

Australian Privacy Policy

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)

Last modified: 5 March 2026

Opus 5K is strongly committed to protecting your privacy when you interact with us, our content, products, and services.

Our goal is to provide you with healthcare software systems. Sometimes this means that we use information that you provide to us about yourself to customise that experience. We do this to improve your enjoyment of our products and services. In providing our services to you, we will be transparent about how and why we collect and use your information. In some cases, if you do not want us to collect or use your information in a particular way, then we will give you the opportunity to say so.

This privacy policy explains:

- the application of this privacy policy;
- what is considered personal information;
- the kind of information we may collect and hold about you, how we collect and hold it, why we collect, hold and use it, and how we use it;
- the protection of your personal information; and
- how and why we may disclose that information, including to overseas recipients and the countries they're located in;
- how you can access and correct the information we hold about you;
- when we may use your information to contact you;
- our use of cookies to collect information, and how you can control or delete these cookies; and
- how you can make a complaint about an alleged breach of the Australian Privacy Principles (**APPs**), and how we deal with such a complaint.

By accessing our website, using our products or services, or providing any personal information to us, you agree to be bound by this privacy policy and consent to our use and disclosure of your personal information as explained within this policy.

If you have any questions about this privacy policy or our handling of your personal information, or if you require a copy of this privacy policy in a particular form, please contact the Privacy Officer by email in the first instance: privacy@opus5k.com. The postal address is:

Privacy Officer
PO Box 569, Ashgrove, QLD 4060
Ph: +61(0)438 462 440

1. Application of this Privacy Policy

Our privacy policy applies to personal information collected by us, whether we have asked for the information or not. We are governed by the Australian Privacy Principles (APPs) under the Privacy Act 1988 (Cth) (Act).

This policy applies only to us. It does not apply to any other company or organisation, including those whose digital services have links to our content or services. Third party services which have links to our content or services will govern the use of personal information you submit to them, which may also be collected by cookies when you visit or use them. We do not accept any responsibility or liability for the privacy practices of such third party digital services.

We have a Privacy Officer who oversees the management of this privacy policy and compliance with privacy laws. This officer may have other duties within our business and may also be assisted by internal and external contractors, professionals, and advisors.

We will review this policy regularly, and may update it from time to time, including taking account of new or amended laws, new technology and/or changes to our operations. If we make changes, we will post those changes on the privacy page of our website.

2. Personal and Sensitive Information

Personal Information in this privacy policy has the same meaning as in the Act. It includes any data from which an individual's identity can be ascertained. The data need not be true, may be mere opinion, and need not be in writing. This may include (but is not limited to) your name, age, gender, postcode and contact details (including phone numbers and email addresses) and possibly financial information, including your credit card, direct debit, or PayPal account information. If the information we collect personally identifies you, or you are reasonably identifiable from it, the information will be considered personal information.

Sensitive information: The Act defines some types of personal information as sensitive, which includes information about a person's race, ethnic origin, political opinions, health, religious or philosophical beliefs and criminal history. In the event we require any sensitive information we would only collect this with your permission, and we will only use it for the purpose for which you provided it.

We host data (**Client Data**) for service providers in the health care industry, and such data may include Personal Information about our client's patients. However, this privacy policy does not apply to Client Data. Client Data is subject to the privacy policy of the service provider who collected the Client Data, and patients should contact their service provider in this regard.

In the course of providing our services, we may have incidental access to Client Data for the purpose of providing technical support to our clients. However, we do not retain permanent records of such information, as we delete them once no longer required for the purposes of technical support (including the building of our knowledge base).

2.1 Anonymity and pseudonymity

You may access our public-facing website anonymously, however if you choose to not provide us with the personal information described in this policy, some or all of the following may happen:

- (a) we may not be able to provide you with the products or services you requested, either to the same standard, or at all (for example, we require you to verify your identity to access the Opus Portal);
- (b) we may not be able to provide you with information about products and services that you may want; or
- (c) we may be unable to tailor the content of our website to your preferences and your experience of our website may not be as enjoyable or useful.

