DATA PROCESSING AGREEMENT

(the "Agreement")

This Data Processing Agreement is entered into by and between the person or entity that, alone or jointly, determines the purposes and means of processing Personal Information (synonymous with "business" under the California Consumer Privacy Act, as amended), and as identified in the Activation Agreement ("Controller," "Data Controller") and PINEWOOD NORTH AMERICA LLC, any group company or affiliate ("Processor," "Data Processor").

1. INTERPRETATION

1.1. The definitions and rules of interpretation in this clause apply in this Agreement.

Affiliate includes in relation to either party each and any subsidiary or holding company of that party and each and any subsidiary of a holding company of that party

Authorized Recipient has the meaning given to it in clause 12.3(a)

Business Day means Monday to Friday, excluding any public holidays

Business Purpose means the use of Personal Information that is reasonably necessary and proportionate to achieve an operational purpose of the Company, such as account management, security, or compliance,

Confidential Information means all information, data or materials received from the other (including, without limitation, drawings, sketches, photographs, vehicle prototypes, models, computer software, ideas, design, know-how, formulae, processes, copyrights, inventions, techniques, new product details, business plans and such other matters as may reasonably be regarded by either party as confidential and any copies thereof in any media whatsoever) shall be kept strictly confidential at all times.

Controller has the meaning set out in the Data Protection Legislation

Data Protection Legislation means applicable legislation relating to data protection and privacy which applies to either Party or all Parties to this Agreement

Data Protection Officer means a designated person appointed by each party with the same position and tasks to inform and advise, and to monitor compliance with

the requirements of each respective party as set out under the Data Protection Legislation

Data Privacy Notice means a notification given to the Data Subject concerned in relation to the processing of the Data Subject's Personal Data in accordance with the Data Protection Legislation

Data Subject an individual who is the subject of Personal Data

Dispute has the meaning given to it in clause 14

Group means a party and its Affiliates

Insolvency Event means, in respect of a party, the occurrence of any of the following events:

(a) it is unable to pay its debts as they fall due;

(b) it ceases, or threatens to cease, to carry on its business;

(c) any step is taken with a view to the appointment of a liquidator, receiver, administrator or administrative receiver to it or over any part of its undertaking or assets;

(d) it passes a resolution for its winding up (otherwise than for the purpose of a bona fide scheme of solvent amalgamation or reconstruction where the resulting entity assumes all of its liabilities);

(e) a court of competent jurisdiction makes an administration order or liquidation order or similar order in relation to it, or any step is taken with a view to obtaining such an order;

(f) it enters into, or proposes, any voluntary arrangement with its creditors; or

(g) any event analogous to those set out in paragraphs (a) to (f) above occurs in any jurisdiction in relation to it.

Personal Data/Information shall have the meaning set out in the Data Protection Legislation and more particularly described in Annex A and to include any other data processed by the Data Processor for the purposes of this Agreement

Processing and Process have the meaning set out in the Data Protection Legislation.

Processor has the meaning set out in the Data Protection Legislation

Purpose has the meaning given to it in Annex A

Regulator means any person or professional body or law enforcement agency anywhere in the world having regulatory, supervisory or governmental authority (whether under a statutory scheme or otherwise) over all or any part of the businesses of each of the parties to this Agreement

Recipient has the meaning given to it in clause 12.1(a)

Sub-processor means a third party that Processes Personal Information on behalf of the Processor pursuant to a written contract that restricts the Processing to specified Business Purposes.

1.2. The headings in this Agreement do not affect its interpretation. Except where the context otherwise requires, references to clauses and Annexes are to clauses and Annexes of this Agreement.

1.3. Unless the context otherwise requires:

(a) references to the Data Controller include their permitted successors and assigns;

(b) references to statutory provisions include those statutory provisions as amended or re-enacted;

(c) a reference to one gender includes a reference to the other genders; and

(d) references to "including" or "includes" shall be deemed to have the words "without limitation" inserted after them.

1.4. In the case of conflict or ambiguity between any provision contained in the body of this Agreement and any provision contained in the Annexes, the provision in the body of this Agreement shall take precedence.

1.5. Words in the singular include the plural and those in the plural include the singular.

1.6. A **person** includes a natural person, corporate or unincorporated body (whether or not having separate legal personality) and that person's personal representatives, successors or permitted assigns.

