ITAMAR MEDICAL LTD. DATA PROCESSING ADDENDUM
FOR END USERS OF PRODUCTS PURCHASED FROM AUTHORIZED DISTRIBUTORS

This Data Processing Agreement (the "**DPA**") is executed by and between the end user using the Services (as defined herein) ("**Controller**", "**you**" or "**your**") and Itamar™ Medical Ltd. ("**Processor**"), on behalf of itself and its Affiliates, to reflect the parties' agreement with regard to the Processing of Personal Data by the Processor solely on behalf of the Controller in the course of the Controller's use of the Services pursuant to the agreement, service order, purchase order or similar (the "**Agreement**") executed by and between the Controller and the Processor's authorized distributor ("**Authorized Distributor**"). Both parties shall be referred to as the "**Parties**" and each, a "**Party**". Capitalized terms not defined herein shall have the meanings assigned to such terms in the Agreement.

By using the Services, the Controller accept this DPA and represents and warrants that it has full authority to be bound by its terms.

In the event of any conflict between this DPA and the Agreement, the provisions of this DPA shall prevail over the conflicting provisions of the Agreement solely with respect to the Processing of Personal Data.

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", for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

(b) The terms, "**Controller**", "**Member State**", "**Processor**", "**Processing**" and "**Supervisory Authority**" shall have the same meaning as in the GDPR.

(c) "**Data Protection Laws**" means all binding privacy and data protection laws and regulations known or reasonably expected by the Processor to be applicable to the Processing of Personal Data and in effect at the time of the Processor's performance hereunder, including but not limited to such laws and regulations of the European Union ("**EU**"), the European Economic Area ("**EEA**"), and their member countries, Switzerland, Australia, New Zealand, Brazil, Mexico, Bermuda, the Republic of El Salvador, and Singapore, including (without limitation) the GDPR and the FADP, each as amended or superseded from time to time.

(d) "**Data Subject**" means the identified or identifiable person to whom the Personal Data relates.

(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) "**FADP**" means the Swiss Federal Act on Data Protection of 25 September 2020.

(g) "**Personal Data**" means any information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, to or with an identified or identifiable natural person, and that is Processed by the Processor solely on behalf of the Controller in the course of the Controller's use of the Services pursuant to the Agreement.

(h) "**Restricted Transfer(s)**" means: (a) where the GDPR applies, a transfer of Personal Data originating from the EEA to a recipient in any country outside of the EEA that is not subject to an adequacy determination by the European Commission; or (b) where the FADP applies, a transfer of Personal Data originating from Switzerland to a recipient in any other country that is not recognized by the Swiss Federal Council as providing an adequate level of data protection.

(i) "**Services**" means the Processor's proprietary mobile applications, cloud-based platforms, and/or on-premises test management software (as applicable) and any other software and services which may be used together with the Processor's medical devices, provided by the Processor to the Controller pursuant to the Agreement.

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

(k) "**Special Categories of Personal Data**" means Personal Data deemed sensitive and requiring specific protections under Data Protection Laws, including, but not limited to, Personal Data revealing racial or ethnic

origin, political opinions, religious or philosophic beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning sex life or sexual orientation, as defined under Article 9 of the GDPR and equivalent provisions under other applicable Data Protection Laws.

(l) "**Standard Contractual Clauses**" means: (a) 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 (b) where the FADP applies, the EU SCCs as amended in accordance with guidance from the Swiss Federal Data Protection and Information Commissioner.

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

2. PROCESSING OF PERSONAL DATA

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

2.2 **Processor's Processing of Personal Data**. When Processing on the Controller's behalf under this DPA, the Processor shall Process Personal Data solely for the following purposes: (i) Processing in accordance with this DPA; (ii) Processing for the Controller as part of the facilitation of its use of the Services; (iii) Processing to comply with the Controller's reasonable and documented instructions, where such instructions are consistent with the provisions of this DPA regarding the manner in which the Processing shall be performed; (iv) Processing to render Personal Data fully anonymous, non-identifiable and non-personal in accordance with applicable standards recognized by Data Protection Laws and guidance issued thereunder; and (v) Processing as required under the laws applicable to the Processor, and/or as required by a court of competent jurisdiction or other competent governmental or semi-governmental authority, provided that the Processor shall inform the Controller of the legal requirement before Processing, unless such law or order prohibit such information on important grounds of public interest.

