+45 70 20 31 24
info@auditdata.com
www.auditdata.com

SCHEDULE 5 DATA PROCESSING AGREEMENT (AUSTRALIA)

1. PREAMBLE

1.1 This Data Processing Agreement (this "Agreement") sets out the rights and obligations that apply to Auditdata's (the "Data Processor" or the "Service Provider") processing of personal data on behalf of the Customer (the "Data Controller" or the "APP Entity").

1.2 This Agreement has been designed to ensure the Parties' compliance with the *Privacy Act 1988 (Cth)* (the "Privacy Act") includes Privacy and Other Legislation Amendment Act 2024 and the *Australian Privacy Principles* ("APPs").

1.3 The Data Processor's processing of personal data shall take place for the purposes of fulfilment of the Parties Enterprise Master Service Agreement (the "MSA").

1.4 This Agreement shall take priority over any similar provisions contained in other agreements between the Parties, including the MSA.

1.5 This Agreement and the MSA shall be interdependent and cannot be terminated separately. This Agreement may however – without termination of the MSA – be replaced by an alternative valid data processing agreement.

1.6 Four appendices are attached to this Agreement. The Appendices form an integral part of this Agreement.

1.7 Appendix A of this Agreement contains details about the processing as well as the purpose and nature of the handling, type of personal information, categories of individuals and duration of the processing.

1.8 Appendix B of this Agreement contains the Data Controller's terms and conditions that apply to the Data Processor's use of Sub-Processors and a list of Sub-Processors approved by the Data Controller.

1.9 Appendix C of this Agreement contains instructions on the processing that the Data Processor is to perform on behalf of the Data Controller, the minimum security measures that are to be implemented, and how inspection with the Data Processor and any Sub-Processors is to be performed.

1.10 This Agreement and its associated Appendices shall be retained in writing as well as electronically by both Parties.

1.11 This Agreement shall not exempt the Data Processor from obligations to which the Data Processor is subject pursuant to the Privacy Act or other applicable legislation.

2. THE RIGHTS AND OBLIGATIONS OF THE DATA CONTROLLER

2.1 The Data Controller is responsible for ensuring that the handling of personal information complies with the Privacy Act, applicable Australian laws, and this Agreement.

+45 70 20 31 24
info@auditdata.com
www.auditdata.com

2.2 The Data Controller has both the right and obligation to make decisions about the purposes and means of the handling of personal information.

2.3 The Data Controller shall be responsible for ensuring that the processing of personal data, which the Data Processor is instructed to perform, has a legal basis.

3. THE DATA PROCESSOR ACTS ACCORDING TO INSTRUCTIONS

3.1 The Data Processor shall process personal information only on documented instructions from the Data Controller, unless required by Australian law to process otherwise.

3.2 Instructions from the Data Controller shall be specified in Appendices A and C. Additional instructions may be provided throughout the duration of the processing, provided they are documented.

3.3 The Data Processor shall immediately inform the Data Controller if, in the opinion of the Data Processor, any instruction contravenes the Privacy Act 1988 (Cth) or the APPs.

4. CONFIDENTIALITY

4.1 The Data Processor shall ensure that only authorised persons have access to the personal information and that access is promptly revoked when authorization ends.

4.2 Access shall be limited to those individuals who require it for the performance of their duties.

4.3 The Data Processor shall ensure that all authorised persons are bound by appropriate confidentiality obligations, either contractually or by law.

4.4 The Data Processor shall at the request of the Data Controller be able to demonstrate that the employees concerned are subject to the above confidentiality.

5. SECURITY OF PROCESSING

5.1 The Data Processor shall implement reasonable steps to protect personal information from misuse, interference, loss, unauthorized access, modification, or disclosure, as required by APP 11.

5.2 The Data Processor shall perform a risk assessment and implement measures to mitigate identified risks, considering the nature, scope, context, and purposes of processing. To this effect, the Data Controller shall provide the Data Processor with all information necessary to identify and evaluate such risks.

5.3 Security measures may include:

- Pseudonymization and encryption of personal information

+45 70 20 31 24
info@auditdata.com
www.auditdata.com

- Ensuring ongoing confidentiality, integrity, availability, and resilience of processing systems and services
- The ability to restore availability and access to personal information in a timely manner in the event of a physical or technical incident
- Regular testing, assessment, and evaluation of the effectiveness of technical and organizational measures

5.4 The Data Processor shall implement at least the security measures specified in Appendix C. Additional measures may be specified by the Data Controller as needed.

