Effective Date: 12 March 2026

HILOTOOLS PRIVACY POLICY

Applicable to: www.hilotools.com and related services that link to this Privacy Policy
Effective Date: 12 March 2026
Last Updated: 12 March 2026

This Privacy Policy describes how HiloTools ("HiloTools," "we," "us," "our") collects, uses, discloses, and otherwise processes Personal Data in connection with: (i) the website hilotools.com (the "Website"); and (ii) any hosted software, tools, APIs, client portals, dashboards, documentation portals, or professional services that reference or link to this Privacy Policy (collectively, the "Services").

If you enter into a written agreement with us (including a Master Services Agreement, Subscription Agreement, Statement of Work, and/or Data Processing Addendum), that agreement may govern processing of Customer Content (defined below) and may supplement or override this Privacy Policy to the extent permitted by applicable law.

1. Controller identity, roles, and contact

1.1 Controllers / operating entities.

The Website and Services are operated by:

- **HiloTools Inc.** (a corporation incorporated in Delaware, United States).
  Registered office: 251 Little Falls Drive, Wilmington, New Castle County, Delaware 19808
- **Hilo Tools S.A.S.** (Colombia), identified as NIT 901731290-4, domiciled in Bogotá D.C., Colombia ("HiloTools S.A.S.").
  Registered office: Cra 4 No 80-28 Of 802

Depending on the engagement, the contracting entity will be identified in the applicable proposal, order form, statement of work, or executed agreement.

1.2 Controller vs. Processor / Service Provider boundary (critical).

- Controller processing ("HiloTools as controller"). We act as an independent controller (or "business" under certain U.S. state laws) for Personal Data we process to operate the Website, manage leads and enterprise relationships, administer accounts, invoice, maintain security, manage vendors, and comply with legal obligations.
- Processor / Service Provider processing ("HiloTools processing Customer Content"). Where a business customer uses our Services and provides Customer Content (including end-user data) for processing on its behalf, the customer is typically the controller/business and we act as a processor/service provider. In that case, our processing is governed by the customer contract and/or DPA, and the customer is responsible for appropriate notices and lawful basis selection for that processing (subject to applicable law).

1.3 Contact.

Privacy inquiries and rights requests: contact@hilotools.com
Recommended subject line: “Data Protection Rights Request / Ejercicio de derechos de protección de datos”

If you are an authorized agent, include proof of authorization and sufficient verification information.

2. Scope and definitions

2.1 Scope.

This Privacy Policy applies to Personal Data processed when you:

- access or use the Website;
- submit inquiries through forms (e.g., contact, demo, meeting, intake);
- communicate with us (email, conferencing, chat, support tickets);
- access Services that require authentication; or
- interact with cookies and similar technologies on the Website/Services.

This Privacy Policy does not apply to third-party websites, products, or services that we do not control, even if linked from our Website.

2.2 Definitions.

- “Personal Data” / “Personal Information”: information relating to an identified or identifiable individual, or otherwise defined as personal data/personal information under applicable law.
- “Sensitive Data”: (as applicable) GDPR special categories of data and/or “Sensitive Personal Information” under California law.
- “Customer Content”: any data, files, documents, records, messages, or other content submitted to the Services by or on behalf of a business customer, including Personal Data contained therein.
- “Processing”: any operation performed on Personal Data (collection, use, storage, disclosure, deletion, etc.).
- “Subprocessor”: a third party engaged by HiloTools to process Personal Data on HiloTools’ behalf.

3. Categories of Personal Data we collect

We collect (or receive) the following categories of Personal Data depending on your interaction with the Website/Services.

3.1 Directly provided data (direct identifiers).

- Identity and contact data: name, business email, phone number, job title, company/organization.
- Inquiry and communications content: messages, attachments, meeting requests, and related correspondence.
- Commercial and contracting data: proposal and contracting communications, invoicing contacts, and account administration records.

3.2 Automatically collected data (indirect identifiers).

- Device and technical data: IP address, device type, operating system, browser/user agent, language settings, approximate location derived from IP, timestamps, and referrer URLs.
- Usage and interaction data: website navigation paths, page views, clickstream, session diagnostics, and (where applicable) authenticated feature usage.
- Security telemetry: authentication events, access logs, anomaly indicators, and related security signals.

3.3 Third-party sourced data.

- Business contact enrichment: public professional information and business contact data obtained from lawful sources (e.g., corporate websites, professional directories, event lists), subject to applicable law.
- Security and fraud signals: risk indicators from security providers (e.g., bot detection, abuse prevention).

3.4 Customer Content (processed on behalf of customers).

When we process Customer Content, the categories depend on the customer's configuration and instructions and may include identifiers, documents, records, and user-generated content about the customer's own end users, employees, contractors, or clients.

