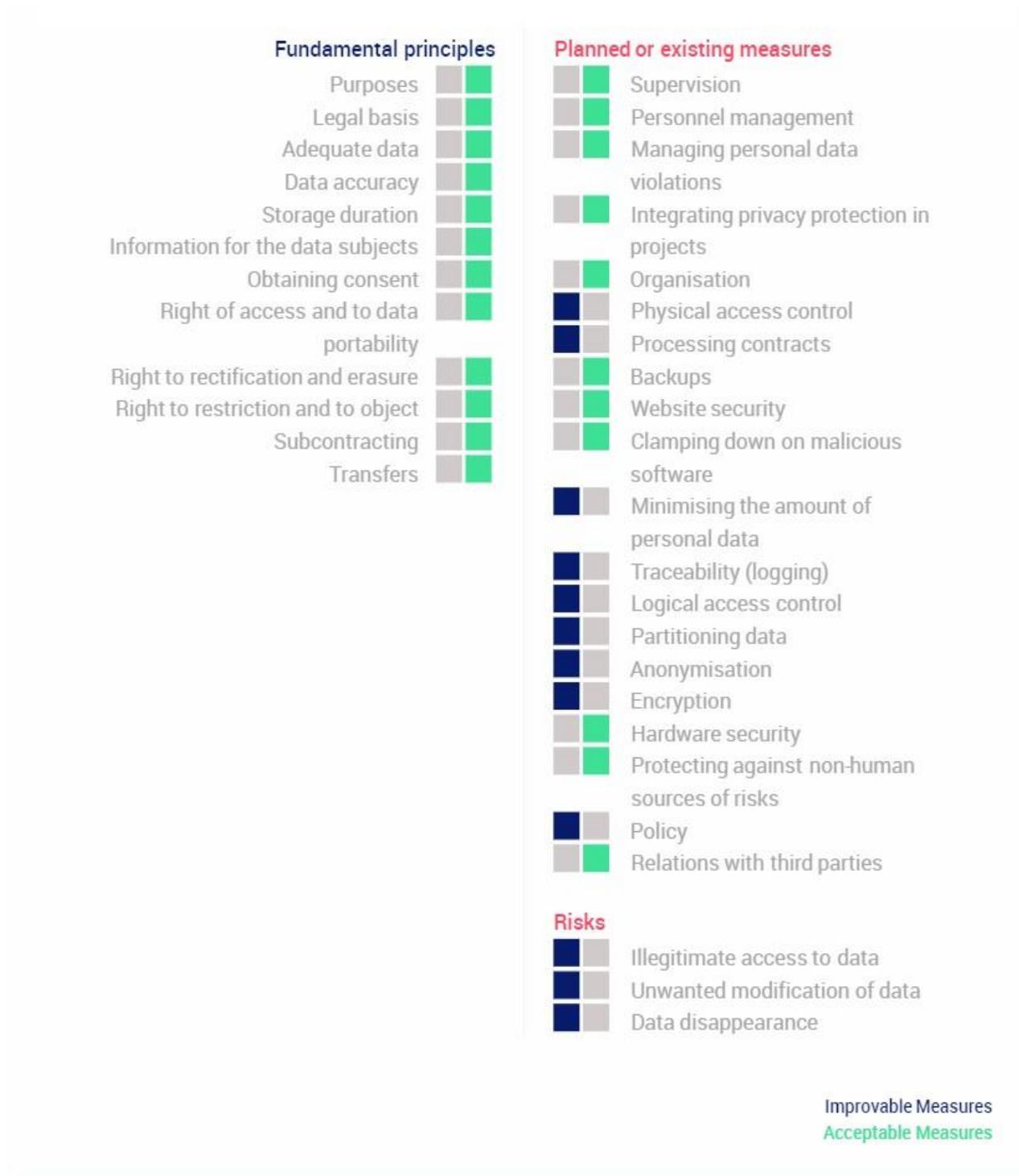




Privacy Impact Assessment

Version 0.3 – October 18th, 2020

Overview^{1,2}



1 Based on a debug version of the App submitted on September 23th 2020.
 2 Performed in accordance to GDPR Art. 35 and with help of the open source software and guidelines published by the French Commission nationale de l'informatique et des libertés (CNIL).
 Reference: <https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assessment>

Part 1 – Context

1.1 – Overview

What is the processing under consideration?

