License Agreement
Scan Tool Central Gateway and MAC Keys Access

This License Agreement (this "**Agreement**"), dated and effective as of the __ day of Select _____ 202_ (the "**Effective Date**"), is made and entered into by and between _____, a Select An Item , Select An Item ("**Company**"), and Nissan North America, Inc., a Delaware corporation ("**Nissan**") (each, a "**Party**" and collectively, the "**Parties**"). For purposes of this Agreement, Contractor acknowledges and agrees that all rights granted to Nissan under this Agreement shall also be deemed to include all entities directly or indirectly controlled by, controlling, or under common control with Nissan or its affiliates ("**Affiliates**"). As used in this Agreement, all references to "include" or "including" mean inclusive by way of example, and do not mean restrictive by way of limitation.

WHEREAS, Nissan is engaged in design, development, manufacture, and assembly of various models of motor vehicles and parts thereof and also in the distribution and sale of such motor vehicles and parts throughout the world. Certain Nissan vehicles (including certain Infiniti models) have a central gate way ("**CGW**") that requires unlocking to allow a scan tool to transmit electronic messages to, or read messages from certain electronic control units (each, an "**ECU**");

WHEREAS, certain Nissan/Infiniti vehicles come equipped with message authentication code ("**MAC**") ECU that require MAC keys ("**MAC Keys**") for authentication of in-vehicle communication. A MAC Key is specifically designated for use in connection with a specific vehicle, as designated by the vehicle's unique vehicle identification number ("**VIN**") (such MAC Keys as applied to VINs, the "**VIN-Specific MAC Keys**");

WHEREAS, in the event of damage or failure that requires replacement of an affected MAC ECU (as replaced, the "**Replacement MAC ECU**"), VIN-Specific MAC Keys must be updated in the Replacement MAC ECU by a scan tool in order to allow continued in-vehicle communication by the Replacement MAC ECU with other MAC ECUs, such updating being necessary to the replacement process because a newly installed Replacement MAC ECU automatically defaults to its factory setting standard issue default MAC Keys rather than retaining the VIN-Specific MAC Keys that were previously housed by the pre-replacement MAC ECU;

WHEREAS, VIN-Specific MAC Keys can only be provided to a scan tool via server-to-server communication from Nissan's backend server; and

WHEREAS, Company desires to obtain technical specifications to request and retrieve VIN-Specific MAC Keys, including, but not limited to, API information, client ID, client secret, and certificate details for use by Company as permitted herein, along with Nissan Scan Tool Data (as defined below), which Nissan Scan Tool Data must be also purchased by Company from Nissan pursuant to a separate license agreement entered into by and between the Parties, with the terms and conditions of such separate license agreement governing the licensing of the Nissan Scan Tool Data; and

WHEREAS, for the avoidance of doubt: The Keys and the Nissan Scan Tool Data function together and the Keys and Nissan Scan Tool Data can only function together in combination, with neither able to function independent of the other.

NOW, THEREFORE, in consideration of the fees and mutual promises herein contained and other good and valuable consideration the receipt and sufficiency of which are hereby acknowledged, the Parties agree:

1. **Definitions** – In addition to any other defined terms expressed elsewhere in this Agreement (including the defined terms contained in Exhibit 1 and Exhibit 2) for use herewith, for purposes of this Agreement:

   (a) "**Annual Fee**" means the annual fee owed by Company to Nissan for Company's license of the Nissan Scan Tool Data, as such fee is further described hereinafter (see Exhibit 1).

   (b) **"Authorized Scan Tool**" means a scan tool as described hereinafter (see Exhibit 1).

   (c) **"Initial Fee**" means a one-time set-up fee, as set forth on Exhibit 1 of this Agreement.

   (d) **"Nissan Scan Tool Data**" means electronic messages transmitted between a scan tool and an ECU on-board a Nissan/Infiniti vehicle for the purposes of performing diagnosis, tests, and repairs of the Nissan/Infiniti vehicle within the North American market, and includes without limitation: (a) read only messages (e.g. sensor values, I/O switch states, etc.); (b) bi-directional messages, work support (e.g.,

operation of actuators, initiation of self-checks, etc.); (c) special diagnostic test routine, work support (e.g. VIN initialization, cylinder balance test, etc.); (d) vehicle data communication requirements (e.g. vehicle connector terminal/pin out definitions, physical layer definitions, etc.); (e) ECU data communication requirements (e.g. diagnostic protocols, data link layer definitions, etc.); (f) vehicle application information (e.g. ECU information charts, etc). For the avoidance of doubt, Nissan Scan Tool Data does not include programming/reprogramming software, e.g.: the J2534 software; the files that are flashed into a memory of a controller in a Nissan/Infiniti vehicle when the controller is programmed/reprogrammed; security algorithms; and the like.

(e) "**Permitted Use**" means the permitted use of the Keys by Company as set forth herein.

(f) "**Personal Data**" means any data that can be used, alone or in combination with other data, to identify any individual person or as otherwise prescribed by applicable law. Personal Data includes name, address, date of birth, social security number, email address, VIN, credit card information, mother's maiden name, and other information used to authenticate identity, biometric records, educational information, financial information, or employment information.

(g) "**Term**" means the time period of the Agreement as set forth in this Agreement's Section 6 and described more particularly by Sections 6-7 of this Agreement.

2. **License Grant.** Nissan hereby grants to Company a limited, non-exclusive, revocable, non-transferable, non-sublicensable, license to access and use the Keys for the purpose of making Authorized Scan Tools and distributing such Authorized Scan Tools within the Territory (the "**License**"). This License is granted solely for the Permitted Use in the Territory during the Term. The License shall expire upon the expiration or termination of this Agreement. Upon any such expiration or termination, all license rights granted hereunder shall automatically be extinguished with respect to Company and, contemporaneously therewith, all such rights shall revert to Company's possession with immediate effect. Except for the express License granted herein, no other licenses are granted by implication, estoppel, or otherwise. Nissan may revoke the License with respect to particular specified Keys by notice in writing to Company without termination of this Agreement.

3. **Delivery of the Keys**.

(a) Nissan will activate server-to-server communication for the provision of the Keys as soon as reasonably possible upon Nissan's receipt of the Initial Fee and Annual Fee paid by Company.

(b) From time to time during the Term of this Agreement, Nissan may provide Company any additional and/or updated the Keys in any form without notice.

4. **Restrictions.**

(a) Company shall not use the Keys except for the Permitted Use in the Territory. Nissan Data and Nissan Materials shall only be stored and maintained within the United States and shall not be transferred or used outside of the United States. Except as expressly allowed by the Permitted Use, Company will not: (a) sublicense, resell, rent, lease, transfer, assign, time share, broadcast, republish, modify, distribute, or otherwise commercially exploit or make the Keys available to any third party; (b) other than as expressly agreed between the Parties, modify, adapt, or hack the Nissan Materials to, or otherwise attempt to gain unauthorized access to the Nissan Data, Nissan Materials, or any Nissan networks; (c) remove any proprietary notices, attributions of Nissan, or third party providers, users, or otherwise, or remove any labels from the Keys; or (d) publish, enhance, or display any compilation or directory based upon information derived from the Keys. In addition to the foregoing, Company shall not: (i) use the Keys in any unlawful manner or in violation of any third party rights, or (ii) reverse engineer the Keys, or attempt to do so, in a manner that allows identification of any vehicle or natural person.

(b) Company shall adhere to other restrictions included in this Agreement's Exhibit 1 and Exhibit 2, each of which exhibits is hereby incorporated into this Agreement and made a part hereof by this reference.

(c) Company shall not request or attempt to obtain or process any Personal Data except as set forth in this Agreement. If Company receives any Personal Data from Nissan outside the scope of this Agreement, Company will promptly notify Nissan and delete any such Personal Data from Company's systems.

5. **Fees; Taxes**.

(a) The applicable License Schedule sets forth the fees to be paid to Nissan in exchange for the license granted hereby. Fees shall be paid without offset or deduction within [30 days] of Nissan's issuance of an invoice. The applicable License Schedule or the Purchase Order also designates Nissan's authorized representative for purposes of this Agreement.

