Braskem Idesa

POLÍTICA CORPORATIVA

PE 1050-00025-Privacidad y Protección de Datos Personales

1. OBJETIVO

Esta Política establece las orientaciones generales para la protección de los datos personales dentro del ambiente corporativo, debido a que, en la ejecución habitual de sus operaciones, Braskem Idesa, recolecta, trata y almacena información relacionada con personas físicas identificadas y/o identificables ("Datos Personales"). Esta política busca:

- adherirse a los requisitos de las leyes y regulaciones de protección de Datos Personales y seguir las mejores prácticas;
- proteger los derechos de los Integrantes, clientes, proveedores contra riesgos de violaciones de Datos Personales;
- ser transparente sobre los procedimientos existentes para el procesamiento de Datos Personales; y
- promover la concientización en toda la Compañía sobre las medidas de protección de Datos Personales y Privacidad.

2. ALCANCE

Esta Política aplica para Braskem Idesa y todos sus integrantes que tengan acceso a Datos Personales controlados por Braskem Idesa. En caso que lo requiera la ley local pueden ser creados procedimientos.

Las leyes aplicables en las diferentes regiones en las que opera la Compañía prevalecerán en caso de conflicto con esta Política.

3. REFERENCIAS

- Estatutos de la Compañía
- Código de Conducta de Braskem Idesa
- Política Global Anticorrupción
- Política del Sistema de Compliance
- Política Corporativa de Gestión de Riesgo
- Directriz de Auditoría Interna
- Ley Federal de Protección de Datos Personales en posesión de Particulares ("LFPDPPP") - México.
- General Data Protection Regulation ("GDPR") - Europa
- Ley General de Protección de Datos ("LGPD") - Brasil

4. DEBERES Y RESPONSABILIDADES

4.1 Consejo de administración ("CA")

- Aprobar esta Política y sus futuras alteraciones; y
- Ser responsable por el uso adecuado de los Datos Personales en sus actividades.

4.2 Comité de Compliance ("CC-BI")

- Revisar y recomendar para el CA la aprobación de esta Política y sus alteraciones;
- Ser responsable por el uso adecuado de los Datos Personales en sus actividades;
- Definir y aprobar la estructura de gobierno para cuestiones de privacidad y protección de datos;
- Monitorear de forma continua y efectiva la implementación de iniciativas de privacidad, incluidos los eventos de violaciones de datos personales y las recomendaciones del Comité Global de Privacidad;
- Asegurar que el presupuesto del Área de Compliance, que será aprobado anualmente por el CA, se incluya los recursos necesarios para la implementación y gestión de iniciativas de privacidad;
- Proponer al Comité de Privacidad la resolución de asuntos relacionados con eventos de alto riesgo que son enviados por él al CC; y
- Informar al CA sobre eventos relacionados con violaciones de datos personales y las decisiones del Comité de Privacidad.

4.3 Compliance Officer de Braskem Idesa ("CO-BI")

- Ser responsable por el uso adecuado de los Datos Personales en sus actividades;
- Asegurar que Braskem Idesa cumpla con las leyes y regulaciones relacionadas con privacidad y protección de los Datos Personales, así como con sus políticas y procedimientos internos relacionados con el tema;
- Administrar, coordinar y supervisar la aplicación de la estrategia de protección de datos personales y guiar la implementación de las medidas requeridas para cumplir con los requisitos de la legislación y las regulaciones de protección de datos personales aplicables;
- Participar y orientar, desde una perspectiva de privacidad, los proyectos corporativos que involucren el procesamiento de datos personales para validar el cumplimiento de las leyes y regulaciones aplicables, así como garantizar la privacidad como un estándar que se adoptará e incorporará al diseño de los proyectos a través de las medidas de seguridad necesarias;
- Desarrollar, con el apoyo del Área Legal, acuerdos internacionales de transferencia de datos, así como mantener actualizados los Datos personales que se transfieren entre Braskem Idesa y las diferentes regiones;

