DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") is incorporated by reference into the agreement governing the use of the Services (the "**Agreement**") entered into by and between the ZOLL Contracting Entity specified in the Agreement ("**Processor**") and the entity identified as Customer in the Agreement ("**Controller**"), to reflect the parties' agreement with regard to the Processing of Personal Data by Processor solely on behalf of Controller. Both parties shall be referred to as the "**Parties**" and each, a "**Party**".

This DPA will apply solely in connection with the Services provided under the Agreement where the Processor Processes Personal Data originating in the European Union ("**EU**"), the European Economic Area and their member countries ("**EEA**"), the United Kingdom ("**UK**"), Israel, and Hong Kong. For the avoidance of doubt, this DPA will not apply where the applicable Services are provided from or through a distributor, reseller or other third-party intermediary or when the Processor processes personal data originating in any other areas in the world other than the EU, EEA, UK, Israel and Hong Kong.

1. Definitions

(a) "**Affiliate**" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "**Control**" means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

(b) "**Authorized Affiliate**" means any of Controller's Affiliate(s) which is explicitly permitted to use the Services pursuant to the Agreement but has not signed its own agreement with Processor.

(c) The terms "**Controller**", "**Data Subject**", "**Processor**", "**Processing**" and "**Supervisory Authority**" shall have the meanings given to them in the GDPR.

(d) "**Data Protection Laws**" means applicable privacy and data protection laws and regulations of the EU, EEA, UK, Israel, and Hong Kong that are binding on and applicable to Processor, and in effect at the time of Processor's performance hereunder, including the GDPR, UK GDPR and PPL, each as amended or superseded from time to time.

(e) "**GDPR**" means the 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).

(f) "**Personal Data**" means any information that meets the definition of "personal data" in Article 4 of the GDPR and is Processed by Processor solely on behalf of Controller under the Agreement and DPA.

(g) "**PPL**" means Israel's Protection of Privacy Law 5741-1981 and the regulations promulgated thereunder, each as amended or superseded from time to time.

(h) "**Restricted Transfer(s)** means a transfer of Personal Data originating from the EEA or the UK to a recipient in a country outside the relevant territory that is not subject to an adequacy determination by the European Commission or the UK Government (as applicable).

(i) "**Services**" means the ZOLL Itamar services provided to Controller by Processor under the Agreement.

(j) "**Security Documentation**" means the security documentation applicable to the Services purchased by Controller, as updated from time to time and made available to Controller by Processor, which shall at a minimum comply with applicable law and include the measures identified in **Schedule 2** to this DPA.

(k) "**Standard Contractual Clauses**" means: (i) where the GDPR applies, the standard contractual clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021 ("**EU SCCs**"); or (ii) where the UK GDPR applies, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses as issued by the Information Commissioner's Office under S119A(1) of the Data Protection Act 2018 and in force as of 21 March 2022 ("**UK Addendum**").

(l) "**Sub-processor**" means a Processor Affiliate or third-party entity engaged by Processor or its Affiliate to carry out Personal Data Processing activities on behalf of Controller under this DPA.

(m) "**UK GDPR**" means the GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018, together with the Data Protection Act 2018.

(n) "**ZOLL Contracting Entity**" means the member of the ZOLL Medical group identified as the supplier or service provider in the applicable Agreement.

2. Processing of Personal Data

2.1 **Roles of the Parties**. The Parties acknowledge and agree that with respect to the Processing of Personal Data under this DPA, Controller is the Controller of Personal Data and Processor is the Processor of such Personal Data.

2.2 **Controller's Duties**. Controller, in its use of the Services, and Controller's instructions to Processor, shall comply with Data Protection Laws. Controller shall establish all required legal bases to lawfully collect, Process and transfer to Processor the Personal Data, and to authorize the Processing by Processor, and for Processor's Processing activities on Controller's behalf.

