Privacy Policy for Makesure

Updated 01 October 2025

If you are under 18 years old, it is highly recommended to seek help from a parent, guardian or responsible adult to set up your RatifyID Digital Identity.

Makesure Consulting Pty Ltd (ABN 35 168 163 666) ("Makesure" "we," "us") is bound by the Privacy Act 1988 (Cth) and the Privacy Act 2020 (NZ) ("Privacy Laws") and takes its privacy obligations very seriously. We comply with the Australian Privacy Principles, the Australian Notifiable Data Breaches scheme and the Information Privacy Principles (NZ). This policy sets out how we manage your personal information and applies to all individuals who have dealings with us, either through our websites, our software or otherwise.

This privacy policy applies to RatifyID offered by Makesure.

At Makesure, we respect your privacy and are committed to protecting your personal information. This Privacy Policy sets out how we collect, hold, use, store, and disclose your personal and sensitive information. We may change our Privacy Policy from time to time by publishing changes to it on our website. We encourage you to check our website periodically to ensure that you are aware of our current Privacy Policy.

What personal and sensitive information do we collect and hold?

We may collect and hold the following types of personal information and sensitive information:

- Name
- Mailing or street address
- Email address
- Telephone number
- Age or date of birth
- Nationality
- Government-related identifiers, such as your license number and class, Medicare number, state or national ID card number, passport number, and birth or marriage certificate number
- Indicators of fraudulent activity
- Other information identifiable from scanned ID documents you provide, or images of your face.

- Biometric information, such as templates we create from video footage or photographs of your face.
- Information obtained from fraud-prevention services and document verification services.
- Your device ID, device type, geo-location information, computer and connection information, IP address and standard web log information
- Behavioural information associated with usage of our app
- Any additional information relating to you that you provide to us directly through our website or apps or indirectly through your use of our website or apps or online presence or through other websites or accounts from which you permit us to collect information.
- Information you provide to us through client or customer surveys; and
- Any other personal information that may be required to facilitate your dealings with us.

How do we collect your personal and sensitive information?

We may collect these types of personal or sensitive information either directly from you or from third parties. We may collect this information when you:

- Utilize one of our verification services through one of our apps or web-based platforms.
- If you are a representative of one of our partners or clients, create an administrator account or otherwise use one of our apps or web-based platforms on behalf of one of our partners or clients.
- Communicate with us through correspondence, chats, email, or otherwise through our website; or
- Otherwise interact with our sites, services, content, or advertising

When you use our verification services, we automatically receive and record certain information from your computer (or other device) and/or your web browser.

Why do we collect, hold, use and disclose personal and sensitive information?

The purposes for which we will use personal and sensitive information will depend on the relationship with you and the products or services you require from us. We may collect, hold, use and disclose your personal and sensitive information for the following purposes:

- To enable you to access and use our website or apps.

- To provide verification services, where you are seeking to access one of our clients' products or services (or the products or services of third parties, where our clients act as brokers, resellers, referrers, or representatives of such parties)
- To prevent fraudulent behavior being undertaken on our products
- To operate, protect, improve and optimize our website or apps, business and our clients' and users' experience, such as to perform analytics, conduct research and create new products. We use synthetic data or information about the characteristics of documents (with no personal data) to train our algorithms. We do not use your personal data or biometric data to train the algorithms.
- To improve our systems, and assist in fraud detection we may use your behavioral information. We do not use your behavioural information to train the algorithms or sell to third parties.
- To send you service, support and administrative messages, reminders, technical notices, updates, security alerts in connection with our verification services, and information requested by you.
- To comply with our legal obligations, resolve any disputes that we may have with any of our clients or users, and enforce our agreements with third parties
- To authenticate and bind your identity to your identity we will use an acquired biometric with your consent. The acquired biometric will be stored until you revoke the consent for authentication purposes

Collection and Disclosure of Biometrics

In the context of biometric data collection and disclosure, RatifyID follows Digital ID bill guidelines to protect individual privacy and security.

