PRIVACY POLICY

Effective Date: 26th May 2025
Last Updated: 26th May 2025
Version: 2.0

OVERVIEW

HaloMap (ACN 682391171) ("**we**", "**us**", "**our**", or "**HaloMap**") is committed to protecting your privacy and handling your personal information in accordance with Australian privacy laws. This Privacy Policy explains how we collect, use, disclose, and protect your personal information when you:

- Visit our website at https://halomap.io
- Use our HaloMap software platform and services
- Participate in our pilot program
- Contact us or engage with our services

Important: This Privacy Policy applies to both our website and software platform. By using either, you agree to the practices described in this policy.

---

1. WHO WE ARE AND HOW TO CONTACT US

1.1 About HaloMap

HaloMap is an Australian company that provides cloud based business process management platform. Our platform helps organisations map, manage, analyse, and optimise their business processes through our web-based application. We are bound by the Privacy Act 1988 (Cth) and the Australian Privacy Principles (APPs).

1.2 Contact Information

Privacy Officer: Kylie Pedler-Jones (Head of Operations)
Email: kylie@halomap.io
General Enquiries: kylie@halomap.io
Postal Address: 81-83 Campbell Street SURRY HILLS NSW 2010
Phone: 0400 953 189

1.3 Privacy Complaints

For privacy complaints or concerns, contact our Privacy Officer at kylie@halomap.io or use the contact details above.

---

2. WHAT PERSONAL INFORMATION WE COLLECT

2.1 Information We Collect Directly From You

When you use our website or software platform, we may collect:

Account and Contact Information:

- Name, email address, phone number

- Company name and position
- Postal address
- Login credentials and authentication information

Technical and Usage Information:

- IP address, device identifiers, browser type
- Operating system and device information
- Pages visited, time spent, and navigation patterns
- Software usage data and feature utilisation
- Error logs and performance data

Content and Data You Provide:

- Information you upload, store, or process through our platform
- Communications with us (emails, chat messages, support requests)
- Feedback, surveys, and evaluation responses
- Payment and billing information (if applicable)

2.2 Information We Collect Automatically

We use cookies and similar technologies to collect:

- Session information and preferences
- Analytics data about website and software usage
- Technical performance and error reporting data

Analytics and Optimisation Information:

- Session information and preferences
- Analytics data about website and software usage
- Technical performance and error reporting data

Cookie Types:

- **Essential cookies:** Required for website/platform functionality
- **Analytics cookies:** Help us understand how you use our services
- **Preference cookies:** Remember your settings and choices

You can manage cookies through your browser settings, but disabling essential cookies may affect functionality.

2.3 Information From Third Parties

We may receive information from:

- Business partners or referral sources
- Third-party authentication services (if you choose to use them)
- Publicly available sources for business verification

2.4 Sensitive Information

We generally do not collect sensitive information (as defined by the Privacy Act). If we need to collect sensitive information for specific purposes, we will:

- Obtain your explicit consent
- Only use it for the specific purpose disclosed
- Apply additional security measures

---

3. HOW WE USE YOUR PERSONAL INFORMATION

3.1 Primary Purposes

We use your personal information to:

Provide Our Services:

- Create and manage your account
- Deliver our software platform and related services
- Process pilot program applications and participation
- Provide technical support and customer service
- Process payments and manage billing

Analyse and Improve Our Services:

- Analyse usage patterns and user behaviour
- Develop new features and improve existing ones
- Conduct research and development
- Perform quality assurance and testing
- Create de-identified industry datasets for analytics and insights

Research and Development:

- Aggregate and analyse de-identified data to develop industry insights
- Create predictive models and analytics tools for industry benchmarking
- Develop industry-specific recommendations and best practices
- Improve our algorithms and machine learning capabilities

Communicate With You:

- Send service-related notifications and updates
- Respond to your enquiries and requests
- Provide product updates and security alerts

3.2 Secondary Purposes

With your consent or as permitted by law, we may use your information for:

Business Development and Industry Insights:

- Provide industry benchmarking and analytics services
- Develop market research and industry reports
- Create predictive models for industry trends
- Offer comparative analytics to help improve industry practices

Marketing and Communications:

- Send marketing communications about our products and services
- Invite you to events, webinars, or product demonstrations
- Conduct market research and surveys

Legal and Compliance:

- Comply with legal obligations and regulatory requirements
- Protect our rights and investigate security incidents
- Enforce our terms of service and agreements

3.3 De-identified Data for Industry Insights

What We Do: We may use de-identified and aggregated data from our platform to:

- Create industry benchmarks and performance metrics
- Develop predictive analytics and trend analysis
- Provide comparative insights to help organisations improve
- Build machine learning models for better service delivery
- Generate industry reports and market intelligence

How We Protect Your Privacy:

- **Complete De-identification:** All personal identifiers are permanently removed
- **Aggregation:** Data is combined from multiple users so no individual organisation can be identified
- **Statistical Disclosure Control:** We apply techniques to prevent re-identification
- **Minimum Dataset Size:** We only create insights when we have sufficient data to ensure anonymity
- **No Reverse Engineering:** The de-identified data cannot be used to identify specific users or organisations

Your Benefits:

- Industry benchmarking to understand your performance relative to peers
- Predictive insights to help improve your operations
- Access to anonymised industry trends and best practices
- Enhanced platform features powered by collective intelligence

We may use automated systems for: **Optimise Platform Performance:**

- User authentication and security monitoring
- Platform performance optimisation

- Basic data processing and analysis

Important: We do not use fully automated decision-making that significantly affects your rights. Any automated processes include human oversight and review.

---

4. HOW WE SHARE YOUR PERSONAL INFORMATION

4.1 We Do Not Sell Your Information

We do not sell, rent, or trade your personal information to third parties for their commercial purposes.

4.2 When We May Share Information

We may disclose your personal information to:

Service Providers:

- Cloud hosting and infrastructure providers
- IT support and maintenance services
- Payment processing and billing services
- Analytics and monitoring tools
- Customer support platforms

Industry Analytics Partners:

- Research institutions and industry bodies
- Anonymous benchmarking service providers
- De-identified data analytics platforms

Business Purposes:

- Professional advisors (lawyers, accountants, consultants)
- In connection with business transfers or mergers
- To protect our legal rights or investigate security incidents

Legal Requirements:

- Government agencies when required by law
- Courts or tribunals in response to subpoenas
- Law enforcement for investigations
- Regulatory bodies as required

4.3 Service Provider Protections

Our service providers must:

- Only use your information to provide services to us
- Implement appropriate security measures
- Not use your information for their own purposes
- Comply with applicable privacy laws

5. INTERNATIONAL DATA TRANSFERS

5.1 Where Your Data May Be Stored

Your personal information may be stored and processed in:

- Australia

5.2 Overseas Transfer Protections

When we transfer personal information overseas, we ensure protection through:

- **Adequate Countries:** We only transfer to countries recognised as providing adequate protection
- **Contractual Safeguards:** Standard contractual clauses approved by privacy regulators
- **Your Consent:** Where you have explicitly agreed to overseas transfers

5.3 Cloud Services

We use cloud services that may store data in multiple jurisdictions. All cloud providers must meet our security and privacy requirements.

---

6. HOW WE PROTECT YOUR INFORMATION

6.1 Technical Measures

We implement industry-standard security measures including:

- **Encryption:** Data encryption in transit and at rest
- **Access Controls:** Role-based access with multi-factor authentication
- **Network Security:** Firewalls, intrusion detection, and monitoring
- **Secure Hosting:** Professional grade cloud hosting with security certifications
- **Regular Updates:** Security patches and system updates

6.2 Organisational Measures

We maintain robust organisational security through:

- **Staff Training:** Privacy and security training for all personnel
- **Access Policies:** Strict need to know access principles
- **Incident Response:** Documented breach response procedures
- **Reviews:** Security assessments and audits
- **Privacy by Design:** Building privacy into all new systems and processes

6.3 Data Retention

We retain your personal information only as long as necessary for:

- The purposes for which it was collected
- Legal and regulatory requirements
- Legitimate business purposes

Standard Retention Periods:

- Account information: 7 years after account closure
- Usage and analytics data: 3 years
- Support communications: 7 years
- Financial records: 7 years

When information is no longer needed, we securely delete or de-identify it.

