VITROLIFE GROUP™
EXCELLENCE IN REPRODUCTIVE HEALTH

Vitrolife

General Terms for the Vitrolife Group's Incubator System Services (EmbryoScope and CulturePro systems)

1. Scope

1.1 All maintenance and repair (the "**Services**") of EmbryoScope and CulturePro systems carried out by or on behalf of the contracting Vitrolife Group company ("**Vitrolife**") shall be subject to these General Terms (the "**General Terms**"). Opposing or deviating conditions to these General Terms are only applicable if explicitly accepted by Vitrolife in writing.

1.2 Vitrolife's obligation to provide the Services shall apply only to the instrument (the "**Instrument**") for which the customer ("**You**") has paid the periodic service fee (the "**Service Fee**"), and only for the period of time for which the Service Fee has been paid.

These Terms and Conditions supersede all prior representations, warranties, communications and agreements regarding the Incubator System Services between Vitrolife and You. Any conditions contrary to the content of these Terms and Conditions shall be excluded and of no force or effect. In the event of discrepancy between Vitrolife's order confirmation and these Terms and Conditions, the wording in the order confirmation shall take precedence. Vitrolife may at any time change these Terms and Conditions with effect for orders confirmed after such change.

2. Services

2.1 The Services shall consist of the following, subject always to Sections 2.2 and 3:

a. *on-site scheduled maintenance* consisting of regular preventive maintenance service calls, which will include calibration of the Instrument, replacement to the extent necessary of limited lifespan parts identical or equivalent to the parts being replaced, and supply of a filter package for replacement in the Instrument by Your own staff six months after last Vitrolife on-site visit. Replaced parts shall be the property of Vitrolife.

b. *repair of defects* in the Instrument including replacement of defective parts. The typical on-site response time will be maximum 72 hours in Europe and 96 hours outside of Europe (not including weekends or local holidays) from Vitrolife's determination of the root cause of the defect.

c. *24 hours service hotline* supplied by English speaking staff on an international telephone number.

d. *email support* in English. Response time 48 hours (not including weekends or local holidays).

e. software-updates to the basic functionality of the Vitrolife software (but not the third-party software, cf. Section 3.1 d.) originally supplied with the Instrument, where deemed necessary by Vitrolife. Software changes that introduce new functionalities to the original Vitrolife software shall not be part of the Services.

2.2 All Services for an Instrument shall be limited in time and shall cease automatically as follows:

a) For CulturePro and EmbryoScope incubators the Services shall cease ten years after the first installation date.

b) For EmbryoViewer workstations and VTH servers the Services shall cease five years after their first installation date, provided however, that the Services for these Instruments shall cease immediately if they are no longer connected to an EmbryoScope or CulturePro Instrument for which Services are provided under these General Terms.

2.3 Vitrolife is committed to service and maintain the Instrument in accordance with the market's needs and requirements. Consequently, Vitrolife may – without reducing the quality of the Services – amend the Services when deemed reasonably necessary by Vitrolife. You will receive notice of any such amendment.

2.4 If You want to require Services for an Instrument that has not been serviced and maintained by Vitrolife continuously since its first installation, this is subject to Vitrolife's acceptance which may be provided or declined at Vitrolife's discretion. Vitrolife's acceptance may be conditioned on an inspection of the Instrument at Your expense. Based on the inspection Vitrolife will inform You to what extent prior repair and maintenance is required in order for Vitrolife to accept the performance of future Services for that Instrument. If Vitrolife declines to provide Services under these General Terms, similar services may be offered by Vitrolife on a time and material basis.

3. Work not included in the Services

3.1 The following work is not included in the Services:

a. repair of damage, defects or malfunctioning in the Instrument or its parts caused by (i) accident, abuse, misuse, or misapplication of the Instrument or its parts by You or any third party; (ii) service or maintenance performed by anyone other than Vitrolife certified personnel, excluding however, Your own annual replacement of filters in accordance with Vitrolife's instructions; (iii) use in conjunction with equipment, parts, software or systems not manufactured by or not approved in writing by Vitrolife; (iv) use and operation that does not comply with instructions provided in the operating manual; (v) changes made to the software or the configuration originally supplied with the Instrument; (vi) installation of other software programs than those originally supplied with the Instrument; (vii) force majeure incidents including without limitation lightning, flooding, war, terrorism, riots (viii) the general conditions at the location where the Instrument is installed, such as the air quality, humidity or altitude; or (ix) other causes outside of the Instrument such as power failure, hacking, malware, cyber-attacks, or defects in equipment connected with the Instrument even if Vitrolife has approved such connection.

