

**SUB-RECIPIENT AGREEMENT
CITY OF EVERETT AND NOVOAGLOBAL**

This Agreement, effective the last date signed below, is made by and between the City of Everett, Washington a municipal corporation of the State of Washington hereinafter referred to as “**Licensee**”, having an address at 2930 Wetmore Ave. Suite 10-C, Everett WA 98201, and NovoaGlobal, Inc., hereinafter referred to as “**NG**”, whose address is 8018 Sunport Drive, Suite 203, Orlando, Florida 32809.

WHEREAS, the Licensee is using NG’s Back Office System called Intelligence Center (“**I-C**”) that could have access to Washington State Department of Licensing (“**DOL**”) to receive vehicle owner information.; and

WHEREAS, NG’s Vehicle Data Sharing Agreement with DOL requires that DOL and Licensee enter into a Sub-recipient Agreement in order for NG to provide DOL vehicle owner information to Licensee; and

WHEREAS, the Licensee acknowledges the confidential/exempt nature of the information and data that is captured/contained within NG’s I-C and the legal requirement to ensure security of said data.

NOW THEREFORE, in consideration of the mutual understandings and agreements set forth herein, the parties agree as follows:

1. Agreement Term/Termination

- A. The TERM of this Agreement shall be from the last date of signature of the parties and shall continue until terminated by either party.
- B. Either party may terminate this agreement upon providing thirty (30) days written notice.

2. Purpose

The purpose of this Agreement is to establish terms and conditions under which DOL will allow access to their information through NG to the Licensee.

3. Cooperation

It is agreed that both parties shall provide all reasonable and necessary cooperation and assistance to facilitate the terms of this Agreement.

4. Security/Confidentiality Requirements

For NG to grant the Licensee access to DOL information, the Licensee as a Sub-recipient shall comply with the following requirements.

- a) All Data Security and Permissible Use terms, conditions and requirements set forth in Attachments A – Data Licensing Statement, B – Data Security Requirements, and D – Permissible Use Requirements, of this Agreement. Permissible Use(s) available to the Subrecipient are limited to the Permissible Uses available to the Licensee in Attachment A – Data Licensing Statement, of this Agreement.
 - b) All Security Breach Notification and Non-Conforming Permissible Use Notification requirements included in Section 10, Data Security Breach and Misuse Notification, of this Agreement.
 - c) All records access, inspections, Driver Privacy Protection Act (DPPA), and records maintenance requirements included in Section 34, Records Access, Inspection, and DPPA, of this Agreement.
-

- d) All allowances granting DOL, or DOL's agent, the right to access, investigate, and audit records related to any Data provided under this Agreement. Such access must be afforded to DOL and the Parties will work in good faith to determine if information should be withheld on the basis of privilege or confidentiality.
- e) All audit and annual certification requirements in Attachment E, Annual Internal Assessment, of this Agreement.
- f) Subrecipient to provide DOL with access to its product at no cost to DOL, in cooperation with Licensee when DOL has cause to request access.

5. Governing Law and Equitable Relief

This Agreement shall be governed and construed in accordance with the laws of the United States and the State of Washington and NG consents to the exclusive jurisdiction of the state courts and U.S. federal courts located there for any dispute arising out of this Agreement. Venue shall be in Pierce County, Washington.

6. Severability

If any term of this Agreement is held by a court of competent jurisdiction to be invalid or unenforceable, then this Agreement, including all of the remaining terms, will remain in full force and effect as if such invalid or unenforceable term had never been included.

7. Notices

Any notice required by this Agreement or given in connection with it, shall be in writing and shall be given to the appropriate party by personal delivery or by certified mail, postage prepaid, or recognized overnight delivery services.

If to Licensee:
City of Everett
2930 Wetmore Ave. Suite 10-C
Everett, WA 98201
Attn: David Hall, WA Attorney

If to NG:
NovoaGlobal, Inc.
8018 Sunport Drive, Suite 203
Orlando, FL, 32809
Attn: Carlos Lofstedt, President, CEO

8. No Implied Waiver

Either party's failure to insist in anyone or more instances upon strict performance by the other party of any of the terms of this Agreement shall not be construed as a waiver of any continuing or subsequent failure to perform or delay in performance of any term hereof.

