



## *Deliverable 3.3*

### Security and Privacy Policy

<b>Project Number</b>	AAL-2012-5-249
<b>Project Name</b>	MyLifeMyWay
<b>Duration</b>	March 2016 – Feb 2019 (36 Months)
<b>Coordinator</b>	ENGIE
<b>Document ID</b>	D 3.3
<b>Release Number /Date</b>	V1.0/April 2018
<b>Checked and released by</b>	Daniel Bolliger
<b>Document Type</b>	Project Deliverable
<b>Original Due Date</b>	October 2017
<b>Dissemination Level</b>	Public
<b>Main Editor</b>	Daniel Bolliger (IHL)
<b>Contributing Partners</b>	HAN, SLG, UCLL, VIR, BON, DEV, IHL, ENG
<b>Reviewed by</b>	Contributors



**Abstract**

In the project MLMW there is data record, stored and evaluated. On one hand by operating the system (config and calendar data) and on the other hand evaluating the user interaction by data analysis (telemetry data and gathering information for research (questionnaires)).

It is of utmost importance, that the end user data is protected and privacy is guaranteed, all legal and ethical aspects are respected in all participating countries.

In this document the security and privacy principles are outlined. The consequential requirements are listed, the data flow is described, access and storage framework is shown, the end user informed consent presented and finally the actual situation in every country is depicted.

**What is new since the MTR in November 2017**

*The document presents at MTR in November (Version 0.1) was taken over in March from engie to IHL. As a reaction on the blocking issues list of the MTR report, we decided to completely rework this deliverable. The first version is presented for MTR II in April 2018 to the reviewers. The current (April 2018) GDPR situation of each organization is shown*

**© 2016 MyLifeMyWay Project Consortium.**

This document contains material, which is copyright of certain AAL MyLifeMyWay project consortium parties and may not be reproduced or copied without permission.

Neither the AAL MyLifeMyWay project consortium as a whole, nor a certain party of the AAL MyLifeMyWay project consortium warrant that the information contained in this document is capable of use, nor that use of the information is free from risk, and accepts no liability for loss or damage suffered by any person using the information.

**The MyLifeMyWay project is Co-funded by the European AAL Joint Programme**

<b>Version</b>	<b>Date</b>	<b>Changes</b>	<b>Name</b>	<b>Organisation</b>
0.1	October 2017	Initial Creation	Arzu Barské	ENGIE
0.2	February 2018	Revise /GDPR update and quality check	Arzu Barské	ENGIE
0.3	March 2018	Take over from Azru and reorganize	Daniel Bolliger	IHL
<b>1.0</b>	<b>April 2018</b>	<b>Include all country specific GDPR clarifications</b>	<b>Daniel Bolliger</b>	<b>IHL</b>



**List of Authors**

- Arzu Barske (Engie)
- Camille Zeugers (ENG)
- Daniel Bolliger (iHomeLab)
- Evi Verdonck (UCLL)
- Herman Slagman (VIR)
- Marc Flaeminck (SLG)
- Marco Mans (ENG)
- Marian Adriaansen (HAN)
- Sylvia Hoekstra (HAN)
- Renilde Rottiers (SLG)

**Content:**

- 1 Executive Summary ..... 4
- 2 Principles and Guidelines ..... 5
- 3 Security and Privacy Requirements ..... 7
- 4 Roles Within the Project ..... 9
  - 4.1 End Users ..... 9
  - 4.2 Supporter ..... 9
  - 4.3 System Administrator ..... 9
  - 4.4 Data Scientist ..... 9
  - 4.5 Researcher ..... 9
  - 4.6 Project Partners ..... 9
- 5 Data Within the Project ..... 11
  - 5.1 Informed Consent ..... 11
  - 5.2 Questionnaires ..... 11
  - 5.3 Focus Group and Interview Notes ..... 11
  - 5.4 Telemetry Data ..... 11
  - 5.5 Configuration Data ..... 11
  - 5.6 Google Account ..... 12
- 6 Data Access and Usage of Data ..... 12
- 7 System Overview ..... 13
- 8 Informed Consent ..... 14
  - 8.1 Proposal for extension of the informed consent ..... 14



8.1.1	Telemetry data .....	14
8.1.2	Use of Google-agenda .....	15
8.2	Procedure modifying informed consent .....	15
8.2.1	Replacing existing informed consent.....	16
8.3	Modified Informed Consent .....	16
9	GDPR Status .....	19
9.1	Situation in Belgium.....	19
9.2	Situation NL .....	21
9.3	Situation CH.....	24
9.4	GDPR next Steps .....	26
10	Appendix.....	27
10.1	Privacy Policy of HAN .....	27
10.2	Data Protection Policy of HAN .....	36
10.3	Data and system usage of HAN .....	63
10.4	Data Management Plan of HAN .....	68
10.5	Engie GDPR and AVG Compliance Declaration.....	87





# 1 Executive Summary

Already stated in the project proposal, MLMW project undertakes all actions and efforts, in order to respect privacy and dignity of its end users as highest principle.

The legislation changed in EU during the course of the project, and the new GDPR legislation enters into force on May 2018. Therefore the experts recommended to clarify the juridical situation of MLMW in order to ensure the compliance with all laws during the field tests and then afterwards by entering the market with MLMW as a commercial product.

So we can conclude that privacy, security of the end user data, as well as the dignity of the end users is very well respected within the MLMW project and that there are no major obstacles to roll out the product after finalization of the project as a commercial product to the market.

In this deliverable the information is compiled about security and privacy.

Chapter 2 discuss the principles and guidelines

- Data security and encryption is fundamental
- Privacy is Priority

Chapter 3 enrolls all Security and Privacy Requirements derived from the Principles. They are then also part of the D2.3 Unified Requirements.

Chapter 4 depicts all human actors relevant in the context of our system MLMW

Chapter 5 describes all kind of data used in the project. That are data for operating the system (setup data), automatic registration of telemetry data and the data gathered by the field research activities (questionnaires, interviews...)

In chapter 6 the access and usage of the different actors on data is explained in a matrix

Chapter 7 gives a graphical overview over the whole system in respect to privacy and security.

Chapter 8 describes in detail the new informed consent, given to all end users, before starting research with them. It is updated with the required amendments as result of the discussions with the data protection officers last half year.

In chapter 9 the current status towards data protection and privacy is given for each partner organization.



## 2 Principles and Guidelines

The general principles in building a system for MyLifeMyWay (MLMW) is already described in the *project proposal, Chapter 3.4 Ethical and Legal Issues*:

*MyLife,MyWay touches on sensitive ethical issues because direct user participation is seen as a key aspect within the project. End-users will provide private data on their daily routine, limitations and so forth. The consortium therefore agreed to respect and protect human dignity, including informational self-determination in line with the principles and case law of the European Convention of Human Rights and the EU Charter of Fundamental Rights,*

...

