1. INTRODUCCIÓN

Mientras realiza sus operaciones comerciales, Makro procesa una variedad de datos personales de sus clientes, empleados, proveedores, en documentos físicos o en dispositivos electrónicos.

Los datos personales son cualquier información relacionada con una persona física Identificada o identificable (" Datos personales "), por lo tanto, incluye una gama de información, como nombre, fecha de nacimiento, identificación, teléfono, correo electrónico, género, fotos, número de seguro social, etc.

Los Datos Personales pueden reproducirse en diferentes formatos, que incluyen, entre otros, cartas, contratos, mensajes de fax, correos electrónicos, facturas, órdenes de compra, estados de cuenta, informes, cuentas (anuales), impuestos y / u otras presentaciones, planos, dibujos, fotografías y datos digitales. A los efectos de esta Política, el término "Documento" incluye toda dicha información tanto en copias impresas como en formularios electrónicos.

Makro se asegurará de que solo los Datos y Documentos Personales relevantes y requeridos se conserven solo durante el período requerido o acordado, de acuerdo con las premisas y reglas establecidas por esta Política de Retención de Datos Personales("Política"). Makro necesita mantener el control de esa información y solo los trabajadores que requieran el uso de datos personales para cumplir con sus deberes deben usar estos datos.

Bajo ciertas circunstancias, es necesario conservar los Documentos para cumplir con los requisitos legales, con fines probatorios o para satisfacer las necesidades operativas. La destrucción prematura de los Documentos puede dar lugar a un incumplimiento de la normativa aplicable, incapacidad para defender objetivos litigiososo dificultades o desventajas operativas.

Esta Política establecerá el período durante el cual los Principales Documentos que contienen Datos Personales pueden conservarse sin violar los requisitos legales. Además, los Datos y Documentos Personales, que ya no son necesarios para su propósito respectivo y / o han excedido su período de retención, deben eliminarse, destruirse o anonimizarse de acuerdo con los principios definidos en esta Política. Del mismo modo, la retención eterna de documentos y datos personales es poco práctica e ilegal.

Se recomienda y es necesario eliminar y anonimizar adecuadamente porque ayuda a Makro a cumplir con los requisitos de cumplimiento, proporcionar suficiente espacio de almacenamiento electrónico y de oficina para facilitar un entorno de trabajo más eficiente y sostenible.

2. OBJETIVO

El propósito de esta Política es proporcionar a los empleados de Makro las reglas sobre si los Datos Personales o documentos deben conservarse, destruirse, eliminarse o anonimizarse, de acuerdo con los períodos de retención apropiados.

La eliminación de datos está destinada y es necesaria para cumplir con los principios de minimización, necesidad y adecuación de datos establecidos por las leyes de protección de datos y los códigos de privacidad de Makro, como para evitar violaciones de datos, divulgación de información y garantizar que los dispositivos electrónicos tengan su contenido eliminado y / o destruido de forma segura.

Esta Política tiene como objetivo que Makro cumpla con los requisitos legales proporcionados por las regulaciones legales locales y el cumplimiento interno de los códigos de privacidad de Makro, con respecto a todos los procesos de Datos Personales en las actividades realizadas por Makro.

3. APLICABILIDAD

Esta Política se aplica MAKRO SUPERMAYORISTA S.A.S., en lo sucesivo denominado MAKRO, sus empleados, contratistas y vinculados que están procesando datos personales en nombre de Makro, de modo que todos deben cumplir con esta Política, incluido los períodos de retención establecidos en el **Anexo A.**

La Política se aplica específicamente a todos los Datos y Documentos Personales de los cuales Makro es el controlador (entidad responsable de todas las decisiones relacionadas con el procesamiento de datos).

