POLÍTICA DE PRIVACIDAD DE DATOS

Contenido

I. INTRODUCCIÓN 1
II. OBJETO 1
III. CONDICIONES GENERALES 1
A. Ámbito de aplicación y alcance 1
B. Referencias normativas 2
C. Términos y definiciones 2
D. Principios de protección de datos personales 3
E. Derechos de los titulares 3
IV. BASES LEGALES PARA EL TRATAMIENTO DE DATOS 4
V. DATOS PERSONALES Y FINALIDADES DEL TRATAMIENTO 4
A. Tipos de datos personales 4
B. Finalidades generales 5
C. Clientes y potenciales clientes 5
D. Consumidores finales 5
E. Proveedores, contratistas y socios comerciales 6
F. Candidatos y colaboradores 6
VI. GESTIÓN DE LOS DATOS PERSONALES 6
A. Obtención de los datos 6
B. Información y consentimiento 6
C. Uso y conservación 6
D. Eliminación de datos 7
VII. SEGURIDAD DE LOS DATOS PERSONALES 7
VIII. COMUNICACIÓN Y TRANSFERENCIA DE DATOS PERSONALES 7
IX. ROLES Y RESPONSABILIDADES 8
A. Alta Dirección 8
B. Delegado u Oficial de Protección de Datos 8
C. Áreas que tratan datos personales 9
D. Infraestructura y tecnología 9

E. Área Legal 9
F. Auditoría Interna 9
G. Colaboradores 9
X. ATENCIÓN DE SOLICITUDES Y EJERCICIOS DE DERECHOS 10
XI. GESTIÓN DE INCIDENTES DE SEGURIDAD 10
XII. DISPOSICIONES FINALES 10
A. Incumplimientos 10
B. Revisión y actualización 10
C. Vigencia 10

I. INTRODUCCIÓN

UNO Corp. reconoce la importancia de proteger los datos personales tratados en el desarrollo de las actividades comerciales, administrativas y operativas de las empresas que conforman el Grupo Empresarial, promoviendo su tratamiento responsable, seguro, lícito y transparente.

En este contexto, la presente Política establece los principios, criterios y responsabilidades que orientan el tratamiento y la protección de los datos personales, de conformidad con las disposiciones legales aplicables en cada jurisdicción y los estándares corporativos.

Asimismo, busca fortalecer la confianza de los clientes, colaboradores, proveedores y demás partes interesadas, mediante la adopción de prácticas que contribuyan a prevenir y mitigar los riesgos asociados al tratamiento inadecuado de datos personales.

II. OBJETO

Establecer un marco corporativo común de principios, lineamientos y responsabilidades para el tratamiento y la protección de los datos personales por parte de las sociedades comprendidas en el ámbito de aplicación de la presente Política, de conformidad con la legislación aplicable en cada jurisdicción, los estándares corporativos y las buenas prácticas en materia de privacidad y protección de datos personales, promoviendo el respeto y ejercicio de los derechos de los titulares y un tratamiento adecuado y seguro de su información.

III. CONDICIONES GENERALES

A. Ámbito de aplicación y alcance

La presente Política es de cumplimiento obligatorio para las sociedades que conforman UNO Corp. y se encuentran comprendidas en su ámbito de aplicación (en adelante, las "Empresas").

Aplica a los colaboradores, proveedores, contratistas, socios comerciales y demás terceros que participen en el tratamiento de datos personales por cuenta de las Empresas, conforme a las responsabilidades que les correspondan.

Comprende los datos personales de clientes, colaboradores, proveedores y demás personas naturales, garantizando el respeto de sus derechos conforme a la legislación aplicable en cada jurisdicción. Cada Empresa asumirá las responsabilidades que legalmente le correspondan respecto al tratamiento de dichos datos.

Su alcance incluye las bases de datos, archivos, sistemas y demás medios físicos o electrónicos, así como las actividades de recopilación, almacenamiento, uso, transferencia, conservación, eliminación y cualquier otra operación relacionada con el tratamiento de datos personales.

B. Referencias normativas

Los lineamientos establecidos se basan en los principios internacionales de protección de datos personales y en la legislación vigente en los países donde operan las Empresas, buscando mantener criterios comunes de protección de datos en toda la organización.

Cada Empresa deberá cumplir con las disposiciones legales y regulatorias que le correspondan, según el país donde opera y la naturaleza de sus actividades.

