POLÍTICA DE PRIVACIDAD Y TRATAMIENTO DE DATOS PERSONALES

Alcance: La presente política de privacidad es un documento vinculante para CORNERSTONE GLOBAL PARTNERS COLOMBIA S.A.S, quien en adelante se conocerá como el responsable del tratamiento de información, en los términos de la Ley 1581 de 2012.

Datos del responsable: CORNERSTONE GLOBAL PARTNERS COLOMBIA S.A.S, identificada con el NIT 901805175-4, con domicilio principal en la ciudad de Bogotá, en la Calle 128 B # 78-90, Casa 34, comunicación a través de la línea de atención 3173598700, o al correo electrónico legal@cgpgroupus.com

Información que recolectamos y almacenamos de nuestros clientes, colaboradores y proveedores: dependiendo de la relación que el titular tenga con El Responsable, la información que se recopila o almacena puede incluir lo siguiente:

- **Datos públicos:** es el dato que no sea privado o sensible. Por ejemplo: número y tipo de documento de identidad, información contenida en documentos públicos, estado civil, oficio o profesión, teléfono y correo electrónico corporativos.

- **Datos privados:** son aquellos que por su naturaleza íntima o reservada sólo son relevantes para el titular. Por ejemplo: nivel de ingresos, datos financieros, capacidad de endeudamiento, patrimonio bruto, personas a cargo, composición del grupo familiar, hobbies o aficiones, bienes que posee, información laboral, preferencias en redes sociales, hábitos de consumo, así como datos de contacto como dirección, teléfono y correo electrónico personal.

- **Datos sensibles**: es la categoría de datos personales más íntima y sensible para su titular, cuyo tratamiento inadecuado, puede conllevar a la discriminación y/o al sufrimiento de un perjuicio grave y de difícil reparación. Por ejemplo: datos biométricos, datos de salud, orientación sexual, creencias religiosas, pertenencia a sindicatos, entre otras. En esta categoría se incluyen los datos de menores de edad, por ser considerados de especial protección.

Tratamiento al cual serán sometidos los datos personales: El Responsable usará la información personal de sus clientes, colaboradores y proveedores para los fines autorizados e informados al titular y aquellos señalados en la presente política, además de los que sean autorizados expresamente por la normatividad.

La autorización de tratamiento de datos sensibles es facultativa, y así se le hará saber al titular al momento de la recolección de la autorización.

Finalidades con las cuales serán tratados los datos: con el objetivo de obtener un mejor servicio para clientes, colaboradores o proveedores, El Responsable realizará el tratamiento de los datos personales recolectados, puntalmente para las siguientes actividades:

Finalidades inherentes al objeto contractual o autorizadas por normatividad.

1. Consultar y reportar datos del comportamiento crediticio y financiero con centrales de información y de riesgos para evaluar las posibilidades de contratación y para informar sobre el cumplimiento o no de obligaciones.
2. Compartir información con los proveedores autorizados, para la coordinación de un servicio o solicitud, con las limitaciones y reglas de la presente política.

3. Realizar control y prevención de fraudes y lavado de activos.
4. Efectuar consultas en centrales de riesgos, bases de datos públicas, listas restrictivas, y contactar referencias, a fin de corroborar la información proporcionada por el titular.
5. Realizar evaluaciones sobre la calidad de los productos y servicios ofrecidos.
6. Gestionar la atención y soporte a clientes, usuarios y prospectos a través de llamadas, canales digitales y otros medios de contacto, incluyendo la grabación y monitoreo para control de calidad y cumplimiento contractual.
7. Realizar las actividades administrativas o comerciales inherentes a la relación contractual y a la prestación de los servicios contratados con los clientes.
8. Gestionar campañas de comunicación, encuestas de satisfacción, análisis de riesgo y manejo de trámites, quejas y reclamos en nombre de los clientes del call center
9. Gestionar y procesar datos personales para facilitar la búsqueda y colocación laboral, tanto de oferentes (candidatos) como de demandantes de empleo (empresas), en cumplimiento de las funciones de consultoría laboral.
10. Ejecutar análisis estadísticos, elaborar informes y reportes según sea requerido contractualmente.
11. Atender solicitudes, quejas, reclamos y encuestas de satisfacción relacionadas con los servicios requeridos contractualmente.
12. Gestionar la información necesaria para diseñar, desarrollar, implementar, mantener y actualizar sitios web, aplicaciones y soluciones tecnológicas bajo parámetros de privacidad desde el diseño y minimización de datos, conforme a las instrucciones del cliente y la normativa aplicable.
13. Procesar datos relacionados con pruebas, soporte y mantenimiento de las soluciones entregadas a los clientes, garantizando la integridad, confidencialidad y disponibilidad de los datos