To the extent that the Processor cannot comply with an instruction from the Controller because, for example, in the Processor's opinion, such instruction infringes applicable Data Protection Laws: (i) the Processor shall inform the Controller, providing relevant details of the issue; (ii) the Processor may, without liability to the Controller or to any third party, temporarily cease all Processing of the affected Personal Data (other than securely storing such data) and/or suspend the 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 any and all Processing services to the Controller, the Processor and the Controller shall each be entitled to terminate this DPA with immediate effect. Upon termination as set forth in this paragraph, the Controller shall have no further claims against the Processor or any third party, nor shall the Processor incur any liability in connection therewith.

2.3 **Details of the Processing**. The subject-matter of Processing of Personal Data by Processor is the facilitation of the Controller's use of the Services pursuant to the Agreement and the purposes set forth in this DPA. The duration of the Processing, the nature and purpose of the Processing, the categories of Data Subject and the types of Personal Data Processed under this DPA are further specified in **Schedule 1** (Details of Processing) to this DPA.

3. DATA SUBJECT REQUESTS

The Processor shall provide reasonable assistance to the Controller in fulfilling the Controller's obligation to respond to requests for exercising the Data Subject's rights under Data Protection Laws (to the extent available under such laws), such as the right of access, rectification, restriction of Processing, erasure, data portability, objection to the Processing, or not to be subject to automated individual decision-making ("**Data Subject Requests**"). Considering the nature of Processing, such assistance shall include the implementation of appropriate technical and organizational measures, insofar as this is possible and reasonable. If the Processor receives a Data Subject Request directly from a Data Subject, the Processor shall, to the extent legally permitted, promptly forward such request to the Controller once the Processor has identified that the request

is from a Data Subject for whom the Controller is responsible. The Processor shall not respond to Data Subject Requests except by referring the Data Subjects directly to the Controller, unless: (i) applicable law to which the Processor is subject requires otherwise; or (ii) the Processor has received explicit instructions from the Controller to respond directly to the Data Subject in a specified manner.

4. CONFIDENTIALITY

The Processor shall grant access to the Personal Data to members of its personnel and individual service providers only to the extent necessary for the provision of the Services and shall ensure that such personnel and individual service providers have committed themselves to confidentiality.

5. SUB-PROCESSORS

5.1 **Appointment of Sub-processors**. The Controller acknowledges and agrees that: (a) the Processor's Affiliates may be engaged as Sub-processors; and (b) the Processor and the Processor's Affiliates on behalf of the Processor may each engage third-party Sub-processors in connection with the provision of the Services, all subject to this Section **Error! Reference source not found.**.

5.2 **List of Current Sub-processors, Notification of and Objection to New Sub-processors**. The Processor makes available to the Controller the current list of Sub-processors used by the Processor to Process Personal Data at **Schedule 1** to this DPA. Such Sub-processor list includes the identities of those Sub-processors, the type of service rendered by each Sub-processor, the location of the Processing performed by each of them and (where applicable) the transfer mechanism used ("**Sub-Processors List**"). The Sub-Processor List as of the date of first use of the Services by the Controller is hereby deemed authorized upon first use of the Services. The Controller shall subscribe to notifications of Sub-processor changes by sending an email to ItamarDPO@zoll.com with the subject 'SUBSCRIPTION TO SUB-PROCESSOR NOTIFICATION', or through any other subscription mechanism provided by the Processor and communicated to the Controller. When the Controller so subscribes, the Processor shall notify the Controller at least fourteen (14) days before engaging a new Sub-processor, providing the information necessary to enable the Controller to exercise its right to object.

5.3 **Objection to New Sub-processors**. To object to a new Sub-processor within the notice period, the Controller can: (i) discontinue use of the relevant Services affected by the new Sub-processor; or (ii) terminate the Agreement pursuant to its terms and this DPA solely with respect to the affected Services. The Controller will have no further claims against the Processor or any other third party due to the termination of the Agreement and/or the DPA in the situation described in this paragraph.