Cuando exista alguna diferencia entre estos lineamientos y la legislación aplicable en cada país, se deberá cumplir con lo establecido en la ley, manteniendo los demás lineamientos que no sean contrarios a ella.

C. Términos y definiciones

Empresas: Sociedades que conforman UNO Corp. y se encuentran comprendidas en el ámbito de aplicación de esta Política.

Datos personales: Cualquier información que permita identificar a una persona, directamente o mediante su combinación con otros datos, como su nombre, número de identidad, dirección, teléfono o correo electrónico.

Datos sensibles: Datos personales que requieren especial protección porque pueden afectar la privacidad de una persona o dar lugar a discriminación, como información sobre su salud, origen étnico, creencias, opiniones políticas, datos biométricos, genéticos u orientación sexual.

Derechos de los titulares: Derechos que permiten a las personas conocer, corregir y controlar el tratamiento de sus datos personales, de acuerdo con la legislación aplicable en cada país.

Encargado del tratamiento: Persona o empresa que trata datos personales por cuenta de un responsable, siguiendo sus instrucciones.

Perfilamiento: Uso automatizado de datos personales para analizar o predecir características, comportamientos o preferencias de una persona.

Responsable del tratamiento: Persona o empresa que decide para qué y cómo se utilizan los datos personales.

Titular: Persona a quien pertenecen los datos personales.

Transferencia de datos: Comunicación o entrega de datos personales a otra persona o entidad, conforme a las condiciones legales aplicables en cada país.

Tratamiento de datos personales: Cualquier actividad realizada con datos personales, como recopilarlos, registrarlos, almacenarlos, consultarlos, utilizarlos, compartirlos o eliminarlos, por medios físicos o electrónicos.

D. Principios de protección de datos personales

Las Empresas deberán aplicar los siguientes principios como estándares comunes para el tratamiento de datos personales, respetando las disposiciones legales de cada país:

Exactitud: Mantener los datos correctos, completos y actualizados cuando sea necesario.

Lealtad: Obtener y utilizar los datos de manera honesta, sin prácticas engañosas o que manipulen las decisiones de las personas.

Consentimiento y finalidad: Utilizar los datos para fines legítimos, específicos e informados, obteniendo el consentimiento cuando sea legalmente necesario.

Minimización: Recopilar y utilizar únicamente los datos necesarios para cada finalidad.

Transparencia: Proporcionar información clara y comprensible sobre el uso de los datos personales.

Seguridad: Aplicar medidas para evitar el acceso, uso, modificación, pérdida o divulgación no autorizada de datos.

Licitud: Tratar los datos conforme a la legislación aplicable en cada país y los lineamientos internos.

Temporalidad: Conservar los datos durante el tiempo necesario para cumplir su finalidad y las obligaciones legales correspondientes.

Responsabilidad demostrada: Mantener medidas y controles que permitan comprobar el cumplimiento de las obligaciones de protección de datos.

Ejercicio progresivo de las facultades: Proteger los datos de niñas, niños y adolescentes, considerando su edad, madurez e interés superior, así como la autorización de sus representantes legales cuando corresponda.

Privacidad desde el diseño y por defecto: Incorporar la protección de datos desde la creación de procesos, productos y servicios, procurando que únicamente se utilice la información necesaria.

E. Derechos de los titulares

Las personas podrán ejercer los derechos relacionados con sus datos personales, de acuerdo con la legislación aplicable en cada país.

Entre estos derechos se encuentran, cuando sean reconocidos por la normativa correspondiente:

Información: Conocer quién utiliza sus datos, para qué se necesitan y con quién podrán compartirse.

Acceso: Consultar los datos personales que las Empresas mantienen sobre ellas.

Rectificación: Solicitar la corrección o actualización de datos incorrectos, incompletos o desactualizados.

Cancelación o supresión: Solicitar la eliminación de sus datos cuando corresponda.

Oposición: Solicitar que sus datos dejen de utilizarse para determinados fines.

Portabilidad: Solicitar sus datos en un formato que permita trasladarlos a otro responsable.

Olvido: Solicitar la eliminación o desvinculación de datos difundidos en medios digitales.

Limitación: Solicitar restricciones sobre el uso de sus datos.

Protección frente a decisiones automatizadas: Ejercer las garantías que correspondan frente a decisiones basadas únicamente en el tratamiento automatizado de datos.

Las condiciones, requisitos y excepciones para ejercer estos derechos dependerán de la legislación de cada jurisdicción y de los mecanismos establecidos por la Empresa responsable del tratamiento.

