

Novara International, 30 N Gould St Ste N, Sheridan, WY 82801 USA

Last updated: December 4, 2025

This Data Processing Addendum ("DPA") forms part of the Terms of Service or other agreement governing the use of the Novara platform (the "Agreement") between:

- (1) The Novara customer identified in the Agreement ("Customer", "Controller"); and
- (2) Novara International ("Novara", "Processor").

Customer and Novara are together referred to as the "Parties" and individually as a "Party".

1. Purpose and Scope

1.1 This DPA applies to Novara's Processing of Personal Data on behalf of Customer in connection with the provision of the Services under the Agreement.

1.2 The Parties intend this DPA to satisfy the requirements of applicable Data Protection Laws, including (where applicable) the EU and UK General Data Protection Regulation ("GDPR"), in respect of the Processing of Personal Data.

1.3 In the event of any conflict between this DPA and the Agreement, this DPA shall prevail with respect to the subject matter herein.

2. Definitions

2.1 "Controller", "Processor", "Data Subject", "Personal Data", "Personal Data Breach", and "Processing" have the meanings given in the GDPR.

2.2 "Data Protection Laws" means all laws and regulations relating to data protection and privacy applicable to the Processing of Personal Data under the Agreement, including, where applicable, the GDPR, the UK GDPR and Data Protection Act, and similar laws.

2.3 "Services" means the services provided by Novara to Customer under the Agreement, including the Novara sourcing and collaboration platform.

2.4 "Sub-Processor" means any third party engaged by Novara to Process Personal Data on behalf of Customer in connection with the Services.

3. Roles of the Parties

3.1 For the purposes of Data Protection Laws, Customer is the Controller and Novara is the Processor with respect to the Processing of Personal Data described in Annex 1.

3.2 Customer determines the purposes and means of Processing of Personal Data. Novara shall Process Personal Data only on behalf of Customer and in accordance with this DPA and Customer's documented instructions.

4. Customer Responsibilities

4.1 Customer is responsible for ensuring that:

- (a) it has a valid legal basis for Processing the Personal Data and for authorizing Novara to Process the Personal Data on its behalf;
- (b) the instructions it provides to Novara comply with Data Protection Laws;
- (c) Data Subjects are provided with all information required by Data Protection Laws.

4.2 Customer shall not instruct Novara to Process Personal Data in a manner that would cause Novara to breach Data Protection Laws. Novara may inform Customer if, in its opinion, an instruction infringes Data Protection Laws.

5. Novara's Obligations

Novara shall:

5.1 Process Personal Data only on documented instructions from Customer, including with regard to transfers of Personal Data to a third country, unless required to do so by applicable law. In such case, Novara shall inform Customer of that legal requirement unless the law prohibits such information.

5.2 Ensure that persons authorized to Process Personal Data are subject to appropriate confidentiality obligations.

5.3 Implement and maintain appropriate technical and organizational measures to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access, as described in Annex 2, taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of Processing.

5.4 Assist Customer, taking into account the nature of the Processing and the information available to Novara, in fulfilling Customer's obligations to respond to Data Subjects' requests to exercise their rights under Data Protection Laws.

5.5 Assist Customer in ensuring compliance with Customer's obligations relating to security of Processing, Personal Data Breach notifications, data protection impact assessments, and prior consultation with supervisory authorities, taking into account the nature of the Processing and the information available to Novara.

5.6 Notify Customer without undue delay after becoming aware of a Personal Data Breach affecting Personal Data Processed on behalf of Customer. Such notification shall describe, to the extent reasonably possible:

- (a) the nature of the Personal Data Breach;
- (b) the categories and approximate number of Data Subjects and data records concerned;
- (c) the likely consequences of the Personal Data Breach; and
- (d) measures taken or proposed to address the Personal Data Breach.

5.7 At Customer's choice, delete or return all Personal Data to Customer after the end of the provision of the Services relating to Processing, and delete existing copies unless applicable law requires storage of the Personal Data.

5.8 Make available to Customer all information necessary to demonstrate compliance with this DPA and allow for and contribute to audits, including inspections, conducted by Customer or an auditor mandated by Customer, as described in Section 8.

6. Sub-Processors

6.1 Customer authorizes Novara to engage Sub-Processors to Process Personal Data in connection with the Services. A current list of categories of Sub-Processors may be provided in the Agreement, on Novara's website, or upon request.

