Global Privacy Policy

FLAIM Systems Pty Ltd | ABN 71 620 462 946 | Document P-10-003 | November 2026

1. About this policy

1.1 Who we are. This Global Privacy Policy applies to FLAIM Systems Pty Ltd (ABN 71 620 462 946) of 337 Moray Street, South Melbourne, VIC, 3205, Australia (**FLAIM, we, us, our**). We are committed to protecting your privacy and to handling your personal information openly and transparently.

1.2 Scope. This policy explains how we collect, use, hold, disclose and otherwise handle personal information about our customers, prospective customers, authorised resellers of our products and services **(Authorised Resellers),** suppliers, website visitors and other people who deal with us, including through our website, our FLAIM XR training systems (**Systems**), the FLAIM Scenario Library and the FLAIM Capture learning analytics platform (**FLAIM Capture**). Clause 9 explains how we handle personal information that we process on behalf of our customers.

1.3 Applicable Data Protection Laws. We handle personal information in accordance with the Australian *Privacy Act 1988* (Cth) and the Australian Privacy Principles (**Privacy Act**), and with the other privacy and data protection laws that apply to us in the countries where we operate or where you are located (**Applicable Data Protection Laws**). Depending on where you are, these may include the EU General Data Protection Regulation (**EU GDPR**), the UK General Data Protection Regulation and *Data Protection Act 2018* (**UK GDPR**), the California Consumer Privacy Act (**CCPA**) and other US state privacy laws, the New Zealand *Privacy Act 2020*, the Canadian *Personal Information Protection and Electronic Documents Act* (**PIPEDA**), the Singapore *Personal Data Protection Act 2012* (**PDPA**) and similar laws. Where a local law gives you greater protection than this policy, that law prevails.

1.4 Controller. For the purposes of the EU GDPR and UK GDPR, FLAIM is the controller of the personal information described in this policy, except where clause 9 applies.

2. Personal information we collect

2.1 Meaning of personal information. Personal information means information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether or not the information or opinion is true. It includes "personal data" and "personal information" as defined in Applicable Data Protection Laws.

2.2 Information you give us. We collect personal information when you request a quote, place or manage an order, register a System, use our support services, attend training or events, subscribe to updates, apply to become an Authorised Reseller, call or email us, or visit our website. This may include your name, job title, organisation, contact details, billing and delivery details, purchase and System registration history, communications with us, and details of any enquiries, support requests or complaints you make.

2.3 Website and technical information. When you visit our website, we and our analytics providers, such as Google Analytics, collect information about how you access, use and interact with it. This may include the site from which you came to our website, the pages you visit, your IP address and approximate location, the type and attributes of the device you use, and your browser type, language and operating system.

2.4 System and usage data. When a System is used, we may collect technical, performance and usage data, such as device identifiers, software version, error logs and usage statistics. We use this data to support, secure and improve our products and, where practicable, we use it in de-identified or aggregated form.

2.5 Information from third parties. We may collect personal information about you from: (a) Authorised Resellers; (b) contractors and product champions authorised to represent us or to deliver services on our behalf; (c) your employer or organisation; and (d) publicly available sources, such as business networking sites. Where we collect personal information from a third party, we will take reasonable steps to make you aware of that collection where required by Applicable Data Protection Laws.

2.6 Sensitive information. We do not seek to collect sensitive information, such as information about your health, biometric information, racial or ethnic origin, or criminal record. If we need to collect sensitive information, we will do so only with your consent or as otherwise permitted by Applicable Data Protection Laws.

2.7 Children. Our website and services are directed to businesses and organisations, not to children. We do not knowingly collect personal information directly from children under 16. Where a customer allows a person aged 14 to 17 to use a System, the customer is responsible for obtaining any parental or guardian consent required by law. If you believe we hold a child's personal information without appropriate consent, please contact us and we will delete it.

2.8 Anonymity. Where it is lawful and practicable, you may deal with us anonymously or by using a pseudonym, for example when making a general enquiry. We will usually need your name and contact details to supply products or services to you.

2.9 If you do not provide information. If you do not provide the personal information we request, we may not be able to supply our products or services, communicate with you or respond to your enquiries.