Stichting Onderzoek Marktinformatie (SOMI) will launch an App that aims to exercise the rights of data subjects referred to in Articles 15, 16, 17, 18, 19 20, 21 and 22 of the General Data Protection Regulation (“GDPR”), to represent the data subject in exercising the rights referred to in Articles 77, 78 and 79 GDPR and 82 GDPR, which representation is based on Article 80 GDPR.

What are the responsibilities linked to the processing?

Stichting Onderzoek Marktinformatie (SOMI) is the data controller.

Dotswan, Stichting Bewaarder, Shufti Pro and Mihos.net are data processors for SOMI.

Are there standards applicable to the processing?

Not applicable.

Evaluation : Acceptable

1.2 – Data, processes and supporting assets

What are the data processed?

The categories of data processed are:

- Account information (email, password, account number) collected when the user makes an account;
- Contact information (first and last name, address, phone number, email address);
- Personal identification information (copy of national ID card) in order to exercise the rights of data subjects;
- Payment information and related data in order to provide goods and services and/or to manage user rights (bank account number, statements, contracts, etc.);
- Analytical data about activities using the app (login, IP, tabs accessed, time spent, etc.);
- Data provided by third parties when the data subjects explicitly ask us to exercise his/her right of access;
- Data collected about the data collected from third parties when the data subjects explicitly ask of to perform analysis of the data provided;
- Metadata regarding the rights the user has exercised;
- Other data that the data subjects actively provide to us, for example in correspondence when asking for support.

The maximum period the data will be stored:

- Data regarding activities on the app and will be stored for a maximum of 12 months;
- Contact information and data that data subjects actively provide to us will be stored for a maximum of 36 months after the last contact between the data subject and the data controller;
- Contracts, data regarding payments and invoices are stored 10 years in order to comply with our legal responsibilities;
- All personal data collected from third parties will be deleted at the simple request of the user or ultimately after the expiration of the user account (after 36 months of inactivity).

The persons with access to this data:

- Only the technical support staff of SOMI and mentioned data processors will have access to the data;
- All data collected from third parties will be automatically encrypted when processed. Any further processing will require the data subject to provide a unique password.

How does the life cycle of data and processes work?

See attachment:

- SOMI App Purchase Workflow

Evaluation: Acceptable

Part 2 – Fundamental principles

2.1 – Proportionality and necessity

Are the processing purposes specified, explicit and legitimate?

SOMI processes personal data for the following purposes:

- Identifying and investigating for long-term perspective issues of social importance, in particular, those relating to market information;
- Informing, educating and advising consumers, government agencies, policy or opinion makers, agents, advisers and experts, regulators and market parties;
- Promoting interests, taking actions and claiming compensation of its affiliated or registered persons, legal entities, injured parties, proxy or clients or participants;
- Providing support to other natural or legal persons who stand up in any way for those on behalf of which SOMI conducts research or takes action;
- Entering into, elaborating and executing agreements on behalf of the person on behalf of which SOMI acts.

The data collected in the context of the App purposely aims to exercise the rights of data subjects as referred to in Articles 15, 16, 17, 18, 19,20, 21 and 22 of the GDPR, to represent the data subject in exercising the rights referred to in Articles 77, 78,79, and 82 (the right to receive compensation).

Evaluation: Acceptable

What are the legal bases for making the processing lawful?

SOMI processes personal data based on the following principles:

- Identification data, account information and data collected from third parties are always processed on the basis of the informed and explicit consent of the data subject;
- Functional and analytical data about the behavior of data subjects in the app are processed on the basis of the legitimate interest of SOMI;
- Data necessary to be able to provide goods and services are collected where necessary for the performance of a contract or in order to take steps at the request of the data subject prior to entering into a contract;
- Personal data relating to an identity document (e.g. citizen service number or copy ID) are processed to the extent this is strictly necessary for the establishment, exercise or defense of legal claims;
- Certain data about payments, invoices, agreements, statements, etc. are kept for a longer period of time to the extent that we are legally obliged to do so;

The App does not aim to process special categories of personal data, such as data

revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

However, while collecting data from third parties it could happen that such data is processed. Therefore, such data will only be processed based on the explicit consent of the data subject to the processing of this data for the specified purpose of exercising his/her rights as a data subject.