IV. BASES LEGALES PARA EL TRATAMIENTO DE DATOS

Las Empresas deberán contar con una base legal válida para recopilar y utilizar datos personales, de acuerdo con la legislación aplicable en cada país.

Entre las condiciones que pueden permitir el tratamiento se encuentran:

Consentimiento: Cuando la persona haya autorizado el uso de sus datos de manera libre, específica e informada.

Relación contractual: Cuando los datos sean necesarios para preparar, establecer o cumplir una relación comercial, laboral o contractual.

Obligación legal: Cuando el tratamiento sea necesario para cumplir obligaciones legales, regulatorias, fiscales o laborales.

Interés legítimo: Cuando la legislación lo permita y exista una necesidad legítima que justifique el tratamiento, respetando los derechos de la persona.

Cada Empresa deberá verificar qué condiciones reconoce la legislación de su jurisdicción y cumplir los requisitos correspondientes.

El tratamiento de datos sensibles y de información de niñas, niños y adolescentes estará sujeto a las medidas especiales de protección que correspondan.

V. DATOS PERSONALES Y FINALIDADES DEL TRATAMIENTO

Las Empresas podrán recopilar y utilizar diferentes tipos de datos personales, según sus actividades y la relación que mantengan con cada persona.

A. Tipos de datos personales

Identificación y contacto: Nombre, documento de identidad, fecha de nacimiento, firma, dirección, teléfono y correo electrónico.

Comerciales y financieros: Historial de compras, facturación, medios de pago, información bancaria, tributaria, crediticia y transaccional.

Laborales y profesionales: Formación académica, experiencia, referencias, remuneración, desempeño, beneficios, seguridad social y datos de beneficiarios o familiares cuando sean necesarios.

Cumplimiento y debida diligencia: Información de representantes, accionistas, beneficiarios finales y demás datos necesarios para la evaluación y gestión de riesgos.

Digitales y de navegación: Información relacionada con aplicaciones, sitios web, plataformas digitales y datos de ubicación, cuando corresponda.

Imágenes y registros audiovisuales: Fotografías, grabaciones de voz, videovigilancia y registros de acceso.

Datos sensibles: Información biométrica, de salud u otros datos que requieran especial protección, cuando exista una justificación y se cumplan los requisitos legales.

B. Finalidades generales

Cuando corresponda, las Empresas podrán utilizar datos personales para:

- Cumplir obligaciones legales, regulatorias y contractuales.
- Atender requerimientos de autoridades competentes.
- Administrar sistemas, expedientes y registros.
- Proteger las instalaciones, las personas y los activos.
- Realizar auditorías, controles internos, investigaciones y actividades de cumplimiento.
- Prevenir fraudes y gestionar riesgos.
- Compartir información con destinatarios autorizados para cumplir finalidades legítimas.

C. Clientes y potenciales clientes

- Gestionar relaciones comerciales y contractuales.
- Prestar productos y servicios.
- Realizar procesos de identificación, debida diligencia y evaluación de riesgos.
- Evaluar solicitudes de crédito, gestionar cobros y efectuar consultas o reportes crediticios cuando la legislación lo permita.
- Informar sobre cambios relacionados con los productos o servicios contratados.

D. Consumidores finales

- Administrar programas de lealtad, promociones, sorteos y beneficios.
- Gestionar aplicaciones móviles y plataformas digitales.
- Atender consultas y evaluar la satisfacción de los consumidores.
- Analizar hábitos de consumo y preferencias para mejorar productos y servicios.
- Desarrollar comunicaciones y campañas comerciales conforme a los requisitos aplicables.

- Utilizar imágenes, nombres o voces en actividades promocionales cuando exista la autorización correspondiente.

E. Proveedores, contratistas y socios comerciales

- Evaluar y seleccionar contrapartes.
- Realizar procesos de debida diligencia y gestión de riesgos.
- Administrar contratos, pagos, facturación y registros contables.
- Evaluar el desempeño y cumplimiento de las obligaciones comerciales.

F. Candidatos y colaboradores

- Gestionar procesos de reclutamiento, selección y contratación.
- Administrar expedientes y relaciones laborales.
- Gestionar remuneraciones, beneficios, seguros, seguridad social y demás prestaciones.
- Desarrollar actividades de capacitación, bienestar y seguridad ocupacional.
- Utilizar imágenes, nombres o voces para fines corporativos cuando corresponda y se cuente con la autorización necesaria.