5.4 **Agreements with Sub-processors**. The Processor or a Processor's Affiliate on behalf of the Processor has entered into a binding written agreement with each Sub-processor containing appropriate safeguards for the protection of Personal Data. Where the Processor engages a Sub-processor for carrying out specific Processing activities on behalf of the Controller, the same or materially similar data protection obligations as set out in this DPA shall be imposed on such new Sub-processor by way of a binding written contract, in particular obligations to implement appropriate technical and organizational measures so that the Processing will meet the requirements of Data Protection Laws. Where a Sub-processor fails to fulfil its data protection obligations concerning its Processing of Personal Data, the Processor shall fully liable for any acts or omissions of the Sub-processor that result in a breach of Processor's obligations under this DPA.

6. SECURITY & AUDITS

6.1 **Controls for the Protection of Personal Data**. The Processor shall maintain industry-standard technical and organizational measures for the protection of Personal Data Processed (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Personal Data, confidentiality and integrity of Personal Data, including those measures set forth in the Security Documentation in **Schedule 2** hereto), as may be amended from time to time. Upon the Controller's reasonable request, the Processor shall reasonably assist the Controller, at the Controller's cost and subject to the provisions of Section 10.1 below, 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 the Processor.

6.2 **Audits and Inspections**. Upon the 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 as defined in Section 7.17 below) and subject to strict confidentiality undertakings by the Controller, the Processor shall make available to the

Controller that is not a competitor of Processor or any of its Affiliates (or the Controller's independent, reputable, third-party auditor that is not a competitor of the Processor or any of its Affiliates and not in conflict with the Processor of any of its Affiliates, subject to their confidentiality and non-compete undertakings) information necessary to demonstrate compliance with this DPA, and allow for and contribute to audits, including inspections, conducted by them (provided, however, that such information, audits, inspections and the results thereof, including the documents reflecting the outcome of the audit and/or the inspection, shall only be used by the 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. Upon the Processor's first request, the Controller shall return all records or documentation in the Controller's possession or control provided by the Processor in the context of the audit and/or inspection, including all copies thereof to the extent permitted by Data Protection Laws).

6.3 In the event of an audit or inspection as set forth above, the Controller shall ensure that it (and each of its mandated auditors) will not cause (or, if it cannot avoid, minimize) any damage, injury or disruption to the Processor's premises, equipment, personnel and business while conducting such audit or inspection.

7. DATA INCIDENT MANAGEMENT AND NOTIFICATION

7.1 The Processor maintains security incident management policies and procedures and shall notify the 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**"). The Processor shall provide the 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. Where, and insofar as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay. The Processor shall take reasonably necessary steps to remediate and mitigate the cause of such a Data Incident to the extent that remediation and mitigation are within the Processor's reasonable control. The Processor shall also provide the Controller with all reasonably necessary cooperation and assistance in: (i) investigating, mitigating, and remediating a Data Incident; and (ii) enabling the Controller to fulfil its obligations under Data Protection Laws, including notifying the competent regulatory or Supervisory Authority and affected Data Subjects, taking into account the nature of the Processing and the information available to the Processor.

7.2 The Controller will not make, disclose, release or publish any finding, admission of liability, communication, notice, press release or report concerning any Data Incident which directly or indirectly identifies the Processor (including in any legal proceeding or in any notification to regulatory or Supervisory Authorities or affected individuals, excluding disclosure to third-party consultants and advisors of the Controller that are subject to appropriate confidentiality undertakings) without the Processor's prior written approval, unless, and solely to the extent that, the Controller is compelled to do so in order to notify any competent data protection authority of a Data Incident in a mandatory manner prescribed by such authority, or pursuant to Data Protection Laws. In the latter case, unless prohibited by such laws, the Controller shall provide the Processor with reasonable prior written notice to provide the Processor with the opportunity to object to such disclosure, and in any case, the Controller will limit the disclosure to the minimum scope required.