b. the loading or restoration of data lost. You are solely responsible for securing external back-up of all data stored in the Instrument.

c. service relating to or necessitated by relocation of the Instrument even if Vitrolife has accepted such relocation.

d. updates, upgrades, and modifications to third party software not developed by Vitrolife, including without limitation the operating systems and antivirus programs, whether such third-party software is supplied with the Instrument or installed later.

3.2 Vitrolife will invoice You for work not included in the Services based on Vitrolife's actual expenses, including without limitation work and travel expenses. Vitrolife will charge its regular hourly fee for the employees, consultants or agents who provide the work. If possible, Vitrolife will provide You with an estimate prior to the performance of work not included in the Services.

4. Preconditions for Service

4.1 In order to enable Vitrolife to perform the Services You shall:

a. at Vitrolife's reasonable request upload technical log-information from the Instrument to Vitrolife;
b. grant remote and on-site access to the Instrument as required by Vitrolife.
c. immediately inform Vitrolife of problems or potential problems with the Instrument;
d. allow Vitrolife to process data stored in the Instrument to the extent needed for remote and on-site evaluation, repair and maintenance of the Instrument, subject always to Section 9;
e. provide complete information with regard to the circumstances surrounding Instrument failure;
f. ensure that only persons fully trained in the operation of the Instrument use the Instrument; and
g. appoint an English-speaking member of Your staff trained in the operation of the Instrument as the contact person for Vitrolife;
h. refrain from attempting to repair or otherwise interfere with the Instrument except as expressly permitted in these General Terms.

4.2 Vitrolife reserves the right to carry out preventive maintenance on the same day on all Instruments installed in the same clinic.

5. Payment and Adjustment of Service Fee

5.1 The Service Fee covers all costs for the performance of the Services including labour costs, all limited lifespan and spare parts, and travel expenses.

5.2 Vitrolife will invoice You for the Service Fee for a certain time period in advance (the "**Invoice Period**"). Payment terms are 30 days net. If the Service Fee for an Invoice Period has not been received in full by Vitrolife by the due date, then Vitrolife is under no obligation to perform any Services for that Invoice Period and Vitrolife may terminate the Services in accordance with Section 10.3. Any resumption of the Services shall be subject to payment of the due Service Fee and to the procedure described in Section 2.4.

5.3 The Service Fee is automatically adjusted on December 31 each year. Adjustment takes place in accordance with the annual increase (but not decrease) from October to October in the Danish net price index (nettopris-indeks) calculated by Statistics Denmark or, at Vitrolife's choice, an equivalent net price index generated by a public central authority in the country of the contracting Vitrolife company. In addition to the automatic adjustment, Vitrolife is entitled to increase the Service Fee each year for reasons of its own on the giving of three months' written notice, provided however, that if You do not accept such increase then You shall be entitled to terminate the Services with immediate effect.

6. Warranty

6.1 Vitrolife will complete or rectify free of charge any Services that have been performed defectively. Defects in the spare parts used in connection with the Services will be rectified or the spare parts will be exchanged at Vitrolife's costs except where the defect is a result of the conditions mentioned in Section 3.

6.2 The above warranty shall apply for 90 days after the performance of the Services that were defective or resulted in a defect, provided however, that the warranty shall always expire when the Services cease according to Section 2.2

7.1 Limitation of Liability

7.1 Under no circumstances shall Vitrolife be liable for any loss of profit, loss of production or any indirect, special, incidental, or consequential losses whatsoever, including without limitation loss of data, loss of goodwill, loss of contracts, or any additional treatments that You may offer to Your patients as a result of a delay in performance of the Services or a defect or alleged defect in the Instrument or in the performance of the Services.