*The measurement, processing and storage of personal data are subject to the European Data Protection Directive and the respective national implementations thereof. These regulations will be taken into consideration in the project and its pilot implementations by any of the partner organisations.*

...

*MyLife,MyWay will direct special attention to identify critical privacy and confidentiality requirements of data with respect to information flow security.*

*All partners will work with older adults as well as with their informal caregivers in Belgium, Switzerland and the Netherlands according to high ethical standards. User participation will target those groups of older adults that are legally capacitated and capable of giving informed consent. In order to ensure a common level of data protection, the project coordinator will set up a data protection agreement, incorporating the points raised above.*

...

*Every activity undertaken with the users will be fully compliant to the international and European and national privacy and data protection law.*

...

*Providing a PA to help older adults managing their daily activities can only work if the aims and wills of the people concerned are taken into account carefully. The provided solution should be prepared to support people but not to incapacitate them. Distributive justice and fairness in the access to the provided services should be considered throughout pilot implementations and commercial launch. Furthermore the directly and indirectly involved actors respectively users of data and information as well as their aims and wills have to be considered.*

Additionally in the section *3.3 Data Security and Encryption is Fundamental of (D3.1 System Requirements and Architecture Specification)*, the following basic principles are described:

### **Data security and encryption is fundamental**

*The safety of the data of the MyLifeMyWay users is a fundamental design goal of MyLife-MyWay. Protecting sensitive data is the end goal of almost all IT security measures. Two strong arguments for protecting sensitive data are to avoid identity theft and to protect privacy.*

*Therefore authentication, authorization and encryption are fundamental components of the MyLifeMyWay system architecture.*



## **Privacy is Priority**

*The evolution of Web technologies has increased collection, processing and publication of personal data. Privacy concerns are raised more often as applications built on the Web platform have access to more sensitive data — including location, health and social network information — and users' activity on the Web is ubiquitously tracked.*

*The privacy of MyLifeMyWay's users is therefore a paramount concern. MyLifeMyWay will not use any of the user's personal data for anything outside the core MyLifeMyWay system use cases – no advertising and no selling of data. The solution design will make sure that every user has only access to his own data and shares only the minimum information needed with other users to enable communication and interaction inside MyLifeMyWay. Other user related information is kept and stored during the project duration for internal analysis and development of collaborative intelligence algorithms only. ...*

*The system architecture needs to ensure that a single end-user device or a single end-user will never have access to other data than its own. Furthermore, the system architecture must take care of obfuscating data so that a single entry never can be traced back to a specific end-user or end-user device. This applies for secured data transmission as well as for aggregated data mentioned in the paragraph above.*

We extend these principles with the following important topics

### **New GDPR Legislation**

Our project is executed in three countries: Netherlands, Belgium and Switzerland. Each country has its special legislation rules for the appliance of data protection and privacy. Additionally, the legislation of the European Union is in force for Netherlands and Belgium. A new EU GDPR regulation coming into effect in May 2018. All involved organizations have a strong focus on the consequences of introduction of the new EU-GDPR at the current time (spring 2018). Therefore, for each country the actual GDPR state is depicted in chapter 9 of this deliverable. All responsible external experts are very busy with this introduction of GDPR and makes it a time consuming process. Therefore, some statements in Chapter 9 are not final and will be updated, as soon the answers of the specialists are available.

### **Proportionality of Data Usage and Controlled Access**

Data is collected on different aspects in the project. On one hand, we collect during the research activities of HAN, UCLL and IHL personal data, off the participants, about their vulnerability, daily habits and biography.

On the other hand, we are able to record user behavior on the MyLifeMyWay systems (telemetry) to enable AI analysis for the product improvement, as described in the proposal.

We do not aggregate the biographical research data with the telemetry data and vice versa, to keep privacy. The project members analyzing research data do not have access to the telemetry data and reverse. We strictly regulate the access on the different data sets.

The data is stored in a secure environment and not accessible to unauthorized personnel.



### 3 Security and Privacy Requirements

Taking into account all principles and guidelines compiled in chapter 2, a set of security and privacy requirements evolve. They have to be followed in the definition of the system architecture. We tried to focus on a set of 11 requirements, giving a reasonable frame for the project MyLifeMyWay and respect the dignity and privacy of all of the MLMW users in an optimal way. This set is shown in table below.

Topic	Requirements
<b>Compliance</b>	<p>The system must be compliant with</p> <ul style="list-style-type: none"> <li>the national data protection, privacy and ethical legislation in each participant country</li> <li>the EU GDPR regulations coming into effect in May 2018</li> </ul>
<b>Voluntariness</b>	<ul style="list-style-type: none"> <li>All persons taking part as users in the project MLMW must participate with their free will.</li> <li>They can quit the project without any drawback any time.</li> <li>They can request, that their stored, non-aggregated personal data can be deleted within a specific time frame on their request completely</li> </ul>
<b>Data Sharing</b>	<p>All data recorded and stored in this project</p> <ul style="list-style-type: none"> <li>must be kept in the protected project environment.</li> <li>is not allowed to be sold or used for advertisement purposes</li> </ul> <p>Data stored in the personal agenda can be shared by the end users selectively with their supporters.</p>
<b>Lifetime</b>	<ul style="list-style-type: none"> <li>All persona data, collected during the project must be deleted after the completion of the project. This is valid for configuration data, telemetry data, questionnaires, interview notes</li> <li>Aggregated data – not back-traceable to an individual user – can be kept beyond the project end. E.g. project reports, publications etc.</li> </ul>



<b>Pseudonymisation</b>	<ul style="list-style-type: none"> <li>• All data stored in any form must be pseudonymised</li> <li>• No clear text names are stored together with measurement data, questionnaires, telemetry data</li> <li>• The key between data sets and real persons must be stored securely, with access of clear defined authorized personnel</li> </ul>
<b>Transmission</b>	<ul style="list-style-type: none"> <li>• No clear text transmission of data between one and another system component is allowed</li> <li>• All data transmitted from one physical system component to another must utilize a secure transport layer. The applied techniques must be state of the art</li> </ul>
<b>Storage</b>	<ul style="list-style-type: none"> <li>• All data stored in paper form (notes, forms...) containing personal data must be kept in safe area. This means unauthorized access is prohibited in an efficient way.</li> <li>• Electronic stored data must be protected against unauthorized physical and electronic access with suitable technical measures</li> </ul>
<b>Access</b>	<ul style="list-style-type: none"> <li>• Access to the front and backend devices must be protected</li> <li>• An access scheme must be defined for each user group and each data type, to ensure adequate data usage.</li> </ul>
<b>Evaluation</b>	<ul style="list-style-type: none"> <li>• Evaluation of must be done on pseudonymised data only</li> <li>• Evaluation of the data must follow the principle of proportionality</li> </ul>
<b>Aggregation</b>	<ul style="list-style-type: none"> <li>• Usage data (telemetry) and research data (questionnaires, interviews) must not be aggregated for joint evaluation</li> </ul>

**Table 1: Security and Privacy Requirements**



## 4 Roles Within the Project

In this chapter all actors, playing a role in the project, are described. This are on one hand the primary users and their carers, but on the other hand also the project team and the system administrator. During the lifetime of the project they have access to different types of data. They are described in chapter 5.