8. RETURN AND DELETION OF PERSONAL DATA

Following the earlier of the termination of the Agreement or the completion of the Controller's use of the Services, the Controller shall notify the Processor in writing via email at ItamarDPO@zoll.com, whether to delete or return all Personal Data the Processor Processes under this DPA. Upon receiving such instructions, the Processor shall, without undue delay, carry out the Controller's decision to either return or delete all the Personal Data. Subsequently, the Processor shall also delete any existing copies of such Personal Data unless and solely to the extent that Data Protection Laws to which the Processor is subject require otherwise. In the latter case, the Processor warrants that it will only Process such retained Personal Data to the extent and for as long as required under such laws. Until the Personal Data is fully deleted, the Processor shall continue to ensure compliance with this DPA. Upon the Controller's written request, the Processor shall provide written certification to the Controller confirming that the Processor has fully complied with this Section.

9. CROSS-BORDER DATA TRANSFERS

9.1 **Location of Processing.** The Controller acknowledges that the Processor is located in Israel, a country that has been recognized by the European Commission and the Swiss Federal Data Protection and Information Commissioner as providing an adequate level of data protection and, therefore, transfers of Personal Data originating from the EEA or Switzerland to the Processor do not constitute Restricted Transfers. The Parties agree that the Processor may only transfer and Process Personal Data to and in the EEA, United Kingdom, and other locations in which the Processor or its Sub-processors (including the Processor's Affiliates) maintain data Processing operations, as more particularly described in the Sub-Processors List set out in **Schedule 1** hereto, and in any subsequent Sub-processor notification made to and authorized by the Controller in accordance with Section **Error! Reference source not found.**5.2 above. The Processor shall ensure that such transfers are made in compliance with Data Protection Laws (particularly, Chapter V of the GDPR and Section 3 under Chapter 2 of the FADP) and this DPA.

9.2 **Transfer Mechanism.** To the extent the Processing of Personal Data under this DPA involves a Restricted Transfer (either directly or via onward transfer) by the Processor or its Sub-processors (including the Processor's Affiliates), 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 or Article 16 of the FADP, as applicable.

10. OTHER PROVISIONS

10.1 **Data Protection Impact Assessment and Prior Consultation**. Upon the Controller's reasonable request, the Processor shall provide the Controller, at the Controller's cost, with reasonable cooperation and assistance needed to fulfil the Controller's obligation under Data Protection Laws to carry out a data protection impact assessment related to Controller's use of the Services, to the extent the Controller does not otherwise have access to the relevant information, and to the extent such information is available to the Processor. The Processor shall provide, at the Controller's cost, reasonable assistance to the Controller in the cooperation or prior consultation with the Supervisory Authority in the performance of its tasks relating to this Section 10.1, to the extent required under the GDPR or the FADP.

10.2 **Modifications**. Each Party may, by at least thirty (30) calendar days' prior written notice to the other Party, request any variations to this DPA if they are required as a result of any change in, or decision of a competent authority under, any Data Protection Laws, to allow Processing of Personal Data to be made (or continue to be made) without breach of those Data Protection Laws. Pursuant to such notice: (a) The Parties shall make commercially reasonable efforts to accommodate such modification requested by the Controller or that the Processor believes is necessary; and (b) the Controller shall not unreasonably withhold or delay agreement to any consequential variations to this DPA proposed by the Processor to protect the Processor against additional risks, or to indemnify and compensate the Processor for any further steps and costs associated with the variations made herein at the Controller's request. The Parties shall promptly discuss the proposed variations and negotiate in good faith with a view to agreeing and implementing those or alternative variations designed to address the requirements identified in the Controller's or the Processor's notice as soon as is reasonably practicable. In the event that the Parties are unable to reach such an agreement within 30 days of such notice, then each Party may, by written notice to the other Party, with immediate effect, terminate this DPA to the extent that it relates to the Services which are affected by the proposed variations (or lack thereof). The Controller will have no further claims against the Processor pursuant to the termination of the DPA as described in this Section.

SCHEDULE 1 – DETAILS OF THE PROCESSING

The Processor offers two separate types of Services, set out in this schedule: (1) **on-premises solutions** (including zzzPAT™ Software, WatchPAT300 (when operated through zzzPAT), and EndoPAT); and (2) **cloud-based solutions** (including CloudPAT™ Software, WatchPAT300 (when operated through CloudPAT), WatchPAT ONE, and WatchPAT400). The details of Processing will depend on the type of product or service the Controller is using.