Cada Empresa deberá informar las finalidades específicas del tratamiento y cumplir los requisitos legales de su jurisdicción.

VI. GESTIÓN DE LOS DATOS PERSONALES

Las Empresas deberán proteger los datos personales durante todas las etapas de su tratamiento, desde su obtención hasta su eliminación.

A. Obtención de los datos

Los datos deberán recopilarse de manera lícita y transparente, solicitando únicamente la información necesaria para las finalidades establecidas.

B. Información y consentimiento

Las personas deberán recibir información clara sobre el tratamiento de sus datos mediante los avisos de privacidad correspondientes.

Cuando la legislación lo requiera, deberá obtenerse y conservarse el consentimiento conforme a las condiciones establecidas en cada país.

C. Uso y conservación

Los datos deberán utilizarse para las finalidades autorizadas y mantenerse en medios físicos o electrónicos protegidos.

Su conservación estará limitada al tiempo necesario para cumplir dichas finalidades y las obligaciones legales o contractuales aplicables.

D. Eliminación de datos

Cuando los datos ya no sean necesarios y hayan concluido los plazos de conservación correspondientes, deberán eliminarse, anonimizarse o destruirse de forma segura, siguiendo los procedimientos internos.

VII. SEGURIDAD DE LOS DATOS PERSONALES

Las Empresas deberán implementar medidas técnicas, organizativas y físicas para proteger los datos personales frente a accesos no autorizados, pérdidas, alteraciones, divulgaciones o usos indebidos.

Estas medidas comprenderán:

Seguridad tecnológica: Controles de acceso, autenticación, respaldo, recuperación de información y protección de los sistemas.

Seguridad organizativa: Procedimientos internos, acuerdos de confidencialidad, capacitación, clasificación de información y evaluaciones periódicas.

Seguridad física: Controles de acceso a instalaciones y espacios donde se almacene información personal.

Las medidas deberán ajustarse a la naturaleza de los datos, los riesgos identificados y las obligaciones legales aplicables en cada jurisdicción.

Los requisitos específicos de seguridad tecnológica, incluidos los relacionados con cifrado, continuidad operativa y protección de plataformas digitales, se desarrollarán en los procedimientos y estándares internos correspondientes.

VIII. COMUNICACIÓN Y TRANSFERENCIA DE DATOS PERSONALES

Las Empresas podrán compartir datos personales cuando exista una finalidad legítima, una base legal válida y se cumplan las condiciones de protección establecidas en cada jurisdicción.

Los destinatarios podrán incluir:

- Otras sociedades de UNO Corp., cuando sea necesario para actividades administrativas, comerciales, operativas o de cumplimiento.
- Proveedores y contratistas que traten datos por cuenta de las Empresas.
- Entidades financieras, aseguradoras, auditores, asesores y otros terceros necesarios para el desarrollo de las operaciones.

- Autoridades administrativas, judiciales o regulatorias, cuando exista una obligación legal o un requerimiento válido.

Cuando se compartan datos con terceros, deberán establecerse las obligaciones de confidencialidad, seguridad y protección de datos que correspondan.

Las transferencias internacionales deberán cumplir los requisitos legales del país desde el cual se compartan los datos y, cuando corresponda, del país receptor.

Antes de realizar una transferencia internacional, la Empresa responsable deberá verificar los requisitos aplicables y establecer las garantías necesarias, que podrán incluir acuerdos contractuales, autorizaciones, consentimiento u otros mecanismos legalmente reconocidos.

La pertenencia a UNO Corp. no exime a las sociedades de cumplir las obligaciones legales relacionadas con el intercambio de datos personales.

IX. ROLES Y RESPONSABILIDADES

La protección de los datos personales es una responsabilidad compartida. Cada Empresa y sus áreas deberán cumplir las obligaciones que les correspondan conforme a sus funciones y a la legislación aplicable.

A. Alta Dirección

- Promover una cultura de protección de datos personales.
- Aprobar los lineamientos y recursos necesarios.
- Impulsar la implementación y mejora de las medidas de protección.

B. Delegado u Oficial de Protección de Datos

Cada Empresa deberá contar con esta figura cuando lo exija la legislación aplicable. También podrá designarse una función equivalente como parte de los lineamientos corporativos.

Sus funciones, independencia y condiciones de designación deberán ajustarse a las disposiciones legales de cada jurisdicción.

