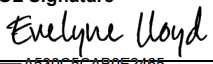


 WASHINGTON STATE DEPARTMENT OF LICENSING	DATA LICENSING AGREEMENT AMENDMENT BETWEEN DEPARTMENT OF LICENSING AND WASHINGTON STATE PATROL	DOL Contract No. K7798 Amendment No. 03 WSP Contract No. K18262-7
Contract		
Contract start date Upon Execution	Contract end date October 31, 2028	Contract amount for this Amendment Non-financial
Purpose This Amendment extends the term of the current Agreement and updates a number of other terms and conditions.		
Data Type for this Amendment, if applicable		
☒ Driving Record ☒ Vehicle ☒ Vessel	☒ Aggregate driver data ☐ Manufactured home ☒ Other: Firearms data	☒ Protected Personal Information (CAT 3, 4) ☐ Non-Protected Personal Information (CAT 1, 2)
Recipient		
Recipient Name Washington State Patrol		Recipient UBI
Address 106 11 th Ave SW, Olympia, WA 98501		
Contract Manager Wes Vradenburg	(Area code) Telephone (360) 534-2103	Email wesley.vradenburg@wsp.wa.gov
Compliance Manager Wes Vradenburg	(Area code) Telephone (360) 534-2103	Email wesley.vradenburg@wsp.wa.gov
Technical Contact (IT) Wes Vradenburg	(Area code) Telephone (360) 534-2103	Email wesley.vradenburg@wsp.wa.gov
Department of Licensing (DOL)		
Department administration Data Management Office		Division Office of Equity, Performance and Accountability
Address PO Box 2076, Olympia, WA 98507-2076		
Contract Manager Eimear Power	(Area code) Telephone (360) 902-3920	Email datacontracts@dol.wa.gov
Compliance Manager Wesley Marks	(Area code) Telephone (360) 902-3920	Email datacontracts@dol.wa.gov
Amendment		
This Amendment includes (a) an extension to the Agreement term, (b) updates the DOL contract manager and compliance manager, (c) adds language to Permissible Use, (d) modifies the Annual Statement of Compliance, (e) removes the requirement for Professional Liability (Errors & Omissions) insurance and updates language pertaining to cyber liability insurance, (f) updates Recipient Legal Compliance Standards, and (g) inserts a new audit due-date in Attachment D.		
The terms and conditions of this Agreement are an integration of the final, entire, and exclusive understanding between the Parties, superseding all previous agreements, writings, and communications, oral or otherwise, regarding the subject matter of this Agreement. This Agreement is effective upon execution by both Parties. The Parties signing below represent that they have read and understand this Agreement and have the authority to execute on behalf of their entity.		
Recipient Signature Shannon Oien, Chief Contracts Officer	Signed by:  DOL Signature	Date 10/3/2025
PRINT Signatory's Name, Title Shannon Oien Chief Contracts Officer	Name, Title Evelyne Lloyd Assistant Director, Administrative Services Division	
Email: shannon.oien@wsp.wa.gov		

Upon execution, this Agreement Amendment is entered into by and between DOL and Recipient. In consideration of the terms and conditions contained herein, the Parties agree to amend the original Agreement, as follows:

- A. Section 4 - **TERM** is hereby extended to October 31, 2028.
- B. Updates the DOL contract manager and compliance manager listed on page one.
- C. Section 11 - **PERMISSIBLE USE** is replaced in its entirety with the following:

11. PERMISSIBLE USE

- 11.1 The Recipient may only use Data containing Protected Personal Information for the Permissible Use as set forth in Attachment A – Data Licensing Statement. This Agreement does not constitute a release of Protected Personal Information for the Recipient's discretionary use. The Data may be accessed and used only as authorized herein, including internally for system maintenance and testing. Any other use not specifically authorized herein is strictly prohibited.
- 11.2 The Recipient may not use Data not meeting the definition of Protected Personal Information to discern, establish, or determine the identity of, or otherwise re-identify an individual without prior written approval of DOL.
- 11.3 In accordance with RCW 43.17.425 and Washington Executive Order 17-01, Recipient and Subrecipients are explicitly prohibited without limitation against sharing or using Data, including Protected Personal Information, for purposes of investigating, enforcing, cooperating with, or assisting in the investigation or enforcement of any federal or state regulation or surveillance programs or any other laws, rules, or policies that target Washington residents solely on the basis of race, religion, immigration, or citizenship status, or national or ethnic origin.
- 11.4 Any violation of the Permissible Use of the Data, RCW 43.17.425 or RCW 7.115.010 is strictly prohibited and may be cause for immediate termination of this Agreement, as well as other possible civil and criminal penalties.
- 11.5 When prior Protected Personal Information received and retained by Recipient is refreshed with new Data, Recipient must refrain from using the older Protected Personal Information and must dispose of it, unless otherwise required by federal or state law or regulation. Recipient may only use, sell, distribute, and disseminate Protected Personal Information that is the most current Protected Personal Information received under this Agreement unless specifically waived by DOL.
- 11.6 Recipient shall further comply with all Permissible Use requirements set forth on Attachment B – *Privacy and Security Requirements*.
- 11.7 DOL may monitor and investigate the use and security of Protected Personal Information received by the Recipient or its Subrecipients through this Agreement. The Recipient has a duty to cooperate with DOL's investigation and ensure Subrecipient's cooperation with such investigations.
- 11.8 In accordance with RCW 7.115.010 (Shield law) the Recipient and Subrecipients are explicitly prohibited without limitation against sharing or using Data, including Protected Personal Information, for purposes of investigating, enforcing, cooperating with, or assisting in the investigation or enforcement of any federal or state programs or any other laws, rules, or policies that target those who are, or were, in receipt of protected health care services that are

