Privacy Policy

EFFECTIVE 27 APRIL 2026 · VERSION 1.0

Red Hornet Pty Ltd (**"Red Hornet"**, **"we"**, **"us"** or **"our"**) is a specialist cyber intelligence and preparedness practice based in Victoria, Australia. We are committed to protecting the privacy of individuals whose personal information we hold and to handling that information in accordance with the *Privacy Act 1988* (Cth), the Australian Privacy Principles (APPs), the *Privacy and Data Protection Act 2014* (Vic) where applicable, and any other relevant Australian privacy laws.

> This Policy explains what personal information we collect, how we use and protect it, who we may share it with, and how you can access, correct or complain about our handling of it. By engaging with us — including via our website at **redhornet.dev** — you acknowledge the practices described below.

1. Scope

This Policy applies to personal information collected and held by Red Hornet in connection with:

- our website at redhornet.dev and any sub-domains we operate;
- our cyber threat intelligence, research, advisory and exercising services;
- our products and platforms, including *Seer* and *Firebreak*;
- email and other correspondence with prospective and existing clients, partners and contacts.

2. What is "personal information"?

"Personal information" has the meaning given in the *Privacy Act 1988* (Cth): information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information is true or not and whether recorded in a material form or not.

3. Information we collect

We collect only the personal information reasonably necessary for our functions and activities. Categories may include:

3.1 Information you provide directly

- **Contact details** — name, business email address, employer, role and phone number when you email us (including via contact@redhornet.dev) or otherwise correspond with us;
- **Engagement information** — details of your enquiry, project or proposed scope of work, and any background information you choose to share;
- **Contractual information** — billing contacts, signatories and authorised representatives of client organisations.

3.2 Information collected automatically

- **Server logs** — when you visit our website, our hosting provider may automatically log standard web request data such as IP address, browser user-agent, requested URL, referrer and timestamp for security, diagnostic and abuse-prevention purposes;
- **Cookies** — our website does not currently set tracking, advertising or analytics cookies. Strictly necessary cookies may be used by our hosting platform to support core site delivery;
- **Embedded content** — some pages embed third-party content (for example, YouTube videos and Google Fonts). Those providers may collect technical information about your device when the content is loaded. We do not control their collection.

3.3 Information collected from third parties

We may collect publicly available information about you or your organisation from open sources, business registers, professional networks (such as LinkedIn) and reputable threat intelligence sources, where this is relevant to a current or proposed engagement, due diligence, or to research and reporting we publish.

3.4 Sensitive information

We do not generally collect sensitive information (as defined in the Privacy Act). Where collection is unavoidable — for example, security clearance status relevant to an engagement — we will only collect it with your consent and where reasonably necessary.

4. How we use personal information

We use personal information for purposes connected with our business, including to:

- respond to enquiries and provide information about our services;
- scope, deliver, manage and invoice for advisory, intelligence, research and exercising engagements;
- operate our products and platforms (including Seer and Firebreak) and notify users of operational, security or service changes;
- conduct cyber threat research, produce intelligence reporting and warn affected parties;
- maintain the security and integrity of our systems and our clients' systems;
- meet our legal, regulatory, insurance, tax and professional obligations;
- improve our services, methodologies and website.

5. Disclosure of personal information

We do not sell personal information. We may disclose personal information to:

- **Service providers** — including cloud hosting, email, document management, communications and accounting providers who assist us in running our business under appropriate confidentiality and security obligations;
- **Clients and engagement counterparties** — where disclosure is necessary to deliver an engagement (for example, identifying an exercise participant or a contact within a client organisation);
- **Affected parties and law enforcement** — in limited circumstances during cyber threat research, where disclosure is necessary or appropriate to warn a victim, mitigate ongoing harm, or cooperate with a lawful investigation;
- **Professional advisers** — including legal, audit and insurance advisers;

- **Regulators and authorities** — where required or authorised by Australian law (for example, in response to a lawful subpoena, summons, or notice).

6. Overseas disclosure

Some of our service providers (for example, cloud hosting, communications and font delivery) may store or process information on servers located outside Australia, including in the United States, the European Union and the United Kingdom. Before disclosing personal information overseas we take reasonable steps to ensure recipients handle it consistently with the APPs, including by selecting providers with recognised security and privacy certifications and by entering into contractual protections where appropriate.

7. Direct marketing

We do not run mass marketing campaigns. From time to time we may contact existing business contacts directly with information about our services, research or events, in accordance with the *Spam Act 2003* (Cth). Every electronic marketing message will identify Red Hornet and provide a functional unsubscribe option. You can opt out at any time by emailing contact@redhornet.dev.

8. Security

As a cyber security practice, protecting information is core to what we do. We take reasonable steps, appropriate to the sensitivity of the information, to protect personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure. Measures include access controls, multi-factor authentication, encrypted storage and transport, principle-of-least-privilege provisioning, secure development practices, and supplier security assessment. No method of transmission or storage is perfectly secure, and we cannot guarantee absolute security.

9. Data retention

We retain personal information only for as long as it is reasonably required for the purposes for which it was collected, to meet our legal, regulatory and contractual obligations, or to defend or pursue legal claims. When personal information is no longer required, we take reasonable steps to destroy or de-identify it.

10. Notifiable data breaches

We comply with the Notifiable Data Breaches scheme established under Part IIIC of the *Privacy Act 1988* (Cth). Where a data breach involving personal information is likely to result in serious harm and the harm cannot be remediated, we will notify the Office of the Australian Information Commissioner (OAIC) and affected individuals as soon as practicable.

11. Your rights — access and correction

You may request access to the personal information we hold about you, and ask us to correct it if it is inaccurate, out of date, incomplete, irrelevant or misleading. We will respond within a reasonable period and will not charge you for making a request, although we may charge a reasonable cost-recovery fee for providing access in some circumstances. We may need to verify your identity before responding.

12. Complaints

If you believe we have breached the Australian Privacy Principles or any other applicable privacy law, please contact us using the details in section 14. We will acknowledge your complaint promptly, investigate it, and aim to provide a written response within 30 days.

If you are not satisfied with our response, you may refer the matter to:

- **Office of the Australian Information Commissioner (OAIC)** — www.oaic.gov.au · 1300 363 992;
- **Office of the Victorian Information Commissioner (OVIC)** — ovic.vic.gov.au, where the matter falls within its jurisdiction (for example, information handled on behalf of a Victorian public sector body).

13. Changes to this Policy

We may update this Policy from time to time to reflect changes in our practices, technology, legal requirements or other factors. The current version will always be available on our website, with the effective date shown at the top. Material changes will be highlighted where reasonably practicable.

14. Contact us

For privacy enquiries, access or correction requests, or to make a complaint, please contact our Privacy Officer:

ENTITY	Red Hornet Pty Ltd
ABN	29 696 894 434
ATTENTION	Privacy Officer
EMAIL	contact@redhornet.dev
POSTAL	By arrangement — please request via email
JURISDICTION	Victoria, Australia