15 July 2024 Version 3

GENERAL TERMS AND CONDITIONS (GTC) – Vitrolife Genomics Software and Service

1 GENERAL PROVISIONS

Customer's right to use the Software, as defined below, together with any updates and permitted copies is strictly subject to the terms and conditions set out below.

By installing, copying, or otherwise using the Software, you agree to be bound by these GTC. If you do not agree to the terms of these GTC, do not install or use the Software.

The Software and the Services, as defined below, are provided to you by Vitrolife Sweden AB, Gustaf Werners gata 2, 400 92, Gothenburg, Sweden, Swedish company registration number 556546-6298, in these GTC referred to as "Vitrolife".

2 DEFINITIONS

In these GTC the terms set forth below shall have the following meanings:

"**Confidential Information**" means such information as referred to in section 10.

"**Consumables**" means the EmbryoMap and/or the KaryoMap reagent kit with which the Software must be used.

"**Customer Data"** means all data (including personal data) provided by, or on behalf of the Customer and/or the Users of the Service.

"Data Processing Agreement" means the data processing agreement in Appendix 1 below.

"Data Protection Laws" means all applicable laws and regulations that govern the processing of personal data, including, but not limited to the EU General Data Protection Regulation ((EU) 2016/679) and any national data protection laws and regulations implementing the EU Electronic Communications Privacy Directive (2002/58/EC), as well as any amendments to or replacements of such laws and regulations.

"Device" means the sequencing machine from Illumina Inc. and/or a computer with which the Software operates.

"eMap Software" and "kMap Software" means the software, developed by Vitrolife and/or to which Vitrolife has licensed rights, that enables the genetic analysis of samples operating with the Device.

"Uploader Software" means the software, developed by Vitrolife or to which Vitrolife has licensed rights, that enables the Customer's use of the Service.

"Force Majeure Event" means any occurrence beyond the parties' will and control and shall include, without limitation, natural disasters, governmental acts, decisions of authorities, war and other military conflicts, mobilisation, riots, terror attacks, seizure, embargos, labor conflicts, epidemics, pandemics or other occurrences which are unforeseeable, material and not negligently caused by any of the parties. In order to be relieved from liability, the relevant party must undertake all necessary and reasonable actions within its control in order to limit the extent of the damages and consequences of a force majeure event. The party affected by the force majeure event shall also immediately inform the other party in Writing of the beginning and the end of such occurrence and resume its performance as soon as reasonably possible.

"Intellectual Property Rights" means any and all intellectual and industrial property rights, including but not limited to patents, inventions (whether patentable or not), trademarks and design rights (registered and unregistered), utility models, copyright and related rights, know-how including trade secrets and any similar rights, whether registered or not, as well as rights of enforcement in relation to any of the foregoing.

“**Installation Services**” means installation of the Uploader Software or other software on the Device.

“**in Writing**” means messages sent by email or post.

“**Party**” means the Customer or Vitrolife, individually.

“**Parties**” means the Customer and Vitrolife jointly.

“Service” means the software-as-a-service that enables the genetic analysis of samples by using the Software, operating with the Device including the licensed rights under section 3 to use the Uploader Software with the Device.

“**Software**” means the eMap Software, the kMap Software and the Uploader Software as well as any other software, library, utility, tool or other computer or program code in object code form only provided by Vitrolife to the Customer.

“Third Party Supplier Software License Terms” means the third-party license terms in Appendix 2 .

“Term” means the period commencing on the date of the installation of the Uploader Software on the Customer’s Device and ending in accordance with section 11 of these GTC.

“Users” means the employees of the Customer that are appointed by the Customer as authorised users of the Service in line with the procedure instructed by Vitrolife.

3 LICENSE GRANT

3.1 In order to enable the Customer’s use of the Service the Customer is required to install a copy of the Uploader Software on the Device.

3.2 For the above purpose Vitrolife grants to Customer a non-exclusive, non-transferable and non-sublicensable license to install, execute, store, transmit and display one copy of the Uploader Software locally on one or more Devices and allow for its Users to use the Uploader Software solely with the Devices during the Term.