(b) Nissan and Company shall each be responsible for any personal property taxes or other similar taxes on property it owns or leases for its own use, for franchise and privilege taxes on its business, and for taxes based on its net income or gross receipts.

(c) Company shall be responsible for any sales, use, excise, value-added, goods and services, consumption, withholding, and other similar taxes and duties that are imposed by law on Company in connection with the consumption and/or use of the License, the Nissan Data, and/or Nissan Materials. Company shall be responsible for such taxes whether those taxes exist as of the Effective Date or, during the term of the Agreement, go into effect or increase.

(d) Nissan shall be responsible for any sales, use, excise, value-added, goods and services, consumption, withholding, and other similar taxes and duties that are imposed by law on Nissan in connection with the provision of the License, the Nissan Data, and/or Nissan Materials. Nissan shall be responsible for such taxes whether those taxes exist as of the Effective Date or, during the term of the Agreement, go into effect or increase.

(e) Nissan and Company shall cooperate with each other to enable each to more accurately determine its own tax or duty liability and to minimize such liability to the extent legally permissible.

(f) Company shall provide and make available to Nissan the following information, if applicable: (1) resale or exemption certificates; and (2) applicable withholding tax forms, including federal forms W-9, W8-BEN, and W8-ECI.

(g) Nissan and Company shall promptly notify each other of, and coordinate with each other regarding the response to and any settlement of, any claim for taxes asserted by applicable taxing authorities. It is understood that the party against whom such claim is asserted shall have the right to control the response to and settlement of such claim, but the other party shall have the right to participate in any response or settlement that involves its own potential responsibilities or liabilities.

6. **Term and Termination**.

(a) This Agreement shall have an initial term of one (1) year commencing on the Effective Date. Upon expiration of the initial term, this Agreement shall automatically renew for successive one (1) year terms (each, a "Renewal Term") unless either party provides written notice of its intent not to renew at least thirty (30) days prior to the expiration of the then-current term. This automatic renewal shall continue for successive Renewal Terms under the same terms and conditions unless otherwise agreed in writing by the parties or terminated in accordance with this Agreement.

(b) In addition to other termination rights expressly set forth in this Agreement, either party may terminate this Agreement effective upon written notice to the other if the other party violates any covenant, agreement, representation, or warranty contained herein in any material respect or defaults or fails to perform any of its obligations or agreements hereunder in any material respect, which violation, default, or failure is not cured within thirty (30) days after notice thereof from the non-defaulting party stating its intention to terminate this Agreement by reason thereof. Material breach by Company includes: (i) breach of any restriction or otherwise infringing Nissan's proprietary rights by Company or third parties; (ii) violation of the license grants; (iii) nonpayment of fees; (iv) attempts to assign this Agreement; or (vii) breach of confidentiality obligations.

(c) If underpayment or nonpayment of the fees occurs more than two (2) times, then Nissan will have the right to terminate this Agreement immediately for cause and Company shall have no right to cure.

(d) Either may terminate this Agreement by delivering written notice to the other party upon the occurrence of any of the following events: (i) a receiver is appointed for either party or its property; (ii) either party makes a general assignment for the benefit of its creditors; (iii) either party commences, or has commenced against it, proceedings under any bankruptcy, insolvency, or debtor's relief law, which proceedings are not dismissed within sixty (60) days; or (iv) either party is liquidated or dissolved.

(e) Nissan may terminate this Agreement to the extent any continued performance by the Company is deemed to be unlawful, as determined in Nissan's sole discretion.

(f) Any provision in this Agreement that, in order to give proper effect to its intent, would or should survive any expiration or termination of this Agreement shall so survive.

7. **Effect of Termination**. Upon the conclusion of the Term (and any time upon request of Nissan) Company will delete the Nissan Data and Nissan Materials, and promptly shall provide written certification of such deletion to Nissan. Paper, film, or other hard copy media shall be shredded or destroyed such that the information contained thereon cannot be read or reconstructed. Electronic media shall be cleared, purged or destroyed consistent with the most current revision of NIST Special Publication 800-88, Guidelines for Media Sanitization, such that the Nissan Materials cannot be retrieved.

8. **Intellectual Property Rights**. Nissan shall retain all right, title and interest in and to the Nissan Data and Nissan Materials and all derivative works thereof, including all analog, digital, or other works that are created from and/or based in any way on the Keys. Nothing herein shall be deemed to grant, transfer, assign, or set over unto Company any other right, title, interest, or ownership in or of the Nissan Materials, all of which rights, title, interest, and ownership are hereby expressly reserved by Nissan.

9. **Confidential Information.** "**Confidential Information**" means any proprietary information, software, and know-how disclosed or made available by either party or its (as applicable) Affiliates or affiliates (the "**Disclosing Party**") to the other party (the "**Receiving Party**") hereunder, including, but not limited to, the Keys, financial, marketing, technical, engineering, design, or other information. The Receiving Party shall: (i) not use the Disclosing Party's Confidential Information except for the exercise of its rights or performance of its obligations hereunder; (ii) not disclose such Confidential Information to any party, other than its employees and consultants (including its advisors and other agents) who have a "need to know" for the Receiving Party to exercise its rights or perform its obligations hereunder; and (iii) use at least reasonable measures to protect the confidentiality of such Confidential Information. Further, the provisions of this Agreement shall be deemed Confidential Information of both Parties, and the Nissan Materials shall be deemed Nissan's Confidential Information. If the Receiving Party is required by law to make any disclosure of such Confidential Information, the Receiving Party shall first give written notice of such requirement to the Disclosing Party and shall permit the Disclosing Party to intervene in any relevant proceedings to protect its interests in the Confidential Information and provide full cooperation to the Disclosing Party in seeking to obtain such protection. Information will not be deemed Confidential Information hereunder if such information: (1) is known or becomes known (independently of disclosure by the Disclosing Party) to the Receiving Party prior to receipt from the Disclosing Party from a source other than one having an obligation of confidentiality to the Disclosing Party; (2) becomes publicly known, except through a breach hereof by the Receiving Party; or (3) is independently developed by the Receiving Party without any use of the Disclosing Party's Confidential Information. Company acknowledges and agrees that Nissan (a) is actively involved in evaluating potential transactions and business opportunities with many third parties and may consider or enter into a transaction with a third party in the same or similar business as the Company; and (b) may currently or in the future be developing information internally, or receiving information from other parties, that is similar to the Company's Confidential Information. Accordingly, provided that Nissan complies with the provisions of this Agreement regarding the use and disclosure of Confidential Information, this Agreement shall not in any manner (1) preclude, limit or affect Nissan's present or future business activities of any nature, including business activities which are or could be competitive with the business activities of the Company; or (2) be construed as a representation or agreement that Nissan is not in the process of, will not develop or have developed for it or for its use products, concepts, systems or techniques that are similar to or compete with the products, concepts, systems or techniques contemplated by or embodied in such Confidential Information. Nissan shall be free to use for any purpose the residuals resulting from access to or work with the Company's Confidential Information; provided, that Nissan shall not disclose the Confidential Information of the Company except as expressly permitted pursuant to the terms of this Agreement. The term "residuals" means information which is retained in memory by persons who have had access to Confidential Information, including ideas, concepts, know-how or techniques contained therein (if any). Nissan shall not have any obligation to limit or restrict the assignment of such persons or to pay royalties for any work resulting from the use of residuals. The terms of this Agreement will be treated as confidential by Company. The provisions of this Section shall survive the expiration or termination of this Agreement for any reason.

10. **Compliance with Laws**: Company shall at all times comply with all laws applicable to the use of the Nissan Data and Materials.

11. **Disclaimer of Warranties:** THE KEYS ARE PROVIDED "AS IS" WITHOUT ANY WARRANTY OF ANY KIND. NISSAN DISCLAIMS ANY AND ALL WARRANTIES, REPRESENTATIONS, AND CONDITIONS RELATING TO THE KEYS, WHETHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, ANY REPRESENTATION,

WARRANTY, OR CONDITION OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR TITLE WITH RESPECT TO THE KEYS.