2.3 **Processor's Duties**. Processor shall Process Personal Data only: (i) to provide, operate, support and improve the Services and perform its obligations in compliance with the Agreement and this DPA; (ii) to facilitate Controller's use of the Services; (iii) to comply with Controller's documented instructions that are consistent with the terms of the Agreement; (iv) to render Personal Data anonymous, de-identified or non-personal in accordance with Data Protection Laws; and (v) as required by applicable law, a competent court or other governmental authority, provided that Processor shall inform Controller of the legal requirement before Processing, unless such law or order prohibits such information on important grounds of public interest.

2.4 To the extent Processor cannot comply with an instruction from Controller because, for example, such instruction infringes applicable Data Protection Laws: (i) Processor shall inform Controller, providing relevant details of the issue; (ii) Processor may, without liability to Controller or to any third party, temporarily cease all Processing of the affected Personal Data (other than securely storing

such data) and/or suspend Controller's access to the Services (either directly or indirectly); and (iii) if the Parties do not agree on a resolution to the issue in question and the costs thereof, either Party may, as its sole remedy, terminate this DPA solely with respect to the affected Processing. Should such disagreement render it impossible to lawfully provide the Processing services to Controller, Processor and Controller shall each be entitled to terminate this DPA upon written notice. Processor shall not be liable for any suspension or termination pursuant to this Section.

2.5 **Details of the Processing**. The subject-matter of Processing of Personal Data by Processor is the performance of the Services pursuant to the Agreement and the purposes set forth in this DPA. The duration, nature and purpose of the Processing, and the types and categories of Personal Data and Data Subjects Processed under this DPA are further specified in **Schedule 1** to this DPA.

2.6 **PPL Terms**. If Processor Processes Personal Data hereunder that originates from Israel or is otherwise subject to the PPL, Processor shall comply with the PPL Schedule available at https://www.itamar-medical.com/wp-content/uploads/2026/09/Itamar-Medical-PPL-Terms-31.8.26-1.pdf, which is hereby incorporated by reference into this DPA with respect to such Personal Data and Processing.

3. Data Subject Requests

3.1 Considering the nature of the Processing, Processor shall assist Controller by implementing appropriate technical and organizational measures, insofar as this is possible and reasonable, for the fulfilment of Controller's obligations to respond to requests from Data Subjects for exercising applicable rights under Data Protection Laws ("**Data Subject Request(s)**").

3.2 If Processor receives a Data Subject Request directly from a Data Subject, Processor shall, to the extent legally permitted, promptly forward such request to Controller. Processor shall not respond to Data Subject Requests except by referring the Data Subjects directly to Controller, or as otherwise required by Data Protection Laws.

4. Confidentiality

4.1 Processor shall ensure that its personnel and advisors engaged in the Processing of Personal Data have committed themselves to appropriate confidentiality obligations, or are otherwise subject to a statutory duty of confidentiality.

5. Sub-Processors

5.1 **Appointment of Sub-processors**. Controller agrees that: (i) Processor's Affiliates may be engaged as Sub-processors; and (ii) Processor and Processor's Affiliates may each engage third-party Sub-processors in connection with the provision of the Services, subject to this Section 5.

5.2 **List of Current Sub-processors and Notification of New Sub-processors**. Processor makes available to Controller, in Schedule 1 to this DPA, the current list of Sub-processors engaged by Processor to Process Personal Data (the "**Sub-Processors List**"). The Sub-processors identified in the Sub-Processor List are hereby deemed authorized upon execution of this DPA. Processor shall notify Controller via email at the address indicated in the Agreement or as otherwise communicated to Processor at least fourteen (14) days before engaging a new Sub-processor and provide information necessary to enable Controller to exercise its right to object.

5.3 **Objection to New Sub-Processors**. Controller may reasonably object to Processor's intended use of a new Sub-processor, for reasons relating to the protection of Personal Data to be Processed by such Sub-processor, by notifying Processor promptly in writing via email to ItamarDPO@zoll.com within fourteen (14) days of Processor's notice of such new appointment. Such written objection shall include the reasons for objecting to Processor's use of the new Sub-processor. If Controller does not object to such new Sub-processor in writing within fourteen (14) days of notice issuance from Processor, that new Sub-processor shall be deemed accepted.

