Política de Privacidad y Protección de Datos Personales

Versión	01
Día de aprobación	Febrero 2025
Dueño	Oficialía de Cumplimiento

Control de Cambios

Versión N°	Fecha	Observaciones
01	Febrero 2025	Generación del Política Privacidad y Datos Personales de Clinng

Tabla de Contenido

I. ASPECTOS GENERALES 6
I.1. Introducción 6
I.2. Objetivo 7
I.3. Alcance 7
I.4. Datos de identificación de Responsable del tratamiento 8
I.5. Finalidad 8
I.6. Legislación 8
I.7. Responsabilidades 9
I.7.1. Máximo Órgano de Administración 11
1.7.2. Gerente de Riesgos y Cumplimiento 11
1.7.3. Oficial de Protección de Datos Personales (OPD) 11
1.7.4. Responsable de Seguridad Lógica 12
1.7.5. Responsable de Seguridad Física 12
1.7.6. Responsable de la Base de Datos 12
1.7.7. Dueño de la Base de Datos 12
1.7.8. Custodio del Banco de Datos 13
I.8. Definiciones 13
I.9. Principios 16
I.9.1. Principio de Legalidad 16
I.9.2. Principio de Finalidad 16
I.9.3. Principio de Libertad 16
I.9.4. Principio de Veracidad o Calidad 16
I.9.5. Principio de Acceso y Circulación Restringida 16
I.9.6. Principio de Seguridad 16
I.9.7. Principio de Confidencialidad 16
II. DERECHOS DEL TITULAR 17
II.1. DERECHOS DEL TITULAR DE LOS DATOS PERSONALES 17
II.2. CAPACIDAD Y CONDICIONES PARA EL EJERCICIO DE LOS DERECHOS 18
III. PROCEDIMIENTO PARA LA ATENCION DE PQRS 19
III.1. LEGITIMACIÓN PARA PRESENTAR RECLAMOS Y SOLICITUDES 19
III.2. CANAL DE PRESENTACIÓN DE RECLAMOS Y SOLICITUDES 19
III.3. SOLICITUD DEL RECLAMO 19
III.4. SUBSANACIÓN Y DESESTIMIENTO DE RECLAMOS 19

III.5. COMPETENCIA PARA RESOLVER RECLAMOS 20
III.6. REGISTRO DEL RECLAMO 20
III.7. PLAZO DE ATENCIÓN A RECLAMOS 20
IV. PROCEDIMIENTO PARA EL EJERCICIO DEL DERECHO DE HABEAS DATA 20
IV.1. REQUISITOS 20
IV.2. RECEPCIÓN DE LA SOLICITUD 21
IV.3. PROCEDIMIENTO DE ATENCIÓN A LA SOLICITUD 21
IV.4. PLAZO DE RESPUESTA A SOLICITUDES 21
V. USO DE DATOS 21
V.1. TRATAMIENTO AUTORIZADO 22
V.1.1. Datos Públicos 22
V.1.2. Datos Privados 22
V.1.3. Datos Sensibles 22
V.2. TRATAMIENTO PROHIBIDO 22
V. 2.1. Datos Sensibles sin Consentimiento 22
V.2.2. Uso Contrario a la Finalidad Informada 23
V.2.3. Transferencia y Transmisión de Datos Personales 23
V.2.4. Confidencialidad y Seguridad de los Datos 23
V.5. EXCEPCIONES AL TRATAMIENTO DE DATOS 24
V.6. BASES DE DATOS DE CLINNG 24
V.6.1. Tipos de base de datos 24
V.6.2. Periodo de Vigencia de las Bases de Datos Personales 25
VI. MECANISMOS DE RECOLECCIÓN 26
VI.1.1. Formularios Electrónicos 26
VI.1.2. Registros y Contratos 27
VI.2.1. Registro de Consentimiento en Medios Verificables 27
VI.2.2. Recolección por Terceros Autorizados 27
VI.2.3. Uso de Bases de Datos Públicas 27
VI.2.4. Tratamiento de Datos Sensibles 28
VI.3. AUTORIZACIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES 28
VI.3.1. Autorizaciones y consentimientos del titular 28
VI.3.2. Prueba de la autorización 29
VI.3.3. Tipos de autorizaciones de tratamiento de datos personales 29
VI.3.4. Medios y manifestaciones para otorgar la autorización 29
VI.3.5. Revocatoria de la autorización 30

VII. MEDIDA DE SEGURIDAD APLICADO AL TRATAMIENTO DE DATOS PERSONALES 30
VIII. CAPACITACIONES..... 32
IX. VIGENCIA..... 32
XI. ADMINISTRACION DE LA POLITICA 33

I. ASPECTOS GENERALES

I.1. Introducción

En Monnet Pagos en Línea S.A.S (en adelante **"Clinng"**) valoramos la confianza que nuestros clientes depositan en nosotros. Reconocemos la importancia de proteger la privacidad y la confidencialidad de los datos personales que manejamos en el transcurso de nuestras operaciones.

La seguridad y el manejo responsable de la información personal son pilares fundamentales de nuestra filosofía empresarial y de nuestro compromiso con nuestros clientes, colaboradores y consultores.

Nuestro Política de Privacidad y Protección de Datos Personales (en adelante, **Política**) ha sido diseñada para garantizar que todos los datos recolectados, almacenados, procesados y compartidos por Clinng se manejen con el más alto nivel de seguridad y conformidad con las leyes y regulaciones vigentes en los países donde operamos.

