My Fleet Safety

DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") is incorporated into and forms part of the agreement (the "**Agreement**") between the entity identified as the customer under the Agreement ("**Customer**") and You're Doin' It, LLC ("**Provider**") for Provider's provision of the My Fleet Safety platform (the "**Services**").

1. DEFINITIONS

1.1 "**Applicable Data Protection Law**" means all federal and state laws and regulations governing the processing of Personal Data applicable to the parties' performance under this DPA, including, as applicable, the California Consumer Privacy Act, as amended by the California Privacy Rights Act (Cal. Civ. Code §§ 1798.100 et seq.) ("**CCPA**"), and other applicable state privacy laws, as each may be amended from time to time.

1.2 "**Controller**" means the entity that determines the purposes and means of Processing Personal Data. For purposes of this DPA, Customer is the Controller.

1.3 "**Data Subject**" means an identified or identifiable individual to whom Personal Data relates, including drivers and other personnel whose data is Processed through the Services.

1.4 "**DOT Regulations**" means all applicable regulations of the U.S. Department of Transportation ("DOT"), including 49 CFR Parts 40, 382, and 391, and related guidance issued by the Federal Motor Carrier Safety Administration ("**FMCSA**"), as each may be amended from time to time.

1.5 "**Driver Qualification Data**" means Personal Data relating to driver qualification files maintained under 49 CFR Part 391, including medical certificates, employment applications, road test results, driving records, investigation history files, medical information, and related records.

1.6 "**Drug and Alcohol Testing Data**" means any records relating to DOT-mandated or non-DOT drug and alcohol testing, including test results, refusals, return-to-duty documentation, and substance abuse professional reports, to the extent uploaded to or stored within the Services by Customer.

1.7 "**Personal Data**" means any information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, to an identified or identifiable Data Subject. Personal Data includes, without limitation, names, email addresses, Social Security numbers, driver's license numbers, medical information, employment history, and Driver Qualification Data.

1.8 "**Processing**" (and its cognates) means any operation or set of operations performed on Personal Data, whether or not by automated means, including collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, restriction, erasure, or destruction.

1.9 "**Security Incident**" means any unauthorized access to, acquisition of, use of, or disclosure of Personal Data that compromises the security, confidentiality, or integrity of such Personal Data.

1.10 "**Sensitive Personal Data**" means Personal Data that includes Social Security numbers, driver's license numbers, medical information (including medical certificates and physical examination records), Drug and Alcohol Testing Data, and any other category of data classified as sensitive under Applicable Data Protection Law.

1.11 "**Subprocessor**" means any third party engaged by Provider to Process Personal Data on behalf of Customer in connection with the Services.

2. SCOPE AND ROLES

2.1 Scope. This DPA applies to all Processing of Personal Data by Provider on behalf of Customer in connection with the Services.

2.2 Roles. Customer is the Controller of Personal Data. Provider Processes Personal Data as a processor (or "service provider" as defined under the CCPA) on behalf of Customer and in accordance with Customer's documented instructions.

2.3 Customer Responsibilities. Customer is solely responsible for: (a) the accuracy, quality, and legality of all Personal Data submitted to the Services; (b) obtaining all necessary consents, authorizations, and legal bases required under Applicable Data Protection Law and DOT Regulations before submitting Personal Data to the Services; and (c) determining that the Services are appropriate for the storage and Processing of Personal Data, including any Sensitive Personal Data or Drug and Alcohol Testing Data that Customer elects to upload.

2.4 Drug and Alcohol Testing Data. Customer acknowledges that Provider does not request, order, or administer drug or alcohol tests and does not act as a Consortium/Third-Party Administrator ("C/TPA"), Medical Review Officer, or Substance Abuse Professional. To the extent Customer uploads Drug and Alcohol Testing Data to the Services, Customer represents and warrants that it has obtained all consents and authorizations required under 49 CFR Part 40 and other applicable DOT Regulations prior to uploading such data, including any required specific written consent from the applicable Data Subject.

3. PROCESSING OBLIGATIONS

3.1 Purpose Limitation. Provider shall Process Personal Data solely for the purpose of providing the Services to Customer in accordance with the Agreement and Customer's documented instructions. Provider shall not: (a) sell Personal Data; (b) retain, use, or disclose Personal Data for any commercial purpose other than providing the Services; or (c) retain, use, or disclose Personal Data outside of the direct business relationship between Provider and Customer.

