



2019 Privacy Impact Assessment

Transportation Regulation Improvement Project

Finance and Administrative Services Department



Contents

| | |
|--|-----------|
| Privacy Impact Assessment Overview | 1 |
| What is a privacy impact assessment? | 1 |
| When is a privacy impact assessment required? | 1 |
| How to complete this document? | 1 |
| 1.0 Abstract | 2 |
| 2.0 Project / Technology Overview | 3 |
| 3.0 Use Governance | 4 |
| 4.0 Data Collection and Use..... | 5 |
| 5.0 Data Storage, Retention and Deletion..... | 8 |
| 6.0 Data Sharing and Accuracy | 9 |
| 7.0 Legal Obligations, Risks and Compliance | 11 |
| 8.0 Monitoring and Enforcement..... | 13 |

Privacy Impact Assessment Overview

What is a privacy impact assessment?

A Privacy Impact Assessment (“PIA”) is a method for collecting and documenting detailed information collected in order to conduct an in-depth privacy review of a program or project. It asks questions about the collection, use, sharing, security and access controls for data that is gathered using a technology or program. It also requests information about policies, training and documentation that govern use of the technology. The PIA responses are used to determine privacy risks associated with a project and mitigations that may reduce some or all of those risks. In the interests of transparency about data collection and management, the City of Seattle has committed to publishing all PIAs on an outward facing website for public access.

When is a privacy impact assessment required?

A PIA may be required in two circumstances.

- The first is when a project, technology, or other review has been flagged as having a high privacy risk.
- The second is when a technology is required to complete the Surveillance Impact Report process. This is one deliverable that comprises the report.

How to complete this document?

As department staff complete the document, they should keep the following in mind.

- Responses to questions should be in the text or check boxes only, all other information (questions, descriptions, etc.) should **NOT** be edited by the department staff completing this document.
- All content in this report will be available externally to the public. With this in mind, avoid using acronyms, slang, or other terms which may not be well-known to external audiences. Additionally, responses should be written using principally non-technical language to ensure they are accessible to audiences unfamiliar with the topic.

1.0 Abstract

1.1 Please provide a brief description (one paragraph) of the purpose and proposed use of the project/technology.

The Integrated Code Management System (ICMS) project will implement a system within the Accela enterprise platform to improve administration of programs in the Regulatory Compliance and Consumer Protection (RCCP) division of FAS. ICMS will serve as a single platform for regulatory information and activities including license applications/renewals, invoicing, fee collection, inspections, code enforcement and case management. Phase 1 will build the system foundation and implement the for-hire regulatory program (taxi, flat rate for-hire vehicles, and transportation network companies) and is collaborative effort with King County Records and Licensing Services (RALS) division. The first phase is referred to as the Transportation Regulation Improvement Project (TRIP).

1.2 Explain the reason the project/technology is being created or updated and why the PIA is required.

ICMS is a critical technological update to aging systems, creating a single platform for regulatory information and activities including license applications/renewals, invoicing, fee collection, inspections, code enforcement and case management. ICMS will improve administration of regulatory programs and will include collection and storage of personal information associated with regulatory licensing and case management.

2.0 Project / Technology Overview

Provide an overview of the project or technology. The overview gives the context and background necessary to understand the purpose, mission and justification for the project / technology proposed

2.1 Describe the benefits of the project/technology.

The project is replacing multiple legacy systems built on platforms that are no longer supported. The new system will create efficiencies for regulatory administration and compliance processes for for-hire transportation vehicles, drivers, and companies, leveraging the partnership between King County and City of Seattle to streamline business processes. Additionally, ICMS will provide access to real-time data in the field, automate routine processing and verifications, provide online applications and payments for customers, and provide improved data analytics and performance metrics.

2.2 Provide any data or research demonstrating anticipated benefits.

A public survey was conducted in 2017 to gather input from customers regarding how for-hire regulatory processes could be made easier. Responses from the survey indicated a preference to submit applications and make payments on a computer or smartphone and receive regulatory information via email or text messages. ICMS will transition many paper based and in-person processes to digital workflows.

The survey results were posted on both the King County and Seattle.gov website.

2.3 Describe the technology involved.

ICMS will be built within the existing Accela enterprise platform on the city's network.

2.3 Describe how the project or use of technology relates to the department's mission.

This project is part of the citywide permit system integration initiative and supports the Mayor's IT Subcabinet priorities of Public Experience and Service and System Maturity. It also supports FAS priorities of providing excellent customer service, increasing operational efficiency, and reducing risk.