5.4 **Consequences of Objection**. If Controller reasonably objects to a new Sub-processor, Processor shall use reasonable efforts to provide an alternative. If no alternative is available within thirty (30) days, Controller may terminate the affected Services and this DPA with respect thereto. If Controller's objection prevents Processor from providing the Services, Processor may terminate the Agreement and this DPA without liability.

5.5 **Agreements with Sub-processors**. Processor or Processor's Affiliate has entered into a binding written agreement with each Sub-processor containing appropriate safeguards for the protection of Personal Data. Processor shall ensure that each Sub-processor is bound by written obligations providing a level of protection for Personal Data materially equivalent to those set out in this DPA. Processor remains responsible for its Sub-processors' performance of such obligations.

6. Security & Audits

6.1 **Controls for the Protection of Personal Data**. Processor shall maintain appropriate technical and organizational measures for the protection of Personal Data Processed (including measures consistent with the requirements of Article 32 of the GDPR and UK GDPR for protecting Personal Data against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss, alteration or damage, unauthorized disclosure of, or access to Personal Data, including those measures set forth in the Security Documentation in **Schedule 2**), as may be amended from time to time. Upon Controller's written request, Processor shall reasonably assist Controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR, taking into account the nature of the Processing and the information available to Processor.

6.2 **Audits and Inspections**. Upon Controller's thirty (30) days' prior written request, at reasonable intervals (no more than once every 12 months, except in the event of a Data Incident) and subject to strict confidentiality undertakings by Controller, Processor shall make available to Controller that is not a competitor of Processor or any of its Affiliates (or a third-party auditor, subject to confidentiality undertakings), information necessary to demonstrate compliance with this DPA. Processor shall allow for and contribute to audits, including inspections,

conducted by Controller, provided, however, that such information, audits, inspections and the results thereof, shall only be used by Controller to assess compliance with this DPA, and shall not be used for any other purpose or disclosed to any third party without Processor's prior written approval.

7. Data Incident Management and Notification

7.1 Processor maintains security incident management policies and procedures and shall notify Controller without undue delay after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data (a "**Data Incident**"). Processor shall provide Controller with information on the nature of the Data Incident (including, where possible, the categories and approximate number of Data Subjects and Personal Data records concerned), its likely consequences and the measures taken or proposed to address the Data Incident including, where appropriate, measures to mitigate its possible adverse effects. Processor shall take all steps reasonably necessary to remediate and mitigate the cause of such a Data Incident to the extent that remediation and mitigation are within Processor's reasonable control. Taking into account the nature of the Processing and the information available to Processor, Processor shall also provide Controller with all reasonably necessary cooperation and assistance in investigating, mitigating, and remediating a Data Incident, and enabling Controller to fulfil its obligations under Data Protection Laws.

7.2 Controller shall not publicly identify Processor in connection with a Data Incident without Processor's prior written approval, unless required by applicable law. Where permitted, Controller shall provide Processor with reasonable prior written notice of such disclosure.

8. Termination; Return & Deletion of Personal Data

8.1 **Termination**. Either Party may terminate this DPA upon written notice if the other Party materially breaches this DPA and fails to cure such breach within thirty (30) days following receipt of written notice thereof. Any termination of this DPA shall automatically terminate the Agreement and Controller's right to use the Services.

8.2 **Return or Deletion**. Following the earlier of the termination of the Agreement or the completion of Controller's use of the Services, Controller shall notify Processor in writing via email at ItamarDPO@zoll.com, whether Processor should delete or return Personal Data Processor Processes under this DPA. Upon receiving such instruction, Processor shall carry out Controller's decision to either return or delete all the Personal Data. Subsequently, Processor shall also delete any existing copies of such Personal Data unless and solely to the extent that Data Protection Laws to which Processor is subject require otherwise. Upon Controller's written request, Processor shall provide written certification to Controller confirming that Processor has fully complied with this Section.

