PRIVACY POLICY

Last updated: October 2026

VALD Pty Ltd (ABN 16 603 446 171)

This Privacy Policy applies to VALD Pty Ltd and its affiliates and related bodies corporate (including VALD Operations Limited, VALD Performance (Aust) Pty Ltd, VALD Performance (Intl) Pty Ltd, VALD (Canada) Inc and VALD Group Inc) (**VALD, we, us, our**) in relation to their operations. It explains how we handle Personal Data and comply with the requirements of applicable privacy laws and other related laws regulating the handling of Personal Data, including without limitation the *Privacy Act 1988* (Cth) and the Australian Privacy Principles, the General Data Protection Regulation (Regulation (EU) 2016/679), the UK GDPR and applicable EU Member State laws (together, **Privacy Laws**). For the purposes of EU data protection law, where VALD processes Personal Data on behalf of a Client, the Client is the data controller and VALD is a data processor. VALD Pty Ltd is the data controller only in the limited circumstances described in section 3.5. If you have further questions relating to this Privacy Policy, please contact our Data Protection Officer at DPO@vald.com.

This Privacy Policy also serves as notification to individuals of the matters required to be notified on collection of their Personal Data.

This Privacy Policy forms part of, and should be read together with, the Terms of Use and, where applicable, the Data Processing Agreement and Business Associate Agreement (each as defined in section 18).

We recognise the importance of your privacy, and that you have a right to control how your Personal Data is collected and used.

Key terms are defined in section 18.

1. CATEGORIES OF PERSONAL DATA COLLECTED

1.1 We collect Personal Data from Clients (existing and prospective), as well as end users of the VALD websites, VALD software and applications (including any AI Features made available through them, and any other software that interfaces with VALD's products) (**Apps**) and individuals who engage with us via our social media accounts. We also collect Personal Data from suppliers, contractors, prospective employees, and consumers and other individuals who interact with us or our Clients for various business and other purposes further listed in this Privacy Policy. In this section 1, we explain the kinds of Personal Data which we usually collect and hold as well as how we collect this information.

1.2 The kinds of Personal Data VALD will collect and hold about you will depend on the circumstances in which that information is collected. It may include:

(a) contact details which may include your name, address, email and phone details;

(b) age or date of birth information;

(c) Personal Data that you include in any content that you enter into the VALD websites or the Apps;

(d) information required for you to open an account with us or subscribe to any of the VALD websites or the Apps or to otherwise do business with us, including bank account details, and any other relevant financial information;

(e) information about your device and your use of the VALD websites and the Apps, including device ID(s), device type, IP address, geo-location and device location, the country from which you accessed the websites and the Apps, dates, times and durations of visits, computer and connection information (including browser type and operating system), statistics on page views, traffic to and from the sites, referring website addresses, ad data, standard web log information and any other online analytics, unless you object to such processing pursuant to rights that exist under applicable Privacy Laws (including the GDPR);

(f) information on your dealings with VALD, including details of the products and services we have provided to you or that you have enquired about, including any additional information necessary to deliver those products and services and respond to your enquiries;

(g) behavioural information and information on preferences and past behaviours;

(h) any additional information relating to you that you provide to us directly through our websites or the Apps or indirectly through your use of our websites or the Apps or online presence or through other websites or accounts from which you permit us to collect information;

(i) information you provide to us through client surveys;

(j) Input you provide to, and Output generated by, AI Features (see section 13); and

(k) content you upload to, link to or make available through the Apps, including content hosted on third-party platforms such as Dropbox, and information we receive from third-party platforms and applications connected to the Apps (for example, through an integration or API).

1.3 If you are a healthcare professional, we may collect additional Personal Data including:

(a) your medical specialty; and

(b) your clinical interests.

1.4 If you are a patient, athlete or other individual whose information is recorded through the Apps, we may collect additional Personal Data including:

(a) details of your healthcare professional, practitioner or the Client that administers your profile;

(b) information about your health, including medical conditions;

(c) your responses to patient-reported outcome measures, questionnaires and clinical outcome assessments completed through the Apps;

(d) physical characteristics, such as your sex at birth, height and weight;

(e) your sport, position and team;

(f) performance and movement measurements, such as forces, distances and speeds of movement;

(g) video recordings and photos (for example, when using HumanTrak); and

(h) notes recorded about you by your practitioner.

1.5 We usually collect Personal Data either directly from you, someone acting on your behalf, or from third parties through:

(a) your use of VALD websites and the Apps, including when you register or subscribe for an account, create a profile, post or otherwise submit content or via our use of website analytics;

(b) use of social media;

(c) information that you communicate to us including through correspondence, chats, and other social media applications, services or websites, email, telephone, SMS, third party apps and any other forms of communication sent or given to us electronically or in hard copy;

(d) interaction with our services, content, and advertising;

(e) orders for products or services;

(f) third-party service providers;

(g) requests for brochures, to join a mailing list, or to be contacted for further information about our products or services;

(h) warranty claims;

(i) provision of client service and support;

(j) responses to surveys or research conducted by us or on our behalf;

(k) entries into competitions or trade promotions conducted by us or on our behalf;

(l) third-party platforms and applications that you connect to the Apps (for example, through an integration or API); and

(m) a Client or its Authorised Users, where they create an account or profile for you, or record or upload information about you, through the Apps, including by connecting a third-party platform or application to the Apps (for example, through an integration or API).

