CORPORATE POLICY

GLOBAL DATA PRIVACY & PROTECTION POLICY

1. OBJECTIVE

This Policy establishes the guidelines for data protection within the corporate environment of Braskem S.A., all its subsidiaries, Controlled Companies, and Controlled Companies with Participation of External Partners ("Braskem" or "Company"). In carrying out its operations, Braskem collects, processes and stores information that could be related to identified or identifiable individuals (henceforth referred to as "Personal Data") in order to

- comply with applicable data protection laws and regulations and follow the best practices;
- protect the rights of Team Members, customers and Third Parties from the risks of Personal Data breaches;
- be transparent about how Braskem processes Personal Data; and
- raise awareness throughout the Company on data privacy and protection.

2. SCOPE

This Policy applies to Braskem S.A., all its Controlled Companies and Controlled Companies with Participation of External Partners, and all Team Members who have access to any Personal Data held by or on behalf of Braskem. Additional procedures and work instructions may be formulated in agreement with the Corporate Privacy Leader or another Team Member responsible for data protection, if required by local law. Controlled Companies with Participation of External Partners may approve their own policies in compliance with governance requirements and local laws, provided these comply with Braskem's governance and this Policy and there is no contradiction with its guidelines.

In case of conflict between any applicable local laws and this Policy, the applicable local laws will prevail.

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

4. DUTIES AND RESPONSIBILITIES

Board of Directors (Board)

- Approve this Policy and amendments.

Compliance & Statutory Audit Committee (CCAE)

- Monitor and follow up on compliance with the directives established in the Company's Policies on Personal Data privacy and protection;
- Evaluate, prior to deliberation by the Board, matters of the Compliance Area, related to data privacy and protection, which may be submitted to the Board by those responsible for compliance and risks, internal controls and internal audit;
- Evaluate and permanently and effectively monitor the Global Privacy & Data Protection Policy;
- Propose to the Board the creation of complementary policies and updates to the Global Privacy & Data Protection Policy;
- Monitor the quality and integrity of work and adequacy of activities of the Personal Data Protection and Privacy Area;
- Permanently and effectively monitor the implementation of the Company's Personal Data protection and privacy initiatives, including events related to Personal Data breaches and the decisions of the Privacy Committee;
- Submit to the Board annually, the CCAE agenda for the fiscal year, including the compliance area's budget compatible with the scope of its activities and needs, ensuring that the resources necessary for implementing and managing the Data Protection and Privacy Program initiatives are covered;
- Evaluate privacy events that are forwarded by the Privacy Committee to CCAE and propose its forwarding as applicable; and
- Report material events related to Personal Data Breaches to the Board of Directors and the appropriate measures taken by the Company.

Leaders

- Ensure, within the scope limits of their activities, that the requirements of law and regulations applicable in the country where they operate are met, and that Team Members under their leadership act in accordance with this Policy;
- Provide the information required by the Privacy Area so that the mapping of Personal Data is periodically reviewed and updated, and also analyze any significant changes, with assistance from the Data Protection Expert (DPE) responsible; and

- Ensure that, when using the Consent for Personal Data Processing, that it is obtained, registered and managed such that the Data Subject's choice is respected and that it generates the necessary evidence for submission to authorities or to the Personal Data Subject, when required.

Corporate Privacy Leader

- Propose to CCAE, revisions and updates to this Policy as appropriate and in alignment with the CCO;
- Ensure that Braskem complies with data protection laws, regulations, as well as internal Policies and procedures;
- Lead and supervise the corporate data protection and privacy strategy and provide guidance during the implementation of the measures required to comply with applicable data protection laws and regulations;
- Participate and guide global corporate projects involving Personal Data Processing;
- Conduct training, awareness and communication programs on data protection and privacy;
- Prepare and keep updated Normative Documents related to data protection and privacy that are within the scope of their responsibilities;
- Monitor the compliance with internal privacy standards;
- Implement, when necessary and with support from Legal Area, international data transfer agreements;
- Coordinate the enforcement of Data Protection Impact Assessment (DPIA);
- Periodically align the targets and key points of attention related to Personal Data protection issues with the DPEs;
- Define, review and update privacy notices;
- Perform the Data Protection and Privacy Program's maturity assessment periodically;
- Monitor and support the implementation of action plans for correcting gaps in Data Protection Privacy Program initiatives;
- Follow up on requests from Personal Data Subjects to ensure that these are responded to promptly and in accordance with applicable laws and regulations in each country and the Company's Normative Documents;
- Report Personal Data Breaches to the Privacy Committee and to CCAE, and the measures taken to mitigate exposure;
- Cooperate and communicate with the Personal Data protection authorities of each country when required by applicable laws and regulations, including in the context of Personal Data Breaches; and

- Organize initiatives to raise awareness on data protection and request the CCO to report to the CCAE issues related to the implementation of Personal Data protection initiatives, when necessary.