9. Headings

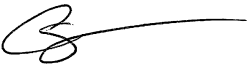
Headings used in this Agreement are provided for convenience only and shall not be used to construe meaning or intent.

10. Entire Agreement

It is understood and agreed that the entire Agreement of the parties is contained herein, and that this Agreement supersedes all oral agreements and negotiations between the parties relating to the subject matter hereof, as well as any previous Agreement presently in effect between the parties relating to the subject matter hereof. Any alterations, amendments, deletions, or waivers of the provisions of this Agreement shall be valid only when expressed in writing, approved by the respective parties and duly executed on behalf of each party as set forth herein.

IN WITNESS HEREOF, the parties hereto have caused this agreement to be executed by the proper officers and officials.

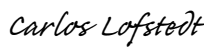
CITY OF EVERETT

BY: 

Cassie Franklin, Mayor

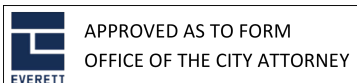
Date: 05/16/2024

NOVOAGLOBAL, INC.

BY: 

Carlos Lofstedt, President, CEO

Date: 05/16/2024



Attest:



Attachment A – Data Licensing Statement

1. PERMISSIBLE USE

Data containing Confidential Information may only be used for the Permissible Use(s) as set forth below:

PERMISSIBLE USE DESCRIPTION	
I.	Any governmental agency of the United States or Canada, or political subdivisions thereof, to be used by it or by its authorized commercial agents or contractors only in connection with the enforcement of motor vehicle or traffic laws by, or programs related to traffic safety of, that government agency. Only such parts of the list as are required for completion of the work required of the agent or contractor can be used shall be provided to such agent or contractor. This Permissible Use is pursuant to RCW 46.12.630 (2b).

Attachment B - Data Security Requirements

For all Confidential Information to be electronically stored, processed, or transmitted, Licensee shall apply the following requirements:

1. Data Security

Licensee must protect the confidentiality, integrity and availability of Data with administrative, technical and physical measures that meet generally recognized industry standards and best practices or standards established by the Office of the Chief Information Officer (OCIO).

Examples of industry standards and best practices include any of the following:

- a) [ISO 27002](#)
- b) [PCI DSS](#)
- c) [NIST 800 series](#)
- d) OCIO 141.10 (<https://ocio.wa.gov/policies/141-securing-information-technology-assets/14110-securing-information-technology-assets>)

2. Network Security

Licensee's network security must include the following:

- a) Network firewall provisioning
- b) Intrusion detection
- c) Quarterly vulnerability assessments
- d) Annual penetration tests (when Data is defined as Category 3 or higher). This requirement only applies if the Licensee is hosting the DOL data.

3. Access Security

Licensee shall restrict Authorized User access to the Data by requiring a login using a unique user ID and complex password or other authentication mechanism which provides equal or greater security. Passwords must be changed on a periodic basis at least quarterly. The sharing of user ID and passwords is strictly prohibited. Licensee is solely responsible for protection of all of its user IDs and passwords, and is responsible for all Data Security Breaches caused through the use of its user IDs and passwords.

4. Application Security

Licensee shall maintain and support its software and subsequent upgrades, updates, patches, and bug fixes such that the software is, and remains secure from known vulnerabilities. Licensee must secure web applications that minimally meet all the security controls as generally described in either:

- a) The Open Web Application Security Project Top Ten (OWASP Top 10), or
- b) The CWE/SANS TOP 25 Most Dangerous Software Errors.

5. Computer Security

Licensee shall maintain computers that access Data by ensuring the operating system and software are updated and patched monthly, such that they remain secure from known vulnerabilities. Licensee computer device(s) must also be installed with an Anti-Malware solution and signatures updated no less than monthly.