4. NORMAS GENERALES:

a. Principios de retención, almacenamiento, destrucción y anonimización

- Las decisiones relacionadas con la retención, eliminación y destrucción de un Documento o Datos Personales, o con respecto a la anonimización de datos personales, deben tomarse de acuerdo con esta Política.
- Los documentos deben almacenarse durante el período de conservación aplicable, tal como se menciona en el **Anexo A.**
- Para evitar dudas, el almacenamiento y la destrucción de todos los datos digitales (por ejemplo, correos electrónicos, sesiones de chat, formularios, etc.) calificados como Documentos, cualquier dato digital está cubierto por esta Política.
- Los datos personales solo se conservarán si existe un propósito comercial legítimo y una base legal (base legal) para hacerlo, como se establece en las políticas y códigos de privacidad de Makro. Cuando los Datos Personales ya no sean necesarios para el propósito para el que fueron recopilados, los Datos Personales serán eliminados. La eliminación de los Datos Personales puede hacerse a través de la eliminación / destrucción, o la anonimización (transformando los datos personales disociados a una persona natural).
- Los datos personales se eliminarán según el período de retención de datos, teniendo en cuenta los requisitos legales de retención que puedan imponerse en los registros de datos y documentos.
- La destrucción de dispositivos electrónicos o digitales debe ser coordinada por el área de TI, considerando el proveedor apropiado y autorizado o el personal competente.
- La anonimización de los Datos Personales digitales debe ser coordinada por el área de TI con el empleado que los está procesando debidamente.
- Los dispositivos electrónicos, como computadoras de escritorio, computadoras portátiles, teléfonos, etc., que ya no están en uso (retirados), se destruirán o se pueden entregar a un tercero para su uso posterior. En caso de entrega a un tercero, todos los datos deben eliminarse, limpiarse o sobrescribirse de forma segura de los dispositivos electrónicos antes de la devolución.
- El borrado de datos digitales (eliminación / borrado de datos para que ya no se puedan leer) es necesario antes de reutilizar dispositivos electrónicos, dispositivos de almacenamiento extraíbles o internos (por ejemplo: memorias USB o HDD / SSD), solo TI es el área que está autorizado para realizar dicha limpieza.
- Todos los datos en dispositivos móviles deben eliminarse antes de su reutilización o destrucción por parte del área de TI.
- Las cuentas de administración en la nube de teléfonos / tabletas (es decir, iCloud) deben desvincularse del hardware y todos los datos personales y copias de seguridad deben eliminarse (es decir, seguimiento de dispositivos, historial histórico de navegación, contactos, fotos y otros).
- Los teléfonos / tabletas deben restaurarse a la configuración de fábrica o reacondicionarse antes de reutilizarlos o al entregarlos al área de TI.
- Datos e información en plataformas alojadas y propias no internas (plataformas de terceros y plataformas basadas en la nube que no son propiedad de Makro. Ejemplos: AWS, Salesforce y otros servicios alojados, SaaS o PaaS) se eliminarán según el programa de retención de datos, teniendo en cuenta la legislación local, y los detalles deben incluirse en el contrato.
- Los documentos y datos personales deben almacenarse de manera segura y accesible. Cualquier Documento o Dato Personal que sea esencial para el negocio de Makro debe ser duplicado y/o respaldado y mantenido fuera del sitio, de acuerdo con las políticas y procedimientos de TI de Makro.
- El almacenamiento de documentos electrónicos y datos personales en la nube debe coordinarse con el área de TI, también para asegurarse de que se mantienen las actualizaciones y se siguen correctamente los pasos de destrucción y anonimización.
- Los documentos que se destruirán que contengan datos confidenciales o personales deben triturarse en lugares adecuados para evitar eventuales infracciones y evitar la fuga de información comercial o de datos personales sensibles.
- Los documentos que se destruyan que no contengan datos confidenciales o personales deben triturarse y eliminarse mediante binning, reciclaje, eliminación (en el caso de documentos electrónicos) y, si corresponde, la

entrega a terceros. La transferencia de documentos a terceros es inusual, pero podría ser apropiada cuando los documentos son de interés histórico y, por lo tanto, pueden enviarse a los archivos oficiales. Dicha decisión está sujeta a la aprobación del Oficial de Protección de Datos.