- Ensure Express Consent is obtained from an Individual prior to collecting, using, or disclosing that Individual's Biometric Information.
- RatifyID will not collect, use or disclose an Individual Biometric information unless as an credential service provider
- Biometric information will be destroyed if collected with the Express Consent of an Individual for the purpose of authenticating that Individual to their Digital Identity, immediately after the consent is withdrawn
- Ensure destruction or retention of all collected Biometric Information, including all copies, caches, and intermediary databases, including any subcontracted or third-party components

- When destroying Biometric Information, create and maintain a record that the destruction of Biometric Information has occurred.
- RatifyID will not use a Biometric Matching algorithm to perform one-to-many matching

Other circumstances where we may disclose your personal or sensitive information

- Business Transactions: If we are involved in a merger, acquisition or asset sale, your personal and sensitive information may be transferred. We will endeavour to provide notice before your personal and sensitive information is transferred and becomes subject to a different Privacy Policy.
- To detect, manage and investigate Digital Identity Fraud Incidents or other fraudulent activity
- Law enforcement: Under certain circumstances, we may be required to disclose your personal and sensitive information if required to do so by law or in response to valid requests by public authorities (e.g., A Commonwealth, state or territory court or a government agency).
- Other legal requirements: We may disclose your personal and sensitive information in the good faith belief that such action is necessary to comply with a legal obligation, protect and defend the rights or property of the Company, prevent, or investigate possible wrongdoing in connection with our services, protect the personal safety of users of the services or the public, or protect against legal liability.

Do we use your personal information for direct marketing?

If we use your personal information for direct marketing of our services, we will ensure we comply with our obligations under relevant laws including having your consent to do so.

We do not use personal information collected as part of our identity verification services for marketing purposes and we do not sell any of your data to any third party. We do not use or disclose Personal information for direct marketing purposes including:

1. offering to supply goods or services;
2. advertising or promoting goods or services;
3. enabling another entity to offer to supply goods or services;
4. enabling another entity to advertise or promote goods or services; or
5. market research.

This requirement does not apply to the disclosure of Personal Information if:

6. the information is disclosed for the purposes of offering to supply services or advertising or promoting credential services to provide to an Individual; and
7. the individual about whom the information is disclosed has expressly consented to the disclosure and receiving communications for purposes permitted by paragraph (f)

To whom do we disclose your personal information?

We may disclose personal information (but not sensitive or biometric data) for the purposes described in this Privacy Policy to:

1. Our clients and third parties, where you are seeking to access their products and/or services and are required to verify your identity in order to do so. We do not sell any of your data to any third party.
2. Our employees and contractors, for the purposes of managing our products and systems and providing our services
3. Third-party suppliers and service providers (including providers of document verification services to help us verify the validity of identity documents you disclose to us, and other providers for the operation of our websites and/or our business or in connection with providing our products and services to you)
4. Specific third parties authorized by you to receive information held by us,
5. Compliance with court orders and other legal obligations and regulatory requirements; in
    1. The investigation, resolution and defense of complaints and legal claims;
    2. Other persons, including government agencies, regulatory bodies, and law enforcement agencies, or as required, authorized, or permitted by law
    3. As otherwise required or permitted by law
    4. Any insurance claim that legally requires disclosure of your personal information.

Overseas transfer of personal and sensitive information

We may disclose your information to overseas recipients for specific purposes.

The developers who service our websites and may have access to personal information are based in Romania. Otherwise, we will not disclose user personal information to overseas recipients. Obligations under the contract between the parties identify the responsibility in regarding to protecting personal information in their possession against

misuse or loss, in agreeing to the obligations under the privacy act 1988 (Cth) section 16C of the Privacy Act (Cth), Australian Privacy Principle 8.1 and chapter 1 of the App Guidelines.

In addition, Personal Information will not be transferred or stored overseas. All Ratify ID will be stored in Australia including any backups. The personal information will not leave the Ratify ID server and the access to the server is strictly under RatifyID control which can choose at any time to restrict access.

Security and storage

Your information will be stored on a secure database which has restricted access to only those personnel that need to have access to this information. Access to our computer environment is through a secure login environment and all efforts have been made to ensure that it cannot be accessed by unauthorized personnel.

