DATA PROTECTION POLICY HBITS

Index

DATA PROTECTION POLICY HBITS

A Data Protection Policy (DPP) is designed to consider potential data protection and privacy impacts of processes and projects. It combines instruments like Data Protection Impact Assessment (DPIA), Data Management Plan (DMP) and Privacy Policy documentation. A Data Protection Policy is a deep dive to achieve protection goals but also a method for recording (identified) risks, issues and the safeguarding factors introduced to alleviate such concerns or potential impacts.

This document is a living document. It will be updated at least every year, or when necessary (e.g. after an evaluation, expertise or incident).

Last version: 01 June 2021

1 hbits CV

This DPP is related to the work of *hbits* (hbits CV). As part of its social responsibility *hbits* wants to operate in line with the data protection laws, regulation and rules as described in the General Data Protection Regulation (GDPR) and the national law(s).

hbits is a research company based in Belgium with address Witte Patersstraat 4, 1040 Etterbeek and company registration number (VAT) BE0712.734.818, and is related to the Vrije Universiteit Brussel (VUB) as the officially recognized Spin-Off of the Research Group TOR of the Sociology Department.

The main function of *hbits* is to collect insights on how people behave in their daily life and in which context their actions take place. Therefore *hbits* depends on the collection and analysis of information about people. The protection of peoples identity is one of the important actions to keep the respondents' and public's confidence.

To collect and analyze this information hbits mainly makes use of the MOTUS platform as it is able to collect survey data, time diary data and sensor data. *hbits* is the licensee of the MOTUS platform (more information https://www.motusresearch.io), and the related BEHAVE platform (more information https://www.be-have.io) which provides respondents for the researches ran via the MOTUS platform. VUB is the product owner of both platforms, and therefore besides *hbits* also the Research Group TOR of VUB uses the platforms for their research purposes. To settle this the usage of the platforms a Joint Data controller Agreement between VUB and *hbits* is in place.

For the projects and researches that *hbits* performs in relation to VUB projects and researches, the DPO of the VUB is in charge. In case of any data breach or complaints the VUB DPO is to be contacted (as well).

Nevertheless *hbits* holds a DPP as an independent research company. This document will describe the DPP of *hbits*, incorporating various other security and privacy related documents.

2 Introduction

Data protection laws require a DPP to be completed to assess proposed measures that pose particular risks relating to how personal data is used. This includes a (full) DPIA.

It is essential that each person, client, employee, supplier or other persons and/or organization that comes in contact with *hbits* has an oversight of the scope of the projects and researches that run within *hbits*. The responsibility for completing and respecting the DPP ultimately falls with the Executive Board of *hbits*.

This document describes the minimum standards of how personal data must be processed, collected, handled and stored to meet *hbits* data protection standards.

Anyone who works for *hbits* has a responsibility for ensuring personal data are collected, stored and handled appropriately.

Data users are obliged to comply with *hbits*' DPP when processing personal data on *hbits*' behalf. An agreement has to be signed defining possible disciplinary actions in case of a breach.

3 Identification of the need of a DPIA

Article 35 of the General Data Protection Regulation (GDPR) prescribes that a DPIA shall be conducted by a controller where a type of data processing, in particular using new technologies, is likely to result in a high risk to the rights and freedoms of individuals.

As a controller, under the GDPR an organization will need to assess, decide and document whether a DPIA is necessary for each proposed data processing operation. Although *hbits* states that no individual nor organization face a high risk to their rights and freedom it acknowledge that most of the projects or researches have a benefit in conducting a DPIA.

Especially when

- systematically monitoring, tracking and observing individuals' location and behavior, and

- combining, linking or cross-referencing separate datasets where such linking significantly contributes to or is used for profiling or behavioral analysis of individuals

are two of the elements on an EU-privacy regulators' list describing to have a high(er) risk to the rights and freedoms of individuals pursuant to GDPR Article 35(1).

4 Processing personal data

The main activity of *hbits* is to collect information on the behavior of people within a contextualized setting. During the respondents' participation personal data, research data and user data are being collect, stored and processed. All data are dealt with properly, irrespective of how they are collected, recorded and processed.

The Privacy Policy MOTUS gives a detailed overview on the personal data that are collected, as well as on the research data and the user data. This Privacy Policy is updated when necessary.

To arrive data security, *hbits* follows privacy- and security protection goals aligned with the data protection principles defined in article 5 GDPR. The goal is to receive and maintain the confidence of individuals. This document discusses seven protection goals within 2 level. Below the levels are explained.

GDPR considers respondents as 'Data Subjects'. However Data Subjects are a general term for respondents, employees/consultants, market contacts and organizations from which *hbits* holds personal data. This document will mainly discuss the protection of personal data of respondents[1]. They will also be addressed as 'individuals' and 'persons' and can be part of a group.