- Coordinar la ejecución del análisis de impacto de privacidad de datos ("DPIA": Análisis de impacto de protección de datos);
- Alinear periódicamente, junto con el Líder de Privacidad Corporativa, las definiciones y los criterios con el DPE;
- Definir, revisar y actualizar los avisos de privacidad;
- Realizar evaluaciones periódicas a fin de identificar la madurez de las iniciativas de privacidad, identificando mejoras y su verificando su evolución;
- Monitorear y apoyar la implementación de planes de acción para corregir las brechas de iniciativas de privacidad;
- Atender las solicitudes de los Titulares de Datos Personales de acuerdo con las leyes y regulaciones vigentes en cada país y la Documentación de Orientación de la Compañía;
- Cooperar y relacionarse con el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales;
- Asegurar que la evidencia de ejecución e implementación de las iniciativas de privacidad se mantenga de acuerdo con el principio de responsabilidad.
- Realizar, alineado con el Líder de Privacidad Corporativa, capacitación, campañas de concientización, comunicación interna, etc.;
- Contar con un Data Protector Officer ("DPO") y establecer los presupuestos correspondientes para llevar a cabo sus actividades, siendo responsables de su gestión;
- Desarrollar y mantener actualizado la Documentación Orientadora de privacidad que es de su competencia;
- Monitorear el cumplimiento de las reglas internas de privacidad;
- Aprobar la documentación orientadora de protección de datos personales, alineada con esta Política; y
- Informar al CC el estatus de la implementación de las iniciativas de privacidad.

4.4 Líderes

- Ser responsable por el uso adecuado de los Datos Personales en sus actividades.
- Asegurar que se cumplan los requisitos de las leyes y regulaciones aplicables en el país de operación, así como que sus Integrantes actúen de acuerdo con esta Política;
- Revisar y mantener actualizada el mapeo de los datos personales al menos una vez al año (o en caso de cambios sustanciales), con el área de Compliance.
- Cuando se utilice el consentimiento para el procesamiento de datos personales, asegurar que el mismo se recopile y administre de tal manera que se respete la opción dada por el interesado y que proporcione las evidencias necesarias para su presentación a las autoridades o al titular de los datos, cuando sea necesario.

4.5 Todos los Integrantes (Incluyendo a los Líderes)

- Ser responsable por el uso adecuado de los Datos Personales en sus actividades;
- Cumplir con las leyes y regulaciones aplicables, así como con la Documentación Orientadora con respecto a la protección de Datos Personales y la aplicación de medidas de seguridad de TI apropiadas;
- Informar al Área de Compliance o al Data Protection Expert ("DPE") la ocurrencia de cualquier Incidente de Datos Personales o de seguridad de datos, así como cualquier deficiencia identificado o posibles riesgos de privacidad; y
- Participar de las actividades de capacitación en protección de datos.

4.6 Comité Global de Privacidad ("Braskem")

- Ser responsable por el uso adecuado de los Datos Personales en sus actividades;
- Revisar periódicamente las iniciativas de privacidad adoptadas por la Compañía;
- Promover el conocimiento adecuado de todas las partes interesadas con respecto a la importancia de la protección de datos personales y las actividades internas inherentes a las iniciativas de privacidad;
- Discutir y recomendar sobre nuevas actividades de procesamiento de datos personales, con base a los informes de impacto sobre la protección de datos personales;
- Sugerir cuales medidas técnicas se aplicarán para eventos de alto riesgo, así como medidas disciplinarias;
- Enviar y explicar al CC de Braskem Idesa las medidas técnicas propuestas en los eventos de alto riesgo que no están dentro de su alcance; y
- Informar al CC de Braskem Idesa sobre eventos relacionados con violaciones de Datos personales y sus decisiones operacionales.

