Verify Assist

Privacy Policy

Garuda Corp Pty Ltd (ABN 67 680 372 543) trading as Verify Assist
Effective date: 27 June 2026 | Version 1.0

---

1. Introduction

Garuda Corp Pty Ltd (ABN 67 680 372 543), trading as Verify Assist (**we**, **us**, **our**), is committed to protecting the privacy of personal information. This Privacy Policy explains how we collect, hold, use and disclose personal information, and how we comply with the Privacy Act 1988 (Cth) (**Privacy Act**) and the Australian Privacy Principles (**APPs**).

This policy applies to our Website at www.verifyassist.com and to the Verify Assist platform, which provides KYC (Know Your Customer) and AML (Anti-Money Laundering) identity verification and screening services to business customers.

By using our Website or Service, you acknowledge this Privacy Policy. If you do not agree, please do not use our Website or Service.

2. Our role: when we are a collector and when we act for our customers

We collect personal information directly for our own purposes (for example, information about visitors to our Website and the staff of our business customers who administer accounts). In these cases we determine how that information is handled.

We also process personal information about **End Individuals** (the people our business customers verify) **on behalf of, and on the instructions of, those customers**. In that context, our business customer is generally responsible for obtaining the necessary consents and notifications from the End Individual. This policy describes our practices; the relevant business customer's own privacy policy will also apply to that processing.

3. What is personal and sensitive information

Personal information is information or an opinion about an identified individual, or an individual who is reasonably identifiable. **Sensitive information** is a subset of personal information that includes biometric information and biometric templates, and attracts higher protection under the APPs.

4. The kinds of information we collect and hold

Depending on how you interact with us, we may collect:

Website visitors and enquirers: name, business email, phone number, company, the content of your enquiry, and technical information such as IP address, device and browser type, and pages visited.

Customer account users: name, work contact details, job title, login credentials, and records of your use of the Service.

End Individuals (processed for our business customers): identity information such as full name, date of birth, residential address and nationality; government-issued identity document details and images (for example passport, driver licence or national ID); a photograph or "selfie"; **biometric facial-geometry data** derived from images for the purpose of liveness and face-

match checks; and the results of identity, sanctions, PEP (politically exposed person) and adverse-media screening.

Billing contacts: billing name, address and payment-related information (card payments are handled by our payment processors; we do not store full card numbers).

5. How we collect information

We collect personal information directly from you (for example when you complete a form, create an account, or contact us), automatically through cookies and analytics when you use our Website, and from our business customers and their End Individuals when KYC/AML Checks are performed through the Service. KYC/AML verification is performed using our technology partner, Sumsub, which collects and processes identity and biometric data on our and our customers' behalf.

Where it is reasonable and practicable, we collect personal information directly from the individual concerned. In the KYC context, much of the End Individual information is provided by, or collected at the direction of, our business customer.

6. Why we collect, hold, use and disclose information

We collect and use personal information to:

- provide, operate, maintain and improve the Website and Service;
- perform identity verification and KYC/AML screening on behalf of our business customers;
- create and manage accounts, authenticate users, and provide support;
- process payments and manage our customer relationships;
- detect, investigate and prevent fraud, security incidents and misuse;
- comply with our legal and regulatory obligations and respond to lawful requests; and
- communicate with you, including about service, security and (where permitted) marketing.

7. Sensitive and biometric information

KYC/AML Checks may involve sensitive information, including biometric facial-geometry data extracted from identity documents and selfies for liveness detection and face matching. We (and Sumsub) use this biometric data only for the purpose of identity verification and fraud prevention, and we do not use it for any unrelated purpose.

Under the APPs, sensitive information is generally collected only with consent. For End Individuals, the relevant business customer is responsible for obtaining that consent before the check is performed. We retain biometric data only for as long as necessary for the verification purpose and applicable legal retention obligations, after which it is securely deleted or de-identified.

8. Disclosure of personal information

We may disclose personal information to:

- **our business customers**, in respect of the End Individuals they ask us to verify;
- **Sumsub** and other service providers (such as hosting, identity-data, sanctions/PEP data, analytics and payment providers) who help us deliver the Service, under obligations of confidentiality and security;
- professional advisers, auditors and insurers;
- regulators, law enforcement and other parties where required or authorised by law; and

- a successor entity in connection with a business sale or restructure.

