Document no.: 00702 **Effective Date:** 2020-07-27 **Version:** 1

Sales Terms - Cortrium Holter Monitor

Cortrium is the manufacturer of an ECG recorder (Holter Monitor) that monitors heart rhythms. The recordings are subject to cloud-based AI analytics or desktop-based analytics. A list of Cortrium products can be accessed via the Cortrium website.

The Sales Terms and conditions shall apply to all contracts that you as Customer has concluded with us (Cortrium ApS German Branch) via the Cortrium web-shop, unless otherwise agreed upon in writing.

The Sales Terms covers Cortrium Holter Monitor including the Software Analytics and is part of the overall contractual relationship between Cortrium and you as the Customer. The Sales Terms, including the referred appendices available on the Cortrium website, must be read and understood before accepting to purchase any Cortrium offerings.

1. Introduction

(1) The legal identity the manufacturer of the Holter Monitor: Cortrium ApS, German Branch, Leipziger Platz 15, 10117 Berlin, Deutschland, HRB 190340 B, Ust-IdNr: DE314 334 444, St.-Nr.: 15/248/10320.

(2). Cortrium is offering the following Products:

	Purchase	**Subscription**
Cortrium Holter Monitor	Price per unit	Monthly Flat-Fee
Cloud-based AI Software Analytics	Price per ECG recording analyzed	Monthly Flat-Fee
Desktop-based Software analytics	Price per license	n/a

The key features of the Products offered can be found on the Cortrium webpage. Cortrium reserves the right to bundle the price offer for both Products and the Software Analytics.

(3) The Customer is not permitted to move the Product to any other business entity without the written approval of Cortrium. Nor is any sub-letting or other transfer of possession to a third party permitted.

(4) Deviations of these Sales Terms shall be applicable only upon a written expressed consent issued by Cortrium.

2. Sales and Payments

(1) Sales via Web-shop of Cortrium Holter Monitor: When purchasing the Cortrium Holter Monitor, you must add the number of monitors to the online shopping cart system. The Products that you wish to purchase shall

then be placed on the "shopping cart". You can access the "Shopping cart" by clicking the relevant button in the navigation bar and you can make changes to the card at any time. After opening the “Continue to pay”, you can type your company data and contact info, your order information shall be displayed.

(2) Sales of Software Analytics via Web-shop: In addition, you can choose which software analytics option you prefer. Also, this is done by adding the either the monthly flat-fee or the payment option of pay per ECG recording analyzed (pay-per-report).

You can always change your payment choice (monthly flat-fee vs. pay-per-report). It is possible to change from single report payment to flat rate at any time. You must inform Cortrium in writing about your wish to change the payment option and your preferred date for the change of payment. The flat rate is calculated pro rata from the time of the change in the current month.
Please remark that when the monthly flat-fee is chosen, the payment is invoiced per month, and changeset back to pay-per-report requires a notice period of three months to the end of the month.

Also, you can choose not to include any software Analytics. In this case, you will only be charged for the purchase of the Cortrium Holter Monitor.

(3) Submitting the order: Before you finalize the order confirmation, you can re-check all the entered data, and change the data or cancel the purchase transaction.

You submit the "'Shopping card" for ordering by clicking the 'submit' button. When you submit the order, your order is sent to Cortrium as a binding order.

(4) ECG Electrodes: The expenses for ECG electrodes are not included in the Product purchase price.

(5) Payment transfer costs: The Customer must bear the costs arising from payment transfers.

3. Cortrium Guaranties

(1) Cortrium is responsible for making available the Products in compliance with all applicable laws and regulations for usage in the healthcare sector within the Territory of the Customer.

(2) For the quality of the products, only the product description provided with the Instruction-for-Use (IFU) shall be deemed to have been agreed. Cortrium guarantees that the Product can be expected to perform substantially as specified in the Instruction-for-Use ("Guarantee Period") for two years. Defect Products are returned to Cortrium at no cost for the Customer required that the Customer notifies Cortrium in writing about the defected product before shipping and follow Cortrium’s guidelines for shipping of the Product.

(3) Cortrium will deliver repair service to the purchased Products for additional three years after the Guarantee Period. Thus, the "Service Lifetime Period" is five years from Purchase date. After the Guarantee Period, Cortrium is entitled to invoice the Customer for any repair of the Product.

(4) For the delivery of the Products, this shall take place approximately as specified in the Order Confirmation or Receipt. If no time of delivery is specified, the delivery must take place within a reasonable time from the Customer's written request.

(5) Cortrium offered Products are neither fault tolerant nor free from errors or interruptions. Minor deviations must, to some extent, be expected and shall not constitute defects. Moreover, the performance of the Products will vary depending on, e.g. software interactions, quality of data recordings as well as other factors outside of the control of Cortrium.

(6) The Customer is entitled to access or contact an online help service desk during Cortrium office opening hours. The help service includes: Introduction and problem solving related to the operation of the Products offered via manuals, brochures, tutorial videos, telephone, support chat and video-links.

(7) If Cortrium cannot replace or repair the defective Product within ninety 90 days of the Guarantee Period, the Customer can terminate the contractual part with Cortrium relevant to the purchase of the defective Product with immediate effect and received the purchase price in return.

4. Customer acknowledgement

(1) The Customer is a legal registered commercial business or health organisation.

(2) The Customer is responsible for the installation and the use of the Products. Cortrium offers online services free-of-charge for supporting the installation.

(3) All Software Analytics are regarded as decision-making support tools for diagnosing patients. The Software Analytics are subject to an End-User-License-Agreement (Appendix I) and a Data Processor Agreement (Appendix II). The Customer accepts the End-User-License-Agreement and the Data Processor Agreement as part of the agreed Sales Terms.

4.1 Customer's Liabilities

(1) The Customer agrees:

- to procure for a Product property insurance to cover general risks (fire, water and housebreaking).

- to procure at his own expense all ordinary maintenance and necessary cleaning to ensure that the Product is at all times in an orderly condition.

- to make available to Cortrium any insurance payments received from an insurance company to procure the repair of the Product.

To sum-up, the Customer is liable for defects caused by matters related to Customer, including the Customer’s misuse actions or omissions. Thus, the risk of unintentional destruction or devaluation of the Product shall lie with the Customer. In any of these events, the Customer shall remain liable for making the full agreed payments.

