



**ORDERGRID INC.  
DATA PROCESSING ADDENDUM**

Last update: March 1, 2026

Document Reference: OrderGrid Data Processing Addendum v2026-03-01

This Data Processing Addendum (this “**DPA**”) is incorporated into and forms part of the OrderGrid Platform Service Terms of Service or other written or electronic agreement between OrderGrid Inc. (“**OrderGrid**”, “**we**”, “**our**” or “**us**”) and the entity identified as “**Client**” in the applicable agreement (“**Client**”, “**you**” or “**your**”) (such agreement, the “**Agreement**”). This DPA applies to the extent OrderGrid processes Personal Data on behalf of Client in the course of providing the Services under the Agreement. All capitalized terms not defined in this DPA shall have the meanings given to them in the Agreement.

**1. DEFINITIONS**

- 1.1 “**Applicable Data Protection Law**” means all laws and regulations applicable to the processing of Personal Data under this DPA, including, where applicable: (a) the EU General Data Protection Regulation 2016/679 (“**EU GDPR**”); (b) the EU GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 (the “**UK GDPR**”) and the Data Protection Act 2018 (“**DPA 2018**”); (c) the Personal Information Protection and Electronic Documents Act (Canada) (“**PIPEDA**”); (d) the California Consumer Privacy Act, as amended by the California Privacy Rights Act (“**CCPA**”); and (e) any other applicable data protection or privacy legislation in any jurisdiction.
- 1.2 “**Controller**” means the entity that determines the purposes and means of the processing of Personal Data.
- 1.3 “**Data Subject**” means the identified or identifiable natural person to whom the Personal Data relates.
- 1.4 “**EEA**” means the European Economic Area.
- 1.5 “**Personal Data**” means any information relating to an identified or identifiable natural person that is processed by OrderGrid on behalf of Client as a result of, or in connection with, the provision of the Services under the Agreement.
- 1.6 “**Personal Data Breach**” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed by OrderGrid.
- 1.7 “**Processing**” (and “**process**”, “**processes**” and “**processed**”) means any operation or set of operations performed on Personal Data, whether or not by automated means, including collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- 1.8 “**Processor**” means the entity that processes Personal Data on behalf of the Controller.
- 1.9 “**Standard Contractual Clauses**” or “**SCCs**” means: (a) with respect to transfers subject to the EU GDPR, the standard contractual clauses annexed to Commission Implementing Decision (EU) 2021/914; and (b) with respect to transfers subject to the UK GDPR, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (the “**UK Addendum**”), issued by the Information Commissioner under section 119A(1) of the DPA 2018.
- 1.10 “**Sub-Processor**” means any third party engaged by OrderGrid to process Personal Data on behalf of Client in connection with the Services.

## 2. ROLES AND SCOPE OF PROCESSING

- 2.1 **Roles.** As between the parties, Client is the Controller and OrderGrid is the Processor with respect to the Personal Data processed under the Agreement.
- 2.2 **Client Obligations.** Client shall: (a) comply with its obligations as Controller under Applicable Data Protection Law, including providing any required notices to and obtaining any required consents from Data Subjects; (b) ensure that all Personal Data provided to OrderGrid has been collected lawfully and that Client has a valid legal basis for such processing; and (c) ensure that its processing instructions to OrderGrid comply with Applicable Data Protection Law.
- 2.3 **Processing Details.** The subject matter, duration, nature, purpose of the processing, and the types of Personal Data and categories of Data Subjects are described in Schedule 1 to this DPA.

## 3. ORDERGRID'S OBLIGATIONS

- 3.1 **Processing Instructions.** OrderGrid shall process Personal Data only in accordance with Client's documented instructions, as set out in the Agreement and this DPA, unless required to do otherwise by applicable law. If OrderGrid is required by applicable law to process Personal Data other than in accordance with Client's instructions, OrderGrid shall inform Client of such requirement before carrying out the processing, unless prohibited from doing so by applicable law.
- 3.2 **Confidentiality.** OrderGrid shall ensure that any person authorized to process Personal Data on its behalf is subject to appropriate obligations of confidentiality (whether contractual or statutory).
- 3.3 **Personnel.** OrderGrid shall ensure that its personnel who have access to Personal Data: (a) are informed of the confidential nature of the Personal Data; (b) have received appropriate training on their data protection responsibilities; and (c) are aware of OrderGrid's obligations under this DPA.
- 3.4 **Compliance Assistance.** Taking into account the nature of the processing and the information available to OrderGrid, OrderGrid shall provide reasonable assistance to Client, at Client's cost, in ensuring compliance with Client's obligations under Applicable Data Protection Law in relation to: (a) Data Subject rights requests; (b) data protection impact assessments; and (c) prior consultation with supervisory authorities, in each case to the extent that Client is unable to fulfil such obligations independently.

