

Ping Intel – Privacy Policy

Last updated: September 14, 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 Enterprise, Ping.Location Self-Service (our direct-to-consumer property data service), Ping.Extraction, Ping.Data, Ping.Maps, and 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.

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.
- Individual users who create accounts and purchase data directly through Ping.Location Self-Service.

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 using a Ping.Location Enterprise account 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 Prighter EU Rep GmbH as its representative in the European Union pursuant to Article 27 of the GDPR. Data subjects and supervisory authorities in the EEA may contact our EU Representative regarding matters relating to Ping Intel's processing of personal data at:

Postal address:
9 Clare Street,
Dublin 2 D02 HH30,
Ireland

Online contact form:

<https://app.prighter.com/dsr/16670255327>

UK Representative

Ping Intel has appointed Prighter Ltd as its representative in the United Kingdom for purposes of the UK GDPR. Data subjects and the Information Commissioner's Office may contact our UK Representative regarding matters relating to Ping Intel's processing of personal data at:

Postal address:

20 Mortlake High Street,
London, SW14 8JN,
United Kingdom

Online contact form:

<https://app.prighter.com/dsr/16670255327>

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).

3.6 Ping.Location Self-Service user data

When you register for a Ping.Location Self-Service individual account and purchase data directly from Ping Intel (rather than through Ping.Location Enterprise, which is governed by an enterprise agreement), we collect the following categories of personal data directly from you:

- **Account and identity data:** Your name, email address, company name, and a password (stored in hashed form). You may also optionally provide your business address and business phone number.
- **Transaction and subscription data:** The property address(es) you query, the data type(s) you select, your selected plan, billing frequency, Subscription start and renewal dates, the date and amount of each charge, Subscription and cancellation

status, included credits or usage allowance, and a transaction reference number provided by our payment processor.

- **Payment metadata and payment-recovery data:** Where provided by our payment processor, the last four digits of your payment card, billing address, and any payment token or other payment credential that Ping Intel receives for recurring payment processing; payment status, payment failures, chargebacks, and payment-recovery or dunning activity. We retain this information only for the purposes described in Sections 5 and 9.
- **Subscription communications and records:** Billing, invoice, Subscription confirmation, renewal, reminder, payment-failure, payment-recovery, plan-change, and cancellation communications, together with associated delivery records.
- **Usage, entitlement, and technical data:** Your Subscription usage, available credits or usage allowance, feature use, and the usage and technical data described in Section 3.2 above.

We do not collect or store your full payment card number, expiration date, or security code. That information is collected and processed directly by our third-party payment processor and does not pass through Ping Intel's systems.

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, Subscription enrollment, account and billing management, emails, support requests, and — for Ping.Location Self-Service users — property address queries and purchase transactions);
- 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))
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.

Purpose	Typical processing activities	Legal basis (GDPR Art. 6)
		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))
Ping.Location Self-Service account creation and management	Registration of individual user accounts; authentication; password management; account maintenance and closure	Performance of a contract (Art. 6(1)(b))
Ping.Location Self-Service service delivery	Receiving property address queries; retrieving and structuring property data; delivering purchased results to the user's account	Performance of a contract (Art. 6(1)(b))
Ping.Location Self-Service Subscription administration, recurring billing, and financial records	Administering pay-as-you-go purchases and Subscriptions; processing authorized recurring charges; maintaining selected-plan, billing-frequency, renewal, transaction, invoice, tax, authorization, confirmation, reminder, cancellation, and billing records	Performance of a contract (Art. 6(1)(b)); compliance with legal obligations (Art. 6(1)(c))
Ping.Location Self-Service platform security, fraud prevention, and payment recovery	Monitoring for unauthorized access; detecting and preventing fraud; maintaining security logs; addressing payment failures, chargebacks, and amounts properly due	Legitimate interests in operating a secure and reliable service, preventing fraud, and recovering amounts properly due (Art. 6(1)(f))
Ping.Location Self-Service analytics and service improvement	Usage analysis; performance metrics; feature evaluation and improvement for the Ping.Location Self-Service interface, including via analytics tools such as PostHog	Legitimate interests in improving and developing the Services (Art. 6(1)(f))

Purpose	Typical processing activities	Legal basis (GDPR Art. 6)
Ping.Location Self-Service marketing communications	Sending promotional communications to individual Ping.Location Self-Service users who have opted in	Consent where required by law (Art. 6(1)(a))

Where we rely on legitimate interests as our legal basis for Ping.Location Self-Service processing, you have the right to object to that processing at any time. See Section 10 for details of how to exercise your rights.

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, payment processing, and 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:

Cancellation or nonrenewal of a Ping.Location Self-Service Subscription stops future recurring charges and ends the Subscription, but does not by itself close your account. The retention periods below distinguish the end of a Subscription from account closure.

