Política Corporativa de Protección de Datos Personales

I. OBJETIVO

SMU S.A. y sus filiales (las "Compañías") están comprometidas con la protección de datos personales de sus trabajadores(as), clientes, proveedores y, en general, de cualquier individuo relacionado con ella. En este contexto, esta Política Corporativa de Protección de Datos Personales define las directrices generales aplicables a las actividades de tratamiento de datos personales que realiza la Compañía, en cumplimiento de la normativa vigente.

En particular, por medio de esta Política se busca:

Establecer los lineamientos generales para la elaboración de normas, procedimientos, instructivos y otros documentos en materia de protección de datos personales.

Establecer normas de conducta para que los trabajadores, proveedores y socios comerciales de la Compañía cumplan con la regulación de privacidad aplicable a sus actividades en relación con la Compañía.

Contribuir al establecimiento de una cultura decididamente orientada a la protección de datos personales que guíe las actividades que involucren tratamiento de datos personales, aplicando los controles adecuados que correspondan.

Asignar roles y responsabilidades asociadas al cumplimiento de esta Política.

II. ALCANCES

Esta Política es aplicable a SMU S.A. y sus empresas filiales, esto es: Rendic Hermanos S.A., Súper 10 S.A., Alvi Supermercados Mayoristas S.A., Red Apoyo S.A., Unidata S.A., Servicios Logísticos Santiago S.A. y Servicios Logísticos La Serena S.A. y a sus trabajadores(as), directores, socios comerciales, proveedores y mandatarios para el tratamiento de datos.

Se regirá por esta Política todo tratamiento de datos personales realizado por la Compañía, con independencia de la forma en que sean recolectados los datos, el medio en que estén almacenados y quiénes son sus titulares.

III. NORMATIVAS

Para la elaboración de esta Política se han tenido en consideración las siguientes normas que regulan u orientan el tratamiento de datos personales realizado por la Compañía:

Constitución Política de la República, artículo 19 Nº 4;

Ley Nº 19.628 sobre Protección de la Vida Privada;

Ley Nº 20.575 que establece el Principio de Finalidad en el Tratamiento de Datos Personales;

Ley N° 19.496 que Establece Normas sobre Protección de los Derechos de los Consumidores.

Reglamento Interno de Orden, Higiene y Seguridad;

Código de Ética y Conducta de Negocios;

Marco Normativo de Seguridad de la Información

En caso de conflicto entre esta Política y una norma legal obligatoria, prevalecerá esta última y la Política se tendrá por no escrita en la parte contradictoria.

Los términos que se usan en esta Política se encuentran definidos en la sección 4 "Definiciones".

IV. DEFINICIONES

Anonimización: Tratamiento de datos personales irreversible que busca la eliminación del nexo entre la persona y el dato resultante, de modo tal que la información que se obtenga como producto de la anonimización no pueda asociarse a persona determinada o determinable ni sea re-identificable.

Base de datos: Conjunto de datos personales almacenados de forma física o digital.

Cesión de datos personales: Transferencia de datos personales de un responsable de datos personales a un tercero, quien los recibe y actúa respecto de ellos como responsable directo.

Compañía: Indistintamente, SMU S.A. y sus filiales Rendic Hermanos S.A., Súper 10 S.A., Alvi Supermercados Mayoristas S.A., Unidata S.A., Red Apoyo S.A Servicios Logísticos Santiago S.A. y Servicios Logísticos La Serena S.A.

Datos Personales: Aquellos datos relativos a cualquier información concerniente a personas naturales, identificadas o identificables. Los Datos Personales incluyen datos de identificación básica como nombre, teléfono, email y domicilio; características físicas, económicas, de salud, de conducta de compras o de navegación, etc. Los datos personales incluyen información que puede ser usada por sí misma, pero también en combinación con otra información para identificar a una persona.

Datos Sensibles: Datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual u otro de similar contenido.

Mandatario: Cualquier tercero, ya sea persona natural o jurídica, que trate datos personales de los cuales alguna de las Compañías es responsable, por mandato o encargo de la Compañía.

Política: Política de Protección de Datos Personales de la Compañía.