3. Cookies and similar technologies

3.1 Cookies. Our website uses cookies. A cookie is a small text file that our website places on your device to remember information about you. Session cookies expire when you end your browsing session and help us manage how information is displayed. Persistent cookies remain on your device after you close your browser and help us recognise you and speed up future visits. We also use analytics cookies to understand how visitors use our website.

3.2 Your choices. Where required by Applicable Data Protection Laws, including in the European Economic Area (**EEA**) and the UK, we will ask for your consent before placing non-essential cookies on your device, and you may withdraw that consent at any time. You can also refuse or delete cookies through your browser settings, although some parts of our website may not then work properly. Where required by law, we treat a recognised opt-out preference signal, such as Global Privacy Control, as a valid request to opt out of the sale or sharing of your personal information.

4. How and why we use personal information

4.1 Purposes. We collect, hold and use personal information to: (a) supply our products and services, process orders and payments, and manage our relationship with you; (b) register Systems and provide warranty, support, onboarding and training; (c) maintain, update and improve the functionality, security and performance of our products and services; (d) develop new services and content, such as new and custom scenarios; (e) contact you, including to respond to your enquiries or complaints or to tell you something important; (f) tell you about products, services and events that may interest you (see clause 5); (g) protect our business, systems and users, including by detecting and preventing fraud and misuse; and (h) comply with our legal obligations, including tax, export control and sanctions laws, and assist government agencies, regulators and law enforcement bodies.

4.2 Legal bases (EEA and UK). Where the EU GDPR or UK GDPR applies, we rely on the following legal bases: (a) performance of a contract with you, or steps taken at your request before entering into a contract; (b) our legitimate interests in operating, securing, improving and promoting our business, where those interests are not overridden by your interests or fundamental rights and freedoms; (c) compliance with our legal obligations; and (d) your consent, for example for non-essential cookies and certain marketing. Where we rely on consent, you may withdraw it at any time. This does not affect the lawfulness of processing carried out before you withdrew your consent.

4.3 Secondary purposes. We will use or disclose personal information for a purpose other than the purpose for which it was collected only where: (a) you would reasonably expect us to do so and the purpose is related to the original purpose; (b) you consent; or (c) the use or disclosure is otherwise required or permitted by Applicable Data Protection Laws.

4.4 Automated decisions. We do not make decisions about you based solely on automated processing, including profiling, that produce legal effects for you or similarly significantly affect you. If this changes, we will update this policy to describe the kinds of personal information used and the kinds of decisions made, as required by the Privacy Act and other Applicable Data Protection Laws.

4.5 De-identified data. We may de-identify or aggregate personal information so that it no longer identifies you and use that data to analyse and improve our products and services. We will not attempt to re-identify de-identified data except as permitted by law.

5. Direct marketing

5.1 Marketing communications. We may use your personal information to send you information about products, services and events offered by us or our Authorised Resellers that we think may interest you. We will do so only where permitted by Applicable Data Protection Laws, including anti-spam laws such as the *Spam Act 2003* (Cth), and, where those laws require it, with your consent.

5.2 Opting out. You may opt out of marketing communications at any time, free of charge, by using the unsubscribe link in any electronic message or by contacting us using the details in clause 12. We will act on your request within a reasonable time and within any period required by law. We may still send you service-related messages, such as order confirmations and safety or warranty notices.

5.3 Third-party marketing. We do not sell or disclose your personal information to third parties for their own direct marketing purposes without your consent.

6. Disclosure of personal information

6.1 Related parties. We may disclose personal information to our related parties, including our related bodies corporate, shareholders, banks and other funding providers, where this is reasonably necessary to manage, finance, report on or assess our business. We disclose only the personal information reasonably required for that purpose, and we require recipients to keep it confidential.

6.2 Service providers. We disclose personal information to service providers who perform services for us or on our behalf, under contracts that require them to protect it and to use it only to provide those services. Our key service

providers are: (a) Microsoft, which provides systems to run our business operations (Microsoft Privacy Statement); (b) Google Analytics, for website analytics (Google Privacy Policy); (c) Odoo, our business management system, including for customer relationship management, inventory and accounting (Odoo Privacy Policy); and (d) VentraIP, our website host (VentraIP Privacy Policy). We also use payment, logistics and freight, IT support and professional service providers.