3.2 Compliance with Instructions. Provider shall Process Personal Data only in accordance with Customer's documented instructions and in providing the Services to Customer, unless required to do otherwise by applicable law. If Provider believes that an instruction from Customer infringes Applicable Data Protection Law, Provider shall promptly notify Customer.

3.3 Confidentiality. Provider shall ensure that all personnel authorized to Process Personal Data are bound by appropriate confidentiality obligations. Provider shall not disclose Personal Data to any third party except as expressly permitted by this DPA or as required by applicable law, and shall promptly notify Customer of any such legally required disclosure (to the extent permitted by law).

3.4 Enhanced Confidentiality for Drug and Alcohol Testing Data. Without limiting Section 3.3, with respect to any Drug and Alcohol Testing Data stored within the Services, Provider shall:

(a) Not release, disclose, or provide access to individual test results or medical information to any third party without Customer's prior written instruction confirming that the applicable Data Subject's specific written consent has been obtained in accordance with 49 CFR § 40.321;

(b) Not provide Drug and Alcohol Testing Data to any employer other than Customer without Customer's prior written instruction confirming that a specific, written consent (not a blanket release) has been obtained from the applicable Data Subject; and

(c) Maintain Drug and Alcohol Testing Data in a manner consistent with the controlled-access requirements applicable to such records under DOT Regulations.

4. DATA CATEGORIES AND DATA SUBJECTS

4.1 The following categories of Personal Data and Data Subjects are Processed under this DPA:

Data Subjects	Commercial motor vehicle drivers; driver applicants; other Customer personnel whose data is submitted to the Services

My Fleet Safety

Categories of Personal Data	Driver name, email address, Social Security number, driver's license number, employment applications, employment history, medical certificates, physical examination records, medical information, road test results, driving records (including motor vehicle records), investigation history files, annual review of driving records, date of birth, job title, and other Driver Qualification Data
Sensitive Personal Data	Social Security numbers, driver's license numbers, date of birth, medical information and records, and Drug and Alcohol Testing Data (if uploaded by Customer)
Purpose of Processing	Monitoring and managing compliance with DOT safety requirements, maintaining driver qualification files, and related fleet safety and compliance management functions

5. SECURITY MEASURES

5.1 Technical and Organizational Measures. During any beta, pilot, evaluation, or pre-release period under the Agreement (the "Beta Period"), Provider shall implement and maintain commercially reasonable technical and organizational security measures designed to protect Personal Data against unauthorized or unlawful Processing, accidental loss, destruction, damage, theft, or disclosure, taking into account the beta status of the Services, the current state of the platform, and the nature of the Personal Data Processed. During the Beta Period, these measures shall include, at a minimum:

(a) Encryption of Personal Data in transit;

(b) Access controls designed to limit access to Personal Data to authorized personnel on a need-to-know basis;

(c) Password-protected user accounts and administrative access controls for systems containing Personal Data;

(d) Internal review and remediation of identified security issues;

(e) Operational logging and review procedures designed to identify unauthorized access to systems containing Personal Data;

(f) Private, non-public storage of uploaded files, with access restricted through the Services and Provider's administrative controls; and

(g) Procedures for escalating and addressing identified security vulnerabilities.

5.2 Updates. Provider may update its security measures from time to time, provided that any update does not materially reduce the overall level of protection afforded to Personal Data.

5.3 Beta Security Roadmap. The parties acknowledge that, as of the effective date of this DPA, the Services are in beta and certain security features remain under development. Unless and until Provider notifies Customer in writing that a feature has been implemented and made available for the Services, Provider is not required under this DPA to maintain: (a) multi-factor authentication for Customer users; (b) infrastructure-level encryption at rest for uploaded files; (c) audit or access logs specific to Sensitive Personal Data file access; (d) a documented vulnerability assessment process; or (e) a documented security testing process. Provider will use commercially reasonable efforts to evaluate and implement these features as part of its post-beta security roadmap. Customer is responsible for determining whether the beta version of the Services is appropriate for the Personal Data Customer elects to submit during the Beta Period.