- Los registros de destrucción o eliminación de datos digitales deben ser mantenidos por el área de TI, y deben detallar el documento o la información eliminada, la fecha y el DPO que autorizó la destrucción / eliminación. En caso de que algún departamento/área decida destruir o borrar algunos datos por sí mismo, será su responsabilidad mantener el registro de esta destrucción.
- Los datos personales solo serán mantenidos por Makro y los contratistas que procesan datos personales en nombre de Makro cuando exista una base legal válida proporcionada por la ley local y exista un contrato formal. Cuando este ya no sea el caso o cuando los datos personales ya no sean necesarios para el propósito para el que fueron recopilados, los datos se eliminarán, teniendo en cuenta cualquier otra obligación legal (por ejemplo, términos mínimos legales de retención) o posibles litigios. La eliminación de datos personales puede ser a través de la eliminación / destrucción, o la anonimización (desidentificación) y la evidencia del proceso debe ser manejada a Makro, para ser guardada adecuadamente.
- La digitalización y el procesamiento de datos personales sensibles (es decir, datos relacionados con las creencias religiosas y / o filosóficas de una persona, raza, opiniones políticas, salud, género y afiliación a un sindicato) solo están permitidos en situaciones definidas (por ejemplo, con el consentimiento explícito de esa persona), teniendo en cuenta la legislación local y las medidas de seguridad (por ejemplo, archivos con contraseña, límite de acceso restringido). La eliminación de datos personales confidenciales puede ser a través de la eliminación / destrucción o la anonimización (desidentificación).
- Las políticas de Makro deben estar alineadas con las directrices de SHV.
- La política debe contener todas las normas. Deben presentar, en su caso, los plazos de entrada en vigencia y de ejecución.
- La Política debe designar a la persona responsable de las actividades, por el puesto y no por su nombre.
- La política debe definir reglas, no detallar los niveles operativos. El "paso a paso" de las actividades debe describirse en los Procedimientos Normativos y/o manual operativo.

4.2 Relación con otras políticas de privacidad de Makro:

La información en esta Política, y en particular el almacenamiento y la presentación de Documentos, también puede estar sujeta a otras políticas o códigos de privacidad de Makro, como el Código de privacidad para los datos de los empleados, la Política de privacidad para los datos de los socios comerciales, el Procedimiento de atención de solicitudes sobre protección de datos personales y el Código de privacidad para los candidatos a empleo.

5. INSTRUCCIONES DE ELIMINACIÓN, DESTRUCCIÓN, ANONIMIZACIÓN Y RETENCIÓN

Cada una de las siguientes consultas debe considerarse antes de la destrucción de cualquier documento o la anonimización de cualquier Dato Personal. Tenga en cuenta que estas consultas solo sirven como orientación y que dependiendo del Documento y los Datos Personales, pueden aplicarse otras regulaciones y / o consideraciones adicionales.

- Compruebe que el documento está sujeto a esta política de retención de datos: La Política de Retención de Datos solo se aplica a los Documentos que son relevantes para el negocio de Makro como se especifica en la Política, de conformidad con el **Anexo A**.
- Verificar que la naturaleza y el contenido del Documento sean adecuados para su destrucción: Ciertos Documentos nunca deben ser destruidos, por ejemplo, Documentos con un cierto valor económico y/o histórico. Este análisis será aprobado por el comité de privacidad y el DPO y el área que maneja los datos.
- Verifique si los Datos Personales pueden ser correctamente anonimizados: Los Datos personales deben ser irreversiblemente anonimizados de tal manera que la persona a la que se refieren los Datos Personales no sea o ya no sea identificable, y que cualquier destinatario de los datos anonimizados no pueda recrear los datos originales.
- Verifique si se requiere retención para cumplir con las obligaciones reglamentarias u otras obligaciones legales/reglamentarias: Los períodos de retención de Makro deben cumplirse, conforme se indica en el **Anexo A**.
- Verifique si se requiere retención para mantener la evidencia: Los documentos y datos personales que puedan ser

necesarios para los procedimientos judiciales, administrativos o arbitrales deben conservarse hasta que concluyan estos procedimientos o se hayan producido sus plazos de prescripción. A este respecto, deben considerarse los plazos de prescripción para iniciar litigios y/o presentar reclamaciones en virtud de la legislación aplicable. En caso de duda, póngase en contacto con el departamento legal y / o el Oficial de Protección de Datos (DPO).

- Verifique si ee requiere retención para satisfacer las necesidades operativas: Considere si el Documento o los Datos Personales en cuestión pueden ser útiles para futuras referencias, como precedente o para fines de gestión del desempeño, por ejemplo, cartas de recomendación de clientes valiosos.

En caso de duda sobre si un documento podría o debería ser destruido, o si los Datos Personales podrían o deberían ser anonimizados, póngase en contacto con el departamento legal y/o el Oficial de Protección de Datos (DPO) y/o Representante de ética y cumplimiento.