2. The Data Processor’s obligations

2.1. The Data Processor shall adhere to the instructions of a controller and shall assist the controller in meeting or complying with the controller’s duties, including the following:

(a) Assisting the controller in responding to consumer rights requests submitted, by using appropriate technical and organizational measures, as reasonably practicable, taking into account the nature of processing and the information available to the processor;

(b) Assisting the controller with regard to complying with the requirement relating to the security of processing personal data and to the notification of a breach of security of the processor’s system, taking into account the nature of processing and the information available to the processor;

(c) Providing necessary information to enable the controller to conduct and document data protection assessments.

3. Controls and other responsibilities of the Data Processor

3.1. The Data Processor shall;

(a) Appoint a Data Protection Officer whose name and contact details are shared with the Data Controller. Any change in the Data Protection Officer's contact details shall be supplied to the Data Controller.

(b) The Data Processor shall maintain confidentiality and all persons who have access to Personal Data belonging to the Data Controller under the terms of this Agreement undertake to maintain confidentiality and shall be informed of any special data protection requirements arising from the Agreement, and the limitation of use to specific purposes as instructed.

(c) The Data Processor shall implement and maintain all technical and organizational security measures required for the Agreement according to the Data Protection Legislation in addition to the measures specified in Annex B to the Agreement.

(d) The Data Processor shall immediately notify the Data Controller of any activities and measures including but not limited to monitoring activities undertaken by a Regulator.

(e) The Data Processor shall give all reasonable assistance to the Data Controller for the fulfilment of the Data Controller’ s accountability and documentation obligations arising under the Data Protection Legislation.

(f) The Data Processor shall assist the Data Controller, by implementing appropriate technical and organizational security measures, to enable the Data Controller to fulfil its obligation to respond to requests for exercising the Data Subject's rights under the Data Protection Legislation.

(g) The Data Processor shall assist the Data Controller to ensure compliance with the obligations pursuant to the Data Protection Legislation including without limitation, security, breach notification, data protection assessments and consulting with supervisory authorities, taking into account the nature of Processing and the information available to Data Processor.

(h) The Data Processor shall take reasonable steps to ensure the reliability of all its employees who have access to the Personal Data and shall ensure that only those of the Data Processor's personnel who need to have access to the Personal Data are granted access to such data and only for the purposes envisaged under this Agreement and all of the Data Processor's personnel required to access the Personal Data are adequately trained in all relevant Data Protection Legislations, and are under the same confidentiality obligations as the Data Processor.

(i) The Data Processor shall assist Data Controller in responding to consumer rights requests, including access, deletion, correction, opt-out of sale/sharing, and opt-out of automated decision-making. Responses must be provided within the statutory timelines and recorded.

(j) The Data Processor warrants that it has power to execute this Agreement and that once executed it will be binding upon it.

4. The Data Controller’s obligations

4.1. The Data Controller shall:

(a) Limit the collection of personal data to data that is adequate, relevant, and reasonably necessary in relation to the purposes for which it is processed, as disclosed to the consumer;

(b) For purposes of protecting the confidentiality, integrity, and accessibility of personal data, establish, implement, and maintain reasonable administrative,

technical, and physical data security practices appropriate to the volume and nature of the personal data at issue;

(c) Provide the Data Processor with the Personal Data, Data Protection Notice and such instructions and other information as are reasonably required to perform the services that the Data Processor has been engaged to do;

(d) Ensure that any instructions will comply with Applicable Laws;

(e) Warrants that it has power to execute this Agreement and that once executed it will be binding on it; and

(f) Appoint a Data Protection Officer whose name and contact details are shared with the Data Processor. Any change in the Data Protection Officer's contact details shall be supplied to the Data Processor.

4.2. The Data Controller may not do any of the following:

(a) Except as otherwise provided by this part, process personal data for a purpose that is neither reasonably necessary nor compatible with the purpose for which the personal data is processed, as disclosed to the consumer, unless the controller obtains the consumer’ s consent.

(b) Process personal data in violation of state or federal laws that prohibit unlawful discrimination against consumers.

(c) Discriminate against a consumer for exercising any of the consumer rights contained in this part, including by denying goods or services, charging different prices or rates for goods or services, or providing a different level of quality of goods or services to the consumer. A controller may offer financial incentives, including payments to consumers as compensation, for processing of personal data if the consumer gives the controller prior consent that clearly describes the material terms of the financial incentive program and provided that such incentive practices are not unjust, unreasonable, coercive, or usurious in nature. The consent may be revoked by the consumer at any time.

(d) Process the sensitive data of a consumer without obtaining the consumer’ s consent, or, in the case of processing the sensitive data of a known child, without processing that data with the affirmative authorization for such processing by a known child who is between 13 and 18 years of age or in

accordance with the Children’s Online Privacy Protection Act, 15 U.S.C. ss. 6501 et seq. for a known child under the age of 13.