6. Data Storage

Licensee shall designate and be able to identify all computing equipment, on which Licensee stores, processes, and maintains Data. No Data at any time may be processed on or transferred to any portable storage medium. Laptop/tablet computing devices are not considered portable storage medium in this context provided that it is installed with end- point encryption.

7. Electronic Data Transmission

Licensee shall maintain secure means (e.g., HTTPS or SFTP) for the electronic transmission or exchange of system and application data with DOL or any other authorized Licensee.

8. Data Encryption

Licensee shall encrypt all Data that is defined as Confidential Information, whether in transit or at rest, by using only NIST or ISO approved encryption algorithms; this includes all back-up copies of Data. Licensee further must install any laptop/notebook computing device, processing Data, with end-point encryption (i.e., full disk encryption).

9. Distribution of Data

Licensee may only use and exchange Confidential Information for the purposes as expressly described and allowed in this Agreement. In addition to any other restrictions on Permissible Use, Confidential Information may not be distributed, repurposed or shared across other applications, environments, or business units of Licensee. Licensee must assure that no Confidential Information of any kind is transmitted, exchanged or otherwise passed to other contractors/vendors or interested parties except Licensee and/or Subrecipients who have an authorized legal Permissible Use according to this Agreement, and who are under contract with the Licensee.

10. Data Disposal

Unless a more immediate disposal requirement is set forth in this Agreement, Licensee, upon termination of this Agreement, shall erase, destroy, and render unrecoverable all DOL Confidential Information and certify in writing that these actions have been completed within thirty (30) days of the termination of this Agreement. At a minimum, media sanitization is to be performed according to the standards enumerated by NIST SP 800-88r1 Guidelines for Media Sanitization.

If Confidential Information, whether on its own or as comingled with other data, is subject to state or federal retention periods, or other legally required purposes, including without limitation class action settlements, such Confidential Information may be retained for the added necessary period. Additionally, if Licensee needs to retain Confidential Information for other commercially required purposes, Licensee may retain the Confidential Information while it seeks approval from DOL to retain the Confidential Information for a longer period, which will not be unreasonably withheld by DOL. For all retained Confidential Information, Licensee shall abide by all Data Security requirements, audit requirements, and Permissible Use requirements stated in this Agreement; such requirements hereby expressly survive the termination of this Agreement for that period.

11. Offshoring

Licensee must maintain the primary, backup, disaster recovery and other sites for storage of Confidential Information only from locations in the United States.

Licensee may not commit the following unless it has advance written approval from DOL:

- a) Directly or indirectly (including through Subrecipients) transmit any Confidential Information outside the United States; or
- b) Allow any Confidential Information to be accessed by Subrecipients from locations outside of the United States.

If the Confidential Information is to be physically stored, processed, or distributed, Licensee shall apply the following requirements:

12. Hardcopy Storage

To prevent unauthorized access to printed information obtained under this Agreement, and loss of, or unauthorized access to this information, printed copies must be stored in locked containers or storage areas, e.g. cabinets or vaults. Hard copy documents must never be unattended or in areas accessible to the public, especially after business hours.

13. Hardcopy Transportation

If hard copy documents containing Data are taken outside a secure area, those documents must be physically kept in possession of an authorized person, or a trusted courier providing tracking services. Records must be maintained for all transported hardcopies showing the person(s)/courier(s) responsible for such transportation, including the receiving party.

14. Offshoring

Licensee must maintain all hardcopies containing Confidential Information only from locations in the United States.

Licensee may not directly or indirectly (including through Subrecipients) transport any Confidential Information outside the United States unless it has advance written approval from DOL.

Attachment C - Subrecipient Requirements

2. CONTRACT WITH SUBRECIPIENT

Prior to Licensee providing any Confidential Information directly to a Subrecipient, Licensee must have a written contract with the Subrecipient. The contract must minimally contain the following or substantially similar provisions, which must be equal in effect against the Subrecipient as DOL has applied them against the Licensee.

