Washington State Department of Licensing
Responses to customer input
Substitute Senate Bill 5152, Draft WAC, Contract requirements

Updated March 10, 2022

For your convenience, we've attempted to sort the questions into broad topics. However, many questions and answers can cover more than one topic, so we encourage you to read all the material provided. Our goal is to update as needed, through March 25, 2022.

If this FAQ did not answer your question, please submit it to DataContracts@dol.wa.gov. Please do not send questions to individual staff members as we're tracking the receipt and response to each question to ensure we don't miss anything. We cannot guarantee responses to your comments and questions unless they're sent to DataContracts@dol.wa.gov. Verbal responses are not official. Please refer to the written responses herein.

We are providing a **one-time extension** for stakeholder input to close of business April 1, 2022. Thank you.

General

1. What is the difference between "e-services" and "bulk"?

   Response: E-services are those data services where customers access data directly through DOL's DRIVES system, generally searching on a single record. They include:

   - Abandoned Vehicle Reporting (AVR)
   - Contracted Plate Search (CPS)
   - Driver and Plate Search (DAPS)
   - Driver Information & Adjudication System (DIAS)
   - Driver Record Request (DRR)

Admittedly, the term “bulk” is misleading. We generally refer to “bulk” customers as those who receive volumes of data through our web services or Secure File Transfer Protocol (SFTP) interfaces. We refer to these services as our “bulk” services, because it’s through those interfaces where most of our data is accessed. However, we do have a few recipients that are getting a high volume of records through our e-services.

2. How many different types of Data Licensing Statements (DLS) are there?

   Response: There is a different Data Licensing Statement (DLS) for each type of data service, including:

   - Driver and Plate Search
   - Driver Record & Monitoring
   - Aggregate data (used for unique files)
   - Abandoned Vehicle Report e-service
   - Contracted Plate Search e-service
   - Driver and Plate Search e-services
   - Driver & Adjudication e-service
   - Driver Record Request e-service

3. I noticed that there are several references to "licensee" in the draft Data Sharing Agreement, but I didn't see that term defined in the WAC. Can you clarify how that licensee is different from recipient or requestor?

   Response: Thank you for pointing that out. The term “licensee” was the word we used to describe Recipients in previous contracts. We have replaced the term “Licensee” with “Recipient” in the contract template. Nice catch!

4. Did I understand from your statement in the Stakeholder Webinar that when personal information is gathered that person must be informed of the access of their information?

   Response: Currently, in most cases, there is no requirement that we proactively notify someone when their Protected Personal Information is accessed. However, to promote transparency to residents of the state, we will be requiring bulk data recipients to provide the name of the Subrecipients or Customer, and the Permissible Use when they request the record. That way, if asked, we can inform customers exactly how their personal information is being used.

Currently, we are not requiring e-service users to provide Subrecipients or Customer, and the Permissible Use information. This is due to current system limitations. However, we anticipate that this will become a requirement in the future.

5. Substitute Senate Bill 5152 authorizes civil penalties of up to $20,000 per incident. How do you see this penalty being applied?

   Response: We are currently working on developing the processes and procedures for how penalties will be assessed and will share that information with you when it's available for comment.

6. Can I pay the invoice using a credit card?

   Response: Unfortunately, no. Our headquarters does not have the capability of processing credit card payments.

7. Can you please speak to timeline for going live/executing the new templates?

   Response: We are accepting stakeholder input through March 4, 2022. After that, we plan to finalize the contract template.

   Current recipients will need to submit a new/updated application. We will use the information in the application to develop the contract with that recipient. We will begin accepting applications this spring.

   If all goes well, we plan to start issuing the new contracts this summer, with an effective date of November 1, 2022.

8. For those who could not attend the webinar when would the video be available to see?

   Response: Unfortunately, the webinar recordings are too big to send out via email. We'll be posting links to the webinars and this FAQ to our rulemaking website at https://www.dol.wa.gov/about/rules.html. We're hoping the webinars will be posted in the next few days.

9. For Section 12, *Permissible Use*, of the draft contract template, the 4th paragraph - motor vehicle record purchasers retain and use older data (for legal purposes).

   Response: It is not clear what is meant by "legal purposes". Generally, DOL expects:

   - For *governmental entities* you follow your approved records retentions schedules.
   - For *private sector entities*, you retain the record long enough to fulfill the permissible use for which it was requested. Example:
     - If you requested a driving record to determine if someone is eligible to driver on your business' behalf, once that decision is made, the record should be destroyed. However, if there is a law that requires the retention of the record for a specific timeframe, such as for Commercial Driver Licenses, you should follow the law.