Chief Compliance Officer ("CCO")

- Propose and submit annually its Action Program for approval by the CCAE, with the respective targets and budget, including the necessary resources for the Data Protection and Privacy Program;
- Recommend the preparation, improvement or revision of the Company's Normative Documents, including this Global Privacy & Data Protection Policy;
- Provide administrative support to Data Protection Experts ("DPEs") and the Corporate Privacy Leader in the form of training, awareness campaigns, internal communications, etc.;
- Hire, if necessary and permitted by local laws, local outsourced Data Protection Officers (DPOs) and establish the corresponding budgets;
- Approve, before submission to competent bodies, the proposals for Local Normative Documents on Data Protection, in compliance with this Policy; and
- Report to CCAE issues related to the implementation of data protection initiatives whenever necessary or when required by the Corporate Privacy Leader.

Privacy Committee (for Brazil matters)

- Provide adequate knowledge to key stakeholders on the importance of data protection and internal activities inherent to privacy initiatives;
- Review annually, or less frequently when necessary, the Company's data protection initiatives;
- Discuss and take decisions on new Personal Data Processing activities based on data protection impact assessments;
- Decide on the technical measures to be adopted for high-risk events;
- Submit to CCAE a resolution on technical measures related to high-risk events that cannot be decided by the Committee; and
- Report to CCAE material events related to Personal Data Breaches and its decisions.

Data Protection Expert (DPE)

- Participate and guide regional projects involving Personal Data Processing;
- Provide operational assistance in monitoring compliance with internal standards and maintenance of Key Performance Indicators (KPIs) related to data protection;
- Assist in conducting periodical regional program maturity assessments and identify opportunities for improvement;

- Support the monitoring and regional implementation of action plans to correct data protection and privacy gaps;
- Support the development of Data Protection Impact Analysis (DPIA) on the Personal Data Processing activities in their respective regions, ensuring alignment with the requirements of this Policy;
- Monitor the regional requests of Personal Data Subjects to ensure that they are answered on time, in accordance with applicable laws and regulations of each country;
- Ensure the maintenance of evidence of implementation and execution of data protection initiatives at the regional level (principle of accountability);
- Coordinate activities and consultations with the Corporate Privacy Leader who supports the region and monitors the budget;
- Provide support, together with the Legal Area, on issues related to Personal Data protection clauses and/or additional documentation, when necessary;
- Provide support in interfacing with local Personal Data protection authorities;
- Review and update the mapping of Personal Data periodically and analyze all significant changes with support from Leaders;
- Inform the Corporate Privacy Leader of any reasonable suspicion of a Personal Data breach; and
- Provide assistance to the Corporate Privacy Leader in cases of Personal Data Breaches.

Information Security (IS)

- Analyze suspected or confirmed Personal Data Breaches and collect technical evidence;
- Monitor and implement security measures to safeguard Personal Data security and prevent Personal Data Breaches involving Personal Data, besides ensuring compliance with applicable laws and regulations;
- Support other areas of the Company in investigating and remedying Personal Data Breaches, when requested;
- Publish privacy notices on the websites of Braskem and external programs;
- Review and keep updated the Normative Documents on Information Security;
- Define and implement a Personal Data Breach Procedure and templates detailing the measures taken to manage and respond to a Personal Data Breach and mitigate the damages arising from it;
- Implement technical measures to guarantee the rights of Personal Data Subjects, such as right of access, rectification, deletion, portability of Personal Data, etc.;
- Provide technical support and analyze new tools and systems focused on the exposure of Personal Data;

- Ensure the application of security measures proportional to the risk generated by Personal Data Processing and in line with the protection expected by Personal Data Subjects, guaranteeing the integrity, availability and confidentiality of such information.