Este Política establece los principios y las prácticas que seguimos para proteger la integridad, disponibilidad y confidencialidad de la información personal, asegurando que se utilice únicamente con los fines específicos y legítimos para los que fue recolectada.

En un entorno digital en constante evolución, donde las amenazas a la privacidad son cada vez más sofisticadas, en Clinng estamos comprometidos a implementar medidas técnicas y organizativas robustas para mitigar estos riesgos.

Nuestro Política no solo cumple con los estándares regulatorios más estrictos de Colombia donde operamos, sino que también refleja buenas prácticas en dicha

materia con la finalidad de mostrar nuestro compromiso continuo con la transparencia y la responsabilidad en el manejo de los datos personales.

A través de este Política, buscamos proporcionar claridad sobre cómo recopilamos, utilizamos, compartimos y protegemos los datos personales, al mismo tiempo que empoderamos a nuestros clientes con el control sobre su propia información.

Clinng se compromete a mantener altos estándares de privacidad y protección de datos como parte integral de nuestra misión de ofrecer soluciones Payins C Payouts seguras, eficientes y confiables en Colombia.

I.2. Objetivo

El objetivo de esta Política es establecer las directrices y prácticas para el tratamiento adecuado de los datos personales gestionados por Clinng, asegurando el cumplimiento de la legislación colombiana en materia de protección de datos personales. A través de esta política, Clinng busca garantizar la privacidad, seguridad y confidencialidad de los datos personales, protegiendo los derechos de los titulares y regulando el tratamiento de la información de acuerdo con los principios establecidos en la Ley 1581 de 2012 y demás normativas aplicables.

I.3. Alcance

Esta Política es de aplicación a todas las actividades de tratamiento de datos personales realizadas por Clinng en el marco de sus operaciones en Colombia, y abarca a todos los colaboradores, proveedores, clientes, usuarios y cualquier persona natural cuyos datos sean recolectados, almacenados, procesados o utilizados por la entidad. La Política se aplica a todas las bases de datos gestionadas por Clinng y se extiende a todas las actividades de recolección, uso, circulación, almacenamiento y supresión de los datos personales, asegurando que el

tratamiento se realice conforme a los principios y normas legales vigentes en Colombia.

I.4. Datos de identificación de Responsable del tratamiento

Clinng actuará como responsable del tratamiento de los datos personales de sus usuarios y hará uso de los mismo únicamente para las finalidades para las que se encuentra facultado. Son datos de identificación de Clinng son:

Nombre: MONNET PAGOS EN LINEA S.A.S - Clinng
Sede Central: Calle 70 4-36 - Bogotá DC, Colombia.
Teléfono: 3112448142
Correo electrónico: comercial@Clinngpayments.com
Sitio web: www.clinngpayments.com

I.5. Finalidad

La finalidad de esta política es establecer los lineamientos y principios para la protección de datos personales dentro del Grupo Monnet, específicamente en lo que respecta al tratamiento de bases de datos por parte de Clinng. Como responsable y/o encargado del tratamiento de datos personales, Clinng se compromete a cumplir con las normativas legales de protección de datos vigentes en Colombia. Esta política tiene como propósito garantizar la privacidad y seguridad de los datos personales, asegurar el respeto de los derechos de los titulares, y regular el tratamiento de la información de acuerdo con la Ley 1581 de 2012 y demás disposiciones aplicables.

I.6. Legislación

- Constitución Política de 1991 artículos 15, 20 y 74 sobre el Habeas Data y el acceso a la información.
- Ley Estatutaria 1266 de 2008 “Por la cual se dictan las disposiciones generales del Habeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones”.
- Ley Estatutaria 1581 de 2012 “Por la cual se dictan las disposiciones generales para la protección de datos personales”.
- Decreto Reglamentario 1377 de 2013 “Por la cual se reglamenta parcialmente la Ley 1581 de 2012”.
- Decreto Reglamentario 1074 de 2015 “Mediante el cual se reglamenta parcialmente la Ley 1581 de 2012”.
- Normas que las modifiquen, deroguen o sustituyan.

En caso de que se produzcan cambios legislativos o normativos en materia de Datos Personales, las referencias realizadas en este Política se entenderán modificadas por las nuevas disposiciones en los apartes pertinentes.

I.7. Responsabilidades

En líneas generales Clinng, en su calidad de responsable y/o encargado del tratamiento de datos personales tiene las siguientes responsabilidades:

- Garantizar al titular en todo momento el pleno y efectivo ejercicio de su derecho de hábeas data, permitiéndole el acceso, actualización y rectificación de sus datos personales.
- Solicitar y conservar la autorización correspondiente otorgada por el titular para el uso y tratamiento de sus datos personales, manteniendo copia de dicha autorización como respaldo.
- Informar adecuadamente al titular sobre la finalidad de la recolección de sus datos

personales y los derechos que le asisten en virtud de la autorización otorgada.