2.6 Who will be involved with the deployment and use of the project / technology?

The system will be developed and deployed with involvement by a third-party system integrator, Avocette, the city's RCCP division in FAS, the RALS division of King County, and the Seattle Information Technology Department. The technology will be used by RCCP and RALS staff and regulatory customers.

3.0 Use Governance

Provide an outline of any rules that will govern the use of the project / technology. Please note: non-City entities are bound by restrictions specified in the Surveillance Ordinance and Privacy Principles and must provide written procedures for how the entity will comply with any restrictions identified.

3.1 Describe the processes that are required prior to each use, or access to/ of the project / technology, such as a notification, or check-in, check-out of equipment.

All internal and public users will be required to have a username and secure password that will be used to log in to the system for each use. Public users are notified of public disclosure requirements and the city's privacy principles, statement and policy and are required to accept the terms prior to creating an online account.

3.2 List the legal standards or conditions, if any, that must be met before the project / technology is used.

The following laws have impacted the design and data collected through ICMS. Additionally, the City's and County's policies as Sanctuary Cities were central to the design and planning, prior to implementing this technology.

[SMC 6.310.200](#): Taxicab association license application

[SMC 6.310.260](#): TNC license eligibility and application

[SMC 6.310.265](#): TNC standards for license application or renewal denial

[SMC 6.310.300](#): Taxicab and for-hire vehicle license application

[SMC 6.310.327](#): TNC vehicle endorsement eligibility and application

[SMC 6.310.405](#): Criminal background check

[SMC 6.310.410](#): For-hire driver's license application

[SMC 6.310.410](#): For-hire driver certification of fitness to drive

[King County Ordinance 18665](#)

[King County Code 6.64.510](#)

3.3 Describe the policies and training required of all personnel operating the project / technology, and who has access to ensure compliance with use and management policies.

System training, including use and security, will be provided and required for all end users prior to implementation. Attendance in training will be documented. Supervisors and managers will have appropriate security permissions to report on and monitor staff usage of the system. System training content will be primarily developed by the system integrator, Avocette, and content regarding use and management of the data will be developed in partnership with Seattle IT and business management staff. Staff supervisors will maintain training attendance records.

4.0 Data Collection and Use

Provide information about the policies and practices around the collection and use of the data collected.

4.1 Provide details about what information is being collected from sources other than an individual, including other IT systems, systems of record, commercial data aggregators, publicly available data and/or other city departments.

The Seattle License Information Management system (SLIM) will be used to verify business license numbers and expiration date (provided by customer).

The American Association of Motor Vehicle Administrators service will be used to verify Driver's License numbers and expiration dates provided by customers.

The Washington State Department of Licensing Vehicle Information Database will be used to verify vehicle plate numbers and registration provided by customer.

The city's Vehicle inspection database (VSID) will be used to access and import vehicle inspection results.

[ProProfs](#) will be used to access and import training and testing results.

[SafeScreener](#) will be used to access driving record and background check results.

Motorola will be used to import customer complaints.

4.2 What measures are in place to minimize inadvertent or improper collection of data?

System interfaces will be built to either verify or import only the data needed to support licensing/permitting requirements. The data elements collected were reviewed by King County and City stakeholders, including Law and the Privacy Office. Additional data will be not accessible.

4.3 How and when will the project / technology be deployed or used? By whom? Who will determine when the project / technology is deployed and used?

The first release of the project is scheduled to go live in August 2018 and a second release is scheduled in the first quarter of 2019. The system and will be deployed and supported by the Seattle Information Technology department. It will be used by RCCP and King County staff to administer and enforce compliance within the for-hire regulatory program.

4.4 How often will the technology be in operation?

The technology will be in operation seven days a week, twenty-four hours a day, excluding maintenance windows.

4.5 What is the permanence of the installation? Is it installed permanently or temporarily?

This is a permanent installation.

4.6 Is a physical object collecting data or images, visible to the public? What are the markings to indicate that it is in use? What signage is used to determine department ownership and contact information?

Not applicable.

4.7 How will data that is collected be accessed and by whom?

Data will be accessed within the system by regulatory staff (director, managers, supervisors, strategic advisors, customer service representatives, cashiers, inspectors, accounting analysts) who are involved in business processes that utilize collected data, e.g. approving and issuing licenses, scheduling and resulting inspections, conducting field inspections and enforcement. Security roles and permissions will be built into the system to limit access to sensitive data. FAS and King County (the business) determine who has what access to the system. The parties that authorize access are specified in the Accela PL-2 Security Plan.

Selected sections of the Accela PL-2 Security Plan:

Internal Users: Since users authenticate with Active Directory (AD) the AD rules and policies around credential renewal and password updates are controlled by the AD settings. Decisions on access revoking and deleting credentials come from the business or HR in the case of departing employees. If a person's AD account is disabled, they would not be able to authenticate, and this would prevent them from accessing Accela.