(2) The Customer agrees to be assigned to make all present and future claims against Cortrium in connection with the supply of the Products. This shall include without limitation claims arising from default or product liability.

(3) The Customer shall immediately and no later than 24 hours after observation, notify Cortrium the case of any incident or adverse events that have led to the death or the serious deterioration of the health of the patient, the healthcare professional or another person in contact with the Product.

(4) The Customer is responsible for notifying Cortrium any unintended use of the Products no later than 24 hours after observation.

(5) The Customer shall immediately and no later than seven business days after observation, notify Cortrium of any Product defects of its use, documentation, packaging, labelling or services, including but not limited to:

a) Any observation relevant to the safe and efficient use of the Product

b) Non-intended use of the Product

c) Technical or performance issues

d) Unintended software behaviour

(5) If the Customer fails to inform Cortrium of a defect by written notice or by calling Cortrium customer service within seven days, Cortrium is entitled to forfeit the Customer's right to make any claim in respect of the defect.

(6) The Customer is entitled and obliged to pursue at his own expense and own risk – in court or out of court – directly towards Cortrium any Product claims which shall include, without limitation, the right to rescind or to reduce the Purchase price of the Product. This must be made with due regard to the need for immediate objection towards Cortrium.

(7) Cortrium agrees to be bound by the result of any disputes. This shall not apply if the Customer has conspired to the detriment of Cortrium. The burden of proof for such conspiracy shall lie with Cortrium. The Customer agrees to notify Cortrium in writing if, based on the above provisions, the Customer will pursue any claims against Cortrium.

5. Cortrium limitation of liabilities

(1) Cortrium is not to be held responsible for product performance advertising made by third parties via public promotions or statements.

(2) Cortrium does not assume any responsibility or liability for the Product other than what has been expressly set out in the contracts with the customers. Any warranties, representations, guarantees or conditions whether express or implied are excluded to the fullest extent permitted by law. This means that, e.g. warranties of merchantability, fitness for a particular purpose and non-infringement are excluded.

(3) In no event and no matter the circumstances shall Cortrium be liable for any loss of anticipated profit, loss of data, damage to records or data or any indirect, special, incidental or consequential damages or loss (including the loss of goodwill, or loss as a consequence of any kind of business interruption) arising out of or in connection with the contractual relationship, the Product or the use or performance hereof, even if Cortrium was advised of the possibility of such losses and regardless of whether the cause of action is in contract or tort.

(4) Cortrium shall in no event and no matter the circumstances be liable for any loss directly or indirectly incurred by a patient (end-user) of the Customer, not being a Customer or Customer of Cortrium itself. The Customer must ensure that the end-user (Patient) is covered by an patient insurance.

(5) To the maximum extent permitted by applicable law, Cortrium disclaims any Product liability as a consequence of loss or damage to property which, given its nature, is normally intended for commercial use.

(6) In any event, no matter the circumstances, Cortrium's total aggregate liability for any losses or damages arising out of or in connection with the contract, the Product or the use or performance hereof shall not exceed the sum of the actually paid invoices by the Customer for the Product in question.

(7) Cortrium shall have no responsibility or liability for any adjustments or other modifications in the Product, or any use of the Product by Customer itself or third parties. Further, Cortrium shall have no responsibility or liability for any defects which are a consequence of external factors.

(8) The Customer must accept that the Products may include third-party software developed and/or manufactured by a third-party and of which Cortrium is the distributor. This third-party software may be subject to license or standard terms that the Customer shall accept prior to provision of the Product. Cortrium's liability in relation to third-party equipment/software only includes receipt of the Customer's defect report and notifying the third-party manufacture of the defect without undue delay. Cortrium assumes no further liability in this respect.

6. Intended Use and regulatory requirements

(1) The Customer agrees to comply at its own expense with all requirements arising from statutory law and applicable medical regulation associated with the customer's use of the Products within the Territory of usage and to ensure the Customer’s compliance with the same. To that extent, the Customer agrees to indemnify Cortrium against any claims of third parties. Thus, the Customer is responsible for being in possession of the necessary authorization to conduct medical diagnosing and treatment of patients from authorities, health insurers and/or other relevant associations before the use of the acquired product(s). To that extent, the Customer agrees to indemnify Cortrium against any claims of third parties.

(2) The Customer agrees to use the Products in accordance with the Intended Use as stipulated in the Instruction-for-Use (IFU) and for his professional business only. The intended use of the Product, the Data Transfer Tool (DTT) and the Software Analytics are defined in the Instruction-for-Use (IFU). To ensure proper usage of the Cortrium Products, DTT and Software Analytics. The Customer must read and understand the Instruction-for-Use (IFU). The latest updated version of the IFU can be found on the Cortrium webpage.

For clarification; the Cortrium Holter Monitor only records ECG data. The Holter Monitor i) has no capacity for automatic ECG analysis and consequently no capacity for automatically generating alerts of potentially critical cardiac conditions, and ii) the ECG data recorded is stored on the monitor and can be transferred by the physician - or the designated operator - for Cloud-based Software Analytics. The Software Analytics will then provide summary reports (Holter reports). If no Software Analytics are chosen, the ECG recording (ECG raw data) can be stored locally on the desktop or server as EDF-format.

(3) The use of the Data Transfer Tool (DTT) and the Software Analytics as defined in the Instruction-for-Use (IFU) are subject to the End-User-License-Agreement (EULA) which is considered an integrated part of the agreed Sales Terms (Appendix I).

(4) The Software Analytics provides only suggested diagnosis as a tool for decision support for the healthcare professionals. Thus, it is the responsibility of the physician or trained medical officer to evaluate the results of the Software Analytics and sign for the stipulated results for suggested diagnosing of the patient.

7. The Cortrium's Right to Termination for Good Cause

(1) If the Customer uses the Product (Holter Monitor and/or Software Analytics) contrary to the contractual terms and, despite a written warning and cure notice, or continues such unauthorised use causing a material infringement of the product manufacturer and/or Cortrium's rights, then Cortrium shall have the right to terminate the contractual relationship with the Customer. This applies also to any sub-letting of the Products to a third party.

