POWERFUL TECHNOLOGY SOLUTIONS
FOR THE CITY AND PUBLIC WE SERVE

City of Seattle Privacy Impact Assessment

ONLINE MONTHLY PARKING SALES PROJECT

Owner: Seattle Center

Date: 1/1/2017

12.7.2017

Seattle
Information Technology

CONTENTS

PURPOSE OF PIA

A Privacy Impact Assessment is designed to outline the anticipated privacy impacts from a City project/program or project/program update that collects, manages, retains or shares personal information from the public. The PIA will provide project/program details that will be used to determine how privacy impacts may be mitigated or reduced in accordance with the City of Seattle Privacy Principles and Privacy Statement.

ABSTRACT

Please provide a brief abstract. *The abstract is the single paragraph that will be used to describe the project and* ***will be published on the Privacy Program website.*** *It should be a minimum of three sentences and a maximum of four, and use the following format:*

- *The first sentence should include the name of the project, technology, pilot, or project/program (hereinafter referred to as "project/program").*
- *The second sentence should be a brief description of the project/program and its function.*
- *The third sentence should explain the reason the project/program is being created or updated and why the PIA is required. This sentence should include the reasons that caused the project/program to be identified as a "privacy sensitive system" in the Privacy Intake Form, such as the project/program requiring personal information, or the technology being considered privacy sensitive.*

The Online Monthly Parking Sales project will implement Software as a Service solution called PermitPoint by Omni Park, Inc. This system will provide online payment and service to Seattle Center's monthly parking customers. This project was created to fill a functional gap with existing Amano McGann Parking Management System. A PIA is required because the system will require customers to provide personal and credit card information for payment processing.

PROJECT/PROGRAM OVERVIEW

Please provide an overview of the project/program. *The overview provides the context and background necessary to understand the project/program's purpose and mission and the justification for operating a privacy sensitive project/program. Include the following:*

- *Describe the purpose of the system, technology, pilot or project/program; the name of the department that owns or is funding the project/program and how it the project/program relates to the department's mission;*
- *Describe how the project/program collects and uses personal information, including a typical transaction that details the life cycle from collection to disposal of the information;*
- *Describe any routine information sharing conducted by the project/program both within City of Seattle departments and with external partners. Describe how such external sharing is designed with the original collection of the information.*
- *Identify any major potential privacy risks identified and briefly discuss overall privacy impact of the project/program on individuals*

- *Identify the technology used and provide a brief description of how it collects information for the project/program.*

The project will provide an online, 24/7 payment system and service to Seattle Center's monthly parking customers by successfully implementing PermitPoint by Omni Park. With this system, customers can take advantage of online payment, but will also have the option to automatically renew, pay in advance, change subscription type, and receive automated email reminders/notifications. This new online payment offering will align Seattle Center with current technology, provide a competitive advantage, and an opportunity to increase monthly parking revenue.

The existing Amano McGann Parking Management System online payment module has limited functionality and requires a high cost of initial investment. The business opportunity is to find a viable online payment system using Software as a Service technology to fill the existing gap while meeting PCI compliance requirements. Replacing the entire Amano McGann Parking Management System is not an option.

The system will have a customer account profile information utilizing their name, address, email, password, and credit card information. The information is saved within the system due to recurring monthly transactions with the option to auto-renew. Customer data is retained as long as the customer's account is active. The saved credit card information can be deleted by the customer at any time. Payment transactions are retained for 7 years per the City's Records Retention Policy.

No information will be shared outside of Seattle Center Parking and Finance Units, and any information shared is directly related to payment reconciliation purposes.

The potential privacy risk exists like any other e-commerce solutions accessible on the Internet; in the event of a system hack, customer personal identifiable information could be at risk -- although the data is encrypted. This project requires that the system go through annual security penetration testing by a third-party provider, and PCI compliance must be maintained.

NOTIFICATION

1. ***How does the project/program provide notice about the information that is being collected?*** *Our Privacy Principles and Statement require that we provide notice to the public when we collect personal information, whenever possible.*
   - *Describe how notice will be provided to the individuals whose information is collected by this project/program and how it is adequate.*
   - *If notice is not provided, explain why not. (For certain law enforcement or other project/programs, notice may not be appropriate.)*
   - *Discuss how the notice provided corresponds to the purpose of the project/program and the stated uses of the information collected.*

   The system requires that the customer accept a use-agreement which will include a statement regarding the use of the information collected; in this case, customer information will be used solely for processing monthly parking payment. Additionally, the system requires customer acknowledgement and acceptance of the user-agreement prior to entering credit card information.

2. ***What opportunities are available for individuals to consent to the use of their information, decline to provide information, or opt out of the project/program?*** *Describe how an individual may provide*

consent for specific uses or whether consent is given to cover all uses (current or potential) of his/her information. If specific consent is permitted or required, how does the individual consent to each use? If notice is provided explain how an individual may exercise the right to consent to particular uses or decline to provide information describe the process. If this is not an option, explain why not. Note: An example of a reason to not provide an opt-out would be that the data is encrypted and therefore unlikely available to identify an individual in the event of a data breach.