<u>Finalidades inherentes al funcionamiento del Responsable</u>

1. Tratar los datos de colaboradores, empleados o aspirantes para efecto de su vinculación con El Responsable, el desempeño de sus funciones o la prestación de sus servicios, el retiro o su terminación. Este tratamiento incluye, entre otros: proceso de selección y actividades vinculantes, planes de desarrollo, reconocimiento y pago de beneficios legales y extralegales, comunicaciones internas y externas, procesamiento de información en diferentes aplicativos tecnológicos instalados en servidores de la compañía o en la nube, compensación.
2. Realizar los pagos y afiliaciones al Sistema General de Seguridad Social Integral de los colaboradores.
3. Adelantar procesos de transcripción y cobro de incapacidad o licencia ante las entidades del Sistema General de Seguridad Social Integral, como la verificación de su autenticidad.
4. Dar cumplimiento a las exigencias normativas en materia laboral, de seguridad social, riesgos profesionales y cualquier otra obligación del Responsable derivada de los Contratos de Trabajo
5. Efectuar consultas en centrales de riesgos, bases de datos públicas, listas restrictivas, y contactar referencias, a fin de corroborar la información proporcionada por el titular.
6. Tratar datos de salud, que son sensibles, por parte del área de Seguridad y Salud en el Trabajo del Responsable, para prevenir enfermedades o accidentes de origen laboral, gestionar de forma adecuada la exposición a los riesgos comunes y laborales que puedan afectar mi salud, bienestar y calidad de vida o determinar las condiciones que puedan afectar mi desempeño, así como monitorear las actividades propias del Sistema de Gestión de Seguridad y Salud en el Trabajo, y participar en el trámite de calificación de origen y pérdida de capacidad laboral.
7. Tratar los datos para la vigilancia y seguridad de las personas, los bienes e instalaciones del Responsable, pudiendo desarrollarse a través de captura de imágenes, video y/o audio en sistemas de video vigilancia y utilizar dicha información en diferentes procesos y procedimientos laborales, disciplinarios, penales y administrativos, tales como, investigación para fraudes, prevención del mismo y/o procesos sancionatorios.

8. Emplear y divulgar su imagen, voz, y/o fotografías durante los eventos, programas, publicidad, y boletines realizados por el Responsable
9. Realizar control y prevención de fraudes y lavado de activos.
10. Entregar informes a entidades como las que, a manera enunciativa, se detallan a continuación: DIAN, DANE, SENA, ICBF, UGPP, Superintendencias, Juzgados, Fiscalía, Cooperativas, Cajas de Compensación, ARL, entre otras.

Otras finalidades.

1. Ser contactado para la entrega de ofertas comerciales e información publicitaria relacionada con los productos y servicios del Responsable o sus aliados comerciales.
2. Usar su nombre como referencia de los servicios prestados por el Responsable.
3. La elaboración de encuestas (comerciales, académicas, o de cualquier otra clase) y en general cualquier estudio técnico o de campo relacionado directa o indirectamente con el Responsable
4. Transmitir o transferir datos a terceros con los cuales se tengan alianzas o convenios, con la finalidad de ofrecer servicios comerciales por parte de estos al Titular.

Derechos de los titulares: de acuerdo con lo establecido en la Ley 1581 de 2012, los titulares tienen derecho a autorizar el tratamiento de sus datos personales, conocer los datos que son tratados, actualizarlos, rectificarlos cuando se considere que existe deficiencia en su calidad, solicitar su supresión, y revocar la autorización siempre y cuando no exista una obligación legal o contractual de continuar con el tratamiento (artículo 2.2.2.25.2.8 Decreto 1074 de 2015), por ejemplo en el caso de las finalidades que son inherentes al objeto contratado y sin las cuales no es posible su ejecución o las inherentes al funcionamiento del Responsable.

Ejercicio de los derechos sobre los datos personales: los titulares de la información podrán ejercer sus derechos en cualquier tiempo, para lo cual podrán enviar un correo electrónico a legal@cgpgroupus.com

Entrega de información personal a proveedores de servicios: es posible que para cumplir con la relación contractual que el Responsable sostenga con el titular de la información, esta sea entregada o compartida mediante transmisión con proveedores para las finalidades autorizadas por el titular o las previstas en la ley, para llevar a cabo el objeto social del Responsable y prestar correctamente la atención. Siempre que su información sea entregada o compartida con proveedores, El Responsable se asegurará de establecer unas condiciones que vinculen al proveedor a sus políticas de privacidad, y así mismo, se establecerán acuerdos de confidencialidad para el manejo de la información y obligaciones responsable-encargado cuando el tipo de entrega lo requiera.

Aceptación de esta política: el Titular de la información acepta el tratamiento de sus datos personales, conforme con los términos de esta política de privacidad, cuando proporciona los datos a través de nuestros canales o puntos de atención y cuando compra, adquiere, se afilia o usa cualquiera de nuestros productos o servicios.

