Privacy Policy

Effective Date: April 22, 2026 **Last Updated: April** 22, 2026

> **Drafting notes — remove before publishing:**
> - Effective Date and Last Updated: set to publication date.
> - Legal review before publishing, particularly the US state-law section and retention periods.

---

1. Who We Are

This Privacy Policy explains how **Abusix** (referred to as "Abusix," "we," "us," or "our") collects, uses, shares, and protects personal data in connection with our website (`abusix.com`, the "Site") and our products and services, including the Guardian platform (Guardian Mail, Guardian Ops, Guardian Intel), the Abuse Contact Database, Threat Intel Lookup, Blackhole MX, XARF, and any related tools, APIs, and portals (collectively, the "Services").

The Abusix group operates through two entities, each of which acts as an **independent data controller** for the customers and data it handles:

Abusix, Inc. — parent company A Delaware corporation One Boston Place, 201 Washington Street Boston, MA 02108, United States Phone: +1 617 356 1581 CEO: Tobias Knecht Email: privacy@abusix.com

Abusix GmbH — wholly-owned subsidiary of Abusix, Inc. Roonstrasse 23a 76137 Karlsruhe, Germany Commercial Register: Amtsgericht Mannheim, HRB 707959 VAT ID: DE268014995 CEO: Tobias Knecht Email: privacy@abusix.com

Abusix GmbH operates as its own entity and contracts with customers in its own name. The controller responsible for your personal data is the Abusix entity that:

- has entered into the agreement for the Services with you (as identified in your order form, invoice, or account contract); or
- where no such agreement exists, operates the specific Service, website, or channel through which you interacted with us.

If you are unsure which entity is the controller for your data, contact us at privacy@abusix.com and we will confirm. Where the two entities share personal data with each other as part of operating the Services (for example, when Abusix GmbH relies on infrastructure operated by Abusix, Inc.), the transfer is governed by the safeguards described in Section 7.

2. Data Protection Officer

We have appointed **GDPRlocal** as our external Data Protection Officer. You can contact our DPO at:

Email: dpo@abusix.com **Postal:** Data Protection Officer, Abusix GmbH, Roonstrasse 23a, 76137 Karlsruhe, Germany

3. Scope

This Policy applies to personal data we process as a **controller** — that is, data we collect from visitors to our Site, prospective customers, customers and their authorized users, contacts at partner organizations, job applicants, and others who interact with us directly.

For data that our customers submit to the Services for processing (such as abuse reports, network logs, mailserver telemetry, and end-user identifiers contained in those reports), Abusix acts as a **processor** on behalf of the customer. The customer is the controller of that data, and the customer's own privacy notice and our Data Processing Agreement with them govern that processing.

4. Personal Data We Collect

We collect the following categories of personal data:

Account and contact data. Name, business email, phone number, employer, job title, country, and similar professional contact details provided when you register, request a demo, contact support, or subscribe to communications.

Authentication data. Usernames, hashed passwords, single sign-on identifiers, API keys, and multi-factor authentication tokens.

Billing data. Billing address, VAT/tax identifiers, purchase order references, and transaction records. Full payment card details are handled by our payment processor and are not stored on our systems.

Service usage data. Logs of how authorized users interact with the Services, including timestamps, IP addresses, user-agent strings, actions taken in the portal, API call metadata, and error events.

Site analytics data. IP address (often truncated), device and browser information, referring URL, pages viewed, time on page, and similar analytics data collected via cookies and similar technologies. See Section 11.

Marketing and communications data. Your preferences for receiving marketing communications, records of consent, and engagement metrics (opens, clicks) for our marketing emails.

Recruitment data. If you apply for a role with us, CV/résumé, cover letter, work history, references, and other information you provide during recruitment.

Data submitted to our Services by customers. As noted in Section 3, we process this as a processor; the types and scope are defined by the customer.

We do not intentionally collect special category data (Art. 9 GDPR) or data relating to children (see Section 13).

5. How We Use Personal Data and Legal Bases

We process personal data only where we have a lawful basis under Art. 6 GDPR. The table below summarizes our main processing activities:

Purpose	Legal basis (Art. 6 GDPR)
Providing, operating, and securing the Services; authenticating users; responding to support requests	Performance of a contract (Art. 6(1)(b))
Billing, invoicing, tax reporting, and debt recovery	Performance of a contract and legal obligation (Art. 6(1)(b), (c))
Maintaining security, preventing fraud and abuse of our Services, and ensuring network and information security	Legitimate interests (Art. 6(1)(f)) — our interest in protecting the Services and our customers
Service improvement, product analytics, and aggregated reporting	Legitimate interests (Art. 6(1)(f))
Sending service-related emails (e.g. outage notices, security alerts, policy changes)	Performance of a contract and legitimate interests (Art. 6(1)(b), (f))
Sending marketing emails and newsletters	Consent (Art. 6(1)(a)); for existing customers, legitimate interests where permitted by applicable law including § 7(3) UWG
Processing job applications	Pre-contractual measures and legitimate interests (Art. 6(1)(b), (f))
Complying with legal obligations, responding to lawful requests from authorities	Legal obligation (Art. 6(1)(c))
Establishing, exercising, or defending legal claims	Legitimate interests (Art. 6(1)(f))

Where we rely on legitimate interests, we have carried out a balancing test to ensure those interests are not overridden by your rights and freedoms. You can request a summary of that balancing test by contacting us.