3.3 Vitrolife, or a third party assigned by Vitrolife, will provide the Installation Services to the Customer.

3.4 The Software includes open-source software and/or third party supplier software. The terms for such software is found in the Third Party Supplier Software License Terms which form an integral part of the GTC.

4 PROVISION OF SERVICE

4.1 Vitrolife hereby grants to the Customer a worldwide, non-exclusive, non-transferable right to access and use the Service, in accordance with these GTC during the Term.

4.2 The Customer acknowledges that the Software is provided as a service and that Vitrolife will not be delivering copies of the same to the Customer as part of the Service.

Vitrolife may change, update and make available new functionalities to the Service from time to time. Vitrolife will make available notifications about material changes in functionality.

4.3 Vitrolife shall use reasonable endeavours to maintain the availability of the Service to the Customer but does not guarantee 100% availability.

4.4 Vitrolife may from time to time suspend the Service for the purpose of maintenance. Vitrolife shall, to the extent possible, ensure that maintenance is carried out outside normal business hours.

4.5 For the avoidance of doubt, downtime caused directly or indirectly by any of the following shall not be considered a breach by Vitrolife:

(a) a Force Majeure Event;

(b) a fault or failure of the internet or any public telecommunications network;

(c) a fault or failure of the Customer's computer systems, networks or Device;

(d) any breach by the Customer of these GTC including the appendices hereto; or

(e) maintenance.

4.6 Vitrolife may suspend Customer´s or Users' access to parts of or all the Service with immediate effect if:

(a) the Customer or the Users do not comply with these GTC, or

(b) Customer´s or Users' use of the Service (i) pose a security risk to the Service, Vitrolife or any third party, or (ii) could adversely impact Vitrolife's systems, the Service or the systems or content of any third party (including Vitrolife's other customers).

4.7 If the access to the Service is suspended Vitrolife may at its sole discretion choose to terminate the Customer's access to and use of the Service in line with section 11.3 or, if the cause for the suspension is remedied by the Customer, give the Customer or Users access again to the Service.

5 CUSTOMER OBLIGATIONS

5.1 The Customer shall provide Vitrolife with all information reasonably requested to provide the Service and provide access to the Service to the Customer's Users.

5.2 The Customer shall comply with and always use the Service in accordance with relevant laws and regulations and any instructions provided by Vitrolife.

5.3 The Customer shall inform Users about the scope and limitations of the Customer's and Users' usage rights, and the Customer is responsible for all acts and use of the Service by Users as for its own acts and use.

5.4 The Customer is responsible for keeping all passwords and account details relating to the Service confidential and shall ensure that no person other than the Customer and its Users gets access to and can use the Service. If the Customer suspects any unauthorised access to or use of the Service, the Customer shall immediately notify Vitrolife thereof.

5.5 The Customer shall at all times maintain the security of its IT environment, such as the operating environment, network, applications, text, pictures or other data used in connection with the Service, and ensure that the Customer Data is secure and free from viruses etc. For the avoidance of doubt, Vitrolife is not liable for the Customer's hardware or software, including files or data uploaded or used in connection with the Service, or for any unauthorised use of User accounts or otherwise of the Service.

5.6 The Service may not be used:

(a) for any unlawful or other purpose for which it is not intended, including transmitting, uploading or posting any computer viruses or harmful files, codes or programs by use of the Service;

(b) in any way so that the Service is interrupted, damaged, rendered less efficient or the functionality of the Service in any way impaired, or that may be damaging or disruptive to Vitrolife's other customers, or their use of the Service, or to computers or other equipment; or

(c) in any other way that could reasonably be expected to affect Vitrolife or the Service adversely or reflect negatively on the goodwill, name or reputation of Vitrolife or the Service.

