Data Processing Addendum

Provider Burnley Consulting, Inc. (myDesklog.com)

1. Parties and purpose

1.1. This Data Processing Addendum ("DPA") forms part of and is incorporated into the agreement between Provider and Customer governing the Services (the "Agreement").

1.2. Customer acts as the business customer that determines the purposes and means of processing the relevant Customer Data. Provider processes such Customer Data on Customer's behalf solely to provide and support the Services and to perform the Agreement.

2. Processing details

2.1. Subject matter of processing: hosted software for post-sale dealership workflow management, revenue estimate reporting, and issue tracking.

2.2. Duration of processing: the term of the Agreement plus any post-termination retention or deletion period stated in the Agreement or required by law.

2.3. Nature of processing: collection, storage, organization, retrieval, reporting, support, troubleshooting, backup, deletion, and other operations necessary to provide the Services.

2.4. Categories of data: employee first and last name, business email address, dealership account data, stock number, VIN, vehicle mileage, sale price, trade ACV, customer last name, revenue estimates, deal comments, lender name, support communications, and system usage logs.

2.5. Categories of data subjects: Customer personnel, dealership employees, and individual vehicle buyers or customers whose data is entered into the Service by Customer.

3. Provider obligations

3.1. Provider will process Customer Data only on documented instructions from Customer, including as set out in the Agreement and this DPA, unless otherwise required by law.

3.2. Provider will ensure that persons authorized to process Customer Data are subject to appropriate confidentiality obligations.

3.3. Provider will implement commercially reasonable technical and organizational measures designed to protect Customer Data against unauthorized or unlawful processing and against accidental loss, destruction, damage, alteration, or disclosure.

3.4. Provider's current measures include encryption in transit and generally at rest, backup and recovery procedures, and audit logging or activity tracking.

3.5. Provider will notify Customer without undue delay after becoming aware of a confirmed security incident affecting Customer Data and will provide reasonably available information needed for Customer to understand the incident and meet its own obligations.

4. Customer obligations

4.1. Customer is responsible for the legality, quality, and accuracy of Customer Data and for providing any notices and obtaining any permissions required for Provider to process it under the Agreement and this DPA.

4.2. Customer will not submit highly sensitive data, including payment card data, Social Security numbers, or bank account numbers, through the Service unless the parties expressly agree in writing to additional controls.

4.3. Customer acknowledges that payment information for subscription billing is collected and processed by Stripe, not stored by Provider within the Service.

5. Subprocessors

5.1. Customer authorizes Provider to use subprocessors to support delivery of the Services, provided Provider remains responsible for their performance of the relevant processing obligations.

5.2. Provider's current subprocessors include Microsoft Azure for hosting and Stripe for payment processing. Provider will maintain a current subprocessor list and will update it as needed.

5.3. If Customer reasonably objects to a new subprocessor based on a demonstrable data protection concern, the parties will work in good faith to address the concern.

6. Assistance and cooperation

6.1. Taking into account the nature of processing and the information available to Provider, Provider will provide reasonable assistance to Customer in responding to verified requests relating to personal information that Customer cannot address through the Service itself.

6.2. Provider will provide reasonable information about its security measures as necessary for Customer to assess Provider's compliance with this DPA, subject to confidentiality obligations and reasonable limits designed to protect security.

7. Deletion and return

7.1. Upon expiration or termination of the Agreement, Provider will make Customer Data available for retrieval for the period stated in the Agreement and will then delete or render inaccessible Customer Data unless legal retention obligations require otherwise.

8. Miscellaneous

8.1. Except as modified by this DPA, the Agreement remains unchanged and in full force.

8.2. If there is a conflict between this DPA and the Agreement regarding processing of Customer Data, this DPA controls to that extent.

8.3. This DPA is governed by the governing law and dispute provisions in the Agreement.