If the analysis reveals such special categories of data are being processed, the user will be given the option of permanently deleting these categories of data.

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')?

- Account information, functional data and analytical data related to activities in the App are strictly necessary in order to create a functional and user-friendly interface for the data subject;
- Contact information and data that the data subjects actively provide to us are strictly necessary in order to communicate with the user regarding functionalities of the app and to provide support whenever requested;
- Personal identification information (e.g. copy of national ID card) will be collected where strictly necessary in order to exercise the rights of data subjects;
- Payment information, contracts, invoices and related data are strictly necessary in order to provide goods and services to the data subjects. In order to comply with tax and anti-money laundering legislation some data must be kept for a longer period of time;
- Metadata regarding the rights the user has exercised is strictly necessary in order to exercise the rights of data subjects and to create a functional user experience;
- Data provided by third parties and any analysis of this data will only be processed when the user explicitly asks us to do so. This data will be collected whenever strictly necessary in order to exercise the rights of the data subjects (e.g. right of access).

Evaluation: Acceptable

Are the data accurate and kept up to date?

Data provided by the data subjects will be periodically reviewed and kept up to date.

Data provided by third parties will only be reviewed on the basis of the explicit and

informed consent of the user. SOMI is therefore not responsible for the quality or accuracy of the data provided by third parties.

Evaluation: Acceptable

What is the storage duration of the data?

The maximum period the data will be stored:

- Data regarding activities on the app and will be stored for a maximum of 12 months. This period is justified in order to make annual statistics and periodically review the workflow of the App;
- Contact information and data the data subjects actively provide to us will be stored for a maximum of 36 months after the last contact between the data subject and the data controller. This period is justified in order to engage with data subjects regarding any queries and/or follow up any support questions. After 36 months of inactivity (and several notifications) the account and collected personal data will be automatically deleted;
- Contracts, data regarding payments and invoices are stored 10 years in order to comply with our legal responsibilities. This period is necessary in order to comply with applicable anti-money laundering and tax law;
- All personal data collected from third parties will be deleted at the simple request of the user or ultimately after the expiration of the user account (after 36 months of inactivity). This period is justified on the basis of allowing the user to use collected data to exercise further rights (such as data portability or file complaints with the data protection authorities).

Evaluation: Acceptable

2.2 – Controls to protect the personal rights of data subjects

How are the data subjects informed on the processing?

The privacy statement of SOMI is published on the website www.somi.nl and will be directly accessible from the App.

Evaluation: Acceptable

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

When signing up, the explicit and informed consent of the data subjects will be asked. Whenever the data subject requests to process data collected from third parties, explicit and informed consent will be asked again.

Evaluation: Acceptable

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

Data subjects can make a request for data access and data portability by sending an email to privacy@somi.nl.

Evaluation: Acceptable

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

Data subjects can make a request for data rectification and data erasure by sending an email to privacy@somi.nl.

Also, in the App functionalities will be added to permanently delete any data gathered from third parties.

Evaluation: Acceptable

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

Data subjects can make a request for restriction and object by sending an email to privacy@somi.nl.

Evaluation: Acceptable

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

SOMI will ensure data processing agreements with all data processors.

Evaluation: Acceptable

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

All data will be stored in data warehouses located within the European Union. When third party SDK's are being used or (analytical) data is shared with data processors outside the EU, the data transfer will be protected by Standard Contractual Clauses (SCC's).

Evaluation: Acceptable

Part3–Riskassessment

Potential impacts

- Data subjects could have pr
- Data leaks could interfer w
- Data loss could interfer wi.
- Data subjects could have pr

Threats

- Illegitimate acces trough h.
- Mistakes managing databas
- Mistakes by data controller
- Illegitimate loss of data t...

