Data processing agreement

This is the signable copy of the DPA published at https://getcargo.io/dpa. Complete the signature page, or execute by DocuSign, Adobe Sign, or another electronic-signature tool.

Last Updated: 25 August 2026

This Data Processing Agreement ("**DPA**") is between GetCargo Inc. ("**Vendor**") and the customer that has entered into the Contract ("**Customer**"). Vendor is the "Provider" under Vendor's Terms of Service. This DPA forms part of the Contract and applies to Vendor's Processing of Customer Personal Data in connection with the services.

1. Background and scope

1.1 This DPA is supplemental to the service agreement, order form, or other written contract between the parties for the services (the "**Contract**"). If there is no separately signed Contract, Vendor's Terms of Service at https://getcargo.io/terms are the Contract.

1.2 This DPA applies only to the extent Vendor Processes Customer Personal Data in the course of providing the services under the Contract.

1.3 Order of precedence. If there is a conflict, the following documents prevail in this order: (a) the Standard Contractual Clauses, but only as to Restricted Transfers and only to the extent required by those Clauses; then (b) this DPA; then (c) the Contract. Notwithstanding the foregoing, the limitation of liability, damages waiver, and indemnification provisions of the Contract apply to all claims arising out of or relating to this DPA, including the Standard Contractual Clauses, as between the parties, and nothing in this DPA expands Vendor's liability to Customer beyond the Contract.

1.4 This DPA, together with the Contract, is the complete agreement between the parties as to the Processing of Customer Personal Data. It supersedes prior discussions and documents on that subject. Pre-contract statements, including verbal statements, are not part of this DPA unless expressly restated here.

2. Definitions

2.1 "**Adequacy Decision**" means a decision of the European Commission, or a corresponding decision under UK or Swiss law, that a country, territory, or sector ensures an adequate level of protection for Personal Data.

2.2 "**Controller**", "**Processor**", "**Data Subject**", "**Personal Data**", "**processing**" / "**Process**", and "**personal data breach**" have the meanings given in Data Protection Laws.

2.3 "**Customer Personal Data**" means Personal Data contained in Customer Content (as defined in the Contract) that Vendor Processes on Customer's behalf in providing the services. It does not include Personal Data that Vendor Processes as an independent Controller, such as account, billing, marketing, or vendor-management data about Customer's personnel that Vendor collects for its own business purposes.

2.4 "**Data Protection Laws**" means the laws applicable to a party's Processing of Customer Personal Data under the Contract, including European Data Protection Laws and US Data Protection Laws.

2.5 "**European Data Protection Laws**" means the GDPR, the UK GDPR, the Swiss Federal Act on Data Protection, and any implementing or successor legislation.

2.6 "**GDPR**" means Regulation (EU) 2016/679.

2.7 "**Personal Data Breach**" means a breach of Vendor's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data. It does not include unsuccessful attempts or activities that do not compromise the security of Customer Personal Data, such as unsuccessful log-in attempts, pings, port scans, denial-of-service attacks, or similar events.

2.8 "**Restricted Transfer**" means a transfer of Customer Personal Data that would be prohibited by European Data Protection Laws in the absence of a transfer mechanism such as an Adequacy Decision, the Standard Contractual Clauses, or the UK Addendum.

2.9 "**Standard Contractual Clauses**" or "**SCCs**" means the clauses annexed to European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, as amended or replaced.

2.10 "**Subprocessor**" means a third-party Processor engaged by Vendor to Process Customer Personal Data in order to provide the services. Subprocessor does not include (a) Vendor's internal productivity, finance, HR, or similar tools that do not Process Customer Personal Data to provide the services, (b) a cloud-provider feature that is not a separate Processor, or (c) a third party that Customer instructs Vendor to connect to, including Customer's own CRM, data warehouse, enrichment provider, model provider, or similar system (those parties are Customer's processors).

2.11 "**UK Addendum**" means the International Data Transfer Addendum issued by the UK Information Commissioner under section 119A(1) of the Data Protection Act 2018.

2.12 "**UK GDPR**" means the GDPR as it forms part of the law of the United Kingdom by virtue of section 3 of the European Union (Withdrawal) Act 2018.

2.13 "**US Data Protection Laws**" means applicable United States federal and state laws relating to the Processing of Personal Data, including the California Consumer Privacy Act as amended by the California Privacy Rights Act (together, the "**CPRA**"). "**Sell**" and "**Share**" have the meanings given in the applicable US Data Protection Laws.

