POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES DE LOS EMPLEADOS	PRO-01
	Revisión 00

REV.	FECHA	DESCRIPCIÓN

ELABORADO POR: Carlos J. Pérez Aguilera	REVISADO Y APROBADO POR: DIRECCIÓN
FECHA: 08-05-2018	

POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES DE LOS EMPLEADOS	PRO-01
	Revisión 00

ÍNDICE

POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES DE LOS EMPLEADOS	PRO-01
	Revisión 00

1.-OBJETO

Esta política regula la gestión de datos personales relacionados con los empleados de la empresa y proporciona reglas y procedimientos que son aplicables a todos los departamentos y personas físicas dentro de la Empresa, con el objetivo de garantizar que los datos personales de los empleados sean tratados y protegidos adecuadamente en todos los países y regiones.

Esta política se aplica al tratamiento de los datos personales de los empleados de todos los departamentos y personas físicas dentro de la Empresas, en todos los países y regiones.

Los usuarios de este documento son todos los empleados de la Empresa

2.-ALCANCE

Este procedimiento es aplicable a todo el personal de la empresa.

3.-DEFINICIONES

Las siguientes definiciones de términos utilizados en este documento provienen del Artículo 4 del

Reglamento General de Protección de Datos de la Unión Europea:

3.1. Datos personales

Toda información sobre una persona física identificada o identificable, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de una persona física. Datos personales incluye la dirección de correo electrónico de una persona física, número de teléfono, información biométrica (como huella dactilar), datos de ubicación, dirección IP, información de atención médica, creencias religiosas, número de seguro social, estado civil, etcétera.

3.2. Datos personales sensibles

Datos personales que son particularmente sensibles en relación con los derechos y las libertades fundamentales, ya que la divulgación de dichos datos podría ocasionar daños físicos, pérdidas financieras, daños a la reputación, robo de identidad o fraude o discriminación, etc.

Los datos personales sensibles normalmente incluyen, pero no se limitan a la revelación de los datos personales de origen racial o étnico, opiniones políticas, convicciones religiosas o filosóficas, afiliaciones sindicales, datos genéticos, datos biométricos (huella dactilar), dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientaciones sexuales de una persona física.

3.3. Tratamiento

Una operación o conjunto de operaciones realizadas sobre datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión, limitación, borrado o destrucción de los datos.

3.4. Responsable de los datos

La persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento.

4.- PRINCIPIOS GENERALES PARA EL TRATAMIENTO DE DATOS PERSONALES DE LOS EMPLEADOS

4.1. Legalidad, imparcialidad y transparencia

Los datos personales deben ser tratados de forma legal, imparcial y transparente en relación a los empleados.

4.2. Limitación de la finalidad

Los datos personales de los empleados deben ser recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines.

4.3. Minimización de datos

Los datos personales de los empleados deben de ser adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. El Responsable de Seguridad debe aplicar anonimización o seudonimización a los datos personales si es posible para reducir el riesgo concerniente a los empleados.

4.4. Exactitud

Los datos personales de los empleados deben ser exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan.

4.5. Limitación del plazo de conservación

Los datos personados no deben ser conservados más de lo necesario para los fines para los cuales los datos personales son tratados, de acuerdo con la política de retención de datos.

4.6. Integridad y confidencialidad

Teniendo en cuenta el estado de la tecnología y otras medidas de seguridad disponibles, el coste de implementación y la probabilidad y gravedad de los riesgos, se deben aplicar medidas técnicas u organizativas apropiadas para tratar los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental.

4.7. Responsabilidad proactiva

Los responsables del tratamiento serán responsables del cumplimiento de los principios descritos anteriormente y serán capaces de demostrarlo.

5. Fines legítimos para el tratamiento de datos personales de los empleados

Los departamentos o personas de la Empresa pueden tratar los datos personales de los empleados para fines legítimos, que incluyen, entre otros:

Gestión de recursos humanos. Este objetivo incluye actividades de gestión de recursos humanos llevadas a cabo durante la contratación o el cumplimiento de un contrato laboral, como entrevistas, incorporaciones, cese de empleo, asistencia, gestión del desempeño, compensación y beneficios, formación, servicios a los empleados, salud y seguridad ocupacional, y otras actividades que tengan como finalidad la gestión de recursos humanos o la protección de los intereses vitales de los empleados.

