3 December 2025

Novata Group Data Processing Agreement

This Data Processing Agreement ("**DPA**") and its Schedules and Annexes reflects your agreement with a company of the Novata Group ("**Novata Group Entity**") with respect to the provisions of Services as defined in the Terms and Conditions to which you agreed as a subscriber available at: www.novata.com/terms-and-conditions or www.atlasmetrics.io/gtc or any separate written agreement which references this DPA (the "Principal Agreement").

Novata Group is made up of Novata, Inc., a Delaware Public Benefit Corporation, with offices at 54 West 21st Street, Suite 1201, New York, NY 10010 USA and all wholly owned subsidiaries including Atlas Metrics GmbH, Adalbertstr. 39, 10179 Berlin, Germany.

This DPA is supplemental to, forms part of, and is effective upon its incorporation into, the Principal Agreement by and between Novata, Inc., **or** the Novata Group Entity as set out in the relevant order for services ("**Service Order**") acting as Data Processor ("**Data Processor**") and you ("**Customer**").

If any terms and conditions contained herein are in conflict with the terms and conditions set forth in the Principal Agreement, the terms and conditions set forth in this DPA shall apply. Unless specifically defined herein, all capitalized terms shall have the same meanings given to them in the Principal Agreement. Terms used in this DPA but not defined herein or in the Agreement shall have the meanings given to them in the European Union General Data Protection Regulation ("**GDPR**").

(each a "**Party**" and together, "**Parties**")

WHEREAS

(A) The Customer acts as a Data Controller.

(B) The Novata Group Entity that is a Party to the Principal Agreement with you acts as Data Processor.

(C) The Customer wishes to contract certain services including collection and dissemination of information regarding corporate performance along Environmental, Social and Governance ("ESG") dimensions and related services (the "Services") as set forth in the Principal Agreement, which imply the processing of personal data by the Data Processor. Further details of the Processing are set out in Schedule 1 to this DPA.

(D) The Parties seek to implement a data processing agreement that complies with the requirements of the current legal framework in relation to data processing and with the 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, and repealing Directive 95/46/EC (General Data Protection Regulation).

(E) The Parties wish to lay down their rights and obligations.

IT IS AGREED AS FOLLOWS:

1. DEFINITIONS. Capitalized terms shall have the meaning set forth in this Section 1 or as otherwise defined in other sections of this DPA. If not defined, Capitalized terms shall have the same meaning set forth in the Principal Agreement or the GDPR, as applicable:

1.1 "**DPA**" means this Data Processing Agreement and all Schedules.

1.2 "**Customer Personal Data**" means any Personal Data Processed by a Contracted Processor on behalf of Customer pursuant to or in connection with the Principal Agreement, including Personal Data provided as Customer Data as defined in the Principal Agreement.

1.3 "**Contracted Processor**" means Data Processor and any Subprocessor.

1.4 "**Data Protection Laws**" means all data protection legislation and regulations applicable to the processing of the Customer Personal Data under this DPA and the Principal Agreement, including 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 ("**GDPR**") and supplementing national legislation, and the United Kingdom Data Protection Act of 2018, the UK General Data Protection Regulation ("**UK GDPR**"), and other applicable UK data protection law (together, "**UK Data Protection Laws**"), in each case as may be amended, repealed, consolidated, or replaced from time to time.

1.5 "**EEA**" means the European Economic Area.

1.6 "**GDPR**" has the meaning set forth in the definition of Data Protection Laws.

1.7 "**Data Transfer**" means:

(a) a transfer of Customer Personal Data from the Customer to Data Processor; or

(b) an onward transfer of Customer Personal Data from Data Processor to a Subprocessor.

1.8 "**Services**" means the services the Customer is provided pursuant to the Principal Agreement.

1.9 "**Subprocessor**" means any person appointed by or on behalf of Data Processor to process Customer Personal Data on behalf of the Customer in connection with the DPA.

1.10 "**Standard Contractual Clauses**" means the Standard Contractual Clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and the Council approved by European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, as may be amended, superseded or replaced from time to time.