Sources

- Internal threats from colla..
- External threats from hacke
- Preassure from government
- External pressure from gov
- Non-human factors (eg. nat

Measures

- Encryption
- Anonymisation
- Logical access control
- Traceability (logging)
- Minimising the amount of p
- Website security
- Physical access control
- Processing contracts
- Personnel management
- Supervision
- Clamping down on malicio
- Organisation
- Managing personal data vic
- Integrating privacy protect.
- Hardware security
- Partitioning data
- Backups
- Protecting against non-hum

Illegitimate access to data

Severity : Important

Likelihood : Important

Unwanted modification of data

Severity : Limited

Likelihood : Important

Data disappearance

Severity : Limited

Likelihood : Limited

3.1 – Planned or existing measures

Supervision

The controller and data protection officer work closely together in order to monitor the effectiveness and adequacy of privacy controls. All new versions of the app will be subject to review by the data protection officer.

Evaluation: Acceptable

Personnel management

Only personnel with relevant assignments will be given access to personal data. All personnel that comes into contact with personal data will be subject to a confidentiality agreement and informed about the responsibilities towards the rights of data subjects.

Evaluation: Acceptable

Managing personal data violations

IT incidents and/or data breaches are logged in an internal incident register. For each incident, a severity impact assessment is performed and adequate measures to control, prevent and mitigate further incidents are implemented in close collaboration with management.

Evaluation: Acceptable

Integrating privacy protection in projects

For each important new project, a data protection impact assessment is made in close collaboration with management and IT support staff.

Evaluation: Acceptable

Organisation

SOMI is a data controller and an independent Data Protection Officer has been appointed. Information security and data protection are discussed regularly with all relevant parties within the organisation.

Evaluation: Acceptable

Physical access control

Access to the offices of SOMI is restricted to outsiders and controlled through the use of an

intercom with a camera.

Evaluation: Improvable

Action plan/corrective actions:

Visitors who could have access to personal data should always be accompanied by an employee of SOMI.

Processing contracts

All data processors are required to sign data processing agreements. These contracts stipulate, in particular, measures regarding Article 32 (Security of processing), conditions regarding engaging sub-contractors and compliance with obligations regarding personal data breaches, data protection impact assessments and prior consultation.

Evaluation: Acceptable

Backups

Daily backups are made of all production data. Weekly backups of the entire database are stored at an external location (within the EU).

Evaluation: Acceptable

Website security

Annually, an external security audit of the website is performed. Adequate steps in order to improve security are discussed and implemented in close collaboration with management and IT support staff.

Evaluation: Acceptable

Clamping down on malicious software

Anti-malware software is installed on all workstations and servers with access to personal data.

Evaluation: Acceptable

Minimising the amount of personal data

SOMI aims to collect minimal data in order to achieve the stated purpose. Several measures have been taken in order to minimise the data collected:

- When asking for user identification, the user is requested to erase all special categories of data such as the photo, citizen service number and machine-readable zone. The user is recommended to use the 'Kopie ID' App provided by the Dutch Government in order to make a safe copy of his/her identification document.
- When collecting data from third parties, the data is automatically encrypted when first processed by SOMI. The user must provide explicit consent and his/her unique

passphrase in order for any further processing of personal data to take place.
- After a period of inactivity, all collected personal data is automatically deleted (except data we are legally obliged to keep for a longer period of time).

Evaluation: Improvable

Action plan/corrective actions:

In the current version, the App requests a full copy of the National ID for ID verification (cf. app purchase workflow). When asking for a copy of the National ID, the data subject should be requested to black out passport photo, passport number, national ID number and Machine Readable Zone in this copy or photo.

Traceability (logging)

Currently, default logging of user activities is enabled on the server.

Evaluation: Improvable

Action plan/corrective actions:

All activities on the server should be logged in order to allow for digital forensics in case of a data breach.

Logical access control

Currently, access to the database is limited to a very small number of people.

Evaluation: Improvable

Action plan/corrective actions:

Clear roles and permissions for users with access to the database should be defined.

Partitioning data

Currently, no partitioning of data is planned.

Evaluation: Improvable

Action plan/corrective actions:

Partitioning measures should be implemented in order to prevent the entire database from being leaked in case of a single security breach.