4.1 Risk of IT security

3 of the goals are related to IT security:

(1) Availability
is the requirement that personal data must be available and can be used properly in the intended process. The data must be accessible to authorized parties and the methods intended for their processing must be applied.

(2) Integrity

[1] Source for definitions used under 'Risk of IT security' and 'Data protection goals': https://www.rug.nl/research/research-data-management/downloads/c2-dataprotection-dl/dpia_guidance_doc_v1_pub.pdf

refers, (i) to the requirement that information technology processes and systems continuously comply with the specifications that have been determined for the execution of their intended functions. (ii) the data to be processed remain intact, complete, and up-to-date.

(3) Confidentiality
refers to the requirement that no person is allowed to access personal data without authorization. It ensures the protection against unauthorized and unlawful processing.

4.2 Data protection goals

4 of the goals are related to data protection goals:

(4) Data minimization
is the requirement to collect, process and use only personal data than are necessary for the achievement of the purpose of the processing.

(5) Unlinkability
refers to the requirement that data shall be processed and analyzed only for the purpose for which they were collected.

(6) Transparency
is necessary for the monitoring and control of data, processes, and systems from their origin to their erasure and is a prerequisite for lawful data processing. Transparency of the entire data processing operation and of the parties involved can help ensure that Data Subjects and supervisory authorities can identify deficiencies and, if necessary, demand appropriate procedural changes.

(7) Intervenability
refers to the requirement that Data Subjects are effectively granted their rights to notification, information, rectification, blocking and erasure at any time, and that the controller is obliged to implement the appropriate measures.

Below *hbits* shows how is dealt with these privacy- and security protection goals.

5 Data minimization

5.1 Automated processing operations following a data collection strategy

Via MOTUS *hbits* is particular focused on the collection of survey and time use data, and this from individuals or groups of people (like households, teams or organizations). Diary

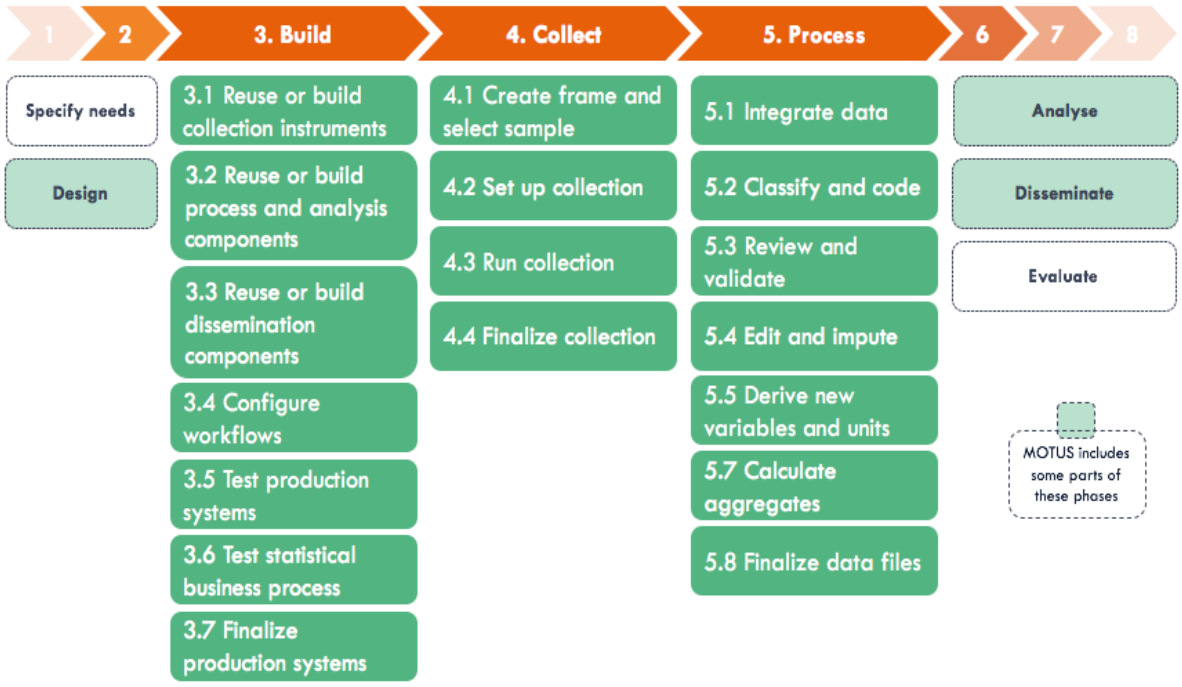
data combine activity data (What people do?) and contextual data (Where, With whom, How, Why, ...).