Legal Area

- Formulate Personal Data Protection and provicy clauses in line with applicable laws and regulations for inclusion in agreements signed by the Company, when applicable;
- Provide legal support in case of Personal Data breaches, when requested;
- Provide legal support in the interpretation of laws and regulations related to data protection and privacy;
- Support the managers of respective agreements in the renegotiation of contracts/amendments with suppliers and customers engaged in Personal Data Processing;
- Comply with the requests of inspection authorities, together with the Corporate Privacy Leader; and
- Conduct and manage legal issues, as per the Normative Documents in force at the Company.

Shared Services

- Receive and distribute to the team responsible, through the Document Distribution System, any and all documents, such as notifications, subpoenas, summons, official letters and correspondence, under pursuant to the Normative Documents in force at the Company.

All Team Members of the Company, including the Leaders

- Process Personal Data appropriately while exercising their functions;
- Comply with applicable Personal Data Protection and Privacy laws and regulations, as well as the Company's Normative Documents on data protection and the application of adequate IT security measures;
- Report to the Corporate Privacy Leader or their regional representatives any Personal Data Breach, as well as any related deficiencies or potential privacy risks; and
- Periodically participate in training activities on data protection as required.

Internal Audit

- Include an assessment of adherence to Normative Documents related to the protection of Personal Data in audit projects and report the findings of such assessments to the Corporate Privacy Leader, CCO and CCAE.

5. POLICY

5.1 Personal Data Protection Principles

This section describes the principles that must be observed during the collection, storage, disclosure and Processing of Personal Data in order to comply with the Personal Data protection rules applicable to Braskem in all the countries where the Company operates or has commercial activities.

5.1.1 Legality, justice, transparency and non-discrimination

The Company treats Personal Data fairly, transparently and in compliance with applicable laws and regulations. The Processing of Personal Data for discriminatory purposes that are unlawful or inappropriate is prohibited.

The Company only Processes Personal Data that fits into at least one of the legal hypotheses permitted, as shown in the examples, provided such legal hypotheses are established in the Personal Data Protection and privacy protection laws and regulations applicable to Braskem and that the Personal Data Subjects are informed how and why their Personal Data is being processed before or during its collection:

- When Processing is necessary for the performance of an agreement to which the Personal Data Subject is a party or to execute procedures requested by the Personal Data Subject before the formalization of an agreement;
- When required to comply with laws or regulations applicable to Braskem;
- When Braskem has a legitimate interest involved, provided such legitimate interest prevails over the fundamental rights and freedoms of the Data Subject;
- When required for the regular exercise of rights in legal, administrative or arbitration proceedings or in agreements;
- When required for the performance of an agreement or for preliminary procedures related to an agreement to which the Personal Data Subject is a party, at the request of the Personal Data Subject;
- When required to protect the life or physical integrity of the Data Subject or Third Party; and
- For credit protection.

When the Personal Data Processing does not fit the legal hypotheses above, the Company must obtain the Consent of Data Subjects for Processing their Personal Data, ensuring that the Consent is obtained only for a specific purpose and freely granted by the Personal 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 the evidence of Consent can be provided when required.

Similarly, Personal Data Subjects can withdraw their Consent at any time and with the same ease as it was provided.

In some circumstances, the Company may also be required to process Sensitive Personal Data. Depending on local laws and regulations, this may include, but is not limited to:

- Data related to health or sex life;
- Biometric data used exclusively to identify an individual;
- Data about an individual's sexual orientation;
- Data about an individual's crimes or criminal convictions;
- Data about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs; and
- Data about union membership.

Sensitive Personal Data Processing must be made only when permitted by law, which may vary according to local laws and regulations. Below is a list of situations when Sensitive Personal Data may be processed pursuant to the laws of some regions where Braskem operates. In any case, when carrying out Sensitive Personal Data Processing, the most rigorous security requirements must be followed:

- When Processing is required in connection with legal proceedings to obtain legal assistance or to establish, exercise or defend legal rights;
- When necessary for the regular exercise of the rights of the Personal Data Subject, as a defense or to file legal, administrative or arbitration proceedings;
- When Processing is necessary to meet obligations and to exercise the specific rights of Braskem for employment, social security and social protection purposes;
- To protect the life or physical integrity of the Personal Data Subject, including medical data for preventive and work-related purposes or to evaluate the work capacity of a Team Member;
- For the purpose of equal opportunities, and based on huge public interest required to identify or check the existence or absence of equal opportunities or treatment of persons of different racial or ethnic origins, in order to ensure this equality;
- When the Personal Data Subject provided their express Consent pursuant to applicable laws and regulations;
- Personal Data Processing related to criminal convictions and offenses or related security measures will be carried out only under the control of a public authority or when the Processing is authorized by local laws that establish adequate protections for the rights and freedoms of Personal Data Subjects.

