 |

**Privacy Impact Assessment**

Team Identifire

Inclusive Safety Communities Track

Odyssey Momentum 2020

**Privacy impact assessment (PIA model Rijksdienst)**

[Part A: Description characteristics data processing 3](#_Toc56333173)

[1. Proposal 3](#_Toc56333174)

[2. Personal data 3](#_Toc56333175)

[3. Data processing 3](#_Toc56333176)

[4. Processing purposes 4](#_Toc56333177)

[5. Involved parties 4](#_Toc56333178)

[6. Interests in data processing 4](#_Toc56333179)

[7. Processing locations 4](#_Toc56333180)

[8. Techniques and methods of data processing 4](#_Toc56333181)

[9. Legal and policy framework 5](#_Toc56333182)

[10. Retention periods 5](#_Toc56333183)

[Part B: Assessment of lawfulness of personal data processing 5](#_Toc56333184)

[11. Legal basis 5](#_Toc56333185)

[12. Special personal data 5](#_Toc56333186)

[13. Purpose limitation 5](#_Toc56333187)

[14. Necessity and proportionality 5](#_Toc56333188)

[a. Proportionality 5](#_Toc56333189)

[b. Subsidiarity 5](#_Toc56333190)

[15. Rights of data subjects 5](#_Toc56333191)

[Part C: Description and assessment of risks for those involved 5](#_Toc56333192)

[16. Risks 5](#_Toc56333193)

[a. The data processing can have negative consequences for the rights and freedoms; of the data subject; 5](#_Toc56333194)

[b. The origin of these consequences; 5](#_Toc56333195)

[c. The likelihood (chance) that these consequences will occur; 5](#_Toc56333196)

[d. The severity (impact) of these consequences for those involved when they occur. 5](#_Toc56333197)

[Part D: Description of proposed measures 6](#_Toc56333198)

[17. Measures 6](#_Toc56333199)

# Part A: Description characteristics data processing

## 1. Proposal

This document will evaluate the impact on the privacy of user of the ‘Citizen Arch’ protocol. The evaluate will identify and adequately address all privacy concerns that were determined during the developing phase of [NAME] at Odyssey Momentum 2020.

By conducting a Privacy Impact Assessment (PIA), team Identifire evaluates compliance with laws and regulations governing privacy and demonstrates the GDPR’s commitment to protect the privacy of any personal information we collect, process and store.

## 2. Personal data

Personal data is understood as information in an IT system or online collection that directly identifies an individual. the ‘Citizen Arch’ protocol processes personally identifiable information, herinafter called PII, namely:

|  |  |
| --- | --- |
| **Category PII** | **Collected, processed or stored PII** |
| General personal data | 1. Name of the citizen volunteer; 2. Notification identifier; 3. Verifiable credential data. |
| Sensitive personal data | 1. Geofence location of the citizen volunteer; 2. Mobile Location Data / Movement Data. |
| Details of criminal offences | N/A |
| Legal identification number (BSN) | N/A |

## 3. Data processing

|  |  |
| --- | --- |
| **Category data processing** | **PII** |
| Collecting PII | 1. Name of the citizen volunteer; 2. Notification identifier; 3. Verifiable credential data; 4. Geofence location of the citizen volunteer; 5. Mobile Location Data / Movement Data. |
| Processing PII | 1. Name of the citizen volunteer; 2. Notification identifier; 3. Verifiable credential data; 4. Geofence location of the citizen volunteer; 5. Mobile Location Data / Movement Data. |
| Storing PII | * Geofence location of the citizen volunteer;   The most recent geofence location shared by the device of the citizen volunteer is stored by the ‘Citizen Arch’ protocol.   * Notification identifier. |

## 4. Processing purposes

|  |  |
| --- | --- |
| **PII** | **Processing purpose** |
| Name of the citizen volunteer | The name of the citizen volunteer is collected and processed by the ‘Citizen Arch’ protocol, to |
| Notification identifier |  |
| Verifiable credential data | The verifiable credential data is collected and processed by [NAME] to |
| Geofence location of the citizen volunteer | The most recent geofence location of the citizen volunteer is collected, processed and stored to locate the citizen when the 112-dispatch center wants to request a citizen volunteer in the area of an emergency incident. |
| Mobile Location Data / Movement Data | The Mobile Location Data / Movement Data of the citizen volunteer is collected and processed to share the live-location of the volunteer during the request phase of the 112-dispatch request to locate the precise location of the citizen volunteer. This is necessary for |

## 5. Involved parties

The most recent architecture of the ‘Citizen Arch’ protocol involves the following parties in the personal data collection and processing process:

|  |  |
| --- | --- |
| **Party** | **Role of the party** |
| The ‘Citizen Arch’ protocol | This party is a processor and/or controller of the PII. |
| Meldkamer 112 (112-Dispatch Center of the Netherlands) | This party is a processor and/or controller of the PII. |
| Citizen participation platforms in the Netherlands | This party is a processor of the PII. |
| Volunteer that is registered at an affiliated citizen participation platform of the ‘Citizen Arch’ protocol | This party is a data subject. |