9. Cross-Border Data Transfers

9.1 **Location of Processing**. The Parties agree that Processor may only transfer and Process Personal Data to and within the EEA, United Kingdom, and other locations in which Processor or its Sub-processors (including Processor's Affiliates) maintain data Processing operations, as described in the Sub-Processors List set out in **Schedule 1** hereto, and in any subsequent Sub-processor notification made to and authorized by Controller in accordance with Section 5 above. Processor shall ensure that such transfers are made in compliance with Data Protection Laws and this DPA.

9.2 **Transfer Mechanism**. To the extent Processing of Personal Data under this DPA involves a Restricted Transfer (either directly or via onward transfer) by Processor or its Sub-processors, any such transfer shall only be made subject to the Standard Contractual Clauses or an alternative recognized compliance mechanism for Restricted Transfers as set out in Article 46 of the GDPR. Transfers of Personal Data originating from any other jurisdiction which mandates a particular compliance mechanism for the lawful transfer of such data be established, Controller shall notify Processor of such applicable requirements, and the Parties may seek to make any necessary amendments to this DPA in accordance with the provisions of Section 11.2 below.

10. Authorized Affiliates

10.1 **Contractual Relationship**. The Parties acknowledge and agree that by executing this DPA, Controller enters into the DPA on behalf of itself and, as applicable, in the name and on behalf of its Authorized Affiliates, in which case each Authorized Affiliate agrees to be bound by Controller's obligations under this DPA, if and to the extent that Processor Processes Personal Data on behalf of such Authorized Affiliates, thus qualifying them as the "**Controller**". All access to and use of the Services by Authorized Affiliates must comply with the terms and conditions of the Agreement and this DPA, and any violation of the terms and conditions therein by an Authorized Affiliate shall be deemed a violation by Controller.

10.2 **Communication**. Controller shall remain responsible for coordinating all communication with Processor under the Agreement and this DPA, and shall be entitled to make and receive any communication in relation to this DPA on behalf of its Authorized Affiliates.

11. General

11.1 **Data Protection Impact Assessment and Prior Consultation**. Upon Controller's written request, Processor shall provide Controller, at Controller's expense, reasonable cooperation and assistance necessary to enable Controller to fulfil its obligations under Data Protection Laws to carry out a data protection impact assessment related to its use of the Services, and to undertake any related prior consultation with a Supervisory Authority.

11.2 **Modifications**. Either Party may request amendments to this DPA as necessary to comply with changes in Data Protection Laws. If the Parties are unable to agree on the required amendments within thirty (30) days, then each Party may terminate the affected Services and this DPA upon written notice.

11.3 **Order of Precedence.** In the event of any conflict between this DPA and the Agreement, the provisions of this DPA shall prevail solely with respect to the Processing of Personal Data.

Schedule 1
Details of the Processing

1. **General**
   - Processor offers two types of Services: (i) an on-premises solution ("**zzzPAT**"); and (ii) a cloud-based solution ("**CloudPAT**").
   - The details of the Processing activities depend on the type of solution used by Controller.
   - In the case of zzzPAT, Controller is responsible for the storage of all Personal Data, except for limited processing carried out by Processor solely for the purpose of providing technical support.
   - In the case of CloudPAT, Processor (including its authorized Sub-processors, as identified below) is responsible for the storage of Personal Data on behalf of Controller.
   - Except as expressly stated above, the Processing activities for both solutions are otherwise substantially the same.

2. **Nature of Processing**
   - zzzPAT: Ad-hoc access to, use, and minimal storage of Personal Data as necessary for and instructed by Controller, and technical support reasons.
   - CloudPAT: Storage of and facilitating access to Personal Data for Controller's authorized Personnel (as defined below), as well as ad-hoc access to and use of Personal Data as necessary for and instructed by Controller and technical support reasons.