2. PROCESSING OF CUSTOMER PERSONAL DATA.

2.1 The Data Processor:

(a) shall comply with all applicable Data Protection Laws in the Processing of Customer Personal Data; and

(b) shall not Process Customer Personal Data other than on the relevant Customer's documented instructions, including the Principal Agreement, unless Data Processor reasonably believes that such documented instructions are unlawful or infringe applicable Data Protection Laws. If the Data Processor reasonably believes that the Customer's documented instructions are unlawful or infringe applicable Data Protection Laws, the Data Processor shall immediately inform the Customer and shall suspend execution of the instruction until the Customer confirms, modifies, or withdraws such instruction. Any material change to instructions that requires adjustments to the Services may be treated as a change order and may be subject to mutually agreed additional fees and timelines.

(c) Where Data Processor is required to Process Customer Personal Data without or contrary to Customer's instructions under Union or Member State law applicable to the Processing activities subject to this DPA, Data Processor shall inform Customer of that legal requirement prior to Processing, unless the law prohibits such notice.

2.2 Data Processor shall document all instructions received from Customer. Oral instructions must be confirmed by Customer in writing or electronically without undue delay. Data Processor is not obligated to act on oral instructions that are not promptly confirmed. Where instructions materially deviate from the Principal Agreement, the Parties will in good faith agree to any necessary changes, timelines, and reasonable fees.

3. DATA PROCESSOR PERSONNEL. Data Processor shall take reasonable steps to ensure that any employee, agent, or contractor of Data Processor, who may have access to the Customer Personal Data, are subject to confidentiality undertakings or statutory obligations of confidentiality, ensuring in each case that access is limited to those individuals who need to know or access the relevant Customer Personal Data, as necessary for the purposes of the Principal Agreement.

4. SECURITY. Taking into account the state of the art, the costs of implementation and the nature, scope, context, and purposes of Processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Data Processor shall in relation to the Customer Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures listed in Article 32(1) of the GDPR. The Parties acknowledge and agree that the measures set out in Annex II of Schedule 3 constitute appropriate security measures and are in compliance with the state of the art. Upon request, Data Processor shall make its written information security program available to Customer, along with descriptions of the security controls in place with respect to Personal Data.

5. SUBPROCESSING.

5.1 The Customer generally agrees that Data Processor may engage Subprocessors (as well as advisors, contractors, and auditors) to Process Customer Personal Data. The Customer authorizes Data Processor to appoint (and permit each Subprocessor appointed in accordance with this Section 5 to appoint) Subprocessors in accordance with this Section 5 and any restrictions in the Principal Agreement.

5.2 Data Processor may continue to use those Subprocessors already engaged by Data Processor as at the date of this DPA, as listed on the Novata Group Subprocessors List available via a permanent hyperlink at www.novata.com/subprocessors (the "**Subprocessors Page**"). If the Data Processor disengages existing Subprocessors and/or engages new Subprocessors, the Data Processor shall update the Subprocessors Page accordingly and will notify you by email where you have provided us with an email address for where updates should be sent to. If you wish to be notified please email privacy@novata.com to provide the designated Customer email address. If Customer's designated notice contact is not up to date or delivery fails, posting on the Subprocessors Page shall serve as written notice.

5.3 Customer may object to the engagement of such new Subprocessor by notifying Data Processor in writing within 14 (fourteen) days from the date the Subprocessors page is updated or the date of the written notice under Section 5.2. Any objection shall set out legitimate data protection reasons and consent shall not be unreasonably withheld. Upon a valid objection, the Parties will cooperate in good faith to implement commercially reasonable alternative measures. If no feasible alternative can be agreed, Customer may suspend only the affected Processing activities. If the affected activities are material and cannot be reasonably suspended or modified, either Party may terminate the affected Services on thirty (30) days' prior written notice, with a pro-rata refund of prepaid, undelivered Services, and without further liability, subject to Section 7 of the Terms and Conditions.

5.4 With respect to each Subprocessor (which, for the purposes of this Section 5.4 includes new Subprocessors engaged in accordance with Section 5.3), Data Processor shall ensure that the arrangement between Data Processor and the relevant Subprocessor is governed by a written contract including terms that offer at least the same level of protection for Customer Personal data as those set out in this DPA and meet the requirements of Article 28(3) of the GDPR.

