Data Protection Agreement for End-Users Purchased Products From Authorized Distributors

This Data Protection Agreement ("**Agreement**") is executed by and between you (the "**Controller**") and Itamar™ Medical Ltd. and its affiliates ("**Processor**"), with regard to the processing of PII (as defined below), in accordance with any applicable Distribution Agreement ("**Main Agreement**") between Processor and authorized Distributor of the Processor ("**Distributor**").

Processor shall comply with the following in respect of personal data and/or personal identifiable information (hereinafter "**PII**") (as defined under Regulation (EU) 2016/679 (General Data Protection Regulation) the "**EU GDPR**", the EU GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 (the "**UK GDPR**"), together the "**GDPR**".

1. **Controller's Compliance**. Controller's instructions for processing of PII shall comply with all applicable privacy and data protection laws, including (as applicable) the GDPR, the UK Data Protection Act 2018 and the French Data Protection Act n°78/17 6 January 1978. Controller shall have sole responsibility for the accuracy, quality and legality of PII and the means by which Controller acquired PII.

2. **Details of Processing**. The details of the processing activities to be carried out by Processor are specified in **Annex 1**.

3. **Processing only on documented instructions:** The Processor will only process PII on documented instructions from the Controller, unless required to do so by law to which Processor is subject. In such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest. The parties agree that all documented instructions regarding the processing are contained within this Agreement and the Main Agreement. The parties also agree that any further instructions regarding the processing of PII must be provided in writing by the Controller to the Processor and they must be consistent with the Processor's preexisting obligations under this Agreement and the Main Agreement.

4. **Data Subjects Rights**. Processor shall assist Controller, by using appropriate technical and organizational measures, in the fulfillment of Controller's obligations to respond to requests by data subjects in exercising their rights under applicable laws.

5. **Data Subject Information.** Controller represents and warrants that, where it provides any PII to Processor for processing or where it contacts any data subjects through the PII provided by Processor:

   (a) it has duly informed the relevant data subjects of their rights and obligations, obtained their consent if necessary, and in particular has informed them of the possibility of Processor processing their PII on the Controller's behalf and in accordance with its instructions;

   (b) it has complied with all applicable data protection legislation in the collection and provision to Processor of such PII. Specifically, the Controller ensures that any disclosure PII to Processor is PII that has been collected lawfully, i.e. processed on a legal basis as described in the articles 6-10 of the GDPR;

   (c) the processing of such PII in accordance with the instructions of Controller is lawful.

6. **Confidentiality**. Processor shall ensure that its personnel engaged in the processing of PII are bound by a confidentiality undertaking.

7. **Data Breach**. Processor will promptly notify Controller after becoming aware of any actual breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, PII ("**Data Breach**").

8. **Records**. Processor will maintain up-to-date written records of its processing activities, including, *inter alia*, Processor's and Controller's contact details, details of data protection officers (where applicable), the categories of processing, transfers of PII across borders and the technical and organizational security measures implemented by the Processor. Upon request, Processor will provide an up-to-date copy of these records to Controller.

9. **Sub-Processors**. Controller acknowledges and agrees that Processor may engage any of the third-party sub-processors listed in **Annex 3**. Such sub-processors shall be bound by data protection obligations no less protective than those in this Agreement to the extent applicable to the nature of the Services provided by such sub-processor. Processor shall not subcontract any processing of the PII to any other third party subprocessor without the prior written consent of the Controller. Notwithstanding this, the Controller consents to the Processor engaging third party subprocessors to process the PII provided that: (i) The Processor provides at least 14 calendar days' prior notice of the addition or removal of any subprocessor (including details of the processing it performs or will perform), which may be given by Processor emailing the Controller or by the Processor posting details of such addition or removal on a webpage that has been set up for this purpose and which Processor has provided the Controller with emailed notice about; (ii) Processor agrees data protection terms with any subprocessor that are no less protective than those in this Agreement to the extent applicable to the nature of the Services provided by such subprocessor; and (iii) Processor remains fully liable for any breach of this Agreement that is caused by an act, error or omission of its subprocessor. If the Controller refuses to consent to the Processor's appointment of a third party subprocessor on reasonable written grounds relating to the protection of the PII and the parties cannot resolve any concerns through good faith discussion, then either the Processor will not appoint the subprocessor or the Controller may elect to suspend or terminate this Agreement and the Main Agreement in accordance with relevant provisions in the Main Agreement.