At any time at your request, we will destroy your personal information. We will do this for any lawful request, provided it is in writing. In our RatifyID application, you can delete your own personal information. Otherwise, we will delete personal information as required by the relevant Privacy Laws.

The development team is certified to ISO27000 in relation to information security standards, and we have taken reasonable steps to ensure that Next Logic does not breach the Privacy Laws.

Unsolicited personal and sensitive information

There may be circumstances where an individual provides us with personal or sensitive information about another person. Where we receive unsolicited personal information which we do not require for the purposes we have outlined above, we will destroy or de-identify that information as soon as practicable (if it is lawful and reasonable to do so).

Accessing and correcting your information

You may ask to access the personal information we hold about you and we will respond to your request as soon as reasonably practicable and in any event within 20 working days.

We will give you access to your personal information unless we are entitled to refuse under the relevant Privacy Laws, in which case we will provide you with a written notice setting out, among other things, the reasons for the refusal.

You may ask us to amend the information if it is not accurate, complete, or up to date and we will respond to your request within the time frames stated above. If we refuse to amend the information:

- We will provide you with a written notice setting out, among other things, the reasons for that refusal; and
- You may ask us to attach a note to the information indicating what you think is inaccurate, incomplete, or out of date or misleading and we will respond to that request as soon as reasonably practical.

If you wish to exercise your rights of access and correction, please contact us using the details provided below. In some cases, we may impose a moderate and reasonable charge for providing access to personal information. We will not charge you simply because you lodge a request for access.

Lodging Your Request to Access or Correct Your Personal Information:

To lodge a request to access or correct your personal information, please provide:

- Your name and contact information.
- Information to verify your identity. This is to ensure that the information is being provided to the correct person. RatifyID may request additional identification documents or information to confirm your identity.
- If you are acting on behalf of another person on whom RatifyID holds personal information, you must provide information to demonstrate that you are authorized to make the request on their behalf, for example, as a legal guardian or authorized agent.
- What personal information you would like to access and/or correct.
- You can submit your request through one of the following methods:
- Email: privacy@makesure.com.au
- Postal Mail: Ratify ID 26-36 High Street Northcote, Victoria 3070

Obtaining consent

By providing your consent through RatifyID, you allow the collection, use, and disclosure of your attributes and Biometric Information for Identity Proofing and Digital Identity authentication purposes. You have the option to give express consent on a one-time basis or provide enduring express consent. Enduring express consent can be withdrawn or modified at any time by adjusting settings in your RatifyID profile or contacting info@makesure.com.au.

If you choose not to provide enduring express consent, you will be asked for express consent each time your attributes or Biometric Information needs to be disclosed. If you

decline to provide either form of consent, RatifyID won't be able to perform Identity Proofing or authenticate your Digital Identity.

It's important to note that alternative methods of identity verification exist outside of RatifyID, such as manually providing identity documents to a third party.

Complaints About a Breach of Privacy

If you believe that we have breached privacy laws or wish to make a complaint about the way we have handled your personal information in our Identity System, please contact us using the details below or alternatively complete this compliant form. We will investigate your complaint and respond to you promptly. If you are not satisfied with our response, you may lodge a complaint with the Office of the Australian Information Commissioner.

Contact Us

If you have any questions or concerns about this Privacy Policy or our privacy practices in relation to our Identity System, please contact us at:

Privacy Officer
Email: privacy@makesure.com.au
Address: 5/26-36 High Street Northcote Vic 3070
Effective Date: 23 May 2023

Amendments to this Policy

This privacy policy will be reviewed annually and updated as required by the Privacy Officer of Ratify ID.

We reserve the right to change this Privacy Policy at any time by posting revisions on our web page. Such changes will be effective upon posting and the current version published on our website shall apply.

Please revisit this page to stay aware of any changes. If the Privacy Policy is part of an agreement with you, we will notify you by e-mail or other appropriate means in case of an amendment. In some cases, we may require you to acknowledge our Privacy Policy before using our app.