## 4. SECURITY

- 4.1 **Security Measures.** OrderGrid shall implement and maintain appropriate technical and organizational measures to protect Personal Data against unauthorized or unlawful processing and against accidental loss, destruction, damage, alteration or disclosure, as described in Schedule 2 to this DPA. OrderGrid may update these measures from time to time, provided that such updates do not materially decrease the overall level of security of the Services.
- 4.2 OrderGrid's security measures shall include, as appropriate:
- (a) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
  - (b) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident;
  - (c) a process for regularly testing, assessing and evaluating the effectiveness of the security measures; and
  - (d) measures to ensure that Personal Data is accessible only to authorized personnel on a need-to-know basis.

## 5. PERSONAL DATA BREACH

- 5.1 **Notification.** OrderGrid shall promptly notify Client without undue delay after becoming aware of a Personal Data Breach affecting Client's Personal Data, and in any event within a timeframe that permits Client to comply with its own notification obligations under Applicable Data Protection Law.
- 5.2 **Breach Details.** OrderGrid's notification shall include, to the extent such information is available to OrderGrid at the time of notification:
- (a) a description of the nature of the Personal Data Breach, including the categories and approximate number of Data Subjects and Personal Data records concerned;
  - (b) the likely consequences of the Personal Data Breach; and
  - (c) a description of the measures taken or proposed to be taken to address the Personal Data Breach, including measures to mitigate its possible adverse effects.
- 5.3 **Cooperation.** Following any Personal Data Breach, the parties shall co-operate with each other to investigate the matter. OrderGrid shall provide reasonable co-operation and assistance to Client in managing the breach, including providing additional information as it becomes available.
- 5.4 **No Acknowledgment of Fault.** OrderGrid's obligation to notify or respond to a Personal Data Breach under this Section 5 shall not be construed as an acknowledgment by OrderGrid of any fault or liability with respect to the Personal Data Breach.

## 6. SUB-PROCESSORS

- 6.1 **General Authorization.** Client provides a general written authorization to OrderGrid to engage Sub-Processors to process Personal Data on Client's behalf. A list of OrderGrid's current Sub-Processors is available at [ordergrid.com/legal/sub-processors](http://ordergrid.com/legal/sub-processors) (or such other URL as OrderGrid may designate from time to time).
- 6.2 **Sub-Processor Agreements.** OrderGrid shall enter into a written agreement with each Sub-Processor containing data protection obligations no less protective than those set out in this DPA with respect to the protection of Personal Data.
- 6.3 **Changes to Sub-Processors.** OrderGrid shall provide Client with reasonable advance notice (of not less than 30 days) of any intended changes to its Sub-Processors, by updating the Sub-Processor list and providing written notification to Client's designated contact. Client may subscribe to receive email notifications of such changes.
- 6.4 **Objection Right.** If Client has a reasonable, good-faith objection to a new Sub-Processor based on data protection grounds, Client shall notify OrderGrid in writing within 15 days of receiving notice of the change. The parties shall discuss such concerns in good faith. If the parties are unable to reach a resolution within 30 days, Client may, as its sole and exclusive remedy, terminate the affected portion of the Services by providing written notice to OrderGrid, and OrderGrid shall refund any prepaid fees for the terminated Services covering the remainder of the then-current subscription term.
- 6.5 **Liability.** OrderGrid shall remain responsible for the acts and omissions of its Sub-Processors to the same extent as if the acts or omissions were performed by OrderGrid itself, subject to the limitations of liability set out in the Agreement.