5.5 The Data Processor shall assist the Data Controller in ensuring compliance with APP 11 by providing information about the technical and organizational measures implemented.

5.6 Any additional security measures shall be subject to separate agreement, including remuneration terms.

6. USE OF SUB-PROCESSORS

6.1 The Data Processor shall not engage another processor (a "Sub-Processor") without the prior written consent of the Data Controller.

6.2 The Data Processor shall inform the Data Controller of any intended changes concerning the addition or replacement of Sub-Processors at least 30 days in advance.

6.3 When authorized to use a Sub-Processor, the Data Processor shall ensure that the Sub-Processor is subject to the same data protection obligations as those specified in this Agreement.

6.4 The Data Processor shall remain fully liable to the Data Controller for the performance of the Sub-Processor's obligations.

7. TRANSFER OF DATA TO THIRD COUNTRIES

7.1 The Data Processor may only transfer personal information outside Australia at the direction of the Data Controller, and must comply with the cross-border disclosure requirements in APP 8. APP 8 regulates the disclosure of personal information to an overseas recipient. According to APP 8.1, an "overseas recipient" is defined as a person or entity who is not in Australia or an external territory and is not the organization or the individual themselves.

The remote access to data stored in Australia does not constitute a cross-border disclosure under APP 8, as the data itself is not being physically transferred or disclosed to an overseas recipient. The data remains stored in Australia, and only authorized personnel are accessing it remotely.

+45 70 20 31 24
info@auditdata.com
www.auditdata.com

7.2 Transfers shall comply with APP 8, ensuring that reasonable steps are taken to ensure that the overseas recipient does not breach the APPs.

8. ASSISTANCE TO THE DATA CONTROLLER

8.1 The Data Processor shall assist the Data Controller in fulfilling obligations to respond to requests for the exercise of data subjects' rights under the Privacy Act 1988 (Cth), including:

- Notification obligations
- Rights of access, correction, and erasure
- Rights to restrict processing and data portability
- Rights to object to processing
- Rights related to automated decision-making (where applicable)

8.2 The Data Processor shall assist the Data Controller in ensuring compliance with relevant obligations under the Privacy Act, including:

- Implementing appropriate technical and organizational measures
- Reporting personal information breaches to the Office of the Australian Information Commissioner (OAIC) without undue delay
- Conducting privacy impact assessments where required
- Consulting with the OAIC if a privacy impact assessment indicates high risk

8.3 Assistance by Data Processor to Data Controller is subject to remuneration to Data Processor at the prices and terms set out in the MSA.

9. NOTIFICATION OF PERSONAL DATA BREACH

9.1 The Data Processor shall notify the Data Controller without undue delay, and preferably within 48 hours, of becoming aware of any actual or suspected personal information breach.
9.2 The Data Processor shall assist the Data Controller in assessing and responding to the breach, including providing:

- Description of the breach, including affected individuals and records
- Likely consequences of the breach
- Measures taken or proposed to address the breach and mitigate harm

10. ERASURE AND RETURN OF DATA

10.1 Upon termination of the data processing services, the Data Processor shall, at the Data Controller's discretion, erase or return all personal information and erase existing copies, unless retention is required by Australian law.

+45 70 20 31 24
info@auditdata.com
www.auditdata.com

11. INSPECTION AND AUDIT

11.1 The Data Processor shall make available to the Data Controller all information necessary to demonstrate compliance with the obligation laid down in the Privacy Act, the APPs, and this Agreement, and allow for and contribute to audits, including inspections performed by the Data Controller or another auditor mandated by the Data Controller.

11.2 The procedures applicable to the Data Controller's inspection of the Data Processor are specified in Appendix C to this Agreement.

11.3 The Data Controller's inspection of sub-processors, if applicable, shall as a rule be performed through the Data Processor. The procedures for such inspection are specified in Appendix C to this Agreement.

11.4 The Data Processor shall be required to provide the supervisory authorities, which pursuant to applicable legislation have access to the Data Controller's and Data Processor's facilities, or representatives acting on behalf of such supervisory authorities, with access to the Data Processor's physical facilities on presentation of appropriate identification.