10. **Assistance**. Processor will assist Controller in ensuring compliance with Controller's obligations related to the security of the processing, notification and communication of Data Breaches, conduct of data protection impact assessments and any inquiry, investigation or other request by a supervisory authority . In the event that the Controller requests the Processor's assistance in relation to the PII processing for the Controller, such assistance services will be provided, subject to feasibility and acceptance by the Processor, at the rates of the Processor in force at that time.

11. **Possible Violation**. Where Processor believes that an instruction would result in a violation of any applicable data protection laws, Processor shall notify the Controller thereof.

12. **Information**. Processor will make available to Controller, upon request, information necessary to demonstrate compliance with the obligations set forth in this Agreement.

13. **Audits**. Upon Controller's request, Processor shall cooperate with audits and inspections of its compliance with the requirements and obligations herein and/or under applicable law. Such audits and inspections may be conducted by Controller or by any third party designated by Controller and may not exceed 2 audits per year. In consultation with Processor, Controller may engage a third party to perform its audit rights, provided that such third party is bound by an agreement of confidentiality with Processor. Processor shall be entitled to invoice the Controller on a time and material basis at the then-current applicable prices for any time expended for any such audit.

14. **Technical and Organizational Measures**.

    14.1 Processor shall implement and maintain all technical and organizational measures that are required for protection of the PII and ensure a level of security that is appropriate to for dealing with and protecting against any risks to the rights and freedoms of the data subjects, and as required in order to avoid accidental or unlawful destruction, loss, alteration or unauthorized disclosure of, or access to PII and/or as otherwise required pursuant to the GDPR, including, *inter alia*, the measures set forth in **Annex 2**. When complying with Section 14 hereof, Processor shall take into consideration the state of technological development existing at the time and the nature, scope, context and purposes of processing as well as the aforementioned risks.

    14.2. Processor shall regularly monitor its compliance with this Agreement and will provide Controller, upon request, with evidence that will enable verification of such monitoring activities. Processor shall promptly implement all changes to **Annex 2**, as requested by Controller. Processor shall ensure that all persons acting under its authority or on its behalf and having access to the PII, do not process the PII except as instructed by Controller and permitted herein.

15. **Transfer of PII to Third Countries**. Processor or any subprocessor will not transfer PII to a recipient located in a country that is not a Member State of the European Union or European Economic Area, unless that country is considered by the European Commission to have an adequate level of protection or pursuant to appropriate safeguards as set out by the GDPR, including the Standard Contractual Clauses of the European Commission.

16. **Return and Deletion of PII**. On the Controller's request, Processor shall return or destroy PII to the extent allowed by applicable law.

17. **Sensitive Data.** Controller is likely to process sensitive data as defined in article 9 of the GDPR. In this context, Controller and Processor undertake to comply with the measures specific to this category of data.

18. **Contact of the DPO-**

    DPO@itamar-medical.com

Annex I
Data Processing Description

This Annex I forms part of the Agreement and describes the processing that the processor will perform on behalf of the controller.

It should be noted that two separate types of products and services are described in this Annex. Namely: (1) On premises solutions (including "zzzPAT™ Software", "WatchPAT300" (this is both an on premises and cloud based solution) and "EndoPAT"); and (2) cloud based solutions (including "CloudPAT™ Software", "WatchPAT300" (this is both an on premises and cloud based solution), "WatchPAT ONE" and "SleePATh"). The details that apply will therefore depend on what type of product or service the Controller is using.

The practical data protection difference between the two types of products and services is that the on premises solutions involve the Controller undertaking all storage of PII itself, except for that required for technical support purposes, while the cloud based solutions involve the Processor (via its subprocessors, Amazon Web Services Inc. and Amazon Web Services EMEA SARL) undertaking all the storage of PII.