3. **Purposes of Processing**
   - Providing Services to Controller and/or the Authorized Affiliate;
   - Complying with the Agreement, this DPA and/or other contracts executed by the Parties;
   - Acting upon Controller's reasonable and documented instructions, where such instructions are consistent with the terms of the Agreement and this DPA;
   - Complying with applicable laws and regulations;
   - All tasks related to any of the above.

4. **Duration and Frequency of Processing**
   - zzzPAT: Processor shall Process Personal Data pursuant to this DPA on an ad-hoc basis, limited to the duration of handling specific Controller and technical support requests.
   - CloudPAT: Subject to the provisions of the DPA, Processor shall Process Personal Data pursuant to this DPA on a continuous basis until the earliest of (i) the termination/expiration of the Agreement; or (ii) the date upon which it is no longer necessary for the performance of Processor's obligations under this DPA.

5. **Categories of Data Subjects**
   - Patients of Controller and/or the Authorized Affiliate ("**Patients**").
   - Healthcare professionals and other personnel employed/engaged by Controller and/or the Authorized Affiliate; (collectively, "**Personnel**").

6. **Types of Personal Data**
   - **In relation to Patients**:
     - Patient profile data (e.g., name, gender, date of birth, associated clinic, referring and interpreting physician)
     - Contact details (e.g., home address, email address, phone number)
     - Medical data (sleep metrics collected through the Services such as Peripheral Arterial Tone signal, heart rate, oximetry, body position, snoring, and chest motions); responses to a patient screening questionnaire (e.g., medical history, medications, current or past treatment for high blood pressure); and diagnostics inferences drawn from such data.
   - **In relation to Personnel**:
     - Personnel professional data (e.g., name, job title, medical specialty, associated clinic and Patients); and
     - Contact details (e.g., work email address and phone number).

7. **Special Categories of Personal Data**
   - In providing the Services, Processor shall Process Special Categories of Personal Data (data concerning health) as outlined above, relating to Patients.

8. **Sub-processors List**
   - **Processor** may use Processor's Affiliates and third-party Sub-processors listed below to deliver the Services:

Entity Name	Type of Service	Processing Location	Corporate Address	Transfer Mechanism	Contact Details
Third-Party Sub-processors					
Amazon Web Services EMEA SARL	Cloud computing / storage	Germany (primary data center); Ireland (redundancy data center)	38 Avenue John F. Kennedy, 1855 Luxembourg	Adequacy Decision (UK); N/A (EU)	aws-EU-privacy@amazon.com
SFDC Ireland Limited (Salesforce)	CRM provider used for logistics and patient reminders for WatchPAT Direct, as well as service-wide customer support management	UK	Salesforce Tower, 60 R801, North Dock, Dublin D01 K8R1, Ireland	Adequacy Decision (EU); N/A (UK)	privacy@salesforce.com
One Software Technologies Ltd.	DevOps and cloud infrastructure maintenance	Israel	17 Yegi'a Kapayim, Petach Tikva, Israel	Adequacy Decision	https://one1.global/contact/
Affiliates engaged as Sub-processors					
ZOLL Medical UK Limited	Technical support; for WPD: operations, shipments, patient guidance and customer support	UK	9 Seymour Court, Tudor Road, Runcorn, Cheshire WA7 1SY, England	Adequacy Decision (EU)	ItamarDPO@zoll.com
Itamar Medical Ltd.	Customer and technical support	Israel	9 Halamish, Caesarea, Israel	Adequacy Decision	ItamarDPO@zoll.com

Schedule 2

Technical and Organizational Security Measures

The following information outlines the technical and organizational security measures implemented by Processor to ensure an appropriate level of security in the processing of Personal Data, as required by Article 28 of the GDPR and other Data Protection Laws.