Data can be collected actively and passively. Active means that data are registered by the respondent him/herself. Respondents make use of the MOTUS web and/or mobile application. Passive means that data is collected via internet connected devices or sensors, or that external databases are linked. An example is location tracking from respondents. Active and passive data streams can be combined within a research and the gathered information can be presented to the respondents in the MOTUS applications.

In the MOTUS back-office the researches are developed: the research components (questionnaires, diary, context, communication) are defined, a fieldwork flow is designed for automated operations and data management is programmed and organized. MOTUS makes it possible to define multiple researches, that can run at the same time, even within the same respondent (for panel research purposes).

MOTUS is able to perform an important number of tasks and subtasks within the process of statistical production. To inform interested parties MOTUS is mapped on the GSBPM-architecture, developed by UNECE, EUROSTAT and OECD. The Generic Statistical Business Process Model (GSBPM) is a means to describe statistics production in a general and process-oriented way. It is used both within and between statistical offices as a common basis for work with statistics production in different ways, such as quality, efficiency, standardization, and process-orientation.

The figure below shows the main phases Build, Collect and Process in which MOTUS provides a service. Also in Design, Analyze and Disseminate MOTUS can play a role.



MOTUS collects new data, and can reuse earlier collected data. Respondents can be newly invited, but can also accept to be reinvited and even become a BEHAVE panel member. These respondents give consent for data collection and research purposes to store and use their personal, research and user data throughout their membership.

The amount of respondents that (can) interact with MOTUS (over time) is undefined.

5.2 Reduction of collected attributes of the data subject

hbits uses MOTUS in various projects. Each project can have its own specifics but the way in which data are collected and how the information flows run, does not exceed the information provided within this DPP. As an example not all researches make use of sensor data. In that case no passive data flow is necessary.

Each individual project has a detailed information fiche to inform the respondents. This information is presented during the invitation, on our webpage and in the applications. The data that is collected from the respondent is related to the research question within a research.

No more information is asked from the respondent then necessary, and the respondent has always an overview of the research tasks to be fulfilled within the research. All actions within the participation to a research are on a voluntary basis. At any time during the participation to a research respondents have an overview of the given information. Also,

for each specific research a Privacy Policy (or an addendum to the General Privacy Policy MOTUS) is defined.

Respondents can contact the responsible researcher via a contact page, via email and when available via telephone.

5.3 Procedures for pseudonymization and anonymization

The effectiveness (and legality) of both anonymization and pseudonymization hinge on their abilities to protect respondent from re-identification.

To achieve this MOTUS works with Universal Unique Identifiers (UUID), and this on 2 levels. Every respondent in MOTUS receives an UUID, every research has a research UUID. Personal and research data are not present in one database. Only based on the UUIDs for respondents and researches personal data and research data can be merged.

When the data collection and data cleaning period is finalized personal data and research data are removed, unless different-wise determined in a contract, from MOTUS and stored in a data archive.

5.4 Storage period

A difference is made between personal data and research data. Research data can also contain anonymized personal data.

For the projects hbits executes independently of VUB, the storage period for projects and researches is defined as follows:

- Personal data
  Based on necessity (data collection, data cleaning), based on a contractual agreement with the respondent (e.g. BEHAVE panel)
- Research data
  Unlimited

For the projects that are executed together with VUB

- Personal data
  Based on necessity (data collection, data cleaning), based on a contractual agreement with the respondent (e.g. BEHAVE panel)
- Research data
  10 years