Regulación Aplicable: Normativa vigente en Chile relativa a protección y tratamiento de datos personales y que sea aplicable a la Compañía, incluyendo leyes, estatutos, códigos, ordenanzas, decretos, tratados internacionales ratificados por Chile y que se encuentren vigentes, directivas, estándares, y cualquier otra normativa que tenga carácter obligatorio.

Responsable: Persona natural o jurídica, pública o privada, que decide sobre los fines (el "para qué") y medios (el "qué": qué datos, durante cuánto tiempo y qué terceros pueden acceder legítimamente a los datos) del tratamiento de datos personales, independientemente de si los datos son tratados directamente por ella o a través de un mandatario del tratamiento.

Titular: Persona natural a la que se refieren los datos personales.

Tratamiento: Cualquier operación o complejo de operaciones o procedimientos técnicos, de carácter automatizado o no, que permitan recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, disociar, comunicar, ceder, transferir, transmitir o cancelar datos de carácter personal, o utilizarlos en cualquier otra forma.

V. POLÍTICA

1. PRINCIPIOS PARA EL TRATAMIENTO DE DATOS PERSONALES

Todo tratamiento de Datos Personales realizado por la Compañía deberá respetar los siguientes principios o reglas de conducta

i. Principio de licitud

El tratamiento de Datos Personales se hará siempre en cumplimiento de la Regulación Aplicable y la Política y, en cualquier caso, estará amparado en una base de licitud (la autorización legal o autorización del Titular).

ii. Principio de finalidad

Los Datos Personales deben ser recolectados con fines específicos, explícitos y lícitos. El tratamiento de Datos Personales deberá limitarse estrictamente al cumplimiento de estos fines, los que deben ser comunicados al Titular.

En consecuencia, la Compañía solo podrá utilizar los Datos Personales para los fines informados, salvo que la Regulación Aplicable autorice el tratamiento con finalidades distintas.

iii. Principio de calidad

Los Datos Personales deben ser exactos, completos y actuales en relación con los fines para los cuales se utilizan por la Compañía.

En este sentido, se deberán adoptar las medidas razonables para suprimir o rectificar, según sea necesario, los Datos Personales inexactos o desactualizados, y para permitir que Titulares puedan ejercer sus derechos de cancelación y rectificación.

iv. Principio de transparencia e información

La Compañía debe, gratuita y permanentemente, dar acceso a los Titulares a las políticas que regulen el tratamiento de sus Datos Personales, y a cualquiera otra información exigida por la Regulación Aplicable. Toda comunicación a los Titulares debe estar escrita en un lenguaje claro, preciso e inequívoco.

Las políticas que regulen el tratamiento de Datos Personales (denominadas comúnmente como políticas o avisos de privacidad) deberán contener, al menos, la siguiente información:

a) Fecha y versión;
b) Identificación de la(s) Compañía(s) Responsable, su representante legal y el Encargado de Protección de Datos; una vez que sea nombrado;
c) Identificación de punto de contacto para que los Titulares puedan enviar sus solicitudes;
d) Identificación del Tratamiento, incluyendo: tipos de datos que son objeto de tratamiento; la descripción genérica del universo de personas que comprenden; los destinatarios a los que se prevé comunicar o ceder los datos, y las finalidades del tratamiento.
e) Identificación genérica de la política y las medidas de seguridad adoptadas para proteger los Datos Personales.
f) Identificación de los derechos de los Titulares.

La Compañía deberá mantener actualizadas sus políticas de privacidad y establecer procesos determinados para que aquellas sean revisadas en caso de modificaciones al contenido informado en ellas y, al menos, una vez cada 2 años, en la medida que haya cambios normativos.

v. Principio de seguridad

Los Datos Personales que estén bajo el control de la Compañía (almacenados en bases de datos propias o de terceros) serán protegidos con las medidas de seguridad técnicas y organizativas idóneas para impedir su tratamiento no autorizado o ilícito y cualquier pérdida, filtración, daño o destrucción.

vi. Principio de confidencialidad

Los destinatarios de la Política deberán guardar secreto o confidencialidad acerca de los Datos Personales a los que accedan con ocasión de su relación con la Compañía, incluso después de haber cesado esta relación.

vii. Principio de minimización

Antes de realizar un tratamiento de Datos Personales determinado, se deberá evaluar si dicho tratamiento es realmente necesario para alcanzar el objetivo deseado. Con tal objeto, previo a iniciar una nueva actividad de tratamiento se deberá analizar si es posible alcanzar el mismo objetivo mediante la utilización de datos anonimizados o estadísticos, o mediante un tratamiento diferente que implique tratar de una menor cantidad de Datos Personales, o en una menor intensidad, en cuyo caso se deberán privilegiar estas opciones.