6. DATA SUBJECT RIGHTS.

6.1 Taking into account the nature of the Processing, Data Processor shall assist the Customer by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfillment of the Customer's obligations, as reasonably understood by Customer, to respond to requests to exercise Data Subject rights under the Data Protection Laws.

6.2 Data Processor shall:

(a) promptly notify Customer if it receives a request from a Data Subject under any Data Protection Law in respect of Customer Personal Data; and

(b) ensure that it does not respond to that request except on the documented instructions of Customer or as required by applicable laws to which the Data Processor is subject, in which case Data Processor shall to the extent permitted by applicable laws inform Customer of that legal requirement before Data Processor responds to the request.

7. PERSONAL DATA BREACH AND NOTIFICATION.

7.1 Data Processor shall notify Customer without undue delay upon Data Processor becoming aware of a Personal Data Breach affecting Customer Personal Data, providing Customer with sufficient information to allow the Customer to meet any obligations to notify, report, or inform Data Subjects and Supervisory Authorities of the Personal Data Breach under the Data Protection Laws.

7.2 Data Processor shall cooperate with the Customer and take reasonable commercial steps as are directed by Customer to assist in the investigation, mitigation, and remediation of each such Personal Data Breach.

8. DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION. Data Processor shall provide reasonable assistance to the Customer with any data protection impact assessments, and prior consultations with Supervisory Authorities or other competent data privacy authorities, which Customer reasonably considers to be required by Articles 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Customer Personal Data by, and taking into account the nature of the processing and information available to, the Contracted Processors.

9. DELETION OR RETURN OF CUSTOMER PERSONAL DATA. Subject to this Section 9, Data Processor shall promptly and in any event within 30 (thirty) days of the date of cessation of any Services involving the processing of Customer Personal Data, either (i) delete and procure the deletion of all copies of the Customer Personal Data or (ii) return all Customer Personal Data to the Customer and delete all existing copies, at the Customer's choice. Notwithstanding Customer's deletion instructions, the Processor may retain Customer Personal Data to the limited extent required by EU or Member State law or for legitimate compliance obligations, or as preserved in automatic backup systems, provided that such data remains subject to the data-protection, confidentiality, and security obligations of this DPA and is deleted in accordance with the Processor's established retention and backup cycles.

10. AUDIT RIGHTS.

10.1 Subject to this Section 10, Data Processor shall make available to the Customer on request reasonable information necessary to demonstrate compliance with this DPA, and shall allow for and contribute to audits, including inspections, by the Customer or an auditor mandated by the Customer in relation to the Processing of the Customer Personal Data by the Contracted Processors.

10.2 Customer shall give Data Processor reasonable advance notice of any audit or inspection to be conducted under Section 10.1 and shall make (and ensure that each of its mandated auditors makes) reasonable endeavors to avoid causing (or, if it cannot avoid, to minimize) any damage, injury, or disruption to Data Processor's premises, equipment, personnel, and business while its personnel are on those premises in the course of such an audit or inspection. Data Processor need not give access to its premises for the purposes of such an audit or inspection to a third party who is performing the audit on behalf of the Customer, unless such third party auditor executes a confidentiality agreement acceptable to Data Processor before the audit.

11. DATA TRANSFER. For those Data Transfers not based on an adequacy decision, as defined in Article 45 of the GDPR, or otherwise subject to appropriate safeguards or a derogation, under

Articles 46 and 49 of the GDPR, respectively, the restricted transfers shall be subject to the Standard Contractual Clauses attached hereto as Schedule 3, and Data Processor may transfer or authorize the Data Transfer to countries outside the EU and/or the EEA consistent with those Standard Contractual Clauses.

For data transfers governed by UK Data Protection Laws, the Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 available at https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf, issued by the UK Information Commissioner's Office and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as revised under Section 18 of those Mandatory Clauses ("**UK Addendum**") shall apply. The information required for Tables 1 to 3 of Part One of the UK Addendum is set out in Schedules 1 and 3 of this DPA (as applicable). For the purposes of Table 4 of Part One of the UK Addendum, neither party may end the UK Addendum when it changes.