6. PROGRAMA DE RETENCIÓN

El **Anexo A** contiene la cláusula de períodos de retención de Makro para Documentos y Datos Personales, que debe ser seguida por todos los empleados responsables del procesamiento y manejo de Documentos y Datos Personales. Esta tabla es solo un referente de los principales tipos de documentos, pero puede haber más, por lo que hay que buscar el equiparable legal más cercado y/o consultar al área legal y/o representante de ética y cumplimiento en caso de dudas..

7. RESPONSABLES

7.1 Junta Directiva Ejecutiva:

El propietario final de esta Política es la Junta directores o Management team quien es responsable de revisar e implementar esta Política.
Debe garantizar el cumplimiento de todas las leyes y regulaciones de privacidad de datos aplicables, incluida esta Política. Esto también significa que sus procesos y decisiones deben estar en línea con los principios, reglas y requisitos mínimos descritos en la Política.
MAKRO espera que la gerencia en todos los niveles apoye activamente esta Política. Con este fin, la alta dirección debe garantizar que se dispone de recursos, procesos y sistemas suficientes. Además, es responsabilidad de la alta gerencia de MAKRO garantizar que los empleados relevantes y los terceros en el alcance de esta Política reciban la capacitación adecuada y conozcan los principios, reglas y requisitos mínimos descritos en esta Política.

7.2 Representante de ética y Cumplimiento (ECR):

El ECR es responsable de ayudar al Grupo Makro y a la administración y negocios de Makro a integrar esta Política en el grupo y las unidades de negocio, y de aclarar cualquier pregunta relacionada con la interpretación de esta Política y los procedimientos establecidos dentro de MAKRO.

7.3 Empleados y representantes

Los empleados que manejan y procesan los Datos Personales, o el Documento, son responsables de determinar formalmente si se debe retener, eliminar, destruir o anonimizar Documentos o Datos Personales específicos para sus entidades, según los períodos de retención. Las excepciones deben estar alineadas con el Oficial / Comité de Protección de Datos.

Los empleados deben buscar el asesoramiento del Oficial de Protección de Datos y/o ECR si no están seguros de si deben retener, eliminar, destruir o anonimizar ciertos Documentos o Datos Personales.

7.4 Equipo de TI

El área de Información de Seguridad y el área de TI apoyarán a los empleados con respecto al almacenamiento, eliminación, destrucción o anonimización de Documentos electrónicos y Datos Personales. Además, el Oficial de protección de datos proporcionará asesoramiento y orientación más importantes sobre los períodos de retención de datos y los principios de destrucción de datos personales.

8. MEDIDAS DISCIPLINARIAS:

El incumplimiento de la política está sujeto a las medidas disciplinarias oportunas.

9. CONTROL DE CAMBIO

VERSIÓN	MODIFICADO POR	DETALLE DEL CAMBIO	FECHA
1	Fabian de la Parra	Documento Inicial	Febrero 2022

10. APROBACIONES – (Vía digital)

	CARGO	NOMBRE
Elaborado	Secretario General E&C Representative	Fabian de la Parra
Aprobado	CFO	David Loaiza
	CEO	Arnoud van Wingerde

ANEXO A: Tabla de los períodos de Retención de Makro para el formulario de Documentos y Datos Personales