1.6 If you do not provide us with the information we request, we may not be able to fulfil the applicable purpose of collection, such as to supply products or services to you or to assess your application for employment.

1.7 Where it is lawful and practicable, you may deal with us anonymously or by using a pseudonym, for example when making a general enquiry. However, it is generally not practicable for us to provide our products and services or the Apps to you, or for a Client to create a profile for you, without information that identifies you.

1.8 Where reasonable and practicable, we will collect Personal Data directly from you. If we collect information about you from someone else (for example, from a distributor or reseller of our products, or from a business partner who refers you to us), that third party will ensure you are aware that we have collected Personal Data about you and the circumstances of the collection and provide any additional disclosure required under applicable Privacy Laws (including the GDPR). Where Personal Data is collected by a Client as Client Data (including where a Client directs a third-party platform to send it to us, for example through an integration or API), the Client is responsible for notifying you (see sections 1.11 and 3.4).

Sensitive information (or special categories of Personal Data)

1.9 Given the nature of the VALD websites and the Apps, it is possible that there could be instances where we collect sensitive information or special categories of Personal Data (as defined under relevant Privacy Laws) such as:

(a) health information or data relating to health; and

(b) other sensitive information or special categories of Personal Data (as defined under relevant Privacy Laws),

but only where you choose to disclose it to us via the VALD websites and the Apps.

1.10 We will only collect such information about you in accordance with applicable Privacy Laws.

1.11 Where a Client or its Authorised Users record sensitive information about you through the Apps, the Client is responsible for providing you with any required notices and obtaining any required consent for that collection and for VALD's handling of that information.

1.12 Video recordings, photos and movement data collected through the Apps are used to measure and analyse movement. We do not use them to identify or verify the identity of individuals by biometric means, or to create biometric templates.

2. USE AND DISCLOSURE OF PERSONAL DATA

2.1 In most cases, VALD handles Personal Data on behalf of Clients, and the Client is the controller of that information. This section 2 describes how we use and disclose Personal Data, both where we handle it on behalf of Clients as a processor and to the extent that VALD acts as a controller (see section 3.5).

2.2 Where we act as a controller, the third column of the table below sets out our legal basis; where we act as a processor, we act on the Client's instructions and our agreement with the Client. The purposes for collecting, holding, using and disclosing Personal Data are set out in both the table below and the table set out in section 3.3.

Purpose	Personal Data used	Legal basis
To supply products and services to Clients and end users of our websites and the Apps (other than processing Client Data on a Client's behalf, which is described in section 3)	Contact details and account details	Performance of a contract with you. Where our contract is with a Client, our legitimate interests in providing the products and services the Client has requested.

Purpose	Personal Data used	Legal basis
To provide the Apps to individuals who create an account directly with us, rather than through a Client	Contact details, account details, physical characteristics, performance and movement measurements, health information and other content entered into the Apps or received from third-party platforms you connect to the Apps	Performance of a contract with you. For health information (if applicable), your explicit consent (see section 10.5).
To manage your account with us	Contact details, account details, financial information	Performance of a contract with you; our legitimate interests in managing our relationship with Clients and users.
To obtain products and services from our suppliers	Business contact details	Where necessary to perform our contract with you, performance of that contract; otherwise, our legitimate interests in conducting business with our suppliers.
To respond to enquiries from existing or prospective Clients	Contact details, details of your enquiry	Where necessary to take steps at your request before entering into a contract with you, taking those steps; otherwise, our legitimate interests in providing quality client service and assistance.
To assess and process warranty claims	Contact details, product and order details, details of your dealings with us	Performance of a contract with you; our legitimate interests in assessing and processing warranty claims.
To process and assess employment applications	Contact details, application and recruitment information	Our legitimate interests in recruiting staff; compliance with a legal obligation where applicable.
To establish, exercise or defend legal claims, including enforcing our agreements	Contact details, account details, details of your dealings with us	Our legitimate interests in establishing, exercising or defending legal claims.
To undertake research and surveys, analyse statistical information about the use of our websites, and use that information and survey responses to develop and improve our products and services	Information about how you use our websites, device information and survey responses. Our use of Client Data, including information about how the Apps are used, for these purposes is described in section 3.	Where necessary to perform our contract with you, performance of that contract; otherwise, our legitimate interests in monitoring, evaluating and improving our products and services. We will only disclose identifiable Personal Data to third parties for research purposes with your consent or as otherwise permitted by applicable Privacy Laws.
To communicate with you about your orders, account and the products and services you use, including service announcements such as scheduled maintenance (other than communications we send through the Apps on a Client's behalf, which are described in section 3)	Contact details, account details, order details	Performance of a contract with you; where our contract is with a Client, our legitimate interests in communicating with users of our products and services.