12. THE PARTIES' AGREEMENT ON OTHER TERMS

12.1 The Parties may agree other terms concerning the provision of the personal data processing service, as long as they do not contradict directly or indirectly this Agreement or prejudice the fundamental rights or freedoms of the data subject and the protection afforded by the Privacy Act.

12.2 Any breach of this Agreement shall be treated as a breach of the MSA.

12.3 Other terms and commercial arrangements between the Parties shall be set out in the MSA.

13. COMMENCEMENT AND TERMINATION

13.1 This Agreement shall become effective on the date of both Parties' signs the MSA.

13.2 Both Parties shall be entitled to require this Agreement renegotiated if changes to the law or inexpediency of the provisions contained herein should give rise to such renegotiation.

13.3 This Agreement may be terminated according to the terms and conditions of termination, incl. notice of termination, specified in the MSA.

13.4 However, this Agreement shall apply for the duration of the personal data processing service. Irrespective of the termination of the MSA, this Agreement shall remain in force until the

+45 70 20 31 24
info@auditdata.com
www.auditdata.com

termination of the processing and the erasure of the data by the Data Processor and any Sub-Processors.

On behalf of the Data Processor,

Name: Denys Lebedev

Position: DPO

E-Mail: compliance@auditdata.com

APPENDIX A: INFORMATION ABOUT THE INFORMATION PROCESSING

A.1. The purpose of the Data Processor's processing of personal information on behalf of the Data Controller:

The purpose of the processing of personal information is for the Data Processor to deliver the service as described in the MSA to the Data Controller.

A.2. The Data Processor's processing of personal information on behalf of the Data Controller shall mainly pertain to (the nature of the processing):

The Data Processor delivers both a software service, a professional service, and tangible items to the Data Controller as described in the MSA. The processing therefore includes, following detailed instructions from the Data Controller, the collection, recording, structuring, storage, use, and if necessary, transfer of personal information.

A.3. The processing includes the following types of personal information about individuals:

(a) General personal information: name, e-mail, telephone number, address, payment details, and national identification number.

+45 70 20 31 24
info@auditdata.com
www.auditdata.com

(b) Sensitive information (as defined in the Privacy Act): Health information in relation to audiological examinations.

A.4. Processing includes the following categories of individuals:

The processing primarily involves the customers or patients of the Data Controller, and to some extent also employees of the Data Controller.

A.5. The Data Processor's processing of personal information has the following duration:

The duration of the processing of personal information is until the Data Processor's services have been terminated in accordance with the MSA, after which the personal information is either returned or deleted in accordance with Clause 10 of this Agreement.

APPENDIX B: TERMS OF THE DATA PROCESSOR'S USE OF SUB-PROCESSORS AND LIST OF APPROVED SUB-PROCESSORS

B1. Approved sub-processors

As of the effective date, the Data Controller approves the engagement of the following sub-processors:

(a) Microsoft Corporation and its affiliates in respect of the Azure public cloud (The purpose of engaging Microsoft is to utilize the Microsoft Azure hosting and storage facilities to provide the cloud-based services to Customers).

(b) [Insert others if applicable]

The Data Controller shall on the commencement of this Agreement specifically approve the use of the above sub-processors for the processing described for that party. The Data Processor shall

+45 70 20 31 24
info@auditdata.com
www.auditdata.com

not be entitled – without the Data Controller's explicit prior written consent – to engage a sub-processor for different processing than the one that has been agreed or have another sub-processor perform the described processing.

APPENDIX C: INSTRUCTION PERTAINING TO THE USE OF CUSTOMER DATA

C.1 The subject of/instruction for the processing

The Data Processor's processing of personal information on behalf of the Data Controller takes place by the Data Processor performing any processing necessary for the Data Processor to fulfill the obligations set out in the MSA.

Reference is also made to A.1 and A.2 of this Agreement.

C.2 Security of processing

The level of security shall take into account the large volume of personal data which also involves sensitive data. Therefore, a high level of security should be established.

The Data Processor has implemented appropriate technical and organizational measures to ensure a level of security appropriate to the risk of the processing. These measures include:

Domain: organization of information security

Security ownership. The Data Processor has appointed a security officer (CIO) responsible for coordinating and monitoring the security rules and procedures. The Data Processor is ISO 27001 certified.

Security roles and responsibilities. The Data Processor's personnel with access to personal data are subject to confidentiality obligations.

