POWERFUL TECHNOLOGY SOLUTIONS
FOR THE CITY AND PUBLIC WE SERVE

## 2018 Privacy Impact Assessment

# EPACT NETWORK

## SEATTLE PARKS AND RECREATION DEPARTMENT (SPR)

03.16.2016

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 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.

ePACT Network is a Cloud-based, Active Net-integrated, service that manages how Seattle Parks and Recreation (SPR) collects and manages emergency information for programs that require emergency contacts and/or health-related information. ePACT is an online emergency network that specializes in the secure collection and storage of this information.

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

This project will involve the collection of sensitive information from participants, including, health information for participants, their legal guardians and emergency contacts, authorized pickup lists, health and health insurance information, consents and waivers.

# 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.

Implementation of ePACT will eliminate the collection of this information on paper forms, improving security around collection of this information, significantly reducing the administrative burden of collecting the information, and improving the experience for participants and their families, but allowing them to enter information only once (and updating it as necessary), rather than completing paper forms for each program they attend. Implementation will also include integrating ePACT with the City's Parks and Recreation Management System – Active Net.

### 2.2 Provide any data or research demonstrating anticipated benefits.

With the adoption of ePACT, the City will benefit in the following ways:

- Improved emergency and safety measures across recreation programs.
- Enhanced privacy: SPR control which staff have access to participants' emergency data, while families own their account and data.
- Enhanced security: Data is regulated under the same security standards as online banking and meets or exceeds privacy standards under government legislation.
- Value added service provided by City to show commitment towards participant safety in recreation programs.
- Streamlined registration process with the integration of the City's Parks and Recreation management software, Active Net.

Families attending recreation programs will benefit from an easier and more secure method for sharing emergency and medical information with SPR staff, therefore increasing customer satisfaction amongst families.

### 2.3 Describe the technology involved.

ePACT is a web-based solution developed in Java and hosted in secure redundant environments in Vancouver and Toronto, Canada. ePACT is SOC 2 Compliant and uses industry standard SSL data encryption, with a 2048-bit certificate that supports encrypted sessions up to 256 bit.

With ePACT, families create a single online emergency record that they can use to share information with Seattle Parks and Recreation (SPR), as well as with any other organizations using ePACT, increasing the convenience to participants, as well as the likelihood that they will keep their information current. SPR will have an Organization ePACT Account which connects to ActiveNet. When new participants are added to programs that require emergency information, the participant (or their legal guardian) will receive an email requesting that they provide emergency information via ePACT. The participant will create an ePACT account or login to an existing account, complete the information requested by SPR, and share it with SPR. Any time the participant returns to their ePACT account and changes any of the information that has been shared with SPR, the information will be updated, and SPR staff will be notified.

Through the Organization Account, SPR Administrators will be able to track receipt of emergency information, send reminders to people who have not completed, and will be able to run reports, helping to quickly identify participants with special needs, health considerations such as allergies, etc.

Through the Organization Account SPR Administrators can assign 'Group Administrators' who will have access to a limited number of records (for kids in a particular camp).

Records are stored online, accessible through the Organization Account, as well as through a secure mobile app.

The system also includes the ability to send email and text messaging to participants and/or guardians and/or emergency contacts.

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

The Seattle Parks and Recreation Department mission includes providing "welcoming and safe opportunities to play, learn, contemplate and build community." By creating a better and more secure way of keeping emergency contact information about participants current and accessible we are supporting this mission.

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

ePACT and Activenet are SaaS applications who will provide the web-based links to the applications. The SPR ePACT Application Administrator will provide the information needed to access the applications. Active Net and ePACT will provide any needed 'backend' changes to integrate the two systems. Seattle IT will provide applications support from the End User team.

# 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 SPR ePACT Organization Account is only accessible with Administrative Permission. Use of the system requires Administrators to Login with a username (email address), and a password (minimum 10 characters).

The SPR Application Business Administrator will manage and authorize who has access by name and role working with the vendor and ITD, if needed.

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

For example, the purposes of a criminal investigation are supported by reasonable suspicion.

SPR does not have legal standards or conditions to meet. However, access to ePACT will be managed by SPR, and will require approvals to gain access.

### 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.

Include links to all policies referenced.

Currently, there are no compliance requirements. SPR is currently developing policies and training for the proper use of the application. A link and notice will be sent to the Privacy Office to those documents when SPR has had some time to familiarize themselves with the application.

# 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.**

ePACT will connect to ActiveNet and will retrieve the following information related to participants in any program that requires an ePACT form: participant first name, participant last name, ActiveNet ID, ActiveNet account holder email address(es), Program/Activity ID, Program/Activity Name.

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

ePACT and The Active Network have worked together for two years and have a partnership agreement in place. The two companies have built an integration collaboratively and tested the integration extensively to ensure that data passed between ActiveNet and ePACT is limited to the expected information.

**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?**

SPR will make all business decisions on deployment. The connection to the ePACT SaaS solution will be implemented by Seattle IT (ITD) working with ePACT with ITD and End User team, if needed. Target date is mid-year 2018. A joint project plan will be developed by SPR, ITD and ePACT.

**4.4 How often will the technology be in operation?**

The technology will be in operation daily.

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

Seattle Parks and Recreation intends to sign a one-year contract with ePACT (the minimum commitment), however this contract can be rolled over for subsequent years. ePACT does also allow for three-year contracts.