In chapter 6 both views are combined and define the data access for the matrix of data types and user groups.

### 4.1 End Users

- Primary target group for MyLifeMyWay system
- Fragile but not too fragile persons who live at home with little external help or in a nursing home with low level of assistance
- Using the client device, where the PVA is running, to structure their daily life

### 4.2 Supporter

- Assist and support the end users.
- This can be a neighbor, relatives, living service provider, care giver
- They support end users by administering the content of Anne and helping the end user to operate the system. E.g. enter calendar details
- The end user organisations recruit end users and in the project often take the role as supporter

### 4.3 System Administrator

- Administers the backend system and keeps it running
- Generates and administers accounts
- Trains supporters and ev. end users
- Provides technical help and support

### 4.4 Data Scientist

- Makes in-depth analysis of collected telemetry data (usage data)

### 4.5 Researcher

- Conducts all end user related research
- Sets up questionnaires, focus groups and interviews
- Collects at the end user site and with the end users together their expectations towards and experiences with the PVA
- Evaluates the results of the questionnaires and interviews quantitatively and qualitatively.

### 4.6 Project Partners

PARTNER	VIR	ENG	HAN	DEV	TMZ	SRL	UCLL	BON	IHL
COUNTRY	NL	NL	NL	NL	NL	BE	BE	CH	CH



ORGANIZATION	SME	LE	UNIV	USER	USER	USER	UNIV	USER	UNIV
END USER				20	20	20		20	
SUPPORTER				X	X	X		X	
SYSADMIN	X								(X)
DATA SCIENTIST		(X)							X
RESEARCHER			X				X		X

**Table 2: Project partners versus role in the project**



## 5 Data Within the Project

Several type of data is collected during the lifetime of the project. three different kinds of data can be distinguished:

- Data required to make complementary research in the project (exptectations, satisfaction, biographic analysis, IPA, CSI...). They are described in sections: 5.1, 5.2, 5.3
- Data recorded automatically during the operation of the device, intended for the use in AI-research. It is described in section 5.4
- And data used for the normal operation of the device, also thinkable in a commercial environment. This data is described in section 5.5 and 5.6

### 5.1 Informed Consent

- End user allows the usage of the data during the project
- On this consent the clear name and the pseudonymization code is noted
- Only available in paper form at the relevant end user site (NL, BE, CH)

### 5.2 Questionnaires

- Electronic questionnaires, that are filled out by end users
- Stored on secured electronic platform FormDesk, with the user account of HAN
- Used for SPSS evaluation of the data
- Used for deriving user requirements, user expectations, user well-being status

### 5.3 Focus Group and Interview Notes

- Taken during face to face interaction with the end users
- Notes taken electronically (stored on research servers locally) or on paper (locally stored at research organizations)
- Used for deriving user requirements, user expectations, user well-being status

### 5.4 Telemetry Data

- Pseudonymized data automatically collected on client devices
- Uploaded to the API server (@Virtask in NL, then mirrored to engie NL)
- This data records the user behavior on the client device
- It is intended for data analysis investigation, with the goal to find common usage patterns and long term behavior

### 5.5 Configuration Data

- All data required to set up/configure the software individually and guarantee the support during the operation of the system
- Either the supporter or the Sysadmin sets up the devices
- Information is stored dynamically on the dashboard in NL @ Virtask
- Configuration data base also contains recurring reminders except google calendar





## 5.6 Google Account

- For each user a specific google account is set up
- This account is used for connection and authentication on client device (oAuth 2.0)
- The underlying google calendar data is fed to the client device
- This calendar can be shared with the supporter
- Calendar data resides on google accounts only – excerpts are displayed on local client devices on request
- Data is not connected to other data for evaluation purposes

## 6 Data Access and Usage of Data

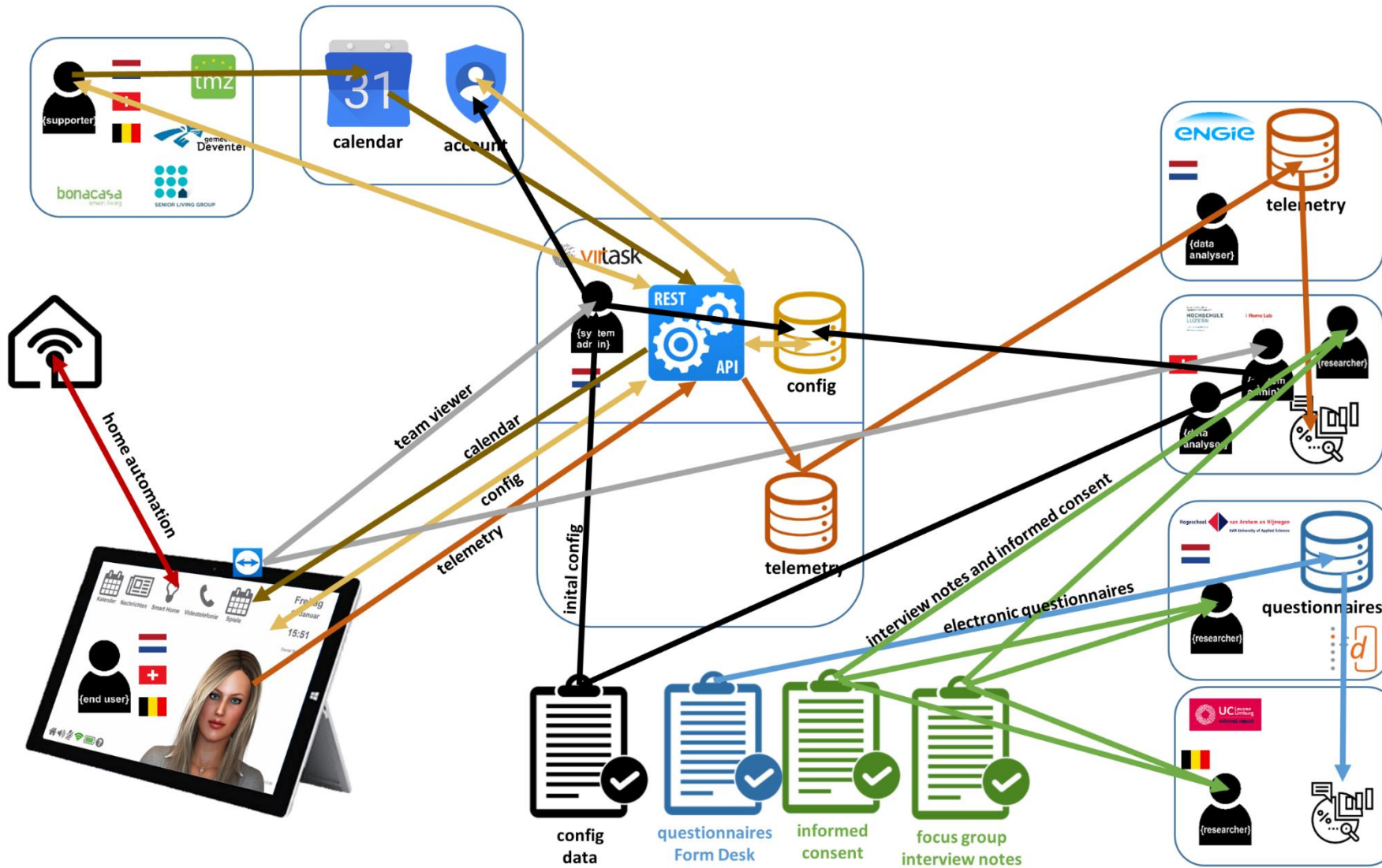
To fulfill the privacy and data protection guidelines and principles (chapter 2) and the derived Requirements (chapter 3), the different user groups and data storage types and locations are depicted in a comprehensive access scheme in Table 3 below