Capitalized terms not defined in this DPA have the meanings given in the Contract.

3. Roles and instructions

3.1 Customer is a Controller of Customer Personal Data, or a Processor acting on behalf of a third-party Controller, as applicable. Vendor acts as Processor for Customer, and as Subprocessor where Customer is itself a Processor. Customer warrants that it is authorized to give instructions on behalf of any third-party Controller whose Personal Data is included in Customer Personal Data.

3.2 Vendor will Process Customer Personal Data only on documented instructions from Customer, unless applicable law requires otherwise, in which case Vendor will inform Customer before Processing unless the law prohibits that notice. The parties agree that the Contract, this DPA, and Customer's use and configuration of the services constitute Customer's complete documented instructions.

3.3 Customer may provide additional written instructions that are consistent with the Contract. If an additional instruction would materially change Vendor's Processing or security obligations, is not commercially reasonable, or requires resources beyond the ordinary operation of the services, it is effective only if the parties

agree in writing, including any additional fees and timelines.

3.4 Vendor will promptly inform Customer if, in Vendor's reasonable opinion, an instruction infringes Data Protection Laws. Vendor may suspend performance of that instruction until Customer confirms, withdraws, or modifies it.

3.5 Vendor will ensure that persons authorized to Process Customer Personal Data are bound by confidentiality and do not Process Customer Personal Data except as instructed in this DPA. Vendor will provide security awareness training and, where permitted by applicable law, conduct background verification for personnel with access to Customer Personal Data, in accordance with Vendor's standard practices.

3.6 Vendor represents that it has not knowingly created back doors or similar programming intended to facilitate unauthorized government access to Customer Personal Data, and that it is not required by applicable law to do so. If that representation ceases to be true, Vendor will notify Customer without undue delay to the extent legally permitted.

4. Customer obligations

4.1 Customer is responsible for the accuracy, quality, and legality of Customer Personal Data and the means by which Customer acquired it. Customer will (a) establish a lawful basis for the Processing, (b) provide all notices and obtain all consents required by Data Protection Laws, (c) ensure it has the right to transfer, or provide access to, Customer Personal Data to Vendor, and (d) not submit Prohibited Data (as defined in the Contract) except as the Contract expressly allows.

4.2 Customer is solely responsible for its instructions and for its use of the services, including its configuration of connectors, models, workflows, and sharing settings.

4.3 Customer's clients and other third parties have no independent rights against Vendor under this DPA. Customer is the sole point of contact for instructions, notices, objections, and audit requests.

5. Security

5.1 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 to Data Subjects, Vendor will implement and maintain appropriate technical and organisational measures to protect Customer Personal Data, as described in Schedule 2. Vendor may update those measures provided the updates do not materially diminish the overall protection of Customer Personal Data.

5.2 Vendor maintains a SOC 2 Type II report covering security, availability, and confidentiality of the services.

6. US state privacy laws

6.1 Where US Data Protection Laws apply to Customer Personal Data, Vendor is a "service provider" or "processor" (or equivalent) and Customer is a "business" or "controller" (or equivalent). Vendor will not (a) Sell or Share Customer Personal Data, (b) retain, use, or disclose Customer Personal Data outside the direct business relationship or for any purpose other than providing the services, performing this DPA, or as otherwise permitted by US Data Protection Laws, or (c) combine Customer Personal Data with Personal Data received from another person or collected from Vendor's own interaction with the Data Subject, except as a service provider or processor is permitted to do under US Data Protection Laws (including for security, debugging, and permitted internal uses).

6.2 Vendor will notify Customer without undue delay if Vendor determines it can no longer meet its obligations under this Section 6. Customer may take reasonable and appropriate steps to stop and remediate unauthorized use of Customer Personal Data upon notice to Vendor.

7. Subprocessors

7.1 Customer generally authorizes Vendor to engage Subprocessors to Process Customer Personal Data. Customer approves the Subprocessors listed in Schedule 3.

7.2 Vendor will enter into a written agreement with each Subprocessor that imposes data-protection obligations no less protective than those in this DPA to the extent applicable to the services the Subprocessor provides. Vendor remains liable to Customer for the Subprocessor's performance of those obligations to the same extent Vendor would be liable if performing the services itself, subject to Section 14.

7.3 Vendor will update Schedule 3 at https://getcargo.io/dpa and notify Customer at the email address associated with Customer's account at least thirty (30) days before authorizing a new Subprocessor to Process Customer Personal Data, except that Vendor may give shorter notice if the change is required to address an actual or suspected security incident, service outage, or similar emergency, in which case Vendor will give notice as soon as reasonably practicable.

