WiseTime
TIME FOR MORE

DATA PROCESSING AGREEMENT

The following data processing agreement (“Agreement”) is made between the customer (“Customer”) and Practice Insight Pty Ltd, 24 Colin Street, West Perth, WA 6005, Australia (“Processor”):

1. Subject of the Agreement

1. The Processor is the licensor of the WiseTime software suite, a cloud-based time recording software and service offered by the Processor. The Customer, having its place of business in the European Union (EU), is licensing the software (the "Main Agreement") for processing time data recorded using the WiseTime software suite.

2. The Processor utilizes private virtualized computing resources located exclusively at the Google Cloud Data Center in Frankfurt, Germany, to provide its services. The Processor’s service offering is therefore subject to the provisions of the GDPR; any data processing conducted by the Processor in the EU shall be subject to the present Data Processing Agreement.

3. In addition to the present Data Processing Agreement, the parties agree on Standard Contractual Clauses applying in cases of remote access by the Processor from Australia to the virtualized computing resources located at the Google Cloud Data Center in Frankfurt, Germany and the data stored therein for the purposes of technical support, software maintenance, software deployment, and software testing.

4. The aim of the processing of personal data by the Processor is to provide the services agreed in the Main Agreement. The categories of data subjects and personal data concerned by the processing are set out in Annex 1.

2. Location of the data processing

1. Notwithstanding section 1.3., the processing of personal data takes place exclusively in a member state of the European Union or in another state that is party to the Agreement on the European Economic Area, unless otherwise agreed with the Customer.

2. Any relocation of the order processing to a third country requires the prior consent of the customer and may only take place if the requirements of Article 44 et seq. GDPR are fulfilled.

3. Responsibility and right of instruction by the Customer

1. The Customer is the data controller within the meaning of Article 4 No. 7 GDPR. It is responsible for compliance with the statutory provisions on data protection, in particular for the lawfulness of the transmission of data to the Processor and for the lawfulness of the data processing by the Processor.

2. The Customer has the right to issue supplementary instructions to the Main Agreement regarding the type, scope and procedures for processing personal data at any time. Instructions can be given in text form.

3. The Processor shall inform the Customer immediately in text form if, in the Processor's opinion, an instruction issued by the Customer violates legal regulations. As long as the parties have not dispelled the Processor's concerns, the Processor shall be entitled to suspend the execution of the instruction in question. If the parties are unable to reach an agreement and the Customer adheres to its instructions, the Processor shall be entitled to terminate this Agreement with a reasonable notice period, which shall not be less than two weeks. If in this case the Main Agreement cannot be executed, the Processor is entitled to terminate the Main Agreement if it can only be executed by implementing the instructions and this was not apparent to either party at the time of conclusion of the contract.

4. If the Processor is of the opinion that it is unable to follow the instructions by the Customer for technical reasons, it shall inform the Customer thereof in text form and shall consult with the Customer for further action.

4. Duties of the Processor

1. Any processing of personal data shall be carried out exclusively in accordance with the provisions of the Main Agreement and any instructions issued by the Customer. This also applies to the transfer of personal data to a third country or international organization. This paragraph 1 shall not apply where the Processor is obliged to process personal data by the law of the Union or of the Member States to which it is subject, in which case the Processor shall notify the Customer of these legal requirements prior to processing, unless the law concerned prohibits such notification on grounds of an important public interest.

2. The Processor confirms that it is not legally obliged to appoint a data protection officer within the meaning of the GDPR. In its place, the Processor shall appoint a contact person for the Customer for all data protection issues and the implementation of this contract.

3. The Processor shall bind any person authorized to process personal data to confidentiality unless they are already subject to an appropriate statutory duty of confidentiality. The scope of the obligation shall be in reasonable proportion to the data processed and the consequences of any breach of the protection of personal data. Any further obligations resulting from a separate confidentiality agreement concluded between the parties shall remain unaffected.

4. Upon request, the Processor shall provide its records of processing activities in respect to the processing for the Customer.