(2) If the Customer is late with a minimum of two consecutive subscription payments of the Software Analytics, then Cortrium shall have the right to terminate the Subscription-based payments of Software Analytics with immediate effect.

(3) Cortrium shall also have a right to termination for good cause and with immediate effect if the Customer’s estate shall become subject to a composition or insolvency petition. This shall be without prejudice to any damage compensation claims that Cortrium may have.

8. Proprietary Rights

(1) All intellectual property rights and other rights, including without limitation patents, utility models, design rights, trademarks, copyright and know-how, in and to the Product, its components, software and any documentation related hereto, remain with Cortrium or its licensors. The Customer agrees to respect such rights whether registered or not.

(2) The Customer shall not reverse engineer, disassemble or decompile the Product or any parts thereof, except where and only to the extent that such operations are permitted according to the applicable mandatory, statutory legislation and subject to Customer’s compliance with all aspects of such legislation.

(3) The Customer must keep the Product free of any third-party rights. The Customer will inform Cortrium immediately about any third-party claims on the Product, about any theft, damaging or loss. The costs of remedies against any of the above-referenced interference in the Product shall be borne by the Customer. The Customer agrees to pay the costs of such action.

(4) The Customer may not make any alterations to the Product without the written approval of Cortrium. If the

Customer has attached any feature to the Product, the Customer shall at own expense, upon demand of Cortrium, be obliged to, remove the attached feature.

(5) The Customer shall not be liable for any changes or impairment on the Products arising from use within the ordinary course of business and the Intended use of the Products.

9. Patient Data

(1) Cortrium warrants that all registered data of the Customer's usage of Cortrium offered software application and analytics are stored for at least ten years from data upload date with back-up procedures for identification, storage, protection, retrieval, retention time and disposition of the stored data.

(2) The link between Patient ECG data and the actual ECG recording is subject for erasure as set in the Data Processor Agreement (Appendix II) between the parties. The Data Processor Agreement is considered an integrated part of Sales Terms.

(3) The Customer shall ensure that the Patient data delivered to cloud-based software analytics is anonymised to the extent that it is not or does not become personal identified or identifiable data as defined in the GDPR (Regulation (EU) 2016/679). To the extent that the Customer delivers or makes such personal data identifiable, the Customer ensures that each Patient has given adequate consent for such operation and that the Patient receives sufficient information on how and where such data is processed.

(4) Data security of processing patient data is regulated by the Data Processor Agreement (Appendix II) and is in compliance with the General Data Protection Regulation in EU - GDPR (Regulation (EU) 2016/679).

10. Customer data

Cortrium collects, processes, and uses customer data according to the contractual relationship between the parties including fulfilling the purpose of servicing the Customer, i.e. data provided by the Customer such as name, address, telephone number, e-mail address, banking details. Processing of such data occurs in accordance with the GDPR and other national data protection legislation, i.e. as defined in Art. 6 sec. 1 lit. a and lit. b of the GDPR, and only for the purposes mentioned above. There is no further data processing.

11. Force majeure

(1) Neither party shall be held liable for any damage sustained by the other party as a direct or indirect consequence of the non-performing party being delayed, prevented or hindered in the performance of its obligations as a result of a force majeure situation. Force majeure situations include war and mobilization, computer viruses, hacking, catastrophes of nature, strikes, lock-out, fire, and damage to production plants, import and export regulations and other unforeseeable circumstances beyond the control of the party concerned.

12. Other Provisions

(1) The Sales terms including appendences shall cover all agreements between Cortrium and the Customer. No verbal side agreements have been made.

(2) If any provision of the Sales Terms shall be partly invalid or unenforceable, then this shall not affect the validity or enforceability of the other provisions. The invalid or unenforceable provision is deemed to be replaced by such valid and enforceable provision that reflects to the closest extent possible the intention that the parties hereto had pursued with the invalid or unenforceable provision.

(3) Each party shall treat as confidential and keep secret any knowledge, information or documentation on the Products and the other party's internal affairs, projects, products, financial status, business operations, customers etc., including information contained or embodied in the Products and the Agreement. This obligation shall remain in force after termination of the contractual relationship for three years.

(4) Cortrium shall be entitled to state Customer as a reference and to include the name of the Customer on its list of references.

(5) Cortrium reserves the right to transfer, fully or partially, rights and obligations relating to the Sales Terms to a third party.

(6) National substantive law of Cortrium shall apply to the Sales Terms and shall have jurisdiction to adjudicate any and all disputes arising out of this Agreement unless mandatory statutory provisions require otherwise. United Nations Convention on Contracts for the International Sale of Goods (CISG) shall be excluded.

Appendix I: End-User-License-Agreement (EULA)

Appendix II: Data Processor Agreement

End-User License Agreement (EULA)

Software Provider: Cortrium ApS, Company Registration Number: DK36445335

End-User: [*Insert Company/Clinic/Hospital/Department & Organisation number*]

1. Scope
(1 The End-User License Agreement ("EULA") shall apply to any use of the Software provided by Cortrium including third party providers of Software Analytics where Cortrium has entered a Data Processor Agreement with the third party provider.

(2) Cortrium is using the following third party providers of Software Analytics:
1. Cardiomatics: The Cardiomatics "Software" is developed and owned by Cardiomatics sp. z o.o. with its registered office in Kraków (address: Wojciecha Weissa 7, 31-339 Kraków, Poland, Company Reg. no: PL 677 238 95 21) ("Owner") and licensed by Cortrium under this EULA.

(3) Cortrium is using its own in-house developed software:
1. Data Transfer Tool (DTT) for transferring ECG data for the processing of Software Analytics.

(4) By using the Software in any way, the End-User accepts to be bound by this EULA. If the End-User does not accept and/or comply with this EULA, the End-User is not entitled to use the Software.

2. The License
(1) Subject to the payment of the agreed license fee per reading of ECG data or as a monthly subscription of unlimited ECG reading from the Cortrium ECG recorder, the End-User is granted a non-exclusive, non-transferable license in the territory of the Customer to use the Software as a License on the terms and conditions set out in this EULA.

(2) The Software License shall expire upon the termination or expiration of the Contractual relationship between the End-User and Cortrium.