Purpose	Personal Data used	Legal basis
To send you marketing communications (directly or through our service providers), including about other VALD products and services that may be useful to you, competitions and trade promotions	Contact details, marketing preferences and information about how you use the Apps (such as which products and features you use)	Your consent, where required by law; otherwise our legitimate interests in promoting our products and services. You can opt out at any time (see section 6).
To advertise our products and services on third-party websites and platforms, including showing advertisements to people who have visited our websites	Online identifiers (such as cookie identifiers and IP address), information about your activity on our websites, and email addresses (usually in hashed form) where we use them to create custom audiences on advertising or social media platforms	Your consent, given through our cookie consent tool. You can withdraw your consent at any time by changing your cookie preferences. For custom audiences, your consent where required by law; otherwise our legitimate interests in promoting our products and services.
To keep our websites secure, prevent misuse of our websites and the Apps, and protect the rights, property or safety of VALD, our Clients and others	Website usage and device information, information about how the Apps and our APIs are used (including metadata about API requests), account details	Where necessary to perform our contract with you, performance of that contract; otherwise, our legitimate interests in protecting our business, users and systems.
To comply with applicable laws and our policy requirements, including in relation to occupational health and safety and environmental matters	Any Personal Data required	Compliance with a legal obligation under EU or UK law; otherwise our legitimate interests in complying with other laws that apply to us and with our internal policies.

2.3 We will only use or disclose Personal Data for a purpose other than for which it was collected or a related purpose if you have consented to such different use or disclosure or to the extent that such use or disclosure is permitted by applicable law. If you provide mobile contact information, we will not share that mobile contact information with third parties for marketing or promotional purposes. We will also not share your consent to be contacted using your mobile contact information with third parties who contact you for their own purposes.

2.4 In carrying out our business, it may be necessary to share information about you with and between our related bodies corporate and organisations that provide services to us. We would not otherwise routinely disclose Personal Data to an organisation other than as set out in this Privacy Policy unless:

(a) required or permitted by law;

(b) we believe it is necessary to provide you with a product or service which you have requested;

(c) it is necessary to protect the rights, property or personal safety of any of our Clients, any member of the public or our interests;

(d) the assets and operations of our business are transferred to another party as a going concern; or

(e) you have provided your consent.

3. CLIENT DATA AND OUR ROLE

3.1 Clients and their Authorised Users may use the Apps to collect and record Personal Data about Data Subjects, such as athletes and patients. Where they do, the Client determines what Personal Data is collected, the purposes for which it is used and the lawful basis for that processing.

3.2 We handle Client Data on the Client's behalf and on its documented instructions, in accordance with our agreement with the Client and, where applicable, our Data Processing Agreement. For the purposes of the GDPR, the Client is the controller and VALD is a processor of Client Data, except in the limited circumstances described in section 3.5. Where VALD is a business associate of a Client under HIPAA, section 15 also applies.

3.3 In addition to the table in section 2.2, the table below summarises the additional ways in which we handle Client Data as a processor on behalf of Clients:

Purpose	Basis on which VALD acts
Hosting, storing and displaying Client Data in the Apps, and receiving Client Data from, and sending it to, third-party platforms the Client connects to the Apps (for example, through an integration or API)	The Client's instructions, our agreement with the Client and, where applicable, the Data Processing Agreement and/ or Business Associate Agreement
Generating reports, analytics and normative comparisons for the Client and its Authorised Users, and providing AI Features (including processing Input and Output)	The Client's instructions, our agreement with the Client and, where applicable, the Data Processing Agreement and/ or Business Associate Agreement
De-identifying Client Data for inclusion in VALD's normative data set to provide comparative aggregated data, and creating VALD Insights (including normative reports for certain demographics)	The Client's instructions, our agreement with the Client and, where applicable, the Data Processing Agreement and/ or Business Associate Agreement
Maintaining and improving the Apps and services provided to the Client, including diagnosing and resolving issues and monitoring performance and reliability, and developing and improving our products and services using Client Data in pseudonymised form and information about how the Apps are used.	The Client's instructions, our agreement with the Client and, where applicable, the Data Processing Agreement and/ or Business Associate Agreement
Monitoring the use of the Apps (including AI Features) for security, misuse and compliance with our Terms of Use, including detecting and responding to security incidents	The Client's instructions, our agreement with the Client and, where applicable, the Data Processing Agreement and/ or Business Associate Agreement
Monitoring the use of patient-reported outcome measures, clinical outcome assessments, AI Features (including VALD AI) and our APIs (including metadata about API requests) for fair use and compliance with third-party licensing requirements	The Client's instructions, our agreement with the Client and, where applicable, the Data Processing Agreement and/ or Business Associate Agreement
Providing support, maintenance and troubleshooting	The Client's instructions, our agreement with the Client and, where applicable, the Data Processing Agreement and/ or Business Associate Agreement
Assisting the Client to respond to requests from Data Subjects	The Client's instructions, our agreement with the Client and, where applicable, the Data Processing Agreement and/ or Business Associate Agreement
Engaging service providers (sub-processors) to help us provide the Apps	The Client's instructions, our agreement with the Client and, where applicable, the Data Processing Agreement and/ or Business Associate Agreement

3.4 Clients are responsible for informing Data Subjects of the uses described in the table above and, to the extent they relate to Client Data, the table in section 2.2 and obtaining any consent or other permission

required under applicable Privacy Laws (see sections 10.4 and 10.6). Where Client Data includes protected health information that is subject to a Business Associate Agreement, we use and disclose it only as permitted by that agreement.