Vigencia del tratamiento de los datos: la información suministrada por los titulares permanecerá almacenada por el tiempo que sea necesario para el cumplimiento de los fines para los cuales fue incorporada, y en todo caso obedecerá a los tiempos de disposición final del ciclo de vida del dato definido por el Responsable de acuerdo con el tipo de finalidad del Titular.

Entrada en Vigor. La presente Política rige a partir de su publicación, dada el 3 de Diciembre del 2025

PRIVACY POLICY AND PERSONAL DATA PROCESSING POLICY

Scope: This privacy policy is a binding document for CORNERSTONE GLOBAL PARTNERS COLOMBIA S.A.S, hereinafter referred to as the data controller, under the terms of Law 1581 of 2012.

Controller information: CORNERSTONE GLOBAL PARTNERS COLOMBIA S.A.S, identified with NIT 901805175-4, with its main address in Bogotá at Calle 128 B # 78-90, Casa 34, can be contacted through the customer service line 3173598700, or via email at legal@cgpgroupus.com.

Information collected and stored from our clients, employees, and suppliers: Depending on the relationship the data subject has with the Controller, the information collected or stored may include the following:

- **Public data:** data that is neither private nor sensitive. For example: identification document number and type, information contained in public documents, marital status, occupation or profession, corporate phone number, and corporate email address.
- **Private data:** data that, by its intimate or reserved nature, is only relevant to the data subject. For example: income level, financial data, indebtedness capacity, gross assets, dependents, family group composition, hobbies or interests, owned assets, employment information, social media preferences, consumption habits, as well as contact details such as home address, personal phone number, and personal email address.
- **Sensitive data:** the most intimate and sensitive category of personal data for its holder, whose mishandling may lead to discrimination and/or serious, hard-to-repair harm. For example: biometric data, health data, sexual orientation, religious beliefs, union membership, among others. This category includes data of minors, as they are considered especially protected

Processing of personal data: The Controller will use the personal information of its clients, employees, and suppliers for the purposes authorized and informed to the data subject, as well as those specified in this policy, and any other purposes expressly authorized by applicable regulations.

Authorization for processing sensitive data is optional, and this will be made clear to the data subject at the time authorization is collected.

Purposes for which the data will be processed: In order to provide better service to clients, employees, or suppliers, the Controller will process the personal data collected specifically for the following activities:

Purposes inherent to the contractual object or authorized by regulations.

1. To consult and report credit and financial behavior data to information and risk centers in order to assess the possibilities for contracting and to inform about the fulfillment or lack thereof of obligations.

2. To share information with authorized providers, for the coordination of a service or request, within the limitations and rules of this policy.
3. To carry out fraud and money laundering control and prevention.
4. To conduct queries in risk centers, public databases, restrictive lists, and to contact references, in order to corroborate the information provided by the data subject.
5. To conduct evaluations regarding the quality of the products and services offered.
6. To manage the care and support of customers, users, and prospects through calls, digital channels, and other contact methods, including the recording and monitoring thereof for quality control and contractual compliance.
7. To perform administrative or commercial activities inherent to the contractual relationship and the provision of services contracted with clients.
8. To manage communication campaigns, satisfaction surveys, risk analysis, and the handling of procedures, complaints, and claims on behalf of call center clients.
9. To manage and process personal data to facilitate job search and placement, both for applicants (candidates) and job seekers (companies), in compliance with the duties of labor consulting.
10. To carry out statistical analyses, and to prepare reports and statements as contractually required.
11. To address requests, complaints, claims, and satisfaction surveys related to the services contractually required.
12. To manage the information necessary to design, develop, implement, maintain, and update websites, applications, and technological solutions under privacy-by-design and data minimization parameters, according to client instructions and applicable regulations.
13. To process data related to testing, support, and maintenance of solutions delivered to clients, ensuring the integrity, confidentiality, and availability of data.

<u>Purposes inherent to the functioning of the Controller</u>

1. To process the data of collaborators, employees, or applicants for their engagement with the Controller, performance of their duties or services, termination, or withdrawal. This processing includes, among others: the recruitment and associated activities, development plans, recognition and payment of statutory and additional benefits, internal and external communications, processing information in various technological applications installed on company servers or in the cloud, and compensation.
2. To make payments and handle affiliations to the General Social Security System for employees.
3. To carry out transcription and collection processes for disability or leave with the entities of the General Social Security System, including authentication verification.
4. To comply with regulatory requirements regarding labor, social security, professional risks, and any other obligation of the Controller arising from employment contracts.

5. To conduct queries in risk centers, public databases, restrictive lists, and contact references, to corroborate the information provided by the data subject.