6 Transparency

6.1 Architecture and data flows

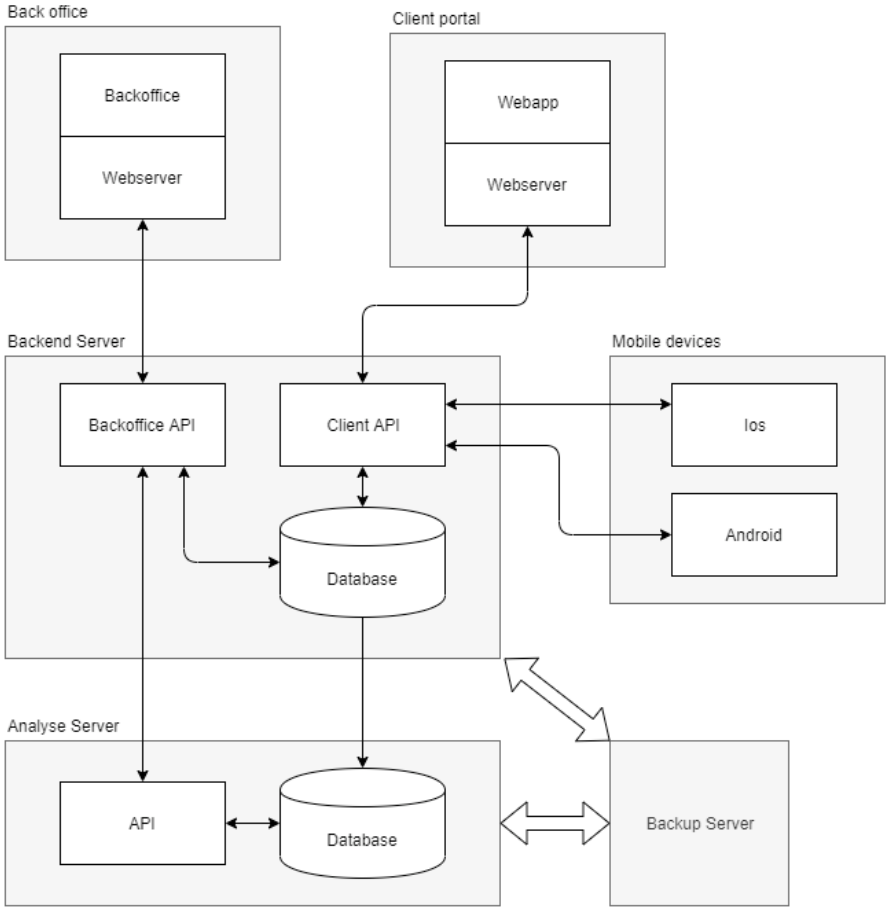
For the data collection and storing of the data MOTUS employs two types of architectures: a monolithic and microservice architecture. When a project or research is finished the data is transferred to a data archive.

6.1.1 Monolithic architecture

The first architecture combines in total 6 components or modules:

- Backend server: the backend server stands central in the MOTUS platform. It holds the database, the back-office API and the client API.
- Back-office: the back-office serves as the research environment where the researcher sets up a research and the fieldwork can be followed. The back-office runs in a browser.
- Analyze server: the analyze server holds a replicate of the database of the backend server and prepares the reports for the backend server, which at its part can be called by the back-office.
- Back-up server: the back-up server is a replicate for secure storing from the backend server and the analyze server.
- Client portal: the client portal holds the MOTUS-web application and an underlying webserver.
- Mobile devices: the mobile application is available for Android and iOS.

All together this is called the MOTUS platform.



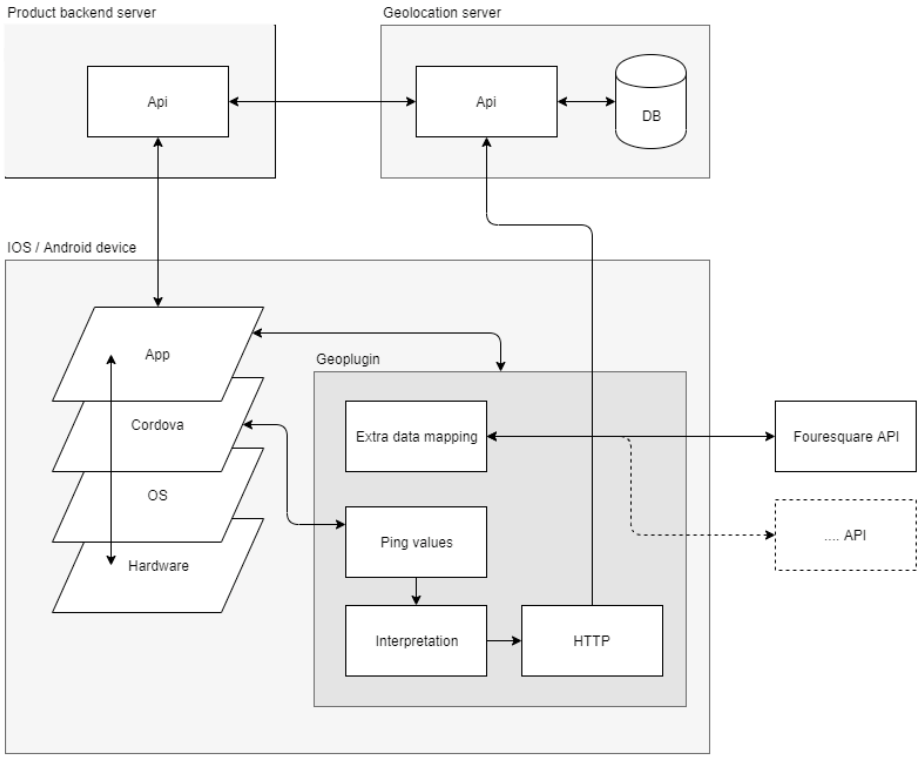
There are three API's that arrange the entrance to the components:

- Backoffice API: both ways webserver back-office and analyze server
- Analyze server API: both ways database (to prepare reports) and back-office API to send over reports and other analytics.
- Client API: Receives the input from the web & mobile app and syncs the data on both applications. It could also function as a data harmonization tool.