Anonymisation

Currently, no anonymisation mechanisms have been implemented.

Evaluation: Improvable

Action plan/corrective actions:

Sensitive user information should be anonymised.

Encryption

All data 'in transfer' is encrypted using SSL. Currently, no additional encryption measures of the data 'at rest' have been implemented.

Evaluation: Improvable Evaluation

comment:

In future versions of the App, all data collected from third parties should be encrypted using a strong algorithm (AES-256) and a complex user-generated key that is not available to the data controller. Whenever the data collected from third parties is processed, the data subject should be asked to give his/her user-generated key.

Hardware security

No data is stored on internal systems.

External systems are secured:

SECURITY

- Security: 24x7 staffed
- Cameras: HD infrared cameras
- Access control: badge and fingerprint system CERTIFICATIONS
- ISO Certified
ISO 9001:2015
ISO 27001:2013
- PCI DDS compliant

Evaluation: Acceptable

Protecting against non-human sources of risks

All data is stored on mihos.net servers.

These include the following measures:

POWER

- Rack feeds: separated A and B feed (32A)
- Diesel stock: 48+ hours, refillable during use
- UPS: 15+ minutes runtime

- Redundancy: N+2

COOLING

- Constant temperature: 21 Celsius
- Humidity: 50% (+/- 20%)
- Redundancy: N+2

FIRE PREVENTION

- Fire detection system: VESDA
- Fire suppression system: Argonite gas
- Redundancy: N+1

Evaluation: Acceptable

Policy

The data controller has been subject to an external GDPR audit and is in the process of implementing measures. All data processing activities are logged in an internal register of data processing activities.

Evaluation: Improvable

Action plan/corrective actions:

Based on this Data Protection Impact Assessment, an information security plan should be rolled out prioritising the measures stipulated in the action plan (cf. infra).

Relations with third parties

All third party relations who could come into contact with personal data are required to sign a non-disclosure agreement.

Evaluation: Acceptable

3.2 – Risks

Illegitimate access to data

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

Data subjects could have private information shared with third parties. This could lead to moral as well as material damages for the data subjects. Data leaks could interfere with the exercising of the rights of data subjects.

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

Illegitimate access through hacking, Mistakes managing databases by collaborators, Mistakes by data controllers.

What are the risk sources?

Internal threats from collaborators, External threats from hackers or interested parties, Pressure from government agencies.

Which of the identified planned controls contribute to addressing the risk?

Encryption, Anonymisation, Logical access control, Traceability (logging), Minimising the amount of personal data, Website security, Physical access control, Processing contracts, Personnel management, Supervision, Clamping down on malicious software, Organisation, Managing personal data violations, Integrating privacy protection in projects, Hardware security, Partitioning data.

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

Important, insufficient control measures have been taken to mitigate and/or control the risk of illegitimate access to data.

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

Important, insufficient control measures have been taken to mitigate and/or control the likelihood of illegitimate access to data.

Evaluation: Improvable

Action plan/corrective actions:

According to the available information, additional measures are needed to properly meet the requirements for the protection of the data.

Taking into account the action plan, how do you re-evaluate the seriousness of this risk (Illegitimate access to data)? **Limited**

Taking into account the action plan, how do you re-evaluate the likelihood of this risk (Illegitimate access to data)? **Limited**

Unwanted modification of data

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

Data subjects could have private information shared with third parties. This could lead to immaterial as well as material damages for the data subjects. Data leaks could interfere with the exercising of the rights of data subjects.

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

Illegitimate access through hacking, Mistakes by data controllers, Mistakes managing databases by collaborators.

What are the risk sources?

External threats from hackers or interested parties, Internal threats from collaborators, Pressure from government agencies.

Which of the identified controls contribute to addressing the risk?

Supervision, Personnel management, Managing personal data violations, Integrating privacy protection in projects, Organisation, Physical access control, Processing contracts, Website security, Clamping down on malicious software, Minimising the amount of personal data, Traceability (logging), Logical access control, Anonymisation, Encryption.

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

Limited, Adequate control measures have been taken to mitigate and/or control the risk of unwanted modification of data.

