POLITICA DE PROTECCIÓN DE DATOS PERSONALES

Adium S.A.S.

INDICE

1. OBJETO

El presente manual tiene el propósito de definir los lineamientos para la implementación, monitoreo, sostenimiento y mejora continua de la Protección de Datos Personales de la Compañía.

2. ALCANCE

Adium S.A.S., en adelante la "Compañía", está comprometida con el adecuado tratamiento de los datos de sus empleados, los clientes, los proveedores y los terceros. Por lo tanto, en el presente documento se articulan los procedimientos y actividades que involucran el tratamiento de los datos personales, los cuales están alineados con las normas y directrices que lo regulan.

Los terceros con quienes contrate la Compañía deberán proceder bajo las pautes de la presente Política.

3. MARCO NORMATIVO

Con el propósito de dar un adecuado tratamiento a los datos personales, la Compañía estará al cumplimiento del Régimen General de Protección de Datos Personales: Ley 1581 de 2012, el Decreto Reglamentario 1074 de 2015 y la Guía de implementación del Principio de Responsabilidad Demostrada de la Superintendencia de industria y comercio (en adelante, la "Normativa de Protección de Datos Personales"). También serán de aplicación:

- La Política de Seguridad de la Información, de la Compañía, a la cual se puede acceder a través del siguiente link: https://www.Adium.com.co/politica-de-privacidad/

- El Código de Ética de la Compañía, al cual se puede acceder a través del siguiente link: https://www.Adium.com.co/sobre-nosotros/

En general, para la aplicación e interpretación del presente manual, cuando fuere procedente, se aplicarán las demás normas que regulen o complementen lo concerniente a la protección de datos personales.

4. PRINCIPIOS APLICABLES AL TRATAMIENTO DE DATOS

La Compañía está comprometida con el adecuado tratamiento de los datos personales, por lo cual, en todas las actividades que impliquen manejo de datos personales, se garantizará la aplicación de los siguientes principios, los cuales se encuentran alineados con los establecidos en Normativa de Protección de Datos Personales:

- Legalidad: la formación de bases de datos será lícita cuando se encuentren debidamente inscriptas (de corresponder), observando en su operación los principios que establece la Normativa de Protección de Datos Personales y demás normas concordantes y complementarias. Las bases de datos no tendrán finalidades violatorias de derechos humanos o contrarias a las leyes o a la moral pública.

Veracidad: los datos personales que se recogieren a los efectos de su tratamiento deberán ser veraces, adecuados, ecuánimes y no excesivos en relación con la finalidad para la cual se hubieren obtenido. La recolección de datos no podrá hacerse por medios desleales, fraudulentos, abusivos, extorsivos o en forma contraria a la Normativa de Protección de Datos Personales. Los datos deberán ser exactos y actualizarse en el caso en que ello fuere necesario.

Cuando se constate la inexactitud o falsedad de los datos, La Compañía, en cuanto tenga conocimiento de dichas circunstancias, deberá

- suprimirlos, sustituirlos o completarlos por datos exactos, veraces y actualizados. Asimismo, deberán ser eliminados aquellos datos que hayan caducado.

- Finalidad: Los datos objeto de tratamiento no podrán ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención. Los datos deberán ser eliminados cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubieren sido recolectados. Tampoco podrán comunicarse datos entre bases de datos, sin previo consentimiento informado del titular.

- Previo consentimiento informado: El tratamiento de datos personales es lícito cuando el titular hubiere prestado su consentimiento libre, previo, expreso e informado, el que deberá documentarse, salvo que la Normativa de Datos Personales exceptúe la exigencia del previo consentimiento.

- Seguridad de los datos: la Compañía adoptará las medidas que resultaren necesarias para garantizar la seguridad y confidencialidad de los datos personales. Dichas medidas tendrán por objeto evitar su adulteración, pérdida, consulta o tratamiento no autorizado, así como detectar desviaciones de información, intencionales o no, ya sea que los riesgos provengan de la acción humana del medio técnico utilizado. Los datos serán almacenados de modo que permitan el ejercicio del derecho de acceso de su titular. La Compañía no registrará datos personales en sus bases de datos que no reúnan condiciones técnicas de integridad y seguridad.