+45 70 20 31 24
info@auditdata.com
www.auditdata.com

Risk management program. The Data Processor performs a risk assessment before processing the personal data on behalf of the Data Controller. The Data Processor retains its security documents pursuant to its retention requirements after they are no longer in effect.

Domain: Asset management

Asset inventory. The Data Processor maintains an inventory of all assets on which the personal data is stored. Access to the inventories of such media is restricted to the Data Processor's personnel authorized by the management authorization process to have such access.

Asset handling

The Data Processor restricts access to personal data. The Data Controller may implement encryption of its personal data within its application.

The Data Processor imposes restrictions on printing personal data and has procedures for disposing of printed materials that contain personal data.

The Data Processor's personnel must obtain its authorization prior to storing personal data on portable devices, remotely accessing personal data, or processing personal data outside its facilities. This includes removing media (e.g., USB sticks and CD ROMs) and documents containing personal data from the Data Processor's facilities.

Domain: Human resources security

Security training. The Data Processor informs its personnel about relevant security procedures and their respective roles. The Data Processor also informs its personnel of possible consequences of breaching the security rules and procedures.

The Data Processor will only use anonymous data in training.

The Data Processor's personnel will not process personal data without authorization from the Data Controller. The Data Processor's personnel are obligated to maintain the security and secrecy of any personal data and this obligation continues even after their engagements end.

Product Development, IT Operations and Support staff may have access to data (only where necessary on a need to know basis).

Domain: Physical and environmental security

Physical access to facilities. The Data Processor (including subcontractors) limits access to facilities where information systems that process personal data are located to identified authorized individuals.

+45 70 20 31 24
info@auditdata.com
www.auditdata.com

Physical access to components. The Data Processor maintains records of the incoming and outgoing media containing personal data, including the kind of media, the authorized sender/recipients, date and time, the number of media and the types of personal data they contain.

Protection from disruptions. The Data Processor uses a variety of industry standard systems to protect against loss of data due to power supply failure or line interference.

Component disposal. The Data Processor uses industry standard processes to delete personal data when it is no longer needed.

Domain: Communications and operations management

Operational policy. The Data Processor maintains security documents describing its security measures and the relevant procedures and responsibilities of its personnel who have access to personal data.

Data recovery procedures

The data centre operating the Data Processor's products and services include replication features that facilitate recovery of personal data in the event a particular machine or cluster within a data centre fails. The Data Processor's products and services include a regular data backup procedure in addition to the data centre replication. The Data Processor is obligated to take backup of data stored within the Software according to the Data Processor's backup and data recovery procedure which is described below. If the Data Controller wants additional safety measures, then the Data Controller is responsible for taking additional steps to provide added fault tolerance, such as creating historical backups of personal data, storing backups of personal data off the platform, etc.

The Data Processor's cloud backup and data recovery procedure – SOP 30.0243, Auditdata internal IT backup and restore procedure in accordance with SOP 30.0251.

On an ongoing basis, but in no case less frequently than once a week (unless no personal data has been updated during that period), the Data Processor maintains multiple copies of personal data from which personal data can be recovered.

The Data Processor stores encrypted copies of personal data and data recovery procedures in a different place from where the primary computer equipment processing the personal data is located.

The Data Processor has specific procedures in place governing access to copies of personal data.

+45 70 20 31 24
info@auditdata.com
www.auditdata.com

The Data Processor logs data restoration efforts, including the description of the restored data, and where applicable, the person responsible and which data (if any) had to be input manually in the data recovery process.

Personal data not covered by the Data Processor Operations SLA's (e.g. temporary databases or data files for migration or trouble shooting etc.) is specifically chosen to not be covered by backup procedures, to reduce risk of non-compliance to data retention requirements.

Malicious software

The Data Processor has anti-malware controls to help avoid malicious software gaining unauthorized access to personal data including malicious software originating from public networks.

Data beyond boundaries

The Data Processor provides encrypting personal data transmitted to and from its data centres over public networks. The Data Processor uses encryption for replication of non-public personal data between its data centres.

The Data Processor restricts access to personal data in media leaving its facilities (e.g., through encryption).

Event logging. The Data Processor logs, or enables the data exporter to log, access and use of information systems containing personal data, registering the access ID, time, authorization granted or denied, and relevant activity.

Domain: Access control

The Data Processor maintains a record of security privileges of individuals having access to personal data.

