NORAMI

Data Processing Addendum

✦ EU Standard Contractual Clauses

Module Two — Controller to Processor

EXECUTION MASTER

This version may be pre-signed by AI BLU, LLC. It becomes binding for a customer only when the customer-specific fields in Annex I are completed and Annex I is signed or validly accepted electronically.

Document	Details
Version	2026-07-15
Processor / data importer	AI BLU, LLC (operating Norami)
Registered address	131 Continental Drive, Suite 305, Newark, Delaware 19713, United States
Privacy contact	privacy@norami.ai
SCC module	Module Two — controller to processor
SCC law and forum	Ireland; courts of Ireland

Customer completion fields

- Exact legal business name, registered or principal business address, and authorised contact.
- Competent EEA supervisory authority under SCC Clause 13.
- Signature or electronic acceptance record, with document version and server-recorded timestamp.

Business-to-business use • EEA-established controllers • GDPR / EU SCC package

Data Processing Addendum

This Data Processing Addendum ("DPA") forms part of the agreement governing the customer's use of Norami (the "Agreement") between the customer identified in Annex I ("Customer" or "Controller") and AI BLU, LLC, a Delaware limited liability company operating Norami ("AI BLU" or "Processor"). It applies where AI BLU processes Customer Personal Data on the Customer's behalf and that processing is governed by Regulation (EU) 2016/679 ("GDPR").

Norami is offered only for business and professional use. For self-service purchases, the person accepting this DPA represents that they are at least 18 years old and authorised to bind the business identified in Annex I. UK and Swiss transfer terms are outside this version.

1. Scope and roles

1.1 Customer is the controller and AI BLU is the processor for Customer Personal Data placed in the Customer workspace or otherwise submitted for processing through Norami. Each party will comply with the obligations that apply to it under Data Protection Law.

1.2 AI BLU acts separately as an independent controller for account registration, contracting, billing, service administration, security, fraud prevention, and support data for which it determines the purposes and essential means. That separate processing is governed by Norami's privacy notice and is outside this DPA.

1.3 "Customer Personal Data" means personal data processed by AI BLU on Customer's behalf under the Agreement. "Data Protection Law" means the GDPR and applicable EEA data-protection laws. Terms such as personal data, processing, controller, processor, and data subject have the meanings given in the GDPR.

2. Processing details

The subject matter, duration, nature and purpose of the processing, the categories of personal data, and the categories of data subjects are described in SCC Annex I.B. Processing generally covers hosting, structuring, AI-assisted querying, answer generation, export, and deletion of business data submitted by Customer for the duration of the Agreement and the deletion period.

Norami is not intended for special-category data under GDPR Article 9 or data relating to criminal convictions and offences under Article 10. Customer must not submit such data unless AI BLU first approves the processing in writing and the parties document appropriate additional safeguards.

3. Documented instructions

3.1 AI BLU will process Customer Personal Data only on Customer's documented instructions, including the Agreement, this DPA, the completed SCC Appendix, and Customer's use of the platform controls, including with respect to transfers, unless processing is required by Union or Member State law. Where legally permitted, AI BLU will inform Customer before carrying out processing required by law.

3.2 AI BLU will immediately inform Customer if, in its opinion, an instruction infringes Data Protection Law. AI BLU will not use Customer Personal Data to train its own or a third party's general-purpose artificial-intelligence models.

4. Confidentiality

AI BLU will ensure that persons authorised to process Customer Personal Data are subject to a binding duty of confidentiality and receive access only as necessary to provide, secure, support, or administer the service in accordance with Customer's instructions.

5. Security

5.1 Taking into account the state of the art, implementation costs, and the nature, scope, context, and purposes of processing, AI BLU will implement and maintain appropriate technical and organisational measures designed to protect Customer Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or access. The current measures are described in SCC Annex II.

5.2 AI BLU may update the measures to reflect technical progress and service changes, provided the overall level of protection is not materially reduced during the term.