- Reserva: la Compañía se obliga a utilizar los datos personales proporcionados en forma reservada y exclusivamente para las operaciones habituales de su giro o actividad, estando prohibida toda difusión a terceros. Las personas que, por su situación laboral u otra forma de relación con la Compañía, tuvieren acceso o intervengan en cualquier fase del tratamiento de datos personales, están obligadas a guardar estricto secreto sobre los mismos, cuando hayan sido recogidos de fuentes no accesibles al público. Lo previsto no se aplicará en los casos de orden de la Justicia competente, de acuerdo con las normas vigentes en esta materia o si mediare consentimiento del titular. Esta obligación subsistirá aún después de finalizada la relación con el responsable de la base de datos.

- Responsabilidad: Toda violación a la Normativa de Datos Personales podrá tener consecuencias para la Compañía, por lo que en ejercicio de una responsabilidad proactiva, la Compañía la adoptará las medidas técnicas y organizativas apropiadas, que podrán incluir: privacidad desde el diseño, privacidad por defecto, evaluación de impacto a la protección de datos, entre otras, a fin de garantizar un tratamiento adecuado de los datos personales y demostrar su efectiva implementación.

- Transparencia: cualquier titular de información podrá tener acceso, en cualquier momento, a la información sobre sus datos personales tratados por la Compañía.

- Confidencialidad: la Compañía garantizará la reserva de la información y datos personales que no estén bajo la categoría de datos públicos, por lo cual, todo el personal de la Compañía que tengan acceso al tratamiento de los datos personales deberá en su manejo de datos evitar la exposición o suministro de datos personales a terceros no autorizados.

5. DERECHOS DE LOS TITULARES DE LOS DATOS PERSONALES:

Todas las personas físicas o jurídicas que brinden datos personales a la Compañía (los “titulares

de los datos personales") gozarán de los siguientes derechos:

5.1 Derecho de acceso. Todo titular de datos personales que previamente acredite su identificación con el documento de identidad o poder respectivo, tendrá derecho a obtener toda la información que sobre sí mismo se halle en las bases de datos de la Compañía.

Este derecho de acceso sólo podrá ser ejercido en forma gratuita a intervalos de seis meses, salvo que se hubiere suscitado nuevamente un interés legítimo de acuerdo con el ordenamiento jurídico o la legislación local establezca un plazo menor.

Cuando se trate de datos de personas fallecidas, el ejercicio del derecho al cual refiere este artículo corresponderá a cualesquiera de sus sucesores universales, cuyo carácter se acreditará debidamente.

La información debe será proporcionada dentro del plazo establecido por la Normativa de Protección de Datos Personales.

La información debe será suministrada en forma clara, exenta de codificaciones y en su caso acompañada de una explicación y en lenguaje accesible.

La información versará sobre la totalidad del registro perteneciente al titular, aun cuando el requerimiento sólo comprenda un aspecto de los datos personales. En ningún caso el informe podrá revelar datos pertenecientes a terceros, aun cuando se vinculen con el interesado.

La información a ser suministrada por la Compañía, a opción del titular, podrá suministrarse por escrito, por medios electrónicos, telefónicos, de imagen, u otro idóneo a tal fin.

5.2 Derecho de rectificación, actualización, inclusión o supresión. Toda persona física o jurídica tendrá derecho a solicitar la rectificación, actualización, inclusión o supresión de los datos personales que le corresponda incluidos en cualquier base de datos de la Compañía, al constatarse error o falsedad o exclusión en la información de la que es titular.

El responsable de la base de datos de la Compañía o del tratamiento deberá realizar la rectificación, actualización, inclusión o supresión, mediante las operaciones necesarias a tal fin dentro del plazo establecido por la Normativa de Protección de Datos Personales o, en su caso, informar de las razones por las que estime no corresponde.

Procede la eliminación o supresión de datos personales en los siguientes casos:

- Perjuicios a los derechos e intereses legítimos de terceros.
- Notorio error.
- Contravención a lo establecido por una obligación legal.

