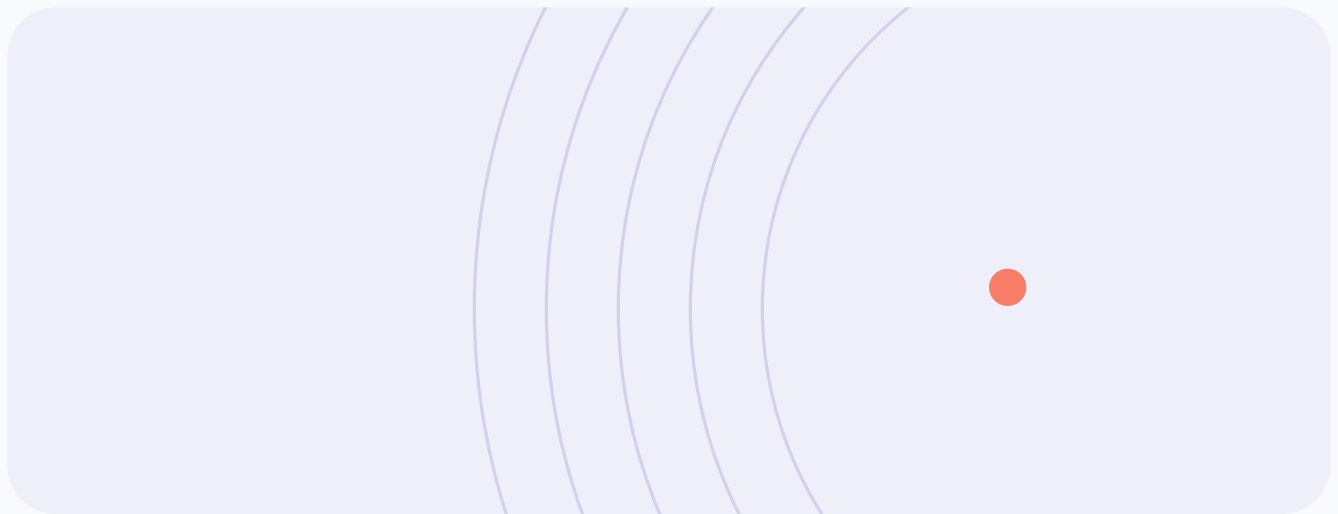


Acuerdo de procesamiento de datos

Datos personales y confidencialidad



Hey Llave S.A.S.

NIT 902093674-4

Última actualización • 14 de octubre de 2026

HEY LLAVE S.A.S.

ACUERDO DE PROCESAMIENTO DE DATOS PERSONALES (DPA) Y ACUERDO DE CONFIDENCIALIDAD.

Cuando EL CLIENTE acepta los Términos y Condiciones Generales o suscribe un Contrato de Condiciones Particulares de Licencia de Uso (Plan Enterprise), se adhiere y acepta íntegramente las disposiciones legales y operativas detalladas a continuación sin perjuicio de las demás aplicables dentro de la masa legal operativa de HEYLLAVE, en estricto cumplimiento de la Ley Estatutaria 1581 de 2012 y el Capítulo 25 del Decreto Único Reglamentario 1074 de 2015.

CLÁUSULA PRIMERA. OBJETO Y CALIDAD JURIDICA DE LAS PARTES.

1.1. El presente Acuerdo tiene por objeto regular las condiciones bajo las cuales HEYLLAVE procesará los datos personales alojados en la Plataforma. Para todos los efectos derivados de la normatividad colombiana, las Partes declaran, reconocen y aceptan la siguiente separación estricta de roles y calidades jurídicas:

HEYLLAVE como Responsable del Tratamiento: Actúa en esta calidad legal única y exclusivamente frente a los datos personales, corporativos, credenciales de acceso, información de facturación y de contacto directo de EL CLIENTE (los representantes legales o personas naturales que adquieren y suscriben la licencia de uso) y de sus dependientes o contratistas.

EL CLIENTE como Responsable del Tratamiento: Ostenta el poder de decisión, control y disposición sobre las bases de datos de sus propios usuarios finales, contactos y prospectos comerciales. Tiene la carga legal, probatoria y exclusiva de obtener la autorización previa, expresa e informada de dichos titulares para someter su información a tratamiento.

HEYLLAVE como Encargado del Tratamiento: Frente a las bases de datos y prospectos controlados por EL CLIENTE, la intervención de HEYLLAVE se limita estrictamente a proveer la

infraestructura de Software como Servicio (SaaS), el alojamiento en la nube y el procesamiento de la información de acuerdo con las instrucciones operativas definidas por EL CLIENTE a través de la interfaz de la Plataforma.