6. SUBPROCESSORS

6.1 Authorization. Customer provides general written authorization for Provider to engage Subprocessors to Process Personal Data in connection with the Services, subject to the requirements of this Section 6.

6.2 List of Subprocessors. Provider shall maintain a current list of Subprocessors and make it available to Customer upon request. Provider shall notify Customer at least thirty (30) days in advance of any intended addition or replacement of a Subprocessor.

6.3 Objection Right. If Customer reasonably objects to a new Subprocessor on data protection grounds within fifteen (15) days of receiving notice, the parties shall discuss Customer's concerns in good faith. If the parties are unable to resolve Customer's objection, Customer may terminate the affected portion of the Services without penalty by providing written notice within thirty (30) days following the end of the discussion period.

6.4 Subprocessor Obligations. Provider shall: (a) enter into a written agreement with each Subprocessor imposing data protection obligations no less protective than those set forth in this DPA; and (b) remain responsible for the acts and omissions of its Subprocessors with respect to Personal Data.

7. DATA SUBJECT RIGHTS

7.1 Assistance. Taking into account the nature of the Processing, Provider shall assist Customer, through appropriate technical and organizational measures, in fulfilling Customer's obligations to respond to Data Subject requests to exercise their rights under Applicable Data Protection Law.

7.2 Notification. If Provider receives a request directly from a Data Subject regarding Personal Data, Provider shall promptly redirect the Data Subject to Customer and notify Customer of the request, unless prohibited by applicable law.

7.3 Driver Access Requests. With respect to requests from drivers or other Data Subjects for copies of their own records (including requests that may arise under 49 CFR § 40.329), Provider shall cooperate with Customer to facilitate the response within any applicable regulatory timeframe.

8. SECURITY INCIDENT NOTIFICATION

8.1 Notification. Provider shall notify Customer without undue delay, and in no event later than seventy-two (72) hours, after becoming aware of a Security Incident affecting Personal Data Processed under this DPA.

8.2 Content. The notification shall include, to the extent reasonably available: (a) the nature of the Security Incident, including the categories and approximate number of Data Subjects and records affected; (b) the likely consequences of the Security Incident; (c) the measures taken or proposed to address the Security Incident; and (d) the identity and contact information of Provider's point of contact.

8.3 Cooperation. Provider shall cooperate with Customer and take reasonable steps to assist Customer in investigating, mitigating, and remediating the Security Incident, including providing information necessary for Customer to comply with any notification obligations under Applicable Data Protection Law.

8.4 No Determination by Provider. Provider's notification of a Security Incident shall not be construed as an acknowledgment of fault or liability.

9. DATA RETENTION AND RETURN

9.1 Retention During the Term. Provider shall retain Personal Data for the duration of the Agreement and shall not delete or destroy Personal Data during the term except upon Customer's documented instruction.

9.2 Regulatory Retention Obligations. Customer acknowledges that certain Personal Data is subject to mandatory minimum retention periods under DOT Regulations, including:

(a) **Five (5) years**: Records of verified positive drug test results, alcohol test results indicating a concentration of 0.02 or greater, documentation of refusals, substance abuse professional reports, and follow-up test records;

(b) **Three (3) years**: Information obtained from previous employers concerning drug and alcohol test results, and driver investigation history files (retention required for the duration of employment plus three years);

(c) **Two (2) years**: Equipment inspection, maintenance, and calibration records;

(d) **One (1) year**: Negative and cancelled drug test results and alcohol test results below 0.02.

Provider shall support Customer's compliance with these retention periods. The parties acknowledge that Provider's obligation to delete or return data under Section 9.3 is subject to Customer's compliance with its own regulatory retention obligations.

9.3 Post-Termination. Upon termination or expiration of the Agreement:

(a) Provider shall, at Customer's election, return or delete all Personal Data in Provider's possession within ninety (90) days following the effective date of termination, except to the extent that retention is required by applicable law or this Section 9.

(b) If Customer elects deletion, Provider shall certify in writing that all Personal Data has been deleted, except for copies retained in routine backup systems, which shall be deleted in accordance with Provider's standard backup rotation schedule (not to exceed one hundred eighty (180) days) and shall remain subject to this DPA until deleted.