The processing details for these two types of products and services are otherwise the same except as specifically clarified in the table below.

Categories of data subjects whose personal data is transferred:	Patients, Health care professionals

Categories of personal data transferred:	Header Section:
	• Patient ID
	  • Prefix
	  • First name
	  • Last name
	  • Office
	  • Gender
	  • Date of birth
	  • Referring Physician
	  • Mobile Phone
	  • Email
	Personal Details:
	  • Height
	  • Weight
	  • BMI
	  • Neck circumference
	  • EPWORTH SCORE
	  • STOP-Bang score
	  • PACEMAKER
	
	Logistic Comments
	  • Edit field
	
	Contact Information
	  • Street
	  • City
	  • ZIP Code
	  • State
	  • Country
	  • Home phone
	  • Work phone
	  • Opt-out from communication
	
	Study Details
	  • Bracelet Study

- Request Script
- Number of Nights dropdown.
- Status

Insurance Information

- INSURANCE PROVIDER
- GROUP NUMBER
- OTHER

Additional Information

- Specialty
- Status
- Custom Field1 to Custom Field5 (if configured for the office)

<u>Compliance Data optional tab:</u>

The Daily Compliance Graph shall show both the usage (h) and AHI (#) graphs.
The compliance fields shall include the following:

• Is Active: Y / N
• Tx Manufacturer:
• Days since Tx started:
• Last update from CPAP:
• WatchPAT AHI:
• Treatment Date:

The compliance table shall display columns for the last 30 days, 90 days, and 180 days and rows of % of days with CPAP, % of days with CPAP > 4h, Average number of hours, PAP Reported AHI.

The compliance table shall show a red indicator if there were less than four hours per night of average use and a green indicator if more.

The CPAP Reported AHI row shall include the following indications:
an arrow when the value is higher than 10:

- Less than 10: Green indication
- More than 10 yet the reduction compared to the WP AHI > 50%: Yellow indication
- More than 10 however the reduction compared to the WP AHI < 50%: Orange indication

<u>Study Details</u>

This tab shall contain the interpreter report if one was created.

CP shall display the minimum desaturation that was used for AHI and RDI calculations, which can be 3% or 4%.

CP shall allow downloading the raw data files of the study.

CP shall allow downloading the PDF file and the secondary report if configured to this office (HTML or RTF)

CP shall show links to files attached by the interpreting physician.

Study Details screen shall include a dropdown called Min Desat for ODI with values of 3% or 4% but If the selected AHI is 4% the ODI must be 4% as well.

The questionnaire answers PDF file shall be appended to the report once the questionnaires are completed or questionnaires timeout has been reached with no need to wait for the save and lock operation.

	The report shall include a subset of the following elements, please see full details in Appendix A: Header, Self-Reported Patient Details, Bedtime Questionnaire, Morning Questionnaire, Main Sleep Complaints, Prior Sleep Diagnosis, Breathing table, CVD Markers, Insomnia, Daytime Sleepiness, Insomnia Severity Index (ISI), Epworth sleepiness scale (ESS), Narcolepsy, Movement, RLS, Sleep Schedule, Circadian, Lifestyle, Diseases, Medications, Appendix including ISI ESS and STOP BANG. <u>Sleep Report (Done through the WP Device Interface)</u> CP shall produce a generic sleep report as a PDF file and a secondary report if configured to this office (HTML or RTF). The report shall include the output of the WP Interface process. Report generated during analysis shall include data from study analysis and the most recent patient data available at the time of analysis.
Sensitive data 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:	**Sensitive data types** All categories of data listed above would likely be considered health data apart from: • First name • Last name • Gender • Date of birth • Mobile Phone • Email **Applied restrictions / safeguards** The applied restrictions / safeguards that apply to this sensitive data are the same as apply to the data generally and which can be found in Annex II beelow.
The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):	**On premises solutions:** As and when needed for technical support reasons.
	Cloud based solutions: Continuous.
Nature of the processing:	**On premises solutions:** Access, use for technical support reasons, minimal storage as necessary for technical support reasons and any use as may be required by law.
	Cloud based solutions: Storage, providing access, use for technical support reasons and any use as may be required by law.
Purpose(s) of the data transfer and further processing:	**On premises solutions:** Incidental use for technical support reasons. Any use as may be required by law.
	Cloud based solutions: Storage and providing so as to provide the services. Use for technical support reasons. Any use as may be required by law.
The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:	**On premises solutions:** As long as needed for technical support reasons or as may be required by applicable law.
	Cloud based solutions: On the Controller's request, and at the ending of the Main Agreement at the latest, Processor shall return or destroy PII to the extent allowed by applicable law.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:	As per above.