Direct Subrecipients, and subsequent entities passing Confidential Information through to other Subrecipients, must have a written contract. The contract must minimally contain the items under this Attachment or substantially similar provisions, which must be equal in effect against each Subrecipient as DOL has applied them against the Licensee.

Any Subrecipient contract that does not carry forward the required terms and conditions, or substantially similar, of this Agreement lacks the inherent authority to grant the Subrecipient access to any Confidential Information. If access to Confidential Information is provided to a Subrecipient without such proper authority, it is a violation of the conditions of this Agreement.

- a) All Data Security and Permissible Use terms, conditions and requirements set forth in Attachments A – Data Licensing Statement, B – Data Security Requirements, and D – Permissible Use Requirements, of this Agreement. Permissible Use(s) available to the Subrecipient are limited to the Permissible Uses available to the Licensee in Attachment A – Data Licensing Statement, of this Agreement.
- b) All Security Breach Notification and Non-Conforming Permissible Use Notification requirements included in Section 10, Data Security Breach and Misuse Notification, of this Agreement.
- c) All records access, inspections, Driver Privacy Protection Act (DPPA), and records maintenance requirements included in Section 34, Records Access, Inspection, and DPPA, of this Agreement.
- d) All allowances granting DOL, or DOL's agent, the right to access, investigate, and audit records related to any Data provided under this Agreement. Such access must be afforded to DOL and the Parties will work in good faith to determine if information should be withheld on the basis of privilege or confidentiality.
- e) All audit and annual certification requirements in Section 16, Audits, and Section 17, Annual Internal Assessment, of this Agreement.
- f) Subrecipient to provide DOL with access to its product at no cost to DOL, in cooperation with Licensee when DOL has cause to request access.

3. SUBRECIPIENT DISQUALIFICATION

If Licensee discovers that DOL has disqualified a Subrecipient from receiving Confidential Information, Licensee must immediately terminate and prevent the Subrecipient's access to Confidential Information.

4. SUBRECIPIENT TRACKING

- a) Licensee must provide DOL with a complete list of all Subrecipients within ten (10) days of request. This information may be marked as being privileged or confidential, but may not be withheld from DOL on such basis. The list must be provided in Excel format, or other format approved by DOL without redactions.
- b) For each request for DOL Data, Licensee must provide information identifying the Subrecipient for whom the request was made.

5. GUIDANCE ON COMPLIANCE

- a) Licensee must audit Subrecipients for compliance with Data Security and Permissible Use requirements at least once in a three-year period. Licensee may accept current third-party audits.
 - b) Licensee is responsible to obtain annual attestations of compliance from direct Subrecipients.
-

Attachment D - Permissible Use Requirements

In addition to Permissible Use limitations and requirements specific to Data imposed by the Driver Protection Privacy Act (DPPA, 18 USC Ch. 123), and RCW 46.12.630-635, Licensee must comply with the following requirements:

1. DATA USE

Licensee must institute and maintain written policies and procedures to ensure Confidential Information is only used as authorized herein. At a minimum, the policies and procedures will include training requirements for all personnel with access to Confidential Information on the Permissible Use(s) of Confidential Information. Licensee must be capable of demonstrating the training and education was delivered to all applicable personnel.

2. DEMONSTRATE PERMISSIBLE USE

Licensee at all times must be able to verify its use(s) of the Confidential Information is in accordance with the limited Permissible Uses established in the Agreement. This requirement applies at all times regardless of changes in staff or other personnel. It is not a defense that certain uses may be consistent with other Acts, such as the DPPA, if such acts, or portions of such acts, are not fully consistent with this Agreement. It is also not a defense that the improper use was due to a request from any law enforcement agency.

3. ACCESS

For every commercial product Licensee makes available to Subrecipients for the purpose of obtaining Confidential Information, Licensee must provide DOL one active and valid login credential on Licensee's product as an authorized user at no cost to DOL for the duration of the period Licensee receives data. Access is limited to searching DOL employees with prior written consent. Licensee will not be charged for such access and Licensee shall not pay DOL for those inquiries.

