Data Processing Agreement

This data processing agreement and its annexures ('**DPA**') are incorporated by reference into the agreement (as amended from time to time) between VALD ('**us**', '**we**', '**our**' or '**VALD**') and you ('**you**' or '**Client**') for the supply of VALD's Equipment and Software ('**Subscription Agreement'**). Execution of or otherwise accepting the Subscription Agreement constitutes acceptance of this DPA.

1 OPERATION OF THIS DPA

(a) This DPA reflects the parties' agreement with respect to our Processing of Personal Data for you in connection with your Subscription.

(b) VALD will only Process Personal Data in accordance with your Instructions. '**Instructions**' means any written, documented instructions issued by a Controller to a Processor (including any verbal instructions documented in writing, or any instructions given in the Subscription Agreement and this DPA, including those set out in Part B of Annexure 1), directing the Processor to perform a specific or general action with regard to Personal Data (including, but not limited to, depersonalising, blocking, deletion, making available).

(c) During the term of this DPA, which is the term of your Subscription Agreement, you may provide additional Instructions to us which must be consistent with:

(i) the scope, functionality and limitations of the services provided by us to you under the Subscription Agreement; and

(ii) the lawful use of the Subscription.

(d) You, as the Controller, acknowledge that any changes to the Instructions that require material modifications to the services we provide to you as the Processor, including but to limited to changes to system configurations, data handling procedures, or reporting requirements, may be subject to a feasibility assessment conducted by us and additional Fees and implementation timelines, as agreed between the parties. The Processor is not obliged to follow additional written Instructions that are technically unfeasible, unlawful, or outside the agreed scope of services under the Subscription Agreement and must promptly notify the Controller if any Instruction cannot be implemented for these reasons.

(e) Capitalised terms not defined in this DPA or by reference to Data Protection Laws have the meaning given to them in the Subscription Agreement. Unless otherwise agreed between the parties, the terms '**Controller**', '**Processor**', '**Processing**' and '**Personal Data**' have the meaning given to them under Data Protection Laws. '**Process'** has the same meaning as 'Processing'. '**Sub-Processor**' means a Processor that is engaged by a Processor, with the prior written authorisation of the applicable Controller. '**Data Protection Laws**' means all laws and regulations applicable to the Processing of Personal Data under the EU GDPR or the UK GDPR as applicable. '**EU GDPR**' means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), as may be amended, superseded or replaced. '**UK GDPR**' means the retained version of the EU GDPR incorporated into UK law under section 3 of the European Union (Withdrawal) Act 2018, and amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (as amended), as may be amended, superseded or replaced.

(f) An overview of the categories of Personal Data, the categories of '**Data Subjects**', and the nature and purposes for which the Personal Data are being processed by VALD are provided in Annexure 1. The security measures we undertake in respect of your data and to secure our environment are provided in Annexure 2 ('**Security Measures'**). All Personal Data processed by VALD in connection with providing the Equipment and services is obtained as part of either (i) Client Data or (ii) data that is generated, inferred,

or derived by VALD from Client Data. '**Client Data**' means all data that is provided to VALD by the Client (or on behalf of the Client to VALD) through any person's use of the Equipment and Software, or otherwise provided to VALD.

(g) This DPA is effective for the Subscription Period and any reasonable period after the end of the Subscription if:

(i) you have provided us with Instructions to retain Client Data; or

(ii) we are required by Data Protection Laws to hold your data for a longer period.

(h) When VALD introduces features, offerings, supplements, or related software that are either new or which were not previously included in your Subscription, VALD may provide terms or make updates to the DPA terms that are reasonably necessary to enable the Client's use of those new features, offerings, supplements, or related software.

2 ROLES AND RESPONSIBILITIES

2.1 General

(a) With respect to the Processing of Personal Data in connection with your Subscription, you are the Controller and VALD is the Processor. VALD may engage Sub-Processors in accordance with clause 4 of this DPA.

