WASHINGTON STATE DEPARTMENT OF LICENSING

Data Management Plan

Use this form to provide the required information needed as part of the procurement process for the Department of Licensing (DOL). The questions below follow the Washington State Agency Privacy Principles and should be completed while viewing DOL Appendix B: Data Stewardship Guidance for Vendors while completing this form. The DOL project lead and the vendor are responsible for the completion of this form.

Questions? Contact datastewards@dol.wa.gov

Title: _____

Creator: _____

Affiliation: _____

Last Modified: _____

Contact Information

This will be the main point of contact who is responsible for the data management.

Name	
Email	10-digit phone number

Data Collection

1. Describe what data is being collected. Describe what operational and analytical needs the data will support. (Why is data collected? When is data collected?)

2. How is the data collected?

3. Who supplies the data?

4. What types of data is collected? (See Data Classification Standard)

☐ Category 1 ☐ Category 2 ☐ Category 3 ☐ Category 4

Continue on next page

5. What categories of data is encrypted at rest and in transit Category 3 and Category 4 data require encryption at rest and transit. (See Encryption Standard).

Documentation and Metadata

1. What documentation will accompany the product?

2. Do you consent to provide the following with your product? (Select all you will share.)
   - ☐ Data dictionary
   - ☐ Metadata schema
   - ☐ Data migration plan including roadmaps or crosswalks
   - ☐ Retirement or retention plan for legacy system
   - ☐ Data flow diagram(s) showing how and where all data is exchanged and stored
   - ☐ Privacy policy
   - ☐ Documentation on “end of life” migration of DOL data back to DOL systems
   - ☐ Data security policy
   - ☐ Data destruction policy / plan
   - ☐ Data incident response / breach plan
   - ☐ Other:

3. Will you provide documentation to our Research and Analytics Office and Data Stewardship Program on data changes (for example: service requests, major upgrades, etc.) when they occur? . . . . . ☐ Yes ☐ No

4. Explain how DOL will be able to fully extract our data from your product during and at the end of our contract. What documentation and support will be provided?

Lawful, Fair, and Responsible Use

1. What data protection and privacy mandates does your product follow?

2. Have you read DOL’s privacy and security requirements?. . . . . ☐ Yes ☐ No

Continue on next page

3. What laws govern your use and processing of DOL data?

4. Who outside your organization has access to or uses the data, and for what purpose?

5. Where will the data be stored, processed, collected, and managed for your primary and backup server? (Specifically include type of servers, name, city and state of secure data center)
   Do not include any information on vulnerabilities to your data security environment on this document.

6. Will you offshore any DOL data while it is stored by your product? . . . . . ☐ Yes ☐ No
   If yes, where:

Due Diligence for Data Partnerships

1. Does your product follow data sharing requirements of the Data Sharing Policy?. . . . . ☐ Yes ☐ No
2. Will you support and cooperate with DOL's compliance and permissible use audit teams, including timely work on corrective action plans if or when deficiencies are found? (These activities are no additional charge to DOL.). . . . . ☐ Yes ☐ No
3. Do you have the resources to conduct an annual self-assessment and submit a statement of compliance to DOL specific to any privacy or security requirements that exist in your contract with DOL? . . . ☐ Yes ☐ No
4. What training does your personnel take on the processing, security, and use of sensitive and confidential data (category 2-4 data)?

5. Will you provide all data-related deliverables in the RFP and contract in a timely manner so we can release funds to pay you as agreed? . . . . . ☐ Yes ☐No

Continue on next page

Open Data, Transparency, and Accountability

1. Can DOL staff obtain a complete version of DOL data—including every business data element, all data related to business activities, and all corresponding metadata—from your product when it reaches production without impacting system's performance? . . . . . ☐ Yes ☐ No
2. Will your product have a separate reporting environment to support analytics? . . . . . ☐ Yes ☐ No
3. If you plan to offer DOL a separate reporting environment, will it be synchronized with production data nightly at minimum? . . . . . ☐ Yes ☐ No
4. If your solution supports APIs, will a complete list of API(s) be shared and kept up-to-date? . . . . . ☐ Yes ☐ No
   ☐ Is the API well-documented?
   ☐ Does it reach across the entire dataset?
   ☐ Is training available for DOL staff?
5. Some part of state data is usually made available to the public, such as the aggregate number of records in a database. Are you able to share or publish these data if we request without custom development or change orders?. . . . . ☐ Yes ☐ No