	User Type					Storage Form						
	End user	Supporter	Sys Admin	Data Scientist	Researcher	Paper	DB VIR	DB ENG	Drives HAN / U-CLL	Drive IHL	Google Account	Google Calendar
<b>Informed consent</b>	A	-	-	-	B/C	X						
<b>Configuration</b>	A	-	C/B	-	-		X					
<b>Google Account (authentication only)</b>	C/B	C	D/C/A	-	-		X				X	
<b>Questionnaire</b>	A	-	-	-	C/B	X			X			
<b>Interview Notes</b>	A	-	-	-	C/B	X			X	X		
<b>Telemetry</b>	A	-	C	C	-		X	X		X*		
<b>Reminder**</b>	A	C	C	C	-		X					
<b>Google Calendar (no medication data)</b>	C/B	C/A	C	-	-							X
<b>TeamViewer</b>	B/A	-	-	-	-							

**Table 3: Data Access, Storage and Usage - A: generates data; B: stores / owns data; C: has access to data; D: administers accounts / data; -: has NO access to data; \*: only evaluation of stored data; \*\* Reminder data can be used for drinking reminder and also for medication intake. They are part of configuration data and can be accessed with the dashboard with defined user access rights.**



## 7 System Overview



The MyLiveMyWay system consists of several distributed components that interact with each other. Furthermore, access rights to the generated and stored data is depending on the users role in the whole ecosystem. All telemetry and questionnaires data are pseudonymized completely. Access to data is restricted to persons only with access rights. An overview as base for discussion is given in the graph below. Refer also to the explanatory chapters 4, 5, 6

## 8 Informed Consent

The initial informed consent was slightly changed for phase II after several discussions with the different data protection officers of the participating countries. Extensions were made with the use of the google calendar and the explicit mention of the telemetry usage data collection capability of the system. Further, the informed consent is also presented to the informal/formal carer for signature, if a carer is involved for a specific end user.

The informed consent is explained in detail to the end users before they are asked to sign it. With this procedure we are sure, that the content of the informed consent is understood by the proband.

The original developed informed consent for this AAL project, is used and signed by the end users involved at the start of the project. At the midterm review one of the issues stated was to check if all the items are covered by new legislation like GDPR. During the project, a decision was made (and the opportunity was developed) to collect telemetry data anonymously. For gathering, storage and use of these data there was no specific item asked by informed consent from each end user but implicitly stated. Due to developments in recent legislation (GDPR) the original informed consent has to be extended for the item gathering of telemetry data. Also it is recommended to address the use of the “Google agenda” in making appointments in the agenda of the PA Anne. The next two items are developed and added to the existing informed consent.

### 8.1 Proposal for extension of the informed consent

#### 8.1.1 Telemetry data

An addendum on this topic telemetry data is developed in close cooperation between the members of the research group and juridical experts. The addendum is translated in the language necessary for each country and added to the existing informed consent.

Language

German (delivered by iHomeLab/Daniel Bolliger)

*«Ich verstehe, dass meine Nutzungsdaten automatisiert aufgezeichnet und gesichert an den geschützten Datenserver des Projektes übermittelt werden. Die so erhobenen pseudonymisierten Daten werden nur innerhalb des Projektes verwendet und können nur von autorisierten Projektmitarbeitern bearbeitet und ausgewertet werden. Die Detaildaten werden vertraulich behandelt und nicht ausserhalb des Projekts weitergegeben und nach Abschluss des Projekts wieder gelöscht.»*

Nederlands/Vlaams (delivered by HAN/Sylvia Hoekstra)

*Ik begrijp dat mijn gebruiksgegevens automatisch worden vastgelegd en veilig worden verzonden naar de beschermde dataserver van het project. De gepseudonimiseerde gegevens die op deze manier worden verzameld, worden alleen binnen het project verwerkt en kunnen alleen worden verwerkt en beoordeeld door geautoriseerde*

projectpersoneel. De gedetailleerde gegevens worden vertrouwelijk behandeld en zullen niet buiten het project worden doorgegeven en zullen na voltooiing van het project worden verwijderd.

English (delivered by HAN/Sylvia Hoekstra)

*I understand that my usage data is automatically recorded and transmitted securely to the protected data server of the project. The pseudonymised data collected in this way will only be processed within the project and can only be processed and evaluated by authorized project staff. The detailed data will be treated confidentially and will not be passed on outside the project and deleted after completion of the project.*

### 8.1.2 Use of Google-agenda

It is strongly recommended by the juridical advisors to state clearly in the informed consent the use of the Google agenda.

Therefore the next statement is developed and added to the modified version.