6. Sub-processors

6.1 Customer gives AI BLU general written authorisation to engage the sub-processors listed in SCC Annex III. AI BLU will give Customer at least 10 business days' prior notice of an intended addition or replacement. Customer may object on reasonable data-protection grounds during that period. The parties will work in good faith to resolve the objection; if no reasonable alternative is available, Customer may terminate the affected service without penalty.

6.2 AI BLU will impose data-protection obligations on each sub-processor that provide at least the level of protection required by this DPA for the processing it performs. AI BLU remains fully liable to Customer for each sub-processor's performance of those obligations.

7. Data-subject rights

7.1 Taking into account the nature of the processing, AI BLU will assist Customer by appropriate technical and organisational measures, insofar as possible, to respond to requests to exercise data subject rights under Chapter III of the GDPR. Available controls include workspace export, correction through data refresh or re-upload, dataset deletion, and workspace deletion.

7.2 If AI BLU receives a request directly concerning Customer Personal Data, it will notify Customer without undue delay and will not respond except on Customer's instructions or as required by law. AI BLU will provide reasonable additional assistance, taking into account the nature of the processing and the information available to it.

8. Personal data breaches

8.1 AI BLU will notify Customer without undue delay after becoming aware of a personal data breach affecting Customer Personal Data. The notice will include, as information becomes reasonably available, the nature of the breach; the categories and approximate numbers of affected data subjects and records; likely consequences; measures taken or proposed; and a contact point for more information.

8.2 Information may be provided in phases. AI BLU will take reasonable steps to contain and remediate the breach and will reasonably assist Customer with notifications to supervisory authorities and data subjects. Notification is not an acknowledgement of fault or liability.

9. DPIAs and prior consultation

Taking into account the nature of processing and the information available to it, AI BLU will provide reasonable assistance with Customer's obligations under GDPR Articles 32 to 36, including data protection impact assessments and prior consultation with a supervisory authority.

10. Return and deletion

10.1 During the term, Customer may export workspace data in available portable formats. At the end of the services, AI BLU will, at Customer's choice and subject to the Agreement, return Customer Personal Data or delete it after a 30-day revocable deletion period, including tenant-scoped database records, storage objects, vector embeddings, and derived workspace artefacts, and will provide deletion confirmation. Customer may cancel deletion during the grace period.

10.2 AI BLU may retain personal data after termination only where required by applicable law or where AI BLU processes limited account, billing, security, or legal-claims records in its separate controller role. Any Customer Personal Data retained because deletion is legally prohibited will be isolated from further processing and deleted when the legal requirement ends. Provider-managed backups age out under the applicable backup-retention cycle.

11. Information and audits

11.1 AI BLU will make available information reasonably necessary to demonstrate compliance with GDPR Article 28 and will allow for and contribute to audits, including inspections, by Customer or an independent auditor mandated by Customer. The parties will first use current documentation, written responses, and available third-party reports where these reasonably address the requested scope.

11.2 Routine audits require 30 days' prior notice, will occur during normal business hours, will avoid unreasonable disruption, and are limited to once in a 12-month period. Those limits do not apply where a competent supervisory authority requires an audit, following a confirmed personal data breach, or where Customer reasonably suspects material non-compliance. Auditors must protect confidential information and may not access data belonging to other customers. Nothing in this section limits the audit rights in the SCCs.

12. International transfers

12.1 The primary restricted transfer covered by this package is from an EEA-established Customer to AI BLU in the United States. The parties enter into the EU Standard Contractual Clauses adopted by Commission Implementing Decision (EU) 2021/914, Module Two (controller to processor), as selected and completed in this package. The SCCs are incorporated into and form part of this DPA.

12.2 AI BLU may make authorised onward transfers using a valid transfer mechanism, including an applicable adequacy decision, an active EU-US Data Privacy Framework certification that covers the transfer, or appropriate contractual safeguards. AI BLU's owner may remotely administer the service from Chile as personnel of the same US Processor entity. No separate Chilean company or importer exists; such access remains subject to this DPA, the SCCs, confidentiality duties, and the measures in Annex II.

