Data Processing Agreement

This data processing agreement (the “**Data Processing Agreement**”) has been made by and between Customer (the data “**Controller**”) and Novacura (the data “**Processor**”), as identified in a Sales Order, (each a “**Party**” and collectively the “**Parties**”).

The Parties have agreed as follows:

1. Background

Controller and Processor have entered into an Agreement (including a Sales Order, the Main Agreement and applicable appendices, collectively below the “**Agreement**”) which involves the Processing of Personal Data by Processor on behalf of Controller. Data Protection Regulations stipulate that processing of personal data by a processor shall be governed by a contract. The Parties have entered into this Data Processing Agreement to comply with the requirements set out in the Data Protection Regulations.

Processor hereby enters into this Data Processing Agreement on its behalf and on behalf of its group companies listed in Appendix 3.

2. Definitions

In this Data Processing Agreement:

“**Application**” means any work flow designed by Controller in Novacura Flow Studio.

“**Data Protection Regulations**” means any and all data protection laws and regulations applicable from time to time during the term of this Data Processing Agreement (including but not limited to the Swedish Act on complementary provisions to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (2018:218), EC Directive 95/46 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and 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)) as interpreted from time to time by the Court of Justice of the European Union or other court of law that is competent to establish a precedent for such data protection laws.

“**Data Subject**” means an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

“**Personal Data**” means any information relating to a Data Subject which is Processed on behalf of Controller by Processor.

“**Processing (of Personal Data)**” means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

3. Processing of Personal Data

3.1. Processor may only Process the Personal Data in accordance with the documented instructions from Controller, including with regard to transfers of personal data to a third country or an international organization, unless required to do so by EU law (including the laws of its member states) to which Processor is subject; in such a case, Processor shall inform Controller of that legal requirement before Processing, unless EU law prohibits Processor from informing Controller on important grounds of public interest.

3.2. Controller takes full responsibility for that the data (both Personal Data and other data) Processed under this Data Processing Agreement, including Appendix 1, does not violate any third party rights or otherwise violate applicable laws. Controller takes full responsibility for that the instructions for Processing of Personal Data under this Data Processing Agreement, including in Appendix 1, comply with applicable Data Protection Regulations. The Parties agree that this Data Processing Agreement constitutes the complete and final instructions to Processor for the Processing of Personal Data, including but not limited to a complete list of the categories of Personal Data in Appendix 1 that will be Processed under this Data Processing Agreement. Controller takes full responsibility for Processing of any category of Personal Data not specified in Appendix 1 and all such data shall be excluded from the applicability of this Data Processing Agreement.

3.3. Processor shall immediately inform Controller if, in its opinion, an instruction infringes the Data Protection Regulations. Processor shall not implement such an instruction until it has been confirmed as legally permissible by Controller.

3.4. Processor shall Process the Personal Data for the duration of the Agreement. The (i) type of Personal Data Processed under this Data Processing Agreement, (ii) categories of Data Subjects that the Personal Data concern, and (iii) nature and purpose of the Processing are set forth in Appendix 1.

3.5. When Processing Personal Data under this Data Processing Agreement, Processor shall comply with the Data Protection Regulations.

3.6. Processor shall ensure that persons authorized to Process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

3.7. Processor shall assist Controller by the technical and organizational measures, as set forth in Appendix 2, for the fulfilment of Controller's obligation to respond to requests for exercising the Data Subject's rights under the Data Protection Regulations.

3.8. Taking into account the nature of the Processing and the information available to Processor, Processor shall assist Controller in ensuring compliance with Controller's obligations pursuant to the Data Protection Regulations, including (where applicable) its obligations to (i) implement appropriate technical and organizational measures, (ii) notify personal data breaches to the supervisory authority, (iii) inform Data Subjects of personal data breaches, (iv) carry out data protection impact assessments, and (v) carry out prior consultation with the supervisory authority.

Processor is entitled to fair remuneration in form of an hourly consultancy fee for work undertaken in respect of this commitment, as agreed upon with Controller and if no such fee has been agreed, Processor's price list shall apply as applicable from time to time.

3.9. Processor shall, at the choice of Controller, delete or return all Personal Data to Controller after the end of the provision of services relating to the Processing of the Personal Data and delete existing copies unless EU law (including the laws of its member states) requires storage of the Personal Data.

4. Security of Processing

4.1. Processor shall implement appropriate technical and organizational measures as set forth in Appendix 2. Processor makes available a number of security features and functionalities that Controller may elect to use. Controller is responsible for properly (i) configuring the Applications, (ii) using the functions available in connection with the Application (including the security functions), and (iii) taking steps as Controller considers necessary to maintain an adequate level of security, protection, deletion and backup of Controller's Personal Data appropriate to the risk of Processing such Personal Data. Such steps may include implementing encryption technology to protect the Personal Data from unauthorized access and routine archiving of Personal Data.