3.5 VALD acts as a controller only in the following limited circumstances:

(a) where we collect Personal Data for our own business purposes, rather than to provide our products and services to a Client, such as Personal Data about prospective Clients, visitors to our websites and social media accounts, suppliers and job applicants;

(b) where an individual creates an account directly with VALD in their personal capacity, rather than through a Client; and

(c) where we are required by law to process Personal Data, or need to do so to establish, exercise or defend legal claims.

Our purposes, and the legal bases we rely on, in these circumstances are set out in the table in section 2.2.

3.6 If your information is recorded by a Client, the Client's privacy policy will also apply, and requests about your information should generally be directed to that Client (see sections 9.5 and 10.10).

4. SERVICE PROVIDERS

4.1 Like most large organisations, we use a range of service providers to help us maximise the quality and efficiency of our products and services and our business operations. This means that individuals and organisations outside of VALD, such as cloud and web hosting service providers, software as a service providers, providers of IT support services, providers of analytics and marketing support services, providers of artificial intelligence services and online payment system providers, will sometimes have access to or be disclosed Personal Data held by us and may only use it on behalf of us to facilitate our services, provide services on our behalf, perform service-related services or assist us in analysing how our service is used. We take steps to ensure our service providers adhere to the same standard of privacy practices set out in this Privacy Policy, including not allowing the service providers to keep this information, nor to use it or disclose it for any unauthorised purposes. A list of the service providers that process Personal Data on our behalf (sub-processors), and further information about how we protect Personal Data, is available at Trust Centre (trust.vald.com).

4.2 Where you use AI Features, your Input and the Output generated may be transmitted to, and processed by, our third-party artificial intelligence providers on our behalf, solely to provide those features. We require those providers not to use that information to train or improve their own models.

5. DISCLOSURE OF PERSONAL DATA OUTSIDE THE JURISDICTION OF COLLECTION

General disclosure

5.1 We may access or process Personal Data outside of the jurisdiction in which it was collected which may include accessing or processing the data in Australia, the United Kingdom, the United States of America and countries in the European Economic Area. Our third-party artificial intelligence providers may also be located outside of the jurisdiction in which the Personal Data was collected. The privacy laws of those countries may not provide the same level of protection as the privacy laws of the country from which the Personal Data was collected. However, this does not change our commitments to safeguard your privacy and we will comply with laws applicable to cross-border data disclosure and processing.

Data transfers from the EEA and the United Kingdom

5.2 Where the GDPR applies, we will take all reasonable and necessary steps to ensure your Personal Data is treated securely and in accordance with this Privacy Policy and applicable Privacy Laws, and will not transfer Personal Data outside the EEA or the United Kingdom unless an appropriate safeguard is implemented (other than to a jurisdiction whose privacy laws have been deemed adequate by the European Commission or the UK Government, as applicable), such as entering into the EU Standard Contractual Clauses or the UK International Data Transfer Agreement or Addendum (or equivalent measures) with the party outside the EEA or the United Kingdom receiving the Personal Data.

6. DIRECT MARKETING

6.1 Like most businesses, marketing is important to our business' success. We therefore, from time to time, send marketing materials to current or prospective Clients and users of our products and services. This includes using your Personal Data (such as your contact details and information about which of our products and features you use) to tell you about other VALD products and services that may be useful to you. These communications may be sent on our behalf by our service providers, such as email and marketing platform providers, who may only use your Personal Data to provide those services to us. We only do so in accordance with applicable laws.

6.2 If you are receiving promotional information from us and do not wish to receive this information any longer, please use the unsubscribe link included in the message or contact VALD directly at DPO@vald.com asking to be removed from our mailing lists.

6.3 After you opt out or update your marketing preferences, please allow us sufficient time to process your marketing preferences. Unless otherwise required to process your requests earlier by law, it may take up to 5 business days to process your opt-out requests in relation to receipt of electronic marketing materials such as emails and SMS, and up to 30 days for all other marketing-related requests.

6.4 **Right to object to direct marketing.** You have the right to object at any time to our use of your Personal Data for direct marketing purposes. If you object, we will stop using your Personal Data for direct marketing.

7. WEBSITE AND APPS PRIVACY PRACTICES

7.1 We sometimes use cookie and similar tracking technology on VALD websites and the Apps to provide information and services to site visitors and improve your experience on our websites and the Apps. Cookies are pieces of information that a website transfers to your device for record-keeping purposes and are a necessary part of facilitating online transactions, and include standard internet log information and visitor behaviour information. Most web browsers are set to accept cookies. Cookies are useful to keep you signed in, remember your preferences, estimate our number of users and determine overall traffic patterns through our sites. With your consent where required by law, we also use advertising cookies and similar technologies provided by third parties to measure and deliver advertising, including on third-party websites (see section 15 if you are a California resident).