External Users: To ensure user privacy, Accela provides a mechanism that prevents external users from accessing data and records until the user identification is verified with government identification. Once this has been completed, the user may not be added to another account or have records claimed by other users. After this verification is complete, a user may be matched to their historical records within the system.

4.8 If operated or used by another entity on behalf of the City, provide details about access, and applicable protocols. Please link memorandums of agreement, contracts, etc. that are applicable.

King County regulatory staff will be remotely accessing the system and using it for daily operations. Users will be required to comply with the City's acceptable use agreement. County staff will be provided AD accounts and will access the system within the city's network via a Virtual Private Network (VPN) connection.

4.9 What are acceptable reasons for access to the equipment and/or data collected?

As noted in section 4.7, access to data within the system will be given to regulatory staff (director, managers, supervisors, strategic advisors, customer service representatives, cashiers, inspectors, accounting analysts) who are directly involved in business processes that utilize the collected data. This may include workflow processing, administration, enforcement, or performance metrics/reporting. User groups within the system are anticipated to include the following (additional roles may be created to provide additional security for specific functions):

| User Role | Description | Criteria for Access |
|--------------|--|--|
| Admin | Staff with administrative rights to configure the software and manage user roles in the system | Must be an IT staff member with advanced system training |
| Supervisor | Staff who manage/supervise staff who perform daily work in Accela; can provide approvals, allow exceptions to rules, and have access to management metrics and reporting | Must be a RCCP or RALS staff member in a supervisory or management role |
| Super User | Person working in the back office with ability to make minor, limited configuration changes and create ad-hoc reports | Must be a RCCP or RALS staff member with advanced system training |
| General User | Typical person working in the back office or customer service role | Must be a RCCP or RALS staff member |
| Payment | Internal staff performing payment functions | Must be a city or county staff member who is responsible for processing payments |
| Read Only | Person who can view, but not edit any data | Must be a city or county staff member with demonstrated business need to view data |
| Public User | Person with customer portal account who can apply, make payments and view account information online | Must create a secure account with a unique username and email address |

4.10 What safeguards are in place, for protecting data from unauthorized access (encryption, access control mechanisms, etc.) and to provide an audit trail (viewer logging, modification logging, etc.)?

Access to the system will require a secure username and password. Sensitive data will only be accessible for specific user roles and user activities within the system will be logged and accessible via audit reports. Accela has system activity audit logs that are accessible by ITD system admin staff.

5.0 Data Storage, Retention and Deletion

5.1 How will data be securely stored?

The data will be stored within the Accela enterprise database that is hosted on the city's network. Documents will be stored in the Oracle document management system on the city's network, which is integrated with Accela.

5.2 How will the owner allow for departmental and other entities, to audit for compliance with legal deletion requirements?

Record retention reports will be available to monitor and audit data retention requirements. Deletion is not automated within the system; however, purging tools can be used to delete identified data. The record retention period for regulatory license and violations is 6 years:
<http://inweb/clerk/RecordsManagement/images/DEA-RevenueandConsumerAffairs.pdf>

5.3 What measures will be used to destroy improperly collected data?

Improperly collected data will be purged within the system and database. This can be done using purging tools within the system.

5.4 Which specific departmental unit or individual is responsible for ensuring compliance with data retention requirements?

The RCCP division in FAS is responsible for compliance with data retention. An Admin Support Analyst is currently responsible for this body of work.

6.0 Data Sharing and Accuracy

6.1 Which entity or entities inside and external to the City will be data sharing partners?

Data will be shared with King County Regulatory and Licensing Services (RALS) division.

6.2 Why is data sharing necessary?

The City of Seattle and King County have a cooperative agreement to jointly regulate for-hire drivers and vehicles within the two jurisdictions. This requires that data be shared between agencies to properly license and enforce code requirements.

6.3 Are there any restrictions on non-City data use?

Yes No

6.3.1 If you answered Yes, provide a copy of the department's procedures and policies for ensuring compliance with these restrictions.

Data sharing is restricted to use by King County for the purpose of licensing and code enforcement activities for the for-hire regulatory program. Policies regarding access and use of data are outlined in the operations and maintenance agreement between the City and County.

6.4 How does the project/technology review and approve information sharing agreements, memorandums of understanding, new uses of the information, new access to the system by organizations within City of Seattle and outside agencies?

MOUs, MOAs and/or data sharing agreements are reviewed and by IT management, business management, legal, and contracting and are approved/signed by Department Directors. King County is the only agency outside of the City of Seattle expected to have access to the system and data.