4.2. Processor shall ensure that there are technical and practical solutions for investigating suspicions that someone working for Processor or any of its sub-processors has had unauthorized access to the Personal Data.

4.3. Processor shall be prepared to follow any decisions from the supervisory authorities regarding measures needed to meet legal security requirements.

4.4. Processor shall notify Controller, without undue delay, after becoming aware of a personal data breach (as defined in the Data Protection Regulations) affecting the Personal Data and provide Controller with any information reasonably required by Controller regarding such personal data breach. Processor is entitled to fair remuneration in form of an hourly consultancy fee for work undertaken in respect of this commitment, as agreed upon with Controller and if no such fee has been agreed, Processor's price list shall apply as applicable from time to time.

5. Information and audits

5.1. Processor shall make available to Controller all information necessary to demonstrate compliance with the obligations laid down in this Data Processing Agreement. Furthermore, when a notice has been given thirty (30) days in advance, Processor shall allow for and contribute to audits, including inspections, conducted by Controller or another auditor mandated by Controller. The purpose of such audits shall be to verify Processor's compliance with the obligations laid down in this Data Processing Agreement. The content and extent of an audit may not exceed what is necessary to achieve the purpose of the audit. Any audits shall be at Controller's expense, but Processor shall provide any reasonably required assistance free of charge.

5.2. Inspections on Processor's premises may be performed only in the presence of a representative of Processor, on business days between 9 am and 4 pm. The Controller or auditor shall agree on necessary confidentiality undertakings and comply with the security measures of the Processor at the site where the audit shall be performed. Controller or other mandated auditor shall not have access to confidential information that relates to Processor's other customers or other personal data that is not Processed under this Data Processing Agreement or Appendix 1. Any information collected in connection with the audit shall be deleted immediately after the completion of the audit or as soon as the information is no longer required for achieving the purpose of the audit.

6. Sub-processors

6.1. Processor is hereby given a general written authorization of Controller to engage another processor to Process the Personal Data (i.e. a sub-processor). Processor shall inform Controller of any intended changes concerning the addition or replacement of sub-processors, thereby giving Controller the opportunity to object to such changes.

6.2. If Processor engages a sub-processor for carrying out specific Processing activities on behalf of Controller, as instructed to Processor in Appendix 1, the same data protection obligations as set out in this Data Processing Agreement shall be imposed on that sub-processor by way of a contract. In particular, such data protection obligations shall provide sufficient guarantees that the sub-processor implements appropriate technical and organizational measures in such a manner that the Processing will meet the requirements of the Data Protection Regulations. Processor shall at all times remain fully responsible for all obligations, acts and omissions of any sub-processor to the same extent as if performed or not performed by Processor itself.

6.3. Upon Controller's request, Processor shall make available a list of all sub-processors engaged by Processor pursuant to this Section 6, including the locations of where such sub-processors Process the Personal Data.

6.4. Processor is able to provide the following products and services to Controller:

(i) Novacura Flow platform**;**

(ii) Implementation services for IFS products or other business administration systems; and

(iii) Cloud hosting services.

When providing implementation services for IFS products or other business administration systems, Controller shall enter into separate data processing agreements directly with the relevant providers of such products and systems.

7. Processing of Personal Data in countries outside EU/EEA

7.1. Processor may transfer or give access to Personal Data to countries outside of the EU/EEA. If Personal Data are transferred outside of the EU/EEA, Processor shall ensure that such Processing at all times complies with the Data Protection Regulations. This may e.g. be achieved by assisting Controller in establishing a binding agreement, in accordance with the applicable EU Commission Model Contracts for the transfer of personal data to third countries, with Processor. Processing in a country outside of the EU/EEA may also take place

SW42554814/4

on the basis of a valid adequacy decision, where the EU Commission has decided that such country ensures an adequate level of data protection.

7.2. If Processor engages sub-processors, and such assistance entails Processing of Personal Data on behalf of Controller outside of the EU/EEA, Processor and sub-processor shall enter into data transfer agreements as required by law for the lawful transfer of Personal Data outside of the EU/EEA, including relevant EU Commission Model Contracts for the transfer of personal data to third countries adopted by the EU Commission (for which Processor is considered the data exporter and sub-processor is considered the data importer).