Una necesidad eventual o mera conveniencia no justificará el tratamiento los Datos Personales.

viii. Principio de proporcionalidad

Se deberán recolectar y tratar los Datos Personales que sean necesarios para cumplir las finalidades que justificaron su recolección. Se entenderá que se cumple con este principio si los datos que se recolectan: (a) son adecuados a la finalidad del tratamiento; (b) son pertinentes a la finalidad, y (c) no son excesivos.

La Compañía no deberá conservar los Datos Personales por más tiempo que el que sea necesario para el cumplimiento de los fines del Tratamiento. Transcurrido el tiempo indicado, la Compañía deberá eliminar o anonimizar los Datos Personales. Con este objeto, la Compañía deberá dictar un procedimiento que identifique los períodos de retención de documentos, en físico y formato electrónico, que contengan Datos Personales, en conformidad con la legislación aplicable.

2. BASES DE LICITUD PARA EL TRATAMIENTO DE DATOS PERSONALES

Todo Tratamiento de Datos Personales realizado por la Compañía deberá estar amparado en una base de licitud, esto es, por una hipótesis legal que autorice realizar el tratamiento de Datos Personales: la autorización legal o el consentimiento del Titular o lo que la ley disponga en su momento.

Deberán observarse las siguientes reglas dependiendo de la base de licitud que se emplee:

i. Tratamiento autorizado por la ley

Esta base de legalidad será aplicable cuando un Tratamiento de Datos Personales esté expresamente autorizado por ley, o sea imprescindible para ejecutar o cumplir una obligación de carácter legal.

Al aplicar esta base de legalidad, la Compañía deberá identificar claramente la(s) obligación(es), disposición(es) o autorización(es) legal(es) que sirven de fundamento. Si la obligación legal puede cumplirse sin el Tratamiento de Datos Personales, esta base legal no se aplicará.

ii. Tratamiento autorizado por el Titular

El consentimiento del Titular es la regla general. Es decir, para todo acto de tratamiento debe recogerse el consentimiento del Titular, salvo que exista una autorización u obligación legal aplicable, en virtud del punto i anterior.

Para levantar el consentimiento, deberá siempre asegurarse que éste es conferido:

- en forma expresa (es decir, no puede presumirse de otra acción),
- por escrito (en soporte electrónico o material), y
- siempre que el Titular sea clara y debidamente informado acerca de los propósitos del Tratamiento de sus datos y la comunicación o cesión de estos a terceros.

En cualquier caso, la Compañía deberá implementar los mecanismos necesarios para que este consentimiento se encuentre debidamente documentado, que le permita poder identificar y poder probar la existencia de la autorización y sus términos.

3. EJERCICIO DE LOS DERECHOS DE LOS TITULARES

La Compañía deberá informar a los Titulares (y mantenerlos permanentemente informado a través de la publicación de Políticas de Privacidad) de los derechos que le asisten en conformidad con la Regulación Aplicable y pondrán a su disposición las herramientas y procedimientos claros y sencillos para permitir su ejercicio.

En conformidad con la Regulación Aplicable, los Titulares tienen los siguientes derechos:

i. Derecho de acceso

Derecho del Titular para exigir a la Compañía información sobre: (a) los datos relativos a su persona que la Compañía esté tratando, (b) su procedencia, (c) los propósitos del almacenamiento y (d) la individualización de las personas a los cuales los datos son transmitidos regularmente.

ii. Derecho de rectificación

Derecho del Titular para exigir a la Compañía la modificación de sus Datos Personales cuando ellos sean erróneos, inexactos, equívocos o incompletos.

iii. Derecho de cancelación

Derecho del Titular para exigir a la Compañía la eliminación de sus Datos Personales cuando: (i) su almacenamiento carezca de fundamento legal; (ii) hayan caducado; (iii) los haya proporcionado voluntariamente; o (iv) ellos se utilicen para comunicaciones de carácter comercial, y el Titular no desee seguir figurando en el registro de datos.

iv. Derecho de bloqueo

Derecho del Titular para exigir la suspensión temporal del Tratamiento cuando: (i) haya proporcionado voluntariamente sus Datos Personales; o (ii) estos se utilicen para comunicaciones de carácter comercial y el Titular no desee seguir figurando en el registro de datos.

v. Derecho a revocar el consentimiento

Derecho del Titular para revocar el consentimiento que haya otorgado para el Tratamiento de sus datos.