7.2 Where required by law, we will ask for your consent before placing non-essential cookies (such as analytics cookies) on your device, using the cookie consent tool on our websites. You can change your cookie preferences at any time through that tool, or set your browser to refuse cookies. Refusing cookies may mean you will not be able to take full advantage of the services on the websites and the Apps.

7.3 Google and other third parties collect data about traffic to our websites. Google Analytics uses cookies to monitor traffic to, and use of, our websites. Google uses this information on our behalf to evaluate your use of our websites, to compile reports on website activity, and to provide additional services connected with our websites. We will not identify you to Google, and will not merge Personal Data with non-personal data collected through this service. You can prevent the use of Google Analytics cookies by declining analytics cookies through our cookie consent tool or by adjusting the settings on your browser software, however, you may not be able to fully use all of the functions of our websites if you do so. If you would like to prevent Google's collection of data generated by your use of our websites (including your IP address), please download and install a browser plugin available at https://tools.google.com/dlpage/gaoptout?hl=en. Alternatively, you can find out how Google Analytics uses data when you use our websites, at www.google.com/policies/privacy/partners.

7.4 Some browsers offer a "Do Not Track" setting. Because there is no common industry standard for responding to these signals, our websites do not currently respond to them. We do, however, treat Global Privacy Control signals as a valid request to opt out of the sharing of Personal Data for advertising purposes (see section 15.6).

8. LINKS TO OTHER WEBSITES AND THIRD-PARTY COLLECTIONS

8.1 Our websites and the Apps may contain links to third-party websites or references to third-party apps. These linked sites and apps are not under our control and we are not responsible for the content of those sites nor are those sites or apps subject to our Privacy Policy. Before disclosing your Personal Data on any other website or app, we recommend that you examine the terms and conditions and

privacy policy of the relevant site. VALD is not responsible for any practices on third-party websites or apps that might breach your privacy.

8.2 VALD is not responsible for the privacy practices of Clients (including healthcare practices) that might breach your privacy.

8.3 The Apps may allow Clients and their Authorised Users to upload, link to or make available content hosted on third-party platforms (such as Dropbox), or to connect third-party platforms and applications to the Apps so that Personal Data is sent to or received from them (for example, through an integration or API). Those platforms are not our service providers, operate independently of VALD and handle Personal Data in accordance with their own terms and privacy policies.

9. ACCESSING AND CORRECTING THE INFORMATION WE KEEP ABOUT YOU

9.1 Sections 9.2 to 9.4 apply unless the GDPR applies to the processing of your Personal Data by VALD, in which case, instead, section 10 applies.

9.2 If at any time you want to know exactly what Personal Data we hold about you, you are welcome to request access to your record by contacting us at DPO@vald.com. We will make our file of your information available to you within a reasonable time from receipt of your request. We will only withhold access where permitted by law.

9.3 If at any time you wish to change Personal Data that we hold about you because it is inaccurate, incomplete, or out of date, please contact us at DPO@vald.com. If you wish to have your Personal Data deleted, please let us know in the same manner as referred to above and we will take all reasonable steps to delete it unless we need to keep it for legal reasons. You should note that you may update certain content and account details directly within the VALD websites and the Apps. You may also request deletion of your account by contacting support@vald.com.

9.4 We may charge a small fee to cover our costs of supplying the information. If we do not grant you access to your Personal Data or do not agree to correct your Personal Data, we will tell you why.

9.5 Where we hold your Personal Data on behalf of a Client (for example, where your profile is administered by a Client), your request will need to be directed to, or actioned by, that Client. We may refer your request to that Client.

10. ADDITIONAL INFORMATION FOR INDIVIDUALS IN THE EEA AND THE UNITED KINGDOM

10.1 This section 10 applies where the GDPR applies to the processing of your Personal Data by VALD.

Controller and contact details

10.2 VALD Pty Ltd is the controller of Personal Data only in the limited circumstances described in section 3.5. Where we process Personal Data (including Client Data), the Client is the controller (see section 3). As VALD's head office is located outside the European Union, VALD has appointed a representative in the European Union, who can be contacted at legal@vald.com. You can also contact our Data Protection Officer about any matter relating to the GDPR at DPO@vald.com.

Legal bases

10.3 The legal bases we rely on for each purpose are set out in the table in section 2.2. Where we rely on our legitimate interests, we have considered that those interests are not overridden by your interests or fundamental rights and freedoms.

10.4 Individuals in the EEA and the United Kingdom are intended to use the Apps only through a Client. Health information and other special categories of Personal Data recorded through the Apps therefore form part of Client Data, and the Client, as controller, is responsible for ensuring that a condition under Article 9 GDPR applies to that processing and for obtaining any applicable consent required from Data Subjects, except as described in sections 10.5 and 10.6.

10.5 If an individual creates an account directly with us rather than through a Client (for example, in error), we will, once we are notified of the account by the relevant Client or the individual, associate it with the relevant Client at the Client's request or delete it. Until then, we process any health information recorded in that account on the basis of the explicit consent the individual gives when creating the account and

accepting our Terms of Use (Article 9(2)(a) GDPR). We do not associate accounts created for VALD Academy with a Client.

