DATA PROTECTION AGREEMENT
TECHNICAL SUPPORT AND MAINTENANCE

This Data Protection Agreement and its annexes ("DPA") establishes minimum data protection and cybersecurity standards and related requirements and forms part of the contract, including a commercial agreement, a service agreement or an order (the "Agreement") (except Cepheid C360 User Agreement). This DPA is entered into by and between the Customer (as defined in the Agreement) and Cepheid (as defined in the Agreement) and shall continue in full force and effect for the duration of the Agreement. Cepheid and Customer are hereinafter individually referred to as a "Party" or collectively as the "Parties".

The Parties agree that where there is Processing of Personal Data under the Agreement, the terms of this DPA will apply to that Agreement, whether or not expressly referenced in that Agreement.

THEREFORE, in consideration of the premises set forth hereinabove and of the mutual covenants herein contained, the parties agree as follows:

1. Definitions.

(A) "Applicable Law" means any law (including all worldwide data protection and privacy laws and regulations applicable to the Personal Data in question including, where applicable, EU Data Protection Law or POPIA), rule or regulation applicable to the Agreement, the Services, or Parties and applicable industry standards concerning privacy, data protection, confidentiality, information security, availability and integrity, or the handling or Processing (including retention and disclosure) of Personal Data, as may be amended, regulated, restated or replaced from time to time.

(B) "Controller", "Processor", "Data Subject", "Personal Data or Personal Information", "Process", "Processing", "Special Categories of Personal Data" and "Sensitive Personal Information" shall have the meanings given in Applicable Law.

(C) "Data Breach" means, (i) the loss or misuse (by any means) of Personal Data; (ii) the inadvertent, unauthorized, and/or unlawful disclosure, access, alteration, corruption, transfer, sale, rental, destruction, or use of Personal Data; (iii) any other act or omission that compromises or may compromise the security, confidentiality, or integrity of Personal Data, or (iv) any breach of security safeguards.

(D) "EU / UK / Swiss Data Protection Law" means (i) Regulation 2016/679 of the European Parliament and of the Council 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 ("EU GDPR"); (ii) the EU GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 (the "UK GDPR"); (iii) in Switzerland the Federal Act on Data Protection of 19 June 1992 (revised version) (the "FADP"); (iv) the EU e-Privacy Directive (Directive 2002/58/EC); and (iv) any and all applicable national data protection laws made under or pursuant to (i), (ii) or (iii); in each case as may be amended or superseded from time to time.

(E) "Personal Data" means, in any form, format or media, any (a) confidential information of Customer; and/or (b) data which means any information that can identify an individual. For clarity, Personal Data also means Personal Information.

(F) “POPIA” means the Protection of Personal Information Act, South Africa, an Act dealing with the protection and regulation of processing personal information within the Republic of South Africa, assented to on November 13, 2013 and commenced application on July 1, 2020.

(G) Restricted Transfer" means (i) where the EU GDPR applies, a transfer of Personal Data to a country outside of the European Economic Area which is not subject to an adequacy determination by the European Commission; (ii) where the UK GDPR applies, a transfer of personal data to any other country which is not based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018; (iii) where the FADP applies, a cross-border disclosure in the absence of legislation that guarantees adequate protection pursuant to Article 6 of the FADP; and (iv) where the POPIA applies, a cross border transfer, disclosure or exchange of information outside the Republic of South Africa.

(H) “Standard Contractual Clauses” means (i) where the EU GDPR applies, the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council ("EU SCCs"); (ii) where the UK GDPR applies, the "International Data Transfer Addendum to the EU Commission Standard Contractual Clauses" issued by the Information Commissioner under s.119A(1) of the Data Protection Act 2018 ("UK Addendum"); (iii) where the FADP applies, the model contracts and standard contractual clauses recognized per the Swiss Federal Data Protection and Information Commissioner (“FDPIC”) pursuant to Article 6 paragraph 2 letter a of the FADP in accordance with the statement of the FDPIC of 27 August 2021 (originally available at https://www.edoeb.admin.ch/dam/edoeb/en/dokumente/2021/Paper%20SCC%20def.en%2024082021.pdf.download.pdf/Paper%20SCC%20def.en%2024082021.pdf) (“Swiss Addendum”); and (iv) where the POPIA applies contractual clauses related to protection, processing and transfer of personal information executed by two or more parties in relation to such information.