6. To process health data, which are sensitive, by the Controller's Occupational Health and Safety area, to prevent occupational diseases or accidents, manage exposure to common and occupational risks that may affect health, well-being, and quality of life, or determine conditions that may impact job performance, as well as to monitor Occupational Health and Safety Management System activities and participate in proceedings related to the origin and loss of work capacity.

7. To process data for surveillance and security of people, property, and facilities of the Controller, which may involve the capture of images, video and/or audio through surveillance systems, and the use of such information in various labor, disciplinary, criminal, and administrative procedures, such as fraud investigations, prevention, and/or sanctioning processes.

8. To use and disclose images, voice, and/or photographs during events, programs, advertising, and bulletins conducted by the Controller.

9. To carry out fraud and money laundering control and prevention.

10. To deliver reports to entities such as, but not limited to: DIAN, DANE, SENA, ICBF, UGPP, Superintendencies, Courts, Prosecutor's Office, Cooperatives, Compensation Funds, Occupational Risk Administrators, among others.

Other purposes

1. To be contacted for the delivery of commercial offers and advertising information related to the Controller’s products and services or those of its business partners.

2. To use your name as a reference for the services provided by the Controller.

3. To conduct surveys (commercial, academic, or of any other kind) and, in general, any technical or field study directly or indirectly related to the Controller.

4. To transmit or transfer data to third parties with whom alliances or agreements exist, for the purpose of offering commercial services by those third parties to the Data Subject.

Exercise of Rights over Personal Data: Data subjects may exercise their rights at any time by sending an email to legal@cgpgroupus.com.

Disclosure of Personal Information to Service Providers: To fulfill the contractual relationship that the Controller has with the data subject, their information may be disclosed or shared with service providers through transmission for the purposes authorized by the data subject or by law, to fulfill the Controller’s corporate purpose and to provide adequate customer service. Whenever information is disclosed or shared with providers, the Controller will ensure that the provider is bound to its privacy policies. Confidentiality agreements for the handling of information and data controller-processor obligations will also be established when required by the type of transmission

Acceptance of this Policy: The Data Subject accepts the processing of their personal data, in accordance with the terms of this privacy policy, when providing their data through our service channels or contact points, and when purchasing, acquiring, enrolling in, or using any of our products or services.

Validity of Data Processing: The information provided by data subjects will remain stored for as long as necessary to fulfill the purposes for which it was collected, and in any case, will be subject to

the data life cycle and final disposition periods defined by the Controller, in accordance with the data subject's type of purpose.

Effective Date: This Policy shall enter into force as of its publication on December 3rd, 2025.

MANUAL DE PROTECCIÓN DE DATOS PERSONALES

En el desarrollo de sus operaciones, el Responsable se compromete a adoptar un manual para el tratamiento de los datos personales, con el propósito de proteger la información personal obtenida de sus clientes, colaboradores y proveedores a través de sus distintos canales de comercialización y contacto.

El presente manual se regirá por las siguientes condiciones:

Objetivo y ámbito de aplicación.

El objetivo del presente manual es establecer los procedimientos a tener en cuenta en el manejo de los datos de carácter personal almacenados por el Responsable.

El presente manual es aplicable a los datos personales almacenados tanto en forma digital como física, los cuales hayan sido capturados o adquiridos por parte del Responsable.

El Responsable del tratamiento es CORNERSTONE GLOBAL PARTNERS COLOMBIA S.A.S, identificada con el NIT 901805175-4, domiciliado en la ciudad de Bogotá, Colombia, cuyo canal de contacto es el correo electrónico legal@cgpgroupus.com

Definiciones.

De acuerdo con lo establecido en la ley 1581 de 2012, para efectos de establecer las políticas, procedimientos, estándares y otras consideraciones sobre el tratamiento de datos personales, se tendrán en cuenta las siguientes definiciones:

a) **Autorización:** consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales;
b) **Dato personal**: cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables;
c) **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.
d) **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;
e) **Titular:** persona natural cuyos datos personales sean objeto de Tratamiento;
f) **Tratamiento:** cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

Principios rectores del tratamiento de datos personales.

Dentro del compromiso legal y corporativo del Responsable para garantizar la confidencialidad de la información personal tratada, se establecen como principios generales para el tratamiento de la información, en desarrollo de los ya presentes en la Ley 1581 del 2012 y el capítulo 25 del Decreto 1074 de 2015, y demás normas aplicables, los siguientes:

a) **Principio de legalidad:** no habrá tratamiento de información personal de los Titulares sin observar las reglas establecidas en la normatividad vigente.
b) **Principio de finalidad:** la incorporación de datos deberá obedecer a una finalidad legítima, la cual será oportunamente informada al titular en la cláusula de autorización para el tratamiento y en la política de privacidad.
c) **Principio de libertad:** el Responsable realizará tratamiento de datos personales de clientes, colaboradores y proveedores cuando cuente con la autorización de estos o cuando por norma exista una facultad para hacerlo, en los términos del art. 3° literal a) y 6° literal a) de la Ley 1581 del 2012, así como la sección II del capítulo 25 del Decreto 1074 de 2015.
d) **Principio de veracidad y calidad:** el Responsable propenderá porque la información de los Titulares sea veraz y se encuentre actualizada, para lo cual dispondrá de medios eficientes para la actualización y rectificación de los datos personales
e) **Principio de transparencia:** dentro de los mecanismos que se establezcan para el ejercicio de los derechos de los titulares de la información personal, se garantizará al titular y a sus causahabientes, así como a los terceros autorizados por este, el acceso a la información sobre datos personales que le conciernan.
f) **Principio de acceso y circulación restringida:** el Responsable se compromete a garantizar que únicamente personas autorizadas podrán acceder a la información personal. Asimismo, su circulación se limitará al ejercicio de las finalidades autorizadas por el Titular o por la normatividad. Se dispondrán de medios contractuales para garantizar la confidencialidad y circulación restringida de la información.
g) **Principio de seguridad:** el Responsable adelantará todas las medidas técnicas, administrativas y humanas para garantizar que la información personal de los titulares, almacenada de forma física o digital, no circule a personas no autorizadas accedan a ella.
h) **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, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la ley y en los términos de la misma.

Lineamientos generales.

- No se podrá utilizar información de datos personales de los afiliados, empleados o proveedores para fines diferentes al objeto del contrato, a menos que se cuente con una autorización expresa para ello.
- Antes de capturar un dato personal privado o sensible, se debe solicitar el diligenciamiento de la autorización para el tratamiento de datos personales.
- En ningún caso es aceptable que se tenga pre diligenciada la autorización de tratamiento de datos personales, es decir, previamente marcada en Sí, pues ello equivaldría a tomar el silencio o inactividad como una aceptación.

Ciclo de vida del dato personal.
El Responsable del tratamiento garantizará el ciclo de vida del dato de acuerdo con las siguientes etapas:

1. **Recolección**: corresponde a la etapa en la cual se obtienen los datos personales de los Titulares, momento en el cual se solicitará la autorización respectiva, la cual puede darse por los siguientes medios:

    - **Física:** cuando los datos son entregados en formularios o documentos (incluyendo digitales) entregados al Responsable, en cuyo caso la autorización será física y se conservará en ese medio o de forma digital.

    - **Verbal:** cuando los datos son entregados mediante llamadas al Responsable, en cuyo caso la autorización puede capturarse mediante grabación o de forma física/digital.

    - **Conductas inequívocas:** cuando el Titular despliega acciones que permiten entender que autoriza el tratamiento, como es el caso de videovigilancia, cuando se puede observar un aviso de filmación por motivos de seguridad y el Titular decide entrar al lugar. En ningún caso se entenderá el solo silencio como autorización, y se requerirán actos positivos (entrar al lugar) para considerar autorizado el tratamiento.

2. **Almacenamiento**: corresponde a la conservación física o digital de la información. En ambos casos debe realizarse bajo medidas de seguridad.

    - Para el caso de almacenamiento físico, se dispondrán de carpetas individualizadas por Titular y ordenadas por orden alfabético o clasificadas de acuerdo a su criticidad, donde se recopilarán los documentos. Las carpetas serán custodiadas en bodegas o archivadores protegidos de elementos naturales (lluvia, fuego, polvo, etc.) que puedan afectar su disponibilidad, y sólo podrán ser consultados por personal autorizado, para lo cual se utilizarán medidas de seguridad (claves, candados, barreras físicas).

    - Para el caso de almacenamiento digital, se dispondrán de los archivos por Titular (comprimidos o no) en medios locales o mediante almacenamiento en nube. Tanto en almacenamiento local como en nube se dispondrá de un medio de respaldo para recuperar información en caso de pérdida, y su seguridad se garantizará mediante el uso de usuarios y claves de acceso, además de medidas de ciberseguridad (antivirus, antimalware, cortafuegos, etc.).

    - Para el caso de datos personales de videovigilancia, el Responsable definirá el tiempo por el cual conservará las grabaciones, así como el medio de conservación digital (en nube o medio local) o física (en citas), atendiendo a los criterios mencionados arriba.

3. **Uso:** corresponde a la utilización de los datos por parte del Responsable, el cual se sujetará exclusivamente a las finalidades autorizadas por el Titular, o aquellas que sean autorizadas por la normativa vigente.

4. **Disposición final:** Corresponde al proceso de eliminación de los datos personales. Para ello se utilizarán medios idóneos tanto en físico (destrucción del papel) como digital (eliminación permanente de archivos), sin posibilidad de contar con respaldo. La disposición final obedecerá al cumplimiento del tiempo de conservación, establecido así:

    - Para clientes y proveedores se conservará durante la ejecución del contrato y hasta por 5 años adicionales, para cubrir eventos de responsabilidad civil contractual donde sea necesario utilizar los datos personales en defensa jurídica del Responsable.