Type of Security Measures	Description
Pseudonymization and Encryption	Processor maintains Personal Data encrypted at rest (AES-256) and in transit (TLS 1.2 / SFTP).
Confidentiality of Processing Systems and Services	Only a minimal number of Processor's staff, who are subject to contractual confidentiality undertakings and whose access is password-protected, are provided with access to Personal Data, on a need-to-know basis. All servers hosted with Processor's Sub-processor, AWS, have custom Firewall rules (WAF), and additional security measures employed by Processor are in place.
Integrity of Processing Systems and Services	Processor shall only amend Personal Data if and as instructed by Controller in writing. Processor has procedures in place to maintain the integrity of the Processed Personal Data.
Availability of Processing Systems and Services	A backup concept for databases, configuration, servers and files is in place, provided by AWS and maintained, monitored and controlled by Processor.
Resilience of Processing Systems and Services	A data security testing concept is in place that involves constant testing for any data security vulnerabilities, provided by AWS and maintained, monitored and controlled by Processor.
Restoration of Availability and Access	A backup concept for databases, configuration, servers and files is in place, provided by AWS and maintained, monitored and controlled by Processor.
Testing and Evaluation	Processor regularly runs internal testing to ensure that its technical and organizational security measures and policies are adequate and effective, adapting measures as necessary for an evolving security landscape.
User Identification and Authorization	Processor enforces password and multi-factor authentication requirements. Additionally, Processor requires personnel to use Processor-issued endpoint devices for accessing any Controller Personal Data. Processor operates under the principle of least privilege which ensures that only those with a business need to access a system or data are authorized and utilizes role-based access controls (RBAC) to provision and control access. Access rights are promptly removed with personnel termination.
Data Encryption In-transit	The encryption standard used for Personal Data in transit is SSL (secure ciphers over TLS 1.2 / SFTP).
Data Encryption At-rest	The encryption standard used for Personal Data at rest is AES-256, provided by AWS.
Physical Security	The Services' infrastructure is hosted with an outsourced cloud provider (AWS). Production servers and client-facing applications are physically secured from Processor's internal corporate information systems. Processor's physical security controls are regularly audited for ISO 27001 and SOC 2 compliance.
Event Logging	All administrative events are logged (including successful logins, failed logins, data views, data modifications, and data deletions). There are alerts triggered to Processor's SOC when elevated privileges are used.
System Configuration, including Default Configuration	All AWS systems hosting the Services are configured and maintained by Processor in a manner ensuring an appropriate level of data security.
Internal IT and IT security governance	Processor has information security policies and procedures in place to ensure effective governance in this area, which are communicated to relevant employees upon recruitment and at least annually. This includes conducting relevant staff information security training at least annually.
Certification/Assurance of Processes and Products	Processes and products undergo certification/assurance to ensure compliance with security standards. As of the date of this DPA, Processor is ISO 27001 and SOC 2 certified.
Data Minimization	The Services were designed with data minimization principles front and center, restricting the collection of Personal Data to only those necessary for the provision of the Services in accordance with Controller's documented instructions.
Data quality	Controller is solely responsible for the quality of the Personal Data submitted to the Services. Processor has procedures in place to maintain the integrity of such Personal Data.
Limited Data Retention	zzzPAT: Processor shall Process the Personal Data on an ad-hoc basis and shall only retain it for as long as necessary for the handling of specific support and technical requests relating to the use of the Services, or as may be required by applicable law. CloudPAT: Processor shall Process the Personal Data on a continuous basis until the earliest of (i) the termination/expiration of the Agreement, or (ii) the date upon which it is no longer necessary for the performance of Processor's obligations under this DPA. At Controller's written instruction following termination of the Agreement at the latest, Processor will return or destroy (at Controller's choice) all Personal Data unless otherwise required by applicable law.
Accountability	Processor employs multiple controls to ensure high visibility and enforcement of change management policies to ensure accountability.
Allowing Data Portability and Ensuring Erasure	Personal Data can be exported to CSV format upon Controller's request, and if so instructed by Controller, Processor also supports FHIR API capabilities for system-to-system data exchange. Processor deletes the Personal Data at Controller's instruction in accordance with the DPA.