## ANNEX: Data processing agreement between Igenomix Spain Lab SLU as data processor and the Customer as data controller located in the EU/EEA

## 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.

(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

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

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 IGX'S SERVICES**

On behalf of the Controller, the instructions to the Processor may come from the:

a) Doctor who was requesting the test
b) The data protection officer/manager of the controller
c) As otherwise agreed in writing between the parties

Contact person: the controller is responsible for providing the Processor with information on the controller's contact person

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

**Processor(s): The processor is IGENOMIX SPAIN LAB, S.L.U.** , a company organized and existing under the laws of Spain, Address: Calle Narcís Monturiol 11B, Edificio Europark, Parque Tecnológico de Paterna (46980), Valencia, Spain

Contact person's name, position and contact details: Data protection officer/privacy@igenomix.com

On behalf of the Controller, the instructions to the Processor may be addressed to:

a) The relevant test director at Igenomix
b) Customer support of Igenomix
c) The data protection officer

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

## 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, DOB, telephone, e-mail address)*
   *b) Health Data collected in the TRF forms*
   c) *Genetic Data collected in the TRF forms*
   *d) Analysis results of the biological samples from patients*
   *e) Other data that may be necessary for a specific test*

   *About staff:*
   *i. Name*
   *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*
4. ***Nature of the processing***

   *The processor will perform genetic test analysis on behalf of the controller depending on the ordered genetic test by the controller. Potential anonymisation of personal data for research purposes.*
   *Steps: 1) sample collection 2)data entering into IGX's ERP/LIMS system 3) data analyzation in house, or in another IGX affiliate or by a third-party 4) diagnostic team generates the report 5) issue of the final report to the controller via IGX's ERP/LIMS system 6) Potential anonymization of data.*
5. ***Purpose(s) for which the personal data is processed on behalf of the controller***
   *a) The personal data is processed by the processor on behalf of the controller to fulfil the genetic services that the controller as a customer ordered from the processor as a service provider.*
   *b) The processor can not use the personal data received from the controller for any other purposes and only as instructed by the data controller.*
   *c) The processor may anonymise the personal data so they can not, directly or indirectly, be traced back to any individual. Processor may use the fully anonymised data for scientific research purposes.*
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*

*and for the retention periods mentioned in paragraph 7 below.*

7. ***Deletion or return of personal data***
   *When the data are no longer useful or necessary for the purposes for which they were collected and processed, or when such purposes have been fulfilled and exhausted, the personal data must be erased, provided that it is not necessary to block the data in order to respond to possible liabilities arising from the processing of personal data and for the period of limitation of such liabilities as provided for by Union or Member State law applicable to the data controller.*
8. ***For processing by (sub-) processors, also specify subject matter, nature and duration of the processing***
   *For some tests the Processor uses one of the subprocessors mentioned in Annex 4 for the performance of genetic testing.*
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;*
10. ***Description of the specific technical and organisational measures to be taken by the processor to be able to provide assistance to the controller.***
    *a. The processor may share the genetic test report directly with the patient in an encrypted e-mail, once the identity of the patient is verified.*
    *b. The processor may disclose the raw data of the genetic test analysis with both the data controller and the patient upon request against a fee.*

## 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 at 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**

42. Centralized IT-department with full responsibility for Group common applications and all IT equipment owned by or connected to the Group's IT environment.
43. The Vitrolife Group IT manager approval of all application, Services, and equipment implementation and connection with IT-environment.
44. IT Security is managed, approved and set by the Vitrolife Group IT department.

### Employee policies

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

### Remote working

47. 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

48. Processor shall have in place a business continuity and disaster recovery plan including a timetable
49. 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 infromation | Purpose | Legal basis for the data transfer |
|---|---|---|---|
| **ABACID 2007, SL** | C/ Oña, 28050 Madrid.<br>CIF / NIF: B-85194199<br>Telephone: (+34) 917 567 878<br>Email: atencionalcliente@mail.abacid.es<br>Email DPO: dpo@mail.abacid.es<br>Domain name: www.abacid.es | To perform some part of the test ordered by the customer (Karyotype) | Data sub-processing agreement |
| **BLUE HEALTHCARE, S.L.**, | 28036 Madrid, avenida de Alberto Alcocer, 7, | To provide post genetic counselling | Data sub-processing agreement |
| **Igenomix FZ, LLC** | 26th Street, Building 40 - Unit 501 & 502, Dubai HealtCare City, Dubai, UAE<br>privacy@igenomix.com | To perform the test ordered by the customer (CGT Bank, CGT Plus, CGT Exome and CGT One – partially outsourced) | Group Data Transfer Agreement |
| **IGENOMIX ITALIA S.R.L.** a | Italy Via Enrico Fermi 1, Marostica (36063), Vicenza, Italia | To perform the test ordered by the customer (CGT Essential) | Group Data Transfer Agreement |