## 7. CROSS-BORDER TRANSFERS OF PERSONAL DATA

- 7.1 **Processing Locations.** OrderGrid may process Personal Data in Canada, the United States, the EEA, and any other jurisdiction where OrderGrid or its Sub-Processors maintain facilities, subject to the requirements of this Section 7.
- 7.2 **Transfer Mechanisms.** To the extent that the processing of Personal Data involves a transfer of Personal Data to a country outside the EEA or the UK that has not been recognized as providing an adequate level of data protection, the parties agree that:

- (a) for transfers subject to the EU GDPR, Module Two (Controller to Processor) of the Standard Contractual Clauses annexed to Commission Implementing Decision (EU) 2021/914 shall apply, and are hereby incorporated by reference into this DPA;
- (b) for transfers subject to the UK GDPR, the UK Addendum shall apply and is hereby incorporated by reference into this DPA; and
- (c) OrderGrid shall ensure that any onward transfers by Sub-Processors are made subject to appropriate safeguards in accordance with Applicable Data Protection Law.

7.3 **SCC Supplementary Terms.** For the purposes of the SCCs:

- (a) Client is the “data exporter” and OrderGrid is the “data importer”;
- (b) Clause 7 (Docking Clause) shall apply;
- (c) for Clause 9(a), Option 2 (General Written Authorisation) is selected, and the time period for prior notice of Sub-Processor changes shall be as set out in Section 6.3 of this DPA;
- (d) for Clause 11(a), the optional language regarding independent dispute resolution does not apply;
- (e) for Clause 17 (Governing Law), Option 1 shall apply and the SCCs shall be governed by the laws of the Republic of Ireland;
- (f) for Clause 18 (Choice of Forum and Jurisdiction), disputes shall be resolved before the courts of the Republic of Ireland;
- (g) Annex I shall be deemed to incorporate the information in Schedule 1 to this DPA; and
- (h) Annex II (Technical and Organizational Measures) shall be deemed to incorporate the information in Schedule 2 to this DPA.

7.4 Where Client’s processing of Personal Data is subject to data protection laws of jurisdictions other than the EU and UK (including laws of Bermuda, or other jurisdictions), the SCCs shall be deemed amended to the extent necessary to provide appropriate safeguards for such transfers in accordance with the applicable local data protection legislation.

**8. CCPA SPECIFIC PROVISIONS**

8.1 This Section 8 applies solely to the extent that OrderGrid processes Personal Data that is subject to the CCPA on behalf of Client.

8.2 **Service Provider Status.** For purposes of the CCPA, OrderGrid is a “service provider” and Client is a “business.” OrderGrid shall process Personal Data solely for the business purposes specified in the Agreement and this DPA, and shall not: (a) sell or share (as those terms are defined in the CCPA) any Personal Data; (b) retain, use or disclose Personal Data for any purpose other than the business purposes specified in the Agreement, including for any commercial purpose other than providing the Services; or (c) retain, use or disclose Personal Data outside of the direct business relationship between OrderGrid and Client.

8.3 **Compliance Certification.** OrderGrid hereby certifies that it understands the restrictions in Section 8.2 and will comply with them. OrderGrid shall notify Client if it determines that it can no longer meet its obligations as a service provider under the CCPA.

8.4 **Consumer Rights Requests.** OrderGrid shall provide reasonable assistance to Client in responding to verifiable consumer requests under the CCPA, including requests to know, delete, or correct Personal Data. OrderGrid shall not respond directly to any consumer request unless directed to do so by Client.

8.5 **Combining Personal Data.** OrderGrid shall not combine Personal Data received from Client with Personal Data received from or on behalf of another person or entity, or collected from OrderGrid’s own interactions with consumers, except as expressly permitted by the CCPA for service providers.

**9. SENSITIVE AND PROHIBITED DATA**

- 9.1 **Prohibited Data.** Client shall not upload to the Services or otherwise submit or make accessible to OrderGrid any: (a) financial account identifiers (e.g., credit card numbers or bank account numbers); (b) government-issued identifiers (e.g., social security numbers, national insurance numbers, or passport numbers); (c) health card numbers or protected health information; (d) biometric data; or (e) any other types of sensitive data that are subject to specific or elevated data protection requirements under Applicable Data Protection Law (collectively, “**Prohibited Data**”), unless OrderGrid has expressly agreed in writing to process such data and the parties have implemented appropriate supplementary safeguards.
- 9.2 **Special Category Data.** Client shall not submit to the Services any “special categories of personal data” as defined in Article 9 of the EU GDPR (including data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for identification purposes, data concerning health, or data concerning a natural person’s sex life or sexual orientation) unless expressly agreed in writing with OrderGrid.
- 9.3 **Sole Responsibility.** If Client submits Prohibited Data or special category data to the Services without OrderGrid’s prior written agreement, Client shall be solely responsible for any resulting non-compliance with Applicable Data Protection Law and shall indemnify OrderGrid against any losses, claims or liabilities arising therefrom.