4.7 Data Protection Expert (DPE)

- Ser responsable por el uso adecuado de los Datos Personales en sus actividades;
- Participar y dar orientación de privacidad en los proyectos que involucren el procesamiento de datos personales a fin de validar el cumplimiento de las leyes y regulaciones aplicables, así como para garantizar la privacidad como un estándar e incorporación en el diseño de las medidas de seguridad necesarias;
- Ayudar operativamente a monitorear el cumplimiento de las normas internas y mantener Key Performance Indicators (KPI) relacionado con la protección de datos y la privacidad;
- Realizar evaluaciones periódicas a fin de identificar la madurez de las iniciativas de privacidad, identificando mejoras y su verificando su evolución;

- Apoyar con el seguimiento a nivel regional y la implementación de planes de acción para corregir las brechas de las iniciativas de privacidad;
- Apoyar el monitoreo regional y la implementación de planes de acción para corregir las brechas de privacidad y protección de datos;
- Apoyar con la preparación de informes de análisis de impacto de protección de datos (DPIA) y en la tomada de decisiones de proyectos regionales, asegurando la adherencia a los requisitos de esta Política;
- Monitorear las solicitudes de los titulares de datos personales para garantizar que se respondan a tiempo;
- Asegurar el mantenimiento de evidencia sobre la ejecución e implementación de iniciativas de privacidad, a nivel regional (principio de responsabilidad);
- Apoyar, junto con el Área Legal, en asuntos relacionados en asuntos relacionados con las cláusulas de protección de Datos Personales y/o documentación adicional, cuando sea necesario;
- Apoyar a las autoridades locales en temas de Protección de Datos Personales;
- Revisar y actualizar periódicamente el Mapeo de Datos Personales, así como revisar todos los cambios significativos con el apoyo de los líderes;
- Informar al Líder de Provacidad Corporativo cualquier sospecha razonable de una violación de datos personales; y
- Coordinar actividades y consultas con el DPO que apoya a la compañía.

4.8 Seguridad Informática (SI)

- Ser responsable por el uso adecuado de los Datos Personales en sus actividades;
- Analizar las infracciones y violaciones de datos personales, así como recopilar pruebas técnicas;
- Monitorear e implementar medidas de seguridad para asegurar el cumplimiento de las leyes y regulaciones aplicables;
- Publicar avisos de privacidad en sitios web y programas externos;
- Revisar y mantener actualizada la documentación orientadora de seguridad de la información que es de su competencia;
- Definir e implementar un procedimiento de violación de Datos Personales y formatos que detallen las medidas para gestionar y responder a una violación de Datos Personales y mitigar los daños derivados del incidente;
- Definir procedimientos y formularios para la formalización de incidentes de datos personales;
- Implementar mecanismos para garantizar los derechos del Titular de datos;
- Proporcionar soporte técnico y analizar nuevas herramientas y sistemas para la protección de datos personales; y
- Asegurar la aplicación de medidas de seguridad proporcionales al riesgo generado por el procesamiento de datos personales y en línea con la expectativa de protección del titular de los datos personales, asegurando la integridad, disponibilidad y confidencialidad de esta información.

4.9 Área Legal

- Ser responsable por el uso adecuado de los Datos Personales en sus actividades;
- Asegurar que los contratos que prevén el procesamiento de Datos Personales contienen cláusulas de privacidad apropiadas a las leyes y regulaciones aplicables;
- Brindar soporte legal en caso de violaciones de datos personales;
- Brindar apoyo legal en la interpretación de la legislación y las reglamentaciones relacionadas con la protección de datos personales;
- Asistir en la renegociación de contratos / aditivos con proveedores y clientes que realizan Procesamiento de datos personales; y
- Apoyar el contacto con autoridades nacionales de datos personales.

4.10 Auditoria Interna

- Ser responsable por el uso adecuado de los Datos Personales en sus actividades; y
- Incluir una evaluación del cumplimiento de la Documentación Orientadora sobre protección de datos personales en los proyectos de auditoría e informar al CC sobre el resultado de estas evaluaciones.

5. POLÍTICA

5.1 PRINCIPIOS DE PROTECCIÓN DE DADOS PERSONALES

Esta sección describe los principios que deben observarse en la recopilación, manejo, almacenamiento, divulgación y procesamiento de "Datos personales" por parte de Braskem Idesa, para cumplir con los estándares de protección de datos corporativos y cumplir con las leyes y regulaciones aplicables en los respectivos países donde la misma tiene operación industrial o actividad comercial.

5.1.1 Legalidad, Justicia, Transparencia y No Discriminación

La Compañía trata los Datos personales de manera legal, justa, transparente y en adherencia a las leyes y regulaciones aplicables.