Durante el proceso de verificación, rectificación o inclusión de datos personales, el responsable de la base de datos de la Compañía o tratamiento, ante el requerimiento de terceros por acceder a informes sobre los mismos, dejará constancia que dicha información se encuentra

sometida a revisión.

En el supuesto de comunicación o transferencia de datos, el responsable de la base de datos de la Compañía o del tratamiento notificará la rectificación, inclusión o supresión al destinatario dentro del plazo establecido por la Normativa de Protección de Datos Personales.

La rectificación, actualización, inclusión, eliminación o supresión de datos personales cuando corresponda, se efectuará sin cargo alguno para el titular.

5.3 Derechos referentes a la comunicación de datos a terceros. Los datos personales objeto de tratamiento sólo podrán ser comunicados a terceros para el cumplimiento de los fines directamente relacionados con el interés legítimo informado por la Compañía y del destinatario y con el previo consentimiento del titular de los datos, al que se le debe informar sobre la finalidad de la comunicación e identificar al destinatario o los elementos que permitan hacerlo.

El previo consentimiento para la comunicación es revocable y no será necesario cuando:

- así lo disponga la Normativa de Datos Personales u otra legislación aplicable.
- se trate de datos personales relativos a la salud y sea necesaria su comunicación por razones sanitarias, de emergencia o para la realización de estudios epidemiológicos, preservando la identidad de los titulares de los datos mediante mecanismos de disociación adecuados cuando ello sea pertinente.
- se hubiera aplicado un procedimiento de disociación de la información, de modo que los titulares de los datos no sean identificables.

El destinatario quedará sujeto a las mismas obligaciones legales y reglamentarias de la Compañía.

6. TRATAMIENTO GENERAL DE DATOS PERSONALES

la Compañía tratará todo dato personal de sus clientes, empleados, proveedores y terceros en general, con una adecuada confidencialidad y protección y en total cumplimiento a la Normativa de Datos Personales.

Para la obtención y procesamiento de datos personales, la Compañía actuará conforme se detalla a continuación:

- Todo dato personal será procesado siempre que se obtenga previo consentimiento expreso de su titular, salvo que tal consentimiento pueda exceptuarse conforme a la Normativa de Datos Personales.

- La Compañía informará a los titulares de los datos personales, la finalidad que motiva la obtención de sus datos personales y el plazo por el cual dichos datos serán mantenidos en sus bases de datos.

- Ningún dato personal será procesado o mantenido en las bases de datos de la Compañía para un fin diferente a aquel que motivó su obtención inicial y que fuere expresamente consentido por su titular.

- Toda modificación de la finalidad inicial por la cual un dato personal fuere obtenido para su procesamiento, será informada a su titular quien deberá previamente consentirla antes de que la Compañía proceda a su procesamiento.

- Una vez que se haya cumplido con la finalidad para la cual se obtuvo el dato personal, la Compañía procederá a la eliminación de dicha información, no pudiendo mantener en sus bases de datos, datos personales sin un fin especifico o con un fin que ya se cumplió.

- Todos los datos personales que la Compañía obtenga y procese serán alocado en bases de datos, debidamente inscriptas conforme a la Normativa de Datos Personales, y gozarán de adecuados niveles de protección.

- La Compañía procurará que el número de personas que tienen acceso a las bases de datos sea reducido y limitado a aquellas áreas y personal vínculos con la finalidad para el procesamiento de la información.

- La Compañía informará a cada titular de los datos personales como ejercer sus derechos de acceso, modificación, rectificación, actualización, inclusión y/o supresión.

7. CONSENTIMIENTO PREVIO

7.1 General. Toda obtención, recolección, uso, procesamiento y almacenamiento de datos personales que realice la Compañía en el desarrollo de sus actividades ordinarias, y extraordinarias, requieren de los titulares un consentimiento libre, previo, expreso, inequívoco e informado.