- Rectificar oportunamente los datos que resulten incorrectos, comunicando dicha actualización al encargado del tratamiento.
- Suministrar al encargado del tratamiento únicamente los datos cuya autorización de tratamiento haya sido obtenida previamente, en conformidad con lo establecido en la Ley 1581 de 2012.
- Conservar la información bajo estrictas condiciones de seguridad para evitar su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- Actualizar la información de manera oportuna, notificando al encargado sobre cualquier novedad que afecte los datos suministrados, adoptando medidas que garanticen su precisión y vigencia.
- Tramitar consultas, quejas y reclamos presentados por los titulares, conforme a los términos señalados por la Ley 1581 de 2012.
- Adoptar un Política interno que contenga las políticas y procedimientos necesarios para asegurar el cumplimiento de la ley y la adecuada atención de consultas, quejas y reclamos.
- Abstenerse de circular información que haya sido controvertida por el titular y cuyo bloqueo haya sido ordenado por la Superintendencia de Industria y Comercio.
- Registrar la leyenda “reclamo en trámite” en la base de datos correspondiente, tal como lo regula la Ley 1581 de 2012.
- Insertar la leyenda “información en discusión judicial” en la base de datos cuando sea notificado por la autoridad competente sobre procesos judiciales que involucren la calidad de los datos.
- Permitir el acceso a los datos personales únicamente a las personas autorizadas para ello.
- Informar a la Superintendencia de Industria y Comercio sobre cualquier violación a los códigos de seguridad que ponga en riesgo la administración de la información de los titulares.
- Cumplir con las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio en relación con la protección de datos personales.

Sin perjuicio de las responsabilidades antes descritas, a continuación, se detallan los roles y responsabilidades en referencia a esta Política:

I.7.1. Máximo Órgano de Administración

- Designar a la persona o área encargada de la protección de datos personales en la organización.
- Aprobar y monitorear el Programa Integral de Gestión de Datos Personales (PIGDP).
- Destinar recursos suficientes para la implementación del PIGDP.
- Establecer las responsabilidades específicas para las distintas áreas de la organización en relación con la recolección, almacenamiento, uso y disposición de datos personales.

1.7.2. Gerente de Riesgos y Cumplimiento

- Supervisar el desarrollo, implementación y ejecución del programa de cumplimiento en materia de privacidad y protección de datos personales.

1.7.3. Oficial de Protección de Datos Personales (OPD)

- Garantizar la implementación efectiva de las políticas y procedimientos para cumplir con la Ley 1581 de 2012 y otras normas relacionadas.
- Implementar buenas prácticas en la gestión de datos personales dentro de Clinng.
- Administrar el Programa Integral de Gestión de Datos Personales (PIGDP), manteniendo los controles necesarios para su cumplimiento.
- Coordinar la evaluación continua del PIGDP y promover un sistema de gestión de riesgos en relación con el tratamiento de datos personales.
- Fomentar la cultura de protección de datos mediante capacitaciones periódicas para todo el personal de la organización.
- Mantener actualizado el inventario de bases de datos y coordinar su inscripción en el Registro Nacional de Bases de Datos (RNBD).

- Acompañar a la organización en la atención de visitas o requerimientos de la Superintendencia de Industria y Comercio (SIC), asegurando el cumplimiento normativo.

1.7.4. Responsable de Seguridad Lógica

- Velar por la protección de la información lógica y garantizar que las medidas de seguridad se implementen conforme a las políticas de gestión de seguridad de la información.

1.7.5. Responsable de Seguridad Física

- Asegurar la protección de la información física, garantizando la seguridad de los documentos y soportes físicos que contienen datos personales.

1.7.6. Responsable de la Base de Datos

- Asegurar el ejercicio de los derechos de los titulares (acceso, actualización, rectificación y supresión).
- Determinar la finalidad y contenido de las bases de datos, garantizando la seguridad y protección de la información.
- Coordinar con el Oficial de Protección de Datos todas las acciones relacionadas con el tratamiento de los datos personales.
- Velar por la correcta eliminación segura de datos y garantizar que el acceso sea restringido a personas autorizadas.

1.7.7. Dueño de la Base de Datos

- Definir los lineamientos para el tratamiento de los datos personales según las políticas de protección de datos.
- Asegurar el cumplimiento de las medidas técnicas, organizativas y legales para proteger las bases de datos personales.
- Garantizar la confidencialidad de los datos y velar por el respeto a los derechos fundamentales de los titulares.

1.7.8. Custodio del Banco de Datos

- Resguardar las bases de datos de los aplicativos de Clinng, cumpliendo con las normativas aplicables.
- Seguir las funciones y responsabilidades relacionadas con la protección y custodia de la información contenida en los bancos de datos.

I.8. Definiciones

Con fines prácticos la definición recogida por la legislación colombiana respecto de la protección de datos personales.

- **Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales.
- **Aviso de privacidad:** Comunicación verbal o escrita generada por el responsable, dirigida al Titular para el Tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las políticas de Tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del Tratamiento que se pretende dar a los datos personales.
- **Base de Datos:** Conjunto organizado de datos personales que sea objeto de Tratamiento.
- **Causahabiente:** Persona que ha sucedido a otra por causa del fallecimiento de ésta (heredero).
- **Datos personales:** Son cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.
- **Dato público:** Es el dato que no es semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias

judiciales debidamente ejecutoriadas que no estén sometidas a reservas.

- **Dato privado:** Es el dato que por su naturaleza íntima o reservada solo es relevante para el titular.
- **Dato semiprivado:** Es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento y divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas, o a la sociedad en general, como el dato financiero y crediticio.
- **Datos sensibles:** Es aquel que afecta la intimidad del titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.
- **Documento de archivo:** Es el registro de información producida o recibida por una entidad pública o privada debido a sus actividades o funciones.
- **Datos abiertos:** Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos.
- **Encargado del Tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento.
- **Habeas data:** Es el derecho permitir a los ciudadanos conocer, actualizar y rectificar toda la información que tengan las diferentes entidades y bases de datos del país.
- **Información:** Se refiere a un conjunto organizado de datos contenido en cualquier documento que los responsables y/o encargados del tratamiento generen, obtengan, adquieran, transformen o controlen.