Annex II
Technical and Organisational
Security Measures

Description of the technical and organisational measures implemented by the processor(s) / data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

The column entitled "Itamar" in the table directly below reflects the security measures of the Processor and its affiliate subprocessor, Itamar Medical Limited. These entities (jointly also referred to as "Itamar" below) only process the PII for the purposes of providing technical support and as may be required by law.

The column entitled "AWS" directly below contains both the "custom" data security measures that the Processor's subprocessor, Itamar Medical Limited, has elected to use from its further subprocessors, Amazon Web Services Inc. and Amazon Web Services EMEA SARL (together "AWS"), along with "standard" AWS data security measures from the data processing agreement that Processor's subprocessor, Itamar Medical Limited, has with AWS and which can be found here - https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf. AWS processes the PII for the purposes of storage, providing access, providing technical support and as may be required by law.

Measures	Itamar	AWS
Measures of pseudonymisation and encryption of personal data	Controller can easily delete all PII from files that are sent to Processor for technical support reasons. SSL (secure ciphers over TLS 1.2) is used as encryption method for any data transfers.	**Custom measures:** Controller can easily delete all PII from files that are sent to Processor and its subprocessors. SSL (secure ciphers over TLS 1.2) is used as encryption method for any data transfers.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	**Confidentiality** Itamar will only access PII if the Controller has specifically requested and approved that Itamar undertake a technical support activity which involves the viewing of PII (e.g. through screen sharing functionality). Itamar does not store PII on its own systems except as may be required by applicable law. Only a minimal amount of Itamar staff, who are subject to contractual obligations of confidentiality and whose access is password protected, will be provided with access to the Controller's PII. **Integrity** Itamar will only change PII if instructed to by Controller. **Availability** Availability is not applicable to the processing undertaken directly by Itamar as it does not actively involve data storage except as may be required by applicable law.	**Confidentiality** **Custom measures:** All servers hosted with AWS have custom Firewall rules and additional security measures employed by Itamar Digital Health Team in place. **Standard measures:** Network Security. The AWS Network will be electronically accessible to employees, contractors and any other person as necessary to provide the Services. AWS will maintain access controls and policies to manage what access is allowed to the AWS Network from each network connection and user, including the use of firewalls or functionally equivalent technology and authentication controls. AWS will maintain corrective action and incident response plans to respond to potential security threats. **Integrity** **Custom measures:** All servers hosted with AWS have custom Firewall rules and additional security measures employed by Itamar Digital Health Team in place.

	Resiliance Resiliance is not applicable to the processing undertaken directly by Itamar as it does not actively involve data storage except as may be required by applicable law.	**Standard measures:** Network Security. The AWS Network will be electronically accessible to employees, contractors and any other person as necessary to provide the Services. AWS will maintain access controls and policies to manage what access is allowed to the AWS Network from each network connection and user, including the use of firewalls or functionally equivalent technology and authentication controls. AWS will maintain corrective action and incident response plans to respond to potential security threats. **Availability** **Custom measures:** A backup concept for databases, configuration, servers and files is in place. **Resiliance** **Custom measures:** A data security testing concept is in place that involves constant testing for any data security vulnerabilities. **Standard measures:** Continued Evaluation. AWS will conduct periodic reviews of the security of its AWS Network and adequacy of its information security program as measured against industry security standards and its policies and procedures. AWS will continually evaluate the security of its AWS Network and associated Services to determine whether additional or different security measures are required to respond to new security risks or findings generated by the periodic reviews.
Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident	Availability and access are not applicable as the processing undertaken directly by Itamar does not involve data storage except as may be required by applicable law.	**Custom measures:** A backup concept for databases, configuration, servers and files is in place.
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational	Itamar regularly runs internal testing to ensure that its data security measures are adequate.	**Custom measures:** A data security testing concept is in place that involves constant testing for any data security vulnerabilities. **Standard measures:** Continued Evaluation. AWS will conduct periodic reviews of the security of its AWS Network and adequacy