10.6 VALD may also process Client Data as a processor to develop and improve the products and services we provide to our Clients (see section 3.3). For this processing, the Client, as controller, is responsible for ensuring that a condition under Article 9 GDPR applies, and obtaining any other permission from the Client required under applicable Privacy Laws. Otherwise, VALD only processes special categories of Personal Data as a controller where necessary for the establishment, exercise or defence of legal claims.

Automated decision-making

10.7 VALD does not make decisions based solely on automated processing (including profiling) that produce legal effects concerning you or similarly significantly affect you (see section 13.6).

International transfers

10.8 Information about transfers of Personal Data outside the EEA and the United Kingdom is set out in section 5.2.

Your rights

10.9 You have the right to:

(a) **Access.** You have the right to request a copy of the Personal Data we are processing about you, which we will provide back to you in electronic form. For your own privacy and security, in our discretion we may require you to prove your identity before providing the requested information. If you require multiple copies of your Personal Data, we may charge a reasonable administration fee.

(b) **Rectification.** You have the right to have incomplete or inaccurate Personal Data that we process about you corrected.

(c) **Deletion.** You have the right to request that we delete Personal Data that we process about you, except we are not obligated to do so if we need to retain such information in order to comply with a legal obligation or to establish, exercise or defend legal claims.

(d) **Restriction.** You have the right to restrict our processing of your Personal Data (so that we only process it) while we check its accuracy or consider your objection, or where our processing is unlawful or you need it kept for a legal claim. We will refer requests about Client Data to the relevant Client.

(e) **Portability.** You have the right to obtain Personal Data we hold about you, in a structured, electronic format, and to transmit such information to another data controller, where this is (a) Personal Data which you have provided to us, and (b) if we are processing that information on the basis of your consent (such as for direct marketing communications) or to perform a contract with you.

(f) **Objection.** Where the legal justification for our processing of your Personal Data is our legitimate interest, you have the right to object to such processing on grounds relating to your particular situation. We will abide by your request unless we have compelling legitimate grounds for the processing which override your interests and rights, or if we need to continue to process the information for the establishment, exercise or defence of a legal claim. You also have the right to object at any time to the processing of your Personal Data for direct marketing purposes (see section 6.4).

(g) **Withdrawing Consent.** If you have consented to our processing of your Personal Data, you have the right to withdraw your consent at any time, free of charge, by contacting us at DPO@vald.com or using the method described in the relevant section of this Privacy Policy. Withdrawal does not affect the lawfulness of processing based on your consent before it is withdrawn.

10.10 You can make any of these requests in relation to your Personal Data by sending the request to our Data Protection Officer by email at DPO@vald.com. Where your request relates to Client Data, we may refer your request to that Client and will assist the Client to respond in accordance with our Data Processing Agreement.

11. STORAGE AND SECURITY OF YOUR PERSONAL DATA

11.1 We will endeavour to implement appropriate technical and organisational measures to keep secure any information which we hold about you, and to keep this information accurate, up to date and complete, and to ensure a level of security appropriate to any risks which may be associated with the processing activities outlined in this Privacy Policy.

11.2 Your information is stored on secure servers that are protected in controlled facilities. These are third-party data storage services, including cloud service providers.

11.3 We require our personnel to respect the confidentiality of any Personal Data held by us.

11.4 We take all reasonable physical, administrative, and technological precautions to store and transmit data securely. For example, Personal Data is encrypted and held with reputable data storage providers. Other measures include computer firewall protection and computer maintenance to prevent unauthorised access. Further information about our security measures is available at our Trust Centre (trust.vald.com).

11.5 In addition to technological measures, VALD also places access controls on its employees and other partners. Our employees are subject to contractual confidentiality obligations that are consistent with this Privacy Policy. Despite these measures, VALD cannot guarantee that the information described in this Privacy Policy will be completely secure.

11.6 You should take reasonable steps to keep your devices and account credentials secure, and should notify us promptly at support@vald.com if you become aware of any actual or suspected unauthorised access to your account or to Personal Data held through the Apps. Where we issue API keys or other access tokens to a Client, the Client is responsible for keeping them secure and confidential, limiting access to them to authorised personnel, and notifying us promptly at the address above if it suspects a key has been compromised.

11.7 If a data breach occurs, we will deal with it in accordance with applicable Privacy Laws (including any applicable notification requirements) and, where applicable, our Data Processing Agreement and Business Associate Agreement.

12. RETENTION OF PERSONAL DATA

12.1 We will retain and process your Personal Data only for as long as is necessary for the purposes for which the information is collected. For Client Data, this generally means for the duration of our agreement with the relevant Client and until the Client deletes it or instructs us to delete it. For other Personal Data, this generally means for as long as your account remains active. In addition, we will retain and use your Personal Data to the extent necessary to comply with our legal obligations and exercise our legal rights (for example, if we are required to retain your data to comply with applicable laws), resolve disputes and enforce our legal agreements and policies.

12.2 When we no longer need to use your Personal Data or retain it to comply with legal obligations or to exercise our legal rights, we will take reasonable steps to remove it from our active systems or take steps to anonymise it so that you can no longer be identified from it in accordance with relevant Privacy Laws.