    - Para colaboradores se conservará durante la ejecución del contrato. La historia laboral se conservará hasta por 80 años, de acuerdo con la recomendación del Archivo General de la República. Los documentos del Sistema de Gestión de Seguridad y Salud en el Trabajo se conservarán hasta por 20 años, contados a partir del momento en que se termine la relación laboral, de acuerdo con el artículo 2.2.4.6.13 del Decreto 1072 de 2015.

Autorización para el tratamiento de datos personales.

Cuando a través de cualquier operación se incorporen datos de personas naturales, se pondrá a disposición del titular una cláusula de autorización para el tratamiento de datos personales, la cual deberá contener como mínimo lo siguiente (artículo 12 Ley 1581 de 2012):

- La finalidad para la cual autoriza el tratamiento de sus datos.
- El tratamiento o tratamientos que autoriza al responsable del tratamiento de los datos personales.
- La indicación del responsable del tratamiento de la información.
- La indicación que señale que la respuesta a las preguntas es facultativa cuando se trate de autorización para el tratamiento de datos sensibles o de niños y adolescentes.
- Los derechos que le asisten al titular de los datos personales.
- Los canales de comunicación puestos a disposición por la compañía para la atención de los derechos de las personas.
- Los formatos de autorización no pueden estar llenados previamente con aceptación, pues el silencio de una persona no puede entenderse como afirmación, debe existir una expresión que permita entender que efectivamente se aceptó. La autorización para tratamiento de estos datos puede ser escrita, verbal o por medio de actos inequívocos (que permitan concluir que se autorizó).

Ejercicio de los derechos sobre los datos personales.

Los titulares de la información podrán, en cualquier tiempo ejercer los derechos consagrados en la ley 1581 de 2012 de conocer, actualizar y rectificar sus datos personales, solicitar prueba de la autorización otorgada para el tratamiento, informarse sobre el uso que se ha dado a los datos, revocar la autorización, solicitar la supresión de sus datos cuando sea procedente y acceder en forma gratuita a los mismos.

Para el ejercicio de los derechos, el Titular podrá comunicarse a través del correo electrónico legal@cgpgroupus.com

Se debe diferenciar si se trata de una consulta o un reclamo, pues tienen tiempos de respuesta distintos como se detalla a continuación:

Tipo	Término
Consultas: solicitud de los datos del titular que tiene la compañía y/o copia de la autorización de tratamiento de datos.	Para consultas 10 días hábiles, prorrogables hasta por 5 días más (art. 14 Ley 1581 de 2012).
Reclamos: actualización, rectificación, revocación de la autorización de tratamiento, supresión de datos, o queja por presunto incumplimiento en el tratamiento.	Para reclamos 15 días hábiles, prorrogables hasta por 8 días más (art. 15 Ley 1581 de 2012).

Tras revisar la solicitud del Titular, el Responsable debe proceder a activar a las áreas respectivas para generar una respuesta, o adelantar la investigación correspondiente. Una vez se tengan los resultados de la investigación o se encuentre la información solicitada por el titular, se debe elaborar una respuesta, y actuando dentro de los términos legales, se debe enviar al solicitante por el medio que este hubiese solicitado o, si no lo aclaró, al que sea más expedito.

Supresión de datos personales.

El Titular podrá solicitar la supresión del dato y revocar la autorización en todos los casos, salvo cuando exista un deber legal o contractual que le imponga el deber de permanecer en la base de datos o archivo del responsable o encargado. Para ello se tendrá en cuenta lo siguiente:

a) Que los datos personales no estén siendo tratados conforme a los principios, deberes y obligaciones previstas en la normatividad vigente sobre Protección de Datos Personales.
b) Que hayan dejado de ser necesarios o pertinentes para la finalidad para la cual fueron recabados.
c) Que se haya superado el periodo necesario para el cumplimiento de los fines para los que fueron recogidos.

Cuando el Titular informe que el dato que se tiene es inexacto (por ejemplo, un número de celular que pertenece a otra persona), se podrá proceder con la supresión del mismo, pese a que exista relación contractual vigente, ya que se trata de un dato que carece de calidad.

Esta supresión implica la eliminación o borrado seguro, total o parcial, de la información personal de acuerdo con lo solicitado por el Titular en los registros, archivos, bases de datos o tratamientos realizados por el Responsable.

La vía para solicitar la supresión de datos personales será gratuita y será la misma definida para la presentación de reclamos. En caso de resultar procedente la supresión de los datos personales, el Responsable realizará operativamente la supresión de los mismos; en caso de que no sea procedente la supresión, se informará al Titular.

Entrada en vigencia.