(I) “Services” means those services that Cepheid performs pursuant to the Agreement.

(J) “Sub-Processor” means any entity or person to whom the Processor sub-contracts its responsibilities.

(K) If applicable, other capitalized terms as defined by the Agreement.

2. Relationship of the Parties:

2.1 Customer (the “Controller”) appoints Cepheid as a Processor to Process the Personal Data described in Annex 1 to this DPA for the purposes described therein (or as otherwise agreed in writing by the Parties) (the “Permitted Purpose”). Each party shall comply with the obligations that apply to it under Applicable Law.
Customer acknowledges and agrees that Cepheid may engage its affiliates and/or third-party sub-processors in connection with the provision of the Services. Cepheid remains fully liable to Customer for such third party and enters into a written and enforceable agreement with such third party that includes terms that are no less restrictive than the obligations applicable to Customer under this DPA.

2.2 Cepheid collects and processes the necessary identification data for the purpose of concluding and performing the Agreement, and more broadly for the management of the Parties business relationship,

for sending information on products, goods and services or related products, goods, or services from affiliates.
For more information, the Cepheid's Privacy Policy is available on Cepheid website or you can contact Cepheid to the email address: privacy.officer@cepheid.com
Customer commits to inform any data subject concerned about Cepheid's processing activities and provide Cepheid's privacy notice accordingly.

3. General Requirements.

3.1 Where Cepheid Processes Personal Data on behalf of Customer, Cepheid shall:

i) comply with all applicable laws, including Applicable Law, when Processing Personal Data;

ii) except as required by applicable law, process Personal Data only on behalf of Customer and solely to the extent necessary to provide the Services to Customer and in accordance with all applicable laws, including Applicable Law, and the documented instructions of Customer;

iii) implement and maintain appropriate and reasonable technical and organizational security measures to ensure a level of security appropriate to the risk, including, as appropriate, the measures referred in Article 32(1) of the EU and UK GDPR (including the Payment Card Industry Data Security Standard requirements if Cepheid Processes cardholder or other financial account data) to protect the Personal Data (i) from accidental or unlawful destruction, and (ii) loss, alteration, unauthorized disclosure of, or access to the Personal Data; at a minimum, such measures shall include the measures identified in Annex 2;

iv) only permit access to Personal Data by Cepheid personnel who need to access the relevant Personal Data as reasonably necessary for the purposes of the Agreement, with all such individuals being subject to a duty of confidentiality;

v) provide all reasonable and timely assistance (including by implementing appropriate and reasonable technical and organizational measures) to assist Customer in responding to: (i) any request from a Data Subject to exercise any of its rights under Applicable Law (including its rights of access, correction, objection, erasure and data portability, as applicable); and (ii) any other correspondence, enquiry or complaint received from a Data Subject, supervisory authority or other third party in connection with the Processing of the Personal Data. If any such request, correspondence, enquiry or complaint is made directly to Cepheid, Cepheid shall promptly inform Customer providing full details of the same;

vi) promptly notify Customer of:

a) any request, inquiry, complaint, notice or communication received from any third party, including a Data Subject or a supervisory authority, with respect to any Personal Data and comply with instructions of Customer in responding to such request, inquiry, complaint, notice or communication; and

b) any instruction by Customer that Cepheid believes to be in violation of applicable laws, including Applicable Law;

vii) in case of international transfer, the Parties agree that when the transfer of Personal Data is a Restricted Transfer it shall be subject to the appropriate Standard Contractual Clauses as set out in Annex 3.

viii) upon Customer's reasonable request and with reasonable advance notice, submit the facilities it uses to Process Personal Data and/or the Personal Data for audit which shall be carried out by Customer representatives, or an auditing body agreed to by both Parties, with the cost associated therewith being borne exclusively by the Customer;

ix) keep appropriate records that support its compliance with its obligations under this DPA and make them available to Customer in connection with any audit referred to in (viii) above;

x) except where Cepheid has put in place Standard Contractual Clauses in respect of any Restricted Transfer of Personal Data not transfer any Personal Data from any jurisdiction to any other jurisdiction without Customer's prior written consent;

xi) reasonably assist and cooperate with Customer, including assisting Customer with any data protection impact assessment or privacy impact assessment (as required by Applicable Law) and prior consultations with applicable authorities, to assist Customer to comply with its obligations under Applicable Law;