A estos efectos, la Compañía pone a disposición de los titulares, la autorización para el tratamiento de sus datos personales en los diversos escenarios en los cuales realiza la recolección del dato, tanto de manera física como digital, el tratamiento al cual serán sometidos incluyendo las finalidades, sus derechos, los canales de ejercicio de sus derechos y la información relacionada sobre la Política de Protección de Datos Personales.

En todos los casos la obtención del consentimiento se realizará bajo las diferentes modalidades que establece la Normativa de Datos Personales, teniendo en cuenta la naturaleza de cada uno de los canales de captura de la información, y el modo en que la misma es obtenida, es decir, si es a través de un canal escrito, o virtual.

Es importante tener en consideración que en todos los casos la Compañía custodiará las autorizaciones obtenidas para el tratamiento de los datos personales, dado que ésta hace parte de las pruebas exigidas por la Normativa de Datos Personales. En consecuencia, se deberán guardar los formatos físicos en donde existan autorizaciones, el registro de llamadas o de los formularios web en los cuales se da trazabilidad sobre la aceptación del tratamiento.

7.2 Aviso de privacidad. De acuerdo con la Normativa de Datos Personales, los avisos de privacidad mediante los cuales se obtiene la autorización de los titulares deben tener incluir un consentimiento libre, previo, expreso, informado y documentado.

El referido consentimiento prestado con otras declaraciones deberá figurar en forma expresa y destacada. No será necesario el previo consentimiento cuando:

a. Los datos provengan de fuentes públicas de información, tales como registros o publicaciones en medios de comunicación masiva.
b. Se recaben en virtud de una obligación legal.

c. Se trate de listados de acceso público cuyos datos se limiten en el caso de personas físicas a nombres y apellidos, documento de identidad, nacionalidad, domicilio y fecha de nacimiento. En el caso de personas jurídicas, razón social, nombre de fantasía, registro único de contribuyentes, domicilio, teléfono e identidad de las personas a cargo de esta.
d. Deriven de una relación contractual, científica o profesional del titular de los datos, y sean necesarios para su desarrollo o cumplimiento.

7.2.1 Contenido mínimo del aviso de privacidad. Derecho de información frente a la recolección de datos.

Cuando se recaben datos personales se deberá informar previamente a sus titulares en forma expresa, precisa e inequívoca:

a. La finalidad para la que serán tratados y quiénes pueden ser sus destinatarios o clase de destinatarios.
b. La existencia de la base de datos, electrónico o de cualquier otro tipo, de que se trate y la identidad y domicilio de su responsable.
c. El carácter obligatorio o facultativo de las respuestas al cuestionario que se le proponga, en especial en cuanto a los datos sensibles.
d. Las consecuencias de proporcionar los datos y de la negativa a hacerlo o su inexactitud.
e. La posibilidad del titular de ejercer los derechos de acceso, rectificación y supresión de los datos.

7.3 Modelos de Consentimiento Informado. Requisitos mínimos. Los modelos de consentimiento informado pueden ser físicos o digitales (incluyendo grabaciones de voz), debiendo cumplir con los siguientes mínimos requisitos:

a. Solicitar sólo aquellos datos personales necesarios conforme con la finalidad del tratamiento.
b. Incluir la autorización del tratamiento de los datos por parte del titular.
c. Validar que en el aviso de privacidad se encuentren todas las finalidades de tratamiento asociadas a la captura de los datos personales.

7.3.1 Formularios digitales. Adicionalmente, los consentimientos recabados digitalmente también deberán cumplir con los siguientes requisitos:

d. El envío de la información a través del formulario, deberá estar condicionado a la previa aceptación de la autorización de tratamiento del dato.

e. Para formularios web, se deberá validar que la plataforma que soporta el formulario tenga la capacidad técnica, operativa y de seguridad para almacenar las autorizaciones, y poder tener la trazabilidad en ellas. Preferiblemente se deberá incluir fecha en la que se obtuvo la autorización.

7.4 Custodia de la autorización. Cada área de la Compañía que realice un tratamiento de datos personales debe garantizar la custodia y almacenamiento de la autorización para el tratamiento de los datos.