5.1.2 Limitation and suitability of purpose

The Company may collect Personal Data only for clearly specified and legitimate purposes. Personal Data will be processed in a manner compatible with the original purpose informed to the Personal Data Subject and for which the Personal Data was collected, as well as in accordance with the context of the Processing.

5.1.3 Principle of necessity (data minimization)

According to the principle of necessity, the Company may collect and process Personal Data only to the extent necessary to achieve a specific purpose. This principle also applies to the sharing of Personal Data with another Area or Controlled Company of Braskem, situation in which it can be shared only with adequate legal justification.

5.1.4 Accuracy (data quality)

The Company must take reasonable measures to ensure that any Personal Data in its possession is maintained accurately and updated for the purposes for which it was collected, and the Personal Data Subject must be able to request the correction of any inaccurate or outdated data.

5.1.5 Storage limitation

The Company must be aware of its Processing activities, and define the periods for retention and periodic revision. It cannot retain Personal Data for longer than required to meet the intended purposes.

5.1.6 Integrity and confidentiality

The Company must ensure that appropriate technical and organizational measures are applied to Personal Data to protect it against unauthorized or illegal Processing, as well as against accidental loss, destruction, alteration, disclosure or damage. Also, the Company should process Personal Data in such a manner as to guarantee due confidentiality.

5.1.7 Accountability

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

- Ensuring that Personal Data Subjects can exercise their rights in accordance with applicable law, as per the non-exhaustive list of examples described in Section 5.5 of this Policy;
- Maintaining records of Personal Data, including:
    - records of Personal Data Processing activities, describing the purposes for such Processing, with whom Personal Data is shared and for how long Braskem retains the Personal Data.
    - Plan and Personal Data Incident Response Plan Procedure and records of each incident.

- Ensuring that Third Parties who are Data Processors also act in accordance with applicable laws and regulations.
- Ensuring that the Company, when required, properly files a formal DPO with the applicable Personal Data protection authority.
- Ensuring that the Company complies with all the requirements and requests from any Personal Data protection authority that Braskem is subject to.

5.2 Security Standards

The Company adopts technical, administrative, security and privacy measures to protect Personal Data against any unauthorized or accidental access or any illegal destruction, loss, changes, communication or any kind of inappropriate or illegal Processing, as per the Information Security Directive of Braskem, through security and privacy measures by design and by default.

5.3 Relationship between Personal Data Controller and Processor

Each Controlled Company is responsible for the Personal Data processed by it. When required, and as determined by the Corporate Privacy Leader, it must nominate a person responsible for ensuring that such Personal Data is treated correctly and according to the laws and regulations applicable in that region.

5.4 International Transfer of Personal Data

The Company may share Personal Data with all its Controlled Companies for legitimate corporate purposes and for general business management, as permitted by applicable laws and regulations.

The Company can also share Personal Data with Third Parties while carrying out its business activities, in compliance with its legal or regulatory obligations, in response to court orders or requests from public authorities, for its defense in legal, administrative and arbitration proceedings, for internal or external audit or in the event of sale, assignment or transfer of its business, fully or partially, as permitted by applicable laws and regulations.

When Personal Data is processed in countries other than where it was collected, the applicable international laws and regulations applicable to the transfer of Personal Data in each country must be observed.

The Company must ensure the maintenance of internal procedures to ensure compliance with applicable data protection laws in order to protect the Personal Data regardless of where it is located. Braskem must also ensure that the country where the information is transferred has a minimum standard of Personal Data protection in compliance with this Policy, as well as the laws and regulations.

When the Company transfers Personal Data to a country whose laws do not guarantee adequate data protection, it must implement adequate Personal Data protection mechanisms and ensure that such Personal Data transfers comply with this Policy and local laws.

For Personal Data transfers within the Braskem group, companies in the group have signed agreements for transfer of Personal Data and they can carry out international transfers only in cases established the applicable laws.