xii) retain Personal Data only for as long as necessary to perform the Services, and at the end of the provision of the Services at Customer's choice delete or return the Personal Data to Customer (unless expressly required otherwise by applicable law) and provide written certification, if requested, to Customer that it has complied with this section;

xiii) if Cepheid reasonably suspects or becomes aware of a Data Breach:

a) provide Customer written notice of the same without undue delay and in no event later than twenty-four (24) hours after becoming aware of such suspected or confirmed Data Breach;

b) provide the Customer with information to allow it to report or inform data subjects of the Data Breach, as necessary;

c) undertake an investigation of such Data Breach and reasonably cooperate with Customer, regulators and law enforcement agencies;

d) not make any public announcements relating to such Data Breach without Customer's prior written approval, which shall not be unreasonably withheld; and

e) take reasonable corrective action in a timely manner to assist in the investigation, mitigation and remediation of a Data Breach, to remediate and mitigate the risk of a recurrence of such Data Breach; and

xiv) submit to the choice of jurisdiction stipulated in the Agreement with respect to any disputes or claims howsoever arising under this DPA, including disputes regarding its existence, validity or termination or the consequences of its nullity; and this DPA and all non-contractual or other obligations arising out of or in connection with it are governed by the law of the country or territory stipulated for this purpose in the Agreement.

3.2 The Parties shall not participate in (nor permit any sub-processor to participate in) any other Restricted Transfers of Personal Data (whether as an exporter or an importer of the Personal Data) unless the Restricted Transfer is made in full compliance with Applicable Law and pursuant to Standard Contractual Clauses implemented between the relevant exporter and importer of the Personal Data.

3.3 Customer authorizes Cepheid to appoint Sub-Processors (and permit each Sub-Processor appointed to appoint other Processors) in accordance with Section 3.3 and any restrictions in the Agreement.

3.3.1 Customer hereby provides a general consent for Cepheid to use Sub-Processors already engaged as of the date of this DPA provided that Cepheid remains fully liable to Customer for such third party and, in each case as soon as practicable, enters into a written and enforceable agreement with such third party that includes terms that are no less restrictive than the obligations applicable to Cepheid under this DPA.

3.3.2 Cepheid maintains a list of its authorized sub processors available upon request.

4. Miscellaneous.

If applicable, the Standard Contractual Clauses, including Annexes 1-4, shall govern and control in the event of any conflict or inconsistency between the terms of this DPA and the Standard Contractual Clauses.

Annex 1
Data Processing Description

This Annex 1 forms part of the DPA and describes the Processing that the Processor will perform on behalf of the Controller.

List of Parties

Processor:

1.	Name:	Cepheid, entity identified in the Agreement
	Address:	As defined in the Agreement
	Contact person's name, position and contact details:	As defined in the Agreement or between the Parties
	Activities relevant to the data transferred under these Clauses:	Described in this Annex 1
	Role:	Processor

Controller:

1.	Name:	Customer, entity identified in the Agreement
	Address:	As defined in the Agreement
	Contact person's name, position and contact details:	As defined in the Agreement or between the Parties
	Activities relevant to the data transferred under these Clauses:	Described in this Annex 1
	Role:	Controller

Description of the transfer

Subject Matter of the Processing
Personal Data is Processed for the following purposes:
Technical Support, workflow optimization), high level support, minimize Customer downtime, responding to feedback from Customer, regulatory issues, metering, customer analytics (connectivity verification (troubleshooting, implementation / LIS (laboratory informatic system)), post market vigilance, audits

Duration of the Processing
Personal Data will be Processed until:
Customer analytics: Processed as long as necessary to fulfil the purposes and provide requested services pursuant to the Agreement, unless otherwise agreed upon in writing
Technical Support, high level support, minimize Customer downtime, responding to feedback from Customer, regulatory issues, metering, connectivity verification: until problem resolution
All data can be stored in archives for post market vigilance or audits purposes for retention period depending on the Regulation

Frequency of transfer

Personal Data will be Processed on a continuous basis.

Nature of the processing:

Processing operations
Personal Data will be subject to the following basic Processing activities:
Record, storage, consultation, use, disclosure by transmission, combination, restriction, erasure or destruction, anonymization, pseudonymization, and as set forth in the Agreement.