## **10. DATA SUBJECT RIGHTS**

- 10.1 OrderGrid shall promptly notify Client if it receives a request from a Data Subject to exercise any right under Applicable Data Protection Law in respect of their Personal Data (including access, rectification, erasure, restriction, portability or objection).
- 10.2 OrderGrid shall provide reasonable assistance to Client, at Client’s cost, in responding to any such Data Subject request, taking into account the nature of the processing. OrderGrid shall not respond directly to any Data Subject request unless authorized to do so by Client or required to do so by applicable law.

## **11. AUDIT**

- 11.1 **Audit Reports.** OrderGrid shall make available to Client, on request (and not more than once per year), copies of its then-current SOC 2 Type II report (or equivalent independent third-party audit report), to the extent available. Such reports are OrderGrid’s Confidential Information and are provided subject to the confidentiality provisions of the Agreement.
- 11.2 **Additional Audit.** To the extent that SOC reports are not sufficient to demonstrate OrderGrid’s compliance with this DPA, Client may, at its own cost and upon at least 30 days’ prior written notice, conduct or commission an independent third-party auditor (subject to reasonable confidentiality obligations) to conduct an audit of OrderGrid’s processing activities, limited to documentation review. Such audit shall: (a) be conducted no more than once per year; (b) occur during normal business hours; (c) not disrupt OrderGrid’s business operations; and (d) be limited to matters relevant to Client’s Personal Data. OrderGrid may charge Client a reasonable fee for time and resources expended in connection with any such audit beyond the provision of SOC reports.

## **12. DATA RETURN AND DELETION**

- 12.1 Upon termination or expiry of the Agreement, OrderGrid shall, at Client’s election, delete or return all Personal Data in its possession or control in accordance with the terms of the Agreement. Client acknowledges that Personal Data will be available for export or download for a period of 30 days following the effective date of termination, after which OrderGrid will delete or destroy the Personal Data in accordance with its standard practices and the retention schedule set out in Schedule 3.
- 12.2 OrderGrid may retain Personal Data to the extent required by applicable law or regulation, or as reasonably necessary for its legitimate business purposes (such as the maintenance of billing records), provided that OrderGrid shall continue to protect such retained data in accordance with this DPA and Applicable Data Protection Law.

12.3 Upon Client's written request, OrderGrid shall certify in writing that it has deleted or destroyed the Personal Data in accordance with this Section 12, within 30 days following such deletion or destruction.

### **13. RECORDS**

13.1 OrderGrid shall maintain records of its processing activities carried out on behalf of Client as required by Applicable Data Protection Law, including records of the categories of processing activities, transfers of Personal Data to third countries, and a general description of technical and organizational security measures.

### **14. LIABILITY**

14.1 The liability of each party under or in connection with this DPA shall be subject to the limitations and exclusions of liability set out in the Agreement. For the avoidance of doubt, the aggregate liability of OrderGrid and its affiliates under or in connection with the Agreement and this DPA shall apply in the aggregate for all claims under both the Agreement and this DPA.

### **15. GENERAL**

15.1 **Conflict.** In the event of any conflict or inconsistency between this DPA and the Agreement, this DPA shall prevail with respect to the processing of Personal Data. In the event of any conflict between this DPA and the SCCs, the SCCs shall prevail.

15.2 **Amendments.** OrderGrid may update this DPA from time to time to reflect changes in Applicable Data Protection Law or OrderGrid's data processing practices. OrderGrid shall provide Client with no less than 30 days' prior written notice of any material changes to this DPA.

15.3 **Severability.** If any provision of this DPA is found to be invalid or unenforceable, the remaining provisions shall remain in full force and effect.

15.4 **Governing Law.** This DPA shall be governed by and construed in accordance with the governing law provisions of the Agreement, except as otherwise required by Applicable Data Protection Law or the SCCs.

15.5 **Entire DPA.** This DPA (including its Schedules) constitutes the entire agreement between the parties with respect to the subject matter hereof and supersedes all prior or contemporaneous understandings regarding such subject matter.