- If you requested the vehicle owner record for the purposes of collecting a private tolling fee, you may retain the information throughout the collection process, then it must be destroyed.

10. For Section 12, *Permissible Use*, of the draft contract template, the last paragraph - this appears to apply to driver license data. Vehicle owner data can be used for more than one purpose.

    Response: To the contrary, the paragraph applies to both vehicle and driver Protected Personal Information.

    The general requirement is for the record to be requested each time a new permissible use is identified, and not for the information to be reused for multiple purposes. The reasoning for this is that vehicle ownership can change between the time the data was pulled for the original permissible use and any subsequent use.

    Sending a tolling or parking violation to the incorrect owner of the vehicle at the time of the violations is considered a misuse of Protected Personal Information and can be subject to penalties.

11. NEW 3/4/22 – What is CAT 3 and CAT 4 data?

    Response: Data classifications are established by the Office of the Chief Information Officer, as part of the IT Security Standards that any Recipient must comply with to receive Protected Personal Information. See OCIO 141.10 (https://ocio.wa.gov/policies/141-securing-information-technology-assets/14110-securing-information-technology-assets). Specifically:

    Category 3 – Confidential Information

    Confidential information is information that is specifically protected from either release or disclosure by law. This includes, but is not limited to:

    a. Personal information as defined in RCW 42.56.590 and RCW 19.255.10.
    b. Information about public employees as defined in RCW 42.56.250.
    c. Lists of individuals for commercial purposes as defined in RCW 42.56.070 (8).
    d. Information about the infrastructure and security of computer and telecommunication networks as defined in RCW 42.56.420.

    Category 4 – Confidential Information Requiring Special Handling

    Confidential information requiring special handling is information that is specifically protected from disclosure by law and for which:

    a. Especially strict handling requirements are dictated, such as by statutes, regulations, or agreements.
    b. Serious consequences could arise from unauthorized disclosure, such as threats to health and safety, or legal sanctions.

12. NEW 3/3/22 – What is the definition of a commercial data broker?

Response: DOL is not adopting a specific definition of a commercial data broker for use in the WAC and contract template; however, we use the term internally. The general definition is: a data broker is a company that specializes in collecting information from public and private sources, and selling or licensing such information to third parties for a variety of uses.

Cyber Liability Insurance (CLI)

1. Regarding insurance requirements for WA State Agencies - Will the DSA template be tailored for interagency DSA agreements where the WA State Agency is covered under the WA State Self Insurance Liability Account or the Alliant Property Insurance Program?

   Response: The requirement will apply regardless if the Recipient purchases the coverage or is self-insured.

2. Regarding cyber and waiver of subrogation, can we assume that best practices for this type of coverage will be used when the requirements are put out there?

   Response: The requirement for the waiver of subrogation has been taken out of the current draft requirement.

3. Will Cyber Liability Insurance be a requirement (assuming there are no mitigating circumstances) for state/local agencies (law enforcement, specifically)?

   Response: We are developing a scaled approach to the Cyber Liability Insurance. Cyber Liability Insurance will be required based on the number of records you receive, regardless of how you access the data (e-service or through a bulk interface). Most Recipients will not be required to have Cyber Liability Insurance because they do not access enough records.

4. For the Cyber Insurance do you have a singular agency in mind, or would we have to find an agent that handles this type of insurance?

   Response: Recipients are responsible for choosing the carrier they purchase the Cyber Liability Insurance from. Insurance carriers must meet the minimum requirement outlined in the contract clause.

5. We are a small state agency and have cyber insurance, but it does not name DOL. Is proof that we have cyber insurance enough?

   Response: At currently drafted, there will be requirement to have DOL named as an additional insured.

6. Can you tell me if government agencies are going to be required to carry insurance?

   Response: All recipients are required to be self-insured or have Commercial General Liability Insurance. Most entities receiving Protected Personal Information, will not be required to have Cyber Liability Insurance. The amount of the coverage will be dependent on the number of records you access.

7. We are trying to determine what reason DOL is requesting that we provide insurance naming DOL as an additional insured. Currently, we have insurance that meets all of the listed requirements; however it is unclear why we are being required to add the state as an additional insured. I need to be able to explain this to our insurance company.