5.7 The right to access and use the Service granted to the Customer under section 4.1 is subject to the following conditions and limitations:

(a) the Customer may only use the Service in connection with the Device;

(b) the Customer may only use the Service together with the Consumables;

(c) the Customer may not overuse the Service and in general only one analysis per sample is allowed except for additional analysis caused by a faulty analysis;

(d) the Customer may not republish or redistribute any content or material from the Service, except for Customer Data or any results/reports including Customer Data generated through the use of the Service;

(e) the Customer may not copy, modify, develop, translate or in any other way amend the Service or permit any third party to do so, or reverse-engineer, decompile or disassemble the Service or by any other means recreate the Service's source code, create derivative works of the except for what is permitted under mandatory law;

(f) the Customer may not use the Service in any way that is unlawful, illegal, fraudulent or harmful or in connection with any such purpose or activity.

6 DATA PROTECTION

6.1 In connection with the supply of the Services, Vitrolife will process personal data on behalf of the Customer. Vitrolife will be the data processor and the Customer will be the data controller in respect of such processing of personal data. The rights and obligations of Vitrolife and Customer in regard to the processing of personal data is regulated in the Data Processing Agreement.

7 CUSTOMER DATA AND INTELLECTUAL PROPERTY RIGHTS

7.1 The Customer retains all rights, title and interest, including any Intellectual Property Rights, in the Customer Data. The Customer (for itself and all of its Users) grants Vitrolife a worldwide, non-exclusive, limited term license to copy, reproduce, store, distribute, publish, export, adapt, edit and translate Customer Data to the extent required for the performance of Vitrolife's obligations and the exercise of Vitrolife's rights under the GTC. The Customer also grants Vitrolife the right to sub-license these rights to its hosting, connectivity, telecommunication and other service providers.

7.2 The Customer is responsible for:

(a) development, content, operation, maintenance, and use of the Customer Data;

(b) ensuring that the Customer Data and Customer´s, Users' and Vitrolife's use of the Customer Data will not infringe the Intellectual Property Rights of any third party or violate any applicable laws; and

(c) taking appropriate action to secure, protect and backup Customer´s and Users' accounts and the Customer Data in a manner that will provide appropriate security and protection, which might include use of encryption to protect the Customer Data from unauthorised access and routinely archiving the Customer Data.

7.3 Vitrolife, or any third party from whom Vitrolife derives its right, owns and shall retain all rights, title and interest, including any Intellectual Property Rights, in and to the Software and the Service.

7.4 Nothing in these GTC shall be deemed as an assignment or transfer of any Intellectual Property Rights from Vitrolife to the Customer or from the Customers to Vitrolife.

8 WARRANTIES AND WARRANTY LIMITATIONS

8.1 Except for the explicit warranties below Vitrolife provides the Service on an "as is" basis without warranty of any kind, either expressed or implied, including, without limitation, warranties that the Software and/or the Uploader Software is free from defects, merchantable, fit for a particular purpose or non-infringing.

8.2 If Vitrolife reasonably determines, or any third party alleges, that the use of the Service by the Customer infringes any third party's Intellectual Property Rights, Vitrolife may at its own cost and expense:

(a) modify the Service in such a way that they no longer infringe the relevant Intellectual Property Rights; or

(b) procure for the Customer the right to use the Service in accordance with these GTC; or

(c) terminate the Services by written notice to the Customer if such alleged infringement cannot be remedied on commercially reasonable terms.

9 INDEMNIFICATION AND LIMITATION OF LIABILITY

9.1 The Customer shall indemnify Vitrolife from and against any liability to third parties arising from Customer's or any of its Users' violation of these GTC.

9.2 Neither Party shall be liable to the other Party for loss of profit, production, goodwill or any indirect damage or loss, including the other Party's liability to pay compensation to a third party, or for loss of data.

9.3 The maximum total and aggregated liability of Vitrolife to the Customer in respect of any event or series of related events is limited to an amount corresponding to the amount paid and payable by the Customer over the past 12 months.

9.4 The limitation in respect of a Party's liability in damages pursuant to this section 9 shall not apply where the Party has acted intentionally or grossly negligent.

9.5 Neither Party shall be liable for breach, delay or damage caused by a Force Majeure Event.

10 CONFIDENTIALITY

10.1 The Parties hereby undertake during the Term and for a period of ten years thereafter to maintain in absolute confidence any Confidential Information (as defined below) disclosed by the other Party in connection with these GTC and not to disclose any Confidential Information thus received to any third parties.