3.5 Sensitive Data / special categories.

- The Website is not designed to solicit Sensitive Data. Do not submit Sensitive Data through the Website unless explicitly requested under a secure channel within a formal engagement.
- If Sensitive Data appears in Customer Content, we process it strictly under the customer's documented instructions and subject to heightened safeguards.

4. How we collect Personal Data

We collect Personal Data through:

- Website and Service forms and submissions;
- cookies and similar technologies (cookies, pixels, SDKs, local storage, scripts);
- server and application logs and security monitoring;
- APIs, webhooks, and integrations configured by customers (including OAuth tokens or API keys where applicable);
- communications (email, conferencing, chat, support tickets); and
- service providers supporting hosting, security, communications, analytics, and customer operations.

5. Purposes of processing and lawful bases

Where GDPR/UK GDPR applies, we process Personal Data only when a lawful basis applies. Depending on context, we rely on one or more of the following.

5.1 Contract / pre-contract steps.

To provide requested Services, respond to inquiries, prepare proposals, administer accounts, provide support, and perform statements of work.

5.2 Consent.

To the extent required or appropriate, we rely on consent for:

- non-essential cookies and similar technologies; and
- certain marketing communications where consent is required.

You may withdraw consent at any time where processing is based on consent. Withdrawal does not affect prior lawful processing.

5.3 Legitimate interests.

We may process Personal Data where necessary for legitimate interests, including:

- securing, maintaining, and improving the Website/Services;
- preventing fraud, abuse, and unauthorized access;
- internal analytics and service measurement (subject to cookie preferences);
- corporate governance, risk management, and legal defense; and
- B2B relationship management and proportionate commercial outreach where permitted.

When we rely on legitimate interests, we evaluate necessity, proportionality, and reasonable expectations and implement mitigations where appropriate.

5.4 Legal obligations.

To comply with applicable laws (e.g., accounting and tax, compliance, sanctions/export controls, lawful regulatory or law enforcement requests).

5.5 Processor/service provider processing (Customer Content).

Where we process Customer Content on behalf of a customer, the customer determines the lawful basis and notice obligations. We process Customer Content under documented instructions and contractual terms.

6. Cookies, analytics, and consent management

6.1 Cookie categories.

We may use the following categories of cookies or similar technologies:

- Strictly necessary: core functionality, load balancing, and security controls.
- Functional: preference saving and enhanced usability.
- Analytics/performance: measurement of service performance and improvement.
- Marketing/advertising (if enabled): campaign attribution and (in some cases) cross-context behavioral advertising.

6.2 Consent and preference controls.

Where required by law, we implement a cookie banner and preference controls to obtain and manage consent for non-essential cookies. You can modify or withdraw your preferences through the same controls or via equivalent mechanisms we provide.

6.3 Opt-out preference signals.

Where required, we honor recognized opt-out preference signals relevant to sale/sharing and certain advertising-related processing.

6.4 Cookie disclosures.

When appropriate, we disclose cookie details (categories, purposes, durations, and third-party recipients) through our cookie banner/preference center and/or a cookie notice.

7. Disclosures to third parties and subprocessors

We disclose Personal Data only as necessary for the purposes described above.

7.1 Subprocessors / service providers.

We engage subprocessors for functions such as:

- cloud hosting and infrastructure;
- content delivery network and web security;
- communications tooling (email, conferencing, messaging);
- customer support and ticketing;
- monitoring, logging, and security operations; and
- professional services and compliance operations.

Contract requirement (mandatory). We require subprocessors by written contract to:

- process Personal Data only on documented instructions and for specified purposes;
- maintain confidentiality and implement appropriate security measures;
- impose restrictions on onward transfers and subprocessing;
- assist with incident response and rights requests where applicable;
- delete or return data upon termination where applicable; and
- permit accountability measures (e.g., audits/assurance) appropriate to the engagement.

7.2 Affiliates.

We may share Personal Data among affiliated entities for internal administration, security, compliance, invoicing, and service delivery.

7.3 Legal and corporate events.

We may disclose Personal Data to comply with law, court orders, or lawful governmental requests, or in connection with corporate transactions (e.g., merger, acquisition, reorganization), subject to confidentiality and continued protection.

8. International transfers

Because we operate internationally, Personal Data may be processed in jurisdictions different from your residence, including the United States and Colombia and/or other jurisdictions where our vendors operate.

Where GDPR/UK GDPR cross-border rules apply, we rely on appropriate safeguards such as:

- adequacy decisions/regulations (where applicable);
- EU Standard Contractual Clauses (SCCs) and supplemental contractual/technical measures where required;
- UK International Data Transfer Agreement (IDTA) and/or the UK Addendum to EU SCCs; and
- transfer risk assessments and supplementary measures where required.

You may request information about applicable safeguards by contacting us.