(b) When VALD acts as a Processor of Personal Data, it will only do so on the documented Instructions of the Controller.

(c) VALD Group has appointed a Data Protection Officer that can be contacted at DPO@vald.com. As VALD's head office is located outside of the European Union, VALD Group has appointed an European Union representative that can be contacted at legal@vald.com. Details of the representative's identity and specific location are available upon written request to legal@vald.com.

2.2 Your obligations

(a) You must comply with your obligations under Data Protection Laws. You must inform us without undue delay if you are not able to comply with your responsibilities under this DPA or Data Protection Laws.

(b) Without limiting the foregoing, you are solely responsible for:

(i) the accuracy, quality and legality of the Personal Data, including ensuring you have legally acquired the Personal Data in accordance with Data Protection Laws;

(ii) complying with all necessary transparency and other lawfulness requirements under Data Protection Laws required for VALD's lawful Processing of the Personal Data in accordance with your Instructions;

(iii) providing Data Subjects with all necessary notices and obtaining all necessary consents required for VALD's lawful Processing of the Personal Data for the purposes set out in your Instructions; and

(iv) ensuring you have the legal right to collect and transfer Personal Data to us, or to provide us with access to the Personal Data, in accordance with your Instructions and Data Protection Laws.

(c) You are responsible for independently determining whether the data security provided by VALD in relation to the Subscription will adequately meet your obligations under Data Protection Laws. You are also responsible for your secure use of the Subscription, including protecting the security of Personal Data in transit to and from VALD.

2.3 VALD's obligations

(a) VALD will only Process Personal Data for the purposes set out in your Instructions, except where and to the extent otherwise required by applicable law. We are not responsible for the compliance with any Data Protection Laws that are applicable to either you or your industry, that are not also generally applicable to us.

(b) If we become aware that a legal requirement in the Data Protection Laws that does not allow us to Process Personal Data in accordance with your Instructions, then we will:

(i) notify you without undue delay of the legal requirement to the extent we are permitted; and

(ii) where necessary, cease all such Processing (other than storing and maintaining the security of the relevant Personal Data) until such time as you issue new Instructions which we are able to comply with.

(c) To the extent that we cease Processing in accordance with clause 2.3(b)(ii), VALD will not be liable to you under the Subscription Agreement or this DPA for any failure to provide the Subscription for the period until such time as you issue new Instructions that we can comply with.

(d) Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risks, of varying likelihood and severity, for the rights and freedoms of natural persons, VALD shall implement appropriate technical and organisational measures to ensure a level of security for the Processing of Personal Data that is appropriate to such risks for the Processing of Personal Data, as detailed in the Security Measures. Notwithstanding any provision to the contrary, VALD may modify or update the Security Measures at our sole discretion provided that such modification or update does not result in a material degradation in the protection offered by the Security Measures.

(e) At your request:

(i) VALD shall provide you with reasonable cooperation and assistance required to fulfil your obligations under Data Protection Laws to carry out a data protection impact assessment that relates to the Client's use of the services under the Subscription Agreement, to the extent that:

(A) you do not otherwise have access to the relevant information; and

(B) such information is reasonably accessible by or available to VALD; and

(ii) VALD will also provide reasonable assistance to you in any prior consultation with the relevant supervisory authority to the extent required under Data Protection Laws.

(f) VALD will ensure that the personnel we engage to Process Personal Data enter into appropriate confidentiality obligations consistent with the confidentiality obligations under the Subscription Agreement, and have received appropriate training on.

(g) On termination or expiration of your Subscription Agreement, VALD will anonymise, delete or return all Personal Data that VALD holds under the Subscription Agreement. This term will apply except where VALD is required to retain the Personal Data in accordance with any applicable law, or where the Personal Data is archived on a back-up system, in which case that data will be securely stored for no longer than what is reasonably necessary, and ultimately deleted in accordance with VALD's policies. VALD will continue to comply with this DPA until your Personal Data is anonymised, deleted or returned.