CLÁUSULA DOS. INSTRUCCIONES DE TRATAMIENTO.

2.1. HEYLLAVE actúa única y exclusivamente como Responsable del Tratamiento frente a los datos personales, corporativos, credenciales de acceso, información de facturación y de contacto directo suministrados por sus clientes directos (los representantes legales o personas naturales que suscriben las Condiciones Generales de Contratación o la Licencia de Uso Particular). El tratamiento de esta información administrativa y comercial se rige por la Política de Privacidad de HEYLLAVE.

2.2. Por el contrario, frente a los datos de terceros alojados en el CRM, HEYLLAVE, en su estricta calidad de Encargado, se obliga a realizar el Tratamiento (entendido como la recolección, almacenamiento, uso, circulación técnica y supresión) de los datos personales de los usuarios finales, prospectos y contactos de EL CLIENTE única y exclusivamente para garantizar el funcionamiento operativo del ecosistema. Este tratamiento estará subordinado a las instrucciones directas, automatizadas o manuales, que EL CLIENTE emita a través de la interfaz del software para la ejecución de sus funcionalidades (envío de campañas, automatizaciones, analítica y gestión comercial), bajo los parámetros de las Condiciones Generales de Contratación, la Política de Privacidad y/o la Licencia de Uso Particular aplicable.

2.3. Queda total y estrictamente prohibido para HEYLLAVE utilizar, explotar, perfilar, comercializar, ceder o transferir las bases de datos alojadas por EL CLIENTE para finalidades propias o de terceros sin autorización del titular de los datos personales. HEYLLAVE no podrá acceder a dicha información para realizar campañas de marketing ajenas a HEYLLAVE, venta de analítica a terceros, estudios de mercado no anonimizados, ni podrá cruzar o fusionar las bases de datos de EL CLIENTE con las de otras empresas alojadas en la plataforma.

2.4. De manera expresa e irrevocable, HEYLLAVE garantiza que la información personal, los historiales de chat, los metadatos y las bases de datos de EL CLIENTE no serán utilizados, bajo ninguna circunstancia, para el entrenamiento, ajuste fino (fine-tuning) o alimentación de modelos de lenguaje o motores de Inteligencia Artificial de carácter público, ya sean propios o pertenecientes a los Sub-Encargados tecnológicos contratados.

2.5. En el evento en que HEYLLAVE destine los datos personales tratados en calidad de Encargado a una finalidad distinta de aquella autorizada por EL CLIENTE, o determine por cuenta propia las finalidades y los medios del tratamiento por fuera de las instrucciones impartidas por EL CLIENTE, dicha actuación será considerada un tratamiento realizado por HEYLLAVE por fuera del alcance de su calidad de Encargado.

Para todos los efectos legales y contractuales, se entenderá que las instrucciones de tratamiento impartidas por EL CLIENTE comprenden: (i) las acciones, configuraciones y órdenes operativas ejecutadas directamente a través de la interfaz de la Plataforma; y (ii) las autorizaciones, finalidades, condiciones de tratamiento y reglas operativas aceptadas por EL CLIENTE mediante los Términos y Condiciones Generales, la Política de Privacidad, el presente Acuerdo de Procesamiento de Datos (DPA) y, cuando exista, la Licencia de Uso Particular o cualquier otro documento contractual que haga parte integral de la relación comercial.

En consecuencia, HEYLLAVE asumirá las obligaciones y responsabilidades que legalmente correspondan respecto de cualquier tratamiento realizado por fuera de dichas instrucciones, de conformidad con la Ley Estatutaria 1581 de 2012 y demás normas aplicables, sin perjuicio de las acciones administrativas, civiles o de cualquier otra naturaleza que resulten procedentes.

CLÁUSULA TERCERA. AUTORIZACIÓN DE SUBCONTRATACIÓN.

3.1. Para garantizar la disponibilidad, escalabilidad y eficiencia operativa del ecosistema SaaS, EL CLIENTE autoriza de manera previa y expresa a HEYLLAVE para subcontratar y realizar la Transmisión de datos personales a terceros proveedores de infraestructura tecnológica. Esta autorización incluye, de forma enunciativa mas no limitativa, a proveedores de alojamiento en la nube (hosting y bases de datos), procesadores de pago transaccional, APIs de comunicación y motores de Inteligencia Artificial (IA).