7.4 Customer may object to a new Subprocessor on reasonable grounds related to the protection of Customer Personal Data by written notice to legal@getcargo.io within fifteen (15) days of Vendor's notice. If Customer objects, Vendor may (a) not use the Subprocessor for Customer Personal Data, (b) take reasonable corrective steps, or (c) cease providing the affected portion of the services. If the parties cannot resolve the objection within thirty (30) days of Vendor's receipt of the objection, Customer may terminate the affected services on written notice, and Vendor will refund prepaid fees for the terminated portion covering the remainder of the then-current subscription term. That termination and refund are Customer's exclusive remedy for an unresolved Subprocessor objection.

8. International transfers

8.1 Vendor may transfer Customer Personal Data outside the EEA, United Kingdom, or Switzerland where the transfer is (a) to a country or sector covered by an Adequacy Decision, (b) subject to the SCCs, the UK Addendum, and/or a Swiss addendum as applicable, (c) subject to another lawful transfer mechanism, including a valid EU-US Data Privacy Framework certification if Vendor maintains one, or (d) otherwise permitted by Data Protection Laws. Transfers to Subprocessors on Schedule 3 are authorized without further Customer approval.

8.2 Vendor will ensure that any onward transfer of Customer Personal Data by a Subprocessor is made in accordance with Data Protection Laws.

8.3 If the SCCs apply to a Restricted Transfer of Customer Personal Data from Customer (data exporter) to Vendor (data importer):

8.3.a Module Two applies to the extent Customer is a Controller. Module Three applies to the extent Customer is a Processor. Module One does not apply to Customer Personal Data.

8.3.b Clause 7 (docking) is not incorporated. The optional language in Clause 11 is not incorporated.

8.3.c In Clause 9(a) of Modules Two and Three, Option 2 applies. The time period for prior notice of Subprocessor changes is the period in Section 7.3.

8.3.d In Clauses 17 and 18, the SCCs are governed by the laws of Ireland, and disputes under the SCCs are resolved in the courts of Ireland. Those selections apply only to the SCCs and do not amend the governing law, venue, or dispute-resolution provisions of the Contract.

8.3.e Annex I is deemed completed with Schedule 1. Annex II is deemed completed with Schedule 2. Annex III is deemed completed with Schedule 3. Execution of the Contract or acceptance of this DPA constitutes execution of the SCCs, including their annexes.

8.3.f If a term of this DPA and a term of the SCCs conflict as to a Restricted Transfer, the SCCs prevail to the extent of the conflict.

8.4 For Restricted Transfers subject to the UK GDPR, the UK Addendum is incorporated. Tables 1, 2, and 3 of the UK Addendum are deemed completed with Schedules 1, 2, and 3. Table 4 is completed by selecting "neither party."

8.5 For Restricted Transfers subject to the Swiss Federal Act on Data Protection, the SCCs are interpreted to refer to that Act and to the Swiss Federal Data Protection and Information Commissioner where required, and references to EU member states include Switzerland.

8.6 Vendor may adopt a successor transfer mechanism that provides a lawful basis for the transfer, including a new Adequacy Decision or a replacement for the SCCs. Customer may not unilaterally substitute a different transfer mechanism.

8.7 Taking into account the nature of the Processing and the information available to Vendor, Vendor will provide reasonable cooperation with a transfer impact assessment that Customer is required to complete in relation to Restricted Transfers to Vendor. Vendor is not required to disclose information that would compromise the security of the services or Vendor's other customers, or that is subject to confidentiality owed to a third party.

9. Data Subject rights and assistance

9.1 Vendor will, without undue delay and to the extent legally permitted, notify Customer if Vendor receives a request from a Data Subject relating to Customer Personal Data, and will direct the Data Subject to Customer. Vendor will not respond to the Data Subject except on Customer's documented instructions or as required by law.

9.2 Taking into account the nature of the Processing, Vendor will provide Customer with reasonable assistance, through the services where available, so that Customer may respond to Data Subject requests. Customer is responsible for meeting any statutory deadlines applicable to Customer or to Customer's clients.

9.3 Taking into account the nature of the Processing and the information available to Vendor, Vendor will provide reasonable assistance to Customer with data-protection impact assessments and prior consultations with supervisory authorities, in each case solely in relation to Vendor's Processing of Customer Personal Data.

