2019 Privacy Impact Assessment

Democracy Voucher Portal

Seattle Ethics and Elections Commission

April 2019

Seattle
Information Technology

Contents

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 PIA 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.

Set to launch Q1 2019, each participant using the Democracy Voucher platform will have the ability to access their unassigned vouchers through a website portal in addition to paper vouchers which will be mailed out on that date. Participants will verify their registration status against King County Elections/Seattle Ethics and Election Committee (SEEC) registration data, leveraging a third-party tool that's able to integrate with the website portal. The website portal will leverage the Microsoft Dynamics 365 platform. Participants can then assign one, two, three or 4 vouchers (valued at $25 each) to qualified candidate(s) of their choice. Once the voucher is assigned and validated, the value will be released to the campaign through business and electronic processes implemented in Phase I. Leveraging the Portal capabilities of Dynamics 365 will give voucher holders the ability to exercise their vouchers online instead of mailing paper vouchers. In implementing this solution, the project will upgrade SEEC's instance of Microsoft Dynamics from version 8.2 to version 9.x across all environments there (Development, Test and Production).

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

This project was initiated by Seattle voters approving Initiative 122 in which several campaign finance reforms were enacted. The most significant reform enabled a "voucher" program providing public financing of campaigns for qualified candidates seeking the Office of Mayor, City Attorney, or City Council. As part of this mandate, an online portal is required to establish a web-based means of voucher allocation which residents may choose over the mail-in, paper voucher format.

This project has been flagged as high privacy risk due to the information collected and required for verification.

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.

This project allows Seattle residents to allocate their Democracy Vouchers using an online web site ("portal") instead of mail in paper vouchers, potentially saving time and money for those wanting to participate.

2.2 Provide any data or research demonstrating anticipated benefits.

This is one of the first initiatives of its kind, and therefore no research on anticipated benefits exists.

2.3 Describe the technology involved.

Democracy Vouchers is built on the Microsoft Dynamics (D365) platform. This project adds Dynamics Portal functionality to the existing instance of Microsoft Dynamics in the Ethics and Elections environment. This additional Portal functionality has been augmented to include identity verification (of Seattle residents) through an API created by Trulioo, a third-party Identity Verification provider. When a resident creates an account within Portal, they submit their year of birth and the last four digits of their SSN; neither of which are accessible, visible nor stored by COS systems or personnel. Through the API, these are matched against databases on the Trulioo side; databases containing credit, banking and other similar information. Once their identity is successfully verified, a message returns to the Portal session essentially denoting a "match" or "no match" response. If the resident supplied information results in a "match", the resident can continue and allocate up to four vouchers (each $25 in public fund value) to one or more candidates of their choosing. Alternatively, if a "no match" message is returned, the resident is presented a different screen informing them to contact SEEC offices for assistance. The vendor for Microsoft Dynamics is Power Objects.

The contracts between the City of Seattle and both Power Objects and Trulioo can be found below.

PowerObjects
C3-0294-18 SIGNED.

Trulioo_End-User_Li
cense_Agreement_C

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

This question is not applicable as this body of work was mandated by Initiative-222.

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

Seattle IT's Project Management Office (PMO), Seattle Ethics and Elections, in addition to the vendor teams listed above, are involved in the deployment and use of the project and technology. Additionally, Seattle IT's Dynamics team will provide ongoing maintenance and support for the platform. The portal is intended for use by eligible Seattle residents.

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.

The outputs of the project, particularly how any resident chooses to allocate their vouchers, is information that is shared publicly. Residents are notified of this on the mailings they receive, on SEEC's seattle.gov pages, and most recently made more prominent on the voucher allocation portal landing page as well. No other personal information is being collected that isn't already publicly available via King County election data. On the landing page of the DV portal appears the language: "Are Democracy Vouchers public information? Yes, as with all donations to candidate campaigns, voucher assignments are public information."

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

This question is not applicable.

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.

The Seattle Ethics and Elections Committee (EEC) personnel have been trained to use the Dynamics platform. Knowledge transfer and code review sessions scheduled between vendor and COS IT teams to ensure the proper operations and maintenance of the platform once the vendor team leaves.

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.

As the basis for the platform, SEEC uses a file of Seattle voter data provided by King County. Seattle residents validate their identity by entering their birth year and the last four digits of their social security number. This, along with address and name fields from King County elections data, are compared against credit, banking and other similar databases at Trulioo via their API. Once verified, the user has the ability to use the online portal. At this point, an email address is added to their entry in the platform, in addition to the encrypted user-generated password for the portal.

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

ID verification is performed using the Trulioo API, the data within it being encrypted. Only a “match” or “no match” response is returned and stored within EEC CRM. Once created by the resident, their password, is also encrypted and stored in the CRM so that City of Seattle personnel are never able to access or decipher them.