measures in order to ensure the security of the processing		of its information security program as measured against industry security standards and its policies and procedures. AWS will continually evaluate the security of its AWS Network and associated Services to determine whether additional or different security measures are required to respond to new security risks or findings generated by the periodic reviews.
Measures for user identification and authorisation	Itamar will only access PII if the Controller has specifically requested and approved that Itamar undertake a technical support activity which involves the viewing of PII (e.g. through screen sharing functionality). Only a minimal amount of Itamar staff, who are subject to contractual obligations of confidentiality and whose access is password protected, will be provided with access to the Controller's PII.	**Custom measures:** Access Control system in place across all Itamar Cloud systems incldluing authenticated access and password protection. **Standard measures:** Network Security. The AWS Network will be electronically accessible to employees, contractors and any other person as necessary to provide the Services. AWS will maintain access controls and policies to manage what access is allowed to the AWS Network from each network connection and user, including the use of firewalls or functionally equivalent technology and authentication controls. AWS will maintain corrective action and incident response plans to respond to potential security threats.
Measures for the protection of data during transmission	The encryption standard used for PII in transit is SSL (secure ciphers over TLS 1.2).	**Custom measures:** The encryption standard used for data in transit is SSL (secure ciphers over TLS 1.2).
Measures for the protection of data during storage	Itamar does not actively store PII on its own systems except as may be required by applicable law.	**Custom measures:** The encryption standard used for data at rest is - AES256.
Measures for ensuring physical security of locations at which personal data are processed	Itamar does not actively store PII on its own systems as part of providing the technical support services. Only a minimal amount of Itamar staff, who are subject to contractual obligations of confidentiality and whose access is password protected, will be provided with access to the Controller's PII.	**Standard measures:** Physical Access Controls. Physical components of the AWS Network are housed in nondescript facilities (the "Facilities"). Physical barrier controls are used to prevent unauthorised entrance to the Facilities both at the perimeter and at building access points. Passage through the physical barriers at the Facilities requires either electronic access control validation (e.g., card access systems, etc.) or validation by human security personnel (e.g., contract or in-house security guard service, receptionist, etc.). Employees and contractors are assigned photo-ID badges that must be worn while the employees and contractors are at any of the Facilities. Visitors are required to sign-in with designated personnel, must show appropriate identification, are

		assigned a visitor ID badge that must be worn while the visitor is at any of the Facilities, and are continually escorted by authorised employees or contractors while visiting the Facilities. Limited Employee and Contractor Access. AWS provides access to the Facilities to those employees and contractors who have a legitimate business need for such access privileges. When an employee or contractor no longer has a business need for the access privileges assigned to him/her, the access privileges are promptly revoked, even if the employee or contractor continues to be an employee of AWS or its Affiliates. Physical Security Protections: All access points (other than main entry doors) are maintained in a secured (locked) state. Access points to the Facilities are monitored by video surveillance cameras designed to record all individuals accessing the Facilities. AWS also maintains electronic intrusion detection systems designed to detect unauthorised access to the Facilities, including monitoring points of vulnerability (e.g., primary entry doors, emergency egress doors, roof hatches, dock bay doors, etc.) with door contacts, glass breakage devices, interior motion-detection, or other devices designed to detect individuals attempting to gain access to the Facilities. All physical access to the Facilities by employees and contractors is logged and routinely audited.
Measures for ensuring events logging	All events are logged and there is no way for the logs to be manipulated.	**Custom measures:** All events are logged and there is no way for the logs to be manipulated.
Measures for ensuring system configuration, including default configuration	Please refer to above and below.	**Custom measures:** All AWS systems are built and maintained by Itamar Medical's Digital Health Team in order to ensure an appropriate level of data security.
Measures for internal IT and IT security governance and management	Itamar has internal IT and IT security policies and / or procedures in place to ensure effective governance in this area. This includes relevant staff training.	**Standard measures**: Information Security Program. AWS will maintain an information security program (including the adoption and enforcement of internal policies and procedures) designed to (a) help Customer secure Customer Data against accidental or unlawful loss, access or disclosure, (b) identify reasonably foreseeable