5. Notification of Infringements

5.1. The Data Processor and the Data Controller shall without undue delay notify each other where errors, irregularities or suspected infringements of provisions relating to the protection of Personal Data occur. The Parties agree to take all reasonable measures in order to remedy infringements immediately.

5.2. The Data Processor shall without undue delay notify the Data Controller in all cases where the Data Processor or persons employed by them infringe provisions relating to the protection of Personal Data belonging to the Data Controller or any other stipulations set out in the Agreement.

5.3. The parties are aware that the Data Protection Legislation imposes a duty to inform in the event of a data protection infringement or breach. Such incidents (including but not limited to any loss, unlawful disclosure or unlawful access to Personal Data) shall therefore be notified to the Data Controller without undue delay. This also applies to serious operational faults or where there is any suspicion of an infringement of provisions relating to the protection of Personal Data or other irregularities in the handling of Personal Data belonging to the Data Controller. Notification shall include the nature of the infringement, categories of data affected, mitigation measures, and contact information. Upon consultation with the Data Controller, the Data Processor shall take appropriate measures to secure the data and limit any possible detrimental effect on the Data Subjects. Where obligations are imposed on the Data Controller under the Data Protection Legislation the Data Processor shall assist in complying with them.

5.4. The Data Processor shall provide the Data Controller with all reasonable co-operation and assistance in relation to any complaint or request made in respect of any Personal Data at the Data Processor’s cost except where the Data Controller is in breach of this Agreement, including by:

(a) providing the Data Controller with details of the complaint or request;

(b) complying with a subject access request within the relevant timescales set out in the Data Protection Legislation and otherwise in accordance with the Data Controller's instructions; and

(c) providing the Data Controller within the timescales reasonably required by the Data Controller (to comply with the Data Protection Legislation) with any Personal Data it holds on behalf of the Data Controller in relation to a Data Subject in accordance with the rights of the Data Subject to be provided in an electronic format together with details of how long the data is stored for and, where applicable, details of any data exports outside the originating jurisdiction and the safeguards deployed.

6. Sub-processors

6.1. The commissioning of sub-processors requires the general prior written consent of the Data Controller. Where the Data Controller grants such sub-processing, the Data Processor shall set out the contractual agreements with the sub-processor(s) in such a way that they reflect the data protection provisions agreed upon between the Data Controller and the Data Processor, including but not limited to technical and organizational security measures. Where a sub-processor is involved, the Data Controller shall be granted the right to monitor and audit the sub-processor in accordance with this Agreement and as required under the Data Protection Legislation. If the sub-processor fails to fulfil its data protection obligations the Data Processor shall remain fully liable to the Data Controller for the sub-processor ' s obligations together with its own.

6.2. Sub-processing does not include ancillary services commissioned by the Data Processor from third parties to assist in the performance of the processing. These may be for example telecommunications services, maintenance and user support (if no access to Personal Data of the Data Controller is possible), cleaning, auditing or the disposal of data media. The Data Controller must be informed of all sub-processing of document/data media disposal if the core activity of the commissioned Processing involves the disposal of documents/data media.

6.3. To safeguard the protection and security of the Data Controller's Personal Data the Data Processor shall nevertheless conclude adequate and lawful contractual agreements and undertake regular monitoring activities, even where ancillary services are commissioned from third parties.

7. Authority of the Data Controller to issue instructions

7.1. The Data Processor shall at all times be bound by the Data Controller`s instructions relating to the execution of this Agreement and the Processing of Personal Data belonging to the Data Controller. The Data Controller retains a general right of

instruction as to the nature, scope and method of data Processing, which may be supplemented with individual instructions. The Data Processor may only pass on information to third parties or to the Data Subject with the prior written consent of the Data Controller.

7.2. The Data Processor must not use the data for any other purpose than the execution of the Agreement and is not permitted to disclose the data to third parties. If the Data Processor is legally obliged to disclose any Personal Data, the Data Processor will immediately inform the Data Controller.

7.3. No copies or duplicates may be produced without the knowledge of the Data Controller. This does not apply to backup copies or to the readout of log files etc. where these are required to assure proper data Processing. The Data Processor shall inform the Data Controller immediately and prior to any Processing if the Data Processor believes that an instruction of the Data Controller constitutes an infringement of the Data Protection Legislation. The Data Processor then can postpone the execution of the relevant instruction until it is confirmed or changed by the Data Controller.