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

Important, insufficient control measures have been taken to mitigate and/or control

the risk of unwanted modification of data.

Evaluation: Improvable

Action plan/corrective actions:

According to the available information, insufficient measures have been taken to mitigate and/or control the risk of modification of data.

Taking into account the action plan, how do you re-evaluate the seriousness of this risk (Unwanted modification of data)? **Limited**

Taking into account the action plan, how do you re-evaluate the likelihood of this risk (Unwanted modification of data)? **Limited**

Data disappearance

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

Data loss could interfere with the exercising of the rights of data subjects, Data subjects could have private information lost.

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

Illegitimate loss of data through hacking, Mistakes by data controllers, Mistakes managing databases by collaborators.

What are the risk sources?

External threats from hackers or interested parties, Internal threats from collaborators, External pressure from government agencies, Non-human factors (e.g. natural disasters).

Which of the identified controls contribute to addressing the risk?

Integrating privacy protection in projects, Organisation, Backups, Traceability (logging), Partitioning data, Protecting against non-human sources of risks.

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

Limited, Adequate control measures have been taken to mitigate and/or control the risk of disappearance of data.

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

Limited, Adequate control measures have been taken to mitigate and/or control the likelihood of disappearance of data.

Evaluation:Improvable

Action plan/corrective actions:

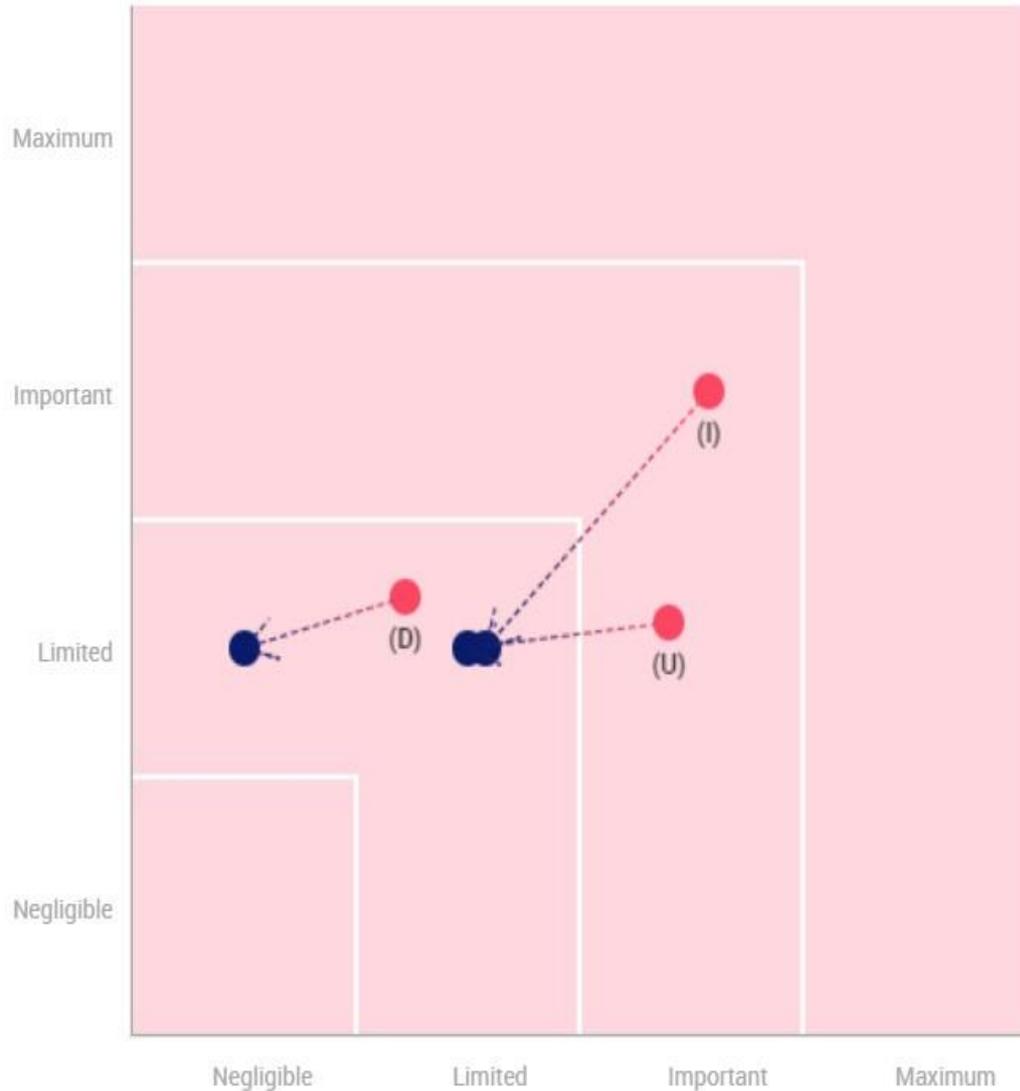
According to the available information, adequate measures have been taken to mitigate and/or control the risk of data disappearance.