Data Retention, Storage, and Minimization

1. Describe your product's ability to systematically manage retention and delete data when it has reached its retention period as described in the State Archives' General and Special Retention Schedules and Department of Licensing Records Retention Schedule.
2. Does your product have controls in place to hold data when a litigation hold or public records request occurs? . . . . . ☐ Yes ☐ No
3. Once the retention period is met, is the product able to transfer data to the State Archives?. . . . . ☐ Yes ☐ No

Protect Sensitive Data and Contexts

1. Does your product use biometrics (facial recognition, machine learning, neural networks, or automated decision systems)? . . . . . ☐ Yes ☐ No
   If yes, describe:

Continue on next page

2. Would your product process DOL data with machine learning, artificial intelligence, expert systems, or similar techniques for making or recommending automated decisions? . . . ☐ Yes ☐ No
   If yes, describe:

3. Describe the controls you have in place to protect sensitive and confidential data (category 2, 3, and 4 data).

Data Quality

1. Is your data ISO 8000 compliant? . . . . . ☐ Yes ☐ No
   If yes, describe:

2. Explain how you evaluate data on DOL's data quality dimensions of accuracy, completeness, consistency, lineage, timeliness, uniqueness, portability, and accessibility.

3. Is your product capable of providing data to us in a form we can readily include in a multi-program data warehouse? . . . . . ☐ Yes ☐ No

Data Security

1. How will you manage access and security of DOL data?

2. Will you be willing to work with our information security team on a security design review until the system is live and fully stabilized? . . . . . ☐ Yes ☐ No

Continue on next page

3. What are your security standards and certifications?

4. Will you keep these certifications current throughout our working relationship? . . . . . ☐ Yes ☐ No

5. Will you use secure protocols to communicate with us? . . . . . ☐ Yes ☐ No

6. Will you inform us within 24 hours of discovery of any data breach or data incident? . . . . . ☐ Yes ☐ No

7. If your product collects or stores Protected Personal Information from DOL, will your product carry the required level of cyber liability insurance? . . . . . ☐ Yes ☐ No

8. Explain how you can restrict access to, and security protocols around, sharing data.

Continue on next page

Definitions

biometric
Data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual. "Biometric identifier" does not include a physical or digital photograph, video or audio recording or data generated therefrom, or information collected, used, or stored for health care treatment, payment, or operations under the federal health insurance portability and accountability act of 1996.

breach
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.

category 1 - public information
Information the Agency can release - or currently releases - to the public. It does not need protection from unauthorized disclosure, but does need integrity and availability protection controls.

category 2 – sensitive information
Information the Agency doesn't generally release to the public unless specifically requested and allowable by law.

category 3 - confidential information
Information specifically protected from disclosure by law. This may include: a) Personal information. b) Information concerning Employee personnel records. c) Information regarding Information Technology infrastructure and security of computer and telecommunication systems. This category of data is also known as 'Personally Identifiable Information (PII)' and/or 'Personal Information'.

category 4 – confidential information requiring special handling
Confidential information requiring special handling is information that is specifically protected from disclosure by law and with: a) Especially strict handling requirements are dictated by statutes, regulations, or agreements. b) Serious consequences that can arise from unauthorized disclosure, such as threats to health and safety, or legal sanctions.

data management plan
A data management plan (DMP) is a written document that describes how data will be managed at each stage of a data lifecycle. DMPs support DOL's strategic plan goal of safer data. DMPs are created by data producers and product vendors, with consultation of data stewards.

offshore (data)
The electronic or hard copy transmission, accessing, viewing, capturing images, storage, or processing of protected personal information outside the United States.

protected personal information (PPI)
Protected personal information means collectively Personal Information and Identity Information, as defined by RCWs 46.04.209, 19.255.005 and 42.56.590, authorized for disclosure by the federal Driver Privacy Protection Act and state law.

sensitive and confidential information (category 2, 3, and 4)
Defined in the DOL Classification and Handling Standards.

security incident
Any unplanned or suspected event that could pose a threat to the integrity, availability or confidentiality of the Agency's, or the State's, data, or systems.

Additional Resources

- Data Management Plans for Washington State Government Agencies