6.4.1 Please describe the process for reviewing and updating data sharing agreements.

A data sharing agreement and operations and maintenance MOU will be established between the City of Seattle and King County for shared use of ICMS. If there is any change in the data being collected and stored in the system, these agreements will be reviewed and updated as deemed necessary.

6.5 Explain how the project/technology checks the accuracy of the information collected. If accuracy is not checked, please explain why.

A majority of the data collected (e.g. driver's license information, vehicle plate and VIN) is verified by system integration with approved third-party providers. Additional audits/accuracy checks may be conducted by back-office regulatory staff through reporting or manual review.

External public users (through the services portal) and internal staff create records in Accela, which is a web application. Accela provides amendment functionality for changes to records by both staff and external users. All record changes are tracked within the system.

6.6 Describe any procedures that allow individuals to access their information and correct inaccurate or erroneous information.

Customers can access account information through the secure [Seattle Services Portal](#) and submit corrections and/or changes for some information online, e.g. contact information. Corrections to submitted applications may also be available online by submitting a change request.

If the information is not available for editing online or if customers prefer not to make changes online, customers can go to the Regulatory Compliance and Consumer Protection customer service office at the Seattle Municipal Tower, 700 Fifth Ave, Floor 42, to have corrections processed.

7.0 Legal Obligations, Risks and Compliance

7.1 What specific legal authorities and/or agreements permit and define the collection of information by the project/technology?

[SMC 6.310.200](#): Taxicab association license application
[SMC 6.310.260](#): TNC license eligibility and application
[SMC 6.310.265](#): TNC standards for license application or renewal denial
[SMC 6.310.300](#): Taxicab and for-hire vehicle license application
[SMC 6.310.327](#): TNC vehicle endorsement eligibility and application
[SMC 6.310.405](#): Criminal background check
[SMC 6.310.410](#): For-hire driver's license application
[SMC 6.310.410](#): For-hire driver certification of fitness to drive
[King County Ordinance 18665](#)
[King County Code 6.64.510](#)

7.2 Describe what privacy training is provided to users either generally or specifically relevant to the project/technology.

All internal users have or will take the City of Seattle privacy training prior to using the system. Privacy/security training specific to the project and data collected will be included in system end user training.

7.3 Given the specific data elements collected, describe the privacy risks identified and for each risk, explain how it was mitigated. Specific risks may be inherent in the sources or methods of collection, or the quality or quantity of information included.

The Privacy Office identified this project as having a high risk because it requires collecting sensitive data from vulnerable populations that will be subject to public disclosure. This project also has special consideration because of the need to balance safety and business requirements with privacy considerations. The Code requires specific data collection from for-hire drivers, a job which is often filled by immigrant labor. Some of the required fields may be used as proxies to identify individuals close to undocumented immigrants (place of birth, language, etc.). An immigrant's address and other personal identifiers are, as the City has experienced first-hand, a tool ICE uses when it has identified an undocumented individual to arrest. However, a driver's contact information is a basic data requirement to administer for-hire driver regulations.

The project team worked with FAS staff, King County staff, King County Law, City Attorney's Office and Privacy Office to reach a data minimization strategy, removing place of birth and language data fields. (Note: language may still be requested in the event that the City must secure a translator any Court proceedings.) Additionally, the collection of background information and images, particularly related to driver's licenses has been minimized so that compliance workers may ensure safe streets, but the City does not directly store the most sensitive data.

7.4 Is there any aspect of the project/technology that might cause concern by giving the appearance to the public of privacy intrusion or misuse of personal information?

Given the recent publicity surrounding the Washington State Department of Licensing sharing information with ICE, there may be some concern around how this data may impact immigrant communities or undocumented workers. However, the mitigations described in 7.3 were designed to address this risk.

8.0 Monitoring and Enforcement

8.1 Describe how the project/technology maintains a record of any disclosures outside of the department.

Public Records Act disclosures are tracked within GovQA, the City's tool for handling public records requests. Any other data extracts would be tracked through Accela audit tools and Outlook records.

8.2 What auditing measures are in place to safeguard the information, and policies that pertain to them, as well as who has access to the audit data? Explain whether the project/technology conducts self-audits, third party audits or reviews.

Logging of all user activity within the system, auditing reports, and self-audits will be performed. See 4.10 for more information. Beyond any audits that may be required by Council or the Mayor's Office, there is an annual Payment Card Industry Data Security Standards (PCI DSS) audit.

The technology will not complete any other self-audits, but all information will be subject to the [Public Records Act RCW 42.56](#).