8. Audit Rights of the Controller

8.1. The Data Controller may carry out audits on the Data Processor's business premises before the start of the Processing and at reasonable intervals thereafter in order to verify compliance of the technical and organizational security measures implemented by the Data Processor to comply with the terms of this Agreement, or appoint auditors to do so. Audits shall not take place more frequently than once a year unless there is a regulatory investigation. The parties shall cooperate in order to agree upon reasonable terms and conditions for such audits. As a first step, upon request by the Data Controller, the Data Processor shall provide the Data Controller with evidence of its implementation of the technical and organizational security measures pursuant to this Agreement and the Data Protection Legislation.

8.2. For on-site audits, the Data Controller shall respect the operational activities and processes of the Data Processor and provide reasonable prior notice of audits at least 24 hours in advance.

8.3. The Data Processor undertakes at all times to assist the Data Controller in the execution of the audits.

8.4. The Data Processor undertakes upon request to provide the Data Controller with all the information required to meet the requirements of the Data Protection

Legislation and the audit rights referred to in this Agreement relating to the Processing of Personal Data, and make the necessary documentation available.

8.5. The Parties shall bear their own costs unless the audit reveals material non-compliance.

9. International transfers

9.1. Any transfer of data to a third country outside of the originating jurisdiction requires:

(a) The prior written consent of the Data Controller and is subject to compliance with the Data Protection Legislation; and

(b) the parties to enter into Standard Contractual Clauses or any equivalent replacement clauses which are issued as standard contractual clauses by the competent Regulator, a government department or any other similar body authorized to issue such clauses; and

(c) such other additional safeguards as required by a Regulator, a government department, any other similar body and/or by Data Protection Legislation regulating such transfers.

10. Correction, Deletion and Return of Personal Data

10.1. The Data Processor may only correct, delete or block Personal Data Processed on behalf of the Data Controller when instructed to do so by the Data Controller. If a Data Subject applies directly to the Data Processor for correction or deletion of his/her Personal Data, the Data Processor shall forward such request to the Data Controller without delay.

10.2. Upon completion of the contractual work or when requested by the Data Controller, the Data Processor shall return to the Data Controller all Personal Data in his possession and all work products and data produced in connection with the Agreement, or irrevocably delete or destroy them in compliance with the Data Protection Legislation with the prior consent of the Data Controller. The deletion log(s) or certificate(s) shall be presented upon request.

10.3. Documentation intended as proof of proper data Processing shall be kept by the Data Processor beyond the end of the Agreement in accordance with relevant retention periods. The Data Processor shall, upon request of the Data Controller,

hand such documentation over to the Data Controller after expiry of the Agreement.

10.4. The Data Processor shall maintain confidentiality also after the expiration of this Agreement relating to all Personal Data or other information from the Data Controller that came to his attention during the execution of this Agreement.

11. Warranties, Liability and Indemnification

11.1. Each party warrants to the other that it will process the Personal Data in compliance with all laws, enactments, regulations, orders, standards and other similar instruments applicable to it.

11.2. Each Party's aggregate liability under this Agreement shall be limited to 100% of the total Fees paid pursuant to the commercial agreement to which this Agreement relates, excluding breaches of confidentiality, data security obligations, or violation of state privacy statutes.

11.3. The Data Processor shall not be liable for any special, indirect or consequential loss, costs, damages, charges or expenses however arising under or in connection with this Agreement.

11.4. The Data Processor shall indemnify Data Controller for third-party claims arising from Data Processor's violation of applicable privacy laws or this Agreement.

11.5. Nothing in this Agreement excludes the liability of the Data Processor: for death or personal injury caused by the Data Processor's negligence; for fraud or fraudulent misrepresentation; or for any other liability which cannot be limited or excluded by applicable law.

12. Confidentiality

Obligation of confidence

12.1. Subject to Clause 12.2:

(a) each party undertakes to keep confidential and secure all Confidential Information given by or made available by one party to the Agreement (Disclosing party) to the other party (Recipient) or otherwise obtained, developed or created by the Recipient relating to the Disclosing party or any affiliate of either party; and

(b) the Recipient shall use the Confidential Information solely in connection with the performance of its obligations or exercise of its rights under the Agreement and not for its own benefit or for the benefit of any third party.

Excluded Categories of information

12.2. The restrictions on use or disclosure of information described in clause 12.1 above do not extend to any information which:

(a) is or becomes generally available to the public other than as a result of a breach of an obligation under this clause; or

(b) is acquired from a third party who owes no obligation of confidence in respect of the information; or

(c) is or has been independently developed by the Recipient or was in the Recipient’ s lawful possession prior to receipt from the Disclosing party.