9. Data retention and deletion

We retain Personal Data only for the period strictly necessary to fulfill the purposes described in this Privacy Policy, unless longer retention is required by law or contract.
Retention criteria include: relationship duration, data sensitivity, legal retention duties, contractual requirements, security needs, and risk/claims management.

When data is no longer necessary:

- we delete it or irreversibly anonymize it; and
- where appropriate, we may "block"/restrict certain records for legal hold, compliance, or dispute purposes, and limit their use to those purposes only.

Customer Content retention and deletion are governed by the customer contract/DPA and documented deletion/export instructions.

10. Security measures

We maintain an information security program designed to protect Personal Data against unauthorized access, disclosure, alteration, loss, or destruction using administrative, technical, and organizational safeguards appropriate to risk. Measures may include:

- authentication controls and role-based access limitations;
- encryption in transit and, where appropriate, at rest;
- logging and monitoring of access and anomalous events;
- secure development and vulnerability management practices;
- backups and restore testing; and
- privacy/security training and confidentiality controls.

No method of transmission or storage is absolutely secure; therefore we cannot guarantee absolute security.

11. Incident response and breach notifications

We maintain incident response procedures to assess, contain, investigate, remediate, and document suspected security incidents.

Where required by law or contract:

- if we act as controller, we will provide regulator and/or individual notifications as required; and
- if we act as processor/service provider, we will notify the customer-controller without undue delay and assist with required notifications as contractually and legally required.

12. Your rights and how to exercise them

Depending on your jurisdiction, you may have rights such as:

- access and confirmation of processing;
- correction/rectification;
- deletion/erasure (subject to exceptions);
- restriction/limitation of processing;
- objection (including to direct marketing);
- data portability (where applicable);
- withdrawal of consent (where applicable); and
- the right to lodge a complaint with a supervisory authority/regulator.

How to submit a request.

Email contact@hilotools.com with the subject line “Data Protection Rights Request.” Include:

- your name and contact details;
- the right you wish to exercise;
- sufficient detail to identify relevant data; and
- verification information appropriate to the request.

We may request additional information to verify identity and prevent unauthorized disclosure.

Processor caveat. If we process your data as a processor/service provider on behalf of a customer, the customer is typically responsible for responding to certain rights requests; we may redirect you to the customer where legally appropriate.

13. California (CCPA/CPRA) disclosures

This section applies to California residents where the CCPA/CPRA applies.

13.1 Categories collected; purposes; sources; disclosures.

We collect categories of personal information described in this Privacy Policy and use them for the business and commercial purposes described above. We collect such information from you, from your device/browser interactions, from security telemetry, and from third parties where permitted.

13.2 Sale/sharing; sensitive personal information.

We do not sell personal information for monetary consideration. If we engage in "sharing" for cross-context behavioral advertising (for example, through certain third-party advertising cookies), you may opt out using the mechanisms described below and via recognized opt-out preference signals where applicable.

To the extent we collect Sensitive Personal Information, we limit its use to permitted purposes and provide the right to limit use/disclosure where required.

13.3 Consumer rights.

Subject to applicable exceptions, California residents may have the right to: know/access, delete, correct, opt out of sale/sharing, limit use of sensitive personal information, and not be discriminated against for exercising rights.

13.4 Submission methods; authorized agents; verification; appeal (if applicable).

Requests may be submitted via email to contact@hilotools.com and, if implemented, via an online request form: www.hilotools.com

Authorized agents must provide proof of authorization. We verify requests using commercially reasonable methods appropriate to the sensitivity of information involved.

14. Automated decision-making and profiling

We may use automated tools for security monitoring, abuse prevention, and service integrity.

We do not intend to make decisions producing legal or similarly significant effects based solely on automated processing unless such processing is lawful, appropriately disclosed, and subject to required safeguards.

Customer-configured automated processing within Customer Content is controlled by the customer-controller, subject to the customer's notices and lawful basis.

15. Children and minors

The Website and Services are not directed to children. We do not knowingly collect Personal Data from children in circumstances requiring parental consent. If you believe a child has provided Personal Data to us, contact us so we can take appropriate action.

16. Marketing communications

Where permitted by law, we may send marketing communications. You can opt out at any time using the unsubscribe mechanism in the message or by contacting us. Operational communications (security notices, account messages, transactional notices) are not affected by marketing opt-outs.

17. Changes to this Privacy Policy

We may update this Privacy Policy periodically. The “Last Updated” date indicates the effective version. If changes are material, we will provide additional notice where required by law.

18. Governing law, jurisdiction, and dispute resolution

To the extent permitted by applicable law and not overridden by mandatory data protection law, privacy-related disputes will be governed by the governing law and dispute resolution approach set out in applicable Website terms and/or the relevant Service agreement. Nothing in this Privacy Policy limits any mandatory rights to lodge complaints with supervisory authorities/regulators or pursue mandatory legal remedies.