## **SCHEDULE 1 — DETAILS OF PROCESSING**

**Subject Matter of Processing:** Provision of the Services to Client under the Agreement, including the OrderGrid Platform Service.

**Duration of Processing:** The term of the Agreement, plus any period during which OrderGrid retains Personal Data in accordance with Section 12 and Schedule 3.

**Nature of Processing:** Collection, storage, organization, retrieval, use, disclosure by transmission, and erasure or destruction of Personal Data as necessary to provide the Services, including order management, fulfilment services, reporting, and platform operations.

**Purpose of Processing:** To provide the Services to Client under the Agreement.

**Categories of Personal Data:** Names, addresses, email addresses, telephone numbers, order details, delivery information, payment references, and any other Personal Data submitted to the Platform Service by or on behalf of Client.

**Special Category Data:** None (Client shall not submit special category data to the Services unless expressly agreed in writing).

**Categories of Data Subjects:** Client's customers, end-users, recipients of orders, Client's employees, contractors and agents, and Authorized Users of the Platform Service.

## SCHEDULE 2 — TECHNICAL AND ORGANISATIONAL MEASURES

OrderGrid employs a combination of policies, procedures, guidelines and technical and physical controls to protect Personal Data from accidental loss and unauthorized access, disclosure or destruction, including the following:

**Infrastructure Security.** OrderGrid’s AWS-hosted infrastructure follows CIS AWS Foundations and AWS EKS benchmarks for platform and server hardening. Security settings are configured to industry standards for all devices, software and services.

**Access Control.** Access is role-based for all employees, following least-privilege principles aligned to zero-trust practices. Changes to access or permissions require explicit approval through internal ticketing systems with management and security review. OrderGrid employs dedicated security engineering resources for identity and access management, anomaly detection and daily operations checks.

**Malware Protection.** All devices are required to have up-to-date anti-malware protection, monitored and enforced via installed compliance agents.

**Software Updates.** OrderGrid monitors and enforces software updates through compliance agents, including OS patch management.

**Data Backup.** OrderGrid maintains regular data backups with appropriate retention policies and recovery procedures.

**Encryption.** Personal Data is encrypted in transit using TLS 1.2 or higher, and at rest using AES-256 or equivalent encryption standards.

**Incident Response.** OrderGrid maintains an incident response plan that includes procedures for identification, containment, eradication, and recovery from security incidents.

**Employee Training.** OrderGrid provides regular security awareness and data protection training to its personnel.

OrderGrid periodically reviews and updates its technical and organizational measures to ensure they remain current and appropriate to the risk.

### SCHEDULE 3 — DATA RETENTION SCHEDULE

OrderGrid applies the following retention and deletion schedule to Personal Data processed on behalf of Client during the term of the Agreement:

- 1. Active Data.** During the term of the Agreement, OrderGrid retains Personal Data as necessary to provide the Services. Client may export or delete its data at any time through the Platform Service.
- 2. Annual Deletion Cycle.** OrderGrid conducts an annual data deletion cycle in the first quarter of each calendar year. During each annual cycle, OrderGrid will delete or anonymize Personal Data from the calendar year that is two years prior to the current year (e.g., in Q1 2027, Personal Data from calendar year 2025 and earlier will be deleted). This ensures that no more than approximately two full calendar years of Personal Data are retained on the Platform Service at any given time, unless a longer retention period is required under the Agreement or by applicable law.
- 3. Post-Termination.** Upon termination or expiry of the Agreement, Personal Data will be available for Client export or download for a period of 30 days. Following that 30-day period, OrderGrid will delete all remaining Personal Data in accordance with its standard deletion procedures, subject to any legal or regulatory retention obligations.
- 4. Backups.** Personal Data may persist in encrypted backup systems for a limited period following deletion from production systems. OrderGrid's backup retention cycle ensures that Personal Data is fully purged from backups within 90 days of deletion from production.
- 5. Exceptions.** OrderGrid may retain limited Personal Data beyond the periods set out above where: (a) required by applicable law or regulation; (b) necessary for the establishment, exercise or defence of legal claims; or (c) contained in aggregated or anonymized form such that it no longer constitutes Personal Data. Any retained data will continue to be protected in accordance with this DPA.
- 6. Deletion Records.** OrderGrid will maintain records of annual deletion cycles performed, including the date of deletion and the scope of data deleted. Client may request confirmation of deletion in accordance with Section 12.3 of this DPA.