6.1.2 Microservice architecture

Microservices are small and independent services handling a particular problem or performing a certain/specific task. Via an API the collected data is presented to the monolithic architecture.

These microservices can be external data sources to MOTUS. However often these microservices are developed in function of MOTUS.



An example is location tracking where the sensor of a respondents' smartphone collects information on the position of the respondent. Also external databases can be connected, like Foursquare or Google to provide extra context.

Every microservice has its own server, database and processing. The connection with the MOTUS core is done via a Rest API. In this way no (personal) data is communicated with the microservice, only the UUID to be able to match the data in the backend server of the monolithic architecture.

6.1.3 Data input and output

MOTUS is a protected environment. All input and output is controlled. Nevertheless there are 3 processes that are linked to MOTUS :

(1) provided input to MOTUS (eg. registration, opt-in, administrative data, sensor data, …)
(2) output internally used within MOTUS (eg. invitation emails, internal dashboard, …)
(3) output made available by MOTUS to externals (eg. research data, external dashboard, …)

6.1.4 Data archive

After the data collection and cleaning phase personal data and research data are erased from the MOTUS environment.

Data are stored in a self-hosted data archive.

6.2 Privacy by design and default

hbits uses a Privacy by Design and Default approach in all its work, but in particular when:

- building new IT systems for storing or accessing personal data;
- developing new applications or research approaches;
- embarking on a data sharing initiative; or
- using data for new purposes.

Privacy by design is an approach to projects that promotes privacy and data protection compliance from the start. It is a key consideration in the early stages of any project, and then throughout its lifecycle.

Taking a privacy by design approach is an essential tool in minimizing privacy risks and building trust and will designing projects, processes, products or systems with privacy in mind from the outset .

6.3 External service providers and third parties

6.3.1 Server provider

hbits makes use of the services of Contabo. MOTUS runs on VPS certified servers.

More information can be found on the service's website: https://www.contabo.com

6.3.2 Email service

hbits makes use of the services of Mailgun to send and track emails to/from respondents.

More information can be found on the service's website: https://www.mailgun.com

6.3.3 External databases

There are various external databases *hbits* works with:

- Administrative databases provided to hbits

  These databases can contain personal data, research data or user data. The acceptance of this data is based on the given consent to the provider of these data.

  For each research the respondent is notified from which organization the data is received in order for the respondent to make a claim on their respective rights. An example is employee data from the VUB.

- Content databases

  These databases contain extra context to the answers/information the respondents have provided to MOTUS.

  For each research the respondent is shown an overview of the services that are used within that research, and how it relates to the protection of their data. An example of a content database is the Places API of Google, or the OverPass API of OpenStreetMap.

  MOTUS acts as an in-between the respondent and the external service. MOTUS anonymizes the respondent in contact with the external service provider.

6.4 Data transfer contracts

hbits is a spin-off of the Research Group TOR of VUB. Via a joint controller agreement Personal Data is shared with and can be processed by VUB. This makes VUB an important stakeholder. VUB and hbits can also outsource work between the two organizations.

Other important stakeholders are statistical organizations (like Statbel or Eurostat), which are important due to a joint development trajectory.

In case of a transfer of personal data recipient can only use the data for the defined purposes. The receiving party has to maintain a data protection level in line with the GDPR to be able to accept the data.

Where personal data are transmitted by a third party (like a sample supplier) to *hbits*, these personal data can only be used for the intended purpose.

There are no other contracts or agreements for the transferring of personal data. Personal data can be merged with research data only when pseudonymized or anonymized.

The conditions for transferring research data are specified in the Privacy Policy MOTUS. *hbits* acts conform the EU data protection shield.

6.5 Overview of consents and objections

A lawful base for processing personal data is obligatory. *hbits* requests a lawful base for every research.

Each running research via MOTUS is listed, and the consents are provided via https://www.motusresearch.io. In case of objections a summary is provided.

Non-MOTUS researches have an informed consent as well, but are not part of the list.

7 Availability

7.1 Data storage and backup

The following server settings apply:

For the backend server:

- VPS
  Linux: Debian 9 // Updated to CentOS (free version of Redhat)
- Ten core CPU
- 60GB RAM
- Disk storage: 1600GBPort/bandwidth: 1Gbit/s

For the backup server:

- VPS
- 2x100GB back-up space
- Internal network only

7.2 Repair strategies and alternative processes

Data collected via the backend VPS server of MOTUS is automatically replicated at the backup VPS server.