3 DATA SUBJECT REQUESTS

(a) The VALD Software provides you with a number of controls you can use to retrieve, correct, delete or restrict Personal Data. You can use these controls to assist you in connection with your obligations under Data Protection Laws, including your obligations to respond to requests from Data Subjects to exercise their rights under Data Protection Laws ('**Data Subject Request**').

(b) To the extent that you are unable to independently address a Data Subject Request through the Software, then upon your written request we will provide reasonable assistance to you to respond to a Data Subject Request or requests from data protection authorities relating to the Processing of Personal Data under the Subscription Agreement. You agree to reimburse us for our commercially reasonable costs arising from such assistance.

(c) If a Data Subject Request or other communication regarding Processing of Personal Data in relation to the Subscription Agreement is made directly to us, then we will inform you of that request and will communicate this to the person or entity making this request. You will be solely responsible for responding substantively to any communications (including from VALD) pertaining to such Data Subject Requests or communications involving Personal Data unless we are otherwise required by Data Protection Laws to respond or communicate directly to them.

4 SUB-PROCESSORS

(a) You agree that VALD may engage Sub-Processors to Process Personal Data on your behalf. VALD engages Sub-Processors in the following ways:

(i) Sub-Processors that assist with hosting, storage and infrastructure services;

(ii) Sub-Processors that support product features and integrations; and

(iii) Sub-Processors that are members of VALD Group who we engage for service and support.

(b) A '**Sub-Processor**' means any Processor engaged by VALD or VALD Group to assist in fulfilling VALD's obligations with respect to the provision of the Subscription under the Subscription Agreement. Sub-Processors may include third parties or members of VALD Group, but excludes any VALD employees or consultants.

(c) A list of Sub-Processors currently appointed by VALD is available at https://trust.vald.com. That list of Sub-Processors may change from time to time. You may subscribe to receive notifications about changes to our list of Sub-Processors at https://trust.vald.com, in which case you will receive a notification of any changes to VALD's Sub-Processors.

(d) If you have a reasonable objection to the engagement of a new material Sub-Processor by VALD, then you have the opportunity to raise your objection within 7 days of the Sub-Processor being updated on https://trust.vald.com. If you notify us of an objection, then we agree to discuss your concerns in good faith with a view to achieving a commercially reasonable resolution. If a resolution cannot be reached within a reasonable period of time, which shall not exceed 60 days, we may, at our sole discretion:

(i) decline to appoint the new Sub-Processor;

(ii) replace the proposed new Sub-Processor with an alternative Sub-Processor; (iii) revert to the existing Sub-Processor; or

(iii) permit you to suspend or terminate the affected elements of your Subscription in accordance with the Subscription Agreement termination provisions (without any liability to either party, but without prejudice to any Fees or interest incurred by you under the Subscription Agreement prior to your exercise of suspension or termination rights under this clause).

If you do not object to a new Sub-Processor within the relevant 7 day period, you will be deemed to have authorised the appointment or replacement of the Sub-Processor that was contained in the notification.

(e) Where VALD engages a Sub-Processor that is engaged in the provision of the services in the Subscription Agreement, VALD will enter into an agreement with the Sub-Processor that requires the Sub-Processor to provide similar or better levels of protection for Personal Data than the requirements specified in this DPA. VALD will remain responsible for each Sub-Processor's compliance with the obligations in this DPA and for any acts or omissions of such Sub-Processors that cause us to breach any of VALD's obligations under the Subscription Agreement.