5. Taking into account the type of processing and the information available to the Processor, the Processor shall assist the Customer in complying with the obligations set out in Articles 32 to 36 GDPR. To this end, the Processor shall in particular provide the services provided for in this Agreement.

6. As far as necessary, the Processor shall support the Customer in carrying out a data protection impact assessment in accordance with Article 35 GDPR and shall provide the Customer with all information required for this from its sphere. The Processor shall be obligated accordingly if the Customer is required to conduct a prior consultation with a supervisory authority in accordance with Article 36 GDPR. For the services to be rendered under this paragraph, the Processor is entitled to an appropriate remuneration based on the time spent. The Processor may not make the performance of the services owed by him dependent on the Customer's acceptance and/or advance payment of a specific remuneration.

7. At the justified request of the Customer, the Processor shall provide the Customer with the information necessary to prove that the Processor has complied with the obligations incumbent on it under Article 28 GDPR.

8. If the data of the Customer are endangered by seizure, confiscation, insolvency or composition proceedings or by other events or measures of third parties or if such measures have been taken, the Processor must inform the Customer without undue delay, unless this is not permitted by law. Furthermore, the Processor is obliged to inform all relevant third parties that the data is personal data for which the Customer is controller and that the Processor only acts as processor.

5. Duties of the Customer

The Customer must inform the Processor immediately, stating the reasons, if it discovers errors or irregularities in the results of the processing or with regard to the Processor's activities with regard to the specifications of this contract or the GDPR.

6. Security

1. The Processor shall take all required measures under Article 32 GDPR, in particular appropriate technical and organizational measures, to ensure a level of protection appropriate to the risk of data processing. At the time of the conclusion of this Agreement these are the measures described in Annex 2. The Processor must prove compliance with these requirements to the Customer by suitable means upon request.

2. In order to adapt to changed technical or legal conditions, the Processor is entitled to make changes to the measures described in Annex 2. Changes that could affect the integrity, confidentiality or availability of personal data, increase the risks to the rights and freedoms of those affected by the processing or generally reduce the agreed level of protection require the consent of the Customer. Other changes, in particular an improvement of the measures taken, can be implemented by the Processor without the consent of the Customer. After such changes have been made, the Processor shall adapt Annex 2 accordingly and shall, without undue delay, send a current version of Annex 2 to the Customer or point out to the Customer where the new version is made available on the Processor's website.

3. The Processor shall regularly evaluate its internal processes and the technical and organizational measures to ensure that the processing in its sphere of responsibility is carried out in accordance with the requirements of this Agreement and the applicable data protection law.

7. Rights of Data Subjects

1. The Processor shall, insofar as it is possible and reasonable, support the Customer with suitable technical and organizational measures to comply with its obligation to respond to requests to exercise the rights of the data subjects as set out in Chapter 3 GDPR. For this purpose, the Customer shall inform the Processor in text form which supporting action of the Processor it requires and to this extent provide the Processor with the data required to fulfill the request. If one party requires further information from the other party, it shall notify the latter without undue delay in text form. The Processor shall perform its services within a reasonable period of time so that the Customer can meet any legal deadlines incumbent upon him. The Processor shall inform the Customer without undue delay, stating the reasons, if it is not in a position to perform the requested service in time.

2. If a data subject contacts the Processor directly in order to exercise the rights to which it is entitled under Chapter 3 GDPR, the Processor will refer the data subject to the Customer, insofar as it is possible for the Processor to assign the data subject to the Customer. If it is not possible for the Processor to make such assignment and if the Processor is not a controller vis-à-vis the data subject, the Processor will inform the data subject that the Processor is acting as a processor for third parties and that it cannot identify the relevant third party with regard to the data subject. If and to the extent that

the Processor is itself controller and responsible pursuant to Chapter 3 GDPR, the Processor alone shall be responsible for fulfilling the corresponding obligations.

3. For the services to be rendered to the Customer under this clause, the Processor is entitled to an appropriate remuneration based on the time spent. The Processor may not make the performance of the services owed by him dependent on the Customer's acceptance and/or advance payment of a specific remuneration.