#### Language

German (delivered by iHomeLab/Daniel Bolliger)

*Ich verstehe, dass meine Kalenderdaten auf einem Googlekonto gespeichert werden. Für die Kalenderdaten gelten die Datenschutzbestimmungen von Google.*

Nederlands/Vlaams (delivered by HAN/Sylvia Hoekstra)

*Ik begrijp dat mijn agendagegevens op een Google account is opgeslagen. Het Google-privacybeleid is van toepassing op de kalendergegevens.*

English (delivered by HAN/Sylvia Hoekstra)

*I understand that my calendar data on a Google account is stored. The Google Privacy Policy apply to the calendar data.*

## 8.2 Procedure modifying informed consent

The addendum concerning the **telemetry data** is added in the original informed consent as item 6 (Dutch version) and 7 (German version). In the Flemish version it is included already.

The addendum **concerning the use of Google agenda** is added in the original informed consent after item 7 (Dutch version) and 8 (German version).



### 8.2.1 Replacing existing informed consent

To be sure every end user is fully aware of and agreed on the state of the art informed consent, we decided to replace the existing informed consent for the modified. All newly recruited end users are informed and asked to sign this modified informed consent.

The group of end users who are included at the beginning of the project and from whom is obtained already a written informed consent (not modified), we decided to let all these end users sign this modified informed consent after clearly communicating to every individual end user what the modified informed consent consists of. If the end user agrees and signed, then the existing version will be destroyed and replaced by the new modified version.

This modified informed consent will be delivered by all known and new end users.

### 8.3 Modified Informed Consent

#### Einwilligungserklärung Forschungsprojekt MyLifeMyWay

Ich, der/die Unterzeichnete, bestätige (bitte ankreuzen, wenn zutreffend):

1.	Die Informationen über dieses Projekt wurden mir während der Demonstration von Anne in Form eines Informationsblatts zur Verfügung gestellt. Ich habe sie gelesen und verstanden.	<input type="checkbox"/>
2.	Ich hatte die Möglichkeit, Fragen über das Projekt und meine Teilnahme zu stellen.	<input type="checkbox"/>
3.	Ich bin damit einverstanden, freiwillig an diesem Projekt zu teilzunehmen.	<input type="checkbox"/>
4.	Ich verstehe, dass ich jederzeit mit meiner Teilnahme in diesem Projekt aufhören kann. Ich muss keine Gründe für das Aussteigen angeben. Bei einem vorzeitigen Ausstieg entstehen für mich keine negativen Folgen.	<input type="checkbox"/>
5.	Ich verstehe, dass ich bei meinem Ausstieg das Recht habe, zu verlangen, dass alle meine persönlichen Rohdaten gelöscht werden.	<input type="checkbox"/>

6.	Ich bin informiert, dass mein Benutzerverhalten auf dem Tablet automatisch aufgezeichnet und zur Verbesserung des Systems ausgewertet werden kann.	<input type="checkbox"/>
7.	Ich verstehe, dass alle erhobenen Daten (Ausnahme Punkt 8) geschützt aufbewahrt werden, nicht ausserhalb des Projekts weitergegeben und nach Projektende gelöscht werden.	<input type="checkbox"/>
8.	Ich verstehe, dass meine Kalenderdaten auf einem Google-Konto gespeichert werden. Für diese Kalenderdaten gelten die Datenschutzbestimmungen von Google.	<input type="checkbox"/>
9.	Mir wurden die Verfahren bezüglich Vertraulichkeit der erhobenen Daten erklärt (z.B. Verwendung von Namen, Pseudonymisierung)	<input type="checkbox"/>

Zusatz Datenschutz CH MyLifeMyWay AAL Project

Page 1/2



10.	Die Verwendung der Daten in der Forschung und in Veröffentlichungen sowie die Nutzung und Archivierung wurde mir erklärt.	<input type="checkbox"/>
11.	Ich verstehe, dass Forscher nur dann Zugriff auf meine Daten haben, wenn sie die Vertraulichkeit der Daten garantieren, und wenn sie mit den Bedingungen, welche in diesem Dokument angegeben sind, einverstanden sind.	<input type="checkbox"/>
12.	Ich verstehe, dass das im Projekt verwendete Tablet während des Projekts nur für projektrelevante Tätigkeiten genutzt werden darf. Das Tablet ist während der Projektdauer gegen Schäden versichert. Nach Beendigung des Projekts darf ich das Tablet kostenfrei behalten.	<input type="checkbox"/>

**Teilnehmer:**

\_\_\_\_\_ Name des Teilnehmers      \_\_\_\_\_ Unterschrift      \_\_\_\_\_ Datum

CHZW-XX-

\_\_\_\_\_ Kennzeichnung des Teilnehmers

**Betreuer** (falls vorhanden):

\_\_\_\_\_  
Name des Betreuers                      Unterschrift                      Datum

**Projektpartner:**

\_\_\_\_\_  
Name des Betreuers                      Unterschrift                      Datum

Die Forschungsaktivitäten in diesem AAL-Projekt entsprechen den geltenden Datenschutzbestimmungen und ethischen Gesetzen und Vorschriften der EU-Länder, in denen die Forschung durchgeführt wird. In der Schweiz entspricht das Projekt allen schweizerischen Ethik- und Datenschutzbestimmungen.

Zusatz Datenschutz CH MyLifeMyWay AAL Pro-  
ject

Page 2/2



**Figure 1: Informed Consent German for Test Phase 2**



## 9 GDPR Status

During Mid Term review in 2017 the data security aspect was discussed. As a result the mid term review report identified the following blocking issue:

*Verify the legal framework applicable for each country during project development and for the roll- out phase. GDPR is just an example of a regulation that the PA will have to comply with, which imposes functional requirements, quality attributes and barriers that the product will have to comply with. Cybersecurity, identity management are other areas of concern at EU level. As we heard on the review some countries may have additional regulations that the project must consider. In parallel with legal requirements, consider appropriate practical controls, who has access to what level of data, who can make edited changes to medication reminders for example.*

The consortium took action and reviewed the new legislation situation with the local juridical authorities. Especially we discussed also the situation with the new EU data protection law (valid from Mai 2018).

In general there is high attention to the subject of new GDPR in all participating countries. All project partners are well aware of the importance of a good way to respect GDPR and the dignity of all participants as first principle. All responsible representative of the project partners are anyway focusing now on this subject. This means the privacy and security is already a topic with high attention within their organizations and we can profit in MLMW project from ongoing activities. On the other hand the authorities are very much overloaded with the actual changes in legislation. So not all authorities were able to respond until the release of this version of the deliverable. Nevertheless we present here the actual available status in Belgium, Netherlands and Switzerland. By April 1<sup>st</sup> 2018.