5 DATA TRANSFERS

(a) VALD will not transfer Personal Data to any country or recipient not recognised as providing an adequate level of protection for Personal Data (within the meaning of Data Protection Laws), unless VALD first takes all such measures as are necessary to ensure the transfer is in compliance with Data Protection Laws. Such measures may include (without limitation) transferring such data to a recipient that:

(i) is covered by a suitable framework or other legally adequate transfer mechanism recognised by the relevant authorities or courts as providing an adequate level of protection for Personal Data;

(ii) has achieved binding corporate rules authorisation in accordance with Data Protection Laws; or

(iii) has executed the Standard Contractual Clauses or an International Data Transfer Agreement,

in each case as adopted or approved in accordance with Data Protection Laws.

(b) The '**Standard Contractual Clauses**' or '**SCC**' means the terms available here which contain the standard contractual clauses approved by the European Commission's decision 2021/914 of 4 June 2021 and, to the extent that such 'Standard Contractual Clauses' are utilised in the future, such amendments or replacement of those clauses issued by the European Commission in the future.

(c) The '**International Data Transfer Agreement**' or '**IDTA**' means the terms available here which contain the international data transfer agreement and addendum terms approved by the UK Information Commissioner's Office for the transferring of personal data outside of the UK and, to the extent that such IDTA is utilised in the future, such amendments or replacement of that agreement that is issued by the UK Information Commissioner's Office in the future.

(d) Subject to clause 5(g), where the EU GDPR and clause 5(a)(iii) applies, the parties agree that the Standard Contractual Clauses will be incorporated by reference and form part of this DPA and form an agreement between you and VALD with the following selections for the relevant parts of the SCC:

(i) you are the 'data exporter' and VALD is the 'data importer';

(ii) the Module Two terms apply to the extent that you are a Controller of Personal Data and we are a Processor of that Personal Data;

(iii) in clause 7 of the SCCs, the optional docking clause does not apply;

(iv) in clause 9 of the SCCs, Option 2 applies and changes to Sub-Processors will be notified in accordance with clause 4 of this DPA;

(v) in clause 11 of the SCCs, the optional language is deleted;

(vi) in clause 17 of the SCCs, Option 1 applies, and the Member State law that applies is the Republic of Ireland;

(vii) in clause 18 of the SCCs, the parties agree that the governing law and forum for disputes for the SCCs will be the Republic of Ireland; and

(viii) the Annexures of the SCCs will be deemed complete with the information from the Annexures of this DPA.

(e) Subject to clause 5(g), where the UK GDPR and clause 5(a)(iii) of this DPA applies and the parties agree that the IDTA will be incorporated by reference and form part of this DPA and form an agreement between you and VALD with the following selections for the relevant parts of the IDTA:

(i) in Part 1 Table 1 (Parties and signatures), you are the 'Exporter' and VALD is the 'Importer' and the contact details for each will be as set out in Part A of Annexure 1 to this DPA;

(ii) in Part 1 Table 2 (Transfer Details):

(A) the UK country's law that governs the IDTA, and the primary place for legal claims to be made by the parties, will be England and Wales;

(B) you are the Exporter and Controller and VALD is your Importer and Processor;

(C) UK GDPR applies to the Importer's Processing of the Transferred Data;

(D) the 'Linked Agreement' is your Subscription Agreement, and the Term of the Linked Agreement is the period the Subscription Agreement is in force;

(E) the IDTA cannot be ended before the end of the Term unless there is a breach of the IDTA or you and VALD agree to end it by mutual agreement in writing;

(F) the Importer can end the IDTA as set out in section 29.2 of the IDTA;

(G) the Importer may transfer the 'Transferred Data' to another organisation or person in accordance with Section 16.1 of the IDTA, with no specific restrictions by you;

(H) the parties will review the 'Security Requirements' at least once every year;

(iii) in Part 1 Table 3 (Transferred Data):

(A) the categories of 'Transferred Data' are set out in Part B of Annexure 1 to this DPA, and will update automatically if the information is updated in the Linked Agreement;

(B) the Transferred Data does not include Special Categories of Personal Data;

(C) the categories of 'Data Subjects' is set out in Part B of Annexure 1 to this DPA, and the categories will update automatically if the information is updated in the Linked Agreement; and

(D) the Importer may Process the 'Transferred Data' for the purposes set out in Part B of Annexure 1 to this DPA, and the purposes will update automatically if the information is updated in the Linked Agreement;

(iv) in Part 1 Table 4, the security requirements will be as set out in Annexure 2 to this DPA, which may be updated automatically if the information is updated in the 'Linked Agreement' which includes amendments to this DPA;

(v) Parts 2 and 3 of the IDTA are not used; and

(vi) the Part 4 'Mandatory Clauses' of the IDTA apply.