Entre sus responsabilidades, cuando correspondan a su designación, se encuentran:

- Informar y asesorar sobre las obligaciones de protección de datos.
- Supervisar el cumplimiento de la normativa y los lineamientos internos.
- Evaluar y dar seguimiento a los riesgos relacionados con datos personales.
- Promover la capacitación y concientización.
- Supervisar los mecanismos de atención de solicitudes de los titulares.
- Participar, según sus competencias, en la evaluación de incidentes y en la coordinación con las autoridades correspondientes.

Cuando no exista una figura legalmente exigida, las Empresas deberán definir las funciones responsables de coordinar estas actividades.

C. Áreas que tratan datos personales

- Utilizar los datos únicamente para finalidades autorizadas.
- Obtener y conservar los consentimientos cuando corresponda.
- Aplicar los controles de seguridad establecidos.
- Informar sobre nuevos procesos, sistemas o proyectos que involucren datos personales.
- Coordinar con las funciones competentes las transferencias de información a terceros.
- Reportar oportunamente los incidentes o riesgos identificados.

D. Infraestructura y tecnología

- Implementar y mantener las medidas técnicas de seguridad.
- Administrar los accesos y mecanismos de autenticación.
- Mantener los mecanismos de respaldo y recuperación.
- Atender los incidentes tecnológicos y coordinar su comunicación a las funciones correspondientes.

E. Área Legal

- Asesorar sobre la legislación aplicable en cada país.
- Revisar los contratos y acuerdos relacionados con datos personales.
- Apoyar la evaluación de riesgos legales y transferencias de información.

F. Auditoría Interna

- Evaluar la eficacia de los controles de protección de datos.
- Verificar el cumplimiento de los lineamientos internos.
- Recomendar mejoras y dar seguimiento a los planes de acción.

G. Colaboradores

- Utilizar los datos personales únicamente para sus funciones autorizadas.
- Mantener la confidencialidad de la información.
- Proteger las credenciales y accesos asignados.
- Cumplir los procedimientos internos.
- Reportar de inmediato cualquier pérdida, acceso indebido o sospecha de vulneración de datos personales.

X. ATENCIÓN DE SOLICITUDES Y EJERCICIOS DE DERECHOS

Las personas podrán presentar consultas, reclamaciones o solicitudes relacionadas con sus datos personales a través de los canales establecidos por la Empresa responsable del tratamiento.

Cada Empresa deberá atender las solicitudes conforme a los derechos, requisitos, plazos y excepciones establecidos en la legislación aplicable en su jurisdicción.

Las áreas competentes deberán verificar la identidad del solicitante, coordinar la atención, comunicar la respuesta y conservar el registro de las actuaciones realizadas.

Cuando no exista un procedimiento legal específico, las Empresas deberán aplicar los mecanismos internos establecidos para garantizar una atención adecuada y oportuna.

Los canales de contacto y los procedimientos particulares deberán ser informados por cada Empresa.

XI. GESTIÓN DE INCIDENTES DE SEGURIDAD

Cualquier pérdida, acceso no autorizado, divulgación, alteración o uso indebido de datos personales deberá reportarse inmediatamente a través de los canales internos establecidos.

Las Empresas deberán activar los procedimientos correspondientes para identificar, contener, evaluar, documentar y corregir el incidente.

El delegado u Oficial de Protección de Datos, o la función equivalente designada, participará según sus competencias en la evaluación de los riesgos y las medidas necesarias.

Cuando la legislación aplicable exija notificar un incidente, la Empresa responsable deberá comunicarlo a las autoridades y a las personas afectadas dentro de los plazos correspondientes.

En los países donde no exista una obligación legal de notificación, deberán documentarse los incidentes, evaluarse sus consecuencias y aplicarse las medidas correctivas necesarias.

XII. DISPOSICIONES FINALES

A. Incumplimientos

El incumplimiento de estos lineamientos podrá dar lugar a medidas disciplinarias, de acuerdo con la gravedad de la conducta, el reglamento interno y la legislación laboral aplicable en cada país, sin perjuicio de otras responsabilidades legales que correspondan.

B. Revisión y actualización

La Política será revisada periódicamente y cuando existan cambios legales, regulatorios u operativos que requieran su actualización.

C. Vigencia

La Política entrará en vigor conforme a los mecanismos de aprobación y adopción establecidos por las sociedades comprendidas en su ámbito de aplicación.