El ejercicio de los derechos de los Titulares no es de aplicación absoluta y se deberá analizar caso a caso si la Compañía puede negar su ejercicio en conformidad a la Regulación Aplicable, debiendo hacer su requerimiento a través del canal de denuncias y consultas en la sección derechos ARCO. Por ejemplo, si la Compañía está tratando un dato en conformidad a una obligación legal, no será aplicable una solicitud de ejercicio de derecho de eliminación.

4. SEGURIDAD Y CONFIDENCIALIDAD

i. Medidas de seguridad

La Compañía adoptará medidas organizativas y técnicas apropiadas para garantizar la seguridad de los Datos Personales que trate, con independencia de que estos se encuentren en formato físico o electrónico. Estas medidas estarán destinadas a:

a) proteger la confidencialidad, integridad, disponibilidad y resiliencia de los sistemas de información de la Compañía en general, y de los Datos Personales en particular.

b) evitar la alteración, destrucción o pérdida de los datos, o el tratamiento o acceso no autorizados.

Antes de la introducción de nuevas formas de tratamiento, particularmente en nuevos productos, servicios, o sistemas tecnológicos, se deberá hacer una revisión de las medidas de seguridad implementadas con el objeto de verificar si son adecuadas o deben ser modificadas.

Las medidas de seguridad de la Compañía estarán determinadas en conformidad con el Marco Normativo de Seguridad de la Información.

La implementación de medidas de seguridad deberá considerar, al menos:

a) el estado actual de la técnica y los costos de aplicación;

b) la naturaleza, alcance, contexto y fines del tratamiento; y

c) la probabilidad de los riesgos y la gravedad de sus efectos en relación con el tipo de Datos Personales tratados.

Todas las gerencias de la Compañía facilitarán al Encargado de Protección de Datos acceso al conocimiento sobre los sistemas y/o procesos que involucren Tratamiento de Datos Personales, con el objeto que el encargado levante un inventario y determine si se deben implementar resguardos adicionales en consideración a la Política.

ii. Acceso a datos personales

Los destinatarios de la Política sólo tendrán acceso a los Datos Personales que sean necesarios para el cumplimiento de sus labores específicas.

Las gerencias de la Compañía deberán implementar las medidas que sean necesarias para que estas reglas sean debidamente observadas por sus trabajadores (as).

iii. Gestión de vulneraciones a medidas de seguridad

5. FORMACIÓN Y CONCIENCIA

La Compañía, a través del Encargado de Protección de Datos, implementarán un plan anual de formación con el objeto de crear y mantener una cultura de protección de Datos Personales. El calendario, y las correspondientes campañas se determinarán el primer trimestre del año en el que se ofrezcan las acciones formativas. Estas podrán ser de carácter general, esto es, dirigidas a todos los trabajadores (as) de la Compañía (y si se estima conveniente, a directores, proveedores, y/o otros que traten Datos Personales por cuenta de la Compañía), o específicas, es decir, dirigidas a aquellas áreas y personas que en virtud de su actividad requieren una mayor profundidad en el tema.

6. CESIÓN Y COMUNICACIÓN DE DATOS PERSONALES

i. Comunicación de datos personales desde un tercero

Si un tercero comunica Datos Personales a la Compañía, se deberán tomar las medidas para asegurar que la Compañía puede usar los datos lícitamente para el propósito deseado. En este contexto, la comunicación y sus especificaciones deberán constar por escrito y se deberán incluir los resguardos contractuales que al efecto haya elaborado la Gerencia Legal.

ii. Cesión de datos personales a un tercero

La Compañía será transparente con los Titulares en cuanto a la existencia de Cesiones de Datos Personales a un tercero y, cuando sea requerido en conformidad a laRegulación Aplicable, deberán obtener su autorización para efectuar la Cesión.