As you access the website, we collect and use temporary session data (cookies) which may include identifiers such as your IP address, which we use to provide the website and services.

As our software is used for audit and compliance purposes, to use the Opus Portal or any other services, we require you to log in with valid credentials, and these often identify you personally. Authentication data used to log-in to our software and services may include personal information. Access attempts are logged and stored securely with other client data.

3. Collection and Use of Personal Information

3.1 Why we collect personal information

We collect personal information about you:

- (a) because you have provided it to us, for instance if you contact us to make comments, complaints or to ask us questions, or you have interacted with one of our digital services;
- (b) because we need it to provide a product or service that you have requested, for instance: (i) to provide our products and services to you, or to provide you with a quote or offer for our products and services;
 - (ii) to communicate with you about your account with us, including issuing bills and seeking payment of those bills;
 - (iii) to set up a direct debit facility to cover payment of any bills issued by us, if you request or agree;
 - (iv) to provide you with information on our products and services if you subscribe to an email list; and
 - (v) to conduct a credit assessment of you and use information we are permitted by law to use to establish or report on your creditworthiness;
- (c) because we would like to improve our products or services, and carry out quality control and research, for instance through the collection and analysis of statistical and research data and use of cookies (see below);
- (d) because you work for us, or apply to us for a job, a cadetship or work experience;

- (e) because we are required or permitted by any law;
- (f) for purposes directly related to any of the above, for example, for administrative or planning purposes, to keep you informed of updates and changes to the software, and to provide technical support.

3.2 How we collect personal information

Broadly, there are two types of information or data we collect:

Information that you specifically give us

For example, you may provide information about yourself when you are filling in a form or when you sign up to a service. This type of information may include your name, email address and age. The information that you give us may be:

- (a) Personal information that is required . In some instances, you must provide personal information if you wish to use a particular service or participate in an activity. For example, your email address may be required if you wish to sign up to a particular service.
- (b) Personal information that is optional . You may choose to provide some personal information which is not required but is directly related to our functions or activities. Usually this type of information will enable us to improve or broaden the services we can offer you. If you choose not to provide this optional information, we would still be able to offer you the service, but perhaps with fewer options than if you had provided the optional information. If we receive unsolicited information about you that we do not require or which is not directly related to our functions or activities, we may be required to destroy or de-identify that information, provided it is lawful and reasonable to do so.
- (c) Permissions . Sometimes you will be asked to confirm that you agree to a particular activity. For example, you may need to expressly agree that you would like to receive a newsletter.

You may be able to make changes to the information you provided us (for example, if you change your email address) or withdraw the permission you gave us for a particular service. We will make it clear how you do that.

Data we collect that tracks your activity

We automatically gather information to monitor the use of our digital services, like the numbers and frequency of visitors to our website.

This information helps us improve our services by learning what our customers use and don't use. It can also help us identify if there are any problems with our services that need fixing.

This data is usually collected using "cookies". "Cookies" are small files that are stored on your browser. Further information about our use of cookies is provided below.

Most of the data we collect is aggregated, and this information is effectively anonymous to us. In some cases we may collect data that can be linked to you individually. For example, if you use our email newsletters we may collect data about the mailings you open and the links you click on from that newsletter.

As well as helping to improve our services, we may use this data to provide recommendations that you might find helpful based on your activity. In some cases, a digital profile may be formed based on your activity. We do this in order to improve your experience or to improve our ability to provide a service.

4. Credit Card Information

Your credit card details are only stored and transmitted in encrypted form. Unencrypted credit card information is NOT stored on our internet servers.

Credit card information is never stored in a cookie.

Our services are not sold via our website, and as such, we do not collect credit card payments via online methods. All credit card payments are currently processed using third party merchant facilities. We do not receive or store any credit card information.

5. Government Identifiers

We do not use government related identifier (eg Medicare Number, or Tax File Number) for any purposes, although such identifiers may be used by our clients. Please refer to our clients' privacy policies for information on their use of any government related identifiers.

