DATA PROTECTION AGREEMENT
VENDOR

This Data protection Agreement ("DPA") is entered between Cepheid on behalf of itself and, to the extent required under applicable Data Protection Laws and Regulations in the name and on behalf of its authorized affiliates, if and to the extent that Vendor processes Personal Data for which such authorized affiliates qualify as the Controller, and Vendor (hereinafter referred to as the "Vendor"). Cepheid and Vendor are hereinafter individually referred to as a "Party" or collectively as the "Parties".

This Agreement is executed in respect of and made part of the business relationship between Cepheid and Vendor ("Agreement") to ensure minimum data protection and cybersecurity standards and related requirements, and is entered into and effective upon the commencement of any transfer of Personal Data.

The terms of the DPA apply when and to the extent they are required by Applicable Law (defined below).

NOW THEREFORE, for good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the Parties agree to the following:

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) "Cepheid" means Cepheid and each subsidiary of Cepheid for which Vendor provides or is engaged to provide Services.

   (C) "Covered Information" means, in any form, format or media, any (i) confidential information of Cepheid, and/or (ii) Personal Data, in each case together with any encryption key used to encrypt such information or data.

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

   (E) "Data Subject Request" means any request by a natural person to access, update, revise, correct, object to Processing or delete Personal Data or any similar request, whether or not made pursuant to Applicable Law.

   (F) "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.

(G) “Personal Data” means all data or information obtained by Vendor from or on behalf of Cepheid, in any form or format, that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, to an identified or identifiable natural person. For clarity, Personal Data also means Personal Information.

(H) “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.

(I) “Process” (including “Processing” or “Processed”) means any operation or set of operations that is performed upon any Covered Information, whether or not by automatic means, including, but not limited to, collection, recording, organization, storage, access, adaptation, alteration, retrieval, consultation, use, disclosure, dissemination, making available, alignment, combination, blocking, deletion, erasure, or destruction.

(J) " 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.

(K) “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 parties in relation to such information.

(L) “Subprocessor” means any entity or person that Processes Personal Data on behalf of Vendor.

(M) “System” means any system, network, platform, database, computer, or telecommunications or other information system owned, controlled or operated by or on behalf of either Party or any of its Affiliates for the purpose of Processing Covered Information.

Any terms and expressions that are used in this DPA and not defined beforehand have the meaning ascribed to them by the Applicable Law.

2. General Requirements. If Vendor Processes Covered Information on behalf of Cepheid, Vendor shall:

(A) Process Covered Information solely as necessary to provide the Services to Cepheid, and in accordance with Applicable Law and the written instructions of Cepheid. Vendor is specifically prohibited from selling Covered Information and from retaining, using, or disclosing Personal Data for a commercial purpose other than providing the Services or in any manner outside of the direct business relationship between Vendor and Cepheid;

(B) Maintain the confidentiality of all Covered Information;

(C) Be responsible for the compliance of its personnel with the terms of this DPA;

(D) Not disclose Covered Information to third parties (including Subprocessors):

(1) without the prior written approval of Cepheid, and provided further that Vendor remains fully liable to Cepheid 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 Vendor under this DPA; or

(2) unless required by Applicable Law, in which case Vendor shall wherever possible: (a) notify Cepheid promptly in writing before complying with any disclosure requirement, (b) comply with all reasonable directions of Cepheid with respect to such disclosure, and (c) promptly inform Cepheid of any Covered Information so disclosed;

(E) Promptly notify Cepheid of:

(1) any request, inquiry, complaint, notice or communication received from any third party, including a data subject or a supervisory authority, with respect to any Covered Information and comply with instructions of Cepheid in responding to such request, inquiry, complaint, notice or communication. Without limiting the generality of the foregoing, Vendor shall notify Cepheid in writing within five (5) business days of receipt of any Data Subject Request relating to Personal Data Processed by Vendor pursuant to this DPA and shall provide Cepheid its reasonable assistance in responding to any such Data Subject Request (whether or not received directly by Vendor);

(2) any instruction by Cepheid that Vendor believes to be in violation of Applicable Law; and

(3) any substantial changes to the Vendor's notices, policies or procedures that would impede Vendor's ability to fulfil the terms of this DPA regarding protection of Personal Data;

