Política de tratamiento de datos personales

Políticas corporativas

POL DP 001 • Versión 2.0 • 13 de octubre de 2026

Esta política explica cómo Hummingbird Consulting S.A.S. trata los datos personales en su actividad de software y consultoría, cómo atiende los derechos de sus titulares y cómo distribuye responsabilidades cuando presta servicios a otras organizaciones. Comprende los canales físicos y digitales de HMB, el sitio hmb-sas.com, sus subdominios y HMB Risk Manager.

1 Identificación y atención al titular

HUMMINGBIRD CONSULTING S.A.S., NIT 901.902.294-8, tiene domicilio en Medellín, Colombia. Dirección de contacto: Avenida 80 No. 28-90. Correo: administracion@hmb-sas.com. Teléfono: +57 322 528 5544. Sitio: https://hmb-sas.com.

La representación legal asume la función de protección de datos y coordina la atención de consultas y reclamos. El titular puede presentar su solicitud por correo o en la dirección física indicada, sin necesidad de contratar un servicio ni de utilizar la Línea Transparente.

2 Alcance y marco jurídico

La política se fundamenta en el artículo 15 de la Constitución Política, la Ley 1581 de 2012 y el capítulo 25 del título 2 de la parte 2 del libro 2 del Decreto 1074 de 2015, además de las normas e instrucciones que resulten aplicables. Los tratamientos sujetos a un régimen especial se gestionarán bajo ese régimen.

La disponibilidad de los sitios desde otros países no implica que HMB declare aplicables indistintamente todas las leyes extranjeras. Cuando una operación esté sometida a otra jurisdicción, se determinarán y documentarán las obligaciones adicionales que correspondan.

Dato personal es la información que identifica o permite identificar a una persona natural. El titular es esa persona; el responsable decide las finalidades y condiciones del tratamiento; el encargado trata información por cuenta del responsable. La transmisión comunica datos a un encargado; la transferencia los entrega a otro responsable.

3 Funciones de HMB y de sus clientes

HMB actúa como responsable respecto de sus contactos comerciales, relaciones contractuales, facturación, proveedores, colaboradores, gestión administrativa, atención de derechos y asuntos corporativos propios.

HMB actúa como encargado cuando aloja, organiza, consulta o procesa información por instrucciones de un cliente en HMB Risk Manager, en una consultoría o en un canal de reportes. El cliente determina la finalidad, los usuarios autorizados y los criterios de conservación, y debe acreditar la autorización de los titulares o la excepción legal aplicable.

En una relación de consultoría multiempresa, el cliente debe identificar a cada responsable y acreditar que puede impartir instrucciones sobre sus datos. Si interviene como encargado, debe

contar con autorización suficiente para vincular a HMB como subencargado. La licencia tecnológica no sustituye esas autorizaciones.

El nombramiento de una persona natural como oficial de cumplimiento puede generar deberes legales propios de reserva y reporte. El contrato de servicios no elimina esos deberes ni convierte a HMB en titular de los datos de las personas reportadas.

4 Principios y criterios de tratamiento

HMB aplicará legalidad, finalidad, libertad, veracidad o calidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad. Cada actividad debe tener un propósito definido, utilizar datos pertinentes y permitir demostrar el cumplimiento de las obligaciones.

La información no se considerará pública por el solo hecho de estar disponible en internet. Las coincidencias en listas o fuentes externas deben examinarse en su contexto; no equivalen por sí mismas a una condena ni justifican una decisión automática adversa.

5 Información y finalidades

Contactos y prospectos. HMB puede tratar nombre, organización, cargo y medios de contacto para responder consultas, agendar reuniones, preparar demostraciones y presentar propuestas solicitadas. El envío periódico de publicidad requiere una autorización diferenciada o la habilitación legal que corresponda, y debe permitir retirar la suscripción.

Clientes y usuarios. Trata datos de identificación, contacto, rol, organización, contratación, facturación y uso del servicio para gestionar contratos, habilitar accesos, capacitar, prestar soporte, atender cobros y cumplir obligaciones legales. Los registros de actividad y seguridad se utilizan para administrar accesos, investigar incidentes y mantener la operación.