12. **Limitation of Liability:** EXCEPT FOR LIABILITY ARISING FROM A BREACH OF SECTIONS 2, 4, 8, 9, 10, AND/OR 14 OR WITH RESPECT TO OR ARISING OUT OF COMPANY'S INDEMNIFICATION OBLIGATIONS HEREUNDER (INCLUDING, FOR THE AVOIDANCE OF DOUBT, WITH REFERENCE TO SECTION 13), IN NO EVENT WILL EITHER PARTY BE LIABLE HEREUNDER FOR (A) LOSS OF PROFITS, REVENUE, OR LOSS OR INACCURACY OF DATA, OR ANY INDIRECT, INCIDENTAL, PUNITIVE, SPECIAL OR CONSEQUENTIAL DAMAGES, OR (B) EXCEPT WITH RESPECT TO FEES AND INTEREST OWED, ANY OTHER AMOUNTS IN EXCESS OF THE FEES PAID DURING THE TWELVE (12) MONTH PERIOD PRECEDING THE EVENT OR CIRCUMSTANCES GIVING RISE TO SUCH LIABILITY, IN EACH CASE EVEN IF THE PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

13. **Indemnity.** Company shall indemnify, defend and hold Nissan, its officers, directors, employees, parent, subsidiaries, and Affiliates, harmless from and against any and all claims, demands, losses, liabilities, costs and expenses, including attorneys' fees (collectively, "**Claims**"), to the extent arising from or alleged to arise from any third party claim arising from or alleged to arise from: (a) a breach of Section 4, Section 9, Section 10, or Section 14 by Company, its employees, agents, permitted subcontractors, or representatives; (b) Company's use of subcontractors in connection with this Agreement; or (d) any claims or allegations by a third party that its copyrights, patent rights (including applications for patent protection); publicity rights, trade secret rights; registered or otherwise protected trademarks, trade names and service marks or other contractual right or obligation or other industrial or proprietary right held of claimed by such third party have been infringed by the use or receipt of Keys to the extent such claim would not exist but for Company's use of the same. Company shall defend any Claim at its expense and shall pay all settlements approved by Nissan and any judgments which shall be finally awarded. With respect to any Claim, Company shall defend the claim at its expense, shall control the defense (subject to the right of Nissan to hire counsel at its own expense to assist in the defense of the claim), and shall pay all settlements that are approved in advance by Nissan and any judgments that are finally awarded. Company shall settle no Claim without the prior approval of Nissan. With respect to any tax claim asserted as described in Section 5(h) of this Agreement, the parties agree that Section 5(h) of this Agreement shall apply together with this Section 13 with Section 5(h) prevailing in the event of any conflict between the two. Company waives all rights of subrogation with respect to the indemnity obligations in this Section 13. The provisions of this Section 13 shall survive the expiration or earlier termination of this Agreement.

14. **Safeguarding Data and Security of Systems**. Company shall abide by all policies and procedures provided by Nissan applicable to Company's provision of the Services, as determined by Nissan, including without limitation all policies and procedures governing access to Nissan's facilities or information security. Company shall establish and maintain safeguards against the disclosure, destruction, loss, copying or alteration of Nissan's Confidential Information in the possession or control of Company in compliance with all applicable laws and which are no less rigorous than those maintained by Nissan, or provided to Company in writing by Nissan. In the event of any loss, destruction or alteration of Confidential Information by Company, Company agrees to promptly correct any errors or inaccuracies in the Confidential Information and restore any losses of any Confidential Information. Nissan shall have the right to establish backup security for Confidential Information in the possession or control of Company. Nissan shall also have the right to audit Company's or its agents' use of Confidential Information to assure compliance with the terms of this Agreement and applicable laws and Company agrees to provide Nissan full cooperation in connection with such audits. Without limiting the foregoing, Company shall maintain privacy and security obligations as set forth in the US Data Protection Agreement attached as Exhibit 3.

15. **Subcontracting**. Company shall ensure that the Keys are accessed only by employees or approved contractors of Company and used only by such employees or contractors with the scope of the Permitted Use in furtherance of Company's carrying out of this Agreement. If Company plans to use any independent contractors, subcontractors, or agents in connection with this Agreement, Company shall provide Nissan with advance written notice listing the independent contractors, subcontractors, or agents whom Company plans to so engage. Nissan shall have the right to disapprove any such subcontractor, independent contractor, or agent. Company shall ensure that each of its employees and subcontractors complies with all terms and conditions of this Agreement. Company shall be responsible for, and liable to Nissan for, any failure by any of Company's employees or subcontractors to adhere to or comply with the provisions of this Agreement, and for any breach of the terms of this Agreement. In each such case, Company shall promptly notify Nissan upon discovery of any actual, suspected, or threatened breach of this Agreement, and Company shall cooperate with Nissan in every reasonable way to assist Nissan with respect to such breach. Company shall in all cases remain responsible for obligations, services, and/or functions performed by subcontractors to the

same extent as if such obligations, services, and/or functions were performed by Company or Company's employees, and for purposes of this Agreement all such work performed by any subcontractor shall be deemed work performed by Company.

16. **Notices**. In addition to notice requirements under Section 14, All notices and correspondence pertaining to this Agreement will be delivered by hand or certified mail, return receipt requested and postage prepaid, or by a nationally recognized courier service, and be addressed as follows:

If to Nissan:

Nissan North America, Inc.
One Nissan Way
Franklin, TN 37067
Attention: Mgr, Technical Information & Serviceability- Aftersales Dealer Support

with a copy to:

Nissan North America, Inc.
One Nissan Way
Franklin, TN 37067
Attention: Legal Department

If to Company:

_____
_____
_____
Attention: _____

Notice will be effective only upon receipt by the party being served, except that notice will be deemed received 72 hours after posting by the United States Post Office, by the method described above. Confirmation of receipt of any facsimile sent must be received in order to presume that the transmission was received. Each party is responsible for informing the other of any changes in his/her or its address by sending proper notice.

17. **Assignment**. Company may not assign its rights or delegate its obligations hereunder, either in whole or in part, whether by operation of law or otherwise, without the prior written consent of Nissan. Any attempted assignment or delegation without Nissan's written consent will be null and void. The rights and liabilities of the parties under this Agreement will bind and inure to the benefit of the parties' respective successors and permitted assigns. For purposes of this Section 17, a reorganization, merger, asset or stock sale, statutory conversion, or a change in control shall constitute an assignment.

18. **Publicity/Trademarks**. Neither Party will use any trademark, service mark, logo or other identifying mark of the other Party, or make any public reference to the other Party in connection with this Agreement, without the prior written consent of a duly authorized representative of the other Party in each instance.

19. **Miscellaneous**. For all purposes under this Agreement each Party shall be and shall act as an independent contractor and shall not bind nor attempt to bind the other to any contract. The validity, interpretation and construction of this Agreement, and all other matters related to this Agreement, will be governed and interpreted by the laws of the State of Tennessee. Any litigation pertaining to the interpretation or enforcement of this Agreement will be filed in and heard by the state or federal court with jurisdiction to hear such disputes in Williamson County, Tennessee, and Company hereby submits to the jurisdiction of such courts. Should either Party institute or participate in a legal or equitable proceeding against the other to enforce or interpret this Agreement, the non-prevailing Party shall pay the prevailing Party's costs, expert and professional fees, attorneys' fees, including in-house counsel expenses, and all other costs incurred by the prevailing party in preparation for the proceeding. Upon a party's breach or default hereunder, the other party's failure, whether single or repeated, to exercise a right hereunder will not be deemed to be a waiver of that right as to any future breach or default. In the event that any provision of this Agreement shall be determined to be illegal or unenforceable, that provision will be limited or eliminated so that this Agreement shall otherwise remain in full force and effect and enforceable. The failure of either Party to exercise or enforce any right or provision of this Agreement shall not be a waiver of that right. No provision of this Agreement will inure to the benefit of any third parties so as to constitute any such person a third-party

beneficiary of this Agreement. This Agreement, together with its attached Exhibits and Appendices (which are incorporated herein and made a part hereof), constitutes the entire agreement between the parties with respect to the subject matter hereof, and supersedes any and all prior expressions, whether written or oral.

[(Remainder of page intentionally blank. Signatures follow.)]