6. How We Share Personal Data

We do not sell personal data. We share personal data only in the following circumstances:

Service providers (processors). We use carefully selected third parties to help us run the business, including cloud hosting (Amazon Web Services), error monitoring (Sentry), customer messaging (Customer.io, Intercom), search infrastructure (Elasticsearch), email delivery

(Postmark), payments and billing (Stripe, PayPal, Chargebee), content delivery and security (Cloudflare), developer tooling (LaunchDarkly), and sales CRM (HubSpot). These providers act on our documented instructions under a Data Processing Agreement that meets the requirements of Art. 28 GDPR. A current list of our sub-processors, including the countries in which each processes personal data, is available on request and in our Data Processing Agreement.

Corporate transactions. If Abusix is involved in a merger, acquisition, financing, reorganization, or sale of assets, personal data may be transferred as part of that transaction. We will notify affected individuals where required by law.

Legal and safety disclosures. We may disclose personal data to comply with applicable law, a lawful request from a public authority, a court order, or legal process; to enforce our Terms of Service; to protect our rights, property, or safety, or that of our customers or others; or to investigate fraud, abuse, or security incidents.

With your consent. We may share personal data in other ways if you have specifically asked us to or consented.

We do not share personal data with third parties for their own direct marketing purposes.

7. International Data Transfers

Abusix's primary processing operations take place in the **United States.** Personal data may also be processed in the EEA (for example, in Germany or the Netherlands) and in other jurisdictions where our sub-processors operate. Where Abusix GmbH (Germany) shares personal data with Abusix, Inc. (United States) as part of operating the Services, that transfer is treated as a restricted transfer and is subject to the safeguards below.

Where we transfer personal data from the EEA, the United Kingdom, or Switzerland to a country that has not received an adequacy decision, we put in place appropriate safeguards under Art. 46 GDPR, including:

- **EU Standard Contractual Clauses** (Commission Decision 2021/914), governed by Irish law, with all four modules incorporated as applicable in our Data Processing Agreement;
- the **UK International Data Transfer Addendum** for transfers subject to the UK GDPR;
- the **EU–US Data Privacy Framework** (and the UK Extension and Swiss–US bridge, where applicable) for transfers to certified US recipients; and
- supplementary technical and organizational measures, including encryption in transit, encryption at rest, and commitments regarding government access requests, as set out in our Data Processing Agreement.

A current list of our sub-processors, including the countries in which they process personal data, is available on request and is referenced in our Data Processing Agreement with customers. You can request a copy of the safeguards that apply to a specific transfer by contacting us at the address in Section 17.

8. How Long We Keep Personal Data

We keep personal data only for as long as necessary for the purposes described in this Policy, and in accordance with applicable law. The main retention periods are:

Data category	Retention period
Account and authentication data for active accounts	For the duration of the account relationship
Billing and tax records	**10 years** from the end of the calendar year in which the transaction occurred (§ 147 AO, § 257 HGB), or the equivalent period under applicable tax law
Service usage and audit logs	Up to **24 months** from the date of the log event
Site analytics data	Up to **14 months**
Marketing contact data (where based on consent)	Until you withdraw consent or object, and in any case no longer than **3 years** of inactivity
Marketing suppression list (to honor unsubscribe requests)	Indefinitely, as required to honor your opt-out
Support tickets and correspondence	**3 years** from closure of the ticket
Job applications (unsuccessful)	**6 months** from the decision, unless you consent to a longer period
Backup copies	Up to **180 days** after deletion from production systems, consistent with our standard backup rotation

8.1 Inactive Free Accounts

This section applies only to **free, non-paying accounts** — for example, self-service accounts used to request removal of an IP address from an Abusix blocklist. Accounts with an active paid subscription are not affected by this section; their retention is governed by the underlying subscription agreement.

A free account is considered **inactive** when, for a period of **12 consecutive months**, there has been: (i) no authenticated login by any user of the account, and (ii) no authenticated API activity under the account.

Please note: we do **not** send individual advance warnings before deleting inactive free accounts. This Policy is the notice. If you wish to keep your account and associated data, log in at least once every 12 months, or export your data at any time using the export tools available in the portal.

When a free account becomes inactive:

- **Account credentials, profile data, and associated configurations** will be deleted or irreversibly anonymized within **30 days** of the account being classified as inactive.
- **Delisting requests, IP reputation records, and other customer-submitted content** associated with the account will be deleted or irreversibly anonymized on the same schedule. Aggregated or anonymized statistics derived from that data (which no longer identify any individual) may be retained.
- **Backup copies** will be purged in line with our standard backup rotation (up to 180 days).
- **Data subject to a legal hold, investigation, or ongoing dispute** will be retained for the duration of that obligation and deleted promptly thereafter.

Deletion is irreversible. Once an account has been deleted, the data cannot be restored, and returning users will need to create a new account.