8. Control Rights of the Customer

1. The Customer is entitled to inspections, which are necessary to comply with the obligations incumbent on him according to the GDPR. The right of inspection is to be exercised with a reasonable notice period and during the normal business hours of the Processor. In order to reduce the effects of inspections on its business operations, the Processor is entitled to combine them with those of other Customers, insofar as this is reasonable for the Customer (e.g. joint inspection dates carried out within a reasonable period of time). The Customer shall ensure that inspections are only carried out to the extent necessary in order not to disrupt the Processor's business operations disproportionately.

2. The Customer is entitled to transfer execution of the inspections to a third party commissioned and paid for by the Customer. If the third party is in a competitive relationship with the Processor, the Processor has a right of refusal against the Customer's activities.

3. The Processor shall cooperate to the extent necessary in exercising the inspection by the Customer. The Processor is entitled to make inspections depend on the execution of a customary and appropriate confidentiality agreement, insofar as this is necessary to protect the Processor’s business secrets in accordance with the statutory provisions it is subjected to.

4. For the services to be rendered under this clause, the Processor shall be entitled to reasonable remuneration based on the time spent. The Processor may not make the performance of the services owed by him dependent on the Customer's acceptance and/or advance payment of a specific remuneration.

9. Actions by Supervisory Authorities

1. The Processor shall, as far as permissible, inform the Customer without undue delay of actions and measures of a supervisory authority, as far as they relate to this Agreement. This shall apply in particular if a supervisory authority investigates in the course of administrative offence or criminal proceedings with regard to the data processing by the Processor.

2. Insofar as the Customer, for its part, is subject to an inspection by a supervisory authority in the course of an administrative offence or criminal proceedings, a liability claim of a data subject or a third party or any other claim in connection with the data processing by the Processor, the Processor shall support the data subject to the extent necessary. For the services to be rendered in this respect, the Processor shall be entitled to a reasonable remuneration based on the time spent, if and to the extent that the Processor is not responsible for the corresponding action and measures by the supervisory authority. The Processor may not make the performance of the services owed by him dependent on the fact that the Customer accepts and/or makes advance payment of a specific remuneration.

10. Subprocessors

1. The Processor uses the sub-processors listed in Annex 3 for processing.

2. The Processor shall inform the Customer in text form about changes to the assignment of sub-processors. For this purpose, the Processor shall send the following information to the Customer in text form:

3. Description of the planned change;

4. Name and address of the sub-processor;

5. which services the sub-processor shall provide and which personal data and category of data subjects are concerned;

6. the content of the relevant agreements with the sub-processor and, where applicable, all evidence of compliance with Chapter 5 GDPR;

7. the above information shall also be made available for all other sub-processors who are to provide corresponding services below a sub-processor.

8. The Customer may object to the change within a period of two weeks after receipt of the information. The Processor will not implement the change before the end of the objection period. In the event of an objection, the Processor is entitled to terminate this Agreement with a notice period of at least one month, provided that the change would have been acceptable for the Customer and the objection is unreasonable to accept by the Processor. Reasonableness for the Customer is given if no disadvantages for the Customer would arise with the change and in particular it is ensured that the requirements of this Agreement and the GDPR would have continued to be observed when implementing the change. Unacceptability of the objection for the Processor is given if it provides its data processing services as an essentially uniform process for a large number of customers and individual deviations in the sub-processors can only be

implement with unreasonable effort (e.g. all customers use the same, standardized software platform).

9. The Processor shall comply with the stipulations set out in paragraphs 2 and 4 of Article 28 GDPR for any sub-processors. The Processor shall also ensure that the contractual agreements otherwise made with the Customer in this respect and any additional instructions made by the Customer are also complied with by the sub-processors. The Processor must provide evidence of this to the Customer at its request.