Pseudonymized or anonymized data is stored in a data archive in relation to the storage time. Archived data are accompanied with meta-data information and a technical report. A technical report includes also a description of privacy preserving actions.

7.3 Configurations and data structures

MOTUS uses a relational database to store all gathered information of the respondents. Personal data and research data are not present in the same database. The matching of the information can only be done via source code and MOTUS internal processes, or manually via an UUID-key. This key is only available to the Admin role.

MOTUS data is stored in a MySQL MariaDB, running on a certified VPS-servers. The performance, updates and security level of the servers is monitored via IT specialists working for *hbits*.

7.4 Protection against external influences

MOTUS takes into account a number of security measures.

Connection to the MOTUS backend database is only allowed from application or analysis server. No external connections to the database are allowed.

Each user application (respondent web frontend, web app, registration website, …) has a unique API key, with configurable rights.

Data transmission is done via a respondent unique UUID key. Data is transmitted over a https protocol which an SSL/TLS encryption layer. The SSL connection encrypts and decrypts requests and responses.

The JSON encoding standard is used to transmit pieces of data between the MOTUS-components.

Actions are undertaken against DDoS attacks.

8 Integrity

8.1 Maintainability strategy

Maintainability deals with the easiness to maintain and (even) further develop the software platform. One aspect is the choice of the programming language. For its front and back-office MOTUS makes use of the frameworks Angular, Ionic, jQuery and Koseven.

The code is documented in Github, and uses code history to track changes in the source code. Particularly important is that the logic between the web and mobile logic is stored in

a common library to improve maintainability, and/or to organize the work between collaborators, whereas the design code has been separated for web and mobile.

Another aspect is the organization of responsibilities via a release management process. This process takes in to account the following elements:

- Deployment strategy
  MOTUS today uses a 2-stage deployment strategy having a development and production environment. In the future a more phased deployment would have benefits including substages for rollout, testing, and rollback in case of problems.

- Modularity client-server
  MOTUS aspires to a 3-tier application architecture. A 3-tier application architecture is a modular client-server architecture that consists of 3 parts:
  - a presentation/client tier: includes the graphical user interface, and communicates (API) with the other tiers
  - an application tier: includes the business logic
  - a data tier: includes information storage

- Agile management
  hbits organizes development stories via an iterative and incremental method of managing new stories, new actions and bugs using Github and Jira. *hbits* also applies (the development of) Unit Testing.

8.2 Documented assigned of rights and roles

Roles are assigned on the Admin level, the group level and the research level. These levels are documented in the MOTUS manual. On the research level another set of rights are defined, 12 at the moment.

On the research level rights and roles are based on the task profiles of an employee or researchers.

An overview is documented of the rights and roles permitted.

8.3 Workflow and profiles

An user guideline on the back-office of MOTUS is available to employees, both of *hbits* as for the Research Group TOR of VUB.

Research components are inventoried in a library and research flows are described in a technical and meta-data documentation.

hbits provides training to its employees and researchers of the Research Group TOR of VUB.

8.4 Security tests

MOTUS has been tested by T-Systems.

9 Confidentiality

9.1 Data secrecy

Personal data are subject to data secrecy. Any unauthorized collection, processing, or use of such data by employees/consultants is prohibited. Any data processing undertaken by an employee/consultant that he/she has not been authorized to carry out as part of his/her legitimate duties is unauthorized. The "need-to-know" principle applies. Employees/consultants may have access to personal data only as is appropriate for the type and scope of the task in question. This requires a careful breakdown and separation, as well as in limitation, of roles and responsibilities.

Employees/consultants are forbidden to use Personal Data for their own private or commercial purposes, to disclose them to unauthorized persons, or to make them available in any other way. Supervisors must inform the employees/consultants at the start of the employment relationship about the obligation to maintain data secrecy. This obligation shall remain in force even after employment has ended. The employment/consultant agreements contain appropriate confidentiality obligations.

9.2 Assignment of rights and roles

4 environments are of importance:

- Backoffice of MOTUS
- Repository of MOTUS
- Server and database
- Data archive *hbits*

9.2.1 MOTUS back-office

This environment is also role protected.

Admin role MOTUS:

- Joeri Minnen – Managing Director

- Ignace Glorieux – Professor at Research Group TOR
- Theun Pieter van Tienoven – Research Director at Research Group TOR

Admin role Research:
- One research responsible for each research

Role distinction between two teams responsible for:
- Data collection
- Data valorization

Besides the Admins no one can be part of both teams within the same research. For every person a more specific role distinction can be specified based on the task description of the person.

