Chapter 308-10A WAC
DATA PRIVACY

NEW SECTION

WAC 308-10A-100 Definitions. For the purposes of RCW 46.22.010, the following definitions apply:

(1) "Access period" is a duration of time under the term of this agreement when recipient is granted access and use of protected personal information.

(2) "Agent" means a representative, or representatives, of a requestor that is under contract with the recipient or subrecipient to request driving records on the requestor's behalf. "Agent" includes insurance pools established under RCW 48.62.031 of which the authorized recipient is a member.

(3) "Authorized legal representative" means someone legally authorized under federal or state law to make decisions for the beneficiary. An authorized legal representative is someone who:

(a) Can provide documentation that they have power of attorney; legal guardianship or conservatorship for the beneficiary; executor, etc.; or

(b) Is a custodial parent of a beneficiary who is under the age of 18.

(4) "Authorized use" means a permissible use granted to a recipient in a fully executed data sharing agreement with the department.

(5) "Bona fide research organization" means an entity, such as a university, that conducts noncommercial research using established scientific methods. There must be an intention to publish the research findings for wider scientific and public benefit, without restrictions or delay. Bona fide research organizations do not use protected personal information for commercial purposes.

(6) "Breach" or "breaches" means an unauthorized acquisition, loss of control or exposure to an unauthorized person or business, or misuse of protected personal information. Ransomware and unauthorized offshoring of protected personal information are included in this definition.

(7) "Course of business" or other similar term means activities that pertain to the use of protected personal information as authorized by the recipient's data sharing agreement with the department.

(8) "Customers" means those entities that the recipient is providing services to using protected personal information but is not receiving protected personal information from the recipient. "Customers" does not include those entities receiving statistical reports.

(9) "E-service" means a data service hosted by the department enabling approved users access to data through a secure access Washington (SAW) or license express account. E-services include, but are not limited to, driver and plate search (DAPS), driver adjudication and information system (DIAS), contracted plate search (CPS), driver record request (DRR), abandoned vehicle report (AVR).

(10) "Governmental entity" means a federal agency, a state agency, board, commission, unit of local government, or quasi-governmental entities.

(11) "Incident" means an event that confirms, or is reasonably thought to be, the unauthorized access to, or misuse of, protected personal information. Ransomware attacks are included in this definition.

(12) "Independent third party" means any entity other than a member of the recipient or any of its stockholders, or any entity controlled by or under common control with any of the stockholders or the company group.

(13) "Individual registered or legal vehicle or vessel owner" or "individual vehicle or vessel owner" means a single vehicle or vessel owner, for the purposes of RCW 46.12.630.

(14) "List" means multiple records containing protected personal information, regardless of the method recipient uses to request or obtain records.

(15) "Misuse" means the access, disclosure or use of protected personal information without the express, written authorization from the department in a data sharing agreement. "Misuse" also includes a violation of any privacy requirement outlined in a data sharing agreement.

(16) "Offshoring" means the electronic or hard copy transmission, accessing, viewing, capturing images, storage, or processing of protected personal information outside the United States.

(17) "Per incident," for the purposes of RCW 46.22.010(4), means each time protected personal information is accessed or used by an unauthorized entity or individual. "Per incident" does not refer to individual records.

(18) "Permissible use" means authorized or required uses as outlined in federal or state law, and authorized in the data sharing agreement.

(19) "Protected personal information" means collectively personal information and identity information, as defined by RCW 46.04.209, 19.255.005, and 42.56.590, authorized for disclosure by the federal Driver Privacy Protection Act and state law.

(20) "Recipient" means an entity directly receiving protected personal information from the department through a data sharing agreement.

(21) "Requestor" means an entity with an authorized permissible use to receive protected personal information from the department. A requestor may be an agent, subrecipient, or a recipient.

(22) "Regulatory bodies," for the purposes of RCW 46.52.130, means a body established by federal or state law and is responsible for regulating compliance with adopted rules or laws.

(23) "Statement of compliance" means a statement signed by an executive of an organization attesting to the recipient's full compliance with requirements in its data sharing agreement with the department.

(24) "Subrecipient" means any entity outside your immediate organization that receives or has access to protected personal information including, but not limited to, subsidiaries, subcontractors, requestors, or agents.