		and internal risks to security and unauthorised access to the AWS Network, and (c) minimise security risks, including through risk assessment and regular testing. AWS will designate one or more employees to coordinate and be accountable for the information security program.
Measures for certification/assurance of processes and products	Itamar is in the process of becoming ISO 27001 certified.	**Standard measures:** AWS ISO-Certification and SOC Reports. In addition to the information contained in this DPA, upon Customer's request, and provided that the parties have an applicable NDA in place, AWS will make available the following documents and information: (i) the certificates issued in relation to the ISO 27001 certification, the ISO 27017 certification and the ISO 27018 certification (or the certifications or other documentation evidencing compliance with such alternative standards as are substantially equivalent to ISO 27001, ISO 27017 and ISO 27018); and (ii) the System and Organization Controls (SOC) 1 Report, the System and Organization Controls (SOC) 2 Report and the System and Organization Controls (SOC) 3 Report (or the reports or other documentation describing the controls AWS GDPR Data Processing Addendum 5 implemented by AWS that replace or are substantially equivalent to the SOC 1, SOC 2 and SOC 3). 10.2 AWS Audits. AWS uses external auditors to verify the adequacy of its security measures, including the security of the physical data centers from which AWS provides the Services. This audit: (a) will be performed at least annually; (b) will be performed according to ISO 27001 standards or such other alternative standards that are substantially equivalent to ISO 27001; (c) will be performed by independent third party security professionals at AWS's selection and expense; and (d) will result in the generation of an audit report ("Report"), which will be AWS's Confidential Information. 10.3 Audit Reports. At Customer's written request, and provided that the parties have an applicable NDA in place, AWS will provide Customer with a copy of the Report so that Customer can reasonably verify AWS's compliance with its obligations under this DPA.
Measures for ensuring data minimisation	Data minimisation is a Controller responsibility.	Data minimisation is a Controller responsibility.
Measures for ensuring data quality	Data quality is a Controller responsibility.	Data quality is a Controller responsibility.

Measures for ensuring limited data retention	Limited data retention is a Controller responsibility. Itamar also does not actively store PII on its own systems except as may be required by applicable law.	Limited data retention is a Controller responsibility.
Measures for ensuring accountability	Accountability is primarily a Controller responsibility. However, Itamar's accountability is also set out above.	Accountability is primarily a Controller responsibility. However, AWS's accountability is also set out above.
Measures for allowing data portability and ensuring erasure	Itamar does not actively store PII on its own systems except as may be required by applicable law.	**Standard measures**: At any time up to the Termination Date, and for 90 days following the Termination Date, subject to the terms and conditions of the Agreement, AWS will return or delete Customer Data when Customer uses the Service Controls to request such return or deletion. No later than the end of this 90-day period, Customer will close all AWS accounts containing Customer Data.

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller (and, for transfers from a processor to a sub-processor, to the data exporter).

Please refer to above.

Annex III

Subprocessors

The controller has authorised the use of the following sub-processors:

1.	Name:	Amazon Web Services EMEA SARL
	Address:	38 Avenue John F. Kennedy, L-1855, Luxembourg
	Contact person's name, position and contact details:	Data Protection Officer, aws-EU-privacy@amazon.com
	Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised):	Processing for the purposes of storage, providing access, providing technical support and as may be required by law