ACCEPTED AND AGREED:

NISSAN NORTH AMERICA, INC.:	***[INSERT NAME OF COMPANY HERE]*:**
By: _____	By: _____
Name:_____	Name: _____
Signature: _____	Signature:_____
Title: _____	Title:_____
Signature Date:_____	Signature Date: _____

Exhibit 1
Certain Additional Definitions; Fees; Payment Information

Authorized Scan Tool
Authorized Scan Tools will be limited to devices that exchange, by and between ECUs, only such electronic messages as are needed for purposes of performing diagnosis, analysis, testing, and/or repair of a specified Nissan/Infiniti vehicle, in each instance only as such action has been properly authorized in pursuit of the four (4) legitimate purposes listed in the immediately preceding statement, or any of them. Except as provided below, the Authorized Scan Tool must not have the capability of modifying any software program or data in any such ECU, including but not limited to: (i) modification or enhancement of any ECU calibration parameter or characteristic curve for the purposes of emission or performing "tuning" (such as, by way of example and not of limitation, calibrating calculating, ascertaining, setting, or fixing air/fuel schedules); (ii) modification or enhancement of any ECU operating parameter or variant coding table; (iii) accessing any protected ECU memory location or secured function in an unauthorized manner; or (iv) reprogramming of any ECU memory location or flash memory partition using any software or flash data not authorized by Nissan. Authorized Scan Tools may have the capability of restoring original factory settings or re-initializing vehicle-specific configuration data following Nissan's ECU/component replacement procedures. Authorized Scan Tool can only be a Non-Authorized Scan Tool unless Company has signed the annual Data License Agreement.

Authenticated Scan Tool
An authenticated scan tool is an Authorized Scan Tool that meets Nissan specifications for authentication through applicable validation of such Authorized Scan Tools, some particulars of which validation protocols are further referenced and more particularly described in this Agreement's Exhibit 2 (as so authenticated, each an "**Authenticated Scan Tool**"), the use of which Authenticated Scan Tools as specified/identified elsewhere in this Agreement – if so, where? or general reference here sufficient? by Company is provided for as set forth in this Agreement. Only Authenticated Scan Tools can have bi-directional access capability for Nissan/Infiniti vehicles having a CGW module; only Authenticated Scan Tools can have bi-directional access capability for Nissan/Infiniti vehicles that do not have the CGW module. Authenticated Scan Tools can only be a Non-Authenticated Scan Tool unless Company has signed this Scan Tool Central Gateway and MAC Keys Access License Agreement.

A non-authenticated scan tool is any Authorized Scan Tool that is not an Authenticated Scan Tool (each, a "**Non-Authenticated Scan Tool**"). Non-Authenticated Scan Tools may have bi-directional access capability for Nissan/Infiniti vehicles that do not have a CGW module but must not have bi-directional access capability for Nissan/Infiniti vehicles having the CGW module. In this regard, Company acknowledges that bi-directional access by Non-Authenticated Scan Tools to Nissan/Infiniti vehicles having the CGW module will be blocked by the CGW module.

Bi-directional access capability includes, but is not limited to, bi-directional control and data stream information (*e.g.*, operation of emission related actuators).

Initial Fee: One-time set-fee of $25,000, to be paid in advance to Nissan.

Company shall pay the initial Fee due within twenty (20) days of invoice receipt to be issued to Nissan's Nominee identified below. Payments under this subsection may be made by electronic funds transfer to an account specified by Nissan or by its designated representative in writing to Company. If payments are not made via electronic funds transfer, the payments shall be made payable in U.S funds to:

The Equipment and Tool Institute ("Nominee")
378899 W. 12 Mile Rd., Suite 220
Farmington Hills, MI. 48331

Annual Fee:
The Date License Annual Fee of $12,500, to be paid in advance to Nissan. Refer to the Data License Agreement. Nissan reserves the right to change the fees set forth prior to any renewal of this Agreement.

Payment Information:
Except as otherwise provided in this Agreement, all payments shall be made by electronic bank transfer to Nissan's

nominated bank account as notified to Company by Nissan from time to time.

Exhibit 2
Technical Details

Nissan and Company agree as follows:

1. Definitions:
a. "**Authenticated Scan Tool**" has the meaning set forth in Exhibit 1 to the Agreement.
b. "**Bridge Server**" means a server operated by the Bridge Server Vendor for validation of an Authenticated Scan Tool as part of the Nissan validation protocol for issuing the Keys to that Authenticated Scan Tool distributed in the countries of European Union ("**EU**"), the countries of European Economic Area ("**EEA**"), the countries of the European Free Trade Association ("**EFTA**") and United Kingdom.
c. "**Bridge Server Vendor**" means an independent company contracted by Company to facilitate the Nissan validation protocol in a manner that both protects the identities of IAM shops and users from being disclosed to Nissan and allows Nissan to obtain these identities in the limited circumstances as set forth in Section 4 of this Exhibit 2.
d. "**Diagnostic Session**" means the communications that take place between the Authenticated Scan Tool and a Nissan/Infiniti vehicle during the period when the Authenticated Scan Tool is connected to the vehicle. For clarity, when an Authenticated Scan Tool is disconnected from the vehicle and reconnected, a new diagnostic session begins.
e. "**IAM Shop**" means an independent aftermarket automotive service facility.
f. "**Non-Authenticated Scan Tool**" has the meaning set forth in Exhibit 1 to the Agreement.

2. Each IAM Shop having an Authenticated Scan Tool of Company must have a valid account with the Bridge Server Vendor. The IAM Shop must have registered each of its Company's Authenticated Scan Tools with Company and also with the Bridge Server Vendor. Each user of Authenticated Scan Tools at the IAM Shop must register with the Bridge Server Vendor and have been assigned a valid User ID by the Bridge Server Vendor.

3. Company is responsible for ensuring that any communication from an Authenticated Scan Tool that Company's validation server sends to the Bridge Server is from an Authenticated Scan Tool having a valid User ID.

4. If it was determined that an ECU in a vehicle was improperly programmed or changed, or any other malicious activity occurred during a Diagnostic Session, Nissan will have the right to obtain from the Bridge Server Vendor as well as Company the actual identity of the IAM Shop having the current registration of the Authenticated Scan Tool used for that Diagnostic Session and the actual identity of the user of that Authenticated Scan Tool who used it for that Diagnostic Session. Otherwise, Nissan is not entitled to obtain the identity of the IAM Shop or the user of any Authenticated Scan Tool from the Bridge Server Vendor.

5. Unlocking a CGW module and enabling in-vehicle communication among MAC ECUs after MAC ECU replacement of a Nissan/Infiniti vehicle manufactured by or for Nissan or an Affiliate of Nissan requires that the Authenticated Scan Tool use the Keys issued by a Nissan system in response to a valid request by the Authenticated Scan Tool in accordance with Nissan's then-current validation protocol. Nissan may change its validation protocol from time to time. Company must obtain all required API's and related CGW unlock requirements and MAC Key provision requirements from Nissan.

6. The license granted for distribution of Authenticated Scan Tools is limited to distribution of the Authenticated Scan Tools in the countries of North America for use in those countries. Company will not sell Authenticated Scan Tools for use outside of the countries of North America. For avoidance of doubt, Company may sell Scan Tools outside the specified markets which are physically and functionally, other than the disabled software, identical to the Authenticated Scan Tools sold within the specified markets, provided that the software required to communicate with the Bridge Server is disabled in such Scan Tools in a manner that prevents this software from being re-enabled.

Exhibit 3
US DATA PROTECTION AGREEMENT

This US Data Protection Agreement ("**DPA**") is entered into effective as the effective date of the License Agreement by and between Nissan North America Inc., for itself and as agent on behalf of and for the benefit of its affiliates ("**NNA** or "**Controller**"), and _____ ("**Processor**"). Processor and NNA are each a "**Party**" and together, the "**Parties**". This DPA is incorporated into and becomes a part of the License Agreement by this reference.

WHEREAS, the Parties entered into one or more agreements for the provision of services (the "**Services**") by Processor to NNA which are set forth on Appendix 1 attached hereto and incorporated by reference and any other agreement between the Parties (the "**Principal Agreements**").