Authorized Recipients

12.3. The Recipient may also disclose the Confidential Information:

(a) to the Recipient’ s members, directors, officers, employees, consultants, agents, advisers, contractors, subcontractors and Affiliates to whom disclosure of the Confidential Information is required for the performance of the Recipient's obligations or the exercise of its rights under the Agreement and then only to the extent necessary to perform such obligations or exercise such rights (together the Authorized Recipients); or

(b) pursuant to a binding request from any government or regulatory authority or as may be required by law or pursuant to a court order provided that, to the extent permitted by law, the Recipient gives prompt written notice of the request for disclosure to the Disclosing party, where practicable before it occurs, so that the Disclosing party may have an opportunity to prevent the disclosure through appropriate legal means.

12.4. Before disclosing Confidential Information to an Authorized Recipient, the Disclosing party shall procure that such Authorized Recipient has entered into confidentiality undertakings no less onerous than those contained in this clause and the Recipient shall remain fully liable to the Disclosing party for any breach of the terms of the Agreement by the Authorized Recipient.

General

12.5. Each party shall keep confidential and secure all copies of the Confidential Information that it holds or may hold.

12.6. This clause shall survive the termination or expiry of the Agreement howsoever arising and shall continue in force indefinitely.

12.7. The parties agree that damages may not be an adequate remedy for breach of this clause and (to the extent permitted by the court) that the party not in breach shall be entitled to seek an injunction or specific performance in respect of such breach.

12.8. Upon termination of the Agreement, the Disclosing party shall be entitled to require the Recipient to return or destroy all Confidential Information upon demand, save that the Data Processor shall be entitled to keep one copy of all Confidential Information provided to it by the Data Controller for record keeping purposes.

13. Miscellaneous

Waiver

13.1. No failure or delay by a party to exercise any right or remedy provided under this Agreement or by law shall constitute a waiver of that or any other right or remedy, nor shall it preclude or restrict the further exercise of that or any other right or remedy. No single or partial exercise of such right or remedy shall preclude or restrict the further exercise of that or any other right or remedy.

Remedies cumulative

13.2. Except as expressly provided in this Agreement, the rights and remedies provided under this Agreement are in addition to, and not exclusive of, any rights or remedies provided by law.

Entire Agreement

13.3. This Agreement, including the Annexes and the documents annexed as appendices to this Agreement contain the whole Agreement between the parties relating to the subject matter hereof and supersede all prior Agreements, arrangements and understandings between the parties relating to that subject matter.

13.4. Each party acknowledges that, in entering into this Agreement, it does not rely on any statement, representation, assurance or warranty (whether it was made negligently or innocently) of any person (whether a party to this Agreement or not) (Representation) other than as expressly set out in this Agreement.

13.5. Each party agrees that the only rights and remedies available to it arising out of or in connection with a Representation shall be for breach of contract.

Variation

13.6. No variation of this Agreement shall be effective unless it is in writing and signed by the parties (or their authorized representatives).

Severance

13.7. If any court or competent authority finds that any provision of this Agreement (or part of any provision) is invalid, illegal or unenforceable, that provision or part-provision shall, to the extent required, be deemed to be deleted, and the validity and enforceability of the other provisions of this Agreement shall not be affected.

Counterparts

13.8. This Agreement may be executed in any number of counterparts, each of which when executed and delivered shall constitute an original of this Agreement, but all the counterparts shall together constitute the same Agreement.

Third-party rights

13.9. A person who is not a party to this Agreement shall not have any rights to enforce any term of this Agreement, but this does not affect any right or remedy of a third party which exists.

Assignment and subcontracting

13.10. Subject to clause 13.11, neither party may assign, novate, sub-contract or otherwise dispose of the Agreement or any part of it without the prior written consent of the other party.

13.11. The Data Processor may assign all of its rights or transfer all of its obligations under the

13.12. Agreement, to any company within the Data Processor's Group or any person which acquires the whole or substantially the whole of the business to which this Agreement relates.

13.13. Subject to the provisions of clause 6, the Data Processor may authorize a third party to process the Personal Data (sub-contractor), provided that the sub-contractor's contract:

(a) is on terms which are substantially the same as those set out in this Agreement; and

(b) terminates automatically on termination of this Agreement for any reason.

No partnership or agency

13.14. Nothing in this Agreement is intended to, or shall be deemed to, establish any partnership or joint venture between any of the parties, constitute any party the agent of another party, nor authorize any party to make or enter into any commitments for or on behalf of any other party.

Notices

13.15. Any notice or other communication required to be given under this Agreement shall be in writing and shall be delivered personally, or sent by recorded delivery, registered post or by commercial courier, to each party required to receive the notice as set out below:

(a) Data Processor: Data Protection Officer, 500 E Broward Blvd, Suite 1025, Fort Lauderdale, Florida, 33394

(b) Data Controller: the Customer as detailed in the Activation Agreement or Master Service Agreement.

or as otherwise specified by the relevant party by notice in writing to each other party.