9.4 If assistance under this Section 9 exceeds the ordinary operation of the services, Vendor may charge reasonable fees, notified to Customer in advance.

10. Personal Data Breach

10.1 Vendor will notify Customer without undue delay, and in any event no later than seventy-two (72) hours, after becoming aware of a confirmed Personal Data Breach affecting Customer Personal Data. Notification will describe, to the extent then known: (a) the nature of the Personal Data Breach, including categories and

approximate numbers of Data Subjects and records concerned; (b) the likely consequences; (c) measures taken or proposed to address the Personal Data Breach; and (d) a point of contact. Vendor may provide information in phases as it becomes available.

10.2 Vendor will investigate and take reasonable steps to mitigate the Personal Data Breach. Taking into account the nature of the Processing and the information available to Vendor, Vendor will provide reasonable assistance so that Customer may notify competent authorities and Data Subjects where Customer is required to do so. Customer is solely responsible for those notifications. Vendor will not notify a supervisory authority, Data Subjects, or the public except as required by law or instructed in writing by Customer.

11. Demonstration of compliance and audits

11.1 Upon written request, and no more than once per twelve (12) months except following a confirmed Personal Data Breach or as required by a supervisory authority, Vendor will make available to Customer, subject to confidentiality: (a) Vendor's then-current SOC 2 Type II report; (b) an executive summary of its most recent independent penetration test, if available; and (c) responses to a reasonable security questionnaire of reasonable scope.

11.2 Customer will exercise its audit rights under this DPA and, where applicable, the SCCs by reviewing the information in Section 11.1. A further audit, including inspection, is available only if Data Protection Laws require it and compliance cannot reasonably be demonstrated by that information.

11.3 Any audit under Section 11.2: (a) requires at least thirty (30) days' prior written notice unless a supervisory authority requires shorter notice; (b) occurs no more than once per twelve (12) months except as required by a supervisory authority or following a confirmed Personal Data Breach; (c) is mutually scoped to minimize disruption to Vendor's business and to Vendor's other customers; (d) takes place during Vendor's normal business hours, onsite only if reasonably necessary, and subject to Vendor's security policies; (e) may be performed by Customer or an independent auditor bound by confidentiality written in favor of Vendor; and (f) is at Customer's expense, unless the audit identifies a material breach of this DPA by Vendor, in which case Vendor will bear Customer's reasonable, documented audit costs.

11.4 Information disclosed in connection with this Section 11 is Vendor's Confidential Information. Customer may share it with a client only under confidentiality no less protective than the Contract, and only as needed for that client's due diligence of Customer. Customer's clients have no independent audit rights against Vendor.

12. Government and legal process requests

12.1 If Vendor receives a request from a governmental, regulatory, or law-enforcement authority for Customer Personal Data, Vendor will, to the extent legally permitted, notify Customer without undue delay and provide reasonable cooperation if Customer wishes to limit, challenge, or seek protection against the disclosure.

12.2 Vendor will not disclose Customer Personal Data in response to such a request unless legally compelled to do so. If disclosure is legally compelled, Vendor will, to the extent legally permitted, give Customer prior notice so that Customer may seek a protective order or other remedy. If prior notice is legally prohibited, Vendor will, after the prohibition lifts, notify Customer of the disclosure to the extent then permitted.

13. Duration, deletion, and return

13.1 This DPA takes effect when the parties enter into the Contract (or when Customer first submits Customer Personal Data, if later) and remains in effect until Vendor has deleted or returned Customer Personal Data in accordance with this Section 13.

13.2 During the term, Customer may delete Customer Personal Data through the services where that functionality is available. Other deletion requests will be handled without undue delay, taking into account the nature of the Processing and technical feasibility. Vendor is not required to delete data from backups other than in accordance with its ordinary backup cycle.

13.3 Upon termination or expiration of the Contract, Vendor will, at Customer's written election received within thirty (30) days after termination, delete or return Customer Personal Data in Vendor's possession or control without undue delay, and in any event within thirty (30) days, except that:

13.3.a Vendor may retain Customer Personal Data to the extent required by applicable law, the Contract, or bona fide dispute, security, billing, or audit obligations, in which case Vendor will isolate the retained data from active Processing and continue to protect it in accordance with this DPA; and

13.3.b Customer Personal Data in backup or disaster-recovery systems will be deleted in accordance with Vendor's ordinary backup cycle.