12.3 De-identified, anonymised or aggregated data that does not identify, and is not reasonably capable of being used to identify, any individual or Client may be retained and used by us after your account is closed or your relationship with us ends.

12.4 In deciding how long to retain Personal Data, we consider:

(a) for Client Data, the Client's instructions and our agreement with the Client. When a Client's subscription ends, we will retain, anonymise, delete or return Client Data in accordance with the Client's instructions, our agreement with the Client and, where applicable, the Data Processing Agreement or Business Associate Agreement;

(b) for account information, the period during which your account is active and any further period required for legal, tax, accounting or dispute resolution purposes;

(c) for marketing information, the period until you unsubscribe or object to direct marketing; and

(d) for pseudonymised Client Data used to develop and improve our products and services, until the data is no longer needed for that purpose or, if earlier, until the relevant Client instructs us to delete it or our agreement with the Client ends, unless the data has been de-identified.

13. ARTIFICIAL INTELLIGENCE FEATURES

13.1 Some Apps include AI Features, including VALD AI. When you use AI Features, we collect your Input and the Output generated in response, which may include Personal Data (including health information).

13.2 Where Input and Output form part of Client Data, we handle them on behalf of the Client as described in section 3. Otherwise, we use Input and Output to provide, maintain, develop and improve the Apps, to comply with our legal obligations, to enforce our Terms of Use and to ensure the security and proper functioning of the Apps. We do not use Input or Output to train artificial intelligence or machine learning models unless you or the relevant Client agree otherwise.

13.3 AI Features are operated using third-party artificial intelligence providers, as described in sections 4.2 and 5.1.

13.4 You should only include Personal Data in Input that is reasonably necessary for your use of the AI Features, and only where you are permitted to do so.

13.5 You may opt out of VALD AI by emailing support@vald.com. Opting out does not apply to other AI Features that we reasonably consider necessary to provide the Apps.

13.6 VALD does not use computer programs to make decisions about individuals, or to substantially and directly assist VALD in making decisions about individuals, that could reasonably be expected to significantly affect their rights or interests, and does not make decisions based solely on automated processing (including profiling) that produce legal effects or similarly significant effects. AI Features are decision-support tools only. They assist Clients and their Authorised Users, who remain responsible for any decisions they make, and any Output is intended to be reviewed by an appropriately qualified person.

14. CHILDREN

14.1 Individuals under the age of 18 (or any higher age of majority or age of digital consent that applies in their jurisdiction) (**Minors**) may only use the Apps with the prior consent of a parent or legal guardian. Where an account is created for a Minor directly, the Minor's parent or legal guardian consents on the Minor's behalf to the handling of the Minor's Personal Data as described in this Privacy Policy.

14.2 A parent or legal guardian may exercise the rights described in sections 9 and 10 on a Minor's behalf.

14.3 In the United States, the Children's Online Privacy Protection Act (**COPPA**) regulates the online collection of Personal Data from children under the age of 13. We do not knowingly collect Personal Data directly from children under 13. If you believe we have done so, please contact us at DPO@vald.com and we will take steps to delete that Personal Data.

15. ADDITIONAL INFORMATION FOR INDIVIDUALS IN THE UNITED STATES

15.1 Where VALD is a business associate of a Client under HIPAA, protected health information is handled in accordance with HIPAA and our Business Associate Agreement with that Client, which prevails over this Privacy Policy to the extent of any inconsistency in relation to that information.

15.2 Some US states have laws that regulate consumer health data or that give residents rights in relation to their Personal Data, which may include rights to access, correct and delete Personal Data and to opt out of certain processing. Where those laws apply to you, you may exercise those rights by contacting us at DPO@vald.com. We may need to verify your identity before responding, and you may appeal our decision on your request by contacting us at the same address.

California residents

15.3 If you are a California resident, the California Consumer Privacy Act (as amended by the California Privacy Rights Act) (**CCPA**) gives you additional rights in relation to your Personal Data. This section applies to Personal Data we collect as a business. It does not apply to Client Data, which we process as a service provider on behalf of Clients (see section 3). This Privacy Policy is our notice at collection for the purposes of the CCPA.

15.4 In the preceding 12 months, we have collected the following categories of Personal Data:

Category (with examples)	Disclosed for a business purpose to	Sold or shared?
Identifiers (such as name, email address, postal address, phone number, IP address, cookie identifiers and account name)	Our related bodies corporate and service providers	Online identifiers (such as IP address and cookie identifiers), and email addresses where we use them to create custom audiences on advertising or social media platforms, are shared with advertising partners. Other identifiers are not sold or shared.
Commercial information (such as products and services purchased, orders and warranty claims)	Our related bodies corporate and service providers	Not sold or shared
Internet or other electronic network activity (such as browsing history on our websites, information about how you use the Apps and interactions with our advertisements)	Our service providers, and analytics and advertising partners	Shared with advertising partners (website and advertising activity only). Information about how you use the Apps is not sold or shared
Approximate geolocation (derived from your IP address)	Our service providers, and analytics and advertising partners	Shared with advertising partners
Professional or employment-related information (such as job title, organisation, medical specialty and job application details)	Our related bodies corporate and service providers	Not sold or shared
Sensitive personal information (such as account log-in credentials and, where you create an account directly with us, health information such as test results and injury or case records)	Our service providers	Not sold or shared

15.5 We collect these categories of Personal Data from the sources described in section 1.5, for the purposes described in section 2.2, and retain them as described in section 12.