5.5 Rights of Data Subjects

The Company is committed to respecting the rights of Data Subjects in accordance with applicable local laws and regulations. These rights may include, but are not limited to:

- Being informed, at the time Personal Data is collected, on how their Personal Data will be processed;
- Obtaining information about the Processing of their Personal Data and access to their Personal Data held by Braskem;
- Requesting Braskem to correct their Personal Data if it is inaccurate, outdated or incomplete;
- Requesting Braskem to delete, block and/or anonymize their Personal Data in certain circumstances. This could include, but is not limited to, circumstances where it is no longer necessary for the Company to retain their Personal Data for the purposes for which it was collected;
- Requesting Braskem to restrict their Personal Data Processing in certain circumstances;
- Withdrawing their Consent at any time, if Personal Data Processing is based on the individual's Consent for a specific purpose;
- Transferring the Personal Data to another service provider or product suppliers upon express request in certain circumstances;
- Reviewing the decisions taken solely on the basis of Automated Personal Data Processing; and
- Filing a complaint with the DPO of Braskem or the competent Personal Data Protection Authority, if the Data Subject believes that their Personal Data protection rights have been violated.

Data Subjects can exercise their rights by sending a request to data_protection@braskem.com.

5.6 Third-Party Service Providers

Third-party service providers that process Personal Data as per instructions from Braskem and its Controlled Companies are subject to the obligations imposed on Processors in accordance with applicable Personal Data protection laws and regulations. The Company must include in service provision agreements, the privacy clauses applicable to Personal Data Processing with Third Parties.

5.7 Management of Personal Data Breaches

All potential Personal Data Breaches must be reported to the Corporate Privacy Leader and/or DPE of each region. All Team Members must be aware of their personal responsibility to escalate potential issues and to report Breaches or suspected Personal Data Breaches immediately after identifying them. It is of critical importance that a Personal Data Breach is reported promptly when discovered.

Personal Data Breaches include, but are not limited to, any loss, deletion, theft or unauthorized access to Personal Data processed by Braskem. For more information, see the Personal Data Incident Response Plan Procedure.

5.8 Internal Personal Data Protection Audit

The Company must ensure that periodic audits to confirm that the initiatives, measures, processes, precautions and other tasks related to the management of Personal Data protection are conducted in accordance with applicable laws and regulations, legal requirements and internal Normative Documents, whether they are being effectively implemented and maintained and whether they effectively meet the requirements and objectives defined.

Moreover, as established in the Global Internal Audit Directive, Personal Data Processing must be evaluated in an adequate frequency and in accordance with existing risks. If the risks are material, Internal Audit must include a specific independent review in the annual internal audit plan.

6. GENERAL PROVISIONS

Team Members are responsible for learning and understanding all Normative Documents that apply to them. Similarly, Leaders are responsible for ensuring that all Team Members understand and observe the Normative Documents applicable to the Company.

Team Members who have questions or doubts about this Policy, including its scope, terms or obligations, must contact their respective Leaders and, if necessary, Braskem's Compliance Area.

Violations of any Normative Documents of the Company may result in severe consequences for Braskem and the Team Members involved. Therefore, failure to comply with this Policy or to report a known violation of this Policy may result in disciplinary action for any Team Member involved.

If any Team Member and/or Third Party becomes aware of a possible illegal or unethical conduct, including potential violations of applicable Anti-Corruption Laws and/or Braskem's Normative Documents, including this Policy, they must immediately report such possible violation to the Ethics

Line or the Compliance Area of the Company. All Leaders must continuously encourage their Team Members to report violations to the Ethics Line Channel.

No rule in Braskem's Normative Documents, including this Policy, will prohibit Team Members or Third Parties from reporting any illegal activity or issue to the competent regulatory authorities.

Board of Directors of Braskem

June 22, 2022

DEFINITIONS

Bellow are the definitions of the capitalized terms used in this Policy.

Anonymization: Use of reasonable technical means available at the time of Processing by which data loses the possibility of being associated, directly or indirectly, with an individual. Anonymous data is not considered Personal Data.

"**Board of Directors**" or "**Board**": Board of Directors of Braskem S.A.

"Braskem" or "Company": Braskem S.A. and all of its Controlled Companies and Controlled Companies with Participation of External Partners in Brazil and abroad.