We do not sell personal information.

9. Overseas disclosure

Some of our service providers, including Sumsub and certain cloud-hosting and identity-data providers, are located or store data outside Australia. As a result, personal information may be disclosed to, or accessible from, overseas recipients.

The countries in which recipients are likely to be located include the **United Kingdom, the European Union (including Germany and Cyprus), and the United States** [recipients and countries to confirm against your current Sumsub and hosting configuration]. Before disclosing personal information overseas, we take reasonable steps to ensure recipients handle it consistently with the APPs, including through contractual safeguards.

10. Security of personal information

We take reasonable steps to protect personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure. These steps include encryption in transit and at rest, access controls, network security, staff confidentiality obligations, and the use of reputable, security-certified service providers. No system is completely secure, and we cannot guarantee absolute security.

11. Data retention

We hold personal information only for as long as necessary for the purposes for which it was collected, to provide the Service to our business customers, and to meet legal, regulatory and record-keeping obligations. Most personal information held in our client files and records is kept for a maximum of 7 years to fulfil our record-keeping obligations, including those that apply to AML/CTF records. When information is no longer required, we take reasonable steps to destroy, anonymise or de-identify it.

12. Direct marketing

We may use your business contact details to send you information about our products and services. You can opt out at any time using the unsubscribe link in our communications or by contacting us. We do not use End Individual KYC data for marketing.

13. Cookies and website analytics

Our Website uses cookies and similar technologies to operate the site, remember your preferences, and understand how the site is used. You can control cookies through your browser settings, although disabling some cookies may affect Website functionality. We may use analytics tools that collect usage information in aggregate.

14. 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 or misleading. We will respond within a reasonable time and may need to verify your identity. There is generally no charge to make a request, although we may charge a reasonable cost for access in some cases. If we refuse access or correction, we will explain why in writing.

If you are an End Individual whose information was processed for one of our business customers, please direct your request to that customer in the first instance; we will assist them as their service provider.

15. Automated processing

Identity verification and screening involve automated processing (for example, automated document checks and face matching). These outputs are designed to support, not replace, a human decision by our business customer, who remains responsible for any onboarding or compliance decision affecting an End Individual. [Note: from 10 December 2026, additional APP transparency requirements apply to certain automated decisions — to be reviewed and updated before that date.]

16. Complaints

If you believe we have breached the APPs or mishandled your personal information, please contact our Privacy Officer at privacy@verifyassist.com. We will acknowledge your complaint, investigate, and respond within a reasonable time (usually 30 days).

If you are not satisfied with our response, you may complain to the Office of the Australian Information Commissioner (OAIC) at www.oaic.gov.au, by phone on 1300 363 992, or by writing to GPO Box 5288, Sydney NSW 2001.

17. Notifiable data breaches

We comply with the Notifiable Data Breaches scheme under the Privacy Act. If an eligible data breach occurs that is likely to result in serious harm, we will notify affected individuals and the OAIC as required by law.

18. European data protection (GDPR)

In some circumstances, the European Union General Data Protection Regulation (GDPR) provides additional protection to individuals located in Europe. The fact that an individual may be located in Europe does not, on its own, mean the GDPR applies. Our Website and Service are not specifically directed at individuals in the European Union, and we do not monitor the behaviour of individuals in the European Union; accordingly, we do not consider the GDPR to apply to our handling of personal information. The use of service providers with infrastructure located in the European Union (such as Sumsub) does not change this position.

19. Changes to this policy

We may update this Privacy Policy from time to time. The current version is published on our Website with its effective date. This policy was last updated on 27 June 2026.

20. Contact us

Privacy Officer — Garuda Corp Pty Ltd (ABN 67 680 372 543) trading as Verify Assist

Registered address: Suite 200, 610 Burwood Road, Hawthorn East VIC 3123, Australia

Email: privacy@verifyassist.com

Website: www.verifyassist.com