13.4 Return will be in a then-available reasonable format. If Customer does not elect return within thirty (30) days after termination, Vendor may delete the data. Residual copies in backup systems remain subject to Section 13.3.b.

14. Liability

14.1 Each party's liability arising out of or relating to this DPA, including the Standard Contractual Clauses, whether in contract, tort, or any other theory of liability, is subject to the limitations and exclusions of liability in the Contract. Any reference in the Contract to a party's liability means that party's aggregate liability under the Contract and this DPA.

14.2 Nothing in this DPA limits a party's liability to a Data Subject to the extent that limitation is prohibited by Data Protection Laws. That reservation does not create any additional indemnification obligation between the parties and does not expand either party's liability to the other beyond the Contract.

14.3 This DPA does not create a separate indemnity for regulatory fines, third-party contract liability, or Customer's own compliance failures. Claims between the parties arising out of this DPA are subject to the indemnification provisions of the Contract, if any.

14.4 Vendor is not liable for any claim arising from Vendor's Processing of Customer Personal Data in accordance with Customer's instructions.

15. Term, termination, and miscellaneous

15.1 A material breach of this DPA is a material breach of the Contract. Either party may exercise the termination rights in the Contract for such a breach. A breach is not material solely because it is a breach of this DPA.

15.2 Notices under this DPA must be in writing. Notices to Vendor should be sent to legal@getcargo.io and to the notice address in the Contract, if any. Notices to Customer may be sent to the email address associated with Customer's account or the notice address in the Contract.

15.3 This DPA is governed by the governing law and venue of the Contract, except as Section 8.3.d provides for the SCCs.

15.4 Vendor may update this DPA where (a) the update is required to comply with Data Protection Laws or a binding order of a competent authority, or (b) the update is commercially reasonable, does not materially reduce the security of the services, does not expand the scope of Vendor's Processing of Customer Personal Data, and does not have a material adverse impact on Customer's rights under this DPA. Vendor will post the updated DPA at https://getcargo.io/dpa and update the "Last Updated" date. If Customer objects to a material update on reasonable data-protection grounds within thirty (30) days of posting, the parties will discuss in good faith. If they cannot agree, Customer may terminate the affected services as its exclusive remedy.

15.5 If any provision of this DPA is held unenforceable, the remaining provisions remain in effect. Failure to enforce a provision is not a waiver.

Schedule 1. Details of Processing

This Schedule completes Annex I of the SCCs.

A. List of parties

Data exporter: Customer. Address, contact, and activities: as specified in the Contract and Customer's account. Role: Controller, or Processor as applicable.

Data importer: GetCargo Inc., 603 Tennessee St, San Francisco, California 94107, United States. Contact: legal@getcargo.io. Activities: providing the Cargo services described in the Contract. Role: Processor.

Signature and date: execution of the Contract or acceptance of this DPA constitutes execution of this Schedule by both parties.

B. Description of transfer

Categories of Data Subjects: depending on Customer's use of the services, Data Subjects may include Customer's users, employees, contractors, customers, prospects, business contacts, and other individuals whose Personal Data Customer submits to the services.

Categories of Personal Data: the Personal Data contained in Customer Content that Customer submits to, or generates through, the services. This may include identifiers, contact details, professional information, communications content, usage and event data, and other GTM, CRM, or workflow data Customer chooses to Process through the services.

Sensitive data: none, unless Customer submits it in violation of the Contract. The Contract prohibits Prohibited Data unless the Order Form or Key Terms expressly allow it.

Frequency: continuous, for as long as Customer uses the services.

Nature of the Processing: collection, storage, retrieval, analysis, transformation, transfer, display, and other Processing as needed to provide, maintain, secure, and support the services, including orchestration, enrichment, scoring, routing, synchronization, logging, troubleshooting, and AI inference where those features

are used.

Purpose: to provide, maintain, secure, support, and improve the services in accordance with the Contract.

Retention: for the term of the Contract and thereafter as described in Section 13.

Subprocessor transfers: as described in Schedule 3, for the duration of Vendor's engagement of each Subprocessor.

C. Competent supervisory authority

The competent supervisory authority is determined in accordance with Clause 13 of the SCCs.

Schedule 2. Technical and Organisational Measures

This Schedule completes Annex II of the SCCs. It describes Vendor's information security program as of the date of this DPA, consistent with Vendor's SOC 2 Type II report and the practices described at https://getcargo.io/security. Vendor maintains these measures and may update them under Section 5.1.