11. Violation of Data Protection Regulations, Agreements or Instructions

1. The Processor is obliged to notify the Customer in text form of any violation of data protection regulations, of the agreements made and/or the instructions given without undue delay but at the latest 48 hours after becoming aware of such violation. The corresponding notification shall contain at least the following information:

    a. A description of the nature of the breach, specifying, where possible, the nature and quantity of the data concerned and the categories of data subjects;

    b. The name and contact details of the data protection officer or other contact point for further information;

    c. A description of the probable consequences of the violation of personal data protection;

2. A description of the measures taken or proposed by the Controller to remedy the violation of the protection of personal data and, where appropriate, measures to mitigate its possible adverse effects.

3. Any and all necessary notification to a supervisory authority or information of affected persons is the sole responsibility of the Customer. The Processor will cooperate in this to the necessary extent.

4. The Processor is further obliged to investigate the infringement to the required extent without undue delay and to provide the Customer with appropriate documentation. The documentation shall include a description of the measures taken by the Processor to prevent further infringements and why it believes that the measures taken are sufficient to comply with the provisions of this Agreement and the statutory provisions.

12. Remuneration of the Processor

The Processor shall not be entitled to any separate remuneration for the services rendered under this Agreement, unless otherwise agreed in this Agreement.

13. Term of the Agreement

The term of this Agreement shall depend on the term of the Main Agreement. It can only be terminated in isolation from the Main Agreement for good cause, unless this Agreement or mandatory legal provisions stipulate otherwise.

14. Consequences of the Termination of the Agreement

1. Upon completion of the provision of the processing services, the Processor shall, at the choice of the Customer, either delete or return all personal data and delete the existing copies, unless there is an obligation to store the personal data under EU law or the law of the member states to which the Processor is subject. The Processor shall confirm to the Customer that the deletion has been carried out in accordance with the Customer 's instructions.
2. The Customer has the right to inspection of the complete and contractual return and deletion of the data by the Processor. The stipulations of Section 8 apply.
3. Any right of retention of the Processor with regard to the processed data and the associated data carriers is otherwise excluded, except for justifiable reasons.

ANNEX 1 – CATEGORIES OF PERSONAL DATA AND DATA SUBJECTS

Data subjects: The personal data transferred concern the following categories of data subjects: data exporter’s representatives and end-users including employees, contractors, and collaborators.

Categories of data: User information, including memberships of a user with a team; usage data in respect to devices on which the WiseTime software is installed on, e.g. applications used, names of documents viewed or edited in an application, subject line information of emails viewed or edited, names of websites browsed, data entered inside the WiseTime application and console by a user, e.g. tags, billing narratives, and manual task descriptions

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

For processing of the personal data, the Processor uses Google Cloud by agreement with Google Australia Pty Limited. Processing of the personal data by Google is subject to the Google data processor agreement pursuant to Art. 28 GDPR. The datacenter in Frankfurt, Germany, is the sole Google data center used by data importer. The measures taken by Google in accordance to Sec. 32 GDPR are specified on https://cloud.google.com/security/compliance/. Data Importer does not transfer the data from the Frankfurt datacenter to third countries.

Confidentiality (Art. 32 para. 1 b DSGVO):

Access to computer systems and network drives is restricted to authorized users.

An authorization concept exists. The authorization concept includes the administration of the access rights by system administrators and the application, approval, allocation and return of access authorizations.

Successful/attempted security breaches are logged and evaluated.

All devices use user accounts portected by passwords with individual accounts for each user on a per devices basis. Each password has to comply with the password policy:

- The password consists of at least 8 characters (randomly selected uppercase, lowercase, special characters and numbers),
- generic terms or proper names may not be used as passwords.

Authentication takes place via user name and password; there is a regulation for the case of absence (vacation, disease etc.).
Authorizations are checked regularly.

The password is immediately blocked if the authorization expires.

An authorized person is automatically logged off the system in case of inactivity.

In case of unsuccessful attempts to enter user credentials, the user ID is blocked.

Access to data is restricted on a strict need to know and need to access basis.

Internal networks are sealed off against external access by firewalls according to the state of the art.

Private storage media are forbidden by contract or by organizational instructions.