9. Your Rights

Subject to applicable law and certain exceptions, you have the following rights in relation to your personal data:

- **Right of access** — to obtain confirmation of whether we process your personal data and a copy of that data.
- **Right to rectification** — to have inaccurate or incomplete personal data corrected.
- **Right to erasure** ("right to be forgotten") — to have your personal data deleted in certain circumstances.
- **Right to restriction of processing** — to limit how we use your personal data in certain circumstances.
- **Right to object** — to object to processing based on our legitimate interests, and to object to direct marketing at any time.
- **Right to data portability** — to receive your personal data in a structured, commonly used, machine-readable format, or to have it transmitted to another controller, where technically feasible.
- **Right to withdraw consent** — where processing is based on your consent, you may withdraw it at any time without affecting the lawfulness of processing carried out before withdrawal.
- **Right not to be subject to automated decision-making** producing legal or similarly significant effects, except as permitted by law.
- **Right to lodge a complaint** with a data protection supervisory authority.

To exercise these rights, contact us at the address in Section 15. We will respond within **one month** of receipt of your request, extendable by up to two further months where the request is complex or where we have received a number of requests; we will notify you of any extension and the reasons for it.

Our lead supervisory authority is:

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg (LfDI BW) Lautenschlagerstraße 20, 70173 Stuttgart, Germany https://www.baden-wuerttemberg.datenschutz.de

You may also lodge a complaint with the supervisory authority in your country of residence or place of work.

10. Security

We maintain appropriate technical and organizational measures designed to protect personal data against unauthorized or unlawful processing and against accidental loss, destruction, damage, alteration, or disclosure. These include encryption of data in transit using TLS, encryption at rest for sensitive stores, access controls based on the principle of least privilege, network segmentation, logging and monitoring, regular vulnerability management, secure software development practices, and staff training. Abusix maintains a **SOC 2 Type II** attestation. Further information about our security program and related policies is available at https://abusix.com/security/ and in our trust center at https://trust.abusix.com.

In the event of a personal data breach likely to result in a risk to the rights and freedoms of natural persons, we will notify the competent supervisory authority without undue delay and, where feasible, within 72 hours, in accordance with Art. 33 GDPR. Where the breach is likely to result in a high risk, we will also notify affected individuals in accordance with Art. 34 GDPR.

11. Cookies and Similar Technologies

We use cookies and similar technologies (such as pixels and web beacons) on our Site. Some are strictly necessary for the Site to function; others are used for analytics, preferences, and marketing. Non-essential cookies are set only where you have given consent through our cookie banner, in line with § 25 TTDSG and the ePrivacy rules.

You can review and change your cookie preferences at any time via the "Cookie Settings" link in our footer. Full details of the cookies we use, including their purposes, providers, and durations, are set out in our separate Cookie Policy.

12. Marketing Communications

We send marketing communications only where you have given consent or where applicable law allows (for example, to existing business customers about similar products under § 7(3) UWG). Every marketing email contains an unsubscribe link, and you can opt out at any time by using that link or by contacting us. Opting out of marketing does not affect service-related communications (such as security notices and billing).

13. Children

Our Services are directed at business users and are not intended for individuals under the age of **16**. We do not knowingly collect personal data from children. If you believe a child has provided

us with personal data, please contact us and we will delete it promptly.

14. Automated Decision-Making

Certain parts of the Services use automated analysis — for example, heuristics and machine-learning models that classify IP addresses, domains, or messages as abusive. These classifications are tools provided to our customers, who decide how to act on them. They are not "decisions based solely on automated processing" producing legal or similarly significant effects on data subjects within the meaning of Art. 22 GDPR. If this changes, we will update this Policy and provide the information required by Art. 13(2)(f) GDPR.

15. US State Privacy Rights

If you are a resident of California, Virginia, Colorado, Connecticut, Utah, Texas, or another US state with a comprehensive privacy law, you may have additional rights regarding our processing of personal data, including rights to know, delete, correct, obtain a portable copy, and opt out of targeted advertising, "sales," and "sharing" (as those terms are defined under applicable law). We do not sell personal data for money, and we do not knowingly share personal data with third parties for cross-context behavioral advertising of our own Services; where we use analytics or advertising tags that may be considered a "sale" or "sharing" under California law, you can opt out via our cookie banner and the "Do Not Sell or Share My Personal Information" link in our footer. To exercise your rights, contact us at privacy@abusix.com. We will verify your request using reasonable means. You may designate an authorized agent to act on your behalf; we may require the agent to provide proof of authorization.

16. Changes to This Policy

We may update this Policy from time to time. If we make material changes, we will provide reasonable notice — for example, by posting a prominent notice on the Site or by emailing registered users before the change takes effect. The "Last Updated" date at the top of this Policy indicates when it was most recently revised. We encourage you to review this Policy periodically.

17. Contact Us

If you have questions, concerns, or requests regarding this Policy or our processing of your personal data, contact us:

Email: privacy@abusix.com **DPO:** dpo@abusix.com (GDPRlocal) **Postal:** Abusix GmbH, Roonstrasse 23a, 76137 Karlsruhe, Germany