Summarizing can be stated:

- No ethical approval has to be applied for MLMW
- With small adaptations in the informed consent the project also respects with its current setup the new GDPR legislation of the EU
- Adapted informed consent is applied to all participating end users with the rollout of phase 2 end user tests in spring 2018.

### 9.1 Situation in Belgium

In Belgium we have two active organisations: SLG and UCLL. Whereas UCLL is the responsible research partner, SLG is the end user organization.

**UCLL** already checked the situation and describes it as follows:

University College Limburg Leuven (UCLL) is member of the KU Leuven association. The KU Leuven is fully committed to the advancement of high quality academic research and to promote high ethical standards of research. In the first instance KU Leuven endorses the national ethical code drawn up by the four Belgian Academies – the Royal Flemish Academy of Belgium for Science and the Arts, the (Flemish) Belgian Royal Academy of Medicine and their respective Francophone counterparts and the European Code of Conduct for Research Integrity, drawn up by ALLEA (All European Academies). KU Leuven has also drawn up some of its own guidelines and policies concerning among other things animal



testing, academic freedom, dual use research and privacy (see <https://www.kuleuven.be/english/research/ethics>).

**Social and Societal Ethics Committee (SMEC)** evaluates **research on human subjects that is not related to health science practices** or includes medical or pharmacological procedures. It includes a multidisciplinary panel of experts for ethical review of research in the humanities and the behavioral or social science research traditions. Also protocols in engineering, natural or life science may be submitted to the SMEC panel. Mixed protocols will be evaluated in collaboration with the Medical Ethics Committee. Ethical review board SMEC was founded on April 1, 2014, by the university executive board GEBU, for the evaluation of research on human subjects, not subject to compulsory review by the medical board MEC. SMEC includes a multidisciplinary panel of experts for the ethical review of research protocols in the humanities, and the behavioral or social science research traditions. Also protocols in engineering, natural or biomedical science may be submitted to the SMEC panel of experts. Focal points of SMEC review include the reconciliation of the interests of participants and researchers, and the implementation of good research practices. SMEC follows legal and international ethical guidelines and standards with regard to participant recruitment, data collection and handling, and the dissemination of research findings. As far as they are not already part of official legislation (e.g., regarding privacy), such guidelines have been defined and endorsed by scientific organizations and professional associations, and the SMEC panel intends to take differences into account that may exist between scientific areas. Although advice by the SMEC panel of experts is often not compulsory, nor legally binding as such, it may be required by publishers or editorial boards, research auditors, legal authorities, or funding agencies. Prior to the practical implementation of protocols and procedures, researchers should determine whether an ethical review certificate may be required at a certain point in time. In most cases, the SMEC panel will not provide post-hoc advice. Applicants should note that any ethical advice by the SMEC panel relates to the verbatim description of protocols and procedures in the application dossier. Amendments or revisions of reviewed protocols should be resubmitted to the SMEC panel for additional review. The SMEC panel will not advise about scientific originality of the application.

Besides SMEC, there is a special ethics committee for clinical research. **The Ethics Committee Research UZ / KU Leuven** evaluates **medical and health related research** (clinical research) and provides advice after scientific and ethical review by a panel of experts. Protocols involve human subjects (patients or healthy subjects), or can be also related to research on human pathological material or embryo's. For more information (only Dutch) see <https://www.uzleuven.be/ethische-commissie/onderzoek>

More information about the policy on processing of personal data at KU Leuven and the KU Leuven contact persons can be found on the privacy webpage of KU Leuven: <https://admin.kuleuven.be/rd/privacy/en/researcher#section-0>

### **Ethical review MLMW**

MLMW is research on elderly people that is not related to health science practices or includes medical or pharmacological procedures. Therefore, for MLMW, UCLL submitted a research protocol and procedures for ethical review by the SMEC panel of experts at October 11<sup>th</sup> 2017. Following favorable review of an application dossier, SMEC provided a certificate of ethical approval (in the form of an email) at October 27<sup>th</sup>. This certificate relates to the verbatim description of protocols and procedures in the application dossier, and can

be included or mentioned as such in applications, publications, etc. It will remain valid upto 4 years of its effective date of issue. Amendments or revisions of approved protocols should be resubmitted to SMEC for additional review using the same application forms, mentioning the previous dossier.