(f) The parties agree that to the extent of any inconsistency between the terms of the SCCs or IDTA as applicable between you and VALD and the terms of this DPA, the SCC or IDTA terms will prevail.

(g) If VALD cannot comply with its obligations under the SCCs or IDTA or is in breach of the warranties under the SCCs or IDTA for any reason, and you intend to suspend the transfer of Personal Data to VALD or terminate the SCCs or IDTA, you agree to provide VALD with reasonable notice to enable VALD to cure such non-compliance and reasonably cooperate with VALD to identify what additional security measures, if any, may be implemented to remedy such non-compliance. If VALD has not or cannot cure the non-compliance, you may suspend or terminate the affected part of the Subscription in accordance with the Subscription Agreement without liability (but without prejudice to any fees you have incurred prior to such suspension or termination).

6 BREACH NOTIFICATION

(a) Upon becoming aware of a security breach that has resulted in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise Processed by VALD (each a '**Security Incident'**), VALD will promptly and without undue delay, but no later than 72 hours after becoming aware of the Security Incident, notify Client of the Security Incident. VALD's notification of or response to a Security Incident under this clause does not constitute any acknowledgement by VALD of any fault or liability with respect to the Security Incident.

(b) VALD will use all reasonable endeavours to assist the Client in fulling the Client's obligations under Article 33 of the EU GDPR, or any other Data Protection Laws relating to the Clients notification of the relevant supervisory authority and data subjects.

7 AUDIT

(a) VALD maintains an audit program to ensure compliance with Data Protection Laws, including conducting annual SOC 2 Type II audits, DSPT Toolkit audits and Cyber Essentials Assessments ('**Third-Party Audit Certifications**'). To demonstrate compliance with the obligations laid down under Data Protection Laws, and subject to the Client agreeing to any confidentiality obligations under the Subscription Agreement, VALD will, upon the Client's written request, make any applicable Third-Party Audit Certifications available at no cost to the Client.

(b) Client may request an audit of VALD's Processing activities that are covered by this DPA ('**Client Audit**'), either through itself or a Third-Party Auditor (as defined below) that is selected by the Client, provided:

(i) the Client provides VALD with written notice from a Third-Party Auditor of why the information under the Third-Party Audit Certifications is not sufficient to demonstrate VALD's compliance with Data Protection Laws; or

(ii) despite the Third-Party Audit Certifications, an audit is required by Data Protection Laws or by the Client's competent supervisory authority (as applicable).

Unless otherwise agreed between the parties, the scope of any Client Audits is limited to the Processing of your Personal Data and storage facilities operated by VALD. The Client acknowledges that VALD does not have a legal right to permit you or your appointed Third-Party Auditor to audit storage facilities operated by VALD's Sub-Processors.

(c) In this DPA, a '**Third-Party Auditor'** is a third-party independent contractor that is not a competitor of VALD. Audits can only be conducted through a Third-Party Auditor if, prior to any Client Audit, the Third-Party Auditor:

(i) enters into a non-disclosure agreement containing confidentiality provisions that protect VALD's proprietary information and are no less protective than the confidentiality arrangements provided under the Subscription Agreement; and

(ii) provides at least 90 days prior notice to VALD before the Client Audit, and only conducts an Client Audit at a time agreed to by VALD.

