

Cosive Privacy Policy

Last Updated: 06 August 2026

Cosive Pty Ltd and its subsidiaries (including Cosive New Zealand Limited), collectively referred to as "Cosive," "we," "us," or "our," are globally recognised leaders in Cyber Threat Intelligence & Security Operations. We are committed to protecting your privacy and providing quality services to you.

This Privacy Policy outlines our ongoing obligations to you in respect of how we manage your Personal Information. We adhere to the **Australian Privacy Act 1988 (Cth)** (the Privacy Act), the **New Zealand Privacy Act 2020**, and the **EU General Data Protection Regulation (GDPR)**.

1. What is Personal Information and Why Do We Collect It?

Personal Information is information or an opinion that identifies an individual. Examples of Personal Information we collect include: names, addresses, email addresses, phone, and facsimile numbers.

We collect your Personal Information for the primary purpose of:

- Providing our cybersecurity and intelligence services to you.
- Providing information and updates to our clients.
- Marketing and communicating relevant industry news.

We may also use your Personal Information for secondary purposes closely related to the primary purpose, in circumstances where you would reasonably expect such use or disclosure. You may unsubscribe from our mailing/marketing lists at any time by contacting us in writing or using the "unsubscribe" links provided in our communications.

2. How We Collect Your Information

Direct Collection: When we collect Personal Information directly from you, we will, where appropriate and possible, explain to you why we are collecting the information and how we plan to use it (in compliance with NZ IPP 3 and AU APP 5). This information is obtained in many ways, including correspondence, by telephone, by email, and via our website (www.cosive.com).

Indirect Collection (Third Parties): Where reasonable and practicable to do so, we will collect your Personal Information only from you. However, in some circumstances, we may be provided with information by third parties. In compliance with NZ IPP 3A and GDPR transparency requirements, if we collect your personal information from a source other than you, we will take reasonable steps to ensure that you are made aware of the information provided to us, the source of that information, and your rights regarding it.

3. Lawful Basis for Processing (GDPR Compliance)

If you are an individual residing in the European Economic Area (EEA), we collect and process your personal data only where we have a legal basis for doing so under the GDPR. Our legal bases include:

- **Contractual Necessity:** Where data processing is necessary to provide our services and fulfill our contract with you.
- **Legitimate Interests:** Where processing is necessary for our legitimate business interests, such as improving our services, provided those interests are not overridden by your fundamental rights.
- **Consent:** Where you have given us specific consent to use your personal information for a specific purpose (e.g., subscribing to our newsletter).
- **Legal Obligation:** Where we need to comply with a legal or regulatory requirement.

4. Sensitive Information

Sensitive information is defined to include information or opinion about such things as an individual's racial or ethnic origin, political opinions, membership of a political association, religious or philosophical beliefs, membership of a professional body, criminal record, or health information.

Sensitive information will be used by us only:

- For the primary purpose for which it was obtained.
- For a secondary purpose that is directly related to the primary purpose.
- With your explicit consent, or where required or authorised by law.

5. Disclosure of Personal Information

Your Personal Information may be disclosed in a number of circumstances, including the following:

- To third-party service providers (such as hosting or cloud infrastructure providers) who assist us in operating our business, provided they are bound by strict data processing agreements.
- Where you consent to the use or disclosure.
- Where required or authorised by law.

6. International Data Transfers

As an international cybersecurity business, your personal information may be transferred to, and stored at, a destination outside of your country of residence (including outside of Australia, New Zealand, or the EEA).

When transferring data across borders, we ensure strict compliance with:

- **GDPR:** Transfers outside the EEA are protected by appropriate safeguards, such as the European Commission's Standard Contractual Clauses or adequacy decisions.
- **New Zealand Privacy Act 2020 (IPP 12):** We ensure that any overseas recipient is subject to privacy safeguards that provide comparable protection to the NZ Privacy Act.
- **Australian Privacy Principles (APP 8):** We take reasonable steps to ensure the overseas recipient does not breach the Australian Privacy Principles.

7. Security and Retention of Personal Information

Your Personal Information is stored in a manner that reasonably protects it from misuse and loss and from unauthorised access, modification, or disclosure. We employ robust, industry-standard cybersecurity measures to protect your data.

In the event of a Notifiable Data Breach, we will comply with mandatory reporting requirements under the GDPR (within 72 hours), the Australian Privacy Act, and the NZ Privacy Act 2020, notifying the relevant supervisory authorities and affected individuals as required by law.

When your Personal Information is no longer needed for the purpose for which it was obtained, we will take reasonable steps to destroy or permanently de-identify your Personal Information. However, most Personal Information is or will be stored in client files which will be kept by us for a minimum of **7 years** for compliance and legal purposes.

8. Your Privacy Rights

Depending on your location, you have specific rights regarding your personal information:

- **Access and Correction (AU/NZ/GDPR):** You may access the Personal Information we hold about you and request that we update and/or correct it. We will take reasonable steps to make sure that your Personal Information is accurate, complete, and up-to-date.
- **Right to Erasure / "Right to be Forgotten" (GDPR):** You have the right to request that we delete your personal data.
- **Right to Restrict Processing (GDPR):** You can ask us to suspend the processing of your data.
- **Right to Data Portability (GDPR):** You can request a copy of your personal data in a machine-readable format to transfer to another provider.
- **Right to Object (GDPR):** You have the right to object to processing based on legitimate interests or direct marketing.

Cosive Pty Ltd will not charge any fee for your access request but may charge a reasonable administrative fee for providing a copy of your Personal Information where legally permitted. In order to protect your Personal Information, we may require additional identification from you before releasing the requested information.

9. Cookies and Website Tracking

Our website uses cookies to analyse site usage, improve our services, and give you the best experience. For users in the EU/EEA, we will only deploy non-essential cookies (such as analytics and marketing trackers) if we have obtained your explicit consent via our cookie consent banner. You may manage or withdraw your cookie preferences at any time.

10. Policy Updates

This Policy may change from time to time and the latest version will always be available on our website.

11. Privacy Policy Complaints and Enquiries

If you have any queries, wish to exercise your data rights, or have complaints about our Privacy Policy, please contact our Privacy Officer:

Cosive Pty Ltd Email: privacy@cosive.com

Address: 219 Lutwyche Road, Windsor QLD 4030, Australia

If you are not satisfied with our response to a complaint, you have the right to lodge a complaint with your local data protection authority, such as the Office of the Australian Information Commissioner (OAIC), the New Zealand Office of the Privacy Commissioner (OPC), or your relevant European Supervisory Authority.