NEW SECTION

WAC 308-10A-201 Recipient compliance requirements. (1) Audits - For a recipient receiving protected personal information:

(a) A recipient receiving recurring lists of data must undergo audits as outlined in the data sharing agreement.

(b) A recipient receiving a one-time list containing multiple records must demonstrate security controls are in place to protect the data and may be required to undergo an audit prior to receiving protected personal information.

(c) A recipient receiving data through an e-service is subject to an audit when the department has cause to investigate a breach or misuse.

(d) The cost of all audits, including actual costs incurred by the department to conduct, process, and review each audit, is the responsibility of the recipient. The department will provide an estimated cost of the audit in advance. The department will minimize the cost of the audit whenever possible.

(e) The department may suspend or terminate a recipient's access to data if the recipient fails to provide an acceptable audit by the due date established by the department.

(f) The department will only accept third-party audits that meet department audit standards and are performed by auditors that meet independent third-party auditor qualifications. Washington state agency internal audit programs that satisfy certification requirements of the office of financial management are considered independent third-party auditors for purposes of this section.

(2) Subrecipient lists - A recipient must provide the department with a list of:

(a) All subrecipients and secondary subrecipients that received protected personal information originating from the recipient in the time frame requested; and

(b) All customers for whom the recipient processes protected personal information.

NEW SECTION

WAC 308-10A-202 Vetting of subrecipients. Before giving a subrecipient access to protected personal information, that the recipient must validate that the subrecipient demonstrates the following minimum requirements:

(1) The subrecipient has a permissible use under federal or Washington state laws, whichever is more restrictive.

(2) The subrecipient is a qualified recipient under federal or Washington state laws.

(3) The subrecipient has sufficient protections in place to secure the privacy of the protected personal information in accordance with the data sharing agreement.

NEW SECTION

WAC 308-10A-203 Subrecipient disqualification. When the department notifies a recipient that its subrecipient is ineligible to receive protected personal information, the recipient must immediately:

(1) Terminate the subrecipient's access to protected personal information; and

(2) Require the subrecipient destroy all protected personal information it obtained through the recipient.

NEW SECTION

WAC 308-10A-204 Subrecipient audit requirements. (1) A recipient must have procedures to audit subrecipients for compliance with the terms and conditions of its contract with the subrecipient.

(2) The audit methodologies must be sufficient for a reasonable person to conclude a subrecipient is compliant with requirements in the contract between recipient and subrecipient.

NEW SECTION

WAC 308-10A-205 Required written consent audits. (1) Recipients who provide protected personal information to subrecipients, when a person must sign a release form under RCW 46.52.130, must establish processes to hold all subrecipients accountable for:

(a) Obtaining and maintaining the release form prior to requesting protected personal information;

(b) Verifying the release form is properly executed before requesting the protected personal information; and

(c) The consent is rightfully executed by the named individual or their authorized legal representative.

(2) The process for requesting driving records must include verifying the consent forms contain the required information in WAC 308-10A-901.

(3) The recipient must make records available to the department demonstrating the process for obtaining consent is in use and is effective. The department will establish minimum requirements for such processes in its data sharing agreement with the recipient.

NEW SECTION

WAC 308-10A-301 Contract with subrecipient. (1) A recipient must have a written agreement with a subrecipient before giving the subrecipient access to protected personal information.

(2) The written agreement must include those requirements that the department has identified in the recipient's data sharing agreement as those to be passed on to subrecipient.

(3) A recipient is subject to the penalties described in RCW 46.22.010(4) if they give a subrecipient access to protected personal information without a data sharing agreement that includes those requirements that the department has identified in the recipient's data sharing agreement as those to be passed on to subrecipient.

NEW SECTION

WAC 308-10A-401 Standards for audits of recipients. When the department requires an audit under this section, it may accept an audit performed in the previous 12 months when it meets recipient audit standards and is performed by an auditor that meets independent third-party auditor qualifications, and for recipients receiving lists of protected personal information:

(1) Auditor procedures must test for the presence of required policies and administrative, technical, or physical controls to reasonably conclude the controls are effective and in use by the recipient.

(2) Audit reports must provide documentation on the procedures, and the results of such procedures, used to determine whether controls align with requirements in the data sharing agreement.

(3) For recipients receiving individual records of protected personal information, audit reports must demonstrate reasonable procedures were used to conclude each recipient is compliant with requirements in the data sharing agreement.