En particular, las políticas de privacidad de la Compañía deberán informar acerca de la identidad de estos terceros y los propósitos asociados a la transferencia.

iii. Comunicación de datos personales a un Mandatario

La Compañía iniciará un proceso progresivo de identificación de los Mandatarios para el Tratamiento, priorizando aquellos que lo hacen de forma habitual o tratan gran cantidad de Datos Personales. Finalizado el proceso indicado, la Compañía tomará las siguientes medidas que estime conveniente implementar en los contratos con Mandatarios y/o sean requeridas por la Regulación Aplicable:

a) Cláusula de mandato para el tratamiento de datos: esta cláusula será incorporada, por defecto, en todos los modelos de contratos utilizados por la Compañía cuyos servicios, por su naturaleza, puedan involucrar tratamiento de Datos Personales.

b) Anexo de mandato para el tratamiento de datos: la cláusula indicada en la letra (a) anterior, deberá ser sustituida por un Anexo de mandato para el tratamiento de datos, que deberá ser solicitado a la Gerencia de Procurement de SMU S.A. siempre que los servicios objeto del contrato con el Mandatario involucren:

i. Entrega habitual, continua o de un gran volumen de Datos Personales al Mandatario.

ii. Entrega, o acceso por parte del proveedor a Datos Sensibles.

7. TRANSFERENCIA INTERNACIONAL DE DATOS PERSONALES

La Comunicación o Cesión de Datos Personales efectuada por la Compañía a un tercero en el extranjero deberá realizarse en cumplimiento con la Regulación Aplicable.

La Compañía informará a los Titulares si sus Datos Personales serán transferidos fuera de Chile en las políticas de privacidad respectivas.

En la medida que sea adecuado bajo la Regulación Aplicable, se privilegiará las transferencias internacionales a terceros que tengan políticas adecuadas de Tratamiento de Datos Personales, y a países que cuenten con una normativa obligatoria para la protección de datos personales de igual o mejor estándar que aquella establecida en Chile.

8. PRIVACIDAD DESDE EL DISEÑO Y POR DEFECTO

En el desarrollo o puesta en marca de productos, servicios, sistemas, aplicaciones, procesos o proyectos que involucren tratamiento de Datos Personales, la Compañía deberá realizar un análisis documentado del cumplimiento de los requerimientos de la Regulación Aplicable. Con este objeto, se deberá informar al Encargado de Protección de Datos sobre el acontecimiento de cualquiera de las situaciones indicadas de forma que aquel pueda tomar, desde el origen, las medidas de resguardo que sean necesarias.

VI. ROLES Y RESPONSABILIDADES

La responsabilidad de la implementación y mantenimiento de la Política recae en el Encargado de Protección de Datos; siendo este último quien tiene la responsabilidad administrativa por su ejecución y supervisión.

Rol	Responsabilidades
Directorio de SMU S.A.	• Nombrar al Encargado de Protección de Datos en atención a sus cualidades profesionales y conocimiento en la normativa y prácticas de protección de Datos Personales, garantizando la independencia que corresponda a sus funciones. • Proporcionar los recursos necesarios dentro del presupuesto disponible de las Compañías para que se puedan desempeñar las funciones asociadas a la protección de Datos Personales. • Sugerir y velar por la implementación de esta Política y los procedimientos dictados conforme a ella. • Velar para que, cada dos años como mínimo, las Compañías lleven una auditoría, interna o externa, que tenga por objetivo la revisión del cumplimiento de los puntos enumerados en esta Política y Regulación Aplicable. Cualquier incumplimiento que ponga de manifiesto la auditora de datos, será objeto de inmediata corrección por la sociedad respectiva.
Comité de ética y conducta de negocios	• Aprobar esta Política, así como las demás normas y procedimientos dirigidas al cumplimiento de la Regulación Aplicable.
Encargado de Protección de Datos	• Supervisar el cumplimiento de la Regulación Aplicable y normativa corporativa en materia de protección de datos. • Asesorar a las Compañías sobre sus obligaciones en materia de protección de Datos Personales de acuerdo con la Regulación Aplicable y esta Política, así como proponer mejoras a esta última al Comité de Protección de Datos. • Proponer al Comité de Protección de Datos la implementación de los controles de cumplimiento pertinentes para el cumplimiento de la Regulación Aplicable. • Velar por la concienciación y formación del personal que participa en las operaciones de Tratamiento de Datos Personales. • Reportar e informar al Comité de Protección de Datos: - las medidas que sean necesarias para el mejor cumplimiento de la Regulación Aplicable y, si corresponde, resolver cualquier deficiencia o incumplimiento, y en general, - todo lo relacionado con la implementación, monitoreo y cumplimiento de esta Política. • Diseñar los procedimientos (i) de gestión de derechos de los Titulares; y (ii) de gestión de incidentes y brechas de seguridad que afecten Datos Personales. • Asesorar a las Compañías en la interpretación y aplicación de esta