13. Order of precedence and liability

If this DPA conflicts with the Agreement on the processing of Customer Personal Data, this DPA prevails. If any provision of the Agreement or this DPA conflicts with the SCCs, the SCCs prevail. No limitation or exclusion of liability in the Agreement applies to the extent it would contradict SCC Clause 12 or restrict enforceable data-subject rights under the SCCs.

14. Term and execution

14.1 This DPA takes effect on the date the last required party signs or validly accepts it and remains in effect while AI BLU processes Customer Personal Data. Obligations that by their nature survive termination, including confidentiality, deletion, audit, liability, and the SCCs, will survive.

14.2 For self-service execution, the customer-specific fields in SCC Annex I may be completed by the order or checkout acceptance record incorporated into this package. That record must identify the Customer's exact legal name and address, the authorised person, the competent supervisory authority, the accepted document version, and the server-recorded acceptance date and time. For negotiated agreements, the parties may execute counterparts and electronic signatures.

EU Standard Contractual Clauses

Commission Implementing Decision (EU) 2021/914

Selected Module: MODULE TWO — Transfer controller to processor

SCC item	Selection
Clause 7	Docking clause included
Clause 9(a)	Option 2 — general written authorisation; 10 business days' notice
Clause 11(a)	Optional independent redress body not selected
Clause 13	Authority responsible for the EEA-established exporter; completed in Annex I.C
Clause 17	Option 1; law of Ireland
Clause 18	Courts of Ireland

The following clauses are reproduced from the European Commission's official English template. Only the adaptations permitted by the template have been made: selection of Module Two and the stated options, deletion of non-applicable modules/options, completion of bracketed selections, and completion of the Appendix.

EUROPEAN
COMMISSION

Brussels, 4.6.2021
C(2021) 3972 final

ANNEX

ANNEX

to the

COMMISSION IMPLEMENTING DECISION

on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council

ANNEX

STANDARD CONTRACTUAL CLAUSES

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 personal data to a third country.

(b) The Parties:

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

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

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

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

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

Clause 2

Effect and invariability of the Clauses

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

[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 of 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 […].

provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

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

Clause 3

Third-party beneficiaries

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

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

(ii) Clause 8 - Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 - Module Two: Clause 12(a), (d) and (f);

(v) Clause 13;

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

(vii) Clause 16(e);

(viii) Clause 18 - Module Two: Clause 18(a) and (b).

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

Clause 4

Interpretation

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

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

(e) 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 - Optional

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.

MODULE TWO: Transfer controller to processor

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 the 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 benefitting 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;

[2] This requires rendering the data anonymous in such a way that the individual is no longer identifiable by anyone, in line with recital 26 of Regulation (EU) 2016/679, and that this process is irreversible.

(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

(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

MODULE TWO: Transfer controller to processor

OPTION 2: GENERAL WRITTEN AUTHORISATION 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 10 business days 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.

(f) 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] 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.

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

(g) 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.

(h) 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.

(i) 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

MODULE TWO: Transfer controller to processor

(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.

MODULE TWO: Transfer controller to processor

(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

MODULE TWO: Transfer controller to processor

(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

MODULE TWO: Transfer controller to processor

(a) 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.

(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

MODULE TWO: Transfer controller to processor

(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 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

MODULE TWO: Transfer controller to processor

15.1 Notification

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

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

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of

[4] 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.

destination; such notification shall include all information available to the importer.

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

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

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

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

15.2 Review of legality and data minimisation

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

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

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

MODULE TWO: Transfer controller to processor

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

MODULE TWO: Transfer controller to processor

(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.

APPENDIX

This Appendix forms an integral part of the Clauses. Customer-specific information may be supplied in an incorporated Order Form or Customer Acceptance Record, provided the executed copy clearly identifies the relevant transfer, parties, roles, supervisory authority, document version, and date.