   Response: We are asking to be included as a named insured because in the event there was a data incident, from the data recipient's system for which they were liable for, and the DOL were to be named in a lawsuit, the data recipient's insurance policy should respond for the DOL as the additional named insured.

8. My business only requests a few records per year. Will we be required to have the Cyber Liability Insurance?

   Response: The Cyber Liability Insurance requirements is based on the number of records you have. The current proposal is if you are storing less than 5,249 people's records, you would not be required to have insurance. If you are storing more than that, the requirement is based on the following sliding scale:

   - Greater than one million persons: $100,000,000
   - 500,001 – 1,000,000 persons: $50,000,000
   - 250,001 – 500,000 persons: $25,000,000
   - 100,001 – 250,000 persons: $15,000,000
   - 50,001 – 100,000 persons: $5,000,000
   - 5,250 – 50,000 persons: $1,000,000
   - 1 – 5,249 persons: No CLI required

   The scale above is the DRAFT scale we're considering. We've sent this to all stakeholders and requesting input by close of business March 4, 2022. DOL executive management will have to approve any Cyber Liability Insurance requirements.

9. We are a governmental entity. Will we be required to have the Cyber Liability Insurance?

   Response: Possibly. The requirement is not based on what type of entity you are (private or public sectors), but on how many records containing Protected Personal Information you have. See Question #8 for how much insurance may be required.

10. NEW 3/4/22 – Are Subrecipients required to carry cyber liability insurance?

    Response: DOL is not planning to require Recipients to pass on the CLI requirements to Subrecipients. That decision is up to the Recipient. However, if there is a breach, DOL will hold the Recipient accountable for the actions of its Subrecipients.

11. NEW 3/10/22 – Is this cyber liability insurance for only the DAPS program or is it for all DOL records through ACCESS?

Response: We will not be requiring the cyber liability insurance for data received through the Washington State Patrol's Access Switch. It's only for records you receive directly from DOL through, including e-services such as Driver and Plate Search (DAPS).

12. NEW 3/10/22 – How can I reduce the amount of cyber liability insurance I have to carry?

    Response: There may be a few ways:
    - Since the amount of insurance is based on how many unique records you keep in your system(s), regularly deleting the Protected Personal Information once it is no longer needed will reduce the number of unique records you hold, and thus could reduce the amount of insurance you'll be required to carry.
    - DOL is also considering other mitigating factors and have asked stakeholders what kinds of things we should consider. To date, we have received no input.

13. NEW 3/10/22 – What if my insurance carrier won't give me a policy for the entire amount?

    Response: Cyber insurance can also be purchased in layers. For example, you may purchase a primary policy and your insurance broker can find a carrier to insure at a level excess of the primary policy. This is done to spread the risk among different carriers. The cost of excess insurance policies is typically less than the primary policy.

14. NEW 3/10/22 - We would like to know under what existing law DOL has the authority to determine the types of insurance serviced entities carry and in what amounts.

    Response: There is no existing law, DOL is seeking to protect our customer's data by virtue of a cyber liability insurance policy.

15. NEW 3/10/22 – For e-services such as DRR, the data is housed by DOL, not by the service entity requesting the information. We are only liable for the information we receive from DOL once the request is acknowledged, and once the information comes to us.

    Response: Agreed.

16. NEW 3/10/22 – We already carry cyber liability insurance that meets the proposed requirements of Section 19. However, the intent and scope of our insurance is to cover the losses incurred when *our* data systems are jeopardized or breached in some way; or if *our* data is compromised. Our cyber liability policy limits are governed by the attached document from Alliant, who manages the largest public entity pooling placement in the world. Our member liability limit is $2M in the aggregate. Based upon the fact that cyber liability policies are becoming harder to obtain, and we already have the highest public pool limits of liability in the market – we believe the limits proposed in the table in the draft clause will be very burdensome to many of the entities who rely upon DOL for its services. We also believe many won't qualify for the limits proposed, let alone be able to afford the premiums.

Response: DOL is seeking coverage for when Protected Personal Information is in your systems and there is a breach. Most of the data recipients fall under the 5,250 records and will not require cyber liability insurance. There are also mechanisms in place to reduce the required limits based on factors that reduce overall risk. If data recipients employ these various mitigating strategies, policy values can be reduced. We understand the challenging market for insurance right now, but we also understand the reasons for it. Cybercrime is on the rise and protecting our customer's data is of paramount importance.