WHEREAS, in connection with the Services, Processor will Process Controller Data (defined below).

WHEREAS, the Parties desire to enter into this DPA setting forth Processor's obligations with respect to processing of Controller Data to ensure Processing will be carried out in compliance with the law and the terms of this DPA.

NOW, THEREFORE, in consideration of the foregoing recitals and other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, and wishing to be legally bound hereby, the Parties agree that:

1. Definitions and Interpretation

1.1. This DPA shall survive the termination or expiration of any or all of the Principal Agreements to the extent the Processor continues to process Controller Data on behalf of NNA.

1.2. The terms "business", "consumer", "controller", "processor", "sale, sell or sold", "service provider", "share", and "third party" shall have the meanings ascribed to them or similar terms under Data Protection Law.

1.3. The following definitions apply in this DPA:

1.3.1. "**Applicable Law**" means all current and future applicable national, provincial, state, and local statutes, laws, ordinances, directives, regulations, rules, codes, orders, and other requirements or rules of law, including the common law, and codes of practice as arising or amended and in force from time to time;

1.3.2. "**Controller Data**" means any and all information, files, records, documentation, or other data, including but not limited to information relating to NNA, NNA Affiliates, consumers, customers, dealers, partners, clients, personnel, employees, contractors, agents, and directors, in any form or format, which is:

1.3.2.1. collected, stored, accessed, processed, or transmitted by or on behalf of NNA (or collected on or via NNA information systems, networks, platforms, or applications); or

1.3.2.2. processed (including disclosed, supplied, or in respect of which access is granted to the Processor (or to any Sub-Processor)) in connection with the Principal Agreements (whether by, or on behalf of, NNA or otherwise);

Controller Data includes, but is not limited to, confidential information of NNA and Personal Data;

1.3.3. "**Data Breach**" means any (a) actual or suspected event (including a breach of any security requirements) that results, or would reasonably be expected to result, in any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Controller Data transmitted, stored or otherwise processed by Processor, Processor Personnel or a Sub-Processor; or (b) unauthorized access, use, disclosure, modification, or destruction of Controller Data, or interference with system operations in an information system accessed, owned, operated, or controlled by Processor, Processor Personnel or a Sub-Processor that contains Controller Data transmitted, stored or otherwise processed by Processor or a Sub-Processor;

1.3.4. "**Data Protection Law**" means all Applicable Laws concerning the protection and/or privacy of Personal Data, including without limitation, the California Consumer Privacy Act, as amended by the California Privacy Rights Act of 2020 (Cal. Civ. Code §§ 1798.100 - 1798.199) ("CCPA"), the Virginia Consumer Data Protection Act as of January 1, 2023, the Colorado Privacy Act as of July 1, 2023, the Utah Consumer Privacy Act as of December 31, 2023, Connecticut's Act Concerning Personal Data Privacy and Online Monitoring as of July 1, 2023, Payment Card Industry Data Security Standard ("PCI DSS") and guidance, directions, determinations, codes of practice, circulars, orders, notices or demands issued by a competent governmental agency or authority;

1.3.5. "**Data Subject**" means an individual who is the subject of Personal Data;

1.3.6. "**NNA Affiliate**" means any entity that directly or indirectly, through one or more intermediaries, controls, is controlled by, or is under common control with NNA (for the foregoing purposes, "control" means the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of NNA, whether through the ownership of voting securities or other interests, by contract or otherwise);

1.3.7. "**Personal Data**" or "**Personal Information**" means any data that: (a) personally identifies, possibly could identify, relates to or is reasonably linkable to an individual or a household, either alone or in combination with other information available, or likely to be available, and may include, but is not limited to: (i) name, address (e-mail or postal), telephone number, passwords; (ii) government-issued identification numbers, such as national identification number, passport number, social security number, or driver's license number; (iii) financial information, such as a policy number, credit card number, and/or bank/financial account number; (iv) personal characteristics, such as race or ethnicity, marital status, health and medical information, sexuality, gender; (v) online identifiers such as IP address, device ID, user ID, advertising ID, online behavior; and/or (vi) location information; and/or (b) any other information that is deemed "personal information" or "personal data" or similar term under Data Protection Law, including without limitation, Sensitive Personal Information;

1.3.8. "**Processing**" means any operation or set of operations that are performed on Controller Data or on sets of Controller Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.3.9. "**Security Incident**" means any of the following events that affect or may affect Controller Data: (a) any log entry with a material negative consequence or potentially material negative consequence, including without limitation system crashes, network packet floods, unauthorized use of system privileges, unauthorized system access, or execution of malicious code that destroys data; (b) any violation of Privacy Laws; or (c) a Data Breach.

1.3.10. "**Sensitive Personal Data**" or "**Sensitive Personal Information**" means (a) Personal Information that reveals: (i) a consumer's social security, driver's license, state identification card, or passport number; (ii) a consumer's log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account; (iii) a consumer's precise geolocation; (iv) a consumer's racial or ethnic origin, religious or philosophical beliefs or union membership; (v) the contents of a consumer's mail, email, and text messages unless the Controller is the intended recipient of the communication; or (vi) a consumer's genetic data; or (b) biometric information that is used for the purpose of uniquely identifying a consumer; or (c) Personal Information collected and analyzed concerning a consumer's health; or (d) Personal Information that is collected and analyzed concerning a consumer's sex life or sexual orientation.

1.3.11. "**Sub-Processor**" means any processor, service provider, sub-contractor or other party (including any Processor affiliates) of a Processor; and

1.3.12. "**Processor Personnel**" means the officers, partners, employees, agents, and Sub-Processors of Processor and Processor's contractors.

1.3.13. "**TOMs**" means appropriate technical and operational measures.

2. Processing of Personal Data

2.1. For the purposes of this DPA and Processor's processing of Controller Data in connection with the performance of its obligations under the Principal Agreements, Processor (and each Sub-Processor) shall be a processor/service provider and shall not act as a controller/third party. NNA acts as a data controller/business and shall be solely responsible for determining the purposes for which and the manner in which Controller Data are processed. Controller Data is and at all times shall remain the sole property of NNA. Processor shall not possess or assert any lien or other right against or to the Controller Data. Processor agrees not to permit any of Processor Personnel to access or use any Controller Data except in furtherance of its obligations under the Principal Agreements.

2.2. Information on the data processed by Processor under this DPA, including the subject-matter, duration, nature and purpose of the processing, type of Personal Data and categories of Data Subjects as well as the retention period(s) for the Personal Data is set out in Appendix 2 (Data Processing Information). To the extent the Personal Data processed by Processor changes (whether by expanding or narrowing in scope) under the Principal Agreements, the Parties acknowledge and agree that Appendix 2 must be updated accordingly to comply with Data Protection Law. NNA will have the right, in its sole discretion, to prepare an amended Appendix 2 and notify Processor in writing. The amended Appendix 2 will take effect on the date thirty (30) days after its notification to Processor, unless Processor notifies NNA prior to this date that it refuses to accept the amended Appendix 2, in which case: (a) the amendment will not take effect, and (b) NNA will have the right to terminate the Principal Agreements (subject to Section 9.1.1) by written notice to Processor with immediate effect, in NNA's sole discretion, with effect from any future date specified in the notice. Such termination shall be without prejudice to any accrued rights and liabilities of the Parties, provided that no termination fees, expenses or other compensation will be payable by NNA in connection with such termination and Processor shall refund NNA within thirty (30) days of termination any fees prepaid by NNA to Processor in respect of the period following termination.

2.3. Processor shall only process Personal Data in compliance with Data Protection Law, and in accordance with this DPA, the Principal Agreements and NNA's other written instructions, unless required to do otherwise by Applicable Law to which Processor is subject (in which case, Processor shall inform NNA of such legal requirement before processing, if permitted by such Applicable Law), and including any instructions to cease or terminate processing of Controller Data.

2.4. Notwithstanding anything to the contrary in the Principal Agreements, Processor shall not:

2.4.1. Sell or share Controller Data;

2.4.2. Retain, use, or disclose Personal Data for any purpose other than as permitted under Appendix 2, except as required by Applicable Law;

2.4.3. Retain, use, or disclose Personal Data outside the direct business relationship between NNA and Processor; or

2.4.4. Combine Controller Data that Processor receives from, or on behalf of, NNA with Controller Data that it receives from, or on behalf of, another person or persons, or collects from its own interaction with a Data Subject, except to perform the business purpose specified in the Principal Agreements.

