UK GDPR Privacy Policy

1. About this policy

This policy explains how Opus 5K handles your personal data when as a data subject you interact with our websites, products, support channels and business operations where we are acting in the capacity as a controller. This policy does not apply where we are acting in a processor capacity and where this is the case **data subjects should review the privacy notice of the health or care organisation of which they are a patient/service-user/staff member**. This policy does not replace, add to or modify a customer organisation's privacy notice in respect of their processing of your personal data where we are acting as a processor.

For UK health and care customers (**customers**) and the data subjects where we act as a controller, this policy sets out your rights. The data processing agreement between Opus 5K and each customer sets out how we process personal data where we are a processor.

Where a customer uses MARS (our product) in its own environment and acts as a controller for patient/service-user/staff data (i.e. where we act as a processor), that customer remains responsible for providing privacy information to its data subjects.

2. Scope and who this applies to

- Website visitors and online content users.
- Customers, prospective customers, customer representatives, suppliers, partners and business contacts.
- Users of Opus 5K / MARS services and portals (authorised users).
- Individuals who contact us for support, enquiries, complaints or events.
- Applicants, contractors and personnel (subject to separate workforce notices where applicable).
- Data subjects where we are acting as a controller.

3. Controller and processor roles

We perform different privacy roles depending on the activity. This affects who provides notices, decides legal basis for the processing, manages retention and responds to your rights requests.

Processing context	Typical data	Our role	Primary responsibility
Opus 5K/MARS website, enquiries, sales, contracting, billing, supplier management and account administration	Business contact details, communications, contract and billing records, website/cookie data	Controller	We determine purposes and means; this policy applies directly.
Customer tenant data in MARS/customer environment (including healthcare or workforce records entered by customer)	Customer content and operational records in the customer tenancy	Processor	Customer is the controller and is responsible for transparency, lawful basis, consent (where required), rights handling, retention, and disclosure decisions for tenant data. Our obligations as processor are set out in our Data Processing Agreement.
Technical support and troubleshooting access (when customer authorises access)	Incidental access to records, logs, screenshots, attachments, diagnostics	Processor (limited and conditional role only)	Opus 5K only accesses personal data when authorised by the customer controller, and only on the customer's documented instructions for support/technical assistance.
Our support tickets, access evidence logs, security logs, admin and service records	Ticket metadata, telemetry, audit evidence, security logs and related records (which may include personal data)	Controller	We process for service operation, security, compliance and legal obligations.

4. Who we are and contact details

Opus 5K group entities:

- Opus 5K Pty Ltd (ABN 99 123 540 189)
- Opus 5K Trading Pty Ltd (ABN 54 127 700 547)
- Opus 5K International Pty Ltd (ABN 18 142 208 231)

Privacy Officer / Privacy contact: privacy@opus5k.com

Postal address: PO Box 569, Ashgrove, QLD 4060, Australia

Telephone: +61 (0)438 462 440

UK Representative (Article 27 UK GDPR): Ametros Group Ltd, Lakeside Offices, Thorne Business Park, Hereford, England. dpo@ametrosgroup.com / www.ametrosgroup.com

Data Protection Officer: Ametros Group Ltd, Lakeside Offices, Thorne Business Park, Hereford, England. dpo@ametrosgroup.com / www.ametrosgroup.com

5. What personal data we collect as a controller

- Identity and contact data (name, job title, organisation, business email, phone number, address).
- Account and authentication data (usernames, identifiers, access records, reset events).
- Commercial and account administration data (contracts, service subscriptions, billing and payment contacts).
- Communications and support data (emails, tickets, call notes, attachments, troubleshooting details, customer instructions).
- Technical and usage data (IP address, browser/device details, operating system, timestamps, application usage metrics, logs).
- Marketing and preference data (subscriptions, opt-in/opt-out status, event registration preferences).
- Recruitment/contractor onboarding data (where applicable and lawfully processed).

6. How we collect personal data as a controller

- Directly from individuals (forms, emails, calls, meetings, contracts, support tickets, portal interactions).
- From customer representatives/your employer (authorised users, contacts, procurement and support information).
- From service provider representatives/integrations used to operate our services (ticketing, hosting, email, monitoring, finance, security).
- From customer representatives when they authorise support access or provide troubleshooting artefacts.
- Automatically from websites/services (cookies, server logs, security and performance monitoring).

7. Why as a controller we process personal data and legal bases

Where we act as controller as noted above, we rely on the following legal basis for each type of processing activity noted below.