- **Información pública:** Es toda información que el responsable y/o encargado del tratamiento genere, obtenga, adquiera o controle en su calidad de tal.
- **Información pública clasificada**: Es aquella información que estando en poder de un sujeto responsable en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica, por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en la ley.
- **Información pública reservada:** Es aquella información que estando en poder de un sujeto responsable en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos.
- **Responsable del Tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos.
- **Titular:** Persona natural cuyos datos personales sean objeto de Tratamiento.
- **Tratamiento:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.
- **Transferencia:** La transferencia de datos tiene lugar cuando el Responsable y/o Encargado del Tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es Responsable del Tratamiento y se encuentra dentro o fuera del país.
- **Transmisión:** Tratamiento de datos personales que implica la comunicación de estos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un Tratamiento por el Encargado por cuenta del responsable.
- **Oficial de Protección de Datos:** Será quién asuma al interior de Clinng, la función de protección de datos personales y dará trámite a las solicitudes de los titulares, para el ejercicio de los derechos a que se refiere la Ley 1581 de 2012, sus decretos reglamentarios y las Circulares Externas expedidas por la SIC y demás normas o disposiciones que la modifiquen complementen o reemplacen.

I.G. Principios

I.G.1. Principio de Legalidad

El tratamiento de datos personales es una actividad reglada que debe sujetarse a lo establecido en la ley y demás disposiciones aplicables en Colombia.

I.G.2. Principio de Finalidad

Los datos personales deben ser recolectados con una finalidad específica, explícita y legítima, la cual debe ser informada al titular.

I.G.3. Principio de Libertad

El tratamiento de datos personales solo puede ejercerse con el consentimiento, previo, expreso e informado del titular.

I.G.4. Principio de Veracidad o Calidad

La información sujeta a tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible.

I.G.5. Principio de Acceso y Circulación Restringida

El tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la ley y la Constitución.

I.G.6. Principio de Seguridad

La información sujeta a tratamiento por el responsable del tratamiento o encargado del tratamiento debe ser protegida mediante el uso de las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros, evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

I.G.7. Principio de Confidencialidad

Todas las personas que intervengan en el tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el tratamiento.

II. DERECHOS DEL TITULAR

II.1. DERECHOS DEL TITULAR DE LOS DATOS PERSONALES

En Colombia, el habeas data es el derecho fundamental que tienen los titulares de datos personales a conocer, actualizar, rectificar y suprimir la información que se haya recogido sobre ellos en bases de datos o archivos. Este derecho garantiza la protección de la intimidad personal y el control sobre los datos personales.

Los titulares de datos personales en Clinng, conforme a la Ley 1581 de 2012 y a los principios establecidos en dicha normativa, tienen los siguientes derechos:

- **Derecho de acceso**: El titular tiene derecho a conocer qué información personal ha sido almacenada, su finalidad y el tratamiento que se les está dando. También puede solicitar ser informado sobre el uso que se les ha dado a sus datos personales.
- **Derecho de rectificación**: El titular puede solicitar la corrección de sus datos cuando sean inexactos, incompletos, fraccionados o erróneos, así como la actualización e inclusión de nuevos datos personales.
- **Derecho de cancelación o supresión**: El titular tiene derecho a solicitar la eliminación de sus datos personales cuando estos ya no sean necesarios para los fines con los cuales fueron recolectados, o cuando el tratamiento no respete los principios y garantías legales. También puede pedir la supresión cuando haya revocado su consentimiento.

- **Derecho de oposición**: El titular puede oponerse al tratamiento de sus datos personales cuando existan motivos legítimos relacionados con su situación personal o cuando no se haya otorgado el consentimiento.
- **Derecho a solicitar prueba de la autorización**: El titular puede requerir a Clinng la prueba de la autorización otorgada para el tratamiento de sus datos, salvo en los casos en que la ley exceptúe este requisito.
- **Derecho a revocar la autorización**: El titular puede revocar su consentimiento en cualquier momento si considera que en el tratamiento no se respetan sus derechos constitucionales y legales.
- **Derecho a presentar quejas ante la Superintendencia de Industria y Comercio (SIC)**: El titular puede presentar quejas ante la SIC por infracciones a la Ley 1581 de 2012 y las normas que la complementen o modifiquen.
- **Derecho a acceder de forma gratuita** a sus datos personales que hayan sido objeto de tratamiento.

Los derechos pueden ser ejercidos directamente por el titular, sus causahabientes, su representante o apoderado debidamente acreditado, cumpliendo con los requisitos establecidos por la ley.

II.2. CAPACIDAD Y CONDICIONES PARA EL EJERCICIO DE LOS DERECHOS

Los derechos de acceso, rectificación, supresión o cancelación y oposición sólo pueden ser ejercidos por el titular de datos personales, sin perjuicio de las normas que regulan la representación. En este sentido, el ejercicio de estos derechos puede ser realizado:

- **Por el titular**: Deberá acreditar su identidad de manera suficiente utilizando los medios proporcionados por el responsable del tratamiento.
- **Por sus causahabientes**: Deberán demostrar su calidad de tal a través de la documentación correspondiente.

- **Por el representante y/o apoderado del titular**: Será necesario presentar la acreditación de la representación o el poder otorgado de forma adecuada.
- **Por estipulación a favor de otro o para otro**: Se deberá contar con la documentación que acredite dicha estipulación.