13.16. Any notice or other communication shall be deemed to have been duly received:

(a) if delivered personally, when left at the address and for the contact referred to in this clause;

(b) if sent by recorded delivery or registered post, at 9.00 am on the second Business Day after posting; or

(c) if delivered by commercial courier, on the date and at the time that the courier's delivery receipt is signed.

14. Dispute resolution

14.1. If there are any grounds for dispute refer to the terms and conditions.

15. Governing law and jurisdiction

15.1. This Agreement and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) shall be governed by the laws of the State of Florida.

15.2. The parties irrevocably agree that the federal courts located in Broward County, Florida shall have exclusive jurisdiction to settle any dispute or claim that arises out of or in connection with this Agreement or its subject matter or formation (including non-contractual disputes or claims).

ANNEX A – DATA INVENTORY

A.1. The purpose of the Data Processor's processing of personal data on behalf of the Data Controller is:

The Data Processor processes personal data on behalf of the Data Controller for the following purposes:

Provision of AI-powered conversational chatbot services for the automotive industry, including vehicle enquiries, lead generation, customer engagement, and dealership support.

Delivery of hosting, data storage, backup, and technical support services as defined in the Agreement.

Analytics, reporting, and performance monitoring of the chatbot platform.

Compliance with applicable legal obligations.

A.2. The Data Processor's processing of personal data on behalf of the Controller shall mainly concern (the nature of the processing):

- The nature of the processing carried out in accordance with the Agreement and in compliance with the Data Processing Agreement will include:
- Collection, storage, organization, and retrieval of personal data.
- Natural language processing (NLP) and AI/ML inference on conversational data, including intent classification, entity extraction, and response generation.
- Automated decision-making and/or profiling, where applicable, in relation to vehicle recommendations, lead scoring, or customer engagement optimization.
- Hosting, backup, and disaster recovery.
- Technical support and incident resolution.
- Analytics and aggregated reporting.
- Logging, monitoring, and security operations.
- Note: Customer personal data is not used for model training or fine-tuning unless the Data Controller provides explicit prior written consent and appropriate safeguards are in place.

A.3. The processing includes the following types of personal data about the data subjects:

- The processing will include the following categories of personal data about the data subjects:
- Identifiers (e.g., name, postal address, email address, phone number).
- Online identifiers (e.g., IP address, cookie identifiers, device IDs, browser fingerprints, session tokens).
- Conversational data (e.g., chat transcripts, messages, queries, and any free-text input provided by Data Subjects through the chatbot interface).
- Vehicle-related data (e.g., vehicle identification numbers (VINs), make, model, year, vehicle preferences, purchase or lease history, trade-in information).
- Commercial information (e.g., transaction history, pricing enquiries, financing interest, service history).
- Internet or network activity (e.g., log data, browsing behavior, referral URLs, interaction timestamps).
- Geolocation data (e.g., approximate location derived from IP address or device settings).
- Professional or employment-related information (e.g., job title, dealership affiliation, employer details where provided).
- Financial information (e.g., budget ranges, financing preferences, credit pre-qualification data where applicable and provided by the Data Subject).
- Inferences drawn from personal data (e.g., profiles, preferences, recommendations, or behavioral characteristics derived from the above categories, as required under CCPA/CPRA).
- Sensitive data: The Data Processor does not intentionally collect or process sensitive data. However, Data Subjects may inadvertently submit sensitive information through free-text chat fields. The Data Processor shall implement reasonable technical measures (e.g., automated detection and redaction) to minimize retention of inadvertently submitted sensitive data and shall promptly notify the Data Controller if systematic patterns are identified.

A.4. The processing includes the following categories of data subjects:

- The categories of data subjects are the identified or identifiable natural persons whose personal data is processed under the Data Processing Agreement. Personal data concerning the following categories of data subjects is processed under the Data Processing Agreement:
- The Data Controller's customers (end consumers interacting with the chatbot).
- Prospective customers, website visitors, and leads who interact with the chatbot before entering a commercial relationship.
- The Data Controller's employees and authorized personnel who access or administer the platform.
- Dealership staff and third-party users who interact with or manage the chatbot on behalf of the Data Controller.

A.5. Duration of processing and retention periods:

Personal data shall be processed for the duration of the Agreement. Upon termination or expiry of the Agreement, the Data Processor shall return or securely delete all personal data in accordance with Clause 9 of this Agreement.