La Compañía solo trata los Datos personales cuando el propósito del tratamiento se ajusta a una de las hipótesis legales permitidas que se enumeran a continuación, garantizando que los titulares de datos sean informados sobre la razón y la forma en que se procesan sus Datos personales antes o durante la recolección:

- necesidad de ejecutar un contrato en el que el interesado sea parte;
- exigencia derivada de alguna ley o regulación a la que está sujeta la Compañía;

- interés legítimo en el Tratamiento, en cuyo caso dicho interés legítimo se comunicará por adelantado; y
- necesidad de proporcionar al Titular de datos el ejercicio regular de la ley en procedimientos judiciales, administrativos o arbitrales.

Cuando el procesamiento de Datos personales no cumpla con las hipótesis anteriores, la Compañía deberá obtener el consentimiento de los interesados para el procesamiento de sus datos personales y se asegurará de que este consentimiento se obtenga de manera específica, gratuita y sin ambigüedades. La Compañía debe recopilar, almacenar y administrar todas las respuestas de consentimiento de manera organizada y accesible para que se pueda proporcionar evidencia de consentimiento cuando sea necesario.

Del mismo modo, el Titular de datos debe tener la posibilidad de retirar su consentimiento en cualquier momento de forma similar al proceso de obtención.

En algunas circunstancias, se le puede solicitar a la Compañía que procese Datos personales sensibles, que involucran, entre otros:

- datos de salud o vida sexual
- datos genéticos o biométricos vinculados a un individuo;
- datos sobre orientación sexual;
- datos sobre condenas o delitos penales;
- datos que revelen origen racial o étnico, opiniones políticas, creencias religiosas o filosóficas; y
- datos sobre creencias religiosas, opinión política, afiliación sindical u organización religiosa, filosófica o política.

El procesamiento de Datos personales Sensibles está prohibido, excepto para los casos específicos que se describen a continuación, donde se deben observar estándares de seguridad más estrictos que los empleados para otros tipos de Datos personales:

- cuando sea necesario para cumplir con una obligación legal o reglamentaria;
- cuando sea necesario para el ejercicio regular de los derechos, como la defensa o propuesta de acciones legales, administrativas o arbitrales;
- cuando sea necesario para el cumplimiento de las obligaciones y el ejercicio de los derechos en materia de empleo, seguridad social y protección social;
- para proteger la vida o la seguridad física del interesado, incluidos los datos médicos preventivos y ocupacionales;
- con el propósito de promover o mantener la igualdad de oportunidades entre personas de diferente origen racial o étnico,
- cuando el titular de datos ha dado su consentimiento explícito de acuerdo con las leyes y regulaciones aplicables; y

- cuando el tratamiento se refiere a condenas penales y delitos relacionados o las medidas de protección relacionadas se llevarán a cabo bajo el control de la autoridad pública o cuando el tratamiento esté autorizado por la legislación local que brinde garantías adecuadas para los derechos y libertades de los titulares de datos personales.

5.1.2 Limitación y Adecuación sobre la Finalidad

El procesamiento de los Datos personales debe realizarse de manera coherente con el propósito original para el que se recopilaron los Datos personales y no puede recopilarse para un propósito y utilizarse para otro. Cualquier otro propósito debe ser coherente con el motivo original por el que se recopilaron los Datos personales.

5.1.3 Principio de la Necesidad (Minimización de Datos)

La Compañía solo puede procesar los Datos personales necesarios para lograr un propósito específico, este es el principio de minimización de datos. Para compartir datos personales con otra área o Compañía debe ser considerado este principio y solo compartir cuando se tienen la protección legal adecuada.

5.1.4 Exactitud (Calidad de los Datos)

La Compañía debe tomar medidas razonables para garantizar que todos los Datos personales en su custodia se mantengan precisos, actualizados en relación a los fines para los que fueron recopilados, garantizando al Titular de los Datos personales la posibilidad de solicitar la eliminación o corrección de los Datos inexactos u obsoletos.

