Data Processing Agreement

This Data Processing Agreement (DPA) is entered into by and between Automotive Development Services (hereinafter referred to as "Processor" or “ADS”) and your dealership or dealership group (hereinafter referred to as "Controller"). This agreement outlines the terms for processing and cleansing of Customer Personal Data by us as a Processor on your behalf in compliance with applicable data protection laws.

1. Definitions

- "Applicable Data Protection Laws" means all laws and regulations relating to the processing of Personal Data and privacy applicable to the Controller and Processor.
- "Personal Data" means any information relating to an identified or identifiable natural person as defined in Applicable Data Protection Laws.
- "Processing" means any operation performed on Personal Data, including collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available.

2. Purpose, Scope and Duration

- The Processor shall process Personal Data only for the purpose of providing data cleansing services to the Controller
- Duration of Processing:
    - Processing shall commence upon receipt of data from the Controller
    - All data shall be deleted within 60 days of project completion
    - Backup files shall be deleted within 10 days after delivery of cleaned files

3. Data Processing Obligations

- The Processor shall ensure that personal data is processed lawfully, fairly, and transparently.
- The Processor shall only act on documented instructions from the Controller.

4. Data Security Measures

The Processor shall implement and maintain appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including the following security measures:

Secure File Transfers

- **SFTP (Secure File Transfer Protocol):** All file transfers will use SFTP to ensure end-to-end encryption during transit.

Data Encryption

- **At Rest:** All data stored on the server is encrypted using AES-256 encryption to protect against unauthorized access.
- **In Transit:** TLS 1.3 encryption ensures all communications between dealers, servers, and systems are secure.

Access Control

- **Unique Credentials:** Each dealership will receive unique credentials to access their secure folder, preventing unauthorized access.
- **Strong Password Policy:** All user accounts are protected by passwords with a minimum complexity standard.

Network Security

- **Firewall Protection:**
    - An advanced OPNsense firewall protects the server, monitoring all incoming and outgoing traffic.
    - The firewall is configured to block unauthorized access and detect potential threats in real-time.
- **VPN Protection:**
    - All access to the server from external locations is secured using OpenVPN, ensuring a private and encrypted connection between users and the server.
    - This prevents unauthorized interception of data during remote access.

Compliance and Best Practices

- **Regular Security Updates:** The system is monitored and regularly updated to mitigate vulnerabilities.
- **Data Privacy Compliance:** All processes align with applicable regulations such as GDPR and CCPA.
- **Data Deletion:** All data is removed within 60 days of project completion.

5. Confidentiality

- The Processor shall ensure that persons authorized to process Personal Data have committed themselves to confidentiality
- Access to Personal Data shall be limited to those who need access

6. Subprocessors

- The Processor shall not engage third-party subprocessors without prior written authorization from the Controller.
- Any authorized sub-processors shall be bound by the same data protection obligations

7. Data Breach Notification

- In the event of a data breach, the Processor shall notify the Controller within 24 hours, providing all relevant details.

8. **Rights and Obligations of the Controller**

- The Controller is responsible for providing complete, accurate, and lawful instructions for processing personal data.
- The Controller must notify the Processor immediately of any potential or actual data breach.

9. **Audits**

- The Processor will
    - Maintain records of all processing activities
    - Make available to the Controller all information necessary to demonstrate compliance
    - Allow for and contribute to audits conducted by the Controller or an auditor mandated by the Controller

10. **Liability**

- The aggregate liability of either party towards the other party under or in connection with this DPA, or the Agreement, shall be limited to the greater of (i) USD $10,000 or (ii) the amount paid or payable by You to Ignitium under the Agreement in the twelve months immediately preceding the event giving rise to the claim.

11. **Governing Law**

This agreement shall be governed by and construed in accordance with the laws of the State of Washington.

12. **Termination and Deletion**

- The terms of this DPA shall continue in effect until the Agreement is terminated in accordance with the terms of the Agreement.
- Upon termination of this agreement, the Processor shall return or delete all personal data in accordance with the Controller's instructions.
- The Processor shall certify that all data has been deleted unless otherwise required by law.