3. The Software, availability and changes
(1) Unless otherwise agreed, the Cortrium will use commercially reasonable efforts to make the Software available at all times, except for planned downtime and any unavailability caused by external events, incl. force majeure circumstances, and to provide the Software in accordance with applicable laws and government regulations.

(2) Unless otherwise agreed, the Software is provided "as is" without warranty of any kind. Cortrium and its third party providers do not warrant that the Software will be error-free or that the Software will work without minor interruptions.

(3) The Software may at the sole discretion of Cortrium be subject to changes from time to time, including by addition or removal of features. Such changes may occur without any notice; however, Cortrium will use reasonable efforts to notify the End-User in advance.

4. Rights to use the Software
(1) The right to use the software is subject to a Data Processor Agreement between the Cortrium and the End-User. The Data Processor Agreement is regulating the processing of sensitive data such as the patient id and

the recorded ECG data in compliance with Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data (GDPR).

(2) The right to use the Software pursuant to this License shall be done in a manner and for the purpose set out in this EULA with the following scope:
i) The License shall include the right to use the Software as part of the ECG recorder by any End-User who are authorized healthcare professionals for the purpose of generating medical reports (Holter reports) and any related medical consultations;
ii) The License shall be granted for the needs and purposes as specified in this EULA, in the following fields of use:
a) Launching, displaying or using the Software via the Cortrium ECG recorder;
b) Storing, displaying, uploading, viewing and browsing data when using the Software via the Cortrium ECG recorder;
c) Entering data to the memory of the Cortrium ECG recorder;
d) Entering anonymized medical data to the Cortrium ECG recorder and the Software for the purpose of generating reports.
e) Generating medical reports using the Software.
(3) The Software or any elements thereof shall only be available to third parties with the prior written consent from Cortrium.

(4) The End-User shall not acquire any rights to the Software, except for a license and an authorization to use the Software on the terms and conditions set forth in this EULA.

(5) The End-User is not authorized, except to the extent permitted under mandatory law, to:
a) Play, decompile or modify the source code of the Software;
b) Perform statistical analysis of the Software;
c) Translate adapts, change the layout of the Software, or make any other changes or modifications in the Software or any part thereof;
d) Reproduce the code or translate, adapt, change the layout or make any other changes to the form of the Software and distribute the Software in a different way than that specified in the EULA. Moreover, the End-User does not have the right to permanently or temporarily reproduce the Software, in whole or in part, by any means and in any form, except for 1) making a backup copy if necessary to use the Software, but the backup shall not be used simultaneously with the Software, or 2) permanent or temporary reproduce of the Software in whole or in part by any means, in any form and for any purpose, except for the right to temporarily reproduce the Software in whole or in part in the memory of the Devices.

(6) Any information obtained in connection with the use of the Software shall not be:
a) Used for purposes other than supporting the diagnostic process as part of the Cortrium ECG recorder, as well as for other purposes than the performance of this EULA;
b) Provided to third parties for a purpose other than achieving the aforesaid compatibility and the performance of this EULA;
c) Used for developing, creating or marketing Software infringing the copyright of the Owner and the Software; and in particular for reverse engineering of the Software;
d) Used for developing, creating or marketing computer software or other tools that use information (reports) generated by the Software.

5. Marketing and sub-licensing of the Software

(1) Pursuant to this EULA, the End-User is also granted a license with regard to the Software, within the scope that the Software is not a computer program (graphics, layout of graphic elements):

a) To record and reproduce it in whole or in part, with the use of digital technology, to present it in public, exhibit, display, reproduce, sub-license, broadcast and re-broadcast as well as make it available to the public in such a way that anybody can have access thereto in a place and time of their choice;

b) The scope of such use is limited by the purpose and the contents of this EULA, and the above shall specifically not be construed in any way as a transfer of any intellectual property rights of the Owner, including rights to logos, designs and know-how.

(2) The End-User undertakes to only publicly present, exhibit, display, reproduce, sub-license, broadcast and rebroadcast the Software together with the Cortrium ECG recorder, while taking care of the good name and reputation of the Owner and any other Vendor in relation to the Software.

6. Warranty and Limitations of Liability

(1) Cortrium is not liable for medical decisions taken on the basis of using the Software Analytics for generating medical reports in any way. A report is not a medical diagnosis; it is only an analytical tool with suggested potential diagnosis. For the avoidance of doubt, any medical diagnosis is solely the responsibility of the healthcare professionals.

(2) In no event and no matter the circumstances shall the Cortrium or the third party Vendor of Software Analytics be liable for any loss of anticipated profit, loss of data, damage to records or data or any indirect, special, incidental or consequential damages or loss (including the loss of goodwill, or loss as a consequence of any kind of business interruption) arising out of or in connection with this EULA, performance of the Software and the results connected thereto.

(3) Cortrium and the third party Vendors aggregate liability towards the End-User in respect of any matters arising out of, or in connection with the Software and this EULA, shall be limited to an amount corresponding to 50 % of all payments made under the contractual relationship between Cortrium and the Customer for the period of twelve (12) months prior to the event(s) having given rise to the claim (the 'Liability Cap').

(4) The End-User shall bear full liability for the actions and omissions of its employees or sub-contractors. The End User undertakes to enforce from the entities to which it provides the Software, including any sub-licensees, that their use of the Software does not violate Cortrium's and its third party Vendors copyright on the Software.

(5) The parties agree to exclude guarantee, warranty and any other implied obligations, not explicitly specified in this EULA, in particular regarding merchantability of the Software and the Reports.

7. Termination

(1) In the event of a material breach by the End-User of the terms of the License set forth in this EULA, the End-User shall cease a breach and remedy the consequences of such a breach. In the event that such material breach has not been remedied within five days of receipt of a written notice from Cortrium or its third party Vendors to do so, or the material breach of the License is not capable of remedy the Vendor shall have the right to terminate the License and this EULA without notice (with immediate effect).

This Data Processing Agreement constitutes Appendix II to the agreed Sales and Subscription Terms between Cortrium and the Customer.

The Data Processing Agreement, including its attached sub-appendices, is an Appendix to the Sales and Subscription Terms agreed by the Customer as part of the contractual relationship between Cortrium and the Customer in regard to the Subscription or Purchase of Cortrium ECG recorders ('Product') and the processing of ECG data for analytics for the provision of Holter reports ('Analytics'). The Data Processing Agreement including the sub-appendices must therefore be read and understood by the Customer before accepting the Sales and Subscription Terms for purchasing or subscription to any Cortrium offerings.

