation thereof may result in disciplinary action for any Team Member(s) involved.

If any Braskem Team Member and/or Third party becomes aware of possible illegal or unethical conduct, including potential violations of Applicable Anti-Corruption Laws and/or Braskem's Normative Documents, including this Document, the Team Member and/or Third Party must immediately report the possible violation to the Ethics Line Channel or the Compliance Area. All Leaders must continually encourage their Team Members to report violations to the Ethics Line Channel.

Nothing in Braskem's Normative Documents, including this Document, prohibits Team Members or Third Parties from reporting any concern or illegal activity to the appropriate regulatory authorities.

Braskem's Board of Directors

November 14, 2019

DEFINITIONS

Below are the definitions of the capitalized terms utilized in this Policy.

"Anonymization": Processes and techniques by which data loses the possibility of direct or indirect association with an individual. Anonymous data is not considered Personal Data.

"**Board of Directors", "BD" or "BD-BAK":** Board of Director of Braskem S.A.

"**Braskem**": Braskem S.A. and all of its Subsidiaries in Brazil and abroad.

"**Chief Compliance Officer**" or "**CCO**": The senior executive leading the Compliance function area of the Company; known in Brazil as R-Conformidade and abroad as Braskem´s Chief Compliance Officer ("CCO").

"**Compliance"** or **"Compliance Area**": the relevant local Compliance Officer and its Team Members.

"**Compliance Committee**" or "**CC-BAK**": Compliance Committee, in support of Braskem S.A's Board of Directors.

"**Consent**": Free, informed and unambiguous statement by which the Data Subject agrees to the Treatment of his Personal Data for a particular purpose.

"**Controller**": Legal entity, governed by public or private law, who is responsible for decisions regarding the Processing of Personal Data.

"**Controlled Company(ies)**" or "**Controlled Entity(ies)**" or "**Entity(ies)**" or "**Subsidiaries**": Companies in which Braskem, either directly or through other Controlled Companies, holds rights that assure it, on a permanent basis, prevalence in corporate deliberations and the power to elect the majority of managers or directors.

"**Corporate Privacy Officer**" is responsible for overseeing the data protection strategy and implementing measures to ensure compliance with external data protection requirements as set by local laws. The Corporate Privacy Officer should maintain independence from management in order to safeguard the rights of Data Subjects, whose Personal Data is processed by the Company, as well as advocate for Data Protection standards beyond the minimum requirements as set by laws and regulations.

"**Data Processing**": Any operation or set of operations performed on Personal Data or Personal Data sets, by automated or non-automated means, such as collection, registration, organization, structuring, conservation, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or any other form of provision, comparison or interconnection, limitation, deletion or destruction.

"Data Protection Expert (DPE)": Local / regional Data Protection specialist, with the duties and responsibilities of a DPO, but with little or no decision-making power.

"Data Protection Officer (DPO)": the individual appointed as formal data protection officer as meant in the GDPR for a certain territory. The DPO could be internal or outsourced.

"Data Subject (s)": An identified or identifiable natural person to whom a specific Personal Data refers.

"GDPR": Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

"**Global Compliance System Policy**": Braskem's Global Corporate Compliance Policy, dated 17 May 2018 or as may be amended from time to time.

"**Information Security**": The Information Security Team is responsible for protecting the integrity, availability and confidentiality of IT systems and shall take suitable measures to achieve this. He/she is the contact person for the Corporate Privacy Officer and the responsible Compliance Area for all questions regarding technical and organizational measures.

"**Information Security Directive**": Braskem's global corporate guidelines regarding Information Security, dated 16 November 2017 or as may be amended from time to time.

"**Leader(s)**": Team Members leading a team.

"Legal": Area responsible for managing the agreements and contracts between the Company and Third Parties.

"**LFPDPPP**": Mexican Law passed in 2010. Federal Personal Data Protection Act in Private Positions, as its notes apply to all natural or legal persons who conduct or process Personal Data in the course of their activities.

"**LGPD**": Brazilian Legislation No. 13.709 / 2018, commonly known as the General Personal Data Protection Act, which regulates Personal Data Processing activities and also amends Articles 7 and 16 of the Internet Civil Framework.

"**LN Braskem**": Braskem Business Leader; Braskem's Global Leader, known in Brazil as LN Braskem and abroad as Braskem's Chief Executive Officer (CEO).

"Normative Document(s)" or **"Normative Documentation"**: A formal Braskem Document that provides content about corporate decisions, rules and orientations that are vital for directing the work of Braskem with legitimacy, traceability and applicability and must be observed and applied by a certain defined universe of Team Members.

"**Program of Action (PA)**": Agreement between the Leader and the Leader that defines the Member's responsibilities and the Leader's commitment to follow-up, evaluate and make a decision regarding the Leader according to their performance.

"**Personal Data**" means any information relating to an identified or identifiable natural person (Data Subject); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

"**Policy**": this Data Protection Policy of Braskem.

"**Privacy Committee**": Global multidisciplinary advisory committee comprised of Leaders from Legal, Compliance, Risk Management, Information Security and P&O to discuss relevant and critical Information Security and Data Privacy topics.

"**Privacy Influencer(s)**": Focal point of commercial offices, or areas that require specific attention, to facilitate contact with the Privacy Leader and / or DPEs to the area and vice versa. The Influencer also serves as a facilitator of training and privacy communications in areas with greater access to Personal Data. The Influencer has no decision making power.

"**Processor**" or "**Operator**": Natural or legal person, governed by public or private law, who performs the Processing of Personal Data on behalf of the Controller.

"**Pseudoanonymization**": Processes and techniques by which data cannot be associated with an individual without another data set acting as a key. Pseudoanonymized data is considered Personal Data in view of the possibility of associating this data with a natural person but is considered to be more secure.

"**Sensitive Personal Data**": Any Personal Data that may generate any kind of discrimination, such as data on racial or ethnic origin, religious belief, political opinion, union membership, or character organization, religious, philosophical or political, health or sex life data, genetic or biometric data.

"**Team Member(s)**": Braskem's employees at all levels, including officers, board members, directors, interns and apprentices (as applicable by geographical location) and also contractors and freelancers.

"**Third Party(ies)**" or "**Partner(s)**": Any individual or legal entity acting in the name, interest or for the benefit of Braskem, rendering services or providing other goods, as well as Trading Partners providing services to Braskem, directly related to obtaining , retention or facilitation of business, or for conducting Braskem business, including without limitation any distributors, agents, brokers, forwarders, intermediaries, supply chain Partners, consultants, resellers, contractors and other professional service providers.