(d) Any audits additional to the Third-Party Audit Certifications (including the Client Audit) will occur at the Client's own expense, at a timeframe that is mutually agreed between the parties. Prior to the occurrence

of any such additional audits, the parties must also mutually agree upon the applicable scope, timing, duration, control and evidence requirements.

8 MISCELLANEOUS

8.1 Governing Law

This DPA will be governed by and construed in accordance with the governing law and jurisdiction provisions in the Subscription Agreement, unless otherwise required by Data Protection Laws or the SCCs as applicable in accordance with clause 5(c).

8.2 Limitation of liability

Despite anything to the contrary and to the extent permitted by law, the liability of each party under this DPA is subject to the exclusions and limitations set out in the Subscription Agreement.

Annexure 1

Part A – List of Parties

	Data Exporter	**Data Importer**
Name:	The person or entity defined as the Client in the Subscription Agreement.	The entity defined as VALD in the Subscription Agreement.
Address:	The address for the Client as set out in the Subscription Agreement.	The address for VALD as set out in the Subscription Agreement.
Contact details:	The contact details for the Client set out in the Subscription Agreement.	VALD's Data Protection Officer DPO@vald.com
Description of the Processing or transfer of Personal Data:	See Part B below.	See Part B below.
Role (Controller/Processor):	Controller	Processor

Part B – Description of the Processing or transfer of Personal Data

You instruct us to Process and transfer Personal Data in accordance with the table below.

	Description
Categories of Data Subjects whose Personal Data is Processed or transferred	Persons that use your services, where you collect data about that person using Equipment and Software, which may include patients and athletes. Your Personnel.
Categories of Personal Data Processed or transferred by the Processor on behalf of the Controller	VALD has the right to Process the following types of Personal Data on behalf of you: • Name; • Email address (or other authentication data); • Date of birth; • Sex at birth; • Video recordings and photos (optional but mandatory with the use of HumanTrak); • Sports (optional); • Position (optional); • Weight (optional); • Height (optional); • Various exercise measurements, forces, distances and speeds of movement; • Clinician notes (optional); • Team and Organisation Data; • Team names (optional); and • User roles and permissions (native to application).

	The categories of Personal Data include "data concerning health" and Personal Data that has been de-identified, pseudonymised and anonymised. For further information on data types and categories, please refer to the VALD Data Management Policy Appendix B available at https://trust.vald.com.
Storage and transfer of Personal Data	Your Personal Data will be stored at rest in the region you nominate as part of your onboarding. VALD may transfer your data to USA, Europe, and Australia, where VALD's client support and client success teams are based. VALD creates global normative reports by aggregating data that is in Europe. The transfer of data to Europe only includes de-identified data. VALD does not control or limit the regions from which you or your clients (including patients and athletes) may access or move Client Data.
Sensitive data Processed or transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures	Not applicable. However, to the extent we Process or transfer sensitive data, we have ensured our existing Security Measures (as further explained in Annexure 2) contain restrictions and safeguards for the relevant data. These include all of the following: strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.
The frequency of the transfer (e.g. whether data is transferred on a one-off or continuous basis)	Continuous basis.
Nature of the Processing or transfer	VALD will Process Personal Data in accordance with your Instructions. That Processing may include collection, organisation, storage, adaptation, alteration, retrieval, analysis, disclosure by transmission, dissemination, pseudonymisation, anonymisation, combination (with identifiable and anonymised data), erasure or destruction. VALD may also use automated means for the Processing or transfer of Personal Data.
Purpose(s) of the Processing or transfer	The dominant purpose of the processing is to present the objective measurement data collected by the Controller to the Controller as part of the Subscription provided under the Subscription Agreement. In addition, as part of the Subscription, the Controller receives access to normative reports (which allows comparison of data collected by the Controller with deidentified population norms). The purpose of de-identifying the data collected by the Controller is to include that data in the normative data set.
The period for which the Personal Data will be retained, or, if that is not possible, the criteria used to determine that period	Data will be processed for as long as reasonably required under Data Protection Laws or until data deletion is requested

	by the Client by emailing VALD's Data Protection Officer at DPO@vald.com.
For transfers to (sub-) processors, also specify subject matter, nature and duration of Processing	Details of the Sub-Processors used by VALD, and their purpose can be found at https://trust.vald.com.