7.2 In no event can Vitrolife's total liability exceed an amount corresponding to the annual Service Fee paid by You.

8. Subcontractors

8.1 Vitrolife may engage subcontractors in the provision of the Services. Vitrolife shall be responsible for the acts and omissions of its subcontractors to the same extent as had the Services been provided by Vitrolife itself.

9. Vitrolife's processing of data

9.1 Vitrolife may process personal data stored in an Instrument (the "Personal Data") for the purpose of performing the Services.

Vitrolife's processing of the Personal Data may result from (i) access to Your Instrument through remote access tools (ii) copying of software including copying of Personal Data for off-line evaluation, repair, and maintenance of the software in the Instrument upon Your express consent in each case, and (iii) direct access to Your Instrument in connection with on-site visits.

Vitrolife's processing of personal data in connection with the performance of the Services is subject to the General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016) referred to as the "GDPR".

In the performance of the Services Vitrolife will be a data processor processing the Personal Data on behalf of You who are the data controller. Vitrolife's processing of Personal Data shall be governed by the terms of the data processing agreement set out in Annex I hereto. In case of discrepancies between these General Terms and the data processing agreement, the data processing agreement shall prevail with regard to the processing of Personal Data.

If You are located outside of the European Economic Area in a country for which the EU Commission has not issued an adequacy decision, not only Annex I but also Annex II, the EU Commission's Standard Contractual Clauses module 4 shall apply for any transfer of Personal Data from Vitrolife to You.

10. Term, Termination and Suspension

10.1 You may terminate the Services for any Instrument without cause on the giving of three (3) months' written notice till the last day of an Invoice Period. If You do not terminate the Services, Vitrolife will automatically invoice You for a new Invoice Period.

10.2 You may terminate the Services with immediate effect (a) in accordance with Section 5.3; or (b) in case of Vitrolife's substantial or repeated breach of its obligations under these General Terms provided that Vitrolife does not remedy such breach within two (2) weeks after having received a written notice from You requesting such remedy. If the termination under this Section 10.2 is effected during an Invoice Period, a proportionate amount of the Service Fee paid for that Invoice Period shall be repaid to You.

10.3 Vitrolife may suspend or terminate the Services with immediate effect in case of Your breach of these General Terms, including without limitation if You do not pay the Service Fee on time, cf. Section 5.2, or comply with the preconditions for Service, cf. section 4; provided however, that termination can only be effected after Vitrolife's prior written notice to You indicating that the Services will be terminated if You do not remedy the breach within a time period of minimum two (2) weeks.

10.4 If Vitrolife deems that the safety for its personnel cannot be guaranteed during on-site maintenance, Vitrolife may, at its own discretion, suspend the Services until the safety of its personnel can be guaranteed. Should the suspension last for more than three (3) months, Vitrolife may terminate the Services with immediate effect through written notice to You.

10.4 Unless terminated sooner, all Services for an Instrument shall automatically terminate in accordance with Section 2.2.

11. FORCE MAJEURE

Neither Party shall be responsible to the other for any failure or delay in performing any of its obligations under this Agreement or for other non-performance hereof, except payment of Services ordered, if such delay or non-performance is caused by strike, stoppage of labour, lockout or other labour trouble, fire, flood, riot, civil commotion, accident, act of any governmental or local authority, pandemics or terrorism or of the public enemy, or by any other cause beyond the reasonable control of that Party.

The Party that is prevented from performing its obligations due to force majeure shall immediately inform the other Party.

Should hindrance due to a force majeure situation continue for more than ninety (90) days, the other Party as its sole remedy shall have the right to terminate the Services with immediate effect.

12. Governing law and Jurisdiction

12.1 These General Terms shall be governed and constructed in accordance with the laws applicable at the contracting Vitrolife company's domicile. All disputes arising from or in connections with contracts to which these General Terms apply shall be finally settled in the courts having jurisdiction at the contracting Vitrolife company's domicile. Vitrolife may also bring proceedings before any competent court having jurisdiction over You.

Vitrolife Group
October 2024

Annex I – Data Processing Agreement as integral part of the GTC
Annex II – For international data transfers EU Commission's Standard Contractual Clauses module 4 (processor to controller)

ANNEX I: Data processing agreement between Vitrolife Group as data processor and the Customer as data controller located in the EU/EEA in connection with the performance of services relating to the customer's EmbryoScope™ and/or CulturePro™ system(s). The services are described in the annual maintenance contract between the customer and the contracting Vitrolife company and in the General Terms for the Vitrolife Group's Incubator System Services.