"Chief Compliance Officer" or **"CCO":** The senior executive leading the Compliance function area of the Company, know in Brazil as R-Conformidade and abroad as Braskem´s Chief Compliance Officer ("CCO"). (não está na versão em português, conferir com o pessoal de GC).

"Compliance" or **"Compliance Area"**: Area responsible for Compliance, and its Team Members.

"**Compliance & Statutory Audit Committee"** or "**CCAE**": Compliance and Audit Committee that advises the Board of Directors of Braskem S.A.

"**Consent**": Free, informed and unambiguous statement by which the Data Subject agrees to the Processing of their Personal Data for a specific purpose.

"**Controlled Company(ies)**": Companies in which Braskem, directly or through other Controlled Companies, holds rights that permanently ensure it prevails in corporate resolutions and the power to elect the majority of managers or directors.

"Controlled Company(ies) with Participation of External Partners": Companies in which Braskem, directly or through other Controlled Companies, holds rights that permanently ensure it prevails in corporate resolutions and the power to elect the majority of managers or directors, and in which a portion of the capital stock is held by third parties.

"**Controller**": Natural person or legal entity, governed by public or private law, responsible for decisions regarding Personal Data Processing.

"**Corporate Privacy Leader"**: Responsible for supervising the data protection strategy and for implementing measures to ensure compliance with external data protection requirements defined in local laws. The Corporate Privacy Leader is deployed in the Compliance Area in order to preserve its autonomy in relation to the management, protect the rights of Data Subjects whose Personal Data are

processed by the Company, and act as the defender of data protection standards over and above the minimum requirements established in laws and regulations.

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

"**Data Protection Officer" (DPO)**: Individual designated as formally responsible for data protection for a certain territory. The DPO could be a Team Member or third party.

"**Data Subjects**": Identified or identifiable natural person to whom certain Personal Data refers to.

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

"**Information Security"** or "**IS**": The Information Security team is responsible for protecting the integrity, availability and confidentiality of IT systems and for implementing adequate measures to achieve this. The Leader of this area is the contact person for the Corporate Privacy Leader and is responsible for issues related to technical and organizational measures in the area.

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

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

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

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

"**Personal Data"**: Any information relating to an identified or identifiable natural person (Data Subject); an identifiable person is one who can be identified, directly or indirectly, by reference to an identifier such as a name, identification number, location, online identifier or one or more factors relating to their physical, physiological, genetic or mental identity or their economic, cultural or social status.

"**Personal Data Breach(es)**": Loss or misuse (by any means) of Personal Data, including, but not limited to, any unauthorized access or disclosure to unauthorized individuals; Unauthorized or illegal processing, corruption, modification, transfer, sale or rental of Personal Data; or any other act or omission that compromises the security, confidentiality or integrity of Personal Data.

"Policy": This Global Privacy & Data Protection Policy of Braskem.

"**Privacy Committee"**: Global multidisciplinary advisory committee coordinated by the Privacy leader and formed by Leaders from the Legal, Compliance, Information Security and P&O Areas to discuss critical topics related to Information Security and Data Privacy.

"**Processing"**: Any operation or set of operations carried out with Personal Data or sets of Personal Data, whether or not through automated means, such as collection, registration, organization, structuring, conservation, adaptation or alteration, recovery, query, use, disclosure by transmission, dissemination or any other form of provision, comparison or interconnection, limitation, exclusion or destruction.

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

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

"**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 due to the possibility of associating this data with a natural person but is considered more secure.

"**Sensitive Personal Data"**: Any Personal Data that may create any type of discrimination, such as data about racial or ethnic origin, religious beliefs, political opinions, membership of labor union or any religious, philosophical or political organization, data relating to health or sexual life, or genetic or biometric data.

"Team Member(s)": Employees working at Braskem at all levels, including executives, directors, executive officers, interns and apprentices (as applicable in different geographical locations).

"**Third Party(ies)**": Any natural person or legal entity acting on behalf of, in the interest or for the benefit of Braskem, providing services or supplying other products, as well as commercial partners that provide services to Braskem directly related to obtaining, retaining or facilitating business or for conducting Braskem's affairs, including, but not limited to, any distributors, agents, brokers, forwarding agents, intermediaries, supply chain partners, consultants, resellers, contractors and other professional service providers.