5.1.5 Retención y Limitación del Respaldo de Datos

La Compañía debe conocer sus actividades de Tratamiento, los períodos de retención establecidos y los procesos de revisión periódica y no puede mantener los Datos personales durante un período más largo del necesario para cumplir con los fines previstos.

5.1.6 Integridad y Confidencialidad (Libre Acceso, Prevención y Seguridad)

La Compañía debe asegurar que se apliquen las medidas técnicas y administrativas apropiadas a los Datos personales para protegerlos del procesamiento no autorizado o ilegal, así como contra pérdidas, destrucción o daños accidentales. El procesamiento de datos personales también debe garantizar la debida confidencialidad. Entre las medidas técnicas más comunes se encuentran:

- **Anonimización** significa que los Datos personales se hacen anónimos, de modo que los datos ya no se refieren más a una persona identificable directa o indirectamente. El anonimato tiene que ser irreversible.

- **Pseudoanonimización** es un proceso mediante el cual los Datos personales ya no se relacionan directamente con una persona identificable (por ejemplo, mencionando su nombre), pero no son anónimos porque aún es posible, con información adicional que se mantiene por separado, identificar a una persona.

5.1.7 Responsabilidad

La Compañía es responsable y debe demostrar el cumplimiento de esta Política, asegurando la implementación de diversas medidas que incluyen, pero no se limitan a:

- asegurar que los Titulares de Datos Personales puedan ejercer sus derechos como se describe en la Sección 5.5 de este Documento;
- registro de datos personales, que incluyen:
    - registros de actividades de procesamiento de datos personales, con una descripción de los propósitos de dicho procesamiento, los destinatarios del intercambio de datos personales y los plazos en los que la Compañía debe retenerlos; y
    - Plan y Procedimiento de Respuesta a Incidentes de Datos Personales y el registro de incidentes y violaciones de datos personales;
- garantizar que los Terceros que son procesadores de datos personales también actúen de acuerdo con esta Política y con las leyes y regulaciones aplicables;
- asegurar que la Compañía, cuando sea necesario, registre con la Autoridad de Supervisión aplicable un Responsable de Datos o DPO; y
- garantizar que la Compañía cumple con todos los requisitos y solicitudes de cualquier Autoridad de Supervisión a la que esté sujeta.

5.2 ESTÁNDARES DE SEGURIDAD

La Compañía está comprometida y adopta medidas técnicas, administrativas, de seguridad y de privacidad para proteger los Datos Personales contra cualquier acceso no autorizado, accidental o situaciones ilícitas de destrucción, pérdida, alteración, comunicación o cualquier tipo de Tratamiento inapropiado o ilícito, en términos de seguridad de la información en la Compañía, a través de medidas de seguridad y privacidad por diseño y defecto.

5.3 RELACIÓN CONTROLADOR-PROCESADOR DE DATOS PERSONALES

Cada Empresa de la Compañía es definida como el Controlador de Datos Personales en su respectiva región y se requiere un responsable para garantizar que los Datos Personales se manejen correctamente y de acuerdo con las leyes y regulaciones aplicables en dicha región. En ciertas circunstancias, una Empresa de la Compañía puede actuar como Procesador de otra, siendo necesaria, cuando así lo determine el Líder Corporativo de Privacidad, la designación de un responsable de asegurar que dichos Datos Personales estén siendo tratados correctamente y de conformidad con la legislación y normativa aplicable al Controlador.

5.4 POLÍTICA DE TRANSFERENCIA INTERNACIONAL DE DATOS PERSONALES

La Compañía puede compartir Datos Personales con Braskem en otros países para fines corporativos legítimos y administración comercial general, según lo permitan las leyes y regulaciones aplicables.

La Compañía también puede compartir Datos Personales con Terceros en el desarrollo de actividades corporativas, en cumplimiento de sus obligaciones legales o reglamentarias, en respuesta a una orden judicial o solicitudes de autoridades públicas, para la defensa en procedimientos judiciales, administrativos y arbitrales, para llevar a cabo auditorías internas o externas o en caso de venta, cesión o transferencia del negocio de la Compañía, en su totalidad o en partes, según lo permitido por las leyes y reglamentos aplicables.