Taking into account the action plan, how do you re-evaluate the seriousness of this risk (Data disappearance)? **Limited**

Taking into account the action plan, how do you re-evaluate the likelihood of this risk (Data disappearance)? **Negligible**

3.3 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

09/09/2020

Risks - Illegitimate access to data

Action plan/corrective actions:

According to the available information, additional measures are needed to properly meet the requirements for the protection of the data.

Taking into account the action plan, how do you re-evaluate the seriousness of this risk (Illegitimate access to data)? **Limited**

Taking into account the action plan, how do you re-evaluate the likelihood of this risk (Illegitimate access to data)? **Limited**

Risks - Unwanted modification of data

Action plan/corrective actions:

According to the available information, adequate measures have been taken to mitigate and/or control the risk of modification of data.

Taking into account the action plan, how do you re-evaluate the seriousness of this risk (Unwanted modification of data)? **Limited**

Taking into account the action plan, how do you re-evaluate the likelihood of this risk (Unwanted modification of data)? **Limited**

Risks - Data disappearance

Action plan/corrective actions:

According to the available information, adequate measures have been taken to mitigate and/or control the risk of data disappearance.

Taking into account the action plan, how do you re-evaluate the seriousness of this risk (Data disappearance)? **Limited**

Taking into account the action plan, how do you re-evaluate the likelihood of this risk (Data disappearance)? **Negligible**

3.4 – Action plan

Existing or planned measures

Physical access control

Action plan / corrective actions:

Visitors who could have access to personal data should always be accompanied by an employee of SOMI.

Minimising the amount of personal data

Action plan / corrective actions:

In the current version, the App requests a full copy of the National ID for ID verification (cf. app purchase workflow). When asking for a copy of the National ID, the data subject should be requested to black out passport photo, passport number, national ID number and Machine Readable Zone in this copy or photo.

Traceability (logging)

Action plan / corrective actions:

All activities on the server should be logged in order to allow digital forensics in case of a data breach.

Logical access control

Action plan / corrective actions:

Clear roles and permissions for users with access to the database should be defined.

Partitioning data

Action plan / corrective actions:

Partitioning measures should be implemented in order to prevent the entire database of being leaked in case of a single security breach.

Anonymisation

Action plan / corrective actions:

Sensitive user information should be anonymised.

Encryption

Action plan / corrective actions:

All data collected from third parties should be encrypted using a strong algorithm (AES-256) and complex user-generated key that is not available to the data controller. Whenever the data collected from third parties is processed, the data subject should be asked to give his/her user-generated key.

Policy

Action plan / corrective actions:

Based on this Data Protection Impact Assessment, an information security plan should be rolled out prioritising the measures stipulated in the action plan (cf. infra).

Part 4 – Validation

DPO opinion

DPO's name

Koen Hostyn

koen@privacyforall.be

DPO's opinion

Adequate measures have been taken to ensure data subjects' rights and freedoms using the current version of the App. Additional measures and an action plan have been formulated to provide additional safeguards when subsequent versions of the App (with additional features) will be launched.

The search of concerned people opinion

A debug version of the App was submitted to a number of peers of SOMI for feedback, however, a concerned people opinion consultation has not been performed.

Any additional questions or concerns can be submitted to privacy@somi.nl