## **PIA** information

| PIA        |                                 |
|------------|---------------------------------|
| Map Helper |                                 |
| Author's   | name                            |
| Entidade   | l .                             |
| Assesso    | r's name                        |
| Entidade   | 2                               |
| Validato   | r's name                        |
| Entidade   | 3                               |
| Creation   | date                            |
| 16/04/20   | 19                              |
| DPO's na   | ame                             |
| entity 4   |                                 |
| DPO's o    | pinion                          |
| It is poss | ble to use the treatment        |
| Search (   | of concerned people opinion     |
| Concerne   | d people opinion was requested. |
| Concern    | ed people opinions              |
| entity5    |                                 |
| Concern    | ed people statuses              |
| The treat  | ment could be implemented.      |
| Concern    | ed people opinions              |
| The treat  | nent can be used                |

## **Context**

#### **Overview**

### Which is the processing under consideration?

Gathering location user data

#### What are the responsibilities linked to the processing?

Get consent from the users to use their location data and keep this data private from other entities.

Are there standards applicable to the processing?

**GDPR** 

**Evaluation: Acceptable** 

## Data, processes and supporting assets

### What are the data processed?

Location data (coordinates), locations of interest.

#### How does the life cycle of data and processes work?

Location data is saved when the user turns on the app, accessed for suggestions of routes, and removed if the user asks for removal.

### What are the data supporting assets?

Servers that can support location data of several users.

## **Fundamental principles**

## Proportionality and necessity

#### Are the processing purposes specified, explicit and legitimate?

Yes, the consent of the user is asked before any location data is gathered.

**Evaluation: Acceptable** 

#### What are the legal basis making the processing lawful?

User consent

**Evaluation: Acceptable** 

# Are the data collected adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')?

Yes, the data is relevant due to being needed for suggesting different routes and similar locations to the user

**Evaluation: Acceptable** 

#### Are the data accurate and kept up to date?

Yes the data is kept up to date and accurate.

**Evaluation: Acceptable** 

#### What are the storage duration of the data?

When the user asks for data removal or when the app is uninstalled.

**Evaluation: Acceptable** 

## Controls to protect the personal rights of data subjects

## How are the data subjects informed on the processing?

When they install the app.

**Evaluation: Acceptable** 

### If applicable, how is the consent of data subjects obtained?

When they install the app.

**Evaluation: Acceptable** 

#### How can data subjects exercise their rights of access and to data portability?

If the user asks for the data stored in the database, he/she will be able to download all of the data gathered until the moment of the request.

## How can data subjects exercise their rights to rectification and erasure?

If the user requests for data removal, all data gathered until now will be erased.

**Evaluation: Acceptable** 

## How can data subjects exercise their rights to restriction and to object?

If the user wants to use the app he needs to consent to the use of location data.

**Evaluation: Acceptable** 

Are the obligations of the processors clearly identified and governed by a contract?

Yes.

**Evaluation: Acceptable** 

In the case of data transfer outside the European Union, are the data adequately protected?

Yes

## **Risks**

## Planned or existing measures

#### Acess to account from another device

The user is asked to confirm that the device is theirs. If the device isn't confirmed in 2 days, the acess to the application is blocked.

**Evaluation: Acceptable** 

## Illegitimate access to data

What could be the main impacts on the data subjects if the risk were to occur?

Visited locations can be discovered

What are the main threats that could lead to the risk?

User location can be found

What are the risk sources?

Attacker can use client location to do harm

Which of the identified controls contribute to addressing the risk?

Acess to account from another device

How do you estimate the risk severity, especially according to potential impacts and planned controls?

Important, Knowing user location data can put him/her in danger

How do you estimate the likelihood of the risk, especially in respect of threats, sources of risk and planned controls?

Limited, The administrators will fix any security flaws so nothing happens to the users

**Evaluation: Acceptable** 

#### Unwanted modification of data

What could be the main impacts on the data subjects if the risk were to occur?

Robbery or selling location data

What are the main threats that could lead to the risk?

Attackers that know the users location

What are the risk sources?

Attackers with hacking skills

Which of the identified controls contribute to addressing the risk?

Acess to account from another device

How do you estimate the risk severity, especially according to potential impacts and planned controls?

Important, We will notify the user if anything happens to his/her location data and steps will be taken to protect the users data

How do you estimate the likelihood of the risk, especially in respect of threats, sources of risk and planned controls?

Limited, It's not very common for this to happen.

**Evaluation: Acceptable** 

## Data disappearance

What could be the main impacts on the data subjects if the risk were to occur?

Losing location data

What are the main threats that could lead to the risk?

Attackers with hacking skills

What are the risk sources?

Attackers with experience in hacking

Which of the identified controls contribute to addressing the risk?

Acess to account from another device

How do you estimate the risk severity, especially according to potential impacts and planned controls?

Negligible, The user will not be able to use the app for some time

How do you estimate the likelihood of the risk, especially in respect of threats, sources of risk and planned controls?

Important, The app can lose users if the time to fix this is too long

## **Action plan**

## **Overview**

### **Fundamental principles**

Purposes
Legal basis
Adequate data
Data accuracy
Storage duration
Information for the data
subjects
Obtaining consent
Information for the data

subjects Right to rectification and

erasure

Right to restriction and to

object Subcontracting Transfers

#### Planned or existing measures

Acess to account from another device

#### Risks

Illegitimate access to data Unwanted modification of data Data disappearance

> Improvable Measures Acceptable Measures

## Fundamental principles

No action plan recorded.

## Existing or planned measures

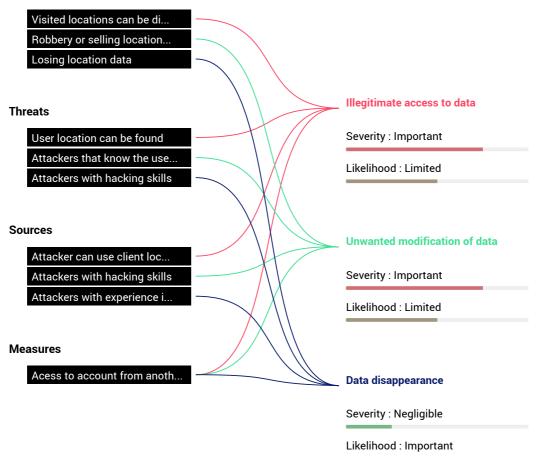
No action plan recorded.

## **Risks**

No action plan recorded.

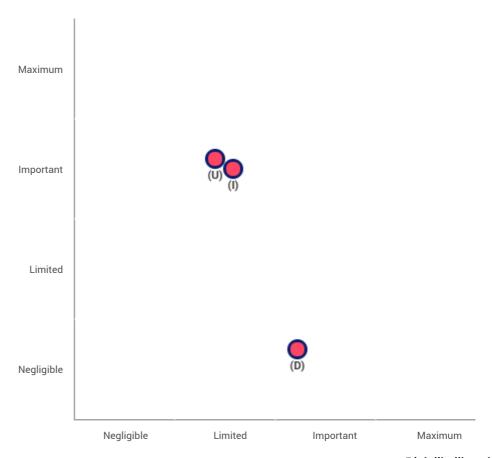
## **Risks overview**

### **Potential impacts**



## **Risk mapping**

### Risk seriousness



- Planned or existing measures
- With the corrective measures implemented
- (I)llegitimate access to data
- (U)nwanted modification of data
- (D)ata disappearance

Risk likelihood

16/04/2019