8. Confidentiality

Processor undertakes not to disclose any information regarding the Processing of Personal Data under this Data Processing Agreement to any third parties or in any other way disclose any other information received as a result of this Data Processing Agreement. The obligation of confidentiality does not apply to information that Processor is ordered to disclose to authorities. In addition to this section 8, any confidentiality commitment in the Agreement shall also be applicable. This confidentiality commitment shall survive the termination of this Data Processing Agreement.

9. Remuneration

Processor is entitled to specific remuneration for the Processing of Personal Data, in accordance with this Data Processing Agreement, in addition to the remuneration stipulated in the Agreement.

10. Responsibility towards third parties

To the extent permitted by applicable laws, any limitation of liability stipulated in the Agreement for Processor shall also be applicable for this Data Processing Agreement. If the Agreement does not include any limitation of liability, the following shall apply to the extent permitted by applicable laws. Novacura's total liability for any damages, claims or loss of any kind under or in connection with this Data Processing Agreement shall, unless caused by intent or gross negligence, be limited to an amount equal to one hundred (100) % of the total price paid by Controller for each relevant product or service delivered by Processor during the immediately preceding calendar year.

11. Term

This Data Processing Agreement will remain in full force and effect until the termination or expiration of the Agreement.

12. Changes and additions

Changes and additions to this Data Processing Agreement, including to this section 12, must be in writing and duly executed by the Parties. Processor shall not unreasonably withhold its consent to any changes and additions requested by Controller that are necessary to implement for the purpose of fulfilling any mandatory requirements in the Data Protection Regulations.

13. Other

13.1. In addition to this Data Processing Agreement, any relevant provisions in the Agreement shall also be applicable to Processor's Processing of Personal Data. In case of any conflict between the Agreement and this Data Processing Agreement, this Data Processing Agreement shall take precedence with regard to Personal Data.

13.2. This Data Processing Agreement and any non-contractual obligations arising out of or in connection with it shall be governed by and construed in accordance with the laws of Sweden, excluding its conflict of laws principles providing for the application of the laws of any other jurisdiction.

13.3. Any dispute concerning the interpretation or application of this Data Processing Agreement shall be settled in accordance with the provisions on dispute resolution in the Agreement.

Appendix 1 – Instructions for processing

DESCRIPTION OF PROCESSING

Categories of Data Subjects whose Personal Data is Processed.	a) System end users b) System designers c) System administrators d) System developers e) Employees f) Contractors g) Suppliers h) Customers
Categories of Personal Data Processed.	a) Log in information b) Names c) Email addresses d) Phone numbers e) Roles f) Positions
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) N/A
The frequency of the Processing (e.g. whether the Personal Data is Processed on a one-off or continuous basis).	a) Processing is on a continuous basis and follows the term of the Data Processing Agreement.
Nature of the Processing.	a) Processor shall Process Personal Data as necessary to provide the Novacura Flow platform to the Controller pursuant to the Agreement. b) Processor may not Process the Personal Data for any other purposes than set forth above. c) Processor shall Process Personal Data as necessary to provide support, system maintenance and advisory to the Controller pursuant to the Agreement. d) Processor may not Process the Personal Data for any other purposes than set forth above.
Purpose(s) of the Processing.	a) Enabling the provision of the Novacura Flow platform to the Controller pursuant to the Agreement.

	b) Enabling the agreed project deliveries according to the Controller pursuant to the Agreement. c) Enabling provision of support, system maintenance and advisory to the Controller pursuant to the Agreement.
The period for which the Personal Data will be retained, or, if that is not possible, the criteria used to determine that period.	a) Personal Data will be retained as long as necessary for enabling the provision of the Novacura Flow Platform. b) Personal Data will be retained as long as necessary for performing agreed project or assignment activities. c) Personal Data will be retained as long as necessary for suppling support, system maintenance and advisory.
Subject matter, nature and duration of the Processing for transfers to (sub-)processors.	a) Enabling the provision of the Novacura Flow platform to the Controller pursuant to the Agreement. b) Enabling the agreed project deliveries according to the Controller pursuant to the Agreement. c) Enabling provision of support, system maintenance and advisory to the Controller pursuant to the Agreement.