## 6. Interests in data processing

|  |  |
| --- | --- |
| **Party** | **Interests** |
| The ‘Citizen Arch’ protocol | Connect a group of qualified citizens to the 112-Dispatch center of the Netherlands. |
| Meldkamer 112 (112-Dispatch Center of the Netherlands) | Request the help from citizen volunteers for an (emergency) incident. |
| Citizen participation platforms in the Netherlands | Provide a platform on which it can connect citizens to an (emergency) incident. |
| Volunteer that is registered at an affiliated citizen participation platform of the ‘Citizen Arch’ protocol | Provide and engage in volunteering services on citizen participation platforms. |

## 7. Processing locations

The intended processing of personal data through the ‘Citizen Arch’ protocol will take place in the following countries:

|  |
| --- |
| **Processing location** |
| The Netherlands |

## 9. Legal and policy framework

Benoem de wet en regelgeving, met uitzondering van de AVG en de richtlijn, en het beleid met mogelijke gevolgen voor de voorgenomen gegevensverwerking.

|  |  |
| --- | --- |
| **Applicable laws and regulations** | **Applicable to the following party** |
| Omgevingswet (Netherlands, implemention in 2022) | All parties, if they participate in citizen participation initiatives. |
| All laws and regulations concerning personal liability (civil and criminal liability) | Citizen volunteer. If a citizen volunteer causes (un)intentional damages during an emergency incident, the available PII concerning the volunteer could be shared with third parties such as an insurance company. |

## 10. Retention periods

|  |  |
| --- | --- |
| **Stored PII** | **Retention period** |
| Most recent geofence location of the citizen volunteer | Most recent geofence location is stored until the citizen participation app has been deleted or if location sharing consent has been revoked by volunteer. |
| Notification identifier | Notification identifier is stored until the citizen participation app has been deleted or notification identifier sharing consent has been revoked by volunteer. |

# Part B: Assessment of lawfulness of personal data processing

## 11. Legal basis

|  |
| --- |
| **Legal basis** |
| Consent of the volunteer that has been provided freely, specifically, informed and with unambiguous expression of will. |

## 12. Special personal data

|  |  |
| --- | --- |
| **Special PII** | **Applicability of legal basis** |
| Geofence location of the citizen volunteer | This special PII can be lawfully processed with consent because the location history is not collected, processed and stored and can therefore not reveal racial, ethnic origin, political opinions, religious or philosophical beliefs; trade-union memberships; genetic data, biometric data processed solely to identify a human being; health-related data or data concerning a person’s sex life or sexual orientation. |
| Mobile Location Data / Movement Data | This special PII can be lawfully processed with consent because the location history is not collected, processed and stored and can therefore not reveal racial, ethnic origin, political opinions, religious or philosophical beliefs; trade-union memberships; genetic data, biometric data processed solely to identify a human being; health-related data or data concerning a person’s sex life or sexual orientation. |

## 13. Purpose limitation

|  |
| --- |
| **Purpose limitation** |
| PII will not be processed for a purpose other than originally collected. |

## 14. Necessity and proportionality

### a. Proportionality

|  |
| --- |
| **Proportionality** |
| The general and special PII that will be collected, processed and stored is proportional to the purpose of the data. It will not invade the privacy of the volunteer because the PII will be shared in an exclusive and secured environment (with the ‘Citizen arch’ protocol and the 112-dispatch center). And the special PII that reveals the location of the volunteer is only collected when the 112-dispatch center has actively requested the help from the volunteer. |

### b. Subsidiarity

|  |
| --- |
| **Subsidiarity** |
| The processing purposes cannot be reasonably changed in a less adverse manner, because the specified PII are necessary for the 112-dispatch center to support and provide instructions to the volunteer during the (emergency) incident. |

# Part C: Description and assessment of risks for those involved

## 16. Risks

### a. The data processing can have negative consequences for the rights and freedoms; of the data subject;

|  |
| --- |
| **Negative consequences for the rights and freedoms of the data subject** |
| The volunteer (data subject) could experience negative consequences for his/her/its rights and freedoms if location data has been exposed through a security leak |

### b. The origin of these consequences;

|  |
| --- |
| **The origin of these consequences** |
| Security breach |

### c. The likelihood (chance) that these consequences will occur;

|  |
| --- |
| **The likelihood that these consequences will occur** |
| Low |

# Part D: Description of proposed measures

## 17. Measures

We have implemented the following measures to safeguard the PII of the volunteer:

* Only the latest known location will be stored. No location history will be stored.