1. The Data Processor & The Data Controller
(1) Cortrium is the Data Processor and the manufacturer of an ECG recorder (Holter Monitor) that monitors heart rhythms. Cortrium's data processing is subject to cloud-based AI analytics or desktop-based analytics. The legal identity of the manufacturer is: Cortrium ApS, Erik Husfeldts Vej 7, 2630 Taastrup, Denmark. Company Registration Number: DK36445335.

(2) The Customer is a legal registered commercial business or health organization with an authorization to act as Data Controller on behalf of end-users (patients) being monitored and subject to analytics provided by Cortrium.

(3) The Agreement is concerning the processing and storage terms of personal data and constitutes the 'Data Processing Agreement'). The Agreement regulates Cortrium - hereinafter defined as the 'Data Processor' - of the processing of personal data on behalf of the Customer - hereinafter defined as the 'Data Controller'.

(4) If there are discrepancies between the rights and obligations under the agreed Sales and Subscription Terms and the Data Processing Agreement, the rights and obligations under the Data Processing Agreement shall prevail.

(5) A Customer who wishes to deviate from the agreed terms of the data processing under this Data Processing Agreement shall be responsible for acquiring a written and signed consent issued by Cortrium.

2. Legislation
(1) The Data Processing Agreement shall ensure that the Data Processor complies with the applicable data protection and privacy legislation (the ”Applicable Law”), including in particular 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 (General Data Protection Regulation) which entered into force on 24 May 2016 and will apply from 25 May 2018 (the “GDPR”) and any applicable national implementation laws.

3. Processing of personal data
(1) In connection with the Data Processor’s delivery of the Products and Analytics to the Data Controller, the Data Processor will process certain categories and types of personal data on behalf of the Data Controller.

(2) ”Personal data” means “any information relating to an identified or identifiable natural person” as defined in article 4(1) of the GDPR that is processed under this Data Processing Agreement (the ”Personal Data”). The categories and types of Personal Data, categories of data subjects, the purposes of the processing and the processing activities performed by the Data Processor as well as the processing locations are listed in Sub-Appendix A. The parties shall update Sub-Appendix A whenever changes occur that necessitates an update.

(3) The Data Processor shall have and maintain records of processing activities by article 30(2) of the GDPR.

(4) Cortrium is allowed to use sub-contractors for the Analytics (e.g. to generate the Holter report) when the subcontractor's data processing is controlled by Cortrium regarding the compliance with the European Regulation on Data Protection and Privacy for data subjects (GDPR - EU/2016/679).

4. Instruction

(1) The Data Processor shall only act and process the Personal Data following the documented instruction from the Data Controller (the ”Instruction”) unless the Data Processor is subject to EU law or national Member State law under which the Data Processor is obliged to process the Personal Data differently. In such a case, the Data Processor shall inform the Data Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest. The Instruction at the time of entering into this Data Processing Agreement is that the Data Processor may only process and store the Personal Data with the purpose of, and to the extent, it is necessary for, provision and delivery of the Product and the Analytics and within the specifications described in Sub-Appendix A.

(2) The Data Controller shall ensure that the Personal Data made available to the Data Processor is processed following the Applicable Law, including the legislative requirements of the lawfulness of processing and information to be provided to the data subject.

(3) In the event that the Data Processor does not comply with this Data Processing Agreement, the Data Controller may instruct the Data Processor to stop further processing of the Personal Data with immediate effect - after an additional period to ensure compliance with this Data Processing Agreement of at least 5 days has expired without effect.

(4) The Data Processor shall immediately give notice to the Data Controller if the Data Processor considers the Instruction to conflict with the Applicable Law.

(5) Both the Data Controller and the Data Processor can request the other party to appoint a Data Protection Officer as responsible for data processing and storage and act as the parties main contact person(s).

(6) In the case of the cessation of the Data Processor’s business, e.g. by dissolution or liquidation, the Data Processor must allow the trustee or curator to exercise data controller's rights and assert them against the Data Processor, e.g. enabling the Data Controller to instruct the Data Processor to delete or return personal data.

(7) In the case of the cessation of business of the Data Controller, e.g. by dissolution or liquidation, the Data Processor must hand-over all stored personal data on the Data Processor's systems to the Data Controller. Hereinafter, the Data Processor is obliged to effectively delete the personal data from the Data Processor's own systems.

(8) Upon termination of the business relationship between the Data Controller and the Data Processor, the Data Processor is required, at the request of the Data Controller, to provide termination assistance to the Data Controller until (i) all personal data is transmitted to the Data Controller in a generally accepted electronic format and (ii) has occurred. The Data Processor shall continue processing the personal data and the provision of services under the business relationship until such transfer has taken place.

5. Confidentiality
(1) The Data Processor shall process the Personal Data as strictly confidential information. The Personal Data shall not be copied, transferred or otherwise processed except from the Instruction, unless the Data Controller in writing has agreed hereto.

(2) The Data Processor's employees that process the Personal Data shall be subject to an obligation of confidentiality that ensures that the employees shall treat the Personal Data with strict confidentiality.

6. Security
(1) The Data Processor shall implement the appropriate technical and organisational security measures as set out in the Data Processor Agreement and in the Applicable Law, including in accordance with article 32 of the GDPR.

(2) The Data Processor's security measures are further described in Sub-Appendix B. .

(3) The Data Processor shall provide documentation for the Data Processor's security measures if requested by the Data Controller in writing. The documentation shall be provided within 10 Business Days of the notification of the Data Processor.

7. Data protection impact assessments and prior consultation
(1) If the Data Processor's assistance is necessary and relevant, the Data Processor shall assist the Data Controller in preparing data protection impact assessments in accordance with article 35 of the GDPR along with any prior consultation in accordance with article 36 of the GDPR.

8. Rights of the data subjects
(1) If the Data Controller receives a request for the exercise of a data subject's rights under the Applicable Law and the correct and legitimate reply to such a request necessitates the Data Processor's assistance, the Data Processor shall assist the Data Controller by providing the necessary information and documentation.