17. NEW 3/10/22 – The requirement for entities to name the state of Washington as an additional insured is not an industry norm, nor do most commercial insurance providers practice this for professional liabilities. We already provide certificate of insurance (COI) on an annual basis to other Washington agencies. We do not name the state or other state agencies as an additional insured on the COI.

    Response: While additional insured is something we have asked for; we not sure we will be successful here in being named as an additional named insured for reasons such as you explained. That's why we're asking for feedback from stakeholders.

E-Services – AVR, CPS, DAPS, DIAS, DRR

1. How can I get a copy of an e-services usage reports?

    Response: DAPS is the only e-services that has a usage report available. Both the administrators and managers can access it. None of the other e-services has that reporting functionality. However, we're working with our IT department to add that reporting functionality. Due to limited staffing resources and a backlog of work, this functionality likely won't be added for near term. You can request an e-service user report by emailing us at DataServices@dol.wa.gov.

2. Will there be a field for us to enter permissible use and subrecipient information within DAPS?

    Response: Currently, we are not requiring e-service customers to enter Subrecipient names and permissible uses. However, we anticipate that this will be a requirement in the future.

3. The obligations and restrictions in the draft Data Licensing Agreement are mainly centered around Protected Personal Information. Based on the definitions for identity information and personal information, it appears that Contracted Plate Search does not provide data that includes Protected Personal Information. Agree?

Response: Disagree. CPS provides the names and addresses of vehicle and vessel owners. Under state law, and DOL policy, name and address are considered personal information, and as a result are included in the definition of Protected Personal Information.

4. We used to get information when someone was deceased in Contracted Plate Search. Will we get that information again?

   Response: Currently death data is not associated with vehicle or vessel records. Pursuant to DOL's current contract with the Department of Health for death data, we can only use that information to update driver and disabled parking records. We do not anticipate that CPS will include death information in the future.

5. During a claim investigation Contracted Plate Search information about registered owners and vehicle identification becomes part of the claim file. During the life of the file there may be litigation and it is necessary to provide the claim file to legal counsel. Will defense or coverage counsel be considered a subrecipient?

   Response: Yes. Anyone who gets Protected Personal Information passed down to them is considered a Subrecipient.

6. Is law enforcement still altering records in DAPS?

   Response: DAPS is a search engine for identify and vehicle ownership information only. Driver and vehicle records cannot be altered in DAPS. If a law enforcement agency needs information beyond what is provided in DAPS, it can make a request through the NextRequest portal at https://www.dol.wa.gov/about/howtorequest.html.

7. As a wrecking yard we receive Junk Vehicle Affidavits that we must check the VIN thru E-Services and see if there is a Legal Owner on the vehicle, if there is a Legal Owner and it is not on the Junk Vehicle Affidavit, we usually turn the vehicle away. Customer state that Law enforcement did not give them a Legal Owner so how are they supposed to get the Legal Owner information?

   Response: See RCW 46.55.100. In Washington, law enforcement agencies make legal owner information available to a registered tow truck operator when a vehicle is impounded. Further, following submittal of an abandoned vehicle report, the department provides the registered tow truck operator with owner information. The registered tow truck operator can provide you, the wrecking yard, with the needed information.

8. Related to Junk vehicles, when you say owner which owner are you talking about? The property owner or the junk vehicle owner?

Response: Vehicle owner, as the law authorizes who we can give vehicle owner information to, and for what purpose. Unfortunately, the law does not explicitly authorize DOL to give vehicle owner information to wrecking/scraping companies. Therefore, those entities must either have written consent from the vehicle owner or get the information from someone authorized to access the vehicle owner information such as law enforcement or the tow truck operator.

9. I am a process server, the reason I use the site is to locate a physical address for the defendant. Most of the time people have their vehicle registered to a PO Box address, is there a change that can take place that allows process servers to view physical address? Most of the time this is to locate them over a complaint for damages stemming from auto accidents.

   Response: We can only provide Protected Personal Information as authorized in state and federal law. State law requires that where both a mailing address and residence address are recorded, DOL only releases the mailing address. Our data services are programmed not to provide residential address when there's a mailing address on record.
   However, you can request the residential address through a public disclosure request through the NextRequest portal at https://www.dol.wa.gov/about/howtorequest.html.

10. For the DRIVE records "consent" requirement, do you mean consent from the person who is being queried in the DOL system? or does this not count for e-Services (DAPS/DIAS)?