El presente manual empezará a regir a partir del 3 de Diciembre del 2025.

PERSONAL DATA PROTECTION MANUAL

In the course of its operations, the Controller undertakes to adopt a manual for the processing of personal data, with the purpose of protecting the personal information obtained from its clients, collaborators, and suppliers through its various marketing and contact channels.

This manual shall be governed by the following conditions:

Objective and Scope of Application

The objective of this manual is to establish the procedures to be observed in the handling of personal data stored by the Controller.

This manual applies to personal data stored both digitally and physically, which have been captured or acquired by the Controller.

The Controller is CORNERSTONE GLOBAL PARTNERS COLOMBIA S.A.S, identified with NIT 901805175-4, domiciled in the city of Bogotá, Colombia, whose contact channel is the email address legal@cgpgroupus.com

Definitions

In accordance with Law 1581 of 2012, and for purposes of establishing policies, procedures, standards, and other considerations regarding the processing of personal data, the following definitions apply:

a) **Authorization**: Prior, express, and informed consent of the Data Subject to carry out the Processing of personal data;
b) **Personal data:** Any information linked or that can be associated with one or more identified or identifiable natural persons;
c) **Data Processor**: Natural or legal person, public or private, who by themselves or in association with others, processes personal data on behalf of the Data Controller;
d) **Data Controller:** Natural or legal person, public or private, who by themselves or in association with others, decides on the database and/or the Processing of the data;
e) **Data Subject:** Natural person whose personal data is subject to Processing;
f) **Processing:** Any operation or set of operations on personal data, such as collection, storage, use, circulation, or deletion.

Guiding Principles for the Processing of Personal Data

As part of the Controller's legal and corporate commitment to ensure the confidentiality of processed personal information, the following are established as general principles for data processing, in development of those already contained in Law 1581 of 2012, Chapter 25 of Decree 1074 of 2015, and other applicable regulations:

a) **Principle of Legality:** There shall be no processing of personal information of Data Subjects without observing the rules established in current regulations.

b) **Principle of Purpose:** The incorporation of data must have a legitimate purpose, which will be duly informed to the data subject in the authorization clause for processing and in the privacy policy.
c) **Principle of Freedom:** The Controller will process personal data of clients, collaborators, and suppliers only when authorization has been obtained from them or when authorized by law, under the terms of Article 3(a) and Article 6(a) of Law 1581 of 2012, as well as Section II, Chapter 25 of Decree 1074 of 2015.
d) **Principle of Truthfulness and Quality:** The Controller will ensure that the information of Data Subjects is truthful and updated, providing efficient means for the updating and rectification of personal data.
e) **Principle of Transparency:** Among the mechanisms established for the exercise of rights of data subjects, access to information about their personal data will be guaranteed to the data subject, their successors, and third parties authorized by the data subject
f) Principle of Access and Restricted Circulation: The Controller is committed to ensuring that only authorized individuals may access personal information. Likewise, its circulation will be limited to the purposes authorized by the Data Subject or by law. Contractual means shall be implemented to guarantee the confidentiality and restricted circulation of the information.
g) Principle of Security: The Controller will undertake all technical, administrative, and human measures to ensure that the personal information of data subjects, whether stored physically or digitally, is not accessed or circulated by unauthorized persons.
h) Principle of Confidentiality: All persons involved in the processing of personal data that is not public in nature are obligated to guarantee the confidentiality of the information, even after their relationship with any of the activities comprising the processing has ended, and may only supply or communicate personal data when this is consistent with activities authorized by law and under its terms

General Guidelines

- Personal data of members, employees, or suppliers may not be used for purposes other than those of the contract, unless express authorization is obtained for such purposes.
- Before capturing private or sensitive personal data, the completion of the authorization for data processing must be requested.
- Under no circumstances is it acceptable to have a pre-completed data processing authorization, that is, previously marked as "Yes," since this would amount to taking silence or inactivity as acceptance.

Personal Data Life Cycle

The Data Controller shall guarantee the life cycle of the data in accordance with the following stages:

1. **Collection:** This refers to the stage in which personal data is obtained from the Data Subjects, at which point the respective authorization will be requested, which may be obtained by the following means:

    - **Physical:** When the data is provided through forms or documents (including digital forms) submitted to the Controller, in which case the authorization will be physical and will be kept in that medium or digitally.

    - **Verbal:** When the data is provided verbally through calls to the Controller, in which case the authorization may be recorded or stored physically/digitally.

- **Unequivocal Conduct:** When the Data Subject engages in actions that permit an understanding that they authorize processing, such as video surveillance, where a notice of filming for security reasons is visible and the Data Subject decides to enter the premises. In no case shall silence be construed as authorization; positive actions (such as entering the premises) are required to consider processing as authorized

2. **Storage:** This refers to the physical or digital preservation of information. In both cases, it must be managed under security measures.