III. PROCEDIMIENTO PARA LA ATENCION DE PQRS

III.1. LEGITIMACIÓN PARA PRESENTAR RECLAMOS Y SOLICITUDES

El titular de los datos o sus representantes legítimos pueden presentar sus reclamos relacionados con el tratamiento de los datos personales. El Oficial de Protección de Datos Personales (en adelante OPD) es responsable de verificar la legitimación del solicitante y asegurarse de que la solicitud sea procesada adecuadamente.

III.2. CANAL DE PRESENTACIÓN DE RECLAMOS Y SOLICITUDES

Las solicitudes de reclamos o PQRS deben enviarse a través del correo electrónico **support@clinngpayments.com**, donde el OPD es el responsable de recibirlas y asegurarse de que sean debidamente registradas.

III.3. SOLICITUD DEL RECLAMO

El OPD se encargará de gestionar la solicitud del reclamo, asegurándose de que esta incluya la información necesaria, como la identificación del titular, los hechos que originan el reclamo y la documentación pertinente.

III.4. SUBSANACIÓN Y DESESTIMIENTO DE RECLAMOS

Si el reclamo presentado es incompleto, el OPD será responsable de solicitar la información adicional necesaria dentro de los cinco (5) días hábiles siguientes a la

recepción del reclamo. El titular tendrá un plazo de cinco (5) días hábiles para subsanar las observaciones.

Si el titular no presenta la información requerida dentro de este plazo, o si no subsana las observaciones dentro del término de dos (2) meses desde la solicitud de subsanación, se considerará que ha desistido del reclamo,

III.5. COMPETENCIA PARA RESOLVER RECLAMOS

El OPD es responsable de evaluar si Clinng es competente para resolver el reclamo. Si no es competente, el OPD trasladará el reclamo a la entidad correspondiente y notificará al titular de esta decisión dentro de los dos (2) días hábiles siguientes.

III.6. REGISTRO DEL RECLAMO

El OPD registrará el reclamo en la base de datos y colocará la leyenda "reclamo en trámite" en un plazo no mayor a dos (2) días hábiles, con el objetivo de mantener un registro claro del estado del reclamo.

III.7. PLAZO DE ATENCIÓN A RECLAMOS

El OPD se encargará de asegurar que el reclamo sea resuelto dentro del plazo máximo de quince (15) días hábiles. Si se requiere más tiempo, el OPD extenderá el plazo hasta un máximo de ocho (8) días hábiles adicionales, notificando previamente al titular.

IV. PROCEDIMIENTO PARA EL EJERCICIO DEL DERECHO DE HABEAS DATA

IV.1. REQUISITOS

El titular de los datos personales podrá ejercer sus derechos de acceso, actualización, rectificación, supresión y revocación de la autorización mediante una solicitud que deberá remitir a Clinng. El responsable de recibir y gestionar esta solicitud es el OPD, quien verificará que los requisitos establecidos se cumplan y coordinará las acciones necesarias para el ejercicio de dichos derechos.

IV.2. RECEPCIÓN DE LA SOLICITUD

Las solicitudes podrán ser enviadas al correo electrónico **support@clinngpayments.com**. El OPD es responsable de recibir estas solicitudes y registrarlas para su posterior gestión.

IV.3. PROCEDIMIENTO DE ATENCIÓN A LA SOLICITUD

El OPD es el encargado de evaluar que la solicitud cumpla con los requisitos mencionados en el apartado anterior. En caso de que la solicitud no cumpla con los requisitos, el OPD formulará las observaciones correspondientes dentro de un plazo máximo de cinco (5) días hábiles. Si el titular no subsana las observaciones en el plazo establecido, se considerará que la solicitud no ha sido presentada. Si la solicitud es suficiente, el OPD iniciará el proceso de resolución correspondiente.

IV.4. PLAZO DE RESPUESTA A SOLICITUDES

El **OPD** gestionará las solicitudes y se asegurará de que se respondan dentro del plazo de diez (10) días hábiles desde la recepción de la solicitud. Si no es posible cumplir con este plazo, el **OPD** informará al titular los motivos de la demora y proporcionará una nueva fecha para la resolución, que no excederá los cinco (5) días hábiles adicionales.

V. USO DE DATOS

Clinng se compromete a garantizar el tratamiento adecuado de los datos personales en conformidad con la Ley 1581 de 2012, aplicando las siguientes directrices respecto al uso, tratamiento, transferencia y transmisión de los datos personales:

V.1. TRATAMIENTO AUTORIZADO

Clinng solo autoriza el tratamiento de los datos personales en los siguientes casos y conforme a las finalidades que han sido debidamente informadas al titular:

V.1.1. Datos Públicos

El tratamiento de datos personales de naturaleza pública puede realizarse sin necesidad de autorización previa, siempre que provengan de registros públicos y se ajusten a los principios establecidos en la Ley 1581 de 2012.

V.1.2. Datos Privados

El tratamiento de estos datos se realiza con el consentimiento previo, expreso e informado del titular, dentro del marco de relaciones comerciales, laborales, contractuales y administrativas, según lo dispuesto por la normativa vigente.

V.1.3. Datos Sensibles

Para el tratamiento de datos sensibles, como los relacionados con la salud, orientación sexual o religión, se requiere una autorización explícita, previa e informada del titular. El titular debe ser informado de que la provisión de estos datos es opcional, y debe conocer con detalle la finalidad de su uso.

V.2. TRATAMIENTO PROHIBIDO

Clinng prohíbe el tratamiento de datos personales en los siguientes casos:

V. 2.1. Datos Sensibles sin Consentimiento

El tratamiento de datos sensibles sin la autorización explícita del titular, salvo en los casos excepcionales establecidos por la ley.