    Response: Washington law requires that an employer or volunteer organization get the signed consent of the employee/prospective employee, or volunteer prior to requesting the driving record.
    DAPS does not contain driver record (including violations, citations) information; it is limited to identity information.
    DIAS is not supposed to be used for employment or volunteer organizations purposes. It is intended only for the use of governmental entities, mainly courts, to fulfill the functions of their jobs. Therefore, consent is not required for records pulled from DIAS. However, if you are using DIAS for employment or volunteer organization purposes, please contact DataServices@dol.wa.gov to request access to the Driver Record Request system.

11. As a small user for Contracted Plate Search queries, we make just a couple of queries per month, so our invoices are very small. Can our agency be billed quarterly or yearly, instead of monthly?

    Response: For governmental entities, we can adjust billing frequency. Please contact DataServices@dol.wa.gov.

12. If you can clarify for me, please, my group of 3 to 4 officers uses DAPS for plate search only however we request registered owner information approximately 8-10,000 times a year. Does that mean we are subject to thousands of dollars' worth of audits?

Response: DOL reserves the right to audit any entity accessing Protected Personal Information. For e-services, our efforts are focused on the Annual Statement of Compliance, and not on performing full audits. The likelihood of an entity accessing an e-service having to go through a full audit is very small.

13. We use DAPS to pull records for law enforcement cases, and send information via bulletins, and email (encrypted). The data is kept per retention policies. How long are we to keep the records?

    Response: There is no issue when your policies and practices are based on current guidance in the Law Enforcement Records Retention Schedule published by the WA Secretary of State. See https://www.sos.wa.gov/_assets/archives/recordsmanagement/law-enforcement-records-retention-schedule-v.8.0-(february-2022).pdf

    Law enforcement entities are authorized to share the Protected Personal Information they access through DAPS. Your use of encrypted emails is a great way to ensure that the Protected Personal Information is protected. We expect that all governmental entities follow their approved records retention schedules for how long to keep the data.

14. The annual audit for DIAS is usually in July, correct?

    Response: Yes, the Annual Statement of Compliance is typically due in July. The schedule may change based on our workload and available resources.

15. Through DRIVES, DAPS and DIAS, can law enforcement access DOL driver and vehicle customer information using their DOL business account to bypass DOL administrative oversight and avoid ACCESS CHRI system security controls?

    Response: No, DOL knows how authorized users access DAPS and DIAS and DOL provides administrative oversight of those systems. DOL does not administer ACCESS CHRI and cannot speak to controls in place for users of that system.

Vehicle Owner Information

1. Is vehicle lienholder information personal or private?

    Response: It is considered Protected Personal Information.

Driving Records, Monitoring, Consent New 3/10/22

1. NEW 3/10/22 – As a requester for an Employer will we be given a contract?

   Response: Whether an entity gets a contract with DOL for data depends on many factors including, but not limited to, if they meet our contracts requirements (such as the Privacy Requirements), if they have the technical expertise to work with our IT staff, the volume of data they anticipate requesting, and the permissible use they're requesting.

   At the time, however, due to limited IT staff, DOL is not currently contracting with new Recipients for bulk data. In those cases, we will try to refer the applicant to a Recipient that already has access to our Driver Record/Monitoring web service. We are working to have this situation resolved by 2023.

Compliance New 3/10/22

1. NEW 3/10/22 – Question about Slide/page 7, Compliance, of the webinar presentation: Is there any consideration being given to having an itemized invoice option? Or perhaps an itemized list available upon request?

   When we've had issues with discrepancies in the past, we have been unable to identify which user was at fault for corrective action.

   Response: Upon request we can provide an itemization of the invoice.

2. NEW 3/10/22 – The audit invoicing in the "5 figure" range, does that mean a Recipient will be paying $10,000 or more for DOL to perform an audit on the roughly 20 inquiries I have into registered vessel owners each year?

   Response: DOL does reserve the right to audit any entity receiving Protected Personal Information. Bulk data users are audited on a risk-based schedule, typically every 2-4 years, and it is these audits that typically run in the 4 to 5 figure range. The actual cost of the audits depends on the size and complexity of the organization and its IT systems, along with other factors.

   For e-services, most users are only being asked to provide an Annual Statement of Compliance. However, should DOL feel that Protected Personal Information is at risk (e.g., due to a data breach), DOL may exercise its option to audit.

3. NEW 3/10/22 – How often will the audit be done?

   Response: Bulk data users are audited on a risk-based schedule, typically every 2-4 years.