8. BASES DE DATOS

Los clientes, empleados, proveedores y terceros son los que permiten desarrollar el objeto social de la Compañía, por ello es indispensable recolectar, almacenar y utilizar los datos personales de ellos, para en esencia conocer la naturaleza del servicio que se les prestará.

Todos los datos personales que los clientes, empleados, proveedores y terceros brindan en forma libre y voluntaria, son incluidos en una Base de Datos a la cual tienen acceso el personal de la Compañía en ejercicio de sus funciones, que en ningún caso está autorizado para el Tratamiento de la información para fines diferente a aquellos a los que motivaron su recolección y que fueren debidamente consentidos por sus titulares.

Todas las bases de datos propiedad de la Compañía deberán registrase conforme la Normativa de Datos Personales. Tal registro deberá mantenerse actualizado.

9. TRATAMIENTO DE DATOS SENSIBLES

La Compañía solo tratará datos personales sensibles para el cumplimiento de fines estrictamente necesarios, solicitando consentimiento previo y expreso a sus titulares (representantes legales, apoderados, causahabientes) e informándoles sobre la finalidad exclusiva de su tratamiento.

Son datos sensibles, aquellos que afectan la intimidad del titular o que revelen origen racial y étnico, preferencias políticas, convicciones religiosas o morales, afiliación sindical e informaciones referentes a la salud o a la vida sexual y los datos biométricos.

La Compañía utilizará y tratará datos catalogados como sensibles, únicamente cuando:

- El tratamiento haya sido autorizado expresamente por el titular de los datos sensibles, salvo en los casos que la Normativa de Datos Personales no requiera el otorgamiento de dicha autorización.

- El tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

- El tratamiento tenga una finalidad estadística o científica o, dentro del marco de procesos de mejoramiento; este último, siempre y cuando se adopten las medidas conducentes a la supresión de identidad de los titulares o el dato esté disociado, es decir, el dato sensible sea separado de la identidad del titular y no sea identificable o no se logre identificar a la persona titular del dato o datos sensibles.

En adición a lo anterior, la Compañía cumple con las siguientes obligaciones:

- Informar al titular que, por tratarse de datos sensibles, no está obligado a autorizar su tratamiento.

- Informar al titular de forma explícita y previa, además de los requisitos generales de la autorización para la recolección de cualquier tipo de dato personal, cuáles datos objeto de tratamiento son de carácter sensible y cuál será la finalidad que se les dará a estos tras obtener del él (el titular) un consentimiento expreso para ello.

- No condicionar ninguna actividad a que el titular suministre datos personales sensibles (salvo que exista una causa legal, material o contractual para hacerlo).

Las bases de datos que contengan datos sensibles contarán con las siguientes medidas de seguridad:

- El acceso a la base de datos se encontrará limitado la menor cantidad posible de personas.
- Las bases de datos contarán con claves de alta complejidad.
- El respaldo de las bases de datos se realizará en forma diaria.

Adicionalmente, la Compañía se compromete a guardar la confidencialidad que corresponda a cualquier otro dato personal que almacene o procese, aunque el dato no sea catalogado como “sensible” por la Normativa de Datos Personales (ej.: salarios y remuneraciones).

10. VULNERACIONES DE SEGURIDAD

10.1 General. la Compañía ha asumido el compromiso de dar una adecuada protección a los datos personales que procesa, implementando para ello mecanismos de seguridad adecuados.

Sin embargo, no existen mecanismos perfectos por lo que a continuación se detalla el procedimiento que la empresa realizará ante una eventual vulneración de sus bases de datos.

10.2 Definiciones

- Incidente de seguridad: acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a la política de seguridad de la información del organismo

- Medidas de seguridad: medidas técnicas y organizativas necesarias para conservar la integridad, confidencialidad y disponibilidad de la información, de forma de garantizar la seguridad de los datos personales.

- Vulnerabilidad de seguridad: debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información, pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma, por lo que es necesario encontrarlas y eliminarlas lo antes posible.

- Vulneración de seguridad: incidente de seguridad que ocasione, entre otras, la divulgación, destrucción, pérdida o alteración accidental o ilícita de datos personales, o la comunicación o acceso no autorizados a dichos datos.