Part C – Competent Supervisory Authority

For the purpose of the SCCs, the supervisory authority that will act as competent supervisory authority will be the authority located in the country identified in the Client's address or the Republic of Ireland.

Annexure 2 – Security Measures

1. Information Security Policy Statement

All VALD staff must adhere to VALD's Information Security Policy Statement. This document acknowledges our responsibilities as data custodians. Supporting policies and technical controls are available via our trust portal at https://trust.vald.com.

2. Access Controls

Preventing Unauthorised Product Access

- **Outsourced Processing:** VALD hosts our service with outsourced cloud infrastructure providers.
- **Contracts with vendors:** VALD maintains contractual relationships with vendors in order to provide the Software in accordance with our DPA. We rely on contractual agreements, privacy policies, and vendor compliance programs in order to protect data processed or stored by these vendors.
- **Physical and environmental security, and audits:** VALD hosts our product infrastructure with multi-tenant, outsourced infrastructure providers. We utilise the Microsoft Azure PaaS service. We do not own or maintain hardware located at the outsourced infrastructure providers' data centres. Production servers and client-facing applications are logically and physically secured from our internal corporate information systems. The infrastructure providers' physical and environmental security controls are audited for SOC 2 Type II compliance, among other certifications. Further details on our inherited compliance pertaining to physical and environmental security can be accessed via https://learn.microsoft.com/en-us/azure/compliance/.
- **Authentication:** VALD implements a uniform password policy for our client products. Clients who interact with the products via the user interface must authenticate their identity before accessing non-public Client Data.
- **Authorisation:** Personal Data is stored in multi-tenant storage systems accessible to you only via application user interfaces and application programming interfaces. You are not allowed direct access to the underlying application infrastructure. The authorisation model in each of our products is designed to ensure that only the appropriately assigned individuals can access relevant features, views, and customisation options. Authorisation to data sets is performed through validating the user's permissions against the attributes associated with each data set.
- **Application Programming Interface (API) access:** External product APIs may be accessed using OAuth authorisation. Our internal & external APIs are protected by different OAuth scopes.
- **VALD Data Access:** Access to Personal Data is strictly limited to authorised personnel based on role-based access controls.

Preventing Unauthorised Product Use: VALD implements industry standard access controls and detection capabilities for the internal networks that support its products.

- **Access controls:** Network access control mechanisms are designed to prevent network traffic using unauthorised protocols from reaching the product infrastructure. The technical measures implemented differ between infrastructure providers and include Virtual Private Cloud implementations, security group assignment, and traditional firewall rules.
- **Intrusion detection and prevention:** VALD leverages first-party cloud native technologies to protect our application supporting webservices. The technical measures implemented differ between infrastructure providers. All measures offer access hardening, detection, and cloud security posture management facilities.
- **Endpoint Harding:** Endpoints are hardened in accordance with industry standard practice. VALD APIs have been penetration tested by an external party. Workstations are protected using anti-malware and endpoint detection and response tools, receiving regular definition and signature updates.

Limitations of Privilege and Authorisation Requirements

- **Privileged Access Management**: Privileged access in our product environment is controlled, monitored, and removed in a timely fashion through "just in time access" (or '**JITA'**) controls.
- **Product access:** A subset of our employees has the capacity to access client environments. The intent of providing access to a subset of employees is to provide effective client support, support product development and research, to troubleshoot potential problems, to detect and respond to Security Incidents and implement appropriate data security measures. Access is enabled through JITA requests for access and all such requests are logged. Employees are granted access eligibility by role, with reviews of high-risk privilege grants performed monthly. A full review of all administrative or access, and user access permissions is performed at least once every three months.