Proveedores y aliados. Trata los datos necesarios para selección, vinculación, validación de identidad y facultades, conflictos de interés, ejecución de servicios, liquidación de comisiones, pagos y controles proporcionales de integridad.

Colaboradores y candidatos. Cuando exista esta relación, trata la información necesaria para selección, contratación, pagos, obligaciones laborales, seguridad social, formación y seguridad y salud en el trabajo. La conservación de hojas de vida para futuras vacantes requiere informar esa finalidad y obtener la autorización correspondiente.

Consultoría y software. Por cuenta del cliente, puede tratar información de empleados, clientes, proveedores, beneficiarios, terceros, operaciones, riesgos, auditorías, controles y evidencias, dentro de los módulos y servicios contratados. Las categorías y operaciones específicas se documentan en el acuerdo de tratamiento y en las instrucciones del responsable.

Reportes éticos. Trata hechos, fechas, lugares, personas relacionadas, evidencias y medios de contacto voluntarios para recibir, clasificar, verificar, gestionar y documentar posibles irregularidades, adoptar medidas y atender obligaciones legales. Estos datos no se incorporan a campañas comerciales.

Sitios y seguridad. Las direcciones IP, identificadores, registros técnicos, dispositivo y navegación pueden constituir datos personales cuando permiten asociar información a una persona. Su tratamiento se limita a operación, seguridad y a las finalidades opcionales autorizadas. La política de cookies explica los controles del usuario.

6 Autorización y prueba

Antes de recolectar datos que requieran autorización, HMB informará el responsable, las finalidades, los derechos, los canales de atención y el carácter facultativo de los datos sensibles y de menores. Conservará evidencia de la autorización mediante formularios, registros electrónicos u otro medio consultable.

Navegar por un sitio, guardar silencio o aceptar genéricamente los términos no reemplaza una autorización cuando esta sea exigible. La autorización comercial será opcional y separada de la atención de una solicitud o de la prestación del servicio.

Las excepciones legales a la autorización se aplicarán de forma concreta y documentada. Una persona no puede autorizar de manera general el tratamiento de datos de terceros por el solo hecho de cargarlos en el sistema. El responsable debe evaluar la base que permite su tratamiento, especialmente en investigaciones y reportes.

7 Datos sensibles y menores de edad

HMB evitará solicitar datos de salud, vida sexual, orientación política, creencias, origen étnico, biometría u otros datos sensibles que no sean indispensables. Su suministro es facultativo. Cuando se requieran, informará cuáles son y para qué se usarán, solicitará autorización explícita si corresponde y limitará accesos y conservación.

La Línea Transparente no requiere firma manuscrita para presentar un reporte. El reportante debe omitir datos íntimos o sensibles innecesarios y puede evitar identificarse. El suministro de evidencia no autoriza su divulgación indiscriminada.

Los servicios comerciales de HMB no están dirigidos a menores. Si resulta necesario tratar sus datos en un servicio autorizado, se protegerán su interés superior y derechos fundamentales, se verificará la legitimación del representante y se escuchará al menor según su madurez, conforme a las reglas aplicables.

8 Proveedores y circulación de información

HMB puede utilizar proveedores de alojamiento, autenticación, almacenamiento, comunicaciones, facturación y soporte, incluidos GoDaddy y servicios de Google Firebase o Google Cloud según la operación. Cada proveedor recibirá únicamente la información necesaria bajo las condiciones contractuales y de seguridad que correspondan.

El uso de infraestructura en la nube puede implicar procesamiento fuera de Colombia. HMB diferenciará transmisión de transferencia, verificará la ubicación y condiciones del proveedor y formalizará los instrumentos exigibles antes de habilitar el tratamiento. Esta política no constituye autorización ilimitada para enviar datos a cualquier país o tercero.

Los datos de clientes no se usarán para entrenar modelos de inteligencia artificial de uso general ni se remitirán a herramientas de IA ajenas al alcance contratado. La activación de una función de IA que trate datos personales exige evaluar proveedor, finalidad, acceso, conservación y las instrucciones del responsable.

HMB no vende datos personales. Podrá comunicar información a autoridades competentes, asesores sujetos a reserva y otros destinatarios autorizados, cuando exista una finalidad legítima y una habilitación aplicable.