Purpose	Examples	Legal basis
Service delivery and administration	Customer onboarding, account administration, service support coordination	Contractual necessity; legitimate interests
Security and service integrity	Authentication, monitoring, logging, abuse prevention, incident response	Legitimate interests; legal obligation (where applicable)

Purpose	Examples	Legal basis
Finance, audit and compliance	Invoicing, tax, audit trails, record-keeping	Contractual necessity; legal obligation
Communications and support	Responding to enquiries, complaints, technical support	Contractual necessity; legitimate interests
Product/service improvement	Usage analytics, trend analysis, reliability improvements	Legitimate interests; consent where required for non-essential tracking
Marketing and events	Product updates, newsletters, event invitations	Consent and/or legitimate interests (subject to applicable e-privacy rules)
Recruitment/contractor onboarding	Candidate assessments and engagement administration	Contractual necessity; legal obligation; legitimate interests

8. AI-powered features and analytics

MARS includes AI-powered search functions. Customers remain responsible for assessing and documenting their controller obligations where personal data is processed by them using this feature and in this case data subjects of our customers should refer to the privacy notice of the relevant UK health or care customer of which you are a **patient/service-user/staff member**.

- We do not use customer tenant personal data for our own purposes.
- We use de-identified or aggregated operational/service data for security, maintenance and service improvement where lawful and proportionate.
- Where a feature changes processing risk significantly, customers may need to update their DPIA and privacy notices; we can assist as processor/service provider.

9. NHS and UK health/social care transparency

- We maintain governance documentation and controls intended to support DSPT-aligned assurance and supplier expectations.
- Where NHS-specific obligations (for example, national data opt-out applicability) apply to a customer controller's processing, the customer is responsible for determining applicability and compliance. Where **Opus 5K is acting in its capacity as the controller,** as noted above, data subjects may contact Opus 5K and request to opt out.

10. Cookies and similar technologies

We use cookies and similar technologies on our website and digital services to support core functionality, security, user preferences, and (where enabled) analytics and service improvement.

These technologies may include cookies, scripts, tags, and similar tools that store or access limited information on your device or browser.

Types of technologies we may use:

- **Browser cookies**: small text files stored on your device/browser.
- **Tags / scripts**: code used to enable website features, measure usage, or manage consent settings.
- **Web beacons / pixels**: small electronic files that may be used in website pages or emails to understand usage, delivery, or engagement (where implemented).

We **do not rely on Flash cookies (Local Shared Objects)** as part of our standard website and service operation.

Session and persistent cookies

Cookies may be:

- **Session cookies**, which are deleted when you close your browser; or
- **Persistent cookies**, which remain on your device for a set period or until deleted.

How we use cookies

We may use cookies and similar technologies for the following purposes:

1. Strictly necessary cookies

These cookies are required for the website or service to operate securely and correctly. They may be used for:

- session management
- security controls
- authentication support
- load balancing
- storing your cookie consent preferences
- maintaining core service functionality

These cookies are essential to provide services you request and to maintain website integrity and security.

2. Functional / preference cookies (where used)

These cookies help remember choices you make (for example, interface preferences) to improve usability and reduce the need to re-enter settings.

3. Analytics / performance cookies (where used)

Where enabled, these cookies help us understand how users interact with our website or services (for example, pages visited, feature usage, and performance issues) so we can improve usability, reliability, and content.

Analytics information may include technical and usage information such as IP address, browser type, device type, operating system, pages viewed, access times, and referring

pages. We aim to use this information in aggregated or de-identified form where practicable.

4. Marketing / communications cookies (where used)

Where we use marketing or campaign measurement tools, cookies or similar technologies may be used to measure communications effectiveness and user engagement. We will describe these in our cookie information and provide choices where required.

Your choices and control

You can manage cookies through:

- our cookie banner / cookie preferences tool (where implemented); and
- your browser settings (including blocking or deleting cookies).

Please note that disabling strictly necessary cookies may affect the operation, security, or availability of some website or service features.

Cookie consent and preferences

Where required by applicable law, we will request your consent before using non-essential cookies (such as analytics, functional, or marketing cookies, unless an exemption applies). We will also provide a way for you to review and update your preferences.

11. Disclosures and recipients

We disclose your personal data that we collect as a controller to:

- Our employees and authorised personnel on a need-to-know basis.
- Related group entities where necessary for administration, service delivery and governance.
- Service providers acting on our behalf (e.g., hosting, ticketing, email, monitoring, analytics, finance and security providers).
- Professional advisers (legal, audit, insurance, compliance) under confidentiality obligations.
- Regulators, courts or law enforcement where required by law.
- Customer-authorised recipients or other parties instructed by the customer in relation to support/service delivery.
- Prospective acquirers or counterparties in a corporate transaction, under confidentiality controls.

We do not sell your personal data.

12. International transfers

Where we act as controller, some of the personal data we collect may be transferred to, stored or accessed in countries outside the United Kingdom, including Australia (where our group entities are based), the European Economic Area, and the United States (where some of our service providers are located).