6. Safety and Security of Your Personal Information

We will take all reasonable and practicable steps to ensure that your personal information is properly protected from misuse or loss, and unauthorised access, modification or disclosure, including by means of authentication credentials, password encryption, session expiry times, firewalls, network traffic encryption, and appropriately securing our physical facilities.

At the same time, we are committed to being available to customers on multiple platforms. Some of those platforms (such as social media platforms) are not operated or controlled by us, and our ability to protect your personal information is limited.

We encourage you to be vigilant about the protection of your own personal information when using third party digital services (such as social media platforms). As far as reasonably practicable, we will make sure that our relationships with those third parties include appropriate protection of your privacy.

By using the site or our services, you acknowledge that the security of online transactions and the security of communications sent by electronic means or by post cannot be guaranteed. You provide information, including personal information, to us via any area of the site requiring

registration, via our contact forms, via email, or via any other method at your own risk. We cannot accept responsibility for misuse or loss of, or unauthorised access to, personal information where the security of information is not within our control.

By using the site or our services, you acknowledge that we are not responsible for the privacy or security practices of any third party (including third parties that we are permitted to disclose or transfer personal information to in accordance with the privacy policy or any applicable laws). The collection and use of personal information by such third parties may be subject to separate privacy and security policies.

If you suspect any misuse or loss of, or unauthorised access to, your personal information, you should let us know immediately.

We are not liable for any loss, damage or claim arising out of another person's use of your personal information.

Where personal information we hold is no longer necessary to our services or for audit or compliance purposes, we delete the information or permanently de-identify it, subject to specific laws in respect of data retention.

7. Disclosure of Personal Information

7.1 Disclosure of personal information to third parties

We may disclose your personal information to:

- (a) our employees, related bodies corporate, contractors or external service providers for:
 - (i) the operation of our websites or our business, including without limitation:
 - (A) financial institutions (for payment processing);
 - (B) credit reporting bodies and other credit providers;
 - (C) for research purposes relating to the performance, quality, maintenance and improvement of our services and products;
 - (D) to customise and promote our services which may be of interest to you; and
 - (ii) fulfilling requests by you, including without limitation:
 - (A) providing products and services to you;
 - (B) providing technical support to you to use our services;
- (b) our existing or potential agents, business partners or joint venture entities or partners;
- (c) specific third parties authorised by you to receive information held by us;
- (d) the police, any relevant authority or enforcement body, or your Internet Service Provider or network administrator, for example, if we have reason to suspect that you have committed a

breach of any of our terms and conditions, or have otherwise been engaged in any unlawful activity, and we reasonably believe that disclosure is necessary;

(e) third parties where required by law, binding regulation or court order; or

(f) third parties otherwise with your consent.

We may disclose your personal information to these service providers for the purpose of their work and, equally, and these service providers may provide us with personal information they have collected from you in the course of providing the relevant products or services.

We may also disclose your personal information to third parties to whom we assign your debt (where applicable).

We are assisted by a variety of external service providers to deliver our services, some of whom may be located overseas. These third parties are too numerous to list, and they change from time to time. Some examples of the types of third parties include:

(g) technology service providers including:

- (i) website analytics providers such as Google located in the US and Ireland;
- (ii) app service providers such as Google located in the US and Ireland;
- (iii) cloud service providers such as Microsoft Azure, Rackspace, and Google located in the US;
- (iv) third party software providers such as PipeDrive, Freshdesk, Sentry, and Quickbooks located in the US and Estonia;
- (v) service providers such as Acunetix located in Malta; and

(h) developers, IT system administrators, and support staff, who may be located overseas.

While our developers and support staff rarely access live data, they may do so when troubleshooting complex support requests or bugs, or designing new functionality to address your feature requests.

Where possible, we impose contractual restrictions equivalent to those imposed on us under the Act in respect of collection and use of personal information by those third parties. In some cases, such as social media networks or large third party service providers, our ability to impose contractual restrictions is limited. In those circumstances, we will carefully consider the risks to the protection of personal information when entering into arrangements with third parties.