3.2. HEYLLAVE declara y garantiza que todos los proveedores tecnológicos subcontratados para la ejecución del servicio operarán jurídicamente bajo la figura de Encargados del Tratamiento. HEYLLAVE se obliga a suscribir los respectivos Acuerdos de Procesamiento de Datos y Acuerdos de Confidencialidad con dichos terceros, garantizando que estos queden sometidos a obligaciones de confidencialidad, cifrado, seguridad y prohibición de uso propio equivalentes o superiores a las establecidas en el presente Acuerdo.

3.3. Transmisión internacional de datos. En caso de que, por razones de infraestructura,

disponibilidad, escalabilidad, seguridad o eficiencia operativa, los datos personales sean alojados, procesados o tratados mediante Sub-Encargados cuyos servidores o centros de procesamiento se encuentren ubicados fuera del territorio colombiano, HEYLLAVE verificará previamente que el país de destino y la operación correspondiente cumplan con las condiciones exigidas por la legislación colombiana para la realización de transmisiones internacionales de datos personales.

La utilización de un determinado proveedor, servidor o infraestructura internacional estará sujeta a la verificación de las condiciones legales aplicables al momento de su selección y/o implementación. Cuando resulte legalmente exigible, HEYLLAVE informará al titular sobre la transmisión internacional y obtendrá la autorización correspondiente, de conformidad con la Política de Privacidad y Tratamiento de Datos Personales aplicable y las demás disposiciones legales vigentes.

En todo caso, HEYLLAVE procurará que las transmisiones internacionales se realicen hacia países que cuenten con un nivel adecuado de protección de datos personales reconocido por la Superintendencia de Industria y Comercio o, cuando ello no sea aplicable, que la operación se encuentre amparada por alguna de las excepciones, mecanismos o declaraciones de conformidad legalmente procedentes. HEYLLAVE conservará los soportes que acrediten el cumplimiento de las condiciones aplicables a cada transmisión.

3.4. La autorización de subcontratación no exime a HEYLLAVE de sus obligaciones legales. HEYLLAVE conservará la responsabilidad directa y principal frente a EL CLIENTE por la idoneidad y el cumplimiento normativo de sus Encargados. En caso de presentarse una fuga de información, vulneración de seguridad o incumplimiento legal imputable a la negligencia de un proveedor tecnológico de HEYLLAVE, este último responderá frente a EL CLIENTE, sin perjuicio de las acciones civiles de repetición que HEYLLAVE pueda ejercer posteriormente contra su Encargado.

CLÁUSULA CUARTA. MEDIDAS DE SEGURIDAD Y NOTIFICACIÓN DE INCIDENTES.

4.1. En estricto cumplimiento del Principio de Seguridad consagrado en el artículo 4 de la Ley Estatutaria 1581 de 2012, HEYLLAVE, en su calidad de Encargado, se obliga a implementar, mantener y actualizar permanentemente las medidas técnicas, humanas y administrativas

necesarias para otorgar seguridad a las bases de datos de EL CLIENTE. Estas medidas estarán orientadas a prevenir, controlar y mitigar los riesgos de adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento. La infraestructura de la Plataforma operará bajo estándares razonables de la industria, incluyendo protocolos de cifrado para datos en tránsito (HTTPS/TLS) y protección perimetral de los servidores en la nube.

4.2. HEYLLAVE garantizará que el acceso lógico a la infraestructura donde se procesan y alojan los datos de EL CLIENTE esté estrictamente restringido al personal técnico autorizado, bajo el principio de privilegio mínimo. Toda persona vinculada a HEYLLAVE que intervenga en cualquier fase del tratamiento de la información estará sujeta a rigurosos acuerdos de confidencialidad y reserva legal, obligación que subsistirá incluso después de finalizada su relación contractual o laboral con la compañía.

4.3. En el evento de materializarse una brecha de ciberseguridad, un acceso ilegítimo, un ataque de ransomware o cualquier incidente informático confirmado que comprometa la confidencialidad, integridad o disponibilidad de los datos personales de EL CLIENTE, HEYLLAVE activará de inmediato sus protocolos de contención. HEYLLAVE notificará formalmente a EL CLIENTE sobre la ocurrencia del evento en un plazo no mayor a veinticuatro (24) horas hábiles, contadas a partir de la confirmación técnica integral del incidente por parte del equipo de ciberseguridad o de los Sub-Encargados de infraestructura.

4.4. Obligaciones relacionadas con el Registro Nacional de Bases de Datos (RNBD). Las Partes reconocen que, respecto de las bases de datos cuyo tratamiento sea determinado y controlado por EL CLIENTE, corresponde a este, en su calidad de Responsable del Tratamiento, cumplir las obligaciones que legalmente le sean exigibles frente al Registro Nacional de Bases de Datos (RNBD), incluyendo, cuando resulte procedente, su inscripción, actualización y reporte de las novedades e incidentes de seguridad que deban ser informados a la Superintendencia de Industria y Comercio.