15.6 We do not sell Personal Data for money. However, we use advertising and retargeting tools on our websites, which may involve "sharing" Personal Data (such as online identifiers and browsing activity) with third parties for cross-context behavioural advertising, as defined in the CCPA. We may also use email addresses to create custom audiences on advertising or social media platforms. You can opt out of this sharing by changing your cookie preferences or by contacting us at DPO@vald.com.

15.7 We only use and disclose sensitive personal information for purposes permitted under the CCPA, and we do not use it to infer characteristics about you.

15.8 Subject to the CCPA, you have the right to:

(a) know what Personal Data we have collected about you, including the categories of Personal Data, the sources from which it was collected, the purposes for collecting, selling or sharing it, the categories of third parties to whom we disclose it, and the specific pieces of Personal Data we hold about you;

(b) request that we delete Personal Data we have collected from you;

(c) request that we correct inaccurate Personal Data we hold about you;

(d) opt out of the sale or sharing of your Personal Data (see section 15.6); and

(e) not be discriminated against for exercising any of these rights.

15.9 You can exercise these rights by contacting us at DPO@vald.com. We will need to verify your identity before responding to a request to know, delete or correct, by matching information you provide with information we hold. You may use an authorised agent to make a request on your behalf, and we may require the agent to provide proof that you have authorised them to do so.

16. CONTACTING US

16.1 If you have any concerns or complaints about how we handle your Personal Data, or if you have any questions about this Privacy Policy, please contact us at DPO@vald.com or at the address below:

Data Protection Officer
VALD Pty Ltd
PO Box 3208
Newstead QLD 4006
Australia

16.2 In most cases, we will ask that you put your request in writing to us. We will investigate complaints and will use reasonable endeavours to respond to you in writing within 30 days of receiving the written complaint.

17. FUTURE CHANGES

17.1 We operate in a dynamic business environment. Over time, aspects of our business may change as we respond to changing market conditions. This may require our policies to be reviewed and revised. We reserve the right to change this Privacy Policy at any time and notify you by posting an updated version of this Privacy Policy on the VALD websites and the Apps. If at any point we decide to use Personal Data in a manner materially different from that stated at the time it was collected, we will take reasonable steps to notify affected users (for example, by email, by a notice on our website or in the Apps) and, where required by law, obtain their consent.

18. KEY TERMS

In this Privacy Policy:

(a) **AI Features** means artificial intelligence or machine learning features made available in the Apps, including VALD AI, and **Input** and **Output** mean, respectively, the information you provide to AI Features and the output they generate;

(b) **Apps** has the meaning given in section 1.1;

(c) **Authorised User** means any person who accesses or uses the Apps on a Client's behalf or under a Client's account, such as a practitioner, coach or administrator;

(d) **Business Associate Agreement** means VALD's business associate agreement (www.vald.com/legal/business-associate-agreement);

(e) **CCPA** has the meaning given in section 15.3;

(f) **Client** means an organisation or individual that has entered into an agreement with VALD for the use of VALD products and/or services;

(g) **Client Data** means Personal Data that is provided to VALD by or on behalf of a Client through the use of VALD products or the Apps (including Personal Data about Data Subjects and Authorised Users, and information about how the Apps are used), and Personal Data that VALD generates, infers or derives from that Personal Data;

(h) **COPPA** has the meaning given in section 14.3;

(i) **Data Processing Agreement** means VALD's data processing agreement (www.vald.com/legal/data-processing-agreement);

(j) **Data Subject** means an individual whose Personal Data is collected, recorded or otherwise processed through the use of VALD products or the Apps, such as an athlete or patient;

(k) **EEA** means the European Economic Area;

(l) **GDPR** means the General Data Protection Regulation (Regulation (EU) 2016/679);

(m) **HIPAA** means the Health Insurance Portability and Accountability Act of 1996 (US);

(n) **Input** and **Output** have the meaning given in the definition of AI Features;

(o) **Minor** has the meaning given in section 14.1;

(p) **Personal Data** means any information about an identified or reasonably identifiable individual, including health information and any information treated as personal data, personal information or protected health information under applicable privacy laws;

(q) **Privacy Laws** has the meaning given in the introduction to this Privacy Policy;

(r) **Terms of Use** means the terms of use for the VALD Apps (www.vald.com/terms-and-conditions);

(s) **UK GDPR** means the GDPR as it forms part of the law of the United Kingdom, and references in this Privacy Policy to the GDPR include the UK GDPR where it applies; and

(t) **VALD Insights** means the databases, benchmarks, normative data, analytics, insights and other materials that VALD creates by applying its expertise, methods and analysis to de-identified, anonymised or aggregated data, which do not identify, and are not reasonably capable of being used to identify, any individual or Client.