Ping Intel – Privacy Policy

Last updated: May 04, 2026

1. About this policy

This Privacy Policy explains how Ping Data Technology, Inc., doing business as Ping Intel ("Ping Intel", "we", "us") collects, uses, shares, and protects personal data when you:

- Visit our websites (including https://pingintel.com and product subdomains);
- Use our products (Ping.Location, Ping.Extraction, Ping.Data, Ping.Vision); or
- Interact with us as a customer, prospect, supplier, or other business contact.

"Personal data" means information relating to an identified or identifiable individual.

This Privacy Policy is intended to meet the information requirements of the EU General Data Protection Regulation ("GDPR"), the UK GDPR, and applicable U.S. privacy laws, including the California Consumer Privacy Act, as amended by the CPRA.

2. Who is the controller?

For most processing described in this Privacy Policy, Ping Intel acts as a data controller, including for:

- Website visitors and product users;
- Contacts at customers and prospective customers;
- Marketing and business communications; and
- Individuals who communicate with us via email or support channels.

When we process personal data solely on behalf of a customer (for example, personal data contained in insurance documents submitted through Ping.Extraction or Ping.Data where the customer determines the purposes and means of processing), we act as a data processor. In those cases, processing is governed by our Data Processing Addendum (DPA) and the customer's own privacy notice.

Contact details

- Controller: Ping Data Technology, Inc. (Ping Intel)

- Email: support@pingintel.com

- Postal address: 1111 Lincoln Road, Suite 500, Miami Beach, FL 33139, USA

EU/UK representative and DPO

EU Representative (GDPR Article 27)

Ping Intel has appointed iuro Rechtsanwälte GmbH t/a Prighter as its representative in the European Union pursuant to Article 27 of the GDPR. Contact details are available upon request to support@pingintel.com.

UK Representative

Ping Intel has appointed Prighter Ltd as its representative in the United Kingdom for purposes of the UK GDPR. Contact details are available upon request to support@pingintel.com.

Data Protection Officer (DPO)

Ping Intel is not required to appoint a Data Protection Officer under Article 37 GDPR and has not appointed one.

Privacy inquiries may be directed to support@pingintel.com.

3. Categories of personal data we collect

The categories of personal data we process depend on your relationship with us and how you use the Services.

3.1 Account and contact data

- Names
- Work email addresses
- Job titles and roles
- Company name and contact details
- Authentication and login data (e.g., usernames, hashed passwords, SSO identifiers)

3.2 Usage and technical data

- IP address
- Browser and device information
- Log files, diagnostics, and security logs
- Feature usage, pages viewed, and interaction data
- Session timestamps and performance metrics

This may include data generated through analytics tools such as PostHog.

3.3 Customer Data and documents

When using Ping.Location, Ping.Extraction, or Ping.Data, customers may provide:

- Insurance submission documents (e.g., ACORD forms, schedules of values, spreadsheets, etc);
- Free-text email content and attachments;
- Property, building, and location data (including addresses and metadata); and
- Names and work contact details of brokers, underwriters, insureds, and other business contacts.

While our services focus on commercial insurance and E&S lines, personal data may appear incidentally in these materials.

3.4 Marketing and communications data

- Newsletter subscriptions and preferences.
- Records of marketing outreach and responses.
- Support tickets, feedback, and correspondence.

3.5 Financial and contract data

- Billing, payment, and contract information related to customers and vendors (generally business-related).

We do not intentionally collect special categories of personal data (e.g., health, ethnicity, religious beliefs) or children's data. If such data appears incidentally in Customer Data, we treat it with appropriate care but ask customers to avoid including it where possible.

4. Sources of personal data

We may collect personal data from:

- You directly (e.g., account registration, emails, support requests);
- Your employer or colleagues (e.g., user provisioning);
- Customers and partners (e.g., documents submitted for processing);
- Public sources and datasets (e.g., property and hazard data); and
- Third-party service providers (e.g., hosting, analytics, CRM), where permitted by law.

5. Purposes and legal bases for processing (GDPR/UK GDPR)

Where the EU GDPR or UK GDPR applies, Ping Intel processes personal data only where a valid legal basis exists under Article 6 GDPR.