2.5. Processor shall maintain an accurate, up-to-date written log of all processing of Personal Data performed on NNA's behalf which shall distinguish between accesses due to regular business operations and accesses due to orders or requests for access. The written log shall include the following information: (a) the categories of recipients to whom Personal Data have been or will be disclosed; and (b) a description of the technical and organizational security measures referred to in this DPA. Processor will provide NNA a copy of such log upon NNA's request.

2.6. Processor certifies that it understands the restrictions set forth in this Section 2 and, without limiting any of its other obligations under this DPA, shall comply with these restrictions. Controller may monitor Processor's compliance with this DPA through reviews, audits or regular assessments at least once per year.

2.7. NNA shall have the right to take reasonable and appropriate steps to help ensure that Processor uses the Personal Data in a manner consistent with Data Protection Law. Upon notice, NNA shall take reasonable and appropriate steps to stop and remediate unauthorized use of Personal Data.

3. Data Subject Requests

3.1. Processor shall establish and maintain TOMs to assist in the fulfillment of NNA's obligation to respond to requests for the exercising of Data Subject or consumer rights (including access requests) set out in Data Protection Law.

3.2. Processor shall provide such assistance and co-operation as NNA reasonably requests, including without limitation, providing and requiring any Sub-Processor to provide Personal Data in a format easily understandable to the Data Subject and in a commonly used, machine-readable format, and immediately (and in any event within ten (10) business days) comply with any request from NNA requiring Processor (or, as relevant, the Sub-Processor) to amend, provide access to, transfer or delete Personal Data.

3.3. In the event Processor receives any request from a Data Subject regarding Personal Data that Processor collects, maintains, processes or sells on behalf of NNA, and not on behalf of itself as a controller or for another entity, Processor shall advise the Data Subject that such request(s) should be submitted directly to NNA, and direct Data Subject to the NNA website. If Processor (or, as relevant, the Sub-Processor) is unable to comply with a Data Subject's request, received by Processor from NNA, due to impossibility or disproportionate effort by Processor (or, as relevant, the Sub-Processor), Processor shall provide written notice to NNA within five (5) days of receipt of the request that includes a detailed explanation as to why compliance with the request is not possible or involves disproportionate effort.

3.4. Except as set forth in Section 3.3., in the event Controller provides Processor with a Data Subject's request to delete Personal Data, Processor shall (a) permanently and completely erase the Personal Data from its existing systems (except with respect to Processor's archived or back-up systems) or enabling NNA to do so; (b) to the extent an exception applies to the deletion of Personal Data as set forth in Data Protection Law, delete or enable NNA to delete the Data Subject's Personal Data that is not subject to the exception and refrain from using the Data Subject's Personal Data retained for any purposes other than the purpose provided for by that exception; and (c) notify and require any of its Sub-Processors to delete from their records such Personal Data in the same manner as the Data Subject's Personal Data is deleted by Processor. Within fourteen (14) days of termination or expiration of this DPA, Processor shall either (i) provide the form certification of deletion as set forth in Appendix 5 (Certificate of Deletion), or (ii) provide documentation verifying deletion of the Data Subject's Personal Data.

4. Security

4.1. Processor shall take all reasonable steps to ensure the reliability of any Processor Personnel who may have access to, or are authorized to process, Controller Data and ensure such Processor Personnel do not process Controller Data except as permitted under this DPA. Processor shall ensure that such Processor Personnel are bound by appropriate contractual confidentiality, data protection, and data security obligations in accordance with this DPA, only have the access required to provide the Services, and at all times act in compliance with Data Protection Law and the obligations of this DPA.

4.2. Processor shall implement and maintain all TOMs, including without limitation the measures set forth in Appendix 4 (Security Measures) attached hereto, to ensure physical, organizational and logical security of Controller Data as required by Data Protection Law and which shall include protection against a Data Breach, and shall ensure that the technical and organizational measures provide best practice security in respect of the processing of Controller Data.

4.3. Processor shall provide all reasonably requested assistance to NNA so it can demonstrate compliance with Data Protection Law.

4.4. Compliance with the Appendix 4 shall not relieve Processor of any liability otherwise arising under this Section or under Data Protection Law and shall not constitute assurance from NNA that such compliance shall satisfy Processor's other obligations under this Section or under Data Protection Law regarding the security of data.

5. Sub-Processors

5.1. Processor has NNA's authorization for the engagement of the Sub-Processors set forth at Appendix 3. Processor shall specifically inform NNA in writing of any intended changes of that list through the addition or replacement of Sub-Processors at least thirty (30) days in advance. Processor shall provide NNA with the information necessary to enable NNA to exercise the right to object. NNA shall have thirty (30) days to respond to such intended change. If NNA objects to any intended changes concerning the addition or replacement of any Sub-Processor, the Parties shall have fourteen (14) business days to discuss the intended change. If the Parties are unable to reach an agreement for the proposed change, Processor shall not engage the proposed Sub-Processor in relation to the Services and shall not transfer or disclose any Controller Data to such proposed Sub-Processor.

5.2. Processor shall provide to NNA an updated list of Sub-Processors in use upon request.

5.3. Processor shall ensure that each Sub-Processor is capable of providing a level of protection for Controller Data required by this Data Protection Law and this DPA.

5.4. Processor shall enter into a written agreement with each approved Sub-Processor containing data protection obligations no less stringent than the ones imposed on Processor in this DPA. Processor shall ensure that the Sub-Processor complies with the obligations to which Processor is subject pursuant to this DPA.

5.5. Processor shall remain fully responsible to NNA for the performance of the Sub-Processor's obligations in accordance with its contract with Processor. Processor shall notify NNA of any failure by the Sub-Processor to fulfil its contractual obligations.

6. Audit.

6.1. Processor shall participate in, contribute to and permit NNA, or a nationally recognized third-party auditor acting under NNA's direction, to conduct, data protection and/or security audits, including without limitation, reasonable on-site inspections of Processor's business premises or processing facilities subject to reasonable prior notice and execution of a confidentiality agreement, manual reviews and automated scans of Processor's system and other technical and operational testing, concerning Processor's data protection and security procedures relating to the processing of Controller Data, including its policies and technical and operational measures and its compliance with this DPA and Data Protection Law. NNA may, in its sole discretion, require Processor to make available all information, access to premises, systems and personnel necessary to demonstrate evidence of Processor's compliance with these procedures, this DPA and Data Protection Law in lieu of, or in addition to, conducting such an audit, including inspections. Processor shall provide a report of such audit to NNA upon request.

6.2. The rights under this Section are in addition to any audit rights under the Principal Agreements and shall survive termination.

7. Data Breach

7.1. Processor shall provide all reasonable assistance to NNA in relation to any Data Breach relating to the Services in accordance with Applicable Law. In particular, Processor shall notify NNA of any Data Breach without undue delay, and in any event within 48 hours, after Processor or a Sub-Processor becomes aware of the Data Breach. Such notification shall be made to infosec@nissan-usa.com and contain, at least:

7.1.1. a description of the nature of the Data Breach (including, where available, the identities and locations of Data Subjects and types of data concerned);

7.1.2. the details of a contact point where more information concerning the Data Breach can be obtained;

7.1.3. its likely consequences and the measures taken or proposed to be taken to address the Data Breach, including to mitigate its possible adverse effects.

Thereafter, Processor shall provide NNA with weekly reports regarding the status of the Data Breach.

7.2. To the extent it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

7.3. Processor shall (a) take all steps to mitigate the effects and to minimize any damage resulting from the Data Breach; (b) promptly comply with any instructions provided by, and cooperate with, NNA in relation to the Data Breach; (c) maintain a log of Data Breaches including facts, effects and remedial action taken; and (d) perform forensics related to the Data Breach as set forth in Appendix 4.