(2) If the Data Controller requests the assistance of the Data Processor to respond to a data subject request, the Data Controller shall request so in writing and the Data Processor shall answer such a request with the relevant and necessary information and documentation as soon as possible and no later than 10 calendar days after the receipt of a request.

(3) If the Data Processor receives a request directly from a data subject for the exercise of data subject rights under the Applicable Law and such request is related to the Personal Data, the Data Processor shall immediately, however no later than within 5 business days from the receipt of such a request, forward the request to the Data Controller and must refrain from responding to the person directly.

(4) If the Data Processor shall assist the Data Controller in providing a copy of the Personal Data regarding one or more defined data subjects under the GDPR, article 15(3) or article 20(1), the Data

Processor shall provide such copies to the Data Controller in the following format(s): Personal data will be provided as .csv or .xls file formats.

9. Personal Data Breaches
(1) The Data Processor shall give notice to the Data Controller if a personal data breach occurs, which can lead to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to the Personal Data (a “Personal Data Breach”). The Data Processor shall notify the Data Controller of a Personal Data Breach immediately and no later than 24 hours after being aware of the Personal Data Breach.

(2) The Data Processor shall have and maintain records of all Personal Data Breaches. The records shall at a minimum include the following for each Personal Data Breach:
a) A description of the nature of the Personal Data Breach, including, if possible, the categories and the approximate number of affected Data Subjects and the categories of affected Personal Data.
b) A description of the likely as well as actually occurred consequences of the Personal Data Breach.
C) A description of the measures that the Data Processor has taken or proposes to take to address the Personal Data Breach, including, where appropriate, measures taken to mitigate its adverse effects.

(3) The records of Personal Data Breaches shall be provided to the Data Controller in a copy if so requested in writing by the Data Controller or the supervisory authority within 7 days from the date of delivery of the request or within any other time-limit indicated by the supervisory authority.

(4) The Data Processor shall, on request, assist the Data Controller in drafting notification to the supervisory authority and/or the data subjects affected by the Personal Data Breach.

10. Documentation of compliance
(1) The Data Processor shall on the Data Controller’s written request hereof provide documentation substantiating the following:
a) The Data Processor complies with its obligations under this Data Processing Agreement and the Instruction.
b) The Data Processor complies with the Applicable Law in respect of the processing of the Personal Data.

(2) The Data Processor’s documentation in connection with section 10.1 shall be provided within 30 business days after the receipt of the request.

(3) The data processor must, as documentation of ongoing compliance with the Data Processor Agreement, make self-assessment reports available to the Data Controller. These self-assessment reports must as a minimum be prepared once a year and must follow the principles and control objectives as set out in the audit standard ISAE3000. The self-assessment reports must be signed by the Data Processor's management. The Data Processor is not obligated to initiate and undertake external audits of its compliance with the Data Processing Agreement on its initiative.

(3) Notwithstanding the above section (3), the Data Processor shall allow for and contribute to audits, inspections, etc., to be conducted by the Data Controller, auditors mandated by the Data controller, or public authorities or other competent jurisdictions, insofar such audits, inspections, etc. are necessary to verify the compliance of the Data Processor with this Data Processing Agreement and the Applicable Law. Any auditors performing said audit, inspections, etc. must have undertaken a duty of confidentiality either by written contract or by statutory law. The Data Controller shall notify the Data Processor 14 calendar days before such an audit. If an audit is carried out by a governmental authority directly at the Data Processor's premises and relates to processing activities performed on

behalf of the Data Controller, the Data Processor must inform the Data Controller hereof and participate in and facilitate such audits. If the audit is not performed due to actions or omissions by the Data Processors or its Sub-Processors, the Data Processor shall be entitled to invoice the Data Controller for its assistance with such audits.

11. Sub-Processors

(1) The following shall apply for the Data Processor's engagement of third parties to process the Personal Data ("Sub-Processors"): The Data Processor has general authorization to engage Sub-Processors without further written consent from the Data Controller provided that the Data Processor informs the Data Controller in writing of the identity of the potential Sub-Processor (and of any data processor of the Sub-Processor) at least 7 calendar days prior to entering into an agreement with the concerned Sub-Processor, thereby giving the Data Controller the opportunity to object to such changes. Such an objection must be reasonable. If the Data Controller has not objected to the named Sub-Processor within 7 calendar days of the Data Processors notification, the non-objection shall be deemed a tacit consent.

(2) The Data Processor shall conclude a written sub-processor agreement with any Sub-Processor. Such an agreement shall at minimum provide the same data protection and security obligations as the ones applicable to the Data Processor in accordance with this Data Processing Agreement and the contractual business relationship between the parties. The Data Processor shall on an ongoing basis monitor and control its Sub-Processors' compliance with such data protection obligations, and the documentation hereof shall be provided to the Data Controller if so requested in writing within 15 business days of the receipt of such a request. The Data Processors involvement of Natural persons (sole entrepreneurs) are not considered as sub-processors, but must work under the company's confidentiality procedures equivalent to employees of the Data Processor.

(3) The Data Processor is accountable to the Data Controller for any Sub-Processor's processing of the Personal Data in the same way as for its own actions and omissions.

(4) The Data Processor is at the time of entering into this Data Processing Agreement using the Sub-Processors listed in Sub-Appendix C. If the Data Processor initiates sub-processing with a new Sub-Processor, such new Sub-Processor shall be added to the list in Sub-Appendix C under paragraph 2.

12. Location of the Personal Data

(1) The Personal Data shall only be processed by the Data Processor at the locations specified in Sub-Appendix A. The Data Processor shall not transfer the Personal Data to third countries or to international organizations in third countries.

(2) If the transfer of the Personal Data to third countries outside the EU/EEA is performed by the Data Processor to Sub-Processors accepted under this Data Processor Agreement, the Data Controller hereby authorizes the Data Processor to enter into the EU Commission's adopted standard contractual clauses on the Data Controller's behalf with said Sub-Processors. If the Data Controller is itself a data processor for its ultimate contracting parties and the Data Processor therefore is a sub-data processor towards the Data Controller's ultimate contracting parties, the Data Controller shall be responsible for collecting any necessary mandate and authorization to enter into the EU Commission's adopted standard contractual clauses with the Data Processor.