9.2.2 Repository source code

The source code is stored in a Github private repository. The Github is accessible for the IT-developers of MOTUS.

9.2.3 Server and database

The servers of MOTUS are present in the Contabo Data Center in Germany. The control panel is available for the IT-developers of MOTUS.

Unauthorized physical entrance is not possible.

9.2.4 Data archive

The data archive runs on a self-hosted server.

The entrance to the data archive is protected via credentials and a 2-step verification. Entrance is allowed for:
- Joeri Minnen – Managing Director
- Ignace Glorieux – Professor at Research Group TOR
- Theun Pieter van Tienoven – Research Director at Research Group TOR

9.3 Definition of organizational procedures

Every *hbits* employee/consultant has signed a confidentiality contract. The same counts for the researchers of the Research Group TOR of the Vrije Universiteit Brussel.

9.4 Implementation of a secure authentication process

Both the respondents and the researchers have to authenticate against either the front- or the back-office to make use of the service. In both instances confidentiality and data integrity are essential.

To meet this criteria, user credentials are issued by MOTUS while these settings can be modified for every different research. Initial credentials are provided to the user by letter or e-mail. Users can change their username/password via the applications. As a setting this password change can be mandatory.

Passwords are encrypted in the database. Each user application has his own unique API-key, as is the same for every respondent. Username and identifier are connected in the database. Connection to the database is strictly ruled.

MOTUS front-office:

- Login with username and/or email + password
- Logins are linked to researches

10 Password are encrypted in the database

- Initial passwords are auto-generated and can contain numbers, characters and signs

The back-office of MOTUS for researchers requires an extra 2-factor authentication.

MOTUS back-office:

- Login for admins with username and/or email + password
- Password are encrypted in the database
- Requires 2-factor authentication
- User role restrictions

Backup tokens can also be created.

10.1 Encryption strategy for stored and transferred data

Passwords and recovery codes are stored by concatenating with the salt and encrypting the result. Information is not encrypted in the database to retain a high performance of the database in the communication with the different front-office options.

Data is transmitted over a https protocol which an SSL/TLS encryption layer. The SSL connection encrypts and decrypts requests and responses.

Any respondent can ask by a simple request to be deleted. If a respondent is deleted from the database all data that is linked to this respondent is deleted from the research and database. MOTUS does not apply soft deletion, the data is fully removed.

11 Unlinkability

11.1 Restriction of processing, utilization and transfer rights

MOTUS is a research platform helpful in the organization of different researches, in the build-up of a research, in the collection and the processing of data.

The qualities of the MOTUS platform can be used for every research. This leads to efficiency but also to better protocols and harmonization of input and output.

Transfer of research components via a library is freely available. The transfer of personal data and research data can be restricted. Besides roles and rights on the person level also rights can be defined on the research level and on the group level. Individual researches can be made invisible and/or can be locked. When researches are related to a group of users, all researches of the group are visible or locked to others.

If the entrance to researches are restricted, no personal or research data can be seen, downloaded or transferred.

11.2 Separation of organization/departmental boundaries

hbits is at this point in time a fairly small research company, and the Research Group TOR of VUB is group of researchers, pre-docs and post-docs. A clear separation between *hbits* and TOR is achieved. For the projects and researches to which *hbits* and TOR share responsibilities a joint controller agreement is in place.

The Admin is able to put further restrictions on the boundaries between the current work organization and work flows, and will update these restrictions/boundaries in the future when necessary.

11.3 Anonymization and pseudonymization strategy

At the moment respondents credentials are created (username and password) also a UUID is attached to the respondent. With this UUID different kinds of information stored and collected from the respondent can be linked during the data collection and data cleaning process.

After the data collection is finalized 2 strategies can be applied:

- Anonymization: information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the Data Subject is not or no longer identifiable. Also the UUID of the respondent is transformed.
- Pseudonymization: processing of personal data in such a manner that the personal data can no longer be attributed to a specific respondent without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person. Personal data are stored separately together with the UUID of the respondent. The new database holds the anonymized data and the UUID. Linkage between with the personal data remains possible on a later moment.

For each research the respondent is informed about the strategy and the consent of the respondent is asked.

12 Intervenability

Every respondent has the following rights. Their request is to be handled immediately by *hbits* and may not result in any disadvantage to the respondent. Where the relevant personal data are not being processed by *hbits* the relevant client contract must be consulted in respect of any process to be followed and the client has to be informed about such request immediately.

- Right of access
  The respondents may request information on which personal data relating to him/her have been stored, how the data were collected and for what purpose. If personal data are transmitted to 3rd parties, information must be given about the identity of the recipient or the categories of recipients.