Otras operaciones empresariales. Esta finalidad incluye actividades empresariales tales como la administrar viajes y gastos, administrar activos de la compañía, proporcionar servicios informáticos, seguridad de la información, realizar auditorías e investigaciones internas, cumplir con las obligaciones de contratos comerciales, asesoría legal o comercial y prepararse para litigios legales, etc.

Cumplimiento con la legislación. El tratamiento de los datos personales de los empleados para cumplir con las obligaciones legales, por ejemplo: la divulgación de los datos personales de los empleados a una autoridad fiscal con el fin de cumplir con las leyes fiscales aplicables.

6. Requisitos para el tratamiento de datos personales de los empleados

Cualquier tratamiento de los datos personales de los empleados por parte de los departamentos y personas físicas de la Empresa debe tener un fin legítimo y debe cumplir con los siguientes requisitos:

6.1. Aviso a los empleados

A los efectos de la transparencia del tratamiento de datos personales del empleado, cuando un departamento de la empresa o una persona física recogen los datos personales de un empleado, el empleado debe ser notificado de los tipos de datos que se recopilan, la finalidad y los tipos de tratamiento, los derechos del empleado y las medidas de seguridad tomadas para proteger los datos personales. La notificación puede tomar la forma de una publicación o actualización de declaraciones sobre la protección de los datos personales de los empleados, por ejemplo: la inclusión de términos en la protección de datos personales de los empleados en los contratos de empleo por el departamento de relaciones con los empleados/RRHH; la inclusión de una declaración de datos personales en los sistemas informáticos relevantes por parte del departamento de gestión de calidad, de procesos de negocio y de TI.

6.2. Elección y consentimiento del empleado

En principio, la Empresa puede tratar datos personales de los empleados para un fin legítimo como empleador y generalmente puede hacerlo sin obtener el consentimiento del empleado, para mejorar la eficiencia de la operación interna.

Las actividades de gestión de recursos humanos tales como entrevistas, incorporaciones, cese empleo, asistencia, compensación y beneficios, servicios al empleado, salud y seguridad ocupacional pueden involucrar el tratamiento de datos personales confidenciales. Si las leyes o reglamentos específicos del país rigen estos asuntos (por ejemplo, la obtención del consentimiento del empleado), la Empresa deberá tomar en cuenta estas leyes o reglamentos. El departamento de asuntos legales de cada país es el responsable de identificar los requisitos de cumplimiento específicos; los departamentos de recursos humanos locales son los responsables de garantizar el cumplimiento.

6.3. Recogida

POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES DE LOS EMPLEADOS	PRO-01
	Revisión 00

Los departamentos de la empresa y las personas físicas deben recopilar datos personales de los empleados para fines legítimos y deben cumplir con el principio de minimización de datos. Si los datos personales de un candidato a un trabajo o empleado se recogen de un tercero (por ejemplo, agencias de contratación o de comprobación de antecedentes), la Empresa debe hacer todo lo posible para garantizar que el tercero obtenga los datos personales por medios legítimos.

Ningún departamento o persona de la Empresa puede recoger datos personales de los candidatos a un trabajo o empleados de una manera que sea incompatible con la ley o la ética empresarial.

6.4. Uso, retención y eliminación

Los departamentos y personas físicas de la Empresa deben usar, retener y eliminar los datos personales de los empleados de manera que sea coherente con el aviso al empleado. También debe garantizar su precisión, integridad y pertinencia. Deben tomar las medidas de seguridad apropiadas para proteger los datos personales del empleado contra la destrucción, pérdida, alteración, acceso no autorizado o divulgación accidental o ilegal según la política de seguridad de la información y otros documentos que describen la seguridad de los datos.

Los departamentos de la Empresa y las personas no deben destruir o alterar ilegalmente los datos personales de los empleados. No deben acceder, vender ni proporcionar datos personales del empleado a ningún tercero de forma ilegal o sin autorización.

En el curso de las operaciones empresariales, el delegado de protección de datos decidirá si los datos personales de los empleados se tratarán de las siguientes maneras para minimizar el riesgo de protección de datos: los datos personales de los empleados se pueden anonimizar con la finalidad de la eliminar de forma irreversible su identificación; o los datos pueden agregarse para resultados estadísticos o de encuestas (Los principios de tratamiento de datos personales no se aplican a los datos anónimos ni a los datos agregados, ya que no son datos personales).