Specific retention periods:

- Active conversational data: retained for the duration of the Agreement or as instructed by the Data Controller.
- Log and system data: retained for a maximum of 12 months for security and operational purposes, unless otherwise instructed.
- Backup data: retained in accordance with the Data Processor's documented backup schedule, not exceeding 90 days after deletion from production systems.
- The Data Controller may issue written instructions to adjust retention periods within the bounds of applicable law.

A.6. Geographic scope and data subject jurisdictions:

This Agreement covers the processing of personal data of Data Subjects located in:

- The United States, including but not limited to jurisdictions covered by the California Consumer Privacy Act (CCPA/CPRA), Colorado Privacy Act (CPA), Virginia Consumer Data Protection Act (VCDPA), Connecticut Data Privacy Act (CTDPA), and other applicable state privacy laws.

ANNEX B – SECURITY MEASURES

Organizational security

- The Data Processor has a documented information security policy, aligned with recognized frameworks (e.g., ISO 42001, SOC2 Trust Service Criteria), that addresses how information security is anchored and implemented in the Data Processor's Organization.
- The Data Processor maintains and enforces policies for the secure handling of information and for the purpose of ensuring that personal data is processed in accordance with applicable law. The Data Processor will take appropriate steps to ensure that such policies are known to all employees by conducting mandatory security awareness training upon onboarding and at regular intervals thereafter (at least annually).
- The Data Processor will ensure that third-party service providers comply with a minimum set of controls prescribed by the Data Processor and are subject to confidentiality obligations before they are commissioned. Vendor security assessments shall include review of SOC2 reports, security questionnaires, and contractual flow-down of data protection obligations.
- The Data Processor regularly checks third-party services and Sub-processors based on the risk of their processing of personal data, including periodic re-evaluation at least annually.
- Taking into account the current technological level, the implementation costs and the nature, scope, context and purpose of the processing in question, the Data Processor will implement and comply with the principles of data protection through design and by default throughout all phases of the information's and system's life cycle.
- The Data Processor maintains a current SOC2 Type II report. A summary or copy of the most recent SOC2 Type II report shall be made available to the Data Controller upon written request.

Physical security

- Locations, including data centers, offices and off-site storage facilities, or locations from which the Data Controller's information can potentially be

accessed, have appropriate physical security controls (e.g., access card systems, visitor logs, CCTV monitoring) to protect against unauthorized access.

- The Data Processor will ensure the secure disposal of information, media, equipment and paper in accordance with recognized industry standards (e.g., NIST SP 800-88 for media sanitization).

System and network security

- Networks and devices on which personal data is processed are protected against unauthorized access or infiltration, both internally and externally.
- Network security is maintained using commercially available equipment and industry-standard techniques, including performing periodic external vulnerability scanning and penetration testing (at least annually by a qualified independent party), and maintaining perimeter defenses, such as firewalls and intrusion prevention and detection.
- The infrastructure will at least be segmented into separate production systems and away from test and development environments. Personal data from production systems is not used in non-production environments without appropriate anonymization or pseudonymization.
- Antivirus and anti-malware programs are used on operating systems together with security configurations. The Provider's recommended security patches are deployed on both applications and operating systems in a timely manner, following a documented patch management process.
- Updated malware protection is installed and maintained on all systems exposed to malware.
- All personal data transmitted by the Data Processor is encrypted in transit (TLS 1.2 or higher) and at rest (AES-256 or equivalent). Encryption key management follows industry best practices.
- Risk assessments are performed and documented using industry-recognized methodologies, such as the Cloud Security Alliance or equivalent, ISO 27001, NIST RMF, or other independent schemes.
- Mobile device administration software is used to manage security controls on both corporate and employee devices used for business purposes.

API and application security

- All APIs exposing or processing personal data are secured with authentication (e.g., API keys, OAuth 2.0), authorization controls, rate limiting, and input validation.
- The Data Processor follows a Secure Development Lifecycle (SDLC), including code review, static and dynamic application security testing (SAST/DAST), and security review as part of the CI/CD pipeline.
- Application dependencies are monitored for known vulnerabilities and updated promptly.

AI/ML-specific security controls

- AI models used to process personal data are subject to access controls, versioning, and change management procedures. Model deployments are logged and auditable.
- The Data Processor implements safeguards against prompt injection, adversarial inputs, and other AI-specific attack vectors, including input sanitization and output filtering.
- Output moderation and content filtering mechanisms are in place to prevent the generation of harmful, discriminatory, or inappropriate content.
- Customer personal data is not used for model training or fine-tuning unless the Data Controller provides explicit prior written consent. Where consent is provided, training data is isolated and subject to additional access controls.
- Model inputs and outputs containing personal data are logged in accordance with the logging requirements in this Annex and are subject to the same retention and deletion policies as other personal data.
- Regular bias and fairness assessments are conducted on AI models that produce recommendations, scores, or other outputs that could materially affect Data Subjects.