SECTION I

Clause 1 Purpose and scope

(a)The purpose of this Data Processing Agreement, based on the Standard Contractual Clauses[1] is to ensure compliance with **Article 28(3) and (4) of 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**.

(b)The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29 (3) and (4) Regulation (EU) 2018/1725.

(c)These Clauses apply to the processing of personal data as specified in Annex II.

(d)Annexes I to IV are an integral part of the Clauses.

(e)These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(f)These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

Clause 2 Invariability of the Clauses

(a)The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.

(b)This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

Clause 3 Interpretation

(a)Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, those terms shall have the same meaning as in that Regulation.

(b)These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively.

(c)These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation or in a way that prejudices the fundamental rights or freedoms of the data subjects.

Clause 4 Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties existing at the time when these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 5 - Docking clause

(a)Any entity that is not a Party to these Clauses may, with the agreement of all the Parties, accede to these Clauses at any time as a controller or a processor by completing the Annexes and signing Annex I.

(b)Once the Annexes in (a) are completed and signed, the acceding entity shall be treated as a Party to these Clauses and have the rights and obligations of a controller or a processor, in accordance with its designation in Annex I.

(c)The acceding entity shall have no rights or obligations resulting from these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 6 Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

Clause7 Obligations of the Parties

7.1. Instructions

(a)The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.

[1] Standard contractual clauses for controllers and processors in the EU/EEA (europa.eu)

(b)The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 or the applicable Union or Member State data protection provisions.

7.2. Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

7.3. Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in Annex II.

7.4. Security of processing

(a)The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

(b)The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.5. Sensitive data

- If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

7.6 Documentation and compliance

(a)The Parties shall be able to demonstrate compliance with these Clauses.

(b)The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.

(c)The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679. At the controller's request, the processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.

(d)The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.

(e)The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

7.7. Use of sub-processors

(a)**GENERAL WRITTEN AUTHORISATION: The processor has the controller's general authorisation for the engagement of sub-processors from the list in Annex IV.** The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least 15 days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.

(b)Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679.

(c)At the controller's request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.

(d)The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.

(e)The processor shall agree a third party beneficiary clause with the sub-processor whereby - in the event the processor has factually disappeared, ceased to exist in law or has become insolvent - the controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

7.8. International transfers

(a)Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under

Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679.

(b)The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

Clause 8 Assistance to the controller

(a)The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.

(b)The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions

(c)In addition to the processor's obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:

(1)the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

(2)the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;

(3)the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

(4)the obligations in Article 32 Regulation (EU) 2016/679.

(d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

Clause 9 Notification of personal data breach

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 Regulation (EU) 2016/679, where applicable, taking into account the nature of processing and the information available to the processor.

9.1 Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

(a)in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

(b)in obtaining the following information which, pursuant to Article 33(3) Regulation (EU) 2016/679, shall be stated in the controller's notification, and must at least include:

(1) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(2) the likely consequences of the personal data breach;

(3) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(c)in complying, pursuant to Article 34 Regulation (EU) 2016/679 , with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2 Data breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

(a)a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

(b)the details of a contact point where more information concerning the personal data breach can be obtained;

(c)its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.
The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

SECTION III – FINAL PROVISIONS

Clause 10 Non-compliance with the Clauses and termination

(a)Without prejudice to any provisions of Regulation (EU) 2016/679, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.

(b)The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:(1)the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;

(2)the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679;

(3)the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679.

(c)The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.d)Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

ANNEX I

List of parties

Controller(s):

Name: The Vitrolife Group Customer that concluded the annual maintenance contract with a Vitrolife company

Address: The address of the Vitrolife Customer stated in the annual maintenance contract

Signature and accession date: No signature is needed for these Clauses. They are an integral part of the General Terms for the Vitrolife Group's Incubator System Services.
As such the conclusion of the General Terms for the Vitrolife Group's Incubator System Services shall constitute the conclusion of these Clauses as well.