	Política. • En coordinación y con el soporte de los Responsables de la Actividad de Tratamiento, (i) cooperar con la Autoridad de Protección de Datos competente, y ser la persona de contacto en SMU; (ii). dar respuesta a las solicitudes de ejercicio de derechos de los Titulares. • Notificar los incidentes de seguridad a la Autoridad de Protección de Datos competente. • Dirigir el Comité de Protección de Datos. • Formar parte del Comité Corporativo de Seguridad de la Información, supervisando y apoyando activamente en el cumplimiento de la Regulación Aplicable. • Establecer el plan de formación en materia de protección de Datos Personales, incluyendo su contenido y calendario. • Compartir mejores prácticas sobre protección de Datos Personales. • Realizar análisis de cumplimiento de la Regulación Aplicable previo a la implementación de nuevos proyectos. • Asesorar en la revisión y actualización de los contratos que impliquen comunicaciones de datos de o a terceros, cualquiera que sea su forma (acceso remoto o transferencia), y que de conformidad con esta Política o con la Regulación Aplicable, requieren cláusulas de protección de Datos. • Supervisar la implementación, en tiempo y forma, de las recomendaciones resultantes de las auditorías de protección de Datos Personales, hasta su efectiva regularización.
Responsables de la Actividad de Tratamiento	• Personas responsables a cargo de coordinar y supervisar el cumplimiento de la Regulación Aplicable y las normas corporativas del Grupo SMU S.A. en materia de protección de Datos Personales en conformidad con las siguientes categorías: - Datos de clientes del club de fidelización: se deberá designar una persona responsable en Unidata S.A. - Datos de clientes e-commerce: se deberá designar una persona responsable en Unidata S.A. - Datos de trabajadores: sin perjuicio de la existencia de Gerencias de Personas para cada una de las Compañías, se deberá designar a una única persona responsable en SMU S.A. - Datos de proveedores personas naturales e interlocutores de personas jurídicas: se deberá designar a una única persona responsable en SMU S.A. • Las Gerencias Generales de cada una de las sociedades indicadas tendrán la obligación de designar a las personas a cargo de realizar las responsabilidades que les competen en conformidad

	con esta Política.
	• Supervisar que las políticas de privacidad en la esfera de su competencia estén completas, actualizadas y sean coherentes con los requerimientos de esta Política y la Regulación Aplicable. • Escalar al Encargado de Protección de Datos las dudas sobre la interpretación y aplicación de la Política y sus procedimientos. • Dar soporte al Encargado de Protección de Datos para la asignación de responsabilidades y formaciones de personal en la sociedad, así como en la realización de auditorías. • Cooperar con el Encargado de Protección de Datos en la realización de los análisis de cumplimiento de la Regulación Aplicable previo a la implementación de nuevos proyectos. • Ejecutar el plan de formación definido por el Comité de Protección de Datos. • Implementar, tiempo y forma, las recomendaciones resultantes de las auditorías de protección de Datos Personales.
Comité de Protección de Datos	• El Comité estará conformado por: - Encargado de Protección de Datos - Responsables de la Actividad del Tratamiento - Responsables de Ciberseguridad de IT - Representante de la Gerencia Legal de SMU S.A.
	• Coordinar las actuaciones de los distintos Responsables de la Actividad de Tratamiento con el Encargado de Protección de Datos, de manera de asegurar un estándar adecuado y homogéneo en las actividades de tratamiento bajo su responsabilidad. • Discutir y proponer mejoras a esta Política y procedimientos que sean dictados conforme a ella. • Sugerir y acordar propuestas dirigidas a solucionar posibles incumplimientos de la Regulación Aplicable y esta Política y sus procedimientos.
Directorio de cada sociedad del Grupo SMU S.A.	• Conocer los informes que emita el Encargado de Protección de Datos sobre las actuaciones de protección de Datos Personales realizadas en el último año, incluyendo estadísticas sobre el ejercicio de derechos de los Titulares, demandas, incidentes y brechas de seguridad que afecten Datos Personales, nuevos proyectos, y el plan de acción para el año siguiente. • Promover y facilitar la efectiva implementación de esta Política dentro del ámbito de sus respectivas funciones y responsabilidades. • Facilitar los recursos que sean necesarios para proteger los Datos