Categories of data subjects
The Personal Data to be Processed concerns the following categories of data subjects:
Patients of Customer
Customer and its employees

Categories of personal data
The Personal Data to be Processed concerns the following categories of data:
Depending on data entered by Customer into the instrument console and/or received by the Laboratory Information System, the following data can be processed for the different purposes listed above: Sample ID, instrument telemetry data (temperature, voltages, pressure, system alerts and alarms), test results, name, surname, patient ID (data may include sensitive or special categories of personal data)

Competent Authority

This will be the supervisory authority of the EU member State where the exporter is established, the Information Commission if the exporter is established in the United Kingdom ("UK") or the FDPIC if the exporter is estabiliched in Switzerland. Where the exporter is not established in an EU member State, the UK or Switzerland but it is subject to EU/UK/Swiss Data Protection Law, this will be the supervisory authority in the jurisdiction where Cepheid's representative is established (as required under EU/UK/Swiss Data Protection Law). Where the appointment of a representative is not required under EU/UK/Swiss Data Protection Law, the supervisory authority will be the CNIL in France if the individuals whose data is transfered are located in the EU, the Information Commissioner if the individuals are located in the UK or the FDPIC if the individuals are located in Switzerland. If the Personal Data originates from Canada, the supervisory authority will be one of the Commissioners who has jurisdiction over the matter as determined by the Applicable Data Protection Law.

Annex 2
Description of Technical and Organizational Measures Implemented by Cepheid

This Annex 2 forms part of the DPA and describes the technical and organizational measures which Cepheid has implemented in accordance with Article 32(1) of the GDPR and other Applicable Data Protection Laws.

1- On site:

Cepheid associate may use encrypted USB drive to extract necessary Customer instrument data to remedy technical issues and instrument performance.
For performance optimization visits, Cepheid associates access only minimum necessary data, which does not contain any patient healthcare data. The data is transferred to the associate's notebook, is processed for customer report generation with recommendations, and is thereafter deleted per Standard Work and Cepheid data retention policies.

2- Remotely:

Access role: Only Cepheid Technical Support and Field Support associates have secured access to the instruments.
For remote support for complaints handling, Cepheid agents can use Remote Desktop Sharing (RDS) sessions, but only after the session is authorized by the customer at each instance.
Data transmission: Per Cepheid policy data is transmitted via secure encrypted method to internal Cepheid servers for associate to engage in customer support activities (TLS 1.2+ protocols are used for secured transactions).

3- Customer sends data:

Sending by email, on web platform or per fax: data is sent by the Customer via secure encrypted method to internal Cepheid associate within region. The Customer, as Controller, is responsible for anonymizing Personal Data and uploading only the minimum data required before transferring to Cepheid (Cepheid instrument software allows the Customer to cloak specific Personal and Healthcare Data in its instrument report before exporting).

4- Data transfers within Cepheid Support functions:

If additional support is needed outside Customer home region, only necessary information will be transmitted; unnecessary Personal and Healthcare Data will be deleted / anonymized where possible* and data will be sent via secure sharing method. Data at rest is encrypted and is destroyed per appropriate Cepheid customer care policy.

5- Policy and Practice:

Cepheid ensures the ongoing confidentiality, integrity, availability and resilience of processing systems and services. For this purpose, it has the ability to restore the availability and access to relevant services support and complaints case handling data in the Cepheid systems in a timely manner in the event of a physical or technical incident.

6- Processes:

Cepheid has a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

* Procedure to de-identify/anonymize is instrument specific.

Annex 3
UK, EU and Swiss Transfer Provisions

This Annex 3 forms part of the DPA and sets out how the Standard Contractual Clauses will be completed:

1. Where the EU SCCs are deemed entered into and incorporated into this DPA by reference between the Parties the EU SCCs will be completed as follows:

   (i) Module Two will apply to the extent that Customer is a controller of the Personal Data;

   (ii) in Clause 7, the optional docking clause will apply;

   (iii) in Clause 9, Option 2 will apply, and the time period for prior notice of Sub-Processor changes shall be as set out in Clause 3.2 of this DPA;

   (iv) in Clause 11, the optional language will not apply;

   (v) in Clause 17, Option 2 will apply, and the EU SCCs will be governed by the law of the jurisdiction of establishment for the data exporter, where applicable and where such law allows for third-party rights, and otherwise the law of France;

   (vi) in Clause 18(b), disputes shall be resolved before the country courts of the data exporter and otherwise the courts of France;