If such contemplated transfers will only occur between the UK and a third country, not involving the EEA, ("**UK Transfers**") the Mandatory Clauses of the Approved International Data Transfer Agreement ("**IDTA**"), being the template UK IDTA A.1.0, available at https://ico.org.uk/media/for-organisations/documents/4019538/international-data-transfer-agreement.pdf, issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 5.4 of those Mandatory Clauses ("**UK IDTA**"), shall apply. The information required for Tables 1 to 3 of Part One of the IDTA is set out in Schedules 1 and 3 of this DPA (as applicable). The information required for Table 4 is of Part One of the IDTA is set forth in Annex II of the Standard Contractual Clauses. For the purposes of UK Transfers, the UK IDTA shall be governed by the laws of England and Wales.

12. MISCELLANEOUS.

12.1 **Notices.** All notices and communications given under this DPA shall be made in accordance with Section 11 of the Principal Agreement.

12.2 **Liability and Indemnification.** The liability of each party to this DPA, arising out of or related to this DPA, whether in contract, tort or under any other theory of liability, shall be subject to the limitations or exclusions of liability set out in Section 8 of the Principal Agreement entitled ["Limitation of Liability."] Furthermore, the terms of indemnification by both Parties shall be governed by Section 7 of the Principal Agreement entitled "Indemnification" as appropriate. For the avoidance of doubt, this Section 12.2 does not affect any liability under applicable Data Protection Laws, in particular Article 82 GDPR.

12.3 **Order of Precedence.** In the event of inconsistencies between the provisions of this DPA and any other agreements between the Parties, including the Principal Agreement and agreements entered into or purported to be entered into after the date of this DPA (except where explicitly agreed otherwise in writing, signed on behalf of the parties), the provisions of this DPA shall prevail. For the avoidance of doubt, this does not apply to the Standard Contractual Clauses attached as Schedule 3; the Standard Contractual Clauses shall prevail in case of any conflict.

12.4 **Governing Law.** Notwithstanding Sections 7 and 9 of the Standard Contractual Clauses, this DPA is governed by the laws of the country or territory stipulated for this purpose in Section 11 of the Principal Agreement.

12.5 **Term and Termination.** The term of this DPA shall commence on the Effective Date of this DPA and shall be coterminous with the Principal Agreement in accordance with Section 10 of the Principal Agreement.

12.6 **Amendment.** This DPA is subject to the applicable terms for amendment set forth in Section 11 of the Principal Agreement.

SCHEDULE 1 – DETAILS OF THE PROCESSING

This Schedule includes certain details of the processing of Customer Personal Data as required by Article 28(3) GDPR.

Subject matter and duration of the processing of Customer Personal Data

The subject matter and duration of the processing of the Customer Personal Data are set out in the Principal Agreement and this DPA.

The nature and purpose of processing of Customer Personal Data

Data Processor will process Customer Personal Data as necessary to perform the Services under the Principal Agreement, as further specified in the applicable Project Addendum or Statements of Work, and as further instructed by the Customer in the use of the Services.

The types of Customer Personal Data to be processed

Customer may submit Customer Personal Data to Data Processor for the provision of the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

Business contact information for investment firms, portfolio companies, and other participants in the public and private markets. Analytics of usage of the Novata platform by customers.

The categories of Data Subject to whom the Customer Personal Data relates

Customer may submit Personal Data to Data Processor for the provision of the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

Contacts at investment firms, portfolio companies, and other participants in the public and private markets.

The obligations and rights of the Customer

The obligations and rights of the Customer are set out in the Principal Agreement and this DPA.

SCHEDULE 2 – APPROVED SUBPROCESSORS

Novata Group Entity acting as Data Processor uses certain subprocessors to support the delivery of the Novata services.

The current list of subprocessors can be found at:

www.novata.com/subprocessors

SCHEDULE 3 – STANDARD CONTRACTUAL CLAUSES

Controller to Processor

SECTION I

Clause 1 **Purpose and scope**

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) ([1]) for the transfer of data to a third country.