	Personales tratados en su sociedad. • Supervisar el cumplimiento e implementación de la Regulación Aplicable, esta Política y los procedimientos dictados al efecto.
Propietarios de la Información	• Usuario dueño de la información asociada a un área/proceso de la compañía, responsable de definir quiénes tienen acceso y qué pueden hacer con la información.
	• Informar al Responsable de la Actividad de Protección de Datos de cualquier proyecto, herramienta, aplicación o proceso que implique o requiera el tratamiento de Datos Personales desde el principio. • Realizar el mapeo de datos de los tratamientos de Datos Personales que realizan. • Implementar y observar las recomendaciones del Responsable de la Actividad de Protección de Datos. • Solicitar al Encargado de Protección de Datos las cláusulas y contratos de protección de datos que deban incorporarse a los contratos con proveedores o terceros que implique un intercambio o revelación de Datos Personales. • Colaborar con el Responsable de la Actividad de Protección de Datos facilitando la información y documentación éste precise para el desempeño de sus funciones, especialmente: - Para la gestión de derechos, quejas y reclamaciones en materia de protección de datos; - para la contención, investigación y respuesta frente a incidentes y brechas de seguridad. • Observar con diligencia las medidas de seguridad técnicas y organizativas de las Compañías. • Asistir y participar de manera proactiva en las formaciones de protección de datos.

VII. DENUNCIAS y CONSULTAS

La Compañía ha dispuesto un Canal de Denuncias y Consultas en su página web para dirigirse al Encargado de Protección de Datos ante cualquier actividad anómala, prohibida o que se contraponga con lo dispuesto en la Política o la normativa de datos personales. En caso de dudas respecto de si una determinada conducta podría infringir lo dispuesto en la Política, la normativa interna que se haya dictado sobre la materia que ella trata y, la Regulación Aplicable, se deberá consultar al Encargado de Protección de Datos y, dentro de lo posible, abstenerse de actuar mientras no reciban respuesta a dicha consulta.

VIII. CUMPLIMIENTO

Los destinatarios de la Política actuarán conscientes de que el incumplimiento de la Política y la Regulación Aplicable puede generar consecuencias para la Compañía en su calidad de Responsable de datos (ej. consecuencias legales, pérdidas asociadas a negocios y daño reputacional); para los trabajadores (ej. medidas disciplinarias); y para los Titulares de datos personales (ej. daño patrimonial o moral). Por consiguiente, todos los destinatarios de la Política deberán cumplirla, así como sus normas, procedimientos y cualquier documento que se cree al efecto.

El incumplimiento de las obligaciones emanadas de la Política, normas específicas, estándares, procedimientos u otro documento que se derive de estos, deberá ser informado por el Encargado de Protección de Datos al Directorio de SMU S.A., quien tomará en consideración la particularidad de cada situación, y adoptará las medidas adecuadas y pertinentes que corresponda.

Cualquier infracción a la Política, y a los procedimientos o normas que deriven de ella, por parte de un trabajador(a) de la Compañía, podrá dar lugar a medidas disciplinarias en contra del infractor de acuerdo con lo establecido en el Reglamento Interno de Orden, Higiene y Seguridad de la Compañía.

IX. DIVULGACIÓN, VIGENCIA Y APLICACIÓN

Esta Política se presume conocida desde su publicación y su vigencia será de carácter indefinido. La misma regla se aplicará en caso de cualquier modificación.

Esta Política es obligatoria para todos los Trabajadores (as) de SMU S.A. y sus filiales.