1. Encryption. Encryption of Customer Personal Data in transit over public networks and at rest in production datastores, using industry-standard protocols.

2. Identity and access. Unique user credentials, multi-factor authentication for workforce access to production systems, role-based access, least privilege, and periodic access reviews. Production access is limited to personnel with a business need.

3. Logging and monitoring. Logging of security-relevant events on production systems, with alerting and retention appropriate to the risk. Intrusion-detection capabilities of the hosting provider (including AWS GuardDuty) may be used as part of this monitoring.

4. Vulnerability management. Regular vulnerability scanning, dependency scanning of application components, and a process to evaluate and remediate identified vulnerabilities according to risk.

5. Secure development. Documented change management, separation of non-production and production environments, and code review practices for production changes.

6. Incident response. A documented incident-response process, including assessment, containment, eradication, recovery, and notification under Section 10.

7. Backup and recovery. Encrypted backups of production data and a disaster-recovery process designed to restore the services following a significant disruption. Vendor tests recovery procedures on a periodic basis.

8. Personnel. Confidentiality obligations, security awareness training, and background verification where permitted by law.

9. Tenant isolation. Logical separation of Customer Personal Data in production environments.

10. Infrastructure. Production workloads hosted with reputable cloud providers under written data-protection terms, with network controls appropriate to a multi-tenant SaaS service.

11. Business continuity. Business-continuity planning covering material dependencies of the services.

12. Vendor risk. Due diligence and written data-protection terms for Subprocessors that Process Customer Personal Data.

Schedule 3. Subprocessors

This Schedule completes Annex III of the SCCs. Vendor may update this list under Section 7. Third parties that Customer connects through the services are Customer's processors, not Vendor's Subprocessors.

Subprocessor	Purpose	Customer Personal Data	Location	Terms
Amazon Web Services, Inc.	Cloud infrastructure, including hosting, storage, networking, and AWS security services such as GuardDuty	Customer content, stored files, platform data, security telemetry	Europe (eu-west-1)	AWS DPA, GDPR Center
Qovery	Cloud deployment platform	Deployment metadata and configuration that may include environment identifiers	Europe	Privacy Policy
Datadog, Inc.	Monitoring, alerting, and observability	System logs, performance data, and related telemetry that may include identifiers	Europe	DPA
ClickHouse Cloud	Analytics warehouse	Orchestration telemetry, usage analytics, and related identifiers	Europe (eu-west-1)	DPA
Temporal Technologies Inc.	Workflow orchestration	Workflow state and execution payloads	Europe (eu-west-1)	DPA, Security
DataStax, Inc. (Astra DB)	Managed database	Workflow execution data and run history	Europe (eu-west-1)	Trust Center
Okta, Inc. (Auth0)	Identity and authentication	Account credentials and login events of Customer's users	Europe (eu-west-1)	Trust & Compliance
Google LLC (BigQuery)	Customer-selected system of record	Customer content stored in BigQuery where Customer enables it	Europe or United States (customer-selected)	Cloud DPA
Snowflake Inc.	Vendor product analytics warehouse	Analytical and usage data, including user identifiers	United States	DPA
RudderStack Inc.	Product analytics event pipeline	Usage events and user identifiers	United States	Privacy Policy
OpenAI, L.L.C.	AI model inference for Vendor-operated platform features (including platform AI credits)	Prompts, outputs, and related context that Customer submits through those features	United States	DPA
Anthropic, PBC	AI model inference for Vendor-operated platform features (including platform AI credits)	Prompts, outputs, and related context that Customer submits through those features	United States	DPA
Pylon	Customer support	Support tickets and communications Customer or its users submit	United States	Security

Signature page

This DPA may be executed in counterparts, including wet-ink and electronic signatures (DocuSign, Adobe Sign, or equivalent), each of which is an original and all of which together are one instrument. Execution of the Contract or acceptance of this DPA also constitutes execution, as stated in Section 8.3.e and Schedule 1. The parties sign below to evidence their agreement to this DPA.

Customer

LEGAL ENTITY NAME

ADDRESS

SIGNATORY NAME

TITLE

EMAIL

DATE

SIGNATURE

Vendor

LEGAL ENTITY NAME

GetCargo Inc.

ADDRESS

603 Tennessee St, San Francisco, CA 94107

SIGNATORY NAME

TITLE

EMAIL

legal@getcargo.io

DATE

SIGNATURE

By signing, each signatory represents that they are authorized to bind the party they sign for. Notices to Vendor under this DPA: legal@getcargo.io.