4. SECURE USE

Licensee must maintain and support administrative, technical or physical methods used to monitor compliance with the Permissible Use(s) authorized in this Agreement across all Licensee business practices, including any Subrecipients. Methods may include, but are not limited to, any of the following:

- a) View only access to Confidential Information
 - b) System limitations or controls
 - c) Use of confidentiality agreements executed by all personnel with access to Confidential Information
-

AUDITS

Licensee shall obtain Permissible Use and Data Security audits as required by RCW 46.12.630 and this Agreement.

Data Security audits must demonstrate compliance with Data Security standards adopted by the Washington State Office of the Chief Information Officer (OCIO), and as set forth in Attachment B - *Data Security Requirements*. At a minimum, audit(s) must determine whether Data Security policies, procedures, and controls are in place to ensure compliance with all Data Security Requirements set forth herein, and as required by state and federal law.

Permissible Use Audits must demonstrate compliance with Permissible Use standards as set forth on Attachment D – *Permissible Use Requirements*. Audit(s) must determine whether Permissible Use policies, procedures, and controls are in place to ensure compliance with all Permissible Use requirements in this Agreement.

DOL will accept all audits that are in compliance with RCW 46.12.630.

- A. Timing of Audit(s): Licensee must submit a Data Security audit and provide DOL with the complete audit report prior to commencing its Access Period and receiving any Data under this License. If Licensee does not provide a complete audit report within six (6) months of the execution date of this Agreement, then this Agreement will be automatically terminated without further notice. DOL may allow more than six (6) months to provide a complete audit report through written notice if a request is received from Licensee prior to the end of the six (6) month period. Any extension issued under the provisions of this paragraph is subject to Licensee demonstrating substantial progress toward completing an audit report.
 - B. Selection of Auditor: The Data Security audit must be performed by an independent third-party auditor. Licensee may select the auditor, providing that at a minimum the auditor meets one of the following certifications: American Institute of Certified Public Accountants' (AICPA), Certified Information Privacy Professional (CIPP), ANSI-ASQ National Accreditation Board (ANAB) or other nationally recognized certification.
Alternatively, if the Licensee chooses not to select its own auditor, or if DOL does not accept the audit, DOL will then select the auditor on the Licensee's behalf. If DOL selects the auditor, Licensee must hold DOL and its selected auditor harmless from any real or perceived damages to the Licensee's company as a result of the audit findings.
Licensee has the option to collaborate with DOL in advance to develop the specifics for the scope of an audit, and to predetermine whether an auditor selected by the Licensee meets the standards necessary for DOL's approval.
The Permissible Use and all contract compliance audits will be performed by DOL or its designated agent.
 - C. Cost of Audit: Licensee will be responsible for all costs associated with the audits. If DOL selects the auditor, Licensee will prepay the estimated audit costs. If the actual costs of the audit differ in amount from the estimate, DOL will reimburse or invoice Licensee the difference; final payment must be made within thirty (30) days of receiving the final invoice.
 - D. Corrective Action Plans: Corrective actions plans are required for all deficiencies identified in an audit. DOL has sole discretion on whether such deficiencies should prohibit Licensee's access to Data. If DOL agrees to maintain access to Data, such access is contingent on the following:
 - Within a timeframe established by DOL, Licensee must submit a corrective action plan for each deficiency identified by the audit. For each deficiency, the corrective action plan must outline the steps to be taken to correct the deficiency, and a timeline for completing all corrective steps.
 - DOL will determine whether Licensee is substantially complying with the corrective action plan. If Licensee is not in substantial compliance, then DOL may suspend access to the Data or take other actions as allowed in this Agreement.
-

ANNUAL INTERNAL ASSESSMENT

On an annual basis, based on the execution date of this Agreement, Licensee shall self- assess its own entity to determine whether it is maintaining the Data Security and Permissible Use requirements. This assessment may be completed by obtaining an independent audit; Licensee will provide a copy of that audit to DOL, and will further comply with all matters noted in the audit report.