NEW SECTION

WAC 308-10A-402 Selection of an auditor. If the department chooses not to perform an audit, the recipient must select a qualified independent third-party auditor to conduct the audit.

NEW SECTION

WAC 308-10A-403 Independent third-party auditor qualifications. Independent third-party auditors conducting data security audits must, at a minimum, hold one of the following certifications:

(1) American Institute of Certified Public Accountants (AICPA);

(2) Certified Information Privacy Professional (CIPP);

(3) ANSI-ASQ National Accreditation Board (ANAB); or

(4) Other nationally recognized information technology auditing certification.

NEW SECTION

WAC 308-10A-404 Statement of compliance. (1) The recipient will:

(a) Perform a self-assessment to determine compliance with the requirements of the data sharing agreement.

(b) Confirm in writing to the department that it complies with requirements in the data sharing agreement.

(c) Document instances of noncompliance with the data sharing agreement and include a corrective action plan to correct all deficiencies.

(d) Include a declaration with their statement of compliance that affirms protected personal information is only used as authorized.

(2) The frequency of the statement of compliance will be outlined in the data sharing agreement.

NEW SECTION

WAC 308-10A-405 Corrective action plans. (1) When notifying the department of any noncompliance with the data sharing agreement, the notification must include a corrective action plan for each deficiency.

(2) The corrective action plan must identify the anticipated date the recipient will complete each action to either bring the recipient into compliance or eliminate the deficiency.

(3) The department may accept the recipient's action, and close the action item, or may require additional action.

NEW SECTION

WAC 308-10A-500 Pertaining to RCW 46.12.630. (1) For the purposes of RCW 46.12.630(1): The sharing of protected personal information will be in accordance with the following vehicle and vessel regulations as they existed on January 1, 2022:

(a) For vehicles:

(i) Titles I and IV of the Anti-Car Theft Act of 1992;

(ii) The Automobile Information Disclosure Act (15 U.S.C. Sec. 1231 et seq.);

(iii) The Clean Air Act (42 U.S.C. Sec. 7401 et seq.); and

(iv) 49 U.S.C. Secs. 30101-30183, 30501-30505, and 32101-33118;

(b) For vessels:

(i) 46 U.S.C. Sec. 4310; and

(ii) Any relevant section of the Code of Federal Regulations adopted by the United States Coast Guard.

(2) For the purposes of RCW 46.12.630(2):

(a) Whenever the recipient grants a request for protected personal information to an attorney or private investigator, the recipient shall provide notice to the vehicle or vessel owner, as required under RCW 46.12.635, and as outlined in its data sharing agreement with the department.

(b) "Federal, state, or local agency," "local governmental entity," "governmental agency," and "government agency" have the same meaning as "governmental entity." (See WAC 308-10A-805.)

(c) For the purposes of section RCW 46.12.630 (2)(e), the permissible use is restricted only to a governmental agency or its agent, as authorized by the Driver Privacy Protection Act 18 U.S.C. Chapter 123.

(d) For purposes of section RCW 46.12.630 (2)(h), "other applicable authority" includes out-of-state or Canadian entities legally authorized to operate a toll facility.

NEW SECTION

WAC 308-10A-700 Research. (1) The department will disclose protected personal information for research purposes to governmental entities and bona fide research organizations only when:

(a) The research cannot reasonably be conducted without the protected personal information, the recipient provides adequate information for the department to reasonably determine that the disclosure of protected personal information will not harm individuals, the benefits to be derived from the disclosure are clearly in the public interest, and the results are not of a commercial interest; or

(b) The research purpose has been approved in writing by an authorized official in the department, legislature, or governor's office.

(2) The department may disclose pseudonymized data for research purposes on the condition the recipient will make no attempt to reidentify individuals.

NEW SECTION

WAC 308-10A-801 Agents. Where agents are permitted, a requestor may access protected personal information through a chain of agents. For example, an employer (requestor) may use an employment agency (agent #1) to request records on its behalf. In turn, the employment agency may request the record through a data broker (agent #2).

NEW SECTION

WAC 308-10A-802 Offshoring. Unless otherwise explicitly authorized in statute, or with prior written authorization from the department, recipients must:

(1) Only transmit, access, view, store, or process protected personal information within the United States.

(2) Maintain the primary, backup, disaster recovery, and other sites for storage of protected personal information within the United States.