10.3 Gestión y comunicación de una vulneración de seguridad de datos personales. La vulneración de seguridad sobre datos personales puede referir a datos que son identificatorios directamente de quien es su titular, pero también a otros datos que, sin que se le identifique directamente, vuelven al titular identificable.

En consecuencia, la gestión y comunicación de las vulneraciones deben contener las mayores garantías para quien es titular de los datos vulnerados, así como una buena integralidad, lo que se acentúa si esos datos personales son sensibles o especialmente protegidos según lo establecido en la Normativa de Datos Personales.

10.3.1 Notificación de vulneraciones. Procedimiento. Plazos. Ante la constatación de una vulneración de seguridad, tanto el responsable como el encargado de la base de datos iniciarán los procedimientos necesarios para minimizar el impacto de los incidentes dentro de las primeras 24 horas.

Los responsables de la base de datos, al conocer la ocurrencia de una vulneración de seguridad deberán informarla a la autoridad de contralor que indique la Normativa de Datos Personales (la “Autoridad de Protección de Datos”) dentro del plazo de 72 horas, dando los mayores detalles posibles del hecho y de las medidas que adoptó hasta el momento de la comunicación. Los mínimos datos a informar son:

- fecha cierta o estimada de la ocurrencia de la vulneración,
- naturaleza,
- datos personales afectados,
- posibles impactos generados.

El responsable o encargado valorará la afectación que la vulneración pueda haber producido en los titulares de los datos. Si la vulneración ocasionó una afectación significativa de los derechos de los titulares de los datos, éstos deberán ser notificados.

En el caso de los encargados de tratamiento, deben hacer la comunicación directamente a los responsables, quienes deberán proceder en la forma indicada anteriormente.

Corresponde señalar que, una vez solucionada la vulneración, la persona responsable del tratamiento deberá elaborar un informe pormenorizado de la vulneración de seguridad y las medidas adoptadas y comunicarlo a la Autoridad de Protección de Datos, dentro del plazo que pueda establecer la legislación local como así también a otras compañías con las que se tenga obligación contractual de informar.

10.3.2 Comunicaciones a titulares. Las comunicaciones a los titulares se realizarán en un lenguaje claro y sencillo, para que éstos comprendan lo sucedido. La información debe ser lo suficientemente completa para que los titulares de los datos tengan conocimiento de las causas y consecuencias de la vulneración, y de las medidas adoptadas para su subsanación.

10.3.3 Gestiones posteriores a la comunicación de la vulneración de seguridad. La comunicación de las vulneraciones de seguridad no agota las tareas que deben realizar responsables y encargados de la Compañía, quienes realizarán todos los procedimientos necesarios para subsanar sus efectos, y adoptar las medidas para evitar futuras vulneraciones.

11. TRANSFERENCIA INTERNACIONAL DE DATOS

La Compañía se compromete a no realizar trasferencias de datos personales a países o entidades internacionales que no brinden niveles adecuados de protección. Sin embargo, en caso de que dichas transferencias internacionales a países o entidades calificadas como “inseguras” por la Autoridad de Protección de Datos sean necesarias, la Compañía seguirá el proceso que se detalla a continuación:

- El titular de los datos deberá consentir en forma previa y expresa la transferencia internacional de sus datos.

- Deberá existir un acuerdo entre la entidad exportadora e importadora de datos cuyas clausulas brinden un nivel adecuado de protección de datos. El acuerdo de transferencia de datos debe proporcionar los mismos niveles de protección que exige la Normativa de Datos Personales.
- Finalmente, la transferencia debe ser autorizada por el regulador del país exportador, si fuera requerido por la normativa local.

Las transferencias internacionales dentro del grupo la Compañía estarán permitidas sin autorización alguna de la Autoridad de Protección de Datos en tanto la filial o tercera parte receptora, que se encuentre en una jurisdicción calificada como insegura, haya adoptado políticas de protección de datos personales debidamente registrado ante su Autoridad de Protección de Datos.