   For e-services, most users are only being asked to provide an Annual Statement Of Compliance. However, should DOL feel that Protected Personal Information is at risk (e.g., due to a data breach), DOL may exercise its option to audit.

4. NEW 3/10/22 – Please clarify your position of charging for reviewing data security audits. Is that isolated to reviewing "IT" Data Security Audits or are you intending to charge for the 3-year Permissible Use audit?

   Response: For permissible use audits, DOL already charges for staff time to prepare for, conduct the audit and write the audit report. We are not changing that process.

   For data security audits, currently the recipient pays a third-party entity to conduct the audit. Historically, DOL has not charged for staff time to review the audit. However, with the passage of SSB 5152, RCW 46.22.010 states that the cost of audits will not be the responsibility of DOL. Therefore, we're changing our invoicing process to include DOL's staff time to review the third-party audit.

5. NEW 3/10/22 – Can we get an estimated invoice prior to signing up, as we need to get approval prior for budgeting and asking for money?

   Response: Yes. Please work with the Compliance staff for the estimate.

6. NEW 3/10/22 – Does DOL provide a privacy and security contact so that we can put our IT people in touch with DOL for questions and ensuring our approach will achieve compliance?

   Response: DOL Compliance staff can help you interpret the Privacy requirements. However, they will not provide consulting services or make recommendations on how to comply with the requirements.

7. NEW 3/10/22 – My organization currently receives a file that includes gender and date of birth, but no name or other personal information. Will we be subject to audits in the future?

   Response: Yes. As a result of SSB 5152, we now must protect identity information, such as gender and date of birth, the same as personal information, even though no name is provided in the file. As a result, at minimum we would expect to receive an annual statement of

compliance from you, and at some frequency you would need to have a data security and permissible use audit. We are transitioning to a risk-based audit schedule but have not finalized it. The audit due dates will be outlined in your new contract.

Record Retention / Destruction

1. As a state agency, we have a retention schedule filed with Secretary of State, will this qualify as our retention schedule justification?

   Response: Governmental entities are expected to follow their approved records retention schedules. Please be prepared to share your approved retention schedule if asked by one of our auditors.

2. Can you please clarify why the Federal Credit Reporting Act (FCRA) data retention requirements aren't necessary when other jurisdictions require it?

   Response: The Fair Credit Reporting Act (FCRA) does not appear to have a requirement to retain records for any length of time; rather, there is a disposal requirement that speaks to methods of disposal.

   Under the FCRA, driver records are pulled when assembling a consumer report. If there is a federal requirement to retain the Protected Personal Information for a minimum period, please share the citation.

   If other jurisdictions have laws in effect regarding minimum retention periods, then you should be prepared to provide DOL Compliance Auditors the citations from the various jurisdictions. DOL would expect that only the records pulled in each jurisdiction would be retained in alignment with the law cited.

3. I have kept all driving records that have been ran in a locked file cabinet. Do I need to shred old records? How long can I keep the records for an employee? This is for regular drivers, not commercial drivers.

   Response: You can keep records until the intended use is achieved and there is no legal requirement to retain the Protected Personal Information. If other jurisdictions (i.e., another state) have laws in effect regarding minimum retention periods, then you should be prepared to provide DOL Compliance Auditors the citations from the various jurisdictions.

Research

1. In the WAC draft - Section 7 Research: the language includes "bona fide research organizations" - what makes an organization bona fide? This needs a definition or removal of subjectiveness; I would hate to see true research not performed because a person decides they are not "bona fide". Suggest adding "research organization" to definitions chapter and ditch the "bona fide" language.

   Response: Section 1, *Definitions*, of the draft WAC includes a definition for "bona fide research organizations", stating "Bona fide research organization" means an entity, such as a university, that conducts non-commercial 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." To provide suggested edits to this definition, please submit them to DataContracts@dol.wa.gov.

Subrecipient, Customers, WA Addendum

1. In the draft data sharing template, Section 15, *Subrecipients*, third paragraph are you intending recipients to provide a list of all non-Protected Personal Information customers?

   Response: We only need to know the names of the Customers if the Recipient is processing Protected Personal Information on their behalf.

   By "Customer" we mean those entities that the Recipient is providing services to using data but is not receiving Protected Personal Information. This definition will be added to the WAC.

2. NEW 3/10/22: As we evaluate outsourcing of our call center and print/mail operations we need to fully understand how this might impact the permissible use and subrecipient provisions of our agreement. Specifically, we need to know whether:
   - Allowing an external call center to access WA DOL registered owner / vehicle data within our systems (view only) would require them to be subject to the permissible use/subrecipient requirements of the contract.
   - Using an external print/mail vendor to print/mail citations and notices would require them to be subject to the permissible use/subrecipient requirements of the contract.