3. Data, Encryption and Transmission Control

- **In-transit:** VALD utilises HTTPS for all application communication and encrypts traffic via TLS 1.3 or TLS 1.2 (for interoperability). Our HTTPS implementation uses industry standard algorithms and certificates.
- **At-rest:** All data within our estate is stored according using industry standard best practise patterns. We leverage the cloud-native storage and encryption technologies native to our cloud service provider. VALD chooses to leverage Auth0 for authentication.
- **Key Management:** Encryption keys are stored and managed exclusively within the country where the data resides.
- **Data Pseudonymisation:** Where applicable, data is pseudonymised prior to transfer with re-identification keys retained by the Processor in the country where the data resides.
- **Data retention:** Data retention policies ensure Personal Data is deleted when no longer necessary.

4. Incident Management, Logging, and Monitoring

- **Incident Response Plan:** We maintain a written Incident Response Plan, playbooks, and other necessary processes and procedures to fulfill the standards and obligations reflected therein.
- **Detection:** We have designed our infrastructure to log extensive information about system behaviour, traffic that is received, system authentication, and other application requests. Internal systems aggregate log data and alert appropriate employees of malicious, unintended, or anomalous activities. Our personnel, including security, operations, and support personnel, are responsive to known incidents.
- **Response and tracking:** We maintain a record of known Security Incidents that includes description, dates and times of relevant activities, and incident disposition. Suspected and confirmed Security Incidents are investigated by security, operations, or support personnel, and appropriate resolution steps are identified and documented. For any confirmed incidents, we will take appropriate steps to minimise product and Client damage or unauthorised disclosure. Notification Clients will be in accordance with the terms of the Agreement. See clause 6 of this DPA for further details on how we respond to Security Incidents.

5. Availability Control

- **Infrastructure availability:** VALD's infrastructure providers use commercially reasonable efforts to ensure a minimum of 99.95% uptime. The providers maintain a minimum of N+1 redundancy to power, network, and heating, ventilation and air conditioning services.
- **Fault tolerance:** Backup and replication strategies are designed to ensure redundancy and fail-over protections during a significant processing failure. Client Data is backed up to multiple durable data stores and replicated across multiple availability zones.
- **Online replicas and backups:** Where feasible, production databases are designed to replicate data between no less than 1 primary and 1 secondary instance. All databases are backed up and maintained using industry standard methods.

- **Disaster Recovery Plans:** We maintain and regularly test disaster recovery plans to help ensure availability of information following interruption to, or failure of, critical business processes. The server instances that support our products are architected as such to limit total product unavailability, in the event of an outage or service degradation from our upstream cloud service provider. This design assists our operations in maintaining and updating the product applications and backend while limiting downtime.

6. Vulnerability Management Program

- **Vulnerability Remediation Schedule:** VALD maintains a vulnerability remediation schedule aligned with industry standards. We take a risk-based approach to determining a vulnerability's applicability, likelihood, and impact in our environment.
- **Vulnerability scanning:** VALD performs daily vulnerability scanning on our products using technology and detection standards aligned with industry standards.
- **Penetration testing:** VALD commits to the annual penetration testing of both the VALD Hub web application product and our corporate networks. The intent of these penetration tests is to identify security vulnerabilities and mitigate the risks and business impacts they pose to the in-scope systems.

7. Personnel Management

- **VALD staff:** We employ qualified personnel to develop, maintain, and enhance our security program. We train all employees on security policy, processes, and standards relevant to their role and in accordance with industry practice.
- **Background checks:** Where permitted by applicable law, VALD employees undergo a third-party background or reference check. Employment offers are contingent upon the results of a third-party background check. All VALD employees are required to conduct themselves in a manner consistent with VALD's Code of Conduct, non-disclosure requirements, and ethical standards ordinarily applicable for companies that are of the same size and nature as VALD.