10.2 "**Confidential Information**" means any and all information (whether in written or oral form), except for:

(a) information which is or becomes common knowledge otherwise than as a result of a breach of these GTC;

(b) information which the disclosing Party can show was in its possession before receiving such information from the other Party;

(c) information which a Party has received or receives from a third party without any lawful restraints as to the disclosure thereof; or

(d) information which a Party is legally obliged to provide under compulsory law, any court order or by order of another authority of competent jurisdiction.

10.3 Each Party shall ensure that the duty of confidentiality pursuant to above is observed by the Party's personnel, consultants and contractors/suppliers, including, in the case of the Customer, the Users.

11 TERM AND TERMINATION

11.1 These GTC are valid for as long as the Customer or any of the Users use the Service.

11.2 Either Party may terminate the Customer's access to and use of the Service by giving the other Party at least one (1) month written notice of termination.

11.3 Vitrolife may terminate the Customer's access to and use of the Service with immediate effect by giving written notice of termination:

a) in the situations described in section 4.8.

b) if the Customer fails to fulfil any of its obligations hereunder; or

c) if the Customer suspends its payments, is the subject of a bankruptcy petition, commences negotiations for a composition with its creditors or applies for company reconstruction, enters into liquidation or may otherwise be deemed to be insolvent.

11.4 Any termination of the Customer's access to and use of the Service shall automatically terminate the license granted to the Customer in section 3.

12 EFFECTS OF TERMINATION

12.1 Upon termination the Customer shall promptly cease all use of the Software and the Service and delete the copy of the Software stored locally on the Device.

13 MISCELLANEOUS

13.1 The Customer may not without Vitrolife's prior written consent, transfer or otherwise assign, partially or in full, any of its rights or obligations hereunder. Vitrolife may transfer its rights and obligations hereunder to any of its affiliated companies or to a third party in connection with a business transfer concerning the Service.

13.2 Should any provision in these GTC or part thereof be found void or invalid, the other provisions of these GTC shall remain in force and the provision may be amended to the extent such invalidity materially affects the rights or obligations of either Party.

Vitrolife reserves the right to update or change these GTC and the Data Processing Agreement from time to time. Changes and updates will become effective on the date set forth in the notice.

14 GOVERNING LAW AND DISPUTE RESOLUTION

14.1 These GTC including the appendices shall be governed by Swedish law, without regard to its conflict of law provisions.

14.2 Any dispute, controversy or claim arising out of or in connection with these GTC or the breach, termination or invalidity thereof, shall be finally settled by arbitration administered by the Arbitration Institute of the Stockholm Chamber of Commerce (the "SCC Institute"). The seat of arbitration shall be Gothenburg and the language to be used in the arbitral proceedings shall be Swedish.

14.3 The Rules for Expedited Arbitrations of the Arbitration Institute of the Stockholm Chamber of Commerce shall apply, unless the SCC Institute in its discretion determines, taking into account the complexity of the case, the amount in dispute and other circumstances, that the Arbitration Rules of the Arbitration Institute of the Stockholm Chamber of Commerce shall apply. In the latter case, the SCC Institute shall also decide whether the arbitral tribunal shall be composed of one or three arbitrators.

14.4 The Parties undertake, indefinitely, not to disclose the existence or contents of any judgment or decision or any information regarding negotiations, arbitral proceedings or mediation in connection therewith. This confidentiality undertaking shall not apply in relation to information, which a Party is required to disclose by law, pursuant to an order of a governmental authority, pursuant to applicable stock exchange rules, or which may be required for the enforcement of a judgment or an award.

Appendix 1: Data processing agreement between Vitrolife Sweden AB as data processor and the Customer as data controller

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.

Clause 7 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.

(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

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

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):THE CUSTOMER OF Vitrolife Genomics SOFTWARE and SERVICE

Processor(s): The processor is Vitrolife Sweden AB, a Swedish company organized and existing under the laws of Sweden, Address: Gustaf Werners gata 2, 400 92, Gothenburg, Sweden

Contact person's name, position and contact details: Data protection officer at dataprotection@vitrolife.com

Signature and accession date: These Clauses are an integral part of Vitrolife Sweden AB's General Terms and Conditions for the Vitrolife Genomics Software and Service. Upon the Customer's acceptance of such General Terms and Conditions these Clauses shall apply between the parties from the same date.