PROGRAMA DE CONSERVACIÓN DE DOCUMENTOS Y DATOS PERSONALES DE MAKRO COD: RDP-PTD-FO022		
Documento	**Retención por IOD**	**Fuente legal (si aplica)**
Datos/Documentos de empleados		
Pagos laborales	Tiempo de relación laboral + 3 años	Código Laboral
Nómina de sueldos	Tiempo de relación laboral + 3 años	Código Laboral
Pagos de seguridad social	Tiempo de relación laboral + 10 años	Ley 962 del 2005 y Código de Comercio
Información relevante sobre accidentes laborales	Tiempo de relación laboral + 3 años	Código Laboral
Información sobre enfermedades	Tiempo de relación laboral + 3 años	Código Laboral
Recibos de salario	Tiempo de relación laboral + 3 años	Código Laboral
Dato/documentos de trabajo de los empleados		
Acuerdo de compensación de horas	Tiempo de relación laboral + 3 años	Código Laboral
Contratos laboraes y otrosies	Tiempo de relación laboral + 3 años	Código Laboral
Acuerdo de hora extra	Tiempo de relación laboral + 3 años	Código Laboral
Préstamos laborales	Tiempo de relación laboral + 3 años	Código Laboral
Documentos / evidencias médicas.	Tiempo de relación laboral + 3 años	Código Laboral
Documentación de procesos sancionatorios laborales	Tiempo de relación laboral + 3 años	Código Laboral
Acuerdos de terminación de relaciones laborales	Tiempo de relación laboral + 3 años	Código Laboral
Certificados médicos	Tiempo de relación laboral + 3 años	Código Laboral
Datos personales generales de los empleados		
Datos personales de los candidatos a trabajar	Tiempo de relación laboral + 3 años	Código Laboral
Datos personales de los trabajadores	Tiempo de relación laboral + 3 años	Código Laboral
Datos sensibles (género, otros).	Tiempo de relación laboral + 3 años	Código Laboral
Datos personales generales de los clientes		
Nombre completo	Relación comercial + 10 años	Ley 962 del 2005 y Código de Comercio
Correo electrónico	Relación comercial + 10 años	Ley 962 del 2005 y Código de Comercio
Número de teléfono/celular	Relación comercial + 10 años	Ley 962 del 2005 y Código de Comercio
Fecha de nacimiento	Relación comercial + 10 años	Ley 962 del 2005 y Código de Comercio
Genero	Relación comercial + 10 años	Ley 962 del 2005 y Código de Comercio
Hobbies de los clientes	Relación comercial + 10 años	Ley 962 del 2005 y Código de Comercio
Documento de identificación	Relación comercial + 10 años	Ley 962 del 2005 y Código de Comercio
Dirección	Relación comercial + 10 años	Ley 962 del 2005 y Código de Comercio
Otros datos personales facilitados por el cliente de forma voluntaria	Relación comercial + 10 años	Ley 962 del 2005 y Código de Comercio
Información de tarjeta de crédito	Relación comercial + 10 años	Ley 962 del 2005 y Código de Comercio
Información crediticia histórica	Relación comercial + 10 años	Ley 962 del 2005 y Código de Comercio
Dirección IP, otro	Relación comercial + 10 años	Ley 962 del 2005 y Código de Comercio
Nombre de usuario, redes sociales, otros relacionados	Relación comercial + 10 años	Ley 962 del 2005 y Código de Comercio
Hábitos de compra, incluyendo geo - localización.	Relación comercial + 10 años	Ley 962 del 2005 y Código de Comercio
Información pública disponible como blogs, otros	Relación comercial + 10 años	Ley 962 del 2005 y Código de Comercio
Documentos generales de los clientes		
Acuerdos y contratos	Relación comercial + 10 años	Ley 962 del 2005 y Código de Comercio
PQRs	5 años	Código Civil
Expedientes de comunicaciones	5 años	Código Civil
Solicitudes de uso de datos personales	Relación comercial + 10 años	Ley 962 del 2005 y Código de Comercio
Proveedores Datos / documentos personales generales		
Nombre completo/ o Razón Social	Relación comercial + 10 años	Ley 962 del 2005 y Código de Comercio
No. De Identificación y documentos tributarios (RUT, Certificado de Cámara y Comercio)	Relación comercial + 10 años	Ley 962 del 2005 y Código de Comercio
Correo electrónico y teléfono	Relación comercial + 10 años	Ley 962 del 2005 y Código de Comercio
Información crediticia histórica	Relación comercial + 10 años	Ley 962 del 2005 y Código de Comercio
Información histórica de pagos / Referencias de pagos	Relación comercial + 10 años	Ley 962 del 2005 y Código de Comercio
Acuerdos firmados	Relación comercial + 10 años	Ley 962 del 2005 y Código de Comercio
Informacion de los Representantes Legales, Socios y Revisor Fiscal y/o Contador	Relación comercial + 10 años	Ley 962 del 2005 y Código de Comercio
Informacion de los estados financieros	Relación comercial + 10 años	Ley 962 del 2005 y Código de Comercio
Actividad económica	Relación comercial + 10 años	Ley 962 del 2005 y Código de Comercio
Solicitudes de uso y tratamiento de datos .	Relación comercial + 10 años	Ley 962 del 2005 y Código de Comercio
Certificaciones bancarias	Relación comercial + 10 años	Ley 962 del 2005 y Código de Comercio
Certificaciones comerciales	Relación comercial + 10 años	Ley 962 del 2005 y Código de Comercio