6.3 Authorised Resellers. We may disclose personal information to our Authorised Resellers where this is needed to quote for, supply, install or support our products in your region.

6.4 Other disclosures. We may also disclose personal information where: (a) we are required or authorised by law to do so, including to comply with a court order or a request from a government agency or regulator; (b) you have expressly consented, or your consent can reasonably be inferred from the circumstances; (c) it is reasonably necessary to establish, exercise or defend legal claims; or (d) the disclosure is otherwise permitted by Applicable Data Protection Laws.

6.5 Business transfers. If the ownership or control of all or part of our business changes, including through a sale, merger or restructure, we may disclose personal information to the prospective or new owner, subject to appropriate confidentiality protections.

6.6 No sale of personal information. We do not sell personal information, and we do not share it for cross-context behavioural advertising or targeted advertising, as those terms are defined in US state privacy laws. In the past 12 months, we have disclosed the categories of personal information described in clause 2 only for the business purposes described in clauses 4 and 6.

7. Overseas disclosure and international transfers

7.1 Overseas recipients. We are based in Australia, and personal information we collect may be disclosed to recipients outside Australia and outside the country in which you are located. Microsoft and Google are primarily located in the United States of America and also operate in a range of other countries; Odoo is based in Belgium and also operates in a range of other countries; and our Authorised Resellers are located in the countries they serve. You can refer to our service providers' privacy policies (listed in clause 6.2) for further information.

7.2 Australian safeguards. Before we disclose personal information to an overseas recipient, we take reasonable steps to ensure that the recipient handles it in a manner consistent with the Australian Privacy Principles, unless an exception under the Privacy Act applies.

7.3 Transfers from the EEA, UK and Switzerland. Where we transfer personal information from the EEA, the UK or Switzerland to a country that has not been recognised as providing an adequate level of data protection, including Australia, we rely on appropriate safeguards. These include the European Commission's Standard Contractual Clauses, the UK International Data Transfer Agreement or Addendum, or the recipient's certification under the EU-US Data Privacy Framework and its UK and Swiss extensions. You may request a copy of the relevant safeguards by contacting us.

7.4 Other jurisdictions. Where the laws of New Zealand, Canada, Singapore or another jurisdiction regulate cross-border transfers of personal information, we take the steps those laws require, such as ensuring that the recipient is subject to comparable safeguards or obtaining your consent.

8. Storage, security and retention

8.1 Storage. We store most personal information in computer systems and databases operated by us or by our external service providers, and in limited cases in hard copy.

8.2 Security. We implement and maintain reasonable technical and organisational measures to protect the personal information we hold from misuse, interference and loss, and from unauthorised access, modification or disclosure. These measures include: (a) identity and access management technologies that control access to the systems on which personal information is processed and stored; (b) encryption of data in transit and, where appropriate, at rest; (c) requiring our employees and contractors to keep information confidential and secure; and (d) monitoring and regularly reviewing our practices against our own policies and industry good practice.

8.3 Data breaches. If a data breach occurs that is likely to result in serious harm to you, or a risk to your rights and freedoms, we will notify you and the relevant regulator where required by Applicable Data Protection Laws, including under the Australian Notifiable Data Breaches scheme and, where applicable, within 72 hours under the EU GDPR and UK GDPR.

8.4 Retention. We keep personal information only for as long as we need it for the purposes for which it was collected, or for any secondary purpose permitted by law, including to meet legal, tax, accounting, warranty and reporting requirements. When we no longer need it, we take reasonable steps to securely destroy or de-identify it.

9. Information we process for our customers

9.1 Our role. When our customers use FLAIM Capture or the Scenario Library, we may process personal information about their trainees and users, such as names, identifiers and training performance records, on the customer's behalf. In those cases, the customer is the controller (or equivalent under Applicable Data Protection Laws) and we act as its processor or service provider. We process that information only on the customer's documented instructions and in accordance with our agreement with the customer, including any data processing agreement.