Cuando los Datos Personales se procesen en países distintos a aquellos en los que fueron recopilados, se deben observar las leyes y regulaciones internacionales aplicables sobre la transferencia de Datos Personales en cada país.

La Compañía debe asegurarse de que se mantengan los procedimientos internos para garantizar el cumplimiento de las leyes de protección de datos aplicables a fin de proteger los Datos personales, independientemente de dónde se encuentren. La Compañía también debe asegurarse de que el país en el que se transfiere la información tenga un estándar mínimo de protección de Datos Personales de conformidad con esta Política, leyes y reglamentos.

Cuando la Compañía transfiere Datos Personales a un país diferente, que no tiene un nivel adecuado de Protección de Datos según las leyes locales, la Compañía debe implementar controles de Datos Personales adecuados para garantizar que dichas transferencias de Datos Personales cumplan con esta Política y las leyes locales.

5.5 DERECHOS DE LOS TITULARES DE DATOS PERSONALES

La Compañía está comprometida con los derechos de los Titulares de Datos Personales, de conformidad con las leyes y reglamentos locales aplicables, que incluyen sin limitación:

- Dar información, en el momento en que se proporcionan los Datos personales, sobre cómo se tratarán sus Datos personales;
- Dar información sobre el procesamiento de sus Datos personales y el acceso a los Datos personales que la Compañía tiene sobre ellos;
- Dar la posibilidad de corregir los datos personales inexactos, incorrectos o incompletos;
- Ofrecer mecanismos de eliminación, bloqueo y / o anonimato de sus datos personales bajo ciertas circunstancias ("derecho a ser olvidado"). Esto puede incluir, pero no se limitar a, circunstancias en las cuales la Compañía ya no está obligada a retener sus Datos personales para los fines para los que fueron recopilados;
- Restringir el procesamiento de los Datos personales en determinadas circunstancias;
- Oponerse al tratamiento si el tratamiento se basa en intereses legítimos injustificado;
- Retirar el consentimiento en cualquier momento si el procesamiento de datos personales se basa en el consentimiento del individuo para un propósito específico;
- la portabilidad de los Datos personales a otro proveedor de servicios o productos a solicitud expresa en ciertas circunstancias;
- Solicitar la revisión de decisiones tomadas únicamente sobre la base del procesamiento automatizado de datos personales; y
- Presentar una queja ante la Compañía o la Autoridad de Protección de Datos aplicable si el Titular de Datos Personales tiene razones para suponer que se ha violado alguno de sus derechos de protección de Datos Personales.

Los Titulares de los Datos Personales pueden ejercer sus derechos enviando una solicitud a data_protection@braskem.com

5.6 PRESTADORES DE SERVICIOS TERCERIZADOS (PROVEEDORES)

Los proveedores de servicios externos que procesan Datos personales de acuerdo con las instrucciones de la Compañía están sujetos a las obligaciones impuestas a los procesadores de acuerdo con las leyes y regulaciones de protección de datos personales aplicables. La Compañía debe asegurarse de que el contrato de servicio incluya las cláusulas de privacidad que requieren que el Procesador de Datos de terceros implemente medidas de seguridad, así como controles técnicos y administrativos apropiados para garantizar la confidencialidad y seguridad de los Datos Personales y para especificar que el Procesador está autorizado a Procesar Datos personales solo cuando la Compañía lo solicite formalmente.

5.7 GERENCIAMIENTO DE UNA VIOLACIÓN DE DATOS

Todos los incidentes y posibles violaciones de datos deben informarse al Área de Compliance y/o DPE. Todos los Integrantes deben ser conscientes de su responsabilidad personal de enviar y compartir problemas potenciales, así como de informar violaciones o sospechas de violaciones de Datos personales tan pronto como las identifiquen. En el momento en que se descubre un incidente o violación real, es esencial que se informen y se formalicen de manera oportuna.

Las violaciones de datos incluyen, entre otras, cualquier pérdida, eliminación, robo o acceso no autorizado de datos personales controlados o procesados por la Compañía. Para obtener más información al respecto, consulte el Procedimiento del Plan de Respuesta a Incidentes de Datos Personales.