Processor(s)

1. Name: The Vitrolife Group company that is the contracting party to the annual maintenance contract with the Customer

Address: The address of the contracting Vitrolife company as stated in the annual maintenance contract.

Contact person: Data Protection Coordinator, dataprotection@vitrolife.com

Signature and accession date: No signature is needed for these Clauses. They are an integral part of the General Terms for the Vitrolife Group's Incubator System Services. As such, the conclusion of the General Terms for the Vitrolife Group's Incubator System Services shall constitute the conclusion of these Clauses as well.

ANNEX II
Description of the processing[2]

1. Categories of data subjects whose personal data is processed

- Incubator system users
- Controller's/processor's patients

2. Categories of personal data processed

a. Personal data regarding Incubator system users:

- Name
- Email address
- Phone number and country code
- IP address
- Initials
- Organization name

b. Personal data registered by the controller about patients in the incubator systems, including sensitive data:

- Name
- Email address
- Phone number and country code
- Date of birth
- Gender
- Address
- Medical/healthcare data such as physiological variables and laboratory results. A high-security level has been established as default.

3. Nature of the processing

Access to the personal data is obtained by the processor in connection with repair and maintenance of incubator systems' software and hardware. As per controller's instructions, processor may move, copy or transfer personal data stored in the incubator system.

4. Purpose(s) for which the personal data is processed on behalf of the controller/processor

Repair and maintenance of Incubator systems remotely and onsite. Trouble-shooting through Vitrolife A/S helpdesk.

5. Duration of the processing

The processing shall continue for the duration of the parties' agreement regarding the processor's services which include processing of personal data. Processing is not continuous, but takes place on an ad hoc basis according to the controller's requirements and the maintenance schedule for the incubator system. Processor can only access the personal data with controller's prior granting of access. After finalization of each repair or maintenance activity all access to the personal data is terminated and processor can only access the data again through a new granting of access by the controller. Normally, a repair or maintenance activity lasts less than a full workday.

[2] If there is a change in the processing activity or the controller gives other instructions to teh processor the Parties shall record it in writing

ANNEX III
Technical and organisational measures to ensure the security of the data

Confidentiality, integrity, availability and resilience of processing systems and services

1. *Employees or other individuals working within Vitrolife Group are bound by confidentiality agreements*
2. *Employees accessing customer data are under strict confidential obligations and instructed to process data only for the purpose described by the customer*
3. *There are procedures in place ensuring that people that have access to personal data have individual access account*
4. *Least access policy is implemented and followed*
5. *Access to personal data is logged for traceability*
6. *Personal data stored is automatically backup on a regular basis*
7. *Procedures, policies and plans in place to ensure ongoing integrity and availability, e.g. a business continuity and disaster recovery plan*
8. *Backup scheme to maintain backups of company resources.*
    a. *Daily mainframe backup with a retention time for 30 days.*
    b. *Quarterly mainframe backup with retention for three quarters.*
    c. *Yearly mainframe backup with retention for 2 years.*
9. *Backups are protected by either being physically secured or encrypted by AES 256-bit encryption*
10. *Monitor system monitoring unauthorized access (or attempt to access) to Vitrolife Group devices, systems, e.g. a firewall*
11. *Customer data related to closed cases (Helpdesk) no longer needed is deleted from all storages*

Data security

12. *End-point traffic and behavior through end-point protection alerts*
13. *Advanced threat protection and monitoring of devices (hardware and software)*
14. *Network traffic through firewalls*
15. *Automated critical patch and updates of defined critical applications*
16. *Detection of deviant behavior and pattern on endpoints*
17. *Detect anomalies with continuous scanning and alerting on managed device, service and applications and user behavior*
18. *Coverage of newly discovered vulnerabilities*
19. *SOC service implemented for monitoring and detection 24/7/365*

User identification, authorization and access security

20. *Personal data can only be accessed by identified and authorized individuals*
21. *Only selected, trained and authorized individuals is granted access to data, backup and infrastructure.*
22. *Access is granted only for the purpose described in the agreement with the customer*
23. *Access is only granted after approval from immediate manager and/or overall responsible*
24. *Password policy ensuring that only identified and authorized individuals have access to the personal data*
25. *All data and devices shall be protected by a strong password, multifactor authentication (MFA) or other security settings*
26. *Removal of users access to data when no longer needed*
27. *Data access and user rights are review and audited on a regular basis*
28. *Restricted access to local computer*
29. *Controlled use of privileged utility programs*
30. *Limitation for software requiring administrative privileges. Temporary administrative access may be given upon request*
31. *Encryption on local hard drives*