The mail thread for this review can be found in the following figure

<p><b>Von:</b> SMEC  <b>An:</b> <a href="mailto:evi.verdonck@ucll.be">Evi Verdonck</a>  <b>Oc:</b> <a href="mailto:anne.groenen@ucll.be">Anne Groenen</a>  <b>Betreft:</b> RE: Nieuwe aanvraag SMEC: project My Life My Way  <b>Datum:</b> Freitag, 27. Oktober 2017 11:19:35  <b>Anlagen:</b> <a href="#">image001.png</a></p> <hr/> <p>Beste Onderzoeker,          Beste Evi,</p> <p>Bedankt voor de aanpassingen m.b.t. uw onderzoeksdossier "Assistent to Live   My Life, My Way".</p> <p>De SMEC raad concludeerde dat uw aangevulde dossier (versie 27/10/2017) volledig is en voldoet aan de gestelde ethische normen met betrekking tot wetenschappelijk onderzoek. Haar beslissing met betrekking tot dit protocol is daarom: <b>Gunstig</b>.</p> <p>Uw protocol kreeg het volgende dossiernummer:  <b>G- 2017 10 966</b></p> <p>Gelieve het G-nummer te vermelden bij verdere communicatie, dus bewaar deze e-mail goed. Deze goedkeuring is 4 jaar geldig.</p> <p>SMEC beschouwt uw dossier bij deze als afgehandeld. Indien u bijkomende vragen heeft kan u ons steeds contacteren.</p> <p>Vriendelijke groeten,          Fabienne          Namens SMEC review board</p> <hr/> <p><b>From:</b> Evi Verdonck [<a href="mailto:evi.verdonck@ucll.be">mailto:evi.verdonck@ucll.be</a>]  <b>Sent:</b> vrijdag 27 oktober 2017 9:14  <b>To:</b> SMEC &lt;<a href="mailto:smec@kuleuven.be">smec@kuleuven.be</a>&gt;  <b>Cc:</b> Anne Groenen &lt;<a href="mailto:anne.groenen@ucll.be">anne.groenen@ucll.be</a>&gt;  <b>Subject:</b> RE: Nieuwe aanvraag SMEC: project My Life My Way</p> <p>Beste Fabienne,</p> <p>Dank voor je bericht en de feedback.          De volgende wijzigingen heb ik aangebracht:</p> <ul style="list-style-type: none"> <li>- De participant wordt eerst geïnformeerd over het project aan de hand van het ICF. De week nadien wordt zijn/haar schriftelijke toestemming gevraagd, zodat de persoon voldoende tijd heeft om over de beslissing na te denken (zie aanvraagformulier p. 6 in bijlage)</li> <li>- De schriftelijke toestemming van de participant wordt gevraagd voor het overhandigen van de tablet en software (zie aanvraagformulier p. 6 in bijlage)</li> <li>- Het comité Medische Ethiek is gewijzigd in Ethische Commissie (zie ICF p. 1 in bijlage).</li> </ul>	<p>Ik hoop u hiermee voldoende te hebben geïnformeerd.</p> <p>Vriendelijke groeten,          Evi Verdonck</p> <hr/> <p><b>Van:</b> SMEC [<a href="mailto:smec@kuleuven.be">mailto:smec@kuleuven.be</a>]  <b>Verzonden:</b> dinsdag 24 oktober 2017 11:06  <b>Aan:</b> Evi Verdonck &lt;<a href="mailto:evi.verdonck@ucll.be">evi.verdonck@ucll.be</a>&gt;  <b>CC:</b> Anne Groenen &lt;<a href="mailto:anne.groenen@ucll.be">anne.groenen@ucll.be</a>&gt;  <b>Onderwerp:</b> RE: Nieuwe aanvraag SMEC: project My Life My Way</p> <p>Beste Onderzoeker,          Beste Evi,</p> <p>Uw onderzoeksproject "Assistent to Live   My Life, My Way" werd gereviseerd door de SMEC raad d.d. 16 oktober 2017.</p> <p>De raad concludeerde dat uw protocol voldoet aan de gestelde ethische normen met betrekking tot wetenschappelijk onderzoek. Haar beslissing met betrekking tot dit protocol is daarom:  <b>Gunstig, mits het bezorgen van volgende aanvullingen:</b></p> <ul style="list-style-type: none"> <li>• Wanneer wordt de informatie van mogelijke deelname bezorgd? Dit moet gebeuren ruim voor het overhandigen van het apparaat. Met andere woorden er moet voldoende tijd voor "nadenken" worden ingebouwd om druk tot deelname te vermijden.</li> <li>• Informed consent vragen vóór het apparaat wordt overhandigd.</li> <li>• SMEC is een ethische commissie van KU Leuven, maar niet het Comité voor Medische Ethiek zoals aangegeven op het ICF. Dat is een andere commissie.</li> </ul> <p>Na het ontvangen van deze extra informatie/correcties zal u een finaal dossiernummer ontvangen.</p> <p>Vriendelijke groeten,          Fabienne          Namens SMEC review board</p> <hr/> <p><b>From:</b> Evi Verdonck [<a href="mailto:evi.verdonck@ucll.be">mailto:evi.verdonck@ucll.be</a>]  <b>Sent:</b> woensdag 11 oktober 2017 10:46  <b>To:</b> SMEC &lt;<a href="mailto:smec@kuleuven.be">smec@kuleuven.be</a>&gt;  <b>Cc:</b> Anne Groenen &lt;<a href="mailto:anne.groenen@ucll.be">anne.groenen@ucll.be</a>&gt;  <b>Subject:</b> Nieuwe aanvraag SMEC: project My Life My Way</p> <p>Beste,</p> <p>Toegevoegd vindt u een nieuw aanvraagformulier (+ bijlagen) voor een ethisch-deontologische review.          Alvast bedankt voor uw feedback.</p>
--	---

**Figure 2: Mail Thread Ethical Review Belgium**

**SLG** does not store any data of the MLMW trials locally at their organization and therefore does not have any special obligations regarding the data protection legislation. One open point is the clarification about the reminder function we have implemented in Anne. Especially, when it is used for reminding of medication intake.

## 9.2 Situation NL

In the Netherlands we have following parties, active in the project: Research organization HAN, end user organization DEV and TMZ, ENG who stores all telemetry data and VIR, that runs the system as development organization.

**HAN** is anyway having a closer look to data protection and privacy with the introduction of new GDPR legislation. We got last few days the following feedback from the responsible bodies from HAN, explaining the compliance of HAN in the MLMW research context. there is a letter from the ethical advisory board that states, that MLMW does not need to have an extra ethical approval, and the research can go on as planned.

Adviesbrief Ethische Adviescommissie  
Onderzoek FGGM

Datum: 8 februari 2018  
 Adviesnr.: EACO 96.02/18  
 Onderwerp: Antwoord Adviescommissie  
 Onderzoeksvoorstel: *My life My Way*  
 Inhoudelijke reactie: Geachte mevrouw Adriaansen,

De Ethische Adviescommissie Onderzoek FGGM verklaart hierbij dat uw onderzoeksvoorstel niet onder de reikwijdte van de *Wet medisch-wetenschappelijk onderzoek met mensen (WMO)* valt, aangezien niet is voldaan aan de twee voorwaarden die gelden voor deze wet. Om onder de WMO te vallen dient het onderzoek een "medisch-wetenschappelijk onderzoek" te zijn én krijgen de deelnemers handelingen opgelegd in de zin van de wet.<sup>1</sup> Het onderzoek kan derhalve doorgang vinden als u zich houdt aan de regels van goed gedrag voor onderzoekers.

De commissie attendeert u graag op het onderstaande:

- Met ingang van 1 januari 2016 is de Wet bescherming persoonsgegevens (Wbp) gewijzigd. Als tot personen herleidbare gegevens zijn gelekt of verloren zijn gegaan (datalek), moet dit aan de Autoriteit Persoonsgegevens (AP, nieuwe naam van CBP) worden gemeld en ook aan alle betrokken personen. Een datalek ontstaat als een "onbevoegde" toegang krijgt tot persoonsgegevens. Onbevoegd is iedere externe partij die wordt ingeschakeld bij (bijvoorbeeld) het verzamelen of opslaan van persoonsgegevens, zonder dat daarmee een bewerkersovereenkomst is afgesloten. U vindt op <http://specials.han.nl/sites/studiecentra/onderzoek/> een lijst met ICT-tools waarmee de HAN een bewerkersovereenkomst heeft afgesloten en die u dus kunt gebruiken bij uw onderzoek.

Hopende u hiermee voldoende te hebben geïnformeerd.