HEYLLAVE, en su calidad de Encargado del Tratamiento, prestará a EL CLIENTE la colaboración técnica y operativa razonablemente necesaria para el cumplimiento de dichas obligaciones. Para tal efecto, HEYLLAVE suministrará, cuando se encuentre bajo su control o custodia y resulte pertinente, la información técnica relacionada con las bases de datos tratadas a través de la Plataforma, incluyendo aquella necesaria para identificar las categorías de información, los mecanismos de tratamiento, los Sub- Encargados, las ubicaciones o países en los que se

realicen transmisiones internacionales y las circunstancias técnicas relevantes de los incidentes de seguridad.

Cuando se presente una violación de los códigos de seguridad, pérdida, robo, acceso no autorizado o cualquier otro incidente de seguridad que afecte información personal de EL CLIENTE bajo tratamiento de HEYLLAVE, este último deberá informar a EL CLIENTE sin dilación indebida y suministrar la información técnica disponible que resulte necesaria para que EL CLIENTE pueda cumplir oportunamente las obligaciones de reporte que legalmente le correspondan ante la Superintendencia de Industria y Comercio.

HEYLLAVE será directamente responsable del cumplimiento de las obligaciones que le correspondan respecto de las bases de datos de las cuales actúe como Responsable del Tratamiento, incluyendo aquellas relacionadas con su propio registro, actualización y reporte ante el RNBD, cuando legalmente resulte exigible.

La colaboración de HEYLLAVE prevista en este numeral no implica que asuma las obligaciones propias de EL CLIENTE como Responsable del Tratamiento, ni exonera a ninguna de las Partes del cumplimiento de las obligaciones que legalmente le correspondan de acuerdo con la calidad que ostente respecto de cada base de datos.

CLÁUSULA QUINTA. ASISTENCIA DE PQRS

5.1. Para la correcta canalización y atención de las solicitudes de Hábeas Data (derecho a conocer, actualizar, rectificar o suprimir información), las Partes reconocen una separación estricta de responsabilidades. Frente a los datos corporativos, credenciales de acceso, información de facturación y de contacto directo de los representantes de EL CLIENTE, HEYLLAVE actúa de manera directa como Responsable del Tratamiento y atenderá cualquier PQR relacionada con estos datos a través de sus canales oficiales de soporte, en estricta sujeción a su propia Política de Privacidad.

5.2. Por el contrario, frente a los datos personales de los usuarios finales, prospectos, leads comerciales o contactos que EL CLIENTE cargue, aloje o procese mediante el entorno digital del CRM, HEYLLAVE actúa exclusivamente como Encargado del Tratamiento. Dado que HEYLLAVE carece de poder de decisión sobre la finalidad, justificación y recolección de dicha información, no admitirá ni resolverá de fondo ninguna solicitud de Hábeas Data que un tercero dirija de forma directa o errónea a las instalaciones o correos de soporte de HEYLLAVE.

5.3. En el evento en que un titular de los datos (usuario final) dirija un reclamo o consulta a HEYLLAVE respecto a la información controlada por EL CLIENTE, la plataforma se limitará a notificar formalmente a EL CLIENTE sobre la recepción de dicha solicitud en un plazo máximo de tres (3) días hábiles. HEYLLAVE trasladará el requerimiento íntegro sin emitir pronunciamiento alguno frente al tercero.

5.4. Una vez notificado el requerimiento, la carga legal y probatoria de emitir la respuesta oficial de fondo al titular recaerá única y exclusivamente sobre EL CLIENTE, dentro de los términos perentorios de diez (10) y quince (15) días hábiles exigidos por los artículos 14 y 15 de la Ley Estatutaria 1581 de 2012. Para facilitar el cumplimiento de este deber legal, HEYLLAVE proveerá la asistencia técnica y operativa razonable, garantizando que EL CLIENTE cuente con las herramientas en la interfaz del software necesarias para buscar, extraer, exportar, modificar o suprimir de manera permanente el registro del titular reclamante de las bases de datos alojadas en la nube.

CLÁUSULA SEXTA. DESTRUCCIÓN, SUPRESIÓN Y RETENCIÓN LEGAL DE LOS

DATOS.