   (vii) Annex I of the EU SCCs shall be deemed completed;

      (A) Part A: with the information set out in Annex 1 to this DPA;

      (B) Part B: with the relevant Processing description set out in Annex 1 to this DPA; and

      (C) Part C: in accordance with the criteria set out Clause 13 (a) of the EU SCCs;

   (viii) Annex II: with the Minimum Security Measures; and

2. Where the UK Addendum is deemed entered into and incorporated into this DPA by reference between the Parties, the UK Addendum will be completed as follows:

   a. The EU SCCs, completed as set out above in clause 1 of this Annex 3, shall also apply to transfers of such Personal Data, subject to sub-clause 2.b of this Annex 3 below;

   b. Tables 1 to 3 of the UK Addendum shall be deemed completed with the relevant information from the EU SCCs, completed as set out above, and the options "neither party" shall be deemed checked in Table 4. The start date of the UK Addendum (as set out in Table 1) shall be the Effective Date.

3. Where the Swiss Addendum is deemed entered into and incorporated into this DPA by reference between the Parties, the Swiss Addendum will be completed as follows:

a. The EU SCCs, completed as set out above in clause 1 of this Annex 3, shall also apply to transfers of such Personal Data, subject to sub-clause 3.b of this Annex 3 below;
b. the Standard Contractual Clauses incorporated per reference shall protect the Personal Data of legal entities in Switzerland until the entry into force of the revised FADP.

4. If neither sub-clause 1, sub-clause 2 or sub-clause 3 of this Annex 3 applies, then Parties shall cooperate in good faith to implement appropriate safeguards for transfers of such Personal Data as required or permitted by the Applicable Law without undue delay.

Annex 4
4.1 Supplemental requirements for the transfer of Personal Data out of the European Economic Area

The following supplemental requirements shall apply to any Restricted Transfer:

1. Customer shall regularly make available to Cepheid information regarding public authority requests for access to Personal Data and the manner of reply provided (if permitted by law);

2. Customer warrants that it has not purposefully created technical back doors or internal processes to facilitate direct access by public authorities to Personal Data, and is not required under applicable law or practice to create or maintain back doors;

3. Customer shall inquire of any public authority making an access request regarding Personal Data whether it is cooperating with any other state authorities in relation to the matter;

4. Customer shall provide reasonable assistance to data subjects in exercising their rights to Personal Data in the receiving jurisdiction;

5. Customer shall cooperate with Cepheid in the event that a relevant supervisory authority or court determines that a transfer of Personal Data must be subject to specific additional safeguards;

6. Customer shall implement encryption and/or other technical measures sufficient to reasonably protect against interception of Personal Data during transit, or other unauthorized access, by public authorities; and

7. Customer shall have appropriate policies and procedures in place, including training, so that requests for access to Personal Data from public authorities are routed to the appropriate function and properly handled.

4.2 Supplemental requirements for the transfer of Personal Data out of the Republic of South Africa

The following supplemental requirements shall apply to transfer of Personal Data out of the Republic of South Africa:

1. Transfer of personal data outside of South Africa shall meet the following parameters:
   (A) the Party who is the recipient of the information is subject to a law, binding corporate rules or binding agreement which provide an adequate level of protection that:
      1. effectively upholds principles for reasonable processing of the information that are substantially similar to the conditions for the lawful processing of personal information relating to a data subject who is a natural person and, where applicable, a juristic person; and
      2. includes provisions, relating to the further transfer of personal information from the recipient to third parties who are in a foreign country;
   (B) the data subject consents to the transfer;
   (C) the transfer is necessary for the performance of a contract between the data subject and the responsible party, or for the implementation of pre-contractual measures taken in response to the data subject's request;

(D) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the responsible party and a third party; or

(E) the transfer is for the benefit of the data subject, and:

1. it is not reasonably practicable to obtain the consent of the data subject to that transfer; and
2. if it were reasonably practicable to obtain such consent, the data subject would be likely to give it.

2. For the purpose of this section:

(A) ‘‘binding corporate rules’’ means personal information processing policies, within a group of undertakings, which are adhered to by a responsible party or operator within that group of undertakings when transferring personal information to a responsible party or operator within that same group of undertakings in a foreign country; and

(B) ‘‘group of undertakings’’ means a controlling undertaking and its controlled undertakings.