Our service providers are not permitted to sell, use or disclose your contact details or contact you for any other purpose unless required by law.

Under no circumstances will we sell or receive payment for licensing or disclosing your personal information.

7.2 Information that is disclosed via other platforms or services

Our website may contain links to other websites operated by third parties. We make no representations or warranties in relation to the privacy practices of any third party website and we are not responsible for the privacy policies or the content of any third party website. Third party websites are responsible for informing you about their own privacy practices.

Some of our services may be integrated with external services, including social media networks. This may mean that information, for instance about your interests and activities, is tracked or pulled from other places (such as Facebook). If you are signed in to one of our services which is integrated with other media tools, this information may be available to others depending on the privacy settings you have in place on other platforms.

The number and nature of social media platforms is changing rapidly, and the way in which information is shared between them is becoming increasingly complex. We do not currently have any social sharing features enabled on our website or within our software, and we have no immediate plans to introduce such features. However, in the event that we do introduce such features, and to help you manage and protect your personal information, we will ask you to opt-in before making your personal information available through an integrated service. If we provide you with any digital services, we will also provide you with the ability to opt-out of your participation in those services. Information about how to opt-out will be provided in the particular service. However, you should be aware that we may continue to store personal information provided by you prior to you opting-out.

Your ability to opt-out of a third party tool or platform will depend on the conditions governing your agreement with that third party.

8. Direct Marketing

We will never knowingly send you unsolicited commercial electronic messages. More information on the Spam Act 2003 (Cth) is available from the regulator's website: <https://www.acma.gov.au/scamsspam-and-telemarketing>.

If you subscribe to our mailing list, or order through our website, we may use or disclose your personal information (excluding sensitive information) for direct marketing purposes. We will obtain your specific consent to disclose sensitive information for the purposes of direct marketing our services. We may include third party offers in marketing materials we send to you.

You will be able to opt-out of direct marketing at any time with no charge to you, or request us to provide you with our source of information, by email to privacy@opus5k.com, or through the unsubscribe link found in all marketing emails we send. We will then ensure that your name is removed from our mailing list.

If you receive communications from us that you believe have been sent to you other than in accordance with this policy, or in breach of any law, please contact us using the details provided below.

9. Use of Cookies Across Our Digital Services

We use a "cookie" system on our digital services. A "cookie" is a small data file placed on your machine or device which lets our digital service store information. This information allows us to make our digital services easier to use and more relevant. For instance, cookies allow our servers to keep track of your customer details between visits to our website. The information stored by the cookie includes data that is provided during online registration processes. Placing

cookies on your device also means we can serve you promotional information that you might be more interested in. The promotional information can appear on third party digital services as well as our digital services. It also allows us to control the number of times you see that promotional information and measure how effective the campaign has been.

Credit card information is never stored in a cookie.

The analytics systems used by us use cookies to gather information regarding visitor activity on our digital services. This is not used to identify personal details but is collated into aggregate results in order to evaluate and improve our services. When you use our digital services, some information is logged automatically, such as your computer's operating system, Internet Protocol (IP) address, access times, browser type, pages visited and videos viewed. We engage independent measurement companies to perform these services.

9.1 Controlling and deleting cookies

Popular browsers will usually give users a level of control over cookies.

You can set your browsers to accept or reject all, or certain, cookies. You can also set your browser to prompt you each time a cookie is offered.

Most cookies are easy to delete, and the Help function within your browser should tell you how. Some digital services may not load properly or function as intended if cookies are disabled, however it is up to you to determine the balance of convenience and computer privacy that you are comfortable with.

9.2 Cookies used by us

We may use the following types of cookies:

- (a) Session Computer Browser Cookies - Session cookies let you move from page to page without the need to repeatedly sign in. A session browser cookie is stored in the browser and deleted when the browser shuts down.