ANNEX I

A. LIST OF PARTIES

Data exporter — Customer (controller)

Required field	Customer-specific information
Name	[Exact legal business name — Order Form or Customer Acceptance Record]
Address	[Registered or principal business address — Order Form or Customer Acceptance Record]
Contact	[Authorised person's name, position, email, and other contact details]
Relevant activities	Use of Norami for business analytics and AI-assisted querying of Customer-controlled workspace data.
Role	Controller / data exporter

Negotiated agreement **Signature:** _____ **Name:** _____ **Title:** _____ **Date:** _____	**Self-service electronic acceptance** **Acceptance record ID:** _____ **Authorised person:** _____ **Version:** 2026-07-15 **UTC timestamp:** _____

Data importer — AI BLU, LLC (processor)

Field	Information
Name	AI BLU, LLC, operating Norami
Address	131 Continental Drive, Suite 305, Newark, Delaware 19713, United States
Contact	Andrés Parodi, Managing Member — privacy@norami.ai
Relevant activities	Hosting, structuring, AI-assisted querying, answer generation, export, support, security, and deletion of Customer Personal Data.
Role	Processor / data importer

For AI BLU, LLC

Signature: Andrés Parodi

Name: Andrés Parodi

Title: Managing Member

Date: 15/07/2026

B. DESCRIPTION OF TRANSFER

Item	Completed description
Categories of data subjects	Customer's employees, workers, contractors, applicants, authorised users, customers and prospects who are natural persons, suppliers and service-provider contacts, and other individuals whose personal data Customer lawfully includes in workspace content.
Categories of personal data	Identification and business-contact data; professional, role, employment, and organisational data; customer and supplier records; operational, transactional, sales, production, and financial-business data; communications, questions, chat content, file contents, and other personal data included by Customer in submitted business datasets.
Sensitive data	None intended or authorised by default. Customer must not submit GDPR Article 9 special-category data or Article 10 criminal-conviction/offence data unless AI BLU approves the processing in writing and the parties document appropriate access restrictions, purpose limitations, and other additional safeguards before transfer.
Frequency	Continuous or intermittent, as initiated by Customer and its authorised users during the service term.
Nature of processing	Collection by transmission; hosting; storage; organisation; structuring; retrieval; consultation; AI-assisted analysis; generation of answers and embeddings; export; restriction; and deletion.
Purposes	Provide, secure, maintain, support, and improve the operation of the contracted Norami service on Customer's documented instructions; enable Customer to query and analyse its business data and receive generated answers.
Retention	For the service term, followed by a 30-day revocable deletion period. Temporary chat attachments are retained for 30 days and export artefacts for 7 days. Provider-managed backup copies age out under the applicable backup-retention cycle. Limited account, billing, security, and legal-claims records processed by AI BLU as an independent controller are outside this transfer description.
Subject matter, nature, duration	Processing of Customer-controlled workspace content for the purposes above, for the Agreement term plus the applicable deletion period.
Onward transfers	To the authorised sub-processors in Annex III, only for the stated functions and using an applicable adequacy decision, Data Privacy Framework certification, SCCs, or another valid transfer mechanism.

C. COMPETENT SUPERVISORY AUTHORITY

The supervisory authority responsible for ensuring the EEA-established data exporter's compliance with Regulation (EU) 2016/679 for the transfer, determined in accordance with Clause 13:

Required field	Customer-specific information
Authority	[Full name and country of the competent EEA supervisory authority — complete before execution]

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES

The following measures apply to the Module Two transfer. They are implemented by AI BLU and, where stated, by infrastructure sub-processors. Measures may evolve, but the overall level of protection will not be materially reduced during the service term.

Tenant isolation

Customer data is logically separated by tenant. PostgreSQL row-level security policies enforce tenant scope at the database layer; application queries and storage paths are tenant-scoped.