9 Seguridad y acceso

HMB aplicará controles proporcionales de acceso, confidencialidad, copias de seguridad, gestión de cambios, proveedores e incidentes. El personal solo debe acceder a la información que necesita para su función. Las credenciales son individuales y no deben compartirse.

Los accesos técnicos por soporte deben estar autorizados y documentados. Los accesos de emergencia se limitarán a lo necesario para contener una amenaza o recuperar el servicio y se informarán al cliente cuando proceda. Ninguna medida permite prometer ausencia absoluta de incidentes.

10 Conservación y eliminación

HMB conservará los datos durante el tiempo necesario para la finalidad informada, la relación correspondiente y los deberes legales de archivo, atención de reclamaciones y defensa de derechos. No se establece una conservación indefinida por defecto.

Los soportes contractuales, contables y tributarios se conservan durante el término legal aplicable a cada categoría. Los contactos comerciales sin relación vigente se revisarán al menos una vez al año para eliminar o actualizar registros sin finalidad activa. Al retirar una autorización comercial, se suspenderán los envíos y solo se conservará la evidencia mínima necesaria para respetar esa decisión.

Para datos de clientes, la devolución, exportación y eliminación se sujetan al contrato y a sus instrucciones lícitas. Para reportes, se considerarán la investigación, medidas adoptadas y términos de reclamación. Si existe obligación de conservación, se restringirá el uso a esa finalidad.

Los datos en respaldos permanecerán protegidos hasta su rotación conforme al ciclo documentado; no se usarán para reactivar información eliminada. Si un respaldo se restaura, se reaplicarán las solicitudes de supresión que correspondan. La vigencia de cada base se limita a sus finalidades y obligaciones de conservación.

11 Derechos del titular

El titular puede conocer, actualizar y rectificar sus datos, solicitar prueba de la autorización, conocer el uso dado a su información, acceder gratuitamente en los términos legales, solicitar supresión o revocatoria cuando procedan y presentar queja ante la Superintendencia de Industria y Comercio después de agotar el trámite previo exigido.

La eliminación o revocatoria puede limitarse cuando exista un deber legal o contractual de conservación. La respuesta explicará el motivo y el alcance de la restricción. HMB no exige de forma automática una copia completa del documento de identidad: verificará la identidad y representación mediante información proporcional al riesgo de la solicitud.

12 Consultas y reclamos

Enviar la solicitud a administracion@hmb-sas.com indicando nombre, identificación suficiente, medio de respuesta, descripción de la petición y, cuando proceda, soporte de representación y documentos pertinentes. Puede utilizarse el asunto “Protección de datos personales”.

Las consultas se responderán dentro de diez días hábiles desde su recibo. Si se requiere prórroga, se informarán las razones antes del vencimiento y la nueva fecha, que no excederá cinco días hábiles adicionales.

Los reclamos se atenderán dentro de quince días hábiles contados desde el día siguiente a su recibo; la prórroga motivada no excederá ocho días hábiles adicionales. Si el reclamo está incompleto, se solicitará subsanación dentro de cinco días desde su recepción; después de dos meses sin respuesta al requerimiento se entenderá desistido.

El reclamo recibido por quien no sea competente se trasladará dentro de dos días hábiles, informando al interesado. Recibido el reclamo completo, se registrará "reclamo en trámite" y su motivo dentro de dos días hábiles, hasta su decisión. La atención protegerá los datos y derechos de terceros.

Cuando HMB actúe por cuenta de un cliente, apoyará el trámite y lo trasladará al responsable competente; no sustituirá sus decisiones sin instrucción o habilitación legal.

13 Vigencia y actualización

La versión 2.0 tiene fecha de 13 de octubre de 2026 y está prevista para entrar en vigor con su aprobación y publicación. Sustituye la política web fechada el 15 de enero de 2025 desde esa publicación. Su adopción corresponde al representante legal, quien conservará la constancia de aprobación y la fecha efectiva.

HMB publicará la versión vigente y comunicará los cambios sustanciales que afecten las autorizaciones. Las nuevas finalidades que lo requieran se someterán a una nueva autorización. Publicar una actualización no modifica por sí solo contratos suscritos ni legitima tratamientos previos.