5.8 AUDITORIAS DE PROTECCIÓN DE DATOS

La Compañía asegurará de que haya revisiones periódicas para confirmar que las iniciativas de privacidad, su sistema, medidas, procesos, precauciones y otras actividades, incluida la gestión de la protección de datos personales, se implementan y mantienen de manera efectiva y cumplen con las leyes y regulaciones aplicables.
Además, y según lo dispuesto en la Directriz Global de Auditoría Interna, este tema debe evaluarse de forma periódica en las áreas de mayor riesgo, si los riesgos son relevantes, Auditoría Interna debe incluir una revisión independiente específica en el Plan Anual de Auditoría Interna.

6. DISPOSICIONES GENERALES

Los Integrantes son responsables por conocer y entender todos los Documentos Normativos aplicables a ellos. Del mismo modo, los Líderes son responsables de asegurar que todos los Integrantes entiendan y cumplan con los Documentos Normativos aplicables a la Compañía.

Los Integrantes que tengan preguntas o dudas sobre esta Política, incluidos sus alcances, términos u obligaciones, deben comunicarse con sus respectivos Líderes y, si es necesario, con el Área de Compliance de la Compañía.

La violación de cualquiera de nuestros Documentos Normativos puede resultar en graves consecuencias para la Compañía y los Integrantes involucrados. Por lo tanto, el incumplimiento o el no reportar una violación conocida de este Documento Normativo, puede resultar en una acción disciplinaria para cualquier Integrante(s) involucrado(s).

Si cualquier Integrante o Tercero se da cuenta de una posible conducta ilegal o no ética, incluidas la posible violación de las Leyes Anticorrupción Aplicables y/o los lineamientos de la compañía, incluido este Documento Normativo, el Integrante o el Tercero debe informar de inmediato la posible violación a la Línea Ética o al área de Compliance. Los Líderes deben promover continuamente que los Integrantes de su equipo reporten dichas desviaciones utilizando la Línea de Ética.

No hay nada en los lineamientos de la Compañía, incluido este Documento Normativo, que prohíba a los Integrantes o a los Terceros informar cualquier inquietud o actividad ilegal a las autoridades reguladoras correspondientes.

Akira Junior
Compliance Officer Braskem Idesa

DEFINICIONES

A continuación, se presentan con mayúscula los términos utilizados en esta Política, y sus definiciones:

"**Anonimización**": Proceso y técnica por los cuales un dato pierde la posibilidad de asociación directa o indirecta con un individuo. Los datos anónimos no se consideran datos personales.

"Braskem", "Braskem Idesa" o **"Compañía":** Braskem Brasil y/o Braskem Idesa y todos sus integrantes.

"**CA**" o "**Consejo**" o "**Consejo de Administración**": Consejo de Administración Braskem Idesa.

"Comité de Compliance" o "CC": Comité de Compliance de Braskem Idesa.

"Coordinador CC": El Director independiente de CC, responsable de coordinar el CC.

"**Comité de Privacidad (Brasil)**": Comité asesor multidisciplinario global compuesto por líderes de las áreas de Legal, de Compliance, Seguridad de la Información y P&O, así como representantes de cada área relevante en las regiones para discutir temas relevantes y críticos de seguridad de la información y privacidad de datos.

"**Consentimiento**": Declaración libre, informada y sin imprecisiones, por la cual el Titular de los datos acepta el Tratamiento de sus Datos personales para un propósito particular.

"Compañía(s) Controlada(s)" o **"Entidad(es) Controlada(s)"** o **"Subsidiarias"**: Son las empresas donde Braskem Idesa, ya sea directamente o a través de otras compañías controladas, posee derechos que aseguran, de forma permanente, su preponderancia en las deliberaciones corporativas y le dan el poder de elegir a la mayoría de los gerentes o directores.

"**Dato(s) Personal(es)**": Cualquier información relativa a una persona física identificada o identificable, que puede reconocerse, directa o indirectamente, por referencia a un identificador, como nombre, número de identificación, datos de ubicación, dirección IP o uno o más factores específicos de la identidad física, fisiológicos, genéticos, mentales, económicos, culturales o sociales de una persona física.