(b) The Parties:

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

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

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

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

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

Clause 2 **Effect and invariability of the Clauses**

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

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

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

Clause 3 **Third-party beneficiaries**

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

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

(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

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

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

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

Clause 4 **Interpretation**

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

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

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

Clause 5 **Hierarchy**

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

Clause 6 **Description of the transfer(s)**

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

Clause 7 **Docking clause**

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

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

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

SECTION II **– OBLIGATIONS OF THE PARTIES**

Clause 8 **Data protection safeguards**

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

8.1 **Instructions**

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 **Purpose limitation**

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 **Transparency**

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets

or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 **Accuracy**

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 **Duration of processing and erasure or return of data**

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 **Security of processing**

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter '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 purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

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

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all 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.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 **Sensitive data**

Where the transfer 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 (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 **Onward transfers**

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union ([2]) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefiting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

[2] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 **Documentation and compliance**

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for 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 audit, the data exporter may take into account relevant certifications held by the data importer.

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

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9 **Use of sub-processors**

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least two weeks in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. ([3]) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor

[3] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

complies with the obligations to which the data importer is subject pursuant to these Clauses.

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

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

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

Clause 10 **Data subject rights**

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

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11 **Redress**

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

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12 **Liability**

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

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

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

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

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

Clause 13 **Supervision**

(a) Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

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

Clause 14 **Local laws and practices affecting compliance with the Clauses**

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

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

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and

format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards ([4]);

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

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

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

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

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data

[4] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15 **Obligations of the data importer in case of access by public authorities**

15.9 **Notification**

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

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

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

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

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

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

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

15.10 **Review of legality and data minimisation**

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When

challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

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

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16 Non-compliance with the Clauses and termination

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

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

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

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

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

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

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

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure

compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

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

Clause 17 **Governing law**

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

Clause 18 **Choice of forum and jurisdiction**

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Ireland.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

Name: Customer, as defined in the Data Processing Agreement and the Terms and Conditions.

Address: The Customer's address.

Activities relevant to the data transferred under these Clauses: the Processing of Personal Data in connection with the Customer's use of Novata Services under the Novata Terms and Conditions.

Role (controller/processor):

Controller

Data importer(s):

Name: Novata, Inc.

Address: 54 W 21st St., Ste. 1201 / New York, NY 10010 / USA

Contact person's name, position and contact details: Elizabeth Meyer / Chief Legal Officer / beth.meyer@novata.com

Activities relevant to the data transferred under these Clauses: the Processing of Personal Data in connection with the Customer's use of Novata Services under the Novata Terms and Conditions.

Role (controller/processor):

Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Contacts at investment firms, banks, portfolio companies, private companies, and other participants in the public and private markets.

Categories of personal data transferred

Business contact information for investment firms, banks, portfolio companies, private companies, and other participants in the public and private markets. Analytics of usage of the Novata platform by customers.

Sensitive data transferred (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.

N/A

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Continuous

Nature of the processing

Personal Data will be Processed in accordance with the Terms and Conditions and Data Processing Agreement.

Purpose(s) of the data transfer and further processing

The Processing of Personal Data in connection with the Customer's use of Novata Services under the Novata Terms and Conditions.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Novata retains personal information necessary to fulfill the purpose for which that information was collected or as required or permitted by law. Novata does not retain personal information longer than is necessary for Novata to achieve the purposes for which it was collected. When Novata destroys your personal information, Novata does so in a way that prevents that information from being restored or reconstructed.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

Novata works with providers of infrastructure services, professional services, and software development services. In the case of infrastructure services, business contact information and user analytics may flow through these systems as an incidental part of the provision of these infrastructure services. In the case of professional services and software development services, these suppliers may have access to systems where business contact information and user analytics reside. Data shall be retained for as long as reasonably necessary to deliver the Services to the Exporter, to fulfill the purposes described in the Terms and Conditions, or as required by law, subject to the applicable terms of the Data Processing Agreement.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

The authority competent at the location of Customer's main establishment in the United Kingdom and/or European Union.