**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?**

N/A

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

Please do not include staff names; roles or functions only.

Data will be accessed by SPR staff upon approval by the Department. The Parks Application Business Manager will be responsible for managing and access.

### 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.

ePACT's Customer Success Team may access data at the explicit request of city staff, and solely for the purpose of providing customer support, as detailed in ePACT's Privacy Policies.

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

Data will only be accessed by approved and credentialed SPR personnel to ensure the safe delivery of programs being attended by the participant providing the data, and/or for compliance audits.

### 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.)?

ePACT uses industry standard SSL data encryption, with a 2048 bit certificate that supports encrypted sessions up to 256 bit. This means that all data passed between our servers and our customers' computers is encrypted, using the highest level of encryption that can be handled by today's web browsers.

Other Security Measures: To protect against a brute force attack, ePACT has security measures at both the application level and the server level. At the application level, accounts are locked if there is an attempt to access the account using the wrong password more than 5 times. At the server level ePACT monitors for attacks is prepared with a number of tools to aid in shutting down an attack (mod_qos, code changes, rate limiting, ipblocking, etc.).

Other security measures to prevent hacking include:

- All database queries are built to prevent sql injection;
- All user data input is validated and marshalled into expected data types before use;
- Entire application is forced to be served over HTTPS, making it next to impossible for a hacker to hijack a session;
- All site input forms include a unique code to prevent Cross-Site Request Forgery attacks.

# 5.0 DATA STORAGE, RETENTION, AND DELETION

### 5.1 How will data be securely stored?

Data is stored on ePACT's secure servers in Tier 3 hosting facilities. Passwords, insurance information, and any documents uploaded to the system are encrypted at rest (other data is stored unencrypted for searchability). All data is encrypted in transit. Details of ePACT's security measures are detailed in the company's SOC 2 Type 2 report.

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

With ePACT the participant owns their own account and can delete their account and the information contained therein at any time. Copies of information provided to SPR are stored in SPR Organization Account, until such a time as the information is no longer required, according to the City's retention policies. ePACT also provides an archival service that we can opt to add on which stores copies of information provided and automatically deletes it on a set retention schedule. The City of Seattle data retention schedule may be found here: http://bloginweb/cityrecords/retention-schedule/ .

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

Improperly collected information (for example information that has been requested from someone who then decides not to participant in a program), will be deleted via the SPR Organization Account. Records related to participants not currently enrolled in a specific program are automatically moved to a 'disconnected tab', making it easy for Administrators to recognize records that need to be deleted. Once a record is deleted from the account it is removed from ePACT within 24 hours, and from ePACT backups within 7 days.

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

SPR will be primarily responsible, working with Seattle IT and ePACT to ensure retention schedules are set and monitored. This will be overseen by the SPR Applications Business Manager working with the ActiveNET Business Project Manager.

# 6.0 DATA SHARING AND ACCURACY

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

N/A

**6.2 Why is data sharing necessary?**

N/A

**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 provided to the City via ePACT includes emergency information that will only be accessed and used in the safe delivery of City programs.

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

N/A

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

Information imported from ActiveNet will be reviewed against rosters to ensure all participants are accounted for. All other data is provided by participants or their legal guardians. ePACT enforces completion of the required information and SPR staff, while they may review information as part of preparation for programs, assume that participants, as the 'owners' of their persona information have conveyed it accurately.

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

Participants or their legal guardians can log in to ePACT any time to review the information they have previously shared with the City and make any desired updates. The City will also be notified of any updates.

# 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?

No specific authorities or agreements have been identified or required at this time.

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

For example, police department responses may include references to the Seattle Police Manual.

SPR ePACT Administrators will complete training with ePACT which includes instruction on the correct use of the system, an introduction to the privacy safeguards and best practices for addressing privacy and security. Seattle IT also provides annual Privacy Training online for all City of Seattle employees.

### 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.

Please work with the Privacy Team to identify the specific risks and mitigations applicable to this project / technology.

SPR will be collecting the same information that is currently collected on paper forms, but through a secure online platform. As with any collection method there is risk of:

a) Data breach of the ePACT system – ePACT maintains a security protocol to mitigate risk of breach, and also maintains a breach response plan that allows for rapid identification of a breach, technical response plan, breach communications plan, and cyber liability insurance.
b) Unauthorized access/use by a City staff member – access to records is limited to only those staff requiring access for program delivery, and even in that case only to the specific records required (i.e. participants in camp they are running). Access is logged, and access rights can be removed, if necessary.

### 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?

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.

Because this is a new method of requesting emergency information from participants there is risk of confusion or mistrust. In order to mitigate this, ePACT will provide the City with messaging that can be included at point of registration, and/or on the SPR website so that the public is educated and feels comfortable with the new process. The request to provide information via ePACT will be branded with City branding, include the City of Seattle Privacy Statement, and staff will be provided with information about ePACT should any questions arise.

# 8.0 MONITORING AND ENFORCEMENT

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

There will be no disclosures outside the department, except in the case of an emergency where information may be passed to a first responder or other emergency/medical service provider. If information is shared in an emergency, this will be noted in comments in the ePACT system.

**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.**

ePACT undergoes an annual privacy audit with Hooper Access and Privacy, and a SOC 2 Type 2 Audit with PwC. Audit reports are available to the City.