NEW SECTION

WAC 308-10A-803 Cost recovery fees. Pursuant to RCW 42.56.120, the department's fees for providing customized services are the actual hourly rate of department staff multiplied by the actual hours, and fractions thereof, it takes to respond to the request.

NEW SECTION

WAC 308-10A-804 Notification of incident/breach. In the event of an incident or breach the recipient must:

(1) Notify the department of an incident or breach, or upon receiving notice from a subrecipient of an incident or breach, as outlined in its data sharing agreement with the department;

(2) Comply with all department requirements in managing the incident or breach.

(a) The subrecipient must notify the recipient of an incident or breach.

(b) All notices to the department must be made before notice to any individual or the public.

(c) Recipients and subrecipients are responsible to make notifications as required by RCW 19.255.010 or 42.56.590, as applicable.

NEW SECTION

WAC 308-10A-805 Applications for data. (1) An application must be submitted to the department when requesting data.

(a) The department may reject incomplete applications.

(b) The department may close the application if the applicant does not provide sufficient information to complete the application process within 90 days of request.

(c) The department may close an approved application to receive data if the applicant does not execute the data sharing agreement within 30 days of department sending the agreement to the applicant for signature.

(2) In the event of a declared emergency, the department may allow a governmental entity to execute a data sharing agreement prior to submitting a formal application. The government entity must submit the application by a date designated by the department. The department may waive the requirement for an application.

NEW SECTION

WAC 308-10A-806 Consent. For the purposes of disclosing protected personal information, an individual's authorized legal representative may authorize the disclosure.

NEW SECTION

WAC 308-10A-901 Authorization to request a driving abstract. (1) When the subject of a driver's abstract must authorize the release of the abstract under RCW 46.52.130, the party requesting the driver's abstract under the terms of a data sharing agreement may use the department's release form, or its own version of the release form provided it contains the information required by federal and state law, and the department. The party requesting the driver's abstract under the terms of a data sharing agreement must verify that its release form is consistent with federal and state law, and department requirements.

(2) If a recipient or subrecipient uses its own version of the release form, the form must not bear the department logo or otherwise indicate it is an official Washington state document.

(3) The release form may be signed in ink or electronically.

(4) A release form must:

(a) Include the name and signature of the person whose record is being requested, or the name and signature of their authorized legal representative.

(b) Include the date the signature was made.

(c) Be signed by the employer or volunteer organization, attesting to:

(i) For employment/prospective employment, driving is a condition of employment or otherwise at the direction of the employer, or the employee or prospective employee handles or will be handling heavy equipment or machinery.

(ii) For volunteering, the information is necessary for purposes related to driving by the individual at the direction of the volunteer organization.

(iii) For employee/prospective employee releases.

(A) Include a statement that any information contained in the abstract related to an adjudication that is subject to a court order sealing the juvenile record of an employee or prospective employee may not be used by the employer or prospective employer, or an agent authorized to obtain this information on their behalf, unless required by federal regulation or law; and

(B) Provide instructions for how someone can demonstrate that an adjudication contained in the abstract is subject to a court order sealing the juvenile record.

(I) The name(s) of the agent(s) authorized to obtain the information on the requestor's behalf.

(II) Include information on where to send the form after it is properly executed.

(5) When the subject of a driver's abstract must authorize the release of the abstract under RCW 46.52.130, the party requesting the driver's abstract under the terms of a data sharing agreement must retain the signed release form for at least six years.

(6) The signed release form may be used for employment or volunteering purposes during the period the subject of the driver's abstract is under continuous employment or volunteering. The employer or volunteering organization must process a new release form for the subject of the driver's abstract when there is a break in employment or volunteering.

(7) For the purposes of prospective employment or volunteering, the release form and the driving record must be disposed of after six months from the date the record was obtained, or as otherwise required

by law, if the subject of the driver's abstract is not placed into a position with the employer or volunteer organization that involves driving as a function of the position.

NEW SECTION

WAC 308-10A-902 Fair Credit Reporting Act (15 U.S.C. Section 1681, as amended). The recipient or subrecipient must not use the statute of limitations for legal action under the Fair Credit Reporting Act (FCRA), or similar federal or state law, as a basis for record retention. The recipient must establish and maintain data retention policies based on using records as authorized in the data sharing agreement and when the business use of the data has been fulfilled, with the intent of destroying the record as soon as the record is no longer needed for the permissible use.