(F) Upon Cepheid's reasonable request, submit the facilities it uses to Process Covered Information and/or Personal Data for audit which shall be carried out by Cepheid representatives or an auditing body agreed to by both Parties;

(G) Keep records that demonstrate its compliance with its obligations under this DPA and make them available to Cepheid in connection with any audit referred to in (F) above;

(H) Reasonably assist and cooperate with Cepheid, including by providing information requested by Cepheid, to allow Cepheid to comply with its obligations under Applicable Law;

(I) Retain Covered Information only for as long as necessary to perform the Services, and at the end of the provision of the Services, at Cepheid's choice, delete or return the Covered Information to Cepheid as specified in Annex 1 below, unless expressly required otherwise by Applicable Law. Without limitation to the generality of the foregoing and the duration defined in Annex 1 below, Vendor shall, within five (5) business days of an applicable request from Cepheid, delete or destroy all copies of Personal Data as directed by Cepheid, and provide a copy of such data in a portable and readily useable format as directed by Cepheid; and

(J) If Vendor suspects or becomes aware of a Data Security Incident:

(1) provide Cepheid written notice without undue delay and no later than twenty-four (24) hours after becoming aware of such suspected or confirmed Data Security Incident;

(2) undertake an investigation of such Data Security Incident and reasonably cooperate with Cepheid, its regulators and law enforcement agencies;

(3) not make any public announcements relating to such Data Security Incident without Cepheid's prior written approval, which shall not be unreasonably withheld; and

(4) take all reasonable corrective action in a timely manner, at the expense of Vendor, to remediate and prevent a recurrence of such Data Security Incident.

3. Cyber and Information Security. Vendor represents and warrants that it shall establish, maintain and comply with:

(A) Administrative, technical, and physical safeguards designed to ensure the security, confidentiality, reliability and integrity of Covered Information, as well as any Systems, facilities, or software that Vendor accesses or supports. Such safeguards should:

(1) be commensurate with the type and amount of Covered Information Processed by Vendor, having regard to the state of the art and industry standards, and should, at a minimum, protect Covered Information and Systems against reasonably anticipated threats or hazards, including from unauthorized access, loss, theft, destruction, use, modification, collection, attack, or disclosure;

(2) address the security controls set forth in the ISO 27000 series and in the Center for Internet Security's Critical Security Controls, formerly known as the SANS Top 20; and

(3) comply with the Payment Card Industry Data Security Standards if Vendor Processes cardholder or other financial account data;

(B) A written security program and policy that meets or exceeds the requirements imposed under Applicable Law and aligns with established industry practices. Such security program and policy should address, at a minimum, the following:

(1) identification of appropriately defined organizational roles related to information security;

(2) controls with respect to the employment of and access given to Covered Information by employees, agents and subcontractors of Vendor including background checks, security clearances that assign specific access privileges to individuals, and training regarding the handling of Covered Information;

(3) an appropriate network security program that includes, without limitation, encryption and network and application partitioning;

(4) access identification and authentication;

(5) maintenance and media disposal;

(6) audit and accountability;

(7) physical and environmental protection;

(8) system and communication security;

(9) incident response and planning; and

(10) the integrity and reliability of facilities, systems and services, including critical asset identification, configuration and change management for software systems, and contingency planning/redundancy.

4. Third-Party Rights. The Parties to this DPA expressly confirm and acknowledge that, where Vendor performs Services for or on behalf of Cepheid, Cepheid shall have the non-exclusive benefit of the rights arising under this DPA. Accordingly, Cepheid may take any action to enforce rights and obligations arising from this DPA.

5. International Transfers.

(A) The parties agree that when the transfer of Personal Data from Cepheid to Vendor is a Restricted Transfer it shall be subject to the appropriate Standard Contractual Clauses as set out in Annex 3.

(B) Vendor shall not participate in (nor permit any Subprocessor to participate in) any other Restricted Transfers of Personal Data (whether as an exporter or an importer of the Personal Data) unless: (i) it has first obtained Cepheid's

prior written consent which, where Cepheid is a processor on behalf of a third party controller, shall reflect the controller's instructions; and (ii) 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.