- 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: Typically deleted within 14 days after processing, unless otherwise required
- Ping.Location Self-Service user account data (active account, including account profile and current Self-Service status): Duration of active account
- Ping.Location Self-Service user account data (after account closure): 30 days after account closure, then deleted, except where a listed longer retention period applies
- Ping.Location Self-Service transaction, invoice, tax, and billing records (including purchase or Subscription charges, amounts, dates, and transaction references): 7

years from the date of the relevant transaction or invoice (tax and accounting legal obligation)

- Ping.Location Self-Service property query results (retained in account): Duration of active account; deleted upon account closure
- Ping.Location Self-Service payment metadata that forms part of a transaction or tax record (transaction reference, last four digits of card, and billing address): 7 years from the date of the relevant transaction (tax and accounting legal obligation)
- Ping.Location Self-Service Subscription administration and entitlement data (selected plan, billing frequency, renewal or cancellation status, and credits or usage allowance): Duration of active Subscription plus 1 year after the Subscription ends, unless the account remains active or a longer listed period applies
- Ping.Location Self-Service payment token or other recurring-payment credential actually received by Ping Intel: Duration of active Subscription plus up to 180 days after the Subscription ends, solely to resolve a payment failure, chargeback, dispute, or other payment-recovery matter; Ping Intel does not retain full payment-card data
- Ping.Location Self-Service payment-failure, chargeback, dunning, and debt-recovery records: 3 years after final resolution, except that information forming part of a transaction, invoice, or tax record is retained for the 7-year period above
- Ping.Location Self-Service Subscription authorization and communications evidence (Subscription Summary, enrollment/authorization record, confirmation, renewal/reminder, plan-change, payment-failure, and cancellation notices and delivery records): the later of 3 years after the relevant authorization or communication, or 1 year after Subscription termination

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

10.1 EEA and UK residents

If you are located in the European Economic Area or the United Kingdom, you have the following rights with respect to personal data for which Ping Intel acts as a data controller (including as a Ping.Location Self-Service user):

— **Right of access (Art. 15 GDPR):** You may request confirmation of whether we process your personal data and, if so, a copy of that data.

- **Right to rectification (Art. 16 GDPR):** You may request correction of inaccurate personal data we hold about you.
- **Right to erasure (Art. 17 GDPR):** You may request deletion of your personal data, subject to our legal retention obligations (for example, we are required to retain transaction records for tax purposes).
- **Right to restriction (Art. 18 GDPR):** You may request that we restrict processing of your personal data in certain circumstances.
- **Right to data portability (Art. 20 GDPR):** Where processing is based on contract or consent and carried out by automated means, you may request your personal data in a structured, machine-readable format.
- **Right to object (Art. 21 GDPR):** You may object to processing based on legitimate interests. We will cease processing unless we can demonstrate compelling legitimate grounds that override your interests.
- **Right to withdraw consent:** Where processing is based on consent, you may withdraw consent at any time without affecting the lawfulness of processing carried out before withdrawal.

To exercise any of these rights, please contact us at support@pingintel.com. We will respond within one month of receipt of your request. We may need to verify your identity before processing your request.

You also have the right to lodge a complaint with your local supervisory authority:

- In the EEA: see the list of supervisory authorities published by the European Data Protection Board.
- In the UK: the Information Commissioner's Office (ICO), <https://ico.org.uk>.

10.2 California residents (CCPA/CPRA)

If you are a California resident, you have the following rights under the California Consumer Privacy Act (CCPA), as amended by the California Privacy Rights Act (CPRA):

For Ping.Location Self-Service, the categories of personal information we collect may include identifiers and account information; business contact information; commercial information, including selected plan, Subscription status, transaction, billing, payment-status, and cancellation information; internet or other electronic network activity information; and, where received from our payment processor, payment metadata or a payment token/credential. We use this information to create and manage accounts, provide pay-as-you-go purchases and Subscriptions, process authorized payments, administer renewals and cancellations, communicate about billing and service status, provide support, prevent fraud and misuse, recover amounts properly due, maintain records, comply with legal

obligations, and improve the Services as described in Sections 3 and 5. We retain the information as described in Section 9. Ping Intel does not sell personal information or share personal information for cross-context behavioral advertising.

— **Right to Know:** You may request disclosure of the categories and specific pieces of personal information we have collected about you, the categories of sources, the purposes for collection, and the categories of third parties with whom it is shared.

— **Right to Delete:** You may request deletion of personal information we have collected from you, subject to certain exceptions (including our legal obligation to retain transaction records).

— **Right to Correct:** You may request correction of inaccurate personal information we maintain about you.

— **Right to Opt-Out of Sale or Sharing:** Ping Intel does not sell personal information and does not share personal information for cross-context behavioral advertising. You therefore have no need to opt out of such activities at this time.

— **Right to Non-Discrimination:** We will not discriminate against you for exercising any of your CCPA/CPRA rights.

To submit a verifiable consumer request, please contact us at support@pingintel.com. We will respond within 45 days, with an extension of up to an additional 45 days where reasonably necessary.

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