The on-premises solutions involve the Controller undertaking all storage of Personal Data itself, except for that required for technical support purposes, while the cloud-based solutions involve the Processor (via its Sub-processors, as listed below) undertaking all storage of Personal Data. The Processing details for these two types of products and services are otherwise the same except as clarified below.

Nature of Processing

- On-premises solutions: Ad-hoc access to, use, and minimal storage of Personal Data as necessary for and instructed by the Controller for customer and technical support reasons.
- Cloud-based solutions: Storage of and facilitating access to Personal Data for the 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 the Controller for customer and technical support reasons.

Purposes of Processing

1. Facilitating the usage of the Services by the Controller;
2. Performing this DPA;
3. Acting upon the Controller's reasonable and documented instructions, where such instructions are consistent with the terms of this DPA;
4. Complying with applicable laws and regulations;
5. All tasks related to any of the above.

Duration and Frequency of Processing

- On-premises solutions: The Processor will Process Personal Data pursuant to this DPA on an ad-hoc basis, limited to the duration of handling specific customer and technical support requests.
- Cloud-based solutions: Subject to any section of the DPA dealing with the duration of the Processing and the consequences of the expiration or termination thereof, the Processor will Process Personal Data pursuant to this DPA on a continuous basis until the earliest of (i) the termination of this DPA, or (ii) the date upon which it is no longer necessary for the performance of the Processor's obligations under this DPA.

Categories of Data Subjects

1. Patients of the Controller ("**Patients**");
2. Healthcare professionals and other personnel (e.g., administrative staff) employed/engaged by the Controller (collectively – "**Personnel**").

Types of Personal Data

1. 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.

2. In relation to Personnel:
    - Personnel professional data (e.g., name, job title, medical specialty, and associated Controller, clinic and Patients);
    - Contact details (e.g., work email address and phone number).

Special Categories of Personal Data

In providing the Services, the Processor will process Special Categories of Personal Data (data concerning health) as outlined above, relating to Patients.

Sub-processors List

The Processor may engage its Affiliates and third-party entities listed below as Sub-processors to provide the Services:

Sub-processor	Type of service	Processing location	Transfer mechanism
Third-party Sub-processor(s)			
Amazon Web Services EMEA	Cloud computing / storage services	Germany	EU Member State
Affiliate(s) engaged as Sub-processor(s)			
ZOLL Medical (UK) Limited	Technical support services	United Kingdom	Adequacy decision

SCHEDULE 2 – TECHINCAL AND ORGANIZATIONAL SECURITY MEASURES

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

Security Measures Type	Description
Pseudonymization and Encryption	The 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 the 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 the Processor's Sub-processor, AWS, have custom Firewall rules (WAF), and additional security measures employed by the Processor are in place.
Integrity of Processing Systems and Services	The Processor will only amend Personal Data if and as instructed by the Controller in writing. The Processor has procedures in place to maintain the integrity of the Processed Personal Data.
Ongoing 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 the 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 the 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 the Processor.
Testing and Evaluation	The 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	The Processor enforces password and multi-factor authentication requirements. Additionally, the Processor requires personnel to use Processor -issued endpoint devices for accessing any Controller Personal Data. The 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 the Processor's internal corporate information systems. The 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 the Processor's SOC when elevated privileges are used.
System Configuration, including Default Configuration	All AWS systems hosting the Services are configured and maintained by the Processor in a manner ensuring an appropriate level of data security.
Internal IT and IT security governance	The 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, the 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 the Controller's documented instructions.
Data quality	The Controller is solely responsible for the quality of the Personal Data submitted to the Services. The Processor has procedures in place to maintain the integrity of such Personal Data.
Limited Data Retention	On-premises solutions: The Processor will Process the Personal Data on an ad-hoc basis and will 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. Cloud-based solutions: The Processor will 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 the Processor's obligations under this DPA. At the Controller's written instruction following termination of the Agreement at the latest, the Processor will return or destroy (at the Controller's choice) all Personal Data unless otherwise required by applicable law.
Accountability	The 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 the Controller's request, and if so instructed by the Controller, the Processor also supports FHIR API capabilities for system-to-system data exchange. The Processor deletes the Personal Data at the Controller's instruction in accordance with the DPA.