(3) Any transfer of the Personal Data shall only be done in accordance with this Data Processing Agreement, including the Instruction and the Applicable Law.

(4) The Data Controller can stipulate the location storage and processing of the patient data to avoid any data on systems that are beyond control of the Data Controller.

(5) The Data Processor applies with the organizational and technical measures indicated in Sub-Appendix B and stores data on servers protected against hacking provided on the basis of relevant agreements with cloud hosting companies.

13. Remuneration and costs
(1) The Data Processor is not entitled to remuneration for fulfilling its obligations under the Data Processing Agreement in addition to the payment already agreed upon in the contractual business relationship between the parties..

(2) The Data Processor is entitled to payment for the time and materials necessitated by and used to comply with any changes to the Instruction, when those changes are made by the Data Controller and are not a direct result of changes in Applicable Law. This includes implementation costs and increased costs for delivery of the Product and the Analytics.

(3) If changes to the Applicable Law, including the interpretations and guidelines hereof, results in increased costs for the Data Processor, the Data Controller shall pay such additional documented costs for the Data Processor.

14. Breach and liability
(1) The Data Processor is not liable for non-delivery or delay of the Product and Analytics in so as its delivery will violate the modified Instruction or delivery following the modified Instruction is impossible. This may, for example, be the case, (i) where the modifications cannot be technically, practically or legally implemented, or (ii) where the Data Controller explicitly states that the modifications must apply before implementation is possible.

(2) Notwithstanding any conflicting provisions in this Data Processing Agreement, the Sales and Subscription Terms accepted by the Data Controller as part of the contractual business relationship between the parties, in regard to clauses on breach and limitation of liability shall apply to this Data Processing Agreement as if this Data Processing was an integral part of the overall business relationship between the parties, however, the maximum cumulative liability of a party under this Data Processing Agreement is limited to the total due payments from the contractual business relationship between the parties in the 12 months immediately preceding the injurious event. If the Data Processing Agreement has not been in force for 12 months, the amount is calculated proportionally based on the period in which the Data Processing Agreed has been in force. Limitation of liability does not apply to damages arising from intent, grossly negligent behaviour, or expenses and resources of the other Party's obligations to a supervisory authority.

15. Duration
(1) The Data Processing Agreement shall remain in force for as long as the Data Processor processes the Personal Data.

16. Termination
(1) This Data Processing Agreement shall remain effective for as long as the Data Processor processes Personal Data on behalf of the Data Controller.

(2) The Data Processor may continue to process the Personal Data for up to three months after the termination of the Data Processing Agreement to the extent it is necessary and required under the Applicable Law and the Data Controller is notified thereof at the same time. In the same period, the Data Processor is entitled to include the Personal Data in the Data Processor's backup. The Data Processor's processing of the Data Controller's Personal Data in the three months after the termination of this Data Processing Agreement shall be considered as being following the Instruction.

(3) At the termination of this Data Processing Agreement, the Data Processor and its Sub-Processors shall, at the Data Controller's choice, return or delete the Personal Data processed under this Data Processing Agreement, provided that the Data Controller is not already in possession of the Personal Data. At the Data Controllers' written request, the Data Processor shall delete all the Personal Data, except when EU-Member State legislation or national legislation stipulates otherwise. The Data Processor shall provide documentation for such deletion to the Data Controller upon request. The Parties must agree on the format and procedure for the return of the Personal Data. The Instruction on erasure and the retention periods for the personal data covered by the Data Processing Agreement are specified in Sub-Appendix A.

17. Additional regulations for processing personal data (Germany)[1]

(1) As part of the overall contractual business relationship between the Data Controller and Data Processor, the patient data must be processed under professional secrecy, cf. § 203 (StGB). The Data Processor is committed to maintain confidentiality about professional secrets and to gain knowledge of the processed data only to the extent necessary to fulfill the tasks assigned to it. It is within the responsibility of the employee accessing the patient data to be aware of the personal data subject to the protection of § 203 (StGB). This must be clarified for the person responsible for the data processing.

(2) The Data Processor ensures that all employees involved in the processing of the patient data on behalf of the Data Controller are subject to professional secrecy including the employees of sub-contracting parties for the data processing. This means that the employees of the Data Processor are committed not to undertake disclosure of confidential data without any authorization. Further, the possible criminal liability according to the Criminal Code Act (StPO) must be clarified for the employees performing the data processing. If violation of the Criminal Code Act occurs, the Data Processor is subject to the penalties in accordance with Section 203 (4), sentence 2, when confidential data and/or information is revealed, or when the authorized Data Processor cannot ensure that the 3rd party subcontractor was obliged to maintain confidentiality.

(3) The Data Processor is advised that data processed on behalf of the Data Controller is subject to the right to refuse to give evidence to so-called 3rd parties, cf. Section 53a (StPO). According to § 53a (StPO), the Data Controller decides on the exercise of the right to remain silent. In the event of an inquiry, the Data Processor will refer to § 53a (StPO) and inform the Data Controller immediately. It is the Data Controller who decides whether to exercise the right to remain silent.

(4) The Data Processor is advised that all confidential data in his custody is subject to the prohibition of confiscation, cf. Section 97 (2) (StPO). The data may not be released without the consent of the Data Controller. In the event of confiscation, the Data Processor will apply and immediately inform the Data Controller about the confiscation.

(5) Furthermore, all employees of the Data Processor are obliged to comply with the duty to protect the business and trade secrets of the Data Controller and must be referred to as §17 UWG.

18. Contact

[1] **German legislation references, Section 17:**
- German Penal Code (in German: Strafgesetzbuch (StGB))
- Code of Criminal Procedure (in German: (Strafprozeßordnung – StPO)
- The German Act against Unfair Competition (in German: Gesetz gegen den unlauteren Wettbewerb - UWG)

(1) The contact information for the Data Processor and the Data Controller is provided as part of the contractual business relationship between the parties.

19. Accept
(1) Both parties agree and guarantee that this Data Processing Agreement is entered into and accepted by persons that are authorized and have the necessary mandate to do so.

20. Signatures
(1) The Data Processor is bound by the Data Processor Agreement without the Parties' signatures. The Data Processor Agreement is thus concluded without physical / digital signatures, as the Data Processor Agreement is binding as part of the contractual business relationship between the Data Processor and the Data Controller in accordance with the requirement of GDPR, article 28(3), first sentence.