La transferencia internacional de datos personales entre el HQ y las filiales de la Compañía o terceros que esta contrate para tal fin, se realizará en tanto existan las respectivas políticas de protección de datos personales registradas ante la Autoridad de Protección de Datos y se cuente con la autorización expresa y previa del titular de los datos personales.

Para consultar los países y organizaciones internacionales considerados “seguros” bajo los criterios de la Normativa de Datos Personales (art. 45 del RGPD), se puede acceder al siguiente link:
https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/transferencias-internacionales

12. DELEGADO DE PROTECCIÓN DE DATOS (“DPO”)

Cuando así lo exija la Normativa de Datos Personales, cada filial del grupo la Compañía designará un Delegado de Protección de Datos (Data Protection Officer o la designación aplicable en cada país, "DPO"), quien será inscripto ante la Autoridad de Datos Personales.

El DPO deberá tener las condiciones necesarias para el correcto desempeño de cargo, las cuales se detallan a continuación:

- contar con conocimientos en Derecho, especializados en materia de protección de datos personales y derechos humanos.
- guardar absoluta confidencialidad de las informaciones a las que tenga acceso por su calidad.
- contar con conocimiento de la industria farmacéutica.

El delegado tendrá como funciones principales las siguientes:

- Asesorar en la formulación, diseño y aplicación de políticas de protección de datos personales.
- Supervisar el cumplimiento de la normativa sobre dicha protección en la Compañía.
- Proponer todas las medidas que entienda pertinentes para adecuarse a la normativa y a los estándares internacionales en materia de protección de datos personales.
- Actuar como nexo entre la filial y la Autoridad de Datos Personales.
- Participar de forma adecuada en todas las cuestiones relativas a la protección de datos personales.
- Toda otra actividad que le sea requerida por la Normativa de Protección de Datos.

Para desarrollar sus tareas en el desempeño de sus funciones, el DPO tendrá pleno acceso a las bases de datos personales y a las operaciones de tratamiento. Actuará con autonomía técnica y no recibirá instrucciones en el desempeño de sus funciones específicas como delegado de protección de datos.

Este delegado podrá desempeñar otras funciones en cuanto no generen conflicto de intereses.

13. VIDEOVIGILANCIA

13.1 General. La instalación y uso de cámaras de videovigilancia en los recintos laborales de la Compañía, así como el procesamiento de los datos obtenidos mediante dichas cámaras se regirá por el presente capítulo del Manual.

- Instalación. Como criterio general, las cámaras se pueden instalar en cualquier espacio, con las siguientes limitaciones: no se pueden utilizar en espacios públicos, locales sindicales, baños, vestuarios o similares, entre otros, ni enfocarse hacia predios linderos.

- Inscripción de la Base de Datos. Los datos recabados por medio de las cámaras de video vigilancia serán volcados en una Base de Datos inscripta ante la Autoridad de Datos Personales, de corresponder.

- Colocación y uso de señalética. Una vez que las cámaras estén instaladas, deberá colocarse la señalética de área videovigilada en lugares visibles. En ella se debe indicar el nombre del responsable y el lugar donde las personas pueden ejercer sus derechos. Conforme la legislación local, carteles con avisos de privacidad serán dispuestos en todos los lugares donde se hayan instalado cámaras de videovigilancia

- Derechos. Frente a una solicitud de acceso a las imágenes registradas por las cámaras, el responsable designado deberá proporcionar la información adoptando medidas que

garanticen la privacidad de otras personas involucradas. Para ello, podrá utilizar máscaras de privacidad o dar información por escrito. También deberá entregar la información cuando así lo requieran las fuerzas policiales conforme la legislación local o la Justicia.

- Acceso a imágenes y grabaciones. El acceso a las imágenes en vivo deberá restringirse al mínimo imprescindible para su control; a ellas solo podrán acceder las personas autorizadas por el responsable. Es importante que las imágenes se conserven por el mínimo tiempo imprescindible y que se adopten protocolos para el acceso y uso de la información ante posibles vulneraciones.