LIST OF SUB-PROCESSORS

The Controller has authorized the use of the following sub-processors:

Sub-processor 1 (for Controller's outside the EU/EEA)

Name:	Microsoft Corporation
Address:	One Microsoft Way, Redmond WA, USA
Contact person's name, position and contact details (optional):	N/A
Description of Processing (including a clear delimitation of responsibilities in case several sub-processors are authorized):	Hosting the Novacura Flow as Software as a Service on the Microsoft Azure platform.
Location of non-EU/EEA Processing (if applicable):	USA

Sub-processor 2 (for Controller's within the EU/EEA)

Name:	Microsoft Ireland Operations, Ltd.
Address:	One Microsoft Place, South County Business Park, Leopardstown, Dublin, Ireland
Contact person's name, position and contact details (optional):	N/A
Description of Processing (including a clear delimitation of responsibilities in case several sub-processors are authorized):	Hosting the Novacura Flow as Software as a Service on the Microsoft Azure platform.
Location of non-EU/EEA Processing (if applicable):	N/A

Appendix 2 - Technical and organizational measures

1. Novacura Flow

1.1. Novacura Flow platform is a process platform enabling the Controller to design its own workflows ("**Applications**") for use within its business operations. The Applications may be used on several different platforms and/or systems with or without the interference of a user. The Applications may include Processing of Personal Data if the Controller chooses to design its Applications in a way that allows Personal Data to be Processed in the Application. Processor provides functionality tools that Controller may use to protect its Personal Data. Controller takes full responsibility for assessing the need for and implementing the adequate level of protection for its Personal Data when designing the Applications. Further, Controller is responsible for documenting what Personal Data is Processed in the Applications.

1.2. Novacura Flow platform provides the following types of user accounts:

(i) **User.** The users' access to and authority to use the Application is designed by Controller. A user account may be designated to physical persons or systems within or outside Controller's organization. Controller may design User accounts with or without restrictions of authorization, e.g. password.

(ii) **Public User.** Applications may be designed to provide access to Public Users, which are generic user accounts that do not require identification for accessing and using the Application.

(iii) **Flow Designer.** The Flow Designer of the Controller designs the Application and may configure connections to underlying sources of data, create User accounts and distribute authority to Users via the Novacura Flow Studio. The Flow Designer is able to control what types of data that are Processed in the Application. If such data includes Personal Data, the Flow Designer is responsible for designing the Application in a way that ensures compliance with applicable Data Protection Regulations.

2. Technical Security

2.1. Interfaces

2.1.1. Novacura Flow provides access to the Applications via the following user interfaces:

(i) Native clients (iOS, android, Windows 10, Windows CE);

(ii) Web clients; and

(iii) Novacura Flow Portal

2.2. Connectors

2.2.1. Controller may design its Application by including so called Connectors to the design. Connectors enable the Novacura Flow platform to read from and write in external sources of data of Controller. Controller is able to control what sources of data are connected to the Novacura Flow platform through Connectors.

2.3. Encryption

2.3.1. Controller may encrypt the Native clients by implementing a Mobile Device Management system of its preference. Processor does not encrypt communication to or from Native clients. Controller is responsible for assessing the level of protection needed and to implement technical protection as appropriate for the Personal Data Processed within the Application.

2.3.2. Controller may encrypt the communication between Web clients and/or Novacura Flow Portal and the underlying sources of data of Controller by implementing appropriate encryption functionalities. Controller is responsible for assessing the level of protection needed and to implement technical protection as appropriate for the Personal Data Processed within the Application.

2.3.3. Processor will implement encryption functionalities for communication within the Novacura Flow Portal.

2.3.4. Passwords to the Novacura Portal are protected with a cryptographic hash function implemented by Processor.

2.4. Logs and traceability

2.4.1. All events of users' log in in and log out are logged for traceability purposes and visible to Processor. When designing the Application, Controller may choose to add additional log points as part of the Application. Controller is responsible for assessing the level of protection needed and to add log points as appropriate for tracing the Processing of Personal Data within the Application.

2.5. Back up

2.5.1. Controller is responsible for backing up its Applications and the results deriving from the use of the Applications as appropriate with regard to applicable Data Protection Regulations. Customer is also responsible for backing up the different underlying sources of data connected to the Application.

2.6. Access for Processor

2.6.1. Processor has no access to the Applications designed by Controller, the results deriving from the use of the Applications or the sources of data connected to the Applications. Processor is not able to see or trace any communication between Controller's Applications and external sources of data connected to the Applications.

Appendix 3 – List of Novacura group companies

Company name	Company registration number
Melar Holding AB	556916-4899
Novacura AB	556675-8156
Novacura Sverige AB	556835-2438
Novacura Benelux	KvK number 62910787
Novacura Finland OY	Y-Tunnus 2780564-2
Novacura Norge AS	Org.no: 914 345 588
Novacura North America Inc	EIN: 30-0934614
Novacura Deutschland GmbH	9241/133/7069
Novacura Schweiz GmbH	CHE-333.602.354
Novacura Lanka (PVT) Ltd.	PV00203168
Novacura Poland SP Z.O.O.	VAT: PL6772372101
Novacura Australia PTY Ltd	ABN: 42 642 605 301