Sub-Appendix A

1. Personal Data
(1) The Data Processor processes Personal Data in connection with its delivery of the contractual business relationship between the parties.

(2) The processed Personal Data includes, but is not limited to, the following types of Personal Data:
- Data Controller's provided personal data: Email, username, password, varying personal data that the Data Controller or the Data Controller's customers or end-users (patients) issue or register without Cortrium's active request, processing and identification thereof.
- Data Controller's provided Patient id: Patient id - provided by the Data Controller's employees (GP/Clinic/Medical officer)
- Data Controller's provided Patient info: Name, Surname, Date-of-birth, Gender, ECG recording start-time and expected recording length, Holter report including listing of the patient's heart arrhythmias and suggested diagnosis (if any) for decision support

2. Purpose
(1) Data Transfer Tool (DTT): The Data Processor processes Personal Data with the purpose to prepare the ECG recorder (Holter Monitor) before the ECG recording of the patient, including giving options for processing data for Analytics to the healthcare professional. The Data Controller's employees (the healthcare professional) can assign a patient id in the Data Transfer Tool, choose the expected length of the recording, and further decide whether the ECG recording is processed for AI supported AI cloud analytics or stored locally on the Data Controllers own PC/Laptop or server.

(2) Cloud Analytics: The purpose of the AI supported Cloud Analytics is to generate a Holter report - based on the transferred ECG data from the Data Transfer Tool - with an overview of detected heart arrhythmias and including suggested diagnosis (if any). It is the healthcare professional's final decision either to accept or reject the suggested diagnosis.

3. Data subjects
(1) The Data Processor processes Personal Data on the following categories of data subjects on behalf of the Data Controller:
- Patients of the healthcare professionals, ambulatory or admitted patients at Clinics or Hospital.

4. Processing activities
(1) The Data Processor processes the Personal Data by performing the following processing activities:

- The Data Transfer Tool is a Cortrium in-house developed software application that is used for preparing the Cortrium Holter Monitor before use with a new patient. The software is also used to process recordings from the Holter Monitor, and convert the recordings to locally readable and analysable data. The Data Transfer Tool processing of ECG data can either be stored as EDF-format on the healthcare professional's local PC, Laptop or Server for other analysis purposes not controlled by Cortrium - or the transfer tool can process the ECG data for AI software cloud analytics. When processed for cloud analytics, the ECG data is encrypted.
- The AI supported cloud analytics is generating a Holter report based on the transferred ECG data with an overview of detected heart arrhythmias and suggested diagnosis (if any). It is the healthcare professional's final decision either to accept or reject the suggested diagnosis.

5. Locations
(1) The Data Processor processes the Personal Data at the following locations:
- Frankfurt am Main, Germany - Amazon Web Services (AWS) Region: EU-central-1, EU- Frankfurt.

6. Instruction about erasure and retention periods
(1) The Data Processor is subject to the following instruction about erasure and retention periods for the personal data:
- The Data Transfer Tool does not store any data. The transfer tool allows for access to ECG recordings on the Cortrium Holter Monitor. The healthcare professional is in full control and can delete ECG recordings on the Holter Monitor in accordance with the Data Controller's (the physician's or the clinic's) own erasure policy of personal data policy.
- When the ECG recordings are processed for AI supported Cloud Analytics, the retention period is ten years from upload time. After ten years, the patient id is decoupled from the ECG data processed to the cloud. As a consequence, after ten years, the healthcare professional can no longer request a copy of the generated Holter report.

Sub-Appendix B

1. Introduction
(1) This description of the technical and organisational security measures (the “Description of Security Measures”) is prepared to demonstrate the Data Processor’s established security measures, implemented in accordance with article 32 of the GDPR or security measures to be established before the processing of the Personal Data.

2. Organisational security
(1) The Data Processor has implemented the following organisational security measures:
a) All employees of the Data Processor are subject to confidentiality obligations that apply to all processing of Personal Data.
b) The employee access to Personal Data is limited, so that only the relevant employees have access to the necessary Personal Data.
c) The processing of Personal Data done by the employees of the Data Processor is logged and can be checked as required.
d) The Data Processor has documentable process descriptions for the processing of Personal Data.
e) The Data Processor has an IT security policy.
f) The Data Processor has established procedures that ensure proper deletion or continuous confidentiality when hardware is repaired, serviced or disposed.
g) The Data Processor has implemented a Multi-Factor Authentication for key tools and services.
h) The Data Processor is using a central workstation management system.

3. Technical and logical security
(1) The Data Processor has implemented the following technical and logic security measures:

a) The Data Processor uses logical access control with username and password or other unique authorization.
b) The Data Processor regularly makes backups.
c) The Data Processor encrypts personal data in systems and/or on devices.
d) Personal data is pseudonymized when relevant and under consideration of the processing nature.
e) The Data Processor's websites and web forms are using SSL certificates/HTTPS (HyperText Transfer Protocol Secure).
f) The Data Processor logs and controls unauthorized or repeated failed login attempts.

4. Physical security
(1) The Data Processor has implemented the following physical security measures:
a) The Data Processor's devices (including PCs, servers, etc.) are secured behind locked doors
b) The Data Processor's premises and facilities or access routes are subject to video or image monitoring.
c) The Data Processor uses alarm systems to detect and prevent burglary.
d) The Data Processor uses fire alarms and smoke detectors to detect and prevent fires.

Sub-Appendix C
1. Approved Sub-Processors
(1) The following Sub-Processors shall be considered approved by the Data Controller at the time of entering into this Data Processing Agreement on the terms of this Data Processing Agreement and the Applicable Law:
Cardiomatics Sp. z o.o.
Address: Wojciecha Weissa 7, 31-339 Krakow, Poland Company Reg. no: PL 677 238 95 21
Phone: +48 790 261 534
Email: contact@cardiomatics.com
Web: www.cardiomatics.com

2. New Sub-Processors
(1) New Sub-Processors may be used by the Data Processor by adding and updating these in a separate document in continuation of this Sub-Appendix C, which shall be sent for information to the Data Controller before a new Sub-Processor is used in accordance with article 28(2) of the GDPR.