"**Dato(s) Personal(es) Sensible(s)**": Cualquier dato personal que pueda generar cualquier tipo de discriminación, como datos sobre origen racial o étnico, creencias religiosas, opinión política, afiliación sindical u organización religiosa, filosófica o política, con respecto a la salud o la vida sexual, datos genéticos o biométrico.

"Data Protection Expert (DPE)": Especialista en el tema de Protección de Datos, con las atribuciones y responsabilidades de un DPO, pero con poder de decisión reducido.

"**Encargado de Protección de Datos**" o "**Data Protection Officer *("DPO")***": La persona formalmente designada como el oficial de datos / Encargado de protección de datos según lo dispuesto por las leyes de protección de datos, para un territorio determinado. El DPO puede ser un integrante o un tercero.

"Documento(s) normativo(s)": documento oficial de Braskem Idesa que proporciona la base que sustenta las decisiones corporativas, reglas y orientaciones vitales para conducir el trabajo de Braskem Idesa con legitimidad, seguimiento apropiado y aplicabilidad, por lo que deberá ser observado y aplicado por un determinado y definido universo de Integrantes.

"**Integrante(s)**": Empleados / colaboradores de Braskem Idesa en todos los niveles, incluidos ejecutivos, directores, directores, pasantes y aprendices.

"**GDPR**": Reglamento (UE)2016/679 del Parlamento Europeo, de 27 de abril de 2016, sobre la protección de las personas en lo que respecta al tratamiento de datos personales y a la libre circulación de dichos datos y por el que se deroga la Directiva 95/46 / CE (Reglamento Política de protección de datos).

"**LFPDPPP**": Legislación mexicana aprobada en 2010. La Ley Federal de Protección de Datos Personales en Posesión de Particulares, y sus disposiciones se aplican a todas las personas físicas o jurídicas que realizan el procesamiento de datos personales en el ejercicio aplicable de sus actividades.

"**LGPD**": Legislación brasileña No. 13.709 / 2018, comúnmente conocida como la Ley General de Protección de Datos Personales, que regula las actividades de procesamiento de datos personales y también modifica los artículos 7 y 16 del Marco Civil de Internet.

"Líder(es)": Integrantes que lideran un equipo.

"Líder de Privacidad Corporativa": es o líder global de las inicitivas corporativas de privacidad de Braskem.

"**Pseudoanonimización**": Acuerdo entre Líder y Líder que define las responsabilidades del Miembro y el compromiso del Líder de acompañar, evaluar y tomar una decisión con respecto al Líder de acuerdo con su desempeño.

"**Seguridad Informática**" **o** "**SI**": Área responsable por proteger la integridad, disponibilidad y confidencialidad de los sistemas de TI y responsable por implementar medidas apropiadas para lograr este objetivo, siendo el soporte técnico del Líder de Privacidad Corporativa y responsable de los asuntos relacionados con medidas técnicas y administrativas.

"Terceros" o "Tercera Parte": cualquier persona, física o moral, que actúe en nombre o interés o en beneficio de Braskem Idesa, sea proveedor de servicios, suministros u otros bienes, así como socios comerciales que presten sus servicios a Braskem Idesa; también aquellos directamente relacionados con la obtención, retención o conducción de los asuntos de Braskem Idesa, lo que incluye, entre otros, a distribuidores, agentes, corredores, promotores, intermediarios, socios en la cadena de suministro, consultores, distribuidores, revendedores, representantes, secciones de empresas conjuntas, contratistas y otros proveedores de servicios profesionales.

"**Titular(es) de Datos**": Persona física identificada o identificable a la que se refiere un dato personal específico

"**Tratamiento de Datos Personales" o "Tratamiento"**: Cualquier operación o conjunto de operaciones realizadas en Datos personales o en conjuntos de Datos personales, por medios automatizados o no automatizados, tales como recopilación, registro, organización, estructuración, conservación, adaptación o alteración, recuperación, consulta, uso, divulgación por transmisión, difusión o cualquier otra forma de provisión, comparación o interconexión, limitación, eliminación o destrucción.