ANNEX II

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

This Annex II contains a description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Novata maintains an enterprise security program, established and overseen by a dedicated team of professionals with expertise in information security, cyber security and data privacy. This program is aligned with the ISO 27001:2022 and SOC 2 security, availability and confidentiality principles. Robust security infrastructure, policies, and related processes are implemented across the Novata Group.

All Novata Group entities handling client data must adhere to the principles of this enterprise security program, including its policies, controls, and minimum security requirements.

I. Physical Security

a. Novata relies upon Microsoft Azure to manage the physical access to their data centers as attested to by 3rd party audits.

b. Novata does not maintain a dedicated physical office location where any processing or sub-processing will occur.

c. Novata does not physically retain any data sets or processing functions outside of the core digital platform.

d. Novata does not authorize or support the use of general access accounts or terminals, with all devices associated to a single individual.

II. Technical Security

a. Access to any service or system requires a unique identity to be provisioned based upon a multi-step approval workflow involving Novata HR, Novata IT, Novata Security and the hiring manager prior to any identity creation.

b. All services and data management functions are reviewed on defined schedule for internal and external cyber risk factors.

c. All services and devices under the management of Novata are required to enforce data encryption at rest and in transit.

d. All devices utilized in the delivery of Novata services and subject to this data processing agreement are inventoried, managed and assessed for cyber hygiene by Novata Security leveraging both manual and automated methods.

e. All identities and associated access is assigned based upon a single user object, with no shared user accounts, requiring password complexity, length, and regular rotation enforced by automated policy.

f. All technical actions that involve interactions or access to data being processed by Novata are logged and recorded with records retained for at least 1 year (or longer).

g. All devices regardless of function that connect to any Novata platform system or supporting function are required to run anti-malware software that is managed and monitored by Novata Security.

h. Regular testing of systems and platform recovery are conducted on a recurring basis to ensure the ability to restore services in the event of an unplanned outage arising from a supplier failure, security event, or malicious activity.

III. Organizational Security

a. All employees, contractors, associates, and affiliates are required to undergo information security awareness training upon hire and annually thereafter

b. All employees, contractors, associates, and affiliates with a need to carry out data processing are trained on the methods for handling data upon hire and annually thereafter.

c. All employees, contractors, associates, and affiliates are required to acknowledge and adhere to published information security and data privacy policies maintained by Novata upon hire and annually thereafter.

d. All policies are reviewed and amended as required, or on an annual basis, whichever is sooner.

e. Security and Data Privacy risk assessment, treatment, and mitigation practices are conducted on a continual basis to ensure visibility and proactive management of risks associated with data loss, destruction, alteration or disclosure

f. Novata, Inc. engages independent auditors at least annually to assess the enterprise security program's adherence to internal policies, controls and practices aligned to ISO 27001:2022 and the SOC 2 Trust Services Criteria.

These audits are performed at the Novata group level and/or for Novata entities that are in scope for certification. Subsidiaries that are not currently certified operate under the same enterprise security program and are subject to internal reviews to ensure conformity with Novata's security policies and control requirements.

IV. Sub-processors

a. Novata enforces by contractual obligation that all sub-processors adhere to the same or more stringent protective measure and requirements for all sub-processors as outlined under the above description of security measures that apply to Novata.

ANNEX III

N/A, in accordance with General Authorization

ANNEX IV – ADDITIONAL DETERMINATIONS

Regarding Clause 7 – Optional Docking Clause

- The parties hereby include Clause 7.

Regarding Clause 9 – Use of sub-processors

- The parties select **Option 2: General Written Authorization.**
- The data importer shall submit notification of new sub-processors at least **two (2) weeks** prior to the engagement of the sub-processor to provide data controllers the opportunity to object.

Regarding Clause 11– Redress

- The **Option** under (a) was intentionally left blank and shall not apply.

Regarding Clause 17 – Governing Law

- The parties select **Option 1**.
- The parties agree that these Clauses shall be governed by the **laws of Ireland**.

Regarding Clause 18 – Choice of forum and jurisdiction

- The parties agree that any dispute arising from these Clauses shall be resolved by **the courts in Ireland**.