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 Democracy Vouchers Portal will be used by Seattle residents with every local election cycle beginning March, 2019. Once an election ends the Portal will be shut down and no longer accessible. Approximately every two years the Portal will be stood back up to reflect the latest election information input into Dynamics at SEEC.

4.4 How often will the technology be in operation?

TheDemocracy Voucher Portal will be in operation continually (24/7/365). The portal will only be available for use approximately 8-9 months prior to local elections.

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

This will be installed permanently; the Portal will be available temporarily and re-deployed as outlined in 4.4 above.

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?

The use of the Democracy Vouchers Portal is voluntary, that requires the member of the public to volunteer the data entered into the system. Additionally, the portal is branded to be similar to Seattle.gov pages, especially those of EEC.

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

The data collected will be accessible via a web interface into Dynamics 365 platform by EEC personnel. The Seattle IT Dynamics support team may also have ancillary access to the data for the purpose of supporting and maintaining the platform.

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.

This technology is not used by an outside entity on behalf of the City. The vendor, Power Objects, had access to the system during building and testing phases of the project.

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

The data collected will be used to determine, and report on, how residents allocate vouchers as well as for determining how to allocate public funds to various candidates and campaigns.

Seattle IT may have access to data, by way of supporting and maintaining the system.

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.)?

Encryption is used both with the data used for ID verification via the Trulioo API (encrypted in transit), as well as for the user-generated password that is created by the resident in order to access the portal (at rest).

5.0 Data Storage, Retention and Deletion

5.1 How will data be securely stored?

The data will be stored in Microsoft’s enterprise grade, public-cloud (Azure)-based Dynamics365 environment.

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

Not included in project scope, however, the City Auditor may audit for compliance as appropriate.

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

This question is not applicable.

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

Seattle Ethics and Elections is responsible for ensuring compliance with data retention requirements as follows (as provided to the project by City Records Management Program): All the data in CRM can be put in a .csv file and put on either a CD or DVD which can be stored in a warehouse with applicable forms being filled out. The information needs to be kept 6 years after the termination of the funding program levy (6 years after the 10 years of funding = 16 years). We are currently storing the data in a SQL server residing in the Western Data Center that is regularly backed up for redundancy and disaster recovery.

6.0 Data Sharing and Accuracy

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

The City of Seattle will receive data from King County Elections. Residents will provide their year of birth and last four digits of their SSN as part of ID verification process, but the City of Seattle will not have the ability to collect, store or share resident year of birth or last four SSN digits. The campaigns to which vouchers are allocated, and by whom, will be published and shared as required by municipal code. All King County Election data is already publicly accessible and includes the following fields:
VoterID StatusCode FirstName MiddleName LastName NameSuffix
HouseNumber PreDirection StreetName StreetSuffix PostDirection UnitNumber
ResidenceState ResidenceCity ResidenceZipCode PrecinctID PrecinctPortion
PrecinctName RegistrationDate Gender BirthDate MailAddress1
MailAddress2 MailAddress3 MailAddress4 StateVoterID DistrictName_1
DistrictName_2 DistrictName_3 DistrictName_4.

6.2 Why is data sharing necessary?

The City of Seattle will not have any data sharing partners outside of the initiative requirement of making voucher allocation information publicly available.

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.

This question is not applicable.

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?

This question is not applicable.

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

King County election data is assumed to be accurate, therefore, no validation is performed or deemed necessary. All other information (voucher allocation and email addresses) is assumed to be accurate as provided as well.

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

Residents can change their self-provided email addresses through the portal. At the time of voucher allocation, residents need to complete a multi-step process in the portal to finalize their voucher submission. That is they need to both select the candidate for each voucher allocation and then confirm it through a two-step process before that allocation is finalized.

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?

This project was initiated by the passing of Initiative I-222. While I-222 does not specifically define the data collection requirements, the information collected is required to execute and implement the project in full. Per Initiative I-222, the allocation of residents' vouchers is required to be public.

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

City of Seattle employees are required to take the annual Privacy and Security Awareness 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.

As only email address is being collected, there are no identified risks and associated mitigations.

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?

People may be concerned that their voucher allocation is public. This is mitigated by providing notification regarding the public nature of a person's voucher allocation in multiple locations on the portal as well as in print materials and on the external Democracy Voucher site.

8.0 Monitoring and Enforcement

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

An archive of previous election cycle CRM databases is created and housed on a server within the Western Data Center. Gov QA is the City's public disclosure request tool that maintains records and tracks the process related to Public Disclosure Requests.

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.

The City Auditor may audit for compliance as appropriate.