- (b) Persistent Cookies - Persistent cookies are used to help us monitor the performance of our digital services by recording your browsing behaviour within the particular digital service. These browser cookies can only be read by the company that places the cookies on the computer. Persistent cookies are saved to the hard drive until they expire. Unlike session browser cookies, they are not deleted when the browser is shut down.

- (c) Flash Cookies - also known as Local Shared Objects, are used to track activity in applications that are running in Adobe Flash Player. Designed for usability, they allow user's custom settings to persist between visits.

We use web beacons in combination with cookies to track activity. Turning off a browser's cookies will prevent web beacons from tracking activity.

9.3 Third party cookies

We use a number of suppliers who also set cookies on our digital services on our behalf in order to deliver the services that they are providing.

For instance, if we embed photos and video content from third parties such as flickr and youTube, those third parties may have set cookies relating to that content. If you then "share" that content, another third party cookie may be set by the service you have chosen to share content through. We do not control these cookies, and do not block cookies set by third parties in these ways.

10. Accessing Your Personal Information

You have the right to request access to personal information that is held by us about you. If you make an access request, we will ask you to verify your identity. There may be instances where we cannot grant you access to the personal information we hold. For example, we may need to refuse access if granting access would interfere with the privacy of others, or if it would result in a breach of confidentiality. If that happens, we will give you written reasons for any refusal. There is no charge for simply making an access request, however, where we permit access, we reserve the right to charge a reasonable fee to cover our costs, assessed on a case by case basis.

You also have the right to request the correction of any of your personal information that we hold. On receiving your request, we will consider if the information requires amendment. We will take reasonable steps to make appropriate corrections to personal information so that it is accurate, complete and up-to-date. If we do not agree that there are grounds for amendment, then we will give you written reasons for our refusal to amend, and we will add a note to the personal information stating that you disagree with that personal information. There is no charge for making any corrections to your personal information.

To seek access to, or correction of, your personal information please contact us as follows:

By email:

privacy@opus5k.com

By telephone:

+61(0)438 462 440

By mail:

Privacy Officer, PO Box 569, Ashgrove, QLD 4060

Please note: as our software and services are used for audit and compliance purposes, we are required to maintain the confidentiality and integrity of our clients' data, even if that data is inaccurate. As such, we do not disclose or update client data without written permission from our client, unless required by law or court order. If you wish to update or correct your personal information stored on our systems by one of our clients, you should instead contact our client and request the change in accordance with that client's privacy processes.

11. Privacy Complaints and Enquiries

11.1 Complaints and disputes

If you have a complaint relating to an alleged breach of the APPs, you should contact us in writing using the details listed in this privacy policy.

We have a formal procedure for investigating and dealing with privacy breaches. Once the Privacy Officer receives a complaint, whether it is in writing or verbal means, the Privacy Officer will commence an investigation into the alleged breach. The Privacy Officer will endeavour to determine the nature of the breach and how it occurred. We may contact you during the process to seek any further clarification if necessary. If a breach is found, the Privacy Officer will escalate the matter to management so that the process can be rectified to prevent any further breaches from taking place. We will also contact you to inform you of the outcome of the investigation. We will endeavour to resolve all investigations within a reasonable time.

We will treat your requests or complaints confidentially. Our representative will contact you within a reasonable time after receipt of your complaint to discuss your concerns and outline options regarding how they may be resolved. We will aim to ensure that your complaint is resolved in a timely and appropriate manner.

If you are unsatisfied with our response, you may refer the complaint to the Office of the Australian Information Commissioner at <http://www.oaic.gov.au>.

11.2 Additions to this privacy policy

We may amend the privacy policy at our sole discretion, and it is your responsibility to review this page from time to time.

We may do things in addition to what is stated in this privacy policy to comply with the APPs, and nothing in this privacy policy shall deem us to have not complied with the APPs.

12. Jurisdiction

The laws of the State of Queensland, Australia apply to this privacy policy and the parties submit exclusively to the courts of that jurisdiction in relation to any alleged breach of this policy.