Access authorization. The Data Processor maintains and updates a record of personnel authorized to access its systems that contain personal data.

The Data Processor deactivates authentication credentials that have not been used for a period of time not to exceed twelfth months.

The Data Processor identifies those personnel who may grant, alter, or cancel authorized access to data and resources.

The Data Processor ensures that where more than one individual has access to systems containing personal data, the individuals have separate identifiers/logins.

+45 70 20 31 24
info@auditdata.com
www.auditdata.com

The Data Processor uses industry standard practices to identify and authenticate users who attempt to access information systems.

Where authentication mechanisms are based on passwords, the Data Processor requires that the passwords are renewed regularly.

Where authentication mechanisms are based on passwords, The Data Processor requires the password to be at least eight characters long.

The Data Processor ensures that deactivated or expired identifiers are not granted to other individuals.

The Data Processor monitors or enables the data exporter to monitor repeated attempts to gain access to personal data using an invalid password.

The Data Processor maintains industry standard procedures to deactivate passwords that have been corrupted or inadvertently disclosed.

The Data Processor uses industry standard password protection practices, including practices designed to maintain the confidentiality and integrity of passwords when they are assigned and distributed, and during storage.

Network design. The Data Processor has controls to avoid individuals assuming access rights they have not been assigned to gain access to personal data they are not authorized to access.

Domain: Information security incident management

Incident response process. The Data Processor maintains a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the procedure for recovering data.

Service Monitoring. The Data Processor security personnel verify logs at least every six months to propose remediation efforts if necessary.

Domain: Business Continuity Management

The Data Processor maintains emergency and contingency plans for the facilities in which its information systems that process personal data are located.

The Data Processor's redundant storage and its procedures for recovering data are designed to attempt to reconstruct personal data to its last replicated state from before the time it was lost, unless it has been specifically decided to not keep data under backup, for data retention requirements compliance.

+45 70 20 31 24
info@auditdata.com
www.auditdata.com

Home/remote working

Working outside of the Data Processor's premises is called "Teleworking". While working outside of the Data Processor's premises, can users connect to the Data Processor's network using our secure Jumphost/direct access VPN connections.

The Data Processor cannot protect user's private computer against virus and theft, and users are not allowed to use this equipment to work with the Data Processor's information or transfer data between your private computer and the work computer.

Company Computers (desktop and laptops) are protected by being properly enrolled to the Data Processor's domain involving corporate managed access control, software patching, secure DNS (domain name server), antivirus system and global policies for local firewall management and automatic timeout screen lock protection. In addition, all laptop computers must have hard disk encryption activated.

C.3 Assistance to the Data Controller

The Data Processor shall, insofar as this is possible – within the scope and the extent of the assistance – assist the Data Controller in accordance with Clause 8.1 and 8.2 of this Agreement.

C.4 Storage period/erasure procedures

The personal data is stored for as long as the processing on behalf of the Data Controller is going on. The duration of the processing of personal data is until the Data Processor's services has been terminated in accordance with the MSA, after which the personal data is either returned or erased.

C.5 Processing location

Processing of the personal data under this Agreement cannot be performed at other locations, without the Data Controller's prior written consent, than: the Data Processor's headquarters or sites (Daughters) or at the locations of the (approved) Sub-Processors.

C.6 Instruction for or approval of the transfer of personal information to third countries

Personal information must be processed within Australia or jurisdictions with substantially similar privacy protections, unless the Data Controller provides express written instructions to allow transfer to another country, consistent with APP 8 and the requirements under the Privacy Act.

For more information see Clause 7 of this Agreement.

+45 70 20 31 24
info@auditdata.com
www.auditdata.com

C.7 Procedures for the Data Controller's audits, including inspections, of the processing of personal information by the Data Processor

The Data Controller may audit the Data Processor's compliance with this Agreement, the Privacy Act, and the APPs by:

- Requesting an annual audit report from an independent third party;
- Sending an annual compliance questionnaire; and/or
- Conducting an on-site inspection at the Data Processor's facilities annually.

C.8 Procedures for audits, including inspections, of the processing of personal information by Sub-Processors

The Data Processor shall annually ensure that Sub-Processors comply with the Privacy Act and APPs and this Agreement through:

- Obtaining an independent third-party audit report;
- Conducting physical inspections; or
- Distributing compliance questionnaires.

The results of such audits and checks shall be made available to the Data Controller upon request.