6.1. Eliminación Operativa de Bases de Datos: Una vez finalizada la relación contractual o en caso de suspensión definitiva por impago –superados los noventa y un (91) días calendario de mora continuada estipulados en los Términos y Condiciones–, HEYLLAVE procederá con la eliminación segura, definitiva e irreversible de los datos personales, metadatos y prospectos de terceros alojados por EL CLIENTE en la infraestructura del CRM que HEYLLAVE no tenga obligación legal de resguardo. A partir de la ejecución de dicho borrado, HEYLLAVE quedará liberado de cualquier obligación de custodia, respaldo o conservación sobre dicha información, y no responderá civil ni comercialmente por la pérdida de dichos registros.

6.2. Excepción por Deber de Conservación Legal: Como excepción a la regla de supresión inmediata establecida en el numeral anterior, aquellos datos corporativos, transaccionales, soportes de pago y registros de facturación directa de EL CLIENTE quedarán bloqueados y bajo estricta custodia técnica de HEYLLAVE. Esta retención se mantendrá de forma imperativa única y exclusivamente para dar cumplimiento a los periodos de resguardo exigidos por el artículo 632 del Estatuto Tributario y el artículo 28 de la Ley 962 de 2005. Durante este periodo, la información solo será accesible para atender requerimientos de la Dirección de Impuestos y

Aduanas Nacionales (DIAN) o autoridades judiciales y administrativas competentes. Cumplido el tiempo legal, se procederá a su supresión definitiva.

CLÁUSULA SÉPTIMA. ACUERDO DE CONFIDENCIALIDAD Y SECRETO EMPRESARIAL.

7.1. Las Partes reconocen y acuerdan que toda información técnica, operativa, financiera, comercial, estratégica o relacionada con las bases de datos intercambiada, revelada, generada o puesta a disposición con ocasión de la relación contractual constituye Información Confidencial, independientemente del medio en que se encuentre contenida o de que haya sido identificada expresamente como tal.

Se incluye, de manera enunciativa y no limitativa, la información relativa a las bases de datos, prospectos y metadatos alojados por EL CLIENTE, así como la arquitectura de software, algoritmos, código objeto, know-how, credenciales técnicas, API Keys, esquemas de precios personalizados, manuales técnicos y demás información interna de HEYLLAVE.

Sin perjuicio de su carácter confidencial, aquella información que, por su naturaleza, contenido, valor comercial, nivel de reserva y medidas razonables adoptadas para mantenerla en secreto, reúna los requisitos establecidos en la legislación aplicable podrá constituir secreto empresarial y gozará, además, de la protección correspondiente bajo la Decisión 486 de 2000 de la Comunidad Andina y demás normas aplicables.

7.2. La Parte Receptora se obliga a mantener la más estricta confidencialidad sobre la información suministrada por la Parte Reveladora. La Información Confidencial no podrá ser reproducida, divulgada, copiada, comercializada, licenciada ni transmitida a terceros ajenos a este Acuerdo sin autorización previa y por escrito. El acceso a la Información Confidencial quedará restringido de forma exclusiva al personal laboral, directivo o a los Sub-Encargados tecnológicos que estrictamente requieran conocerla para la ejecución del servicio (principio de privilegio mínimo), garantizando que estos se encuentren previamente vinculados por acuerdos de confidencialidad de rigor equivalente.

7.3. La obligación de confidencialidad no será aplicable sobre aquella información que:

a) Sea de dominio público al momento de su revelación o pase a serlo con posterioridad, sin mediar incumplimiento o dolo de la Parte Receptora.

- b) Ya estuviera en posesión legítima y demostrable de la Parte Receptora antes de su divulgación por la Parte Reveladora.
- c) Sea desarrollada de forma legítima e independiente por la Parte Receptora sin recurrir a la Información Confidencial.
- d) Deba ser revelada por orden imperativa de una autoridad judicial, administrativa o de inspección y vigilancia competente. En este escenario, la Parte Receptora deberá notificar a la Parte Reveladora de forma inmediata y previa a la divulgación, en la medida en que la ley lo permita, para que esta última pueda ejercer las acciones de protección de su Información Confidencial y, cuando corresponda, de su secreto empresarial.

7.4. Las obligaciones de confidencialidad, reserva y no divulgación aquí pactadas no se extinguirán con la terminación de la Licencia de Uso o del plan de suscripción. Estas obligaciones subsistirán y serán exigibles por un término de cinco (5) años contados a partir de la terminación definitiva de la relación comercial por cualquier causa. Tratándose de datos personales, código fuente, algoritmos, arquitectura tecnológica, know-how, secretos empresariales y demás información cuya naturaleza requiera mantener un nivel permanente de reserva, la obligación de confidencialidad tendrá carácter indefinido, siempre que dicha información conserve su carácter reservado o secreto.