- Responsables. La Compañía designara a los representantes que realizarán el trámite de inscripción y determinaran quiénes son las personas autorizadas para acceder a las imágenes y grabaciones y quiénes deberán dar trámite a las solicitudes de ejercicio de derechos que se realicen.

- Información previa. La Compañía informará a sus empleados acerca de la instalación o existencia de las cámaras, los lugares donde estarán localizadas, si captan imagen y voz, el tiempo de conservación de las imágenes y cómo ejercer sus derechos de acceso a la información y material captado con las cámaras.

- Consentimiento expreso. No se requerirá el consentimiento expreso de las personas que son filmadas, siempre que se considere que la instalación de las cámaras es necesaria para el desarrollo de la relación laboral. Sin embargo, esto no exime a La Compañía de su deber de informar previamente acerca de dicha instalación y/o existencia de las cámaras.

13.2 Disposiciones Varias:

a) Las cámaras que se utilicen podrán instalarse dentro de los recintos de trabajo.

b) No se pueden instalar cámaras en baños, vestuarios, espacios de descanso, lugares destinados a la alimentación o con finalidades sindicales y cualquier otro sitio que pueda invadir la intimidad de los empleados.

c) No se registrarán conversaciones privadas.

d) No se pueden captar imágenes de la vía pública, a excepción de una franja mínima e imprescindible de acceso al lugar.

e) El sistema de grabación debe estar ubicado en un lugar de acceso restringido y solo accesible a personal autorizado.

f) Si se contrata un servicio de vigilancia que incluye videovigilancia, La Compañía suscribirá un contrato en el que se establezca quiénes son los encargados de acceder a la información y todas las condiciones de prestación del servicio

14. ÁREAS RESPONSABLES DE LA IMPLEMENTACIÓN Y OBSERVANCIA DE ESTE MANUAL

Las siguientes áreas tienen un rol fundamental en el cumplimiento de esta Política:

Legales

- Velar por la implementación de la Política.
- Asegurar que la Política se encuentre en línea con la Normativa de Protección de Datos Personales.

- Comunicar a las áreas involucradas los cambios en la Normativa de Protección de Datos Personales.

Compliance

- Verificar que la Política esté en alineada con el Código de Ética de la Compañía.
- Garantizar un entrenamiento mandatorio anual a todos los empleados de la compañía sobre esta Política.
- Notificar a la brevedad posible al DPO y/o Departamento de Legales, por cualquier denuncia recibida a través de la página de denuncias, con temáticas relacionados con el alcance de esta política.

Tecnología y Sistemas:

Se encarga de gestionar, con criterios de eficiencia y efectividad, los riesgos de seguridad de la de la información de la Compañía y, aquellos que puedan representar impactos de privacidad. Entre sus funciones destacan, las siguientes:

- Colaborar en la identificación y gestión de riesgos, amenazas y vulnerabilidades en los procesos de Tratamientos de los datos.
- Controlar la implementación de las medidas de seguridad de los Datos Personales.
- Analizar riesgos y evaluaciones de impacto en materia de seguridad.
- Asesorar en el marco de la aplicación de las directrices corporativas o globales sobre brechas de seguridad, y coordinar con los equipos correspondientes acciones ante dichas eventualidades.
- Implementar la Políticas de Seguridad de la Información de la Compañía en la organización, contribuyendo así a la protección de Datos Personales de los interesados.
- Supervisar el cumplimiento normativo sobre seguridad de la información.
- Supervisar la administración del control de acceso a la información y, en general, la arquitectura de seguridad de la información de la Compañía.

Empleados/ Colaboradores:

La responsabilidad de la protección de los Datos Personales es de todos los empleados / colaboradores de la Compañía. Cada empleado/colaborador que recolecta o usa información personal de clientes, proveedores o de otros individuos es responsable de la protección de los Datos Personales.

La presente Política se actualizará en forma periódica, reflejando las modificaciones normativas y las buenas prácticas que la Compañía y su DPO consideren necesarias y apropiadas.

Fecha de actualización: Diciembre 2023

Versión	Revisión	Fecha	Modificación
1	0	03-02-2023	