Per notification stated previously, acceptance of the use-agreement covers all future use of the system. The customer has opportunity not to accept use- agreement and may decline to participate. A second opportunity is provided prior to entering credit card information and consent is required each time credit card information is entered. The customer may delete stored credit card information on their account profile after each payment is successfully processed.

COLLECTION

3. ***Identify the information, including personal information, that the project/program collects, uses, disseminates, or maintains.*** *Explain how the data collection ties with the purpose of the underlying mission of the department.*

   The system collects only information required to process credit card payments: billing name, address, telephone, and email. Payment transaction logs are maintained for financial and parking operation data reconciliation purposes only. No dissemination of data will be provided outside of Seattle Center Parking and Fiscal Services operational needs

4. ***Is information being collected from sources other than an individual, including other IT systems, systems of records, commercial data aggregators, publicly available data and/or other departments?*** *State the source(s) and explain why information from sources other than the individual is required.*

   The customer name, with an assigned electronic access card number will be manually reconciled monthly between the Amano McGann Parking Management System and the proposed PermitPoint system.

USE

5. ***Describe how and why the project/program uses the information that is collected****. List each use (internal and external to the department) of the information collected or maintained. Provide a detailed response that states how and why the different data elements will be used.*

   Information collected is for Seattle Center internal use only; a payment transaction report will be generated for manual reconciliation with Amano McGann Parking System so that the customer will have access to the parking facility in the future.

6. ***Does the project/program use technology to:***
   a. ***Conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly or***

b. ***Create new information such as a score, analysis, or report?***

If so, state how the City of Seattle plans to use such results. Some project/programs perform complex analytical tasks resulting in other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Explain what will be done with the newly derived information. Will the results be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data?

The project does not use technology for either example A or B.

7. ***How does the project/program ensure appropriate use of the information that is collected?*** *Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above.*

   All parking staff are required to take PCI Awareness Training that covers credit card data security standards. Existing compliance procedures are in place and will be updated in accordance with the requirements of the new system. System security is role and permission based, and will be assigned appropriately within the bounds of each employee's work responsibilities.

RETENTION

8. ***Does the project/program follow the City records retention standard for the information it collects?*** *Departments are responsible for ensuring information collected is only retained for the period required by law. City departments are further responsible for reviewing and auditing their compliance with this process. For more information, please see the internal retention schedule, here, and records retention ordinance, here.*

   In addition, please provide answers to the following questions:
   - *How does it dispose of the information stored at the appropriate interval?*
   - *What is your audit process for ensuring the timely and appropriate disposal of information?*

   The project requires that the vendor (Omni Park, Inc.) follow City data retention standards as stated on the contract agreement per the City's General Records Retention Schedule v8.1 (Sept. 2015).

SHARING

9. ***Are there other departments or agencies with assigned roles and responsibilities regarding the information that is collected?*** *Identify and list the name(s) of any departments or agencies with which the information is shared and how ownership and management of the data will be handled.*

   There are no other departments or agencies with assigned roles or responsibilities regarding collected information.

10. ***Does the project/program place limitations on data sharing?***

Describe any limitations that may be placed on external agencies further sharing the information provided by the City of Seattle. In some instances, the external agency may have a duty to share the information, for example through the information sharing environment.

Data from the Permit Point system will not be provided to external agencies.

11. ***What procedures are in place to determine which users may access the information and how does the project/program determine who has access?*** *Describe the process and authorization by which an individual receives access to the information held by the project/program, both electronic and paper based records. Identify users from other departments who may have access to the project/program information and under what roles these individuals have such access. Describe the different roles in general terms that have been created that permit access to such project/program information. Specifically, if remote access to the system is allowed or external storage or communication devices interact with the system, describe any measures in place to secure the transmission and storage of data (e.g., encryption and/or two-factor authentication).*

    The Seattle Center Transportation/Parking Manager will determine which employees have access to the information. No users from other departments will have access to the system.

    There are two user roles in the PermitPoint system.

    1. Lot Manager: can be granted one or more of the following permissions
        a. Modify Locations and Permit Types
        b. Impersonate Customers
        c. Modify Customers and Permits
        d. Modify Transactions
        e. View Reports
    2. Administrator, will have all roles above and in addition can be granted additional role below.
        a. System Administrator

    The System is accessible via the Internet (outside City network firewall), and all user data is encrypted via HTTPS (AES128+ and TLS 1.2). Complex passwords are required for access and are stored using non-reversible encryption.

12. ***How does the project/program review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within City of Seattle and outside agencies?*** *Please describe the process for reviewing and updating data sharing agreements.*

    All data requests must go through established Department data privacy sponsors and champions. Data in this system will be classified as “Requires Special Handling” and will not be shared.