6.5. Comunicación a terceros

Cuando los departamentos y las personas de la Empresa necesiten comunicar datos personales de los empleados a un proveedor, socio empresarial u otro tercero, deberán asegurarse de que el proveedor, socio comercial u otro tercero proporcionan medidas de seguridad para salvaguardar los Datos Personales de los empleados que sean apropiadas con respecto a los riesgos asociados. También deben exigir que el tercero proporcione el mismo nivel de protección de datos que la Empresas por contrato u otro acuerdo.

Además, cuando los departamentos de la Empresa y las personas físicas comuniquen los datos personales de los empleados en respuesta a una solicitud de una agencia de cumplimiento de la ley o autoridad judicial, primero deben informar al departamento de asuntos legales que esté autorizado por la Empresa para realizar un esfuerzo coordinado para gestionar la solicitud.

6.6. Transferencia transfronteriza de datos personales de empleados

Como empresa que opera en todo el mundo, la empresa transfiere y trata datos personales de los empleados en todo el mundo. Los diferentes países imponen diferentes requisitos para la transferencia transfronteriza de datos personales (como, por ejemplo, la no limitación, la limitación condicional o la prohibición de transferencias de determinados tipos de datos personales fueran del país). Antes de transferir datos personales desde un país, los departamentos de la Empresa y las personas físicas deben consultar al delegado de protección de datos correspondiente (DPD) o al departamento de asuntos legales para determinar si la transferencia transfronteriza es necesaria y legal

Al transferir datos personales de los empleados fuera del Área Económica Europea, el transmisor y el beneficiario deben haber firmado un acuerdo de transferencia de datos de conformidad con las regulaciones de la UE y la política de transferencia de datos transfronterizos. El receptor debe proporcionar una protección adecuada para los datos transferidos de acuerdo con el acuerdo de transferencia de datos.

6.7. Acceso de los empleados

Los departamentos de la Empresa deben proporcionar medios razonables para que los empleados accedan a los datos personales que tienen sobre ellos y permitir que los empleados actualicen, corrijan, borren o transmitan sus datos personales, si fuera apropiado o lo exige la ley. Al responder a una solicitud de acceso de un empleado, los departamentos de la Empresa pueden no proporcionar ningún dato personal hasta que hayan verificado la identidad del empleado. La compañía necesita asegurarse de que conocen la identidad de la persona que realiza la solicitud antes de que puedan enviar los datos personales a la persona.

7. Responsabilidades

El responsable de recursos humanos es responsable de la gestión de la protección de datos personales de los empleados.

POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES DE LOS EMPLEADOS	PRO-01
	Revisión 00

8. Respuesta en caso de incumplimiento

Cualquier persona que tenga conocimiento de una violación de seguridad de datos que involucre datos personales de un empleado debe informarlo a las personas pertinentes dentro de la Empresa. Cuando sea necesario informar de la violación de datos fuera de la Empresa, siga la política de incumplimiento de datos personales.

Sin embargo, si así lo exige la legislación local del país donde se produjo la violación de seguridad de datos, la persona designada en el procedimiento de violación de seguridad de datos debe informar del incidente al legislador y/o partes interesadas dentro del período de comunicación especificado por la ley.

9. Responsabilidad proactiva

Cualquier persona física que viole esta política estará sujeto a medidas disciplinarias (hasta e incluyendo el cese de su empleo); y también puede estar sujeto a responsabilidades civiles o penales si su conducta viola leyes o reglamentos.

10. Excepciones y variaciones

Los departamentos de la Empresa y las personas también deben consultar esta política al tratar los datos personales de otro personal. "Otro personal" incluye: (1) personas que buscan empleo en la Empresa; (2) personas físicas que han sido contratados anteriormente por la Empresa; (3) otro que no es empleado de la Compañía pero que trabaja en las instalaciones de la Compañía (como empleado de socios colaboradores, consultores, becarios).

11. Propietario y contactos

El departamento de recursos humanos es el propietario de esta política, y debe interpretar y gestionarla.

POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES DE LOS EMPLEADOS	PRO-01
	Revisión 00

5.-ARCHIVO Y CODIFICACIÓN DE REGISTROS

Nombre del registro	Ubicación	Persona responsable de su almacenamiento	Controles para la protección de registros	Tiempo de retención
Contratos de empleados	Servidor de archivos seguro	el Responsable de Seguridad	Sólo personal autorizado puede acceder a estos contratos.	Consulte la política de retención de datos