Identity and access

Authentication is provided through Supabase Auth. Role- and department-based controls limit workspace access. Privileged operations require multi-factor authentication and step-up checks. Administrative access is limited to authorised personnel on a need-to-know basis.

Encryption and transmission

HTTPS/TLS protects data in transit between users, the application, infrastructure services, and model providers. Supabase/AWS and other hosting providers encrypt stored data at rest using provider-managed encryption.

Logging and monitoring

Security-relevant actions are recorded in a tenant-scoped append-only audit ledger with SHA-256 hash chaining. Audit records have bounded 730-day retention with integrity-preserving purge anchors. Application error reports and operational logs are designed to exclude or redact customer data literals; generated-code stdout and stderr content is withheld from worker logs.

Data minimisation

The service processes only content submitted or selected by Customer for the requested operation. AI model calls are limited to content needed for the request rather than routine transmission of entire datasets. Customer content is not used to train AI BLU's or third-party general-purpose models.

Sandboxed analysis

Customer-directed code analysis runs in isolated, short-lived sandboxes. Input is limited to the requested task, sandbox credentials are scoped, and the sandbox is terminated after execution.

Retention and deletion

Tenant deletion uses a 30-day revocable grace period followed by a census-driven purge of tenant-scoped database records, storage objects, vector embeddings, derived artefacts, and associated billing-customer linkage, with an erasure certificate. Unconfirmed uploads expire after 24 hours; temporary chat attachments after 30 days; export artefacts after 7 days.

Availability and recovery

Service availability and infrastructure recovery use managed hosting and database-provider controls. Data purged from the live service ages out of provider-managed backups under the applicable backup-retention cycle.

Incident response

AI BLU maintains an incident-response procedure covering detection, containment, investigation, evidence preservation, remediation, and customer notification without undue delay. Provider security notices and audit-chain integrity checks are monitored as incident inputs.

Confidentiality and personnel

Authorised personnel are subject to confidentiality obligations. Access to Customer Personal Data is restricted to what is necessary to provide, secure, support, or administer the service and is audit-logged.

Sub-processor governance

AI BLU reviews sub-processor data-protection terms, imposes equivalent protection obligations, maintains a current list, gives at least 10 business days' notice of changes, and uses a valid transfer mechanism for restricted onward transfers.

Assistance and accountability

Workspace export, correction, dataset deletion, account/workspace deletion, audit evidence, incident information, and data-protection contact channels support Customer's GDPR obligations and data-subject requests.

ANNEX III

AUTHORISED SUB-PROCESSORS

Customer gives general written authorisation for the following sub-processors under Clause 9(a), Option 2. Only the data necessary for the stated function is disclosed. The current public register is available at app.norami.ai/subprocessors.

Sub-processor	Function	Processing location
Anthropic, PBC	AI model processing and answer generation	United States
OpenAI OpCo, LLC and applicable affiliates	AI model processing and text embeddings	United States
FoundryLabs, Inc. (E2B)	Isolated code-execution sandboxes for data analysis	United States; provider-managed cloud
Supabase, Inc.	Database, authentication, and file storage	United States; US East
Vercel Inc.	Application hosting, serverless compute, and content delivery	United States (Washington, D.C. / iad1) and global edge
Railway Corporation	Spreadsheet-ingestion worker	United States (Virginia / US East)
Cloudflare, Inc.	DNS, network security, content delivery, and secure ingestion tunnel	Global
Functional Software, Inc. (Sentry)	Application error monitoring using scrubbed reports	United States
Stripe, LLC	Payment processing and subscription billing	United States
Plus Five Five, Inc. (Resend)	Transactional email delivery	United States
Perplexity AI, Inc.	Optional public-web business-context research during onboarding	United States

Infrastructure note: some sub-processors use their own approved infrastructure providers, including Amazon Web Services and other providers disclosed in their sub-processor registers. AI BLU remains responsible for its obligations under this DPA and the SCCs.