ANNEX II: DESCRIPTION OF THE PROCESSING

1. ***Categories of data subjects whose personal data is processed***
   Patients of the Data Controller
   Relevant Staff of the Data Controller

2. ***Categories of personal data processed***
   About patients:
   a) *Identifying data: name (could be entered anonymised), DOB (optional)*
   b) *Genetic Data*
   c) *Analysed and annotated data of the sample will be generated in the system.*

   About staff:
   i. *Name (could be entered anonymised)*
   ii. *E-mail address*
   iii. *User name, password*

3. ***Sensitive data processed (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.***
   a) *strict purpose limitation*
   b) *access restrictions (including access only for staff having followed specialised training)*
   c) *keeping a record of access to the data (e.g. email trail or log file)*

4. ***Nature of the processing***
   The processor will perform genetic content analysis on behalf of the controller and provide technical support to the extent needed to address controller's specific support issues.

5. ***Purpose(s) for which the personal data is processed on behalf of the controller***
   The personal data is processed by the processor on behalf of the controller to fulfil the genetic content analysis services that the controller as a customer ordered from the processor as a service provider. The processor cannot use the personal data received from the controller for any other purposes and only as instructed by the data controller.

6. ***Duration of the processing***
   The processing will continue as long as the personal data is shared with the processor by the controller in order to fulfil the services the controller has ordered from the processor. The data will be stored no longer than it is necessary to fulfil the purpose it was collected for.

7. ***Deletion or return of personal data***
   The personal data must be erased (or returned upon Controller's request) by the Processor at the time of termination of the Services. Raw data files containing the genetic information may be erased automatically after 30 days if storage capacity is reached. Furthermore, personal data shall be erased from time to time, in accordance with the Controller's written instructions. The personal data may remain in data backups for up to 6 months following all erase events.
8. ***For processing by (sub-) processors, also specify subject matter, nature and duration of the processing***
   The processor may use the technical staff of Vitrolife Group entities and third parties to provide support to the Controller.

The Processor uses BasePair Inc for the following services: (i) Set-up, maintenance and development of the software processing system (ii) Hosting of the Service through Amazon Web Services; and (ii) Technical support of certain significance and/or complexity in exceptional cases

9. ***For transfers to (sub-) processors the below measures are implemented:***
   Pseudonymisation of data transferred to sub-processors;
   Strict need-to-know access control to the data;

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

Description of the technical and organisational security measures implemented by the processor(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, as well as the risks for the rights and freedoms of natural persons.

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

1. Employees or other individuals working within the Processor as an affiliate of Vitrolife Group www.vitrolifegroup.com are bound by confidentiality agreements
2. There are procedures in place ensuring that people that have access to personal data have individual access account
3. Access to personal data shall be logged
4. Personal data stored is automatically backup on a regular basis.
5. Procedures, policies and plans in place to ensure ongoing integrity and availability, e.g. a business continuity and disaster recovery plan including a timetable
6. Backup scheme to maintain backups of company resources.
   - Daily mainframe backup with a retention time for 30 days.
   - Quarterly mainframe backup with retention for three quarters.
   - Yearly mainframe backup with retention for 2 years.
7. Backups are protected by either being physically secured or encrypted by AES 256-bit encryption
8. Monitor system monitoring unauthorized access (or attempt to access) to Vitrolife Group devices, systems, e.g. a firewall

Data security

9. End-point protection on computers, laptops, and servers.
10. End-point traffic and behavior through end-point protection alerts.
11. Monitoring of devices (hardware and software) are kept up to date including enable auto-update on devices for the operating systems currently installed
12. Network traffic through firewalls.
13. Defined personal data breach and data incident procedure.
14. Automated critical patch and updates of defined critical applications.
15. Detection of deviant behavior and pattern.
16. Detect anomalies with continuous scanning and alerting on managed device, service and applications and user behavior.
17. Coverage of newly discovered vulnerabilities.