---

7. YOUR PRIVACY RIGHTS

7.1 Access Rights (APP 12)

You can request access to the personal information we hold about you, including:

- What information we have
- How we collected it
- How we use and disclose it
- Who we share it with

7.2 Correction Rights (APP 13)

You can request correction of personal information that is:

- Inaccurate, out of date, incomplete, or misleading
- Not relevant to our purposes

7.3 Additional Rights

Depending on circumstances, you may also request:

- **Erasure/Deletion:** Removal of your personal information
- **Data Portability:** Transfer of your data in a structured format
- **Restriction:** Limiting how we process your information
- **Objection:** Objecting to certain uses of your information

7.4 Marketing Opt-Out

You can opt out of marketing communications by:

- Clicking unsubscribe links in our emails
- Contacting our Privacy Officer
- Updating your account preferences

7.5 How to Exercise Your Rights

To exercise your privacy rights:

1. Email our Privacy Officer at kylie@halomap.io
2. Provide sufficient detail to identify yourself and your request
3. We will respond within 30 days (or as required by law)

4. Some requests may require identity verification

7.6 No Cost for Reasonable Requests

We don't charge for reasonable requests, but may charge for:

- Excessive or repetitive requests
- Requests requiring significant resources
- Provision of additional copies

---

8. DATA BREACH NOTIFICATION

8.1 Our Commitment

We take data security seriously and have procedures in place to handle potential data breaches.

8.2 What We Do If a Breach Occurs

If we experience a data breach that is likely to result in serious harm:

- We will assess the breach within 72 hours
- Notify the Office of the Australian Information Commissioner (OAIC)
- Notify affected individuals as soon as practicable
- Take steps to contain and remediate the breach

8.3 What You Should Do

If you believe your personal information has been compromised:

- Contact us immediately at kylie@halomap.io
- Change your account passwords
- Monitor your accounts for unusual activity

---

9. CHILDREN'S PRIVACY

9.1 Age Requirements

Our services are not intended for children under 18. We do not knowingly collect personal information from children under 18 without parental consent.

9.2 If We Learn of Child Information

If we discover we have collected information from a child under 18:

- We will delete the information promptly
- We will not use the information for any purpose
- We will implement additional safeguards if needed

---

10. UPDATES TO THIS POLICY

10.1 Policy Changes

We may update this Privacy Policy to reflect:

- Changes in Australian privacy laws
- New features or services we offer
- Changes in our business practices
- Feedback from users or regulators

10.2 How We Notify You

When we make material changes:

- We will update the "Last Updated" date
- We will notify active users by email
- Continued use constitutes acceptance of changes

---

11. COMPLAINTS AND DISPUTES

11.1 Internal Complaints Process

If you have concerns about our privacy practices:

1. **Contact Us:** Email kylie@halomap.io with details of your concern
2. **Investigation:** We will investigate your complaint within 30 days
3. **Response:** We will provide a written response with our findings
4. **Resolution:** If justified, we will take corrective action

11.2 External Complaints

If you're not satisfied with our response, you can complain to:

Office of the Australian Information Commissioner (OAIC)

- Website: www.oaic.gov.au
- Phone: 1300 363 992
- Email: enquiries@oaic.gov.au
- Post: GPO Box 5218, Sydney NSW 2001

---

12. LEGAL BASIS AND COMPLIANCE

12.1 Australian Privacy Act Compliance

This Privacy Policy is designed to comply with:

- Privacy Act 1988 (Cth) and its amendments
- Australian Privacy Principles (APPs)
- Privacy and Other Legislation Amendment Act 2024
- Notifiable Data Breaches scheme

12.2 Other Applicable Laws

We also comply with relevant laws including:

- Competition and Consumer Act 2010 (Cth)
- Corporations Act 2001 (Cth)
- Spam Act 2003 (Cth)
- Telecommunications Act 1997 (Cth)

---

13. DEFINITIONS

Australian Privacy Principles (APPs): The 13 principles in the Privacy Act that govern how we handle personal information.

De-identification: The process of removing or altering information so that individuals cannot be reasonably identified.

Personal Information: Information or an opinion about an identified individual, or an individual who is reasonably identifiable.

Sensitive Information: Personal information about racial/ethnic origin, political opinions, religious beliefs, health information, criminal records, or biometric information.

This Privacy Policy was last updated on 26th May 2025 and reflects current Australian privacy law requirements including the Privacy and Other Legislation Amendment Act 2024.

For questions about this Privacy Policy or our privacy practices, contact our Privacy Officer at kylie@halomap.io