There are organizational instructions for downloading apps to business devices.

Internal networks are protected against external access (firewall etc.) according to the state of the art.

Appropriate access from outside is secured by using Virtual Private Network (VPN).

Internal interfaces (USB port, CD drives etc.) on end devices are blocked or comparably secured.

Data/hard disks of portable devices are encrypted.

Authorized access from outside (VPN, SSH and similar protocols) is secured by two or more authentication factors.

Internal and external networks are completely separated.

Separation control and pseudonymization (Art. 32 para. 1 a GDPR):

Offices are not shared with third parties.

If data is stored for more than one processor this is done under documentation of the purposes for which the data are to be processed.

Data for more than one controller are processed with clear definition of access rights.

Development, test and production systems are separated.

Access restrictions for individual folders, records, fields (database rights) are defined.

Particularly sensitive data is stored on separate servers.

Integrity, transfer control, order control and remote maintenance (Art. 32 para. 1 b GDPR):

Systems used to process data displays or other output devices are arranged in a way so that unauthorized third parties cannot gain access to data.

Firewalls are active on all workstations.

Documentation/logging is used for

- data recipient(s)
- persons authorized to pass on data
- data to be transmitted
- retrieval and transmission programs

Portable devices (USB sticks, external hard disks, laptops, smartphones, etc.) containing personal data may only be used by employees who are specifically authorized.

Data on portable data media is encrypted.

Important logs (e.g. of servers that process personal data) are evaluated by monitoring and those responsible are alerted if necessary (SIEM).

Major systems have automated intrusion detection (IDS).

Network accesses have automated blocking rules for defence against attacks (IPS).

Retrieval and transmission processes are logged.

Cryptographic encryption methods are used (e.g. PGP, S/MIME); at least 256bit encryption is used.

Data transfers takes place via secured connections (e.g. https/SFTP).

Versioning of files and logging of changes and source of a change.

For remote access state of the art encryption is used.

Organizational measures to ensure the security of the processing of personal data (Art. 32 para.1 d GDPR):

A company data protection officer and company information security officer have been appointed.

The data protection officer/information security officer or employees commissioned by him or by the management carry out regular internal checks on compliance with the technical and organizational data security measures.

All employees who process personal data are obliged to maintain confidentiality (data secrecy); external staff is also obliged to maintain confidentiality.

Data protection training courses for employees are held at regular intervals.

Information security training courses for employees are held at regular intervals.

Availability and reliability of data processing systems (Art. 32 para. 1 b GDPR):

We refer to the measures taken by Google in accordance with Sec. 32 GDPR as Google operates the systems.

In addition:

- patch management to keep software up to date,
- use of anti-virus software that is constantly updated,
- procedures are used to regularly review, assess and evaluate the reliability of the data processing systems,

- Implementation of penetration testing.

Restorability of data and data access after physical or technical incident and control procedures (Art. 32 para. 1c GDPR):

Usage of fail over systems, data duplication and encrypted data backups.

Disaster recovery and data recovery procedures that are regularly tested and evaluated.

Backups are automatically deleted after having reached the retention period.

Procedures for the regular review, assessment and evaluation of the effectiveness of data security (Art. 32 para. 1 d GDPR):

A risk analysis to identify critical applications and systems was conducted, documented and is regularly updated.

A technical check of the data processing systems is carried out at least bi-annually.

The systems are checked each quarter by an external vulnerability scan.

Logs of all activities on the data processing system are evaluated at regular intervals for any irregularities.

Security incidents are documented and evaluated.

The awareness of employees is checked by regular (at least half-yearly) exercises such as phishing tests.

APPENDIX 3 – SUBCONTRACT PROCESSORS

Google Australia Pty Limited
Level 5, 48 Pirrama Road
Pyrmont NSW 2009
Australia

Hosting of the WiseTime platform for EU customers at the Frankfurt, Germany, datacenter.

The measures taken by Google to protect personal data in accordance with Article 32 DSGVO are specified on: https://cloud.google.com/security/compliance/