

Política de Retención de Datos Personales

Grupo Makro ARGENTINA



Contenido

1. Generalidades	3
1.1. Introducción	3
1.2. Objetivo	4
1.3. Aplicabilidad	4
1.3. Elegibilidad	4
2. NORMAS GENERALES	5
2.1. Principios de retención, almacenamiento, destrucción y anonimización	5
2.2. Relación con otras políticas de privacidad de Makro	7
2.3. Instrucciones de eliminación, destrucción, anonimización y retención	7
2.4. Compruebe que el documento está sujeto a esta política de retención de datos.	7
2.5. Verificar que la naturaleza y el contenido del Documento sean adecuados para su destrucción	7
2.6. Verifique si los Datos Personales pueden ser correctamente anonimizados	7
2.7. ¿Se requiere retención para cumplir con las obligaciones reglamentarias u otras obligaciones legales / reglamentarias?	7
2.8. ¿Se requiere retención para mantener la evidencia?	7
2.9. ¿Se requiere retención para satisfacer las necesidades operativas?	8
2.10. Programa de retención	8
3. RESPONSABILIDADES.....	8
3.1. Miembros del Equipo Directivo	8
3.2. Representante de Ética y Cumplimiento de Makro	8
3.3. Empleados y representantes	9
3.4. Equipo de TI	9
4. MEDIDAS DISCIPLINARIAS	9
5. VIGENCIA	9
6. APÉNDICE	9

1. Generalidades

1.1. 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. En el caso de Makro Argentina, conforme a la Ley No. 25.326, también le es aplicable a las personas jurídicas en cuanto sea procedente.

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 la mencionada información ya sea que se almacene en copias impresas como en medios electrónicos.

Makro se asegurará de que solo los Datos Personales y Documentos 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 (como serían los códigos de privacidad de SHV, las políticas de Makro Group y la legislación argentina), e incapacidad para defender conflictos litigiosos, o dificultades o desventajas operativas.

Esta Política establece el período durante el cual los Principales Documentos que contienen Datos Personales pueden conservarse sin violar los requisitos legales.

Además, los Datos Personales y Documentos, 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.

1.2. 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 Personales y/o Documentos está destinada y es necesaria para cumplir con los principios de minimización, necesidad y adecuación de datos personales establecidos por las leyes de protección de datos y las políticas de privacidad de Makro Group, 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 las políticas de privacidad de Makro Group, con respecto a todos los procesos de Datos Personales en las actividades realizadas por Makro.

1.3. Aplicabilidad

Esta Política se aplica a Makro Argentina, compuesta por Supermercados Mayoristas Makro S.A. y Roberto Basualdo S.A., en lo sucesivo denominados MAKRO.

Además, esta política se aplica a los empleados y contratistas 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 Apéndice de esta política.

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

1.3. Elegibilidad

Esta Política se aplica a todas las áreas y empleados de MAKRO.

2. NORMAS GENERALES

2.1. 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 apéndice de esta política.

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 un fundamento legal para hacerlo, como se establece en las políticas de protección de datos personales de Terceros, de Empleados y de Candidatos a Empleo. 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 humana).

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 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 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. También deben ser incorporados en la revisión el área de Seguridad TI y el área de E&C.

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 destruyan 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 y/o 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 Privacidad de Datos (DPO).

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 en el que DPO 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 un fundamento legal válido, conforme a la política de protección de datos y de acuerdo a la ley local. 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 dirigida 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).

2.2. Relación con otras políticas de privacidad de Makro

Tenga en cuenta que la información en esta Política, y en particular el almacenamiento y la presentación de Documentos, también puede estar sujeta a otras políticas de Makro, como son la Política de Protección de Datos Personales de Empleados, de Terceros, la de Candidatos a Empleo, y el Procedimiento de Atención de Solicitudes sobre protección de datos personales.

2.3. 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.

2.4. 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 Apéndice de esta política.

2.5. 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.

2.6. 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.

2.7. ¿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 apéndice de esta política.

2.8. ¿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 área de Legales y / o el Oficial de Privacidad de Datos (DPO).

2.9. ¿Se 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 área de Legales y / o el Oficial de Privacidad de Datos (DPO).

2.10. Programa de retención

El Apéndice de esta política 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 ha sido elaborada por las áreas responsables y debe ser acatada por todos los empleados de las distintas áreas que manejan documentos e información personal.

3. RESPONSABILIDADES

3.1. Miembros del Equipo Directivo

El propietario final de esta Política es el Equipo de Directores de MAKRO. El Equipo de Directores de Makro debe garantizar el cumplimiento de esta política y de las regulaciones, al igual que los procesos estén en consonancia con los principios, reglas y requisitos establecidos en esta política.

Makro espera que la gestión en todos los niveles apoye activamente esta política. Para ello, la alta Gerencia debe garantizar que se destinen recursos, procesos y sistemas suficientes y que se encuentren en vigencia.

3.2. Representante de Ética y Cumplimiento de Makro

El Representante de Ética y Cumplimiento (ECR) es responsable de ayudar a gestionar la incorporación en los negocios de Makro de esta política, y de aclarar cualquier pregunta relacionada con su interpretación y sobre los procedimientos establecidos dentro de MAKRO.

El ECR, en conjunto con el DPO y el comité de privacidad, revisaran los periodos de retención y de destrucción de datos personales.

3.3. 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 de Privacidad de Datos (DPO) y por el Comité de Privacidad.

Los empleados deben buscar el asesoramiento del Oficial de Privacidad de Datos (DPO) si no están seguros de si deben retener, eliminar, destruir o anonimizar ciertos Documentos o Datos Personales.

3.4. Equipo de TI

El área de TI (Seguridad de Información y otras, según corresponda) apoyarán a los empleados con respecto al almacenamiento, eliminación, destrucción o anonimización de Documentos electrónicos y Datos Personales. Además, el Oficial de Privacidad de Datos (DPO) proporcionará asesoramiento y orientación más importantes sobre los períodos de retención de datos y los principios de destrucción de datos personales, para lo cual incorporará al comité de privacidad.

4. MEDIDAS DISCIPLINARIAS

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

5. VIGENCIA

La vigencia de esta política es a partir del 1° de abril de 2022.

6. APÉNDICE

Tabla de los períodos de Retención de Makro para Documentos y Datos Personales

Versión	Fecha de vencimiento	Dueño	Aprobado por
1	2 años	Edgar González	Pedro Balestrini
Resumen del cambio: Nueva política.			