Purpose	Typical processing activities	Legal basis (GDPR Art. 6)
Provision and operation of the Services	Account creation and management; authentication; processing insurance submissions; generating and returning structured outputs, analytics, and data	Performance of a contract (Art. 6(1)(b)); where strictly necessary, legitimate interests (Art. 6(1)(f))
Infrastructure, hosting, and security	Hosting Customer Data; maintaining systems and logs; monitoring availability and performance; preventing fraud, abuse, and security incidents	Performance of a contract (Art. 6(1)(b)); legitimate interests in operating a secure and reliable service (Art. 6(1)(f))
Customer support and communications	Responding to support requests; troubleshooting; service notices and operational updates	Performance of a contract (Art. 6(1)(b)); legitimate interests in providing customer support (Art. 6(1)(f))

Purpose	Typical processing activities	Legal basis (GDPR Art. 6)
Product analytics and service improvement	Usage analysis; performance metrics; debugging; feature evaluation and improvement, including via analytics tools such as PostHog	Legitimate interests in improving and developing the Services (Art. 6(1)(f))
Sales, marketing, and business development	B2B marketing communications; newsletters; outreach to business contacts regarding products and services	Consent where required by law (Art. 6(1)(a)); otherwise legitimate interests for B2B marketing where permitted (Art. 6(1)(f))
Contractual, financial, and account management	Order processing; invoicing; payments; accounting; audits; contract administration	Performance of a contract (Art. 6(1)(b)); compliance with legal obligations (Art. 6(1)(c)); legitimate interests (Art. 6(1)(f))
Legal, regulatory, and compliance purposes	Responding to lawful requests; enforcing agreements; handling disputes; preventing misuse of the Services	Compliance with legal obligations (Art. 6(1)(c)); legitimate interests (Art. 6(1)(f))

Where processing is based on consent, consent may be withdrawn at any time.

6. How we use analytics and cookies

We use cookies and similar technologies for essential functionality, security, and service performance. We also use analytics tools (such as PostHog) to understand how users interact with our Services and to improve functionality.

Where required by law (including in the EU and UK), analytics technologies are enabled only after user consent via an appropriate cookie consent mechanism.

Further details are provided in our Cookie Policy.

7. Sharing of personal data

We may share personal data with:

- Service providers and subprocessors (e.g., hosting, analytics, email, billing)
- Third-party data providers integrated into our Services
- Professional advisers under confidentiality obligations
- Regulators and authorities where required by law
- Parties involved in corporate transactions

Ping Intel does not sell personal data and does not share personal data for cross-context behavioral advertising, as those terms are defined under the CCPA/CPRA.

An overview of our subprocessors is available upon request. Please contact support@pingintel.com for more information.

8. International transfers

We may process personal data in the United States and other countries. Where required, we rely on appropriate safeguards such as:

- EU Standard Contractual Clauses
- UK IDTA or Addendum
- Other lawful transfer mechanisms

We rely on the EU-U.S. Data Privacy Framework (DPF) and the UK Extension to the DPF for transfers to certified subprocessors (e.g., AWS, Snowflake). For non-certified subprocessors, we rely on EU Standard Contractual Clauses and the UK IDTA Addendum.

9. Retention periods

We retain personal data only as long as necessary for the purposes described above:

- User accounts: Duration of the account plus 30 days
- Support communications: Up to 3 years after resolution
- Marketing data: Until unsubscribe, plus 30 days
- Contracts and billing: 3–7 years, depending on legal requirements
- Product analytics: Up to 12 months, then deleted or aggregated

- Uploaded documents and emails: Per customer agreement

Exact retention periods may be set out in customer contracts and our internal Records of Processing Activities (ROPA). When personal data is no longer needed, we will delete or anonymize it.

10. Your rights (EEA/UK and similar jurisdictions)

Individuals in the EEA, UK, and similar jurisdictions may have rights including access, rectification, deletion, restriction, portability, objection, and withdrawal of consent.

To exercise these rights, contact support@pingintel.com.

We may need to verify your identity and may be unable to fully comply with your request where certain legal or contractual obligations apply.

You also have the right to lodge a complaint with your local data protection authority. For example:

- In the EEA: see the list of supervisory authorities provided by the European Data Protection Board.

- In the UK: the Information Commissioner's Office (ICO), https://ico.org.uk.

11. Data security

We implement technical and organizational measures designed to protect personal data, including encryption, access controls, monitoring, and vendor safeguards.

No security measures are perfect; if we become aware of a personal data breach that is likely to result in a risk to individuals' rights and freedoms, we will notify affected customers and regulators as required by law.

12. Children

Our Services are not directed to children, and we do not knowingly collect personal data from children. If you believe a child has provided us with personal data, please contact support@pingintel.com so we can take appropriate action.

13. Changes to this Privacy Policy

We may update this Privacy Policy from time to time. Material changes will be communicated where required.

14. Contact

If you have any questions or requests regarding this Privacy Policy, please contact:

Ping Data Technology, Inc. (Ping Intel)

Email: support@pingintel.com

Address: 1111 Lincoln Road, Suite 500, Miami Beach, FL 33139, USA