If this assessment is performed internally by the Licensee, then Licensee must provide DOL with a written certification, acknowledging the completion of the assessment and identifying any deficiency findings. The written certification must be executed by a manager, director, or officer of the Licensee who has the expressed signatory authority to make such a certification on behalf of the Licensee.

Written Certification:

If the assessment determines that Licensee is meeting all Data Security and Permissible Use requirements of this Agreement, then Licensee's certification may simply note that the assessment was completed and no deficiencies were found. However, if deficiencies are discovered, Licensee must submit a completed Attachment E - *Data Security/Permissible Use Non-Compliance/Deviation Form*, and include it with its certification to DOL. The requirement for Attachment E may be met by providing a copy of an audit report if Licensee obtained an additional audit. DOL and Licensee will work together to determine the final actions needed in order to correct all deficiencies noted in the certification.

Licensee's annual assessment findings will be reviewed during the next independent audit. If DOL finds inaccuracies in the Licensee's self-assessments, especially concerning non- reported deficiencies, DOL may deem such inaccuracies and omissions as a possible breach of this Agreement.








NovoaGlobal-DOL Data Sharing-Subrecipient Agreement-CH-SD

Final Audit Report

2024-05-16

Created:	2024-05-09
By:	Marista Jorve (mjorve@everettwa.gov)
Status:	Signed
Transaction ID:	CBJCHBCAABAA2ITqG-RitrANuqPziRBF0U8kf7B6K2Y7

"NovoaGlobal-DOL Data Sharing-Subrecipient Agreement-CH-SD" History

-  Document created by Marista Jorve (mjorve@everettwa.gov)
2024-05-09 - 9:21:39 PM GMT
-  Document emailed to chert@everettwa.gov for approval
2024-05-09 - 9:22:58 PM GMT
-  Email viewed by chert@everettwa.gov
2024-05-09 - 10:34:45 PM GMT
-  Email viewed by chert@everettwa.gov
2024-05-11 - 10:45:33 PM GMT
-  Email viewed by chert@everettwa.gov
2024-05-16 - 12:35:23 PM GMT
-  Signer chert@everettwa.gov entered name at signing as Corey N Hert
2024-05-16 - 12:35:45 PM GMT
-  Document approved by Corey N Hert (chert@everettwa.gov)
Approval Date: 2024-05-16 - 12:35:47 PM GMT - Time Source: server
-  Document emailed to clofstedt@novoaglobal.com for signature
2024-05-16 - 12:35:49 PM GMT
-  Email viewed by clofstedt@novoaglobal.com
2024-05-16 - 12:52:09 PM GMT
-  Signer clofstedt@novoaglobal.com entered name at signing as Carlos Lofstedt
2024-05-16 - 2:40:45 PM GMT



Document e-signed by Carlos Lofstedt (clofstedt@novoaglobal.com)

Signature Date: 2024-05-16 - 2:40:47 PM GMT - Time Source: server



Document emailed to Tim Benedict (TBenedict@everettwa.gov) for approval

2024-05-16 - 2:40:48 PM GMT



Email viewed by Tim Benedict (TBenedict@everettwa.gov)

2024-05-16 - 2:51:15 PM GMT



Document approved by Tim Benedict (TBenedict@everettwa.gov)

Approval Date: 2024-05-16 - 2:51:49 PM GMT - Time Source: server



Document emailed to Cassie Franklin (cfranklin@everettwa.gov) for signature

2024-05-16 - 2:51:51 PM GMT



Email viewed by Cassie Franklin (cfranklin@everettwa.gov)

2024-05-16 - 4:30:24 PM GMT



Document e-signed by Cassie Franklin (cfranklin@everettwa.gov)

Signature Date: 2024-05-16 - 4:30:32 PM GMT - Time Source: server



Document emailed to Marista Jorve (mjorve@everettwa.gov) for signature

2024-05-16 - 4:30:34 PM GMT



Document e-signed by Marista Jorve (mjorve@everettwa.gov)

Signature Date: 2024-05-16 - 4:33:13 PM GMT - Time Source: server



Agreement completed.

2024-05-16 - 4:33:13 PM GMT