7.4. If NNA determines that the Data Breach triggers notification requirements under Data Protection Law, or if NNA otherwise determines in its reasonable discretion that notification to Data Subjects is warranted, then Processor shall provide notifications to Data Subjects and government entities and/or media outlets at Processor's sole cost and expense. Within (5) calendar days of a Data Breach, Processor shall provide NNA with a draft form of notification to be sent to each Data Subjects for review and approval by NNA. If NNA objects to the form of notification, NNA and Processor will cooperate to prepare a form of notification agreeable to both Parties. Within three (3) business days of the Parties' agreement on the form of notification, Processor shall send notifications by first class mail (or by such other method as permitted by Data Protection Law). At a minimum, the form of notification will provide:

7.4.1. a brief description of the incident, including the date of the Data Breach, the date it was discovered and the categories of Personal Data involved;

7.4.2. the steps Data Subjects should take to protect themselves from potential harm;

7.4.3. a description of the steps Processor is taking to investigate the Data Breach, mitigate harm to Data Subjects, and protect against future incidents; and

7.4.4. a detail of the remediation solutions (including without limitation, credit monitoring services, at NNA's discretion) Processor will make available to Data Subjects in accordance with Processor's obligations.

7.5. Processor shall cooperate fully in the investigation and remediation of a Data Breach and take all reasonable measures to limit further unauthorized disclosure or processing on Controller Data in connection with the Data Breach. At NNA's request, Processor shall, at Processor's cost (including attorneys' and forensic professionals' fees): (a) provide notices to affected individuals, and to state and/or federal regulatory bodies; and (b) remedy and otherwise mitigate any potential damage or harm of the Data Breach, including, without limitation, establishing call centers and providing credit monitoring or credit restoration services for a period of one (1) year (or such longer period as required by Applicable Law), or otherwise as requested by NNA, and payment of fines issued or levied by a regulatory authority. The timing, content, and manner of effectuating any notices shall be determined by NNA in its sole discretion.

8. Data Protection Impact Assessments

At NNA's request, Processor shall assist NNA with any data protection impact assessments regarding any existing or new type of processing proposed, in accordance with Data Protection Law, including in order to assess the probability and seriousness of the risks inherent in the processing of Controller Data, taking into account its nature, scope, context, purposes and level of risk. Processor shall provide any necessary information to enable NNA to conduct the data protection impact assessment.

9. Termination

9.1. Except as otherwise provided by Applicable Law, on the expiration or termination of the relevant processing or all of the Principal Agreements, for whatever reason, on NNA's written instructions, Processor shall:

9.1.1. cease all use of Controller Data and shall, at NNA's election, within fourteen (14) days (or such earlier period specified by NNA), destroy all Controller Data and/or transfer all Controller Data to NNA or a third party named by NNA (in a format and a method defined by NNA and at no additional cost to NNA) unless Applicable Law requires a longer retention period; and

9.1.2. certify such destruction or deletion in writing to NNA.

9.2. Without limiting its obligations under Section 9.1, if Processor is identified as Office of Record or Custodian of Record by NNA pursuant to a Principal Agreement, Processor shall retain Controller Data in accordance with any retention period specified by NNA and in any Data Protection Impact Assessment provided to or developed by Processor and keep a written record of such retention period, which it must provide to NNA on request.

10. Liability

10.1. Any exclusions and limitations of liability of Processor set out in the Principal Agreements shall not be applicable to Processor's processing of Controller Data and/or this DPA.

10.2. Processor shall, immediately on demand, fully indemnify NNA and NNA Affiliates and keep NNA and NNA Affiliates fully indemnified against all costs, claims, administrative fines, demands, expenses (including legal costs and disbursements on a full indemnity basis), losses (including indirect losses, loss or corruption of data, loss of reputation, goodwill and profits), actions, proceedings and liabilities of whatsoever nature arising from or incurred by NNA or NNA Affiliates or customers, in connection with any Data Breach of Processor, Processor Personnel or any Sub-Processor to comply with the provisions of this DPA and/or Data Protection Law ("Losses"). All or any such Losses suffered by a NNA Affiliate, shall, for the purposes of this Paragraph, be deemed to have been suffered by NNA.

10.3. Processor shall immediately (and in any event no later than five (5) business days after it makes its determination) notify NNA in the event it can no longer comply with any Data Protection Law or of any breach of this DPA , including without limitation, Appendix 4. Such notice shall not relieve Processor of any liability otherwise arising under this DPA or Data Protection Law.

11. Miscellaneous

11.1. Amendments. In the event of any change in a Data Protection Law, the Parties agree to negotiate in good faith mutually acceptable and appropriate amendments to this DPA to comply with Data Protection Law.

11.2. Governing Law. This DPA shall be governed by and construed in accordance with the laws of the State of Delaware without giving effect to any choice of law provisions thereof.

11.3. Non-Waiver. No course of dealing or failure of either Party to strictly enforce any term, right or condition of this DPA shall be construed as a waiver of such term, right or condition.

11.4. Assignment. This DPA shall be binding upon and inure to the benefit of the Parties hereto and their respective successors, assigns and personal representatives. Processor may not assign this DPA without the prior written approval of NNA, which may not be unreasonably withheld. Any attempted assignment in violation of the foregoing shall be deemed null and void.

11.5. Insurance. In addition to any insurance-related obligations set forth in the Principal Agreements, Processor shall at all times carry a cybersecurity, computer security, and privacy liability insurance policy that will cover actual or alleged acts, errors or omissions committed by Processor, its agents or employees or Sub-Processors. The policy shall also extend to include the intentional, fraudulent, grossly negligent, or criminal acts of Processor, its agents or employees or Sub-Processors. The policy shall provide, but not be limited to, coverage for the following perils:

11.5.1. unauthorized use/access of a computer system or network

11.5.2. data destruction and/or theft, extortion demands, hacking, and denial of service attacks

11.5.3. crisis management activity related to data breaches

11.5.4. defense of any regulatory action involving a breach of privacy

11.5.5. failure to protect confidential information (personal and commercial information) from disclosure

11.5.6. notification costs, whether or not required by statute.

11.6. Severability. If a competent court or administrative body finds that any provision of this DPA is invalid, illegal or unenforceable:

11.6.1. the rest of this DPA shall remain unaffected and in force;

11.6.2. if deleting part of the provision would make it valid, legal or enforceable, it shall apply with all changes necessary to make it valid, legal or enforceable;

11.6.3. if Section 11.6.2 does not apply, the Parties shall try to replace the provision with a valid, legal or enforceable provision which achieves as closely as possible the effect that the relevant provision would have achieved; and

11.6.4. the obligations of the Parties under the relevant provision shall be suspended during any attempt at substitution under Section 11.6.3.

11.7. Order of Precedence. In the event of any conflict between this DPA and any agreement, present or future, involving the Parties, this DPA shall control; unless, and only in the event, this DPA is intentionally superseded through a written agreement signed by both Parties. In addition to the foregoing, where a provision of an agreement imposes on Processor a standard or duty in relation to any obligation which is more onerous than, or additional to, that imposed by a provision of this DPA, such provision shall not be treated as a conflict and that standard or duty shall be treated as cumulative to the maximum extent possible.

11.8. Injunctive Relief. Processor acknowledges that monetary damages may not be a sufficient remedy for a Data Breach or other breach of this DPA, and agrees that NNA shall be entitled, without waiving any other rights or remedies nor the posting of a bond, to such injunctive or equitable relief as may be deemed proper by a court of competent jurisdiction.

11.9. Notice. The parties agree that any notice, demand, or communication required or permitted to be delivered or given by the provisions of this DPA shall be delivered or given in accordance with the notice provision in the Principal Agreements.