    - In the case of physical storage, individualized folders shall be kept for each Data Subject and organized alphabetically or classified according to criticality, where documents are compiled. The folders will be stored in warehouses or cabinets protected from natural elements (rain, fire, dust, etc.) that might affect availability, and only authorized personnel may consult them, for which security measures (passwords, locks, physical barriers) will be used.

    - In the case of digital storage, files for each Data Subject (compressed or not) will be stored on local media or via cloud storage. Both local and cloud storage will include a backup method to recover information in the event of data loss, and security will be ensured by using user accounts and passwords, in addition to cybersecurity measures (antivirus, antimalware, firewalls, etc.).

    - In the case of personal data collected through video surveillance, the Controller will define the retention period for the recordings as well as the digital (cloud or local) or physical (on tapes) storage medium, in line with the criteria described above

3. **Use:** This refers to the use of data by the Controller, which shall be strictly limited to the purposes authorized by the Data Subject, or those authorized by current regulations.

4. **Final disposition**: This corresponds to the process of eliminating personal data. Suitable means shall be used both physically (paper destruction) and digitally (permanent deletion of files), with no backups retained. Final disposition will comply with the retention periods established as follows:

    - For clients and suppliers, data will be retained for the duration of the contract and up to 5 additional years, to cover potential contractual civil liability events in which personal data may be necessary for the legal defense of the Controller.

    - For employees, data will be retained during the duration of the contract. Employment history will be retained for up to 80 years, in accordance with the recommendation of the National General Archive. Occupational Health and Safety Management System documents will be retained for up to 20 years, counted from the end of the employment relationship, as established in Article 2.2.4.6.13 of Decree 1072 of 2015.

Authorization for the Processing of Personal Data

Whenever, through any operation, the data of natural persons is incorporated, an authorization clause for the processing of personal data shall be presented to the data subject, which must contain at a minimum the following (Article 12 of Law 1581 of 2012):

- The purpose for which the processing of their data is authorized.

- The processing or process(es) authorized for the data by the data controller.
- Identification of the data controller.
- An indication stating that answering the questions is optional when the authorization concerns the processing of sensitive data or of children and adolescents.
- The rights available to the data subject.
- The communication channels made available by the company for the exercise of data subject rights.
- Authorization forms may not be pre-filled with acceptance, as silence cannot be construed as affirmation; there must be an explicit expression making clear that acceptance has been granted. Authorization for processing these data may be given in written, verbal, or unequivocal acts (that allow a conclusion that authorization has been granted).

Exercise of Rights Regarding Personal Data

Data subjects may, at any time, exercise the rights established under Law 1581 of 2012: to access, update, and rectify their personal data; to request proof of the authorization granted for processing; to be informed of the use given to their data; to revoke authorization; to request the deletion of their data where appropriate; and to access their data free of charge.
To exercise these rights, the Data Subject may contact the Controller via email at legal@cgpgroupus.com.

A distinction must be made between an inquiry and a complaint, as each has different response times, detailed below

Type	Term
Inquiries: Requests for the data held by the company on the data subject and/or a copy of the authorization for data processing.	10 business days, extendable for up to 5 additional days (Art. 14, Law 1581 of 2012).
Claims: Updates, corrections, revocation of processing authorization, deletion of data, or complaints for alleged noncompliance in processing.	15 business days, extendable for up to 8 additional days (Art. 15, Law 1581 of 2012).

Upon reviewing the Data Subject's request, the Controller must proceed to activate the corresponding departments to generate a response or to carry out the corresponding investigation. Once the results of the investigation are obtained or the requested information is located, a response must be prepared. Acting within the legal time frames, the response must be sent to the requester through the means they indicated or, if not specified, through the most expedient channel.

Deletion of Personal Data

The Data Subject may request the deletion of their data and revoke their authorization in all cases, except when a legal or contractual obligation requires the data to remain in the Controller's or Processor's database or records. The following criteria will be considered:

a) The personal data is not being processed in accordance with the principles, duties, and obligations provided by current data protection regulations.
b) The data is no longer necessary or relevant for the purpose for which it was collected.

c) The period necessary for meeting the purposes for which the data was collected has been exceeded.

If the Data Subject reports that the data on file is inaccurate (for example, a cell phone number actually belongs to another person), the data may be deleted even if a contractual relationship is ongoing, since it constitutes poor-quality data.

Such deletion implies the secure, total or partial removal of personal information in accordance with the Data Subject's request, from the records, files, databases, or processes managed by the Controller.

The procedure for requesting the deletion of personal data will be free of charge and will follow the same channel defined for the submission of claims. If the deletion of personal data is warranted, the Controller will carry out the operational deletion of the data; if deletion is not appropriate, the Data Subject will be informed.

Effective Date

This manual shall enter into force as of December 3rd, 2025.