9.2 Requests. If you are a trainee or user of one of our customers, please direct your privacy questions and requests to that customer. If we receive a request directly, we will refer it to the relevant customer and assist the customer to respond as required by law.

10. Your privacy rights

10.1 Access and correction. You may request access to, or correction of, the personal information we hold about you. We do not charge for making a request but where permitted by law we may charge a reasonable fee for providing access, such as where a request requires us to collate large amounts of material. We take reasonable steps to ensure that the personal information we hold is accurate, up to date, complete and relevant. If we refuse a request, we will give you written reasons and tell you how to complain, unless it would be unreasonable to do so.

10.2 EEA and UK rights. If the EU GDPR or UK GDPR applies, you also have the right to: (a) request erasure of your personal data; (b) restrict, or object to, our processing of your personal data, including processing based on our legitimate interests and processing for direct marketing; (c) receive your personal data in a structured, commonly used and machine-readable format and have it transmitted to another controller; (d) withdraw your consent at any time, where we rely on consent; and (e) not be subject to a decision based solely on automated processing that produces legal effects for you or similarly significantly affects you.

10.3 US state privacy rights. If you are a resident of California or another US state with a comprehensive privacy law, and that law applies to us, you may have the right to: (a) know what personal information we collect, use and disclose about you, and to access it; (b) correct inaccurate personal information; (c) delete your personal information; (d) opt out of the sale or sharing of your personal information, targeted advertising and certain profiling; and (e) limit our use of your sensitive personal information. We will not discriminate against you for exercising these rights. You may use an authorised agent to make a request on your behalf. If we deny your request, you may appeal our decision by contacting us.

10.4 Other jurisdictions. If you are located in New Zealand, Canada, Singapore or another jurisdiction with privacy laws, you may have similar rights, including the right to access and correct your personal information and to withdraw your consent to its collection, use or disclosure, subject to legal or contractual restrictions and reasonable notice.

10.5 Making a request. To exercise any of these rights, please contact us using the details in clause 12. We may need to verify your identity, or the authority of a person acting on your behalf, before we respond. We will respond within a reasonable period and within any time required by law, which is generally 30 days in Australia, one month in the EEA and UK, and 45 days under the CCPA. We may refuse a request, or charge a reasonable fee, where permitted by Applicable Data Protection Laws, such as where a request is manifestly unfounded or excessive, in particular because of its repetitive character.

11. Complaints

11.1 Contact us first. If you have a complaint about how we have handled your personal information, including a request for access or correction, please contact us using the details in clause 12. We will consider your complaint, investigate it where needed, and tell you the outcome, usually within 30 days.

11.2 Regulators. If you are not satisfied with our response, you may complain to the relevant privacy regulator, including: (a) in Australia, the Office of the Australian Information Commissioner (www.oaic.gov.au); (b) in the EEA, the data protection supervisory authority in the member state where you live or work or where the alleged infringement occurred; (c) in the UK, the Information Commissioner's Office (www.ico.org.uk); (d) in New Zealand, the Office of the Privacy Commissioner (www.privacy.org.nz); (e) in Canada, the Office of the Privacy Commissioner of Canada (www.priv.gc.ca); (f) in Singapore, the Personal Data Protection Commission (www.pdpc.gov.sg); and (g) in California, the California Privacy Protection Agency (cppa.ca.gov). In some jurisdictions, including the EEA and UK, you may complain to a regulator without first contacting us.

12. Contact details

12.1 Privacy Officer. If you have any questions, comments, requests or concerns about this policy or your personal information, or you would like to update your details or preferences, please contact our Privacy Officer by email at info@flaimsystems.com or by post at: Privacy Officer, FLAIM Systems Pty Ltd, 337 Moray Street, South Melbourne, VIC, 3205, Australia.

13. Changes to this policy

13.1 Updates. We may update this policy from time to time to reflect changes in our practices or in the law. We will publish the updated policy on our website and, where the changes are material, take reasonable steps to notify you.

13.2 Copies. You may obtain a free copy of our current policy from our website or by contacting us. We will provide it in another format on reasonable request.

13.3 Effective date. This policy was last updated in November 2026 and replaces the version issued on 23 September 2020.