(c) If Customer does not provide instructions within thirty (30) days following termination, Provider may delete all Personal Data and shall have no further obligation to retain it.

(d) Notwithstanding the foregoing, Provider shall cooperate with Customer's reasonable requests to export Personal Data in a structured, commonly used format prior to deletion.

10. AUDITS AND REGULATORY ACCESS

10.1 Audit Rights. Upon Customer's reasonable written request (not more than once per twelve-month period, unless a Security Incident has occurred or a regulatory investigation requires it), Provider shall make available to Customer information necessary to demonstrate compliance with this DPA, and shall permit and contribute to audits, including inspections, conducted by Customer or a qualified third-party auditor designated by Customer (and reasonably acceptable to Provider). Any audit shall be conducted during normal business hours, with reasonable advance notice, and shall not unreasonably interfere with Provider's operations.

10.2 SOC Reports. To the extent Provider maintains a current SOC 2 Type II report (or equivalent certification), Provider may satisfy its audit obligations under Section 10.1 by providing Customer with a copy of such report, unless Customer can demonstrate, on reasonable grounds, that additional audit measures are necessary.

10.3 DOT and FMCSA Regulatory Access. Provider acknowledges that Customer may be subject to inspection, audit, or investigation by DOT, FMCSA, or other federal or state regulatory authorities. Provider shall reasonably cooperate with Customer to facilitate Customer's compliance with regulatory access requirements, including:

(a) Making Personal Data available in an organized, legible, and easily accessible manner, consistent with the requirements of 49 CFR § 40.331(b) and (c); and

(b) Using commercially reasonable efforts to assist Customer in producing records within any timeframe required by DOT Regulations (including the two-business-day production requirement applicable to motor carriers under 49 CFR § 40.333(d)).

10.4 Costs. Each party shall bear its own costs in connection with audits and regulatory access. If an audit reveals a material breach of this DPA by Provider, Provider shall bear the reasonable costs of the audit.

11. CCPA-SPECIFIC PROVISIONS

11.1 Service Provider Status. For purposes of the CCPA, Provider is a "service provider." Provider shall not sell or share (as those terms are defined under the CCPA) Personal Data received from Customer.

11.2 Prohibition on Combining Data. Provider shall not combine Personal Data received from Customer with Personal Data received from or on behalf of another person or entity, or collected from Provider's own interaction with Data Subjects, except as necessary to perform the Services, to detect security incidents, or as otherwise permitted by the CCPA.

11.3 Right to Verify. Customer has the right to take reasonable and appropriate steps to help ensure that Provider uses Personal Data in a manner consistent with Customer's obligations under the CCPA. Provider shall comply with any reasonable verification request from Customer.

11.4 Notification of Inability to Comply. Provider shall notify Customer if it determines that it can no longer meet its obligations under the CCPA.

12. CROSS-BORDER TRANSFERS

Provider shall Process Personal Data within the United States. If Provider needs to transfer Personal Data outside the United States for any reason, Provider shall obtain Customer's prior written consent and ensure that appropriate safeguards are in place.

13. GENERAL PROVISIONS

13.1 Order of Precedence. In the event of any conflict 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 Applicable Data Protection Law or DOT Regulations, the applicable law or regulation shall control.

13.2 Liability. Each party's liability under this DPA shall be subject to the limitations and exclusions of liability set forth in the Agreement, except that neither party excludes or limits its liability for breaches of Section 3.4 (Enhanced Confidentiality for Drug and Alcohol Testing Data) caused by willful misconduct or gross negligence.

13.3 Term. This DPA shall remain in effect for the duration of the Agreement and shall automatically terminate upon termination or expiration of the Agreement, subject to Provider's obligations under Section 9 (Data Retention and Return), which shall survive termination.

13.4 Amendments. This DPA may be amended only by a written instrument signed by both parties. Provider may update the technical and organizational measures described in Section 5 in accordance with Section 5.2 without requiring a formal amendment.

13.5 Severability. If any provision of this DPA is held to be invalid or unenforceable, the remaining provisions shall continue in full force and effect.

13.6 Governing Law. This DPA shall be governed by the law governing the Agreement, unless an applicable Data Protection Law requires otherwise.