Access management

- The Data Processor ensures that the Data Controller's personal data is only accessed by authorized persons using the procedures for access management, which ensure access on a "least privilege" basis, and that access is terminated where and when appropriate.

- The Data Processor has user administration procedures in place that define user roles and their privileges, and how access is granted, changed and terminated.

- The Data Processor performs regular checks of the assigned rights (at least quarterly). The controls are documented and the documentation can be provided to the controller upon request.
- Systems used to process the Data Controller's personal data shall be further secured through multi-factor authentication (MFA) for all remote access, administrative access, and access to systems processing personal data.
- Privileged access is subject to additional controls, including separate accounts, session monitoring, and just-in-time provisioning where feasible.

Logging

- All login attempts, including failed attempts, are logged to register unauthorized access to personal data.
- All access to personal data is logged, and the access log includes the date and time of access, user ID and the type of access (read, edit, delete, search criteria, etc.).
- Security logging is activated on all network equipment, servers and on all applications, including databases and IT system administrators.
- A log of access to personal data and the use of personal data is monitored and regularly reviewed by the Data Processor in order to register unauthorized access to personal data.
- The Data Processor has a documented procedure for how often log files are reviewed and who has carried out the control. Documentation can be made available to the Data Controller upon request.
- Logs are protected against tampering, unauthorized access, and premature deletion. Log retention periods are defined and documented.

Pseudonymization and anonymization

- The Data Processor applies pseudonymization techniques to personal data where feasible and appropriate to the processing activity, ensuring that additional information required for re-identification is kept separately and securely.
- Where personal data is used for analytics or reporting, the Data Processor shall apply anonymization or aggregation techniques such that individual Data Subjects cannot be re-identified.

- Automated detection and redaction mechanisms are implemented for conversational data to identify and minimize the retention of sensitive data inadvertently submitted by Data Subjects through free-text input.

Data loss prevention

- The Data Processor implements Data Loss Prevention (DLP) controls to detect and prevent unauthorized exfiltration, leakage, or exposure of personal data.
- DLP controls cover key data egress points, including email, file transfers, API endpoints, and cloud storage.

Change management

- The Data Processor maintains documented change management procedures for all systems that process personal data. Changes are assessed for security impact, tested in non-production environments, and approved before deployment to production.
- Emergency changes are subject to retrospective review and documentation within a defined timeframe.

Backup

- The Data Processor performs a backup of the personal data processed on behalf of the Data Controller and has procedures in place to ensure the restoration of backed-up data in a timely manner to ensure accessibility and access to personal data.

- The Data Processor has a documented procedure for performing backup copying. Such a procedure has identified the requirements for storing and deleting data.

- The Data Processor has implemented procedures to verify backups upon successful re-introduction of backed up data, software and systems at least every six months.

- Backups are protected against unauthorized access, including destruction, and must be encrypted if the backup contains personal data where encryption based on a risk assessment is required.

Availability, business continuity and disaster recovery

- The Data Processor has implemented procedures for the effective detection, analysis and handling of security incidents to ensure the availability of personal data.
- The Data Processor has implemented a documented and tested disaster recovery plan and a business continuity strategy covering systems used to process personal data.
- Disaster recovery plans and business continuity strategies are tested and updated regularly and at least annually to ensure that they are up-to-date and effective. Documentation can be made available to the Data Controller upon request.

Incident response

- Incident reports shall include the nature and scope of the incident, categories and approximate number of Data Subjects affected, likely consequences, and measures taken or proposed to mitigate impact.
- Post-incident reviews are conducted, root causes identified, and remediation measures implemented and documented.
- Incident reports shall include the nature and scope of the incident, categories and approximate number of Data Subjects affected, likely consequences, and measures taken or proposed to mitigate impact.
- Post-incident reviews are conducted, root causes identified, and remediation measures implemented and documented.

Data retention and secure deletion

- Personal data is retained only for as long as necessary to fulfil the purposes described in Annex A, or as required by applicable law.
- Upon expiry or termination of the Agreement, or upon instruction by the Data Controller, personal data is securely deleted or returned in accordance with Clause 9 of the Agreement.
- Secure deletion methods include cryptographic erasure, overwriting, or physical destruction as appropriate. Deletion certificates are provided upon request.
- The Data Processor maintains documented data retention schedules that align with the retention periods specified in Annex A.