Protection of data during transmission and storage

32. *End-point protection on computers, laptops, and servers such as antivirus/antimalware, firewalls with strict firewall rules, hardware encryption*
33. *AES 256-bit encryption is used during transmitting and storage*
34. *Servers storing personal data stored electronically are located at logically and physically protected premises*
35. *Stored personal data is only accessed by identified and authorized individuals and the access should be logged Access shall require a password, MFA (or a key card if the data is stored physically in cabinets)*
36. *Transmission of customer data via TeamViewer, or customer defined access method*
37. *Investigation data that may contain PatientID is anonymized and deleted after investigation is closed*
38. *The system's log files are created when the system is in use and does not contain patient data. The log files are only "Warnings-Info-Errors"*
39. *The log files are stored in Sharepoint during trouble shooting*
40. *Data transferred to Sharepoint are protected with access control and only for investigation purposes. Any transfer of personal data requires the customer's approval prior to the transfer.*

Physical security of locations at which personal data are processed

41. *Only identified and authorized individuals have access to the premises where the personal data is processed and/or stored*
42. *Offices, cabinets, laptops etc. containing personal data must be secured, e.g. by a lock or access code. The personal data must be locked away after working hours*
43. *Server room(s) including equipment, cables, etc. are secured with sufficient physical measures*

Detection of threats, vulnerability, and incident management

44. *Identification of devices connected to the network*
45. *Risk assessment agents: to identify vulnerabilities on device application or service*
46. *Continuously vulnerability scanning: of device, application and services*
47. *IT Governance framework to enforce security standards for suppliers, contractors and other no employees. (e.g. NDA, Data Protection Agreements)*

48. *Defined personal data breach and data incident response procedure*
49. *Post-incident analysis leads to continuous improvement of framework and procedures.*

Organization

50. *Processes, procedures, and technical measures defined, implemented, and evaluated to ensure personal data is processed per applicable laws and regulations following always the principles relating to the processing of personal data as stated in Art. 5 GDPR as a minimum standard.*
51. *All employees must be trained in the content of policies and procedures related to information security and data protection (including follow up training on a regular basis)*
52. *Centralized IT-department with full responsibility for networks, group common applications and all IT equipment owned by or connected to the group's IT environment*
53. *The Vitrolife Group IT manager approval of all application, Services, and equipment implementation and connection with IT-environment*
54. *IT Security is managed, approved and set by the Vitrolife Group IT department.*
55. *Incident response plan: regularly tested to effectively respond to and mitigate any data breaches or security incidents*
56. *Designated data protection officer and information security manager*
57. *Cyber liability insurance coverage at a reputable insurance company*
58. *Continuous security awareness training for all employees covering information security and data protection (privacy awareness)*

Policies

59. *There is a documented strong complex password policy available for users*
60. *There are policies implemented, but not limited to, for data privacy, information security, incident management and data breach response plan*

Remote working

61. *Devices, software etc. used for remote working is secured in the same way and applicable to the same measures as for processing taking place at the Vitrolife Groups premises*

Business continuity and disaster recovery plan

62. *Processor shall have in place a business continuity and disaster recovery plan including a timetable*
63. *Processor shall have in place an action plan and communication procedure in case of a data breach and/or an incident affecting the business continuity*

ANNEX IV: LIST OF SUB-PROCESSORS

The controller has authorised the processor's engagement of sub-processors from the following list of sub-processors:

Name of the sub-processor	Contact information	Purpose
Any company within the Vitrolife Group of companies	**http://www.vitrolifegroup.com/**	To provide support service

ANNEX II. STANDARD CONTRACTUAL CLAUSES FOR INTERNATIONAL TRANSFERS WHEN THE CUSTOMER IS OUTSIDE OF EU/EEA[3]

SECTION I

Clause 1 Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer")

have agreed to these standard contractual clauses (hereinafter: "Clauses").