6. Miscellaneous. If applicable, the Standard Contractual Clauses, including Annexes 1-5, 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 of the DPA
Data Processing Description

List of Parties

Controller:

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

Processor:

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

Description of the transfer

Subject Matter of the Processing
The Personal Data is Processed for the following purposes:
The data will be used as needed to render the Services and any additional written instructions of Cepheid.

Duration of the Processing
The Personal Data will be Processed until:
The completion of the Services, unless otherwise agreed upon in writing. At the end of Processing, Vendor will carry out one of the following:

- Return Personal Data to Cepheid
- De-Identify/Anonymize Personal Data
- Purge/Destroy Personal Data

Frequency of transfer

The Personal Data will be Processed on a either a one-off or continuous basis.

Nature of the processing:
Processing operations
The Personal Data will be subject to the following basic Processing activities:

As necessary to perform the Services and as further instructed by Cepheid, including record, storage, consultation, use, disclosure by transmission, combination, restriction, erasure or destruction, anonymization, analysis, reports.

Categories of data subjects
The Personal Data to be Processed can include any of the following categories of data subjects:
Employees or contact persons of either Party, independent contractors, customers, patients, other third parties

Categories of personal data
The Personal Data to be Processed can include any of the following categories of data:
Contact details, employment information, personal identification, healthcare data, patient details and demographics, patient disposition

Special Categories of Data (if applicable)
The Personal Data to be Processed can include the following Special Categories of Data:
Biometric information, social security number, health information

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 established 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 of the DPA
Technical and Organizational Security Measures

The Processor guarantees that it has implemented and will continue to implement under the term of this DPA appropriate technical and organizational measures in such a manner that its Processing of Personal Data under this DPA will meet the requirements of Applicable Data Protection Law and ensure the protection of the rights of the Data Subject.

Description of the minimum technical and organizational security measures required to be implemented by Vendor:

- Established standards that all users must agree to that dictate what computers may and may not be used for
- Performance of risk assessments for new companies onboarded that interact with Cepheid data, and for when major changes are made
- Control of what software users are able to install and use and have a process for approving new software
- Performance of several versions of yearly security training, security newsletters, and monthly phishing tests
- Established and tested processes for identifying and responding to security events
- Established and tested processes for performing back-ups and recovery of data and systems
- Rules for provisioning, deprovisioning, and changing access for users
- Password requirement to be 12 characters, complex, and changed every 90 days
- Standards for how cloud services are purchased and configured
- Standard for how computers and systems are tracked in a single place
- Performance of change management meetings to review prior to making changes
- Standards for how network devices are configured, connected, and maintained
- Minimum security baselines for all system types defined
    - Laptops/Desktops require Malware protection software, network access software, and USB protection
- Standards for sending event logs to a central tracking system (SIEM)
- A process for identifying and remediating security vulnerabilities and patches on a regular basis

Annex 3 of the DPA
UK / EU and Swiss Transfer Provisions

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

   (a) Module Two "Controller to Processor" will apply to the extent that Cepheid is a controller of the Personal Data;

   (b) in Clause 7, the optional docking Clause will not apply;

   (c) in Clause 9, Option 1 will apply, and the time period for prior notice of sub-Processor changes shall be (15) days;

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

   (e) 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;

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

   (g) in Annex I:

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

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

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

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

   (i) Annex III: with Annex 5 to this DPA.

2. Where the UK Addendum are 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 the Parties shall cooperate in good faith to implement appropriate safeguards for transfers of such Data as required or permitted by the Applicable Law without undue delay.

Annex 4 of the DPA

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

5. Vendor 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. Vendor 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. Vendor 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:

      (a) 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

      (b) 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:

(a) it is not reasonably practicable to obtain the consent of the data subject to that transfer; and

(b) 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.

Annex 5 of the DPA
List of subprocessors

The Vendor shall maintain documented processes for selecting, evaluating, qualifying and maintaining used sub-processors and third parties involved in provision of services to Cepheid. The Vendor will provide Cepheid with a list of current sub-processors and will inform Cepheid of any planned changes regarding the addition or replacement of sub-processors at least 15 days before the addition/replacement takes effect. Cepheid has the opportunity to object to such changes.