lawful in the state of Washington.

- 11.9 The Recipient and Subrecipients are explicitly prohibited without limitation against sharing or using Data, including Protected Personal Information, for purposes of creating, maintaining, or operating generative artificial intelligence (AI).

D. Section 16 - **INSURANCE** is replaced in its entirety with the following:

16. INSURANCE

a) Required Coverages

Recipient shall maintain self-insurance or commercial insurance as outlined herein. Insurance must be maintained with carriers that are authorized to do business in Washington State and maintain a minimum AM Best rating of A-: VII, or an equivalent rating with a similar rating agency.

All insurance must be primary to any other insurance programs afforded to or maintained by DOL or the state of Washington. Recipient waives all rights against DOL and the state of Washington for recovery of damages to the extent that such damages would be covered by general liability or umbrella insurance maintained by Recipient pursuant to this Agreement.

Recipient must notify DOL within thirty (30) days if a claim has been made under the commercial general liability or self-insurance policy related to the Data provided under this Agreement.

i. Commercial General Liability

Recipient shall maintain self-insurance, or a commercial general liability insurance policy, including contract liability, in adequate quantity to protect against legal liability arising out of activity from this Agreement. Policy shall not be less than the following:

- \$1,000,000 per occurrence
- \$2,000,000 aggregate

ii. ~~Professional Liability (Errors & Omissions)~~ [Removed]

~~Recipient shall maintain Professional Liability insurance covering errors, omissions, or negligence in the activities under this Agreement. Policy shall not be less than the following:~~

- ~~• \$5,000,000 per occurrence~~
- ~~• \$10,000,000 aggregate~~

iii. Cyber Liability

When the Recipient is receiving Protected Personal Information, the Recipient shall maintain cyber liability insurance with policy amounts as outlined below. A Recipient who has access to funds in Washington State's Self-Insured Liability Program is deemed to meet this requirement.

The policy amount is based on the number of unique individuals' records containing Protected Personal Information in Recipient's possession on January 1 after 12 months of receiving Data, and every three (3) years thereafter. When DOL previously approved a reduction in policy value, the approval was valid for no more than three (3) years and must be renewed every three (3) years.

The Recipient's cyber liability insurance policy value is subject to audit to assess if the value accurately corresponds with the number of records held at time of the audit. This insurance shall include coverage for third party claims and losses including with respect to network risks (such as: data Breaches, transmission of virus/malicious code, unauthorized access or criminal use of third party, ID/data theft) and invasion of privacy regardless of the type of media involved in the loss of private information (such as: computers, paper files and records, or voice recorded tapes), covering collection, use, access, etc., of

Protected Personal Information, direct liability, as well as contractual liability for violation of privacy policy, civil suits and sublimit for regulatory defense/indemnity for payment of fines and penalties.

Number of Records Containing Protected Personal Information Held per Policy Period	Policy Value	Policy Value with Mitigations
Greater than one million unique individuals	\$100,000,000	\$15,000,000
500,001 – 1,000,000 unique individuals	\$50,000,000	\$7,500,000
250,001 – 500,000 unique individuals	\$25,000,000	\$3,750,000
100,001 – 250,000 unique individuals	\$15,000,000	\$2,250,000
50,001 – 100,000 unique individuals	\$5,000,000	\$1,000,000
5,250 – 50,000 unique individuals	\$1,000,000	\$1,000,000
1 – 5,249 unique individuals	Policy not required	

DOL will accept the Policy Value with Mitigations when the Recipient demonstrates to DOL's satisfaction certain risk mitigations are in place as described in Exhibit B, *Cyber Liability Insurance Mitigation Table*.