V.2.2. Uso Contrario a la Finalidad Informada

Cualquier uso de datos que no esté alineado con la finalidad específica informada al titular, o que exceda los límites del consentimiento otorgado.

V.2.3. Transferencia y Transmisión de Datos Personales

A. Transferencia Nacional

Clinng podrá transferir datos personales a terceros dentro del país para fines relacionados con su actividad comercial, siempre que los destinatarios cumplan con los principios de protección de datos establecidos en la legislación colombiana. Los proveedores involucrados en el tratamiento de datos personales serán responsables de cumplir con las normativas de seguridad y privacidad.

B. Transferencia Internacional

En caso de que los datos personales sean transferidos fuera de Colombia, Clinng garantizará que se cumpla con los requisitos de la Ley 1581 de 2012 y las normas reglamentarias. Se implementarán medidas contractuales para asegurar que el tratamiento de los datos en el país receptor cumpla con los estándares de protección adecuados.

C. Excepciones en la Transferencia Internacional

En situaciones excepcionales, como la necesidad de proteger el interés vital del titular o cuando la ley permita, los datos podrán ser transferidos a países que no cuenten con un nivel adecuado de protección, siempre que se cumpla con las condiciones legales exigidas.

V.2.4. Confidencialidad y Seguridad de los Datos

Clinng se compromete a mantener la confidencialidad de los datos personales tratados, incluso después de finalizada la relación con el titular de los datos. Esta obligación se extiende a todos los empleados y proveedores que participen en el tratamiento de los datos, quienes deberán suscribir acuerdos de confidencialidad. La información será almacenada de forma segura, y se implementarán medidas de protección para evitar el acceso no autorizado, la pérdida o la alteración de los datos.

V.5. EXCEPCIONES AL TRATAMIENTO DE DATOS

Se exceptúan del régimen de protección de datos personales aquellos tratados con fines de prevención, monitoreo y control en el ámbito de la lucha contra el lavado de activos y financiamiento del terrorismo, conforme a la Ley 1581 de 2012 y otras disposiciones legales relacionadas.

Este apartado cubre tanto el uso autorizado y prohibido de los datos, como las normas para su transferencia y confidencialidad, asegurando que se respeten los derechos de los titulares y las regulaciones vigentes.

V.6. BASES DE DATOS DE CLINNG

V.6.1. Tipos de base de datos

Clinng gestiona varias bases de datos con fines específicos, alineados con la normativa de protección de datos. Las principales bases de datos son:

- **Base de Datos de Candidatos**.- Recoge datos de postulantes para procesos de selección, gestión de vacantes y desarrollo organizacional.
- **Base de Datos de Empleados**.- Contiene datos personales de colaboradores, empleados y excolaboradores para cumplir con obligaciones laborales y de recursos humanos.

- **Base de Datos de Proveedores**.- Contiene información sobre proveedores para su gestión administrativa, contable y de pagos.
- **Base de Datos de PQRS (Peticiones, Quejas, Reclamos y Sugerencias)**. Recopila información de los usuarios del sitio web y de otras interacciones con la empresa para gestionar peticiones, quejas, reclamos y sugerencias. Esta base de datos permite brindar información sobre los servicios ofrecidos, realizar actividades de prospección comercial y analizar los reclamos para mejorar la satisfacción del cliente y optimizar los procesos internos
- **Base de datos de accionistas.-** Contiene información personal de los accionistas, como nombre, documento de identidad, porcentaje de participación en la empresa, información de contacto, y otros datos relevantes para cumplir con obligaciones fiscales y de gobernanza corporativa. Esta base de datos es utilizada para registrar la propiedad de la empresa y asegurar la comunicación con los accionistas.
- **Base de datos de clientes finales.-** Recoge datos personales de clientes finales, incluyendo información de contacto, historial de compras, preferencias de productos y servicios, métodos de pago, entre otros. Esta base de datos permite a la empresa gestionar la relación con los clientes, realizar campañas de marketing, y ofrecer servicios personalizados.
- **Base de datos de usuarios finales del servicio.-** Almacena información de los usuarios finales de un servicio específico, como nombre, contacto, historial de uso, preferencias de servicio y otros datos relacionados con la interacción con el servicio. Esta base de datos es clave para gestionar el acceso al servicio, realizar soporte al cliente y mejorar la experiencia del usuario.

Para mayor detalle de este apartado, puede revisar el Manual de Privacidad y Protección de Datos Personales de Clinng.

V.6.2. Periodo de Vigencia de las Bases de Datos Personales

El periodo de vigencia de las bases de datos personales de Clinng dependerá de la finalidad del tratamiento y las normativas legales colombianas aplicables:

- **Finalidad laboral:** Los datos personales relacionados con historiales laborales deben ser conservados durante la relación laboral y hasta 50 años después de la finalización del vínculo laboral, en cumplimiento con el Código Sustantivo del Trabajo de Colombia y las normativas sobre pensiones.
- **Finalidad de marketing o comercial:** Los datos personales recolectados con fines comerciales o de marketing se conservarán por un plazo máximo de 5 años desde la última interacción significativa o desde el momento en que el titular otorgue su consentimiento, de acuerdo con la Ley 1581 de 2012 y el principio de finalidad.
- **Información financiera y contable:** Los documentos financieros y contables deben ser conservados por al menos 10 años, conforme al Código de Comercio de Colombia y la Ley 222 de 1995, para cumplir con las obligaciones fiscales y de auditoría.