   Response: Our proposed definition of "Subrecipient" is any secondary or subsequent entity who receives protected personal information from a recipient or through a chain of entities originating with the recipient. This definition includes all subsidiaries or subcontractors of the recipient who have access to protected personal information. "Subrecipients" also include requesters and agents.

Your question has been helpful as we want to ensure that we're clear about the expectations. The intent is to ensure that Protected Personal Information is protected and used appropriately regardless of who has access to it, or how. Therefore, to answer your questions, yes, even if they access the Protected Personal Information through your system, they are subject to the permissible use and subrecipient requirements. Additionally, for printing/mailing services, these functions are part of the citation notification process and are permissible for that use.

3. NEW 3/10/22 – Flow Down Requirements- the Flow Down Requirements for sub recipients are much more extensive than previously required. We require that our customers have information security programs, privacy requirements, etc.; however, the specifics of the Exhibit A addendum are very extensive and will be more difficult to implement going forward. Additionally, requiring that the addendum be flowed through "verbatim" will be difficult from a commercial perspective. Typically, flow down requirements require that we would have terms substantially similar to those set forth herein, as a number of these requirements set forth in the addendum are already included in our customer agreements. Is there any appetite for changing to that structure here?

   Response: We discovered during audits we conducted over the last few years that we were not clear on our intent to ensure that Protected Personal Information is protected regardless of how many times it is passed on. DOL is trying to clarify its requirements which exist in the current contract templates. The WA Addendum is a tool that Recipient can use to pass on those requirements to Subrecipients. However, the use of the WA Addendum is not required, as long as the Recipient passes on all the pertinent requirements to Subrecipients. The intent is to ensure that Washington residents' information is secured and used properly, no matter who has the data or how many times it has been passed down.

4. NEW 3/10/22 – Exhibit A "Washington Addendum", the requirements seem to assume the subrecipient is a data company. If a user is not in the data business, they are likely not to have the resources to comply with this much of this. An example would be a small auto manufacturer, they are not going to be able to comply with the 6 pages of terms and conditions.

   Response: DOL expects that Protected Personal Information is protected at all levels, regardless of the size of the entity processing the Protected Personal Information. The WA Addendum provides guidance to any entity choosing to process Protected Personal Information (PPI). The focus is on protecting PPI from harm regardless of the type or size of enterprise given no entity is immune from attack. In fact, in 2021, in the example cited in the question, the biggest increase in breaches occurred in manufacturing and utilities, where the number of breaches more than doubled.[1]

[1] Viewed February 7, 2022; https://www.cnet.com/tech/services-and-software/record-number-of-data-breaches-reported-in-2021-new-report-says/#:~:text=According%20to%20the%20Identity%20Theft,of%201%2C506%20set%20in%202017.

In 2021, it was reported that mid-sized businesses were 490% more likely to experience security breach since 2019. It was further reported most mid-sized companies don't invest in security solutions beyond the basics of email phishing and malware — and out of those who do, the vast majority (70%) of deployments are misconfigured, greatly compromising the defense perimeter.[2]

The Coro report, cited in the above article, was based on data from more than 4,000 mid-size companies of between 100 and 1,500 employees operating in the retail, manufacturing, professional services, health care, transportation, and education industries.

Given the vulnerabilities that exist in organizations processing Protected Personal Information, DOL has a responsibility to its residents to ensure that every organization processing Protected Personal Information has necessary protections and policies in place to protect the information from harm. For organizations unable to comply with the requirements in the Addendum, the data sharing agreement allows for Agents, whereby the processing of Protected Personal Information can be performed by entities with the resources available to secure the information to DOL's standards.

5. NEW 3/10/22 – As Eric mentioned in one of the webinars, the term "subrecipient" has been an area of confusion regarding the DSA requirements. Please confirm or clarify expectations around vendors who, for example, provide IT support or manage IT systems that contains protected DOL data. Even though they don't "use" the data per se, but may come in contact with it as they support our IT systems - are they considered a "subrecipient"? If yes, then the expectation is that our vendor contracts with this kind of vendor must include the new Exhibit A terms/conditions - and we must "audit" their compliance. Correct?