Where we transfer personal data to another organisation in a country that does not benefit from a UK adequacy decision, we use appropriate safeguards as required by UK GDPR, which may include the UK International Data Transfer Agreement (IDTA) or the UK Addendum to the EU Standard Contractual Clauses, together with any supplementary measures necessary to ensure an adequate level of protection for your personal data.

We keep our international transfer arrangements under review and update safeguards as required by changes in law, guidance, or our service provider arrangements.

Where we act as a processor and international transfers arise in connection with customer tenant data, the applicable safeguards and transfer mechanisms are addressed in our Data Processing Agreement with the relevant customer.

13. Security of personal data

We implement technical and organisational measures (TOMs) appropriate to the risk to protect your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed, including:

- Role-based access control and least privilege (i.e. limited access to your personal data).
- Multi-factor authentication where applicable.
- Encryption in transit and at rest where applicable.
- Logging, monitoring and audit trails for administrative and support access.
- Network and infrastructure security controls (including secure connectivity and segmentation where relevant).
- Secure development, patching and change management.
- Backup, business continuity and disaster recovery measures.
- Incident response and personal data breach procedures (see section 17 below).
- Supplier due diligence and contractual controls.
- Staff confidentiality obligations and privacy/security training.

14. Data retention and deletion

We retain personal data only for as long as necessary for the purposes for which it was collected, and as required for legal, contractual, security, audit and dispute-management obligations.

- Customer tenant data retention is determined by the customer as controller and the customer's configuration/contract.
- Support tickets, support artefacts and troubleshooting records are retained in accordance with our approved retention schedule and Freshdesk lifecycle controls.
- Security/audit/access logs are retained for defined periods to support security and compliance activities.
- Where no longer required, data is securely deleted or de-identified, subject to legal retention requirements.

15. Data subject rights and access/correction requests for personal data we hold as a controller

If your personal data is held in a customer tenancy where they are the controller, you should contact that customer first. We will assist our customers with their obligations as the controller where required by contract or law.

Where we hold your personal data as a controller you have rights including requesting access, rectification/correction, erasure, restriction of or objection to processing, portability/transfer of your personal data and withdrawal of consent (where processing is based on consent). Contact us using the details in section 4 of this policy to make a request to exercise any of your rights as a data subject.

We may need to request specific information from you to help us confirm your identity and verify your right to access your personal information (or to exercise any of your other rights). This is a security measure to ensure that personal information is not disclosed to any person who has no right to receive it. We also may contact you to ask you for further information to assist us in responding to your request.

Please also note that in certain circumstances your rights will not apply and/or in certain circumstances some categories of personal information will be exempt from the scope of those rights. We will notify you where this is the case.

We try to respond to all legitimate requests within one month. Occasionally, it may take us longer than one month if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.

We have appointed a data protection officer (DPO) to oversee compliance with this notice. If you have any questions about this notice or how we handle your personal information, please contact our DPO whose details are in section 4 of this policy.

If you would like to make a complaint regarding this notice, you can contact us using the contact details in section 4 of this policy. We will reply to your complaint as soon as we can.

If you feel that your complaint has not been adequately resolved, please note that the UK GDPR also gives you the right to make a complaint directly to the UK Information Commissioner's Office:

> Information Commissioner's Office Water Lane, Wycliffe House Wilmslow, Cheshire SK9 5AF Telephone: +44 303 123 1113 Website: https://ico.org.uk/make-a-complaint/

16. Automated decision-making and profiling

We do not make automated decisions or undertake profiling in our processing of your personal data as a controller that produce legal or similarly significant effects on data subjects unless expressly notified. Customers are responsible for assessing whether any such obligations arise from their own use of MARS features in their processing as controllers.

17. Personal data breaches and incident handling

We maintain incident response and personal data breach management plans and procedures.

- Where we act as controller, we assess notification requirements under applicable law, including whether notification to the ICO and/or affected data subjects is required.
- We keep records of incidents/breaches and corrective actions.

18. Direct marketing

We may send service updates, product information, events and marketing communications in accordance with applicable law (including spam/e-privacy requirements).

You can opt out of marketing communications at any time using the unsubscribe mechanism or by contacting us. Service/security notices may still be sent where necessary.

19. Third-party websites and platforms

Our websites and services may link to third-party websites or services. We are not responsible for the privacy practices of third parties. Their privacy notices/policies apply to their processing.

20. Changes to this policy

We may update this policy from time to time to reflect changes in law, guidance, technology, service features or business operations. We will publish the current version on our website and update the version date. Where the changes are significant we will notify you directly of these changes. In either case your continued use of MARS or providing us any of your personal data after notification of the changes will be understood as your acknowledgement of these changes and, where required by law, your consent to them.