User identification and authorization

18. Personal data can only be accessed by identified and authorized individuals by way of logging the access to personal data for traceability
19. Password policy ensuring that only identified and authorized individuals have access to the personal data.
20. All data and devices shall be protected by a strong password, multifactor authentication (MFA) or other security settings
21. Restricted access to local computer.
22. Limit and control use of privileged utility programs or any software administrative privilege to run requiring administrative privileges to run
23. Access is only granted after approval from closest manager and IT-manager.
24. Synced offline files encryption on local hard drives
25. Continuously security analysis with central outsourcing and cooperation partners.

Protection of data during transmission and storage

26. AES 256-bit encryption is used during transmitting and storage

27. Servers storing personal data stored electronically are located at the premises
28. Automatically backups (when data is stored electronically) should be in place
29. Physical documents are stored at the premises of Processor (unless agreed otherwise with Controller)
30. Physical documents are stored under conditions were not disposed to fire, theft etc.
31. 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)

Physical security of locations at which personal data are processed

32. Only identified and authorized individuals have access to the premises where the personal data is processed and/or stored
33. 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
34. Server room(s) including equipment, cables, etc. are secured with sufficient physical measures

Detection of threats, vulnerability, and incident management

35. Identification of devices connected to the network.
36. Risk assessment agents: to identify vulnerabilities on device application or service.
37. Continuously vulnerability scanning: of device, application and services.
38. Third party security review and penetration test.
39. IT Governance framework to enforce security standards for suppliers, contractors and other no employees. (e.g. NDA, Data protection etc.)
40. Defined personal data breach and data incident procedure.
41. Post-incident analysis leads to continuous improvement of framework and procedures.

Organization Centralized IT-department with full responsibility for Group common applications and all IT equipment owned by or connected to the Group's IT environment.

42. The Vitrolife Group IT manager approval of all application, services, and equipment implementation and connection with IT-environment.
43. IT Security is managed, approved and set by the Vitrolife Group IT department.

Employee policies

44. Awareness training for all employees and other individuals working with data processing covering IT security and/or Data Processing (Privacy awareness)
45. There is a documented strong password policy available for users

Remote working

46. 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 Group's premises

Business continuity and disaster recovery plan

47. Processor shall have in place a business continuity and disaster recovery plan including a timetable
48. 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 as listed here:	**http://www.vitrolifegroup.com/**	To provide support service
Adecco Malaysia	Level 9, Ilham Tower, No. 8, Jalan Binjai, 50450 Kuala Lumpur, Malaysia	To provide support service
Basepair Inc	Madison Ave, Fl 4, New York NY, 10007, USA	*(i) Set-up and development of the software processing system. Hosting of the Service through Amazon Web Services, providing and maintaining the infrastructure of the system including support services; and (ii) Technical support of certain significance and/or complexity in exceptional cases*
Amazon Web Services, Inc. (sub-processor to Basepair Inc.)	410 Terry Avenue North Seattle, WA 98109 United States	*Hosting of the Service locally on Amazon Web Services (AWS).*

For Customers located outside of the EEA and not in any of the countries listed here Data protection adequacy for non-EU countries (europa.eu) **the EU Commission's Standard Contractual Clauses Module Four (transfer from processor to controller) shall apply between Vitrolife and the Customer in addition to the data processing agreement. For the interpretation of such Standard Contractual Clauses Module Four Vitrolife is the 'data exporter' and the Customer is the 'data importer'. [STANDARD CONTRACTUAL CLAUSES FOR INTERNATIONAL TRANSFERS WHEN THE CUSTOMER IS OUTSIDE OF EU/EEA]**

APPENDIX 2 – THIRD-PARTY SUPPLIER SOFTWARE LICENSE TERMS

Source code and third-party software licences for the Upload Software suite can be found at the URL:

kMap Third-party supplier software licence terms at uploadsoftware-third-partysoftware-licenses.pdf (vitrolife.com)

eMap Third-party supplier software licence terms at UploadSoftware-Third-PartySoftware-Licenses (vitrolife.com)

The license terms form an integral part of these GTC.