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

[3] Please note that this agreement does not replace the Data Processing Agreement between the controller and the processor, but secures the international transfer

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2 Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3 Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 - Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 13;

(iv) Clause 15.1(c), (d) and (e);

(v) Clause 16(e);

(vi) Clause 18 - Module Four: Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4 Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5 Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6 Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8 Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data exporter shall process the personal data only on documented instructions from the data importer acting as its controller.

(b) The data exporter shall immediately inform the data importer if it is unable to follow those instructions, including if such instructions infringe Regulation (EU) 2016/679 or other Union or Member State data protection law.

(c) The data importer shall refrain from any action that would prevent the data exporter from fulfilling its obligations under Regulation (EU) 2016/679, including in the context of sub-processing or as regards cooperation with competent supervisory authorities.

(d) After the end of the provision of the processing services, the data exporter shall, at the choice of the data importer, delete all personal data processed on behalf of the data importer and certify to the data importer that it has done so, or return to the data importer all personal data processed on its behalf and delete existing copies.

8.2 Security of processing

(a) The Parties shall implement appropriate technical and organisational measures to ensure the security of the data, including during transmission, and protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter "personal data breach"). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature of the personal

data[4], the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects, and in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

(b) The data exporter shall assist the data importer in ensuring appropriate security of the data in accordance with paragraph (a). In case of a personal data breach concerning the personal data processed by the data exporter under these Clauses, the data exporter shall notify the data importer without undue delay after becoming aware of it and assist the data importer in addressing the breach.

(c) The data exporter shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

8.3 Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The data exporter shall make available to the data importer all information necessary to demonstrate compliance with its obligations under these Clauses and allow for and contribute to audits.

Clause 9 - Intentionally left blank

Clause 10 Data subject rights

The Parties shall assist each other in responding to enquiries and requests made by data subjects under the local law applicable to the data importer or, for data processing by the data exporter in the EU, under Regulation (EU) 2016/679.

Clause 11 Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

Clause 12 Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

(c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

Clause 13 Supervision- Intentionally left blank

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14 Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[5];

(iii) any relevant contractual, technical or organisational safeguards put in place to

[4] This includes whether the transfer and further processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences.

[5] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements

supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

~~(e)~~ The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply. ***Clause 15 Obligations of the data importer in case of access by public authorities***

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to

---

together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16 Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) **Personal data collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof.** The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17 Governing law

These Clauses shall be governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of the contracting Vitrolife Group entity of the annual service and maintenance contract.

Clause 18 Choice of forum and jurisdiction

Any dispute arising from these Clauses shall be resolved by the courts of the contracting Vitrolife Group entity of the annual service and maintenance contract.

APPENDIX ANNEX I

A. LIST OF PARTIES

Data exporter(s): The Vitrolife Group company that is the contracting party to the annual maintenance contract with the Customer

Contact person's name, position and contact details:
Data protection officer dataprotection@vitrolife.com
Role (controller/processor): Processor

Activities relevant to the data transferred under these Transfer Clauses: Service and maintenance

Signature and accession date: These Clauses are an integral part of Vitrolife's General Terms and Conditions. As such, the parties agree that their conclusion of the General Terms and Conditions agreement shall constitute the conclusion of these Transfer Clauses as well.

Data importer(s): The Customer of Vitrolife Groupe's services relating to the customer's EmbryoScope™ and/or CulturePro™ system(s) outside EU/EEA

Contact person's name, position and contact details: the controller is responsible for providing the Processor with information on the controller's contact person

Role (controller/processor): Controller
Activities relevant to the data transferred under these Transfer Clauses: Service and maintenance

Signature and accession date: These Clauses are an integral part of Vitrolife's General Terms and Conditions. As such, the parties agree that their conclusion of the General Terms and Conditions agreement shall constitute the conclusion of these Transfer Clauses as well.

B. DESCRIPTION OF TRANSFER

Unless otherwise stated in this section B the information from the parties' Data Processing Agreement concluded simultaneously herewith shall apply.

Data is transferred continuously for as long as the Customer is buying services from Vitrolife Group.

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Unless otherwise stated in this Annex II the information from the parties' Data Processing Agreement concluded simultaneously herewith shall apply