- Right to rectification
  If personal data are incorrect or incomplete, the respondent can demand that they are corrected or supplemented.

- Right to withdraw consent
  Where the personal data are processed on the basis of consent, the respondent can object to the processing at any time. These personal data must be blocked from the processing that has been objected to.

- Right to erasure
  The respondent may request his or her data to be deleted if the processing of such data has no legal basis, or if the legal basis has ceased to apply. The same applies if

the purpose behind the data processing has lapsed or ceased to be applicable for other reasons. Existing retention periods and conflicting interests meriting protection must be observed.

- Right to object
  The respondent generally has a right to object to his/her data being processed and this must be taken into account if the protection of his/her interest takes precedence over the interests of the data controller owing to the particular personal situation. This does not apply, if a legal provision requires that the personal data are data to be processed.

- Right to data portability
  The respondent has the right to request for the personal data provided by him/her to be made available to such respondent in a easily readable format, like a Word or Excel document.

13 Legal grounds for Data Processing

hbits collects, process and uses personal data only under a legal basis. A distinction is made between respondents, data provided by clients, employee data and marketing contacts.

13.1 Respondent data

Respondents are the most common Data Subjects for hbits. The legal grounds to collect process and use personal data are related to:

- Informed consent
  Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to the respondent.
  The respondent gives a clear affirmative act by means of an active motion or declaration. Examples are ticking a box on a (digital) form, or a written or oral statement, which clearly indicate the respondents acceptance of the proposed processing of their personal data.

- Contractual relationship
  Personal data can be processed within the context of a contract to which the respondents is a party, to fulfil relevant obligations and rights.
  This is the case when respondents are willing to be part of the BEHAVE panel, which is connected to MOTUS. More information is available in the Privacy Policy BEHAVE.

hbits mainly uses a web app, mobile app and connected devices to collect personal data and to process and use this information. The respondent is informed by the Privacy Policy MOTUS and the information fiche for every specific research.

The privacy statement and any cookie information are available so that it is easy to identify, directly accessible, easily understandable and consistently available by and for the respondent.

The same counts for the tracking of respondents via the web app, mobile app and connected devices. *hbits* uses a pseudonym for the respondent, but nevertheless the respondent can opt out of this data collection.

13.2 Personal data provided by clients

hbits is considered the processor when personal data are provided by a client, and can only process these data in line with the instructions agreed with or received from the client.

The received data are subject to the same data protection goals that are applied within *hbits*.

13.3 Employment relationship

Personal data is processed to initiate, carry out and terminate the employment agreement. This also applies to consultancy agreements.

13.4 Marketing contacts

hbits treats marketing contacts no different than respondents in respect of the privacy protections accorded to them.

14 Data incident and recovery plan

14.1 Security breach

A security breach happens when personal data has been lost, or there has been unlawful processing (security incident). This happens when there is:

- A destruction or loss of personal data
  E.g.: Data center fire, accidental deletion of a file without backup
- Damage, unauthorized access, incorrect provision
  E.g.: Loss of USB stick, stolen laptop, malware, hack, email to wrong recipient

14.2 Breach management

The following actions apply to prevent incidents

- Automated check for hack, malware, …
- Reporting every internal incident to a fixed contact person
- Creation of internal procedures and training/awareness
- Agreements on reporting external security incidents

To this end a registration form and a key personal contact list is available. This also includes a list of external contacts if necessary.

14.3 Breach investigation

The following questions apply to get a full picture of the security breach:

- Description of what exactly has happened to the data
- Description of the nature of the personal data affected
  E.g.: Special data, personal data of sensitive nature
- Description of the extent of the incident
  E.g.: Number of people affected, amount of data affected per person, is the affected data shared within a chain?
- Description of the category of persons affected
  E.g. Respondents, employees, clients, market contacts
- Description on the impact on those affected
- E.g. Vulnerable groups, financial loss, material/immaterial damage

14.4 Breach repairing

14.4.1 Measures to limit the consequences of the incident

The flowing measures apply:

- Reporting to the DPO and the Authority for the Protection of Personal Data.
- The persons affected by the data breach must be informed if the security breach is likely to have an adverse effect on their privacy.
- Inform affected persons on how to protect themselves to this infringement.

In case of negative consequences for the affected persons a report has to be done withing 72 hours after the security breach to the Authority for the Protection of Personal Data and the DPO.

Measures also involves communication to the outside world if necessary. It also involves the coverage for third-party liability, own costs, and possible fines.

14.4.2 Prevent similar incidents in the future

Prevention measures apply:

- Plan updating
- Plan documentation storage
- Improve backup strategy
- Renew risk management
- Document triggering events
- Plan emergency response team