VI. MECANISMOS DE RECOLECCIÓN

Clinng emplea diversos mecanismos para la recolección de datos personales, los cuales son adecuados a las finalidades específicas para las que se requiere la información y cumplen con los principios establecidos en la legislación colombiana, particularmente en la Ley 1581 de 2012 y su reglamentación.

VI.1. TIPOS DE MECANISMOS DE RECOLECCIÓN

VI.1.1. Formularios Electrónicos

La recolección de datos personales se puede realizar mediante formularios en línea en la web de Clinng o el sistema interno del Grupo, que permiten a los titulares proporcionar su información de forma voluntaria. En estos formularios se detallan las finalidades específicas del tratamiento de los datos, asegurando que el titular tenga conocimiento claro sobre cómo se utilizarán sus datos.

VI.1.2. Registros y Contratos

Los datos también se recopilan en el contexto de relaciones contractuales, como la firma de contratos laborales, comerciales o de servicios. Estos documentos contienen las autorizaciones correspondientes, donde el titular manifiesta su consentimiento previo, expreso e informado para el tratamiento de sus datos personales.

VI.2. CONSENTIMIENTO EXPRESO A TRAVÉS DE CANALES DIGITALES

Clinng asegura que, al recopilar datos a través de sus canales digitales, se implemente un proceso de autorización clara y directa. En este proceso, los titulares deben marcar una casilla de aceptación o dar su consentimiento de manera digital, lo que permite registrar su autorización de forma verificable.

VI.2.1. Registro de Consentimiento en Medios Verificables

Cada consentimiento otorgado por los titulares se registrará de forma que se garantice su trazabilidad. Esto incluye la conservación de pruebas en formatos físicos o electrónicos que puedan ser consultadas posteriormente si el titular o las autoridades lo requieren.

VI.2.2. Recolección por Terceros Autorizados

En algunos casos, la recolección de datos puede ser realizada por proveedores o terceros autorizados por Clinng, quienes están obligados a cumplir con las disposiciones de protección de datos personales. La autorización para este tipo de recolección también se realizará conforme a los principios de consentimiento libre, previo, expreso e informado.

VI.2.3. Uso de Bases de Datos Públicas

Clinng podrá acceder a ciertos datos personales de naturaleza pública, que provienen de fuentes como registros públicos o entidades oficiales, sin necesidad de autorización previa. Sin embargo, el uso de estos datos está sujeto a los principios establecidos en la Ley 1581 de 2012, como la finalidad específica y la protección de la confidencialidad.

VI.2.4. Tratamiento de Datos Sensibles

Cuando se recojan datos sensibles (por ejemplo, relacionados con la salud, la orientación sexual o la religión), se requerirá una autorización explícita adicional. En estos casos, se informará claramente al titular sobre la necesidad de proporcionar estos datos y las finalidades específicas del tratamiento.

VI.3. AUTORIZACIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES

VI.3.1. Autorizaciones y consentimientos del titular

Clinng solicitará de manera previa, expresa e informada la autorización del titular para el tratamiento de sus datos personales, cumpliendo con lo establecido en la Ley 1581 de 2012. Dicha autorización deberá obtenerse a través de cualquier medio que pueda ser objeto de consulta y verificación posterior, garantizando la trazabilidad del consentimiento.

Esta autorización es necesaria para la recolección, almacenamiento, uso, circulación y supresión de los datos personales, y debe estar alineada con el desarrollo del objeto social de Clinng, así como con sus relaciones comerciales y financieras.

Se exceptúan de la necesidad de autorización los casos en los que la información sea requerida por entidades públicas o administrativas en ejercicio de sus funciones legales, por orden judicial, datos de naturaleza pública, urgencias médicas o sanitarias, tratamientos autorizados por la ley para fines históricos, estadísticos o científicos, o datos relacionados con el registro civil.

Los titulares de los datos deben ser informados, al momento de la recolección, sobre los datos que serán recolectados y todas las finalidades del tratamiento.

VI.3.2. Prueba de la autorización

Clinng conservará, de manera adecuada y segura, la prueba de las autorizaciones otorgadas por los titulares de los datos personales, respetando los principios de privacidad y confidencialidad. Esta prueba puede incluir registros en formato físico, electrónico, verbal o conductas inequívocas del titular que permitan concluir razonablemente que se otorgó el consentimiento para el tratamiento de los datos.

VI.3.3. Tipos de autorizaciones de tratamiento de datos personales

- **Nuevos titulares:** Son aquellas personas cuyos datos personales han sido recolectados con posterioridad a la fecha de emisión de este Política. Se requerirá su autorización expresa para el tratamiento de los datos.
- **Antiguos titulares:** Son aquellas personas cuyos datos fueron recolectados antes de la emisión de este Política. En estos casos, se solicitará autorización para continuar con el tratamiento de los datos personales.

VI.3.4. Medios y manifestaciones para otorgar la autorización

La autorización podrá otorgarse mediante cualquier formato o mecanismo que permita su posterior verificación, como documentos físicos, electrónicos o cualquier tecnología idónea que garantice la trazabilidad del consentimiento.

También puede obtenerse mediante conductas inequívocas del titular que demuestren de manera razonable que su consentimiento fue otorgado, siempre y cuando dichas conductas manifiesten claramente la voluntad del titular de permitir el tratamiento de sus datos personales.

Clinng se asegurará de que la autorización se presente al titular de manera previa al tratamiento de sus datos, de forma que pueda ser consultada o verificada en cualquier momento, garantizando el cumplimiento de las disposiciones legales.

VI.3.5. Revocatoria de la autorización

Los titulares podrán solicitar en todo momento la supresión de sus datos personales y/o revocar la autorización otorgada para el tratamiento de estos mediante la presentación de un reclamo.