Appendix 1 Principal Agreements

1. License Agreement Scan Tool Central Gateway and MAC Keys Access

Appendix 2

Data Processing Information

Subject matter of processing *[Insert subject matter (e.g. description of the Services).]*	
Duration of processing *[e.g., For the length of Principal Agreements]*	
Nature of processing, *[Insert brief description of nature of processing, i.e., any operation such as collection, recording, structuring, storage, adaptation, retrieval, consultation, use disclosure by transmission, dissemination or otherwise making available the Personal Data of the Data Subjects on behalf of NNA.]*	
Purpose or nature of processing *[Insert purpose of Services (e.g., hosting, self-service and analytics).]*	

Categories of Data Subjects *[Insert the types of persons about whom data is being processed (e.g., customers, employees, business contacts, etc.)]*	☐ Customers ☐ Employees ☐ Business Contacts (Check all that apply) List Additional Data Subjects
Categories of personal data and sensitive data *[Choose fields that apply and add description of sensitive data if applicable]* *[Personal Data: (e.g., name, date of birth, address, transaction data, etc.)]* *[Sensitive Data: (e.g., account login data, biometric info, geolocation, government I.D., etc.)]*	Customer Personal Identifier Information (Check all that apply) ☐ First Name ☐ Last Name ☐ Full Name ☐ Pseudonym: ☐ Address ☐ Zip Code ☐ Previous Address ☐ Personal Email ☐ Phone/Cell ☒ VIN ☐Buying History ☐ Vehicle Sales ☐ Other Identifiers ☐ Age ☐ Race ☐ Sex ☐ Education Description of Other Identifiers: (List) Customer Sensitive Data (Check all that apply) ☐ Account Login Data ☐ Biometric Info ☐ Personal Characteristics ☐ Geolocation ☐ Government I.D. Description of Sensitive Data (e.g. Personal Characteristics) (List)
Retention period *[Insert retention period for Personal Data, including different retention periods for different types of Personal Data, if applicable.]*	

Appendix 3

Approved Sub-Processors

[Processor to provide current list of Sub-Processors]

Appendix 4

Security Measures

This Appendix 4 outlines particular administrative, logical, technical and security requirements ("**Security Requirements**") that Processor shall maintain to protect the availability, confidentiality and integrity of all Controller Data and of Processor systems, applications, and platforms processing Controller Data ("**Processor Network**"). Processor's Security Program must meet the following Security Requirements at a minimum. Processor shall provide NNA with appropriate documentation evidencing compliance with the Security Requirements upon request. A failure to comply with these Security Requirements will be considered a material breach of the DPA and Principal Agreements. Capitalized terms used herein but not otherwise defined shall have the meaning set forth in the DPA.

1. **Security Assessment:** Processor will implement and maintain cybersecurity policies, controls, and practices equivalent to or exceeding, at the time, current NIST Cybersecurity Framework.

    1.1. **Report Obligations**: Upon request from NNA, Processor will prepare and deliver a report to NNA within fifteen (15) business days, with evidence including NIST CSF assessment maturity levels in each area and security policies, controls and practices demonstrating compliance with or exceeding the NIST Cybersecurity Framework Level 3.

    1.2 **Security Controls.** During the term of this DPA, Processor's security controls shall include, but are not limited to, the following:

        1.2.1 Penetration Testing: Processor will perform penetration testing on Processor's Networks in compliance with NIST Special Publication – 800-115, using industry standard security testing tools, and shall continue to perform such testing, at a minimum, annually.

        1.2.2 Vulnerability Remediation: Processor will immediately remediate weaknesses and vulnerabilities identified in penetration testing and/or vulnerability management activities within ten (10) days (unless such other time period is agreed to in writing by the parties) of identification of such weaknesses and/or vulnerabilities. If Processor is unable to remediate critical vulnerabilities within ten (10) days then Processor must notify NNA in writing, and NNA shall (i) have the right to terminate this DPA and the Principal Agreements for cause in accordance with the DPA, or (ii) in NNA's sole discretion, allow Processor to perform such remediation during a time period mutually agreed upon in writing by the parties so that Processor's Networks are in compliance with Processor's data security policies, Security Requirements and NIST Special Publication – 800-115.

        1.2.3 SOC2 Assessment: Processor will provide an annual System and Organization Controls (SOC2) compliance assessment. Upon NNA request, Processor shall provide a copy of the report and certify in writing that any deficiencies, weaknesses or areas of non-compliance that may affect Controller Data and/or NNA's networks or computing assets have been remediated.

2 **Security Incident:** Processor will provide NNA via email (**infosec@nissan-usa.com**) with the email address and other contact information for Processor's head of cybersecurity as a contact and shall promptly notify NNA in writing of any change and revalidate security contact annually.

    2.1 **Notification**: Processor will follow a documented Security Incident response management plan. In the event of a Security Incident or a potential Security Incident, Processor must notify NNA within twelve (12) hours of such Security Incident or potential Security Incident.

    2.2 **Impact, Root cause and Remediation:** Processor will prepare and deliver to NNA within five (5) business days of such Security Incident a root cause report that describes in detail (a) a description of the nature and extent of the Security Incident; (b) the Controller Data disclosed, destroyed, or otherwise compromised or altered; (c) all investigative, corrective and remedial actions completed,

and planned actions and the dates by which such actions will be completed; (d) all efforts taken to mitigate the risks of further Security Incidents; and (e) an assessment of the security impact to NNA.

2.3 **Remedies:** In the event of a Security Incident resulting from Processor's failure to meet its obligations under this Appendix 4 or otherwise is the result of Processor's or Processor Personnel's (including any Sub-Processor personnel and agents) actions or inactions, Processor shall immediately take such actions as NNA shall request in good faith to remediate such Security Incident, to preclude further Security Incidents, and to address publicity regarding such Security Incident, and in all cases such actions as are required of Processor by applicable laws. Further, in such event Processor shall be responsible for all costs, fines, claims, penalties, or losses suffered by NNA as a result of such Security Incident.

3 **Software Code Security:** Processor will, for all development, coding, creation of software and/or work product, and/or other similar or related services for, or on behalf of NNA, follow secure coding practices, equivalent to or exceeding the NIST Secure Software Development Framework, as they may be updated and revised from time to time. Processor will notify NNA of any critical software vulnerabilities that are discovered and are not remediated within ten (10) days of discovery. If Processor is unable to remediate critical software vulnerabilities within ten (10) days, then Processor must notify NNA in writing, and NNA shall (a) have the right to terminate this DPA and the Principal Agreements for cause in accordance with the DPA, or (b) in NNA's sole discretion, allow Processor to perform such remediation during a time period mutually agreed upon in writing by the parties so that Processor's Networks are in compliance with the Processor's data security policies, Security Requirements and NIST Secure Software Development Framework.

4 **Audit Rights**: On an annual basis, NNA has the right to audit or hire a third party to audit or request from Processor an audit report conducted by a nationally recognized third-party cybersecurity auditor addressing(a) Processor's security controls following current NIST CSF Framework; and (b) Processor's critical Software code security vulnerabilities.

5 **Data Security:**

5.1 **Encryption**: Processor will ensure that all of Controller Data is encrypted at rest and in transit using AES256 or a higher level of encryption and secure encryption keys following NIST 140-Level3 compliant devices.

5.2 **Access**: Processor will (a) ensure that Controller Data is accessible only to those persons with a need to access such systems or features to perform the Services, and only to the extent necessary to perform such Services. When any Processor Personnel no longer has a business need for the access privileges to Controller Data assigned to him/her/it, the access privileges shall be promptly revoked, even if such Processor Personnel continues to be an employee, agent, or contractor of Processor; (b) perform monthly audits on permissions for Processor's Personnel, and (c) use Multi-Factor authentication for access to the Processor Network and Controller Data located thereon.

5.3 **Notification**: Processor will notify NNA in writing within thirty (30) days if Processor is no longer able to perform any of the Security Requirements.

6 **Questionnaires, Assessments:** Processor will complete security questionnaires and security assessments as required by Controller from time to time as determined by Controller (e.g., Security Risk & Assessment Questionnaire (SRAQ), NIST Assessment) and/or provide Controller with assessments or reports performed by third party assessors conducted as part of Processor's normal security processes.

Appendix 5

Certificate of Deletion

Pursuant to the Data Processing Agreement dated _____ by and between [Insert Processor's Name ("**Processor**")] and Nissan North America, Inc. ("**NNA**"), Processor hereby certifies that as of [Insert Date] Processor has deleted, destroyed or returned to NNA all of the Controller Data as that term is defined under the DPA in accordance with **[Processor's data retention schedule and]** Data Protection Law.

Signed for and on behalf of [Insert Processor Name]

Signed: _____

Print name: _____

Title: _____

Date: _____