LEGAL OBLIGATIONS AND COMPLIANCE

13. ***Are there any specific legal authorities and/or agreements that permit and define the collection of information by the project/program in question?***

- *List all statutory and regulatory authority that pertains to or governs the information collected by the project/program, including the authority to collect the information listed in question.*
- *If you are relying on another department and/or agency to manage the legal or compliance authority of the information that is collected, please list those departments and authorities.*

The System must maintain PCI compliance and will go through annual 3rd party security penetration testing. Compliance will be coordinated with the PCI compliance team and SeaIT Security Office.

14. ***How is data accuracy ensured?*** *Explain how the project/program checks the accuracy of the information. If a commercial data aggregator is involved describe the levels of accuracy required by the contract. If the project/program does not check for accuracy, please explain why. Describe any technical solutions, policies, or procedures focused on improving data accuracy and integrity of the project/program.*

    No data aggregator will be used. The parking staff will manually confirm that the customer key card number stored within the PermitPoint system matches the Amano McGann Parking Management System. Approximately 200 records are expected at this time.

15. ***What are the procedures that allow individuals to access their information?***
    Describe any procedures or regulations the department has in place that allow access to information collected by the system or project/program and/or to an accounting of disclosures of that information.

    Customers may access their information in the system by logging in with their User Name (email) and password (complex password is required).

16. ***What procedures, if any, are in place to allow an individual to correct inaccurate or erroneous information?*** *Discuss the procedures for individuals to address possibly inaccurate or erroneous information. If none exist, please state why.*

    Customers can correct and update their information at any time by logging in to the system.

17. ***Is the system compliant with all appropriate City of Seattle and other appropriate regulations and requirements?*** *Please provide details about reviews and other means of ensuring systems and project/program compliance.*

    PCI review and e-payment standard exception for the PermitPoint system using Imprezzio Tranzgate credit card payment processing has been completed.

18. ***Has a system security plan been completed for the information system(s) supporting the project/program?*** *Please provide details about how the information and system are secured against unauthorized access.*

    Request for Security assessment has been submitted.

    Complex passwords are required for access and are stored using non-reversible encryption.

19. ***How is the project/program mitigating privacy risk? G****iven the specific data elements collected, discuss 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.*

    Omni Park will mitigate any risk since data is available only to the customer and parking unit administrators. No customer data is ever publicly made available.

MONITORING AND ENFORCEMENT

20. ***Describe how the project/program maintains a record of any disclosures outside of the department.*** *A project/program may keep a paper or electronic record of the date, nature, and purpose of each disclosure, and name and address of the individual or agency to whom the disclosure is made. If the project/program keeps a record, list what information is retained as part of the accounting requirement. A separate system does not need to be created to meet the accounting requirement, but the project/program must be able to recreate the information noted above to demonstrate compliance. If the project/program does not, explain why not.*

    All data disclosures requested from outside the department must go through Seattle Center's Privacy Program Manager and recorded per City policy and procedure.

    The following system standard data elements are retained as part of accounting requirement; Transactions date, Location (Parking Garage), Account Name, Transaction Type, Transaction Status, Amount, Tax, Convenience Fee, Method (Online), and Check number (not planning to use). An ID number identifying key card number will be added.

21. ***Have access controls been implemented and are audit logs are regularly reviewed to ensure appropriate sharing outside of the department?*** *Is there a Memorandum of Understanding (MOU), contract, or agreement in place with outside agencies? Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.*

    No information on PermitPoint system will be shared with other departments.

    Every update to the PermitPoint data are logged in audit records including the user/process, timestamp and data changes. These audit records are captured in real-time and retained for at least 12 months.

22. ***How does the project/program ensure that the information is used in accordance with stated practices of the project/program?*** *What auditing measures are in place to safeguard the information and policies that pertain to them? Explain whether the project/program conducts self-audits, third party audits or reviews.?*

    System must maintain PCI compliance and will go through annual 3rd party security penetration testing. Compliance will be coordinated with PCI compliance team and SeaIT Security Office.

23. ***Describe what privacy training is provided to users either generally or specifically relevant to the project/program.*** *City of Seattle offers privacy and security training. Each project/program may offer training specific to the project/program, which touches on information handling procedures and*

sensitivity of information. Discuss how individuals who have access to personal information are trained to handle it appropriately. Explain what controls are in place to ensure that users of the system have completed training relevant to the project/program.

All parking staff are required to take PCI Awareness Training that covers credit card data security standards, and annual City data privacy and security training. The Seattle Center Transportation/Manager will ensure that each employee completes the required training.

24. *Is there any aspect of the project/program that might cause concern by giving the appearance to the public of privacy intrusion or misuse of personal information?* *Examples might include a push of information out to individuals that is unexpected and appears to be intrusive, or an engagement with a third party to use information derived from the data collected that is not explained in the initial notification.*

There is no aspect of the project that might cause concern regarding privacy intrusion or misuse of personal information. The system does not have mass/bulk notification capability by design. Should the customer choose to receive reminders or transaction confirmations via email, they will be required to enable the process. Seattle Center's implementation of PermitPoint System does not integrate with any other 3rd party system.