La solicitud de supresión de los datos personales y la revocatoria de la autorización no procederán cuando el titular tenga un deber legal o contractual de permanecer en la base de datos.

Una vez expire la vigencia de las bases de datos, se debe proceder a la supresión de los datos personales en su posesión. No obstante, los datos personales deberán ser conservados cuando así se requiera para el cumplimiento de una obligación legal o contractual.

VII. MEDIDA DE SEGURIDAD APLICADO AL TRATAMIENTO DE DATOS PERSONALES

Con el fin de salvaguardar la confidencialidad, integridad, disponibilidad y privacidad de la información de Clinng, los colaboradores deberán cumplir con las siguientes medidas de seguridad y confidencialidad en el tratamiento de datos personales, garantizando que toda la información a la que tengan acceso sea tratada conforme a lo dispuesto en la Ley 1581 de 2012 y demás normas aplicables:

VII.1. CONFIDENCIALIDAD Y ACCESO RESTRINGIDO

- Mantener la confidencialidad de toda la información a la que tengan acceso, especialmente aquella relacionada con datos personales de usuarios, información

pública clasificada o reservada, ajustándose a las políticas internas de seguridad de la información.

Los colaboradores deben utilizar contraseñas seguras para acceder a los sistemas y aplicaciones de Clinng, en caso aplique.

- No divulgar, copiar, modificar ni permitir el acceso a terceros de la información contenida en las bases de datos o sistemas de información sin la debida autorización de Clinng.

VII.1.1. Uso Adecuado De Los Recursos

Los recursos y herramientas tecnológicas asignados para el desempeño de sus funciones deberán ser utilizados únicamente para los fines establecidos por la entidad, conforme al artículo 17 de la Ley 1581 de 2012.

VII.1.2. Protección Física y Digital de Documentos

La información física deberá almacenarse en **espacios restringidos**, bajo llave y con medidas de seguridad que garanticen su integridad.

En cuanto a la información digital, se aplicarán controles de acceso y cifrado de datos para prevenir accesos no autorizados.

VII.2. GESTIÓN DE ACCESOS Y FINALIZACIÓN DE RELACIÓN LABORAL

Al finalizar la relación laboral con Clinng, el colaborador deberá entregar formalmente toda la documentación y cuentas de usuario a su jefe inmediato y asegurarse de que todos los accesos a sistemas y aplicaciones sean desactivados.

En caso de que continúe con algún acceso, deberá notificarlo de inmediato al área de Tecnología.

VII.3. CONSERVACIÓN DE DOCUMENTOS

Los documentos financieros y contables deberán ser conservados por un mínimo de 10 años, conforme a lo estipulado en el artículo 60 de la Ley 16 de 1968. Los documentos relacionados con historiales laborales deberán ser conservados durante 80 años para fines de derechos pensionales y reclamaciones, de acuerdo con normativa aplicable.

VII.4. NOTIFICACIÓN DE INCIDENTES DE SEGURIDAD

Informar oportunamente cualquier incidente o vulnerabilidad que comprometa la seguridad de los datos personales a través de los canales establecidos, notificando al Oficial de Protección de Datos cuando se presenten violaciones de seguridad en los sistemas de información, de acuerdo con el numeral n del artículo 17 de la Ley 1581 de 2012.

VIII. CAPACITACIONES

Clinng desarrollará y mantendrá programas periódicos de capacitación y concientización en Protección de Datos Personales, con el objetivo de asegurar que todos los colaboradores comprendan y cumplan con las responsabilidades relacionadas con el tratamiento de datos personales. Estos programas serán obligatorios para todo el personal y se actualizarán regularmente para reflejar los cambios normativos y las mejores prácticas.

IX. VIGENCIA

Esta versión del Política entra en febrero de 2025.

En el caso de las bases de datos personales estarán sujetas a un periodo de vigencia determinado de acuerdo con la finalidad para la cual fueron recolectadas. El periodo de vigencia de cada base de datos será definido conforme a las

normativas vigentes y las disposiciones legales aplicables, asegurando que la información se conserve únicamente durante el tiempo necesario para cumplir con la finalidad para la cual fue recolectada.

El responsable de las bases de datos será el encargado de garantizar que se realicen las actualizaciones necesarias y se mantenga la vigencia de las bases conforme a la legislación aplicable, y que se eliminen cuando ya no sean necesarias para las finalidades previamente informadas.

X. MODIFICACIONES

Clinng se reserva el derecho de modificar esta política en cualquier momento, para adaptarla a cambios normativos, tecnológicos o de operación. Cualquier modificación será comunicada oportunamente a los titulares de los datos personales mediante los canales disponibles, como la página web o comunicación directa. Las modificaciones entrarán en vigor desde su publicación, a menos que se indique lo contrario.

XI. ADMINISTRACION DE LA POLITICA

El Oficial de Protección de Datos es responsable de gestionar esta Política , asegurando su revisión al menos una vez al año o con mayor frecuencia si las circunstancias lo exigen, como en los siguientes casos:

- Implementación de nuevos requisitos regulatorios o guías aplicables.
- Orientaciones emitidas por reguladores o autoridades competentes.
- Cambios en la estrategia corporativa del Grupo Monnet.
- Incidentes o incumplimientos que justifiquen ajustes en esta política.
- Necesidad de alinear la política con las mejores prácticas de la industria.

El OPD preparará y presentará las actualizaciones propuestas al Máximo Órgano de Administración para su revisión y aprobación final.