6.2 Novara shall:

- (a) ensure that any Sub-Processor is bound by a written contract imposing data protection obligations no less protective than those set out in this DPA; and
- (b) remain responsible to Customer for the performance of its Sub-Processors' obligations.

6.3 Novara may add or replace Sub-Processors from time to time. Novara shall notify Customer of any intended changes concerning the addition or replacement of Sub-Processors, thereby giving Customer the opportunity to object on reasonable grounds relating to data protection. If Customer reasonably objects and the Parties cannot agree on a solution, Customer may terminate the relevant Services on written notice.

7. International Transfers

7.1 Novara may Process and transfer Personal Data in and to countries outside the country in which Customer or the Data Subjects are located, including to the United States, Singapore, and other jurisdictions where Novara or its Sub-Processors operate.

7.2 Where required by Data Protection Laws for transfers of Personal Data from the EEA, UK, or Switzerland to countries that do not provide an adequate level of protection, the Parties shall ensure that appropriate safeguards are in place, such as the use of standard contractual clauses or an equivalent transfer mechanism.

7.3 Upon request, Novara shall provide Customer with details of the relevant transfer mechanism used for such transfers.

8. Audits

8.1 Customer may, at its own expense and no more than once in any twelve-month period, conduct or mandate a reasonable audit of Novara's compliance with this DPA, in accordance with this Section.

8.2 Before initiating any audit, Customer shall:

- (a) provide at least thirty (30) days' prior written notice to Novara;
- (b) submit a detailed audit plan describing the proposed scope, duration, and start date; and
- (c) ensure that the audit will not unreasonably interfere with Novara's business operations or the security of its systems.

8.3 Novara may satisfy audit obligations under this Section by providing industry-standard third-party audit reports or certifications (such as SOC 2, ISO 27001, or similar) that demonstrate Novara's compliance with applicable data protection and security obligations.

9. Duration and Termination

9.1 This DPA shall remain in effect for as long as Novara Processes Personal Data on behalf of Customer under the Agreement.

9.2 Termination of the Agreement shall automatically terminate this DPA, subject to the obligations in Section 5.7 relating to deletion or return of Personal Data.

10. Liability

10.1 The Parties' respective liability arising out of or related to this DPA shall be subject to the limitations and exclusions of liability set out in the Agreement, unless otherwise mandated by Data Protection Laws.

10.2 Nothing in this DPA shall limit a Data Subject's rights under Data Protection Laws.

11. Governing Law and Jurisdiction

11.1 This DPA shall be governed by and construed in accordance with the laws governing the Agreement, including any choice of law provisions.

11.2 Any disputes arising out of or in connection with this DPA shall be resolved in accordance with the dispute resolution provisions of the Agreement.

ANNEX 1 – DETAILS OF PROCESSING

Subject matter

Novara Processes Personal Data in order to provide the Services described in the Agreement, including the operation of the sourcing and collaboration platform, RFQ management, messaging, shipment tracking, and related functionality.

Duration

For the term of the Agreement and any additional period during which Novara retains Personal Data in accordance with the Agreement and this DPA.

Nature and purpose of Processing

- Hosting and storage of account and profile data
- Transmission and storage of RFQs, orders, and communications
- Provision of analytics and reporting

- Security monitoring, logging, and incident response
- Support, troubleshooting, and platform improvement

Types of Personal Data

- Business contact details (name, email, phone)
- Job title and role
- Company affiliation and address
- Login credentials and identifiers
- Usage and technical data (IP address, device and browser data)
- Communications and information contained in RFQs and related documents

Categories of Data Subjects

- Employees, contractors, and representatives of Customer
- Employees, contractors, and representatives of Buyers, Manufacturers, and Logistics Providers
- Other individuals whose personal data may be included in RFQs, communications, or documentation uploaded to the Platform

ANNEX 2 – SECURITY MEASURES (SUMMARY)

Novara implements technical and organizational measures appropriate to the risk, which may include:

- Access controls and authentication mechanisms for staff and systems
- Encryption in transit for data exchanged over public networks
- Segmentation of production and test environments
- Regular backups and disaster recovery procedures
- Logging and monitoring of system activity
- Employee confidentiality agreements and security training
- Vendor due diligence and contractual safeguards for Sub-Processors