   Response: That is correct. The draft WAC defines "Subrecipient" as any secondary or subsequent entity who receives Protected Personal Information from a recipient or through a chain of entities originating with the recipient. This definition includes all subsidiaries or subcontractors of the recipient who have access to protected personal information. "Subrecipients" also include requesters and agents.

   This definition includes any contractor that may have access to the Protected Personal Information, including IT staff, printers, collections agencies, etc.

[2] Viewed February 7, 2022; https://venturebeat.com/2021/11/20/report-mid-sized-businesses-are-490-more-likely-to-experience-security-breach-since-2019/

Specific Contract Template Sections New March 10, 2022

1. NEW 3/10/22 – Section 12, Permissible Use. Unless Recipient has prior written approval from DOL, Data containing Protected Personal Information must not be used to validate the accuracy of data received from other sources. Is the DOL saying that you will not allow use of DPPA 3(A)? The DPPA 3(A) states:

   "For use in the normal course of business by a legitimate business or its agents, employees, or contractors, but only—

   (A) to verify the accuracy of personal information submitted by the individual to the business or its agents, employees, or contractors; and

   (B) if such information as so submitted is not correct or is no longer correct, to obtain the correct information, but only for the purposes of preventing fraud by, pursuing legal remedies against, or recovering on a debt or security interest against, the individual

   Response: As pointed out in the question, you must have prior written permission from DOL before doing so.

   According to the DPPA, "personal information" means information that identifies an individual [emphasis added], including an individual's photograph, social security number, driver identification number, name, address (but not the 5-digit zip code), telephone number, and medical or disability information, but does not include information on vehicular accidents, driving violations, and driver's status.

   A person's identity information is not associated with their vehicle record. Therefore, DPPA 3(A) does not apply to vehicle records.

   However, it is a permissible use for driver data. If DOL does not provide authorization in its contract, and a business needs to verify the accuracy of the personal information given them, they can make a public disclosure request through the NextRequest portal at: https://wadolpublicrecords.nextrequest.com/.

2. NEW 3/10/22 – Section 13, Security Incident / Breach Notification. Recipient must notify DOL within 24 hours of an Incident or Breach discovery, including Incidents and Breaches occurring at a Subrecipient – Our corporate policy states that we will notify within 48 hours of a confirmed breach.

   Response: 48 hours may be a reasonable response; however, we're waiting for all stakeholder input before making any changes. Currently, we require notice within 24 hours from discovery, as RCW 19.255.010 requires that entities notify persons following discovery of the breach. Because DOL licenses the use of its data to Recipients, it must know such events within 24 hours of discovery. This helps us know that an incident has happened, and so we can be involved in the incident response.

3. NEW 3/10/22 – Section 44, Records Access, Inspections and Maintenance. The requirements set forth in this section are extensive and will create administrative burdens. If there is a way to pare this requirement back to the necessary items that would be preferable.

   Response: Washington contracting regulations that both parties keep records of the contract relationship for six years beyond the end of the contract. There has been some confusion in the past about what needs to be retained. This revised clause was an attempt to make clarification. Could you please help us understand the parts you think may be burdensome? Thank you.

4. NEW 3/10/22 – Attachment B, Privacy and Security Requirements. The federal Fair Credit Reporting Act (FCRA) and Driver Privacy Protect Act, and threat of future litigation, are in themselves not a legitimate business purpose for retaining Protected Personal Information after the Permissible Use is fulfilled. The FCRA requires that Datalink as a consumer reporting agency retain the data for a certain period of time. We are obligated as a consumer reporting agency to retain information to comply with our FCRA requirements. Additionally, when the data is used for an insurance use case, insurance carriers may be required under applicable laws to retain information in connection with underwriting.

   Response: Please see the response under the section titled Record Retention / Destruction, question number 2.

Penalties New 3/10/2022

1. NEW 3/10/22 – RCW 46.22.010 allows DOL to assess civil penalties of up to $20,000 per incident. How does DOL administer this statute?

   Response: Since this is a new law, DOL is currently working developing those processes, consistent with other state and federal agencies enforcement of similar statutes or provisions.

Offshoring New 3/10/2022

1. NEW 3/10/22 – Can I offshore Protected Personal Information?

   Response: You must have written permission to offshore Protected Personal Information. All current authorizations will expire with the "death" of the current contracts, and Recipients will need to re-apply for authorization to offshore. Information about how to apply for offshoring authority will be available later this spring.

   Offshoring without prior written DOL authority could result in your access to data being terminated, and civil penalties.