Recipient must receive written approval from DOL showing DOL accepted the evidence and approved the policy value with mitigations. DOL will notify the Recipient in writing when insufficient evidence was submitted, and the Recipient may submit new evidence for DOL's consideration at least 30 days prior to expiration of the current policy. Recipient must obtain a policy with the required value within 60 days of being notified by DOL of the requirement.

The Recipient will not be permitted a policy value less-than the value with mitigations.

If at any time Recipient fails to maintain one or more risk mitigations during the policy period, DOL reserves the right to rescind the policy value with mitigations.

~~A Recipient who has access to funds in Washington State's Self Insured Liability Program are deemed to meet this requirement.~~

b) Additional Insureds

The policies shall include, or be endorsed to include the following provisions:

- a) With the exception of Professional Liability insurance, the state of Washington shall be named as an additional insured, when available to the Recipient, to the full limits of liability purchased by the Recipient even if those limits of liability are in excess of those required by this Agreement.
- b) The Recipient's insurance coverage shall be primary insurance and non-contributory with respect to all other available sources.

c) Notice of Cancellation

Recipient shall provide written notice thirty (30) days in advance of the cancellation of any insurance required hereunder.

d) Certificates of Insurance

Prior to receiving any Data, the Recipient shall provide DOL a valid certificate or certificates of insurance demonstrating the fulfillment of all requirements herein.

Recipient will submit new or renewal certificates on a yearly basis during the term of this Agreement without a lapse in coverage. Certificates must be received within thirty (30) days following the issuance or renewal of any policies or at the direction by DOL to obtain a policy with limits prescribed in this Agreement.

Failure to provide DOL with the required Certificates of Insurance may result in immediate suspension of Access Period and may, at DOL's sole discretion, result in termination of this Agreement.

- E. Section 19 – **ANNUAL STATEMENT OF COMPLIANCE** is replaced in its entirety with the following:

19. ANNUAL STATEMENT OF COMPLIANCE

If the Recipient or a Subrecipient is ~~receiving~~ holding Data, the Recipient must submit annual statements of compliance attesting to the Recipient's compliance with the Privacy and Security Requirements, Subrecipient Requirements, and cyber liability insurance requirements in this Agreement for the period it possesses Data and has Subrecipients that possess Data. Annual statements of compliance are due each year on August 1.

- a) A Statement of Compliance is a written statement drafted by the Recipient, attesting to DOL that it is in compliance with requirements in the Agreement. The Statement of Compliance is valid when signed by personnel authorized to bind the Recipient. After conducting a self-assessment:
 - i. If Recipient is meeting all Privacy and Security Requirements, Subrecipient Requirements, and cyber liability insurance requirements in this Agreement, then Recipient's statement must affirm that it is in compliance with all Privacy and Security Requirements, Subrecipient Requirements, and cyber liability insurance requirements in this Agreement.
 - ii. If the Recipient determines it is not fully compliant with all Privacy and Security Requirements, Subrecipient Requirements, and cyber liability insurance requirements of this Agreement, Recipient must submit a completed Exhibit A – Non-Compliance Form. DOL and Recipient will work together to determine the actions needed to correct all deficiencies noted in the form. Actions pertaining to correcting deficiencies in a Statement of Compliance will be handled as a corrective action plan as described in Attachment D – Audit Requirements.
- b) Corrective actions that were incomplete under prior annual statements of compliance are incorporated into this Agreement and will continue to be monitored by DOL to completion.
- c) If Recipient is processing Data under 15 U.S.C. §1681b as part of a Consumer Report, the Statement of Compliance must attest to compliance with the Federal Trade Commission's Disposal Rule (Disposal of Consumer Report Information and Records, 16 C.F.R., §682.3).

Failure to provide the annual Statement of Compliance may result in the suspension of the Recipient's Access Period.

- F. Section 40 – **RECIPIENT LEGAL COMPLIANCE STANDARDS** is replaced in its entirety with the following:

40. RECIPIENT LEGAL COMPLIANCE STANDARDS

Recipient must comply with all applicable local, state, and federal laws rules and regulations. Such compliance minimally includes without limitation, all applicable licensing requirements of the state of Washington, all civil rights and non-discrimination laws, the Americans with Disabilities Act (ADA) of 1990, ~~and~~ all federal and state employment laws, the Protecting Americans' Data from Foreign Adversaries Act of 2024, and the Data Security Program under federal Executive Order 14117. Failure to comply with this provision may be grounds for termination of this Agreement regardless of the affect it may have on the subject matter of this Agreement.

G. The **Data Security Audit Due Date in Attachment D, 4.**, is amended as follows:

	Data Security Audits
Due Date or Timeline	In addition to any audit currently in progress or due, Recipient must obtain and provide a complete audit report and submit it to DOL on or before <u>June 30, 2026</u>.