Met vriendelijke groet,  
 Dr. R. van der Sande, voorzitter  
 Mr. L. Marten, secretaris

<sup>1</sup> De WMO is van toepassing indien:

- sprake is van medisch-wetenschappelijk onderzoek. 'Medisch-wetenschappelijk onderzoek is onderzoek dat als doel heeft het beantwoorden van een vraag op het gebied van ziekte en gezondheid (etiologie, pathogenese, verschijnselen/symptomen, diagnose, preventie, uitkomst of behandeling van ziekte), door het op systematische wijze vergaren en bestuderen van gegevens. Het onderzoek beoogt bij te dragen aan medische kennis die ook geldend is voor populaties buiten de directe onderzoekspopulatie.'
- personen aan handelingen worden onderworpen of hen gedragsregels worden opgelegd. Er wordt op enige wijze inbreuk gemaakt op de fysieke en/of psychische integriteit van de proefpersoon.

Adviesbrief Ethische Adviescommissie  
Onderzoek FGGM

Werkwijze EACO De Ethische Adviescommissie Onderzoek FGGM beoogt te bevorderen dat onderzoekers, docenten en studenten van de faculteit GGM hun onderzoek ethisch verantwoord uitvoeren. Zij informeert daartoe betrokkenen over ethische en juridische aspecten van onderzoek en professionele standaarden van goed gedrag. De Adviescommissie adviseert bij vragen over de noodzaak van toetsing door een medisch-ethische toetsingscommissie (METC).

**Figure 3: Adviesbrief Ethische Adviescommissie Onderzoek FGGM**

The privacy and data protection is guaranteed by following the three documents of HAN:

- Privacy Policy of HAN (attachment 10.1)
- Data Protection Policy of HAN (attachment 10.2)
- Data and system usage of HAN (attachment 10.3)
- Data management plan of HAN (attachment )

**ENG** stores solely the telemetry data of the field tests on their data center. With the discussion on exit of engine of MLMW, the data on their servers will be deleted before the end of the project completely. The data center itself is in line with the highest security standards and is therefore compliant with the new GDPR legislation. Details can be found in the following document in the attachment in chapter 10.5

- Engie GDPR and AVG Compliance Declaration

### **VIR** Protection of personal data and data leaks

To meet the requirements of the GDPR Virtask will add to all the end user agreements the following:

1. Virtask respects and acts accordingly to the European privacy laws (AVG/GDPR), including the law “Wet Meldplicht Datalekken” (obligation to report data leaks). In particular, Virtask will not process personal data for a purpose other than is agreed up on within the scope of the project MLMW. Virtask is required to protect the personal data using technical and organisational measurements within reason. ‘Within reason’ means that the costs of the measurements taken for protection regarding the type of personal data, are reasonable regarding the risks.
2. When personal data is no longer necessary for the purpose of the goals that the involved parties have agreed up on, Virtask will remove and destroy the data.
3. All employees of Virtask that work with personal data are subjected to a duty of confidentiality and work accordingly the current legislation and the regulatory regime.
4. All loss of, illegitimate acquisition of, or damage to personal data will be reported within 24 hours after discovering of that fact to the consortium members of MLMW and will be submitted to an investigation if it is necessary to report it to the supervisory authority.

Virtask works with informed consent form that all participants (end users) have to sign and to meet the requirements of the GDPR Virtask will additionally:

- provide an additional information sheet for the legal representatives of incapable adult participants;
- in the information sheet to the participants, mention that the data of the participants will be protected in accordance with the provisions of the amended law of 2 August 2002 (and then Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 when it will apply);
- regarding the images, videos and sound recordings that will be used to communicate about the study outside, ensure that participants will not be identifiable unless they have given their consent in writing;
- in the informed consent form, in the section where the participant agrees for secondary use of his or her data for future research, specify that this is research in the same field;

- in the information sheet to participants, specify how confidentiality will be ensured, specifying how the data will be processed and whether it can be sent to other countries. If data can be sent to countries outside the European Union, provide a check box in the informed consent form that states: "I accept the transfer of my samples / data made anonymous, outside the EU European Union, where existing legislation on data protection may be less stringent "

**TMZ and DEV** as end user organizations. They do not store any data on the participants of the field trials. Therefore they follow HAN as responsible research organization and do not have to take special precautions.

### 9.3 Situation CH

In Switzerland we have the two organizations IHL and BON. BON is the end user organization and does not store any data. IHL is research and development partner and is in charge for assessing the situation for whole country.

**BON** does not save any data on the user trials and does therefore not take any special precautions regarding GDPR and privacy. They follow the measures of IHL

**IHL** took the lead on security and data protection issues in Switzerland.

In a first step, the system description presented in chapter 4, 5, 6 and 7 was written. This was the information base for all external experts, assessing the project. Without such a documentation it is not possible to assess such a complex system with the privacy experts.

The description was made available for all project parties, for their bilateral discussion of the privacy assessments.

Then IHL approached the data and privacy representative of – Lucerne University of applied Arts & Sciences Prof. Dr. Ursula Sury. An in depth face to face discussion followed. The final advice was, to contact the official juridical representative for data protection of the Kanton Luzern, Dr. Jur. Reto Fanger for a final assessment.

Contact was established end of January and a discussion meeting for clarification of open points took place on March 7<sup>th</sup>. The feedback of the data protection representative to the information on MLMW was very positive.

The following points needed better clarification:

- The informed consent has to be extended by having an extra point on the use of google calendar
- The informed consent has to be extended by having an extra point on the capability of the system to record automatically telemetry data
- If it is possible to encrypt data sets on the data bases regarding to evaluation performance, this should be planned.

These first two points are already implemented for field testing in phase 2 (see chapter 8). The last point (encryption) will be tackled as soon as there is better visibility on exit of engine and the performance of our envisioned data storage environment, using kafka.

Additionally, the situation between the GDPR legislation in EU and Switzerland was discussed. Switzerland will adapt their legislation to be compliant with the new EU GDPR. A

proposal of the 'Bundesrat' was handed out to the parliament in March 2018. Discussion and final laws will enter in force after that. A date for this act is not known until now.

The data protection officer of the Kanton Luzern will hand over a data protection and privacy statement of MLMW. Planned was Eastern 2018. This statement will be added here in an updated version of this document.

## 9.4 GDPR next Steps

Not yet all contacted national data security officers have given their final assessment to the submitted privacy and security policy of the MyLifeMyWay project. We will include the comments and the conclusions into this deliverable upon receipt.

Just on April 6<sup>th</sup> we got from the data and security responsible from SLG Renilde Rottiers (mail from Marc Flaeminck) valuable the following feedback on GDPR implementation:

- *The PA (privacy assessment) must be completed before 25<sup>th</sup> of May 2018, with acknowledging the results.*
- *If the assessment shows too many risks we should ask the Privacy Authority (sic. in BE) for an advice, if we can continue the project in the same way.*
- *Up from May 25<sup>th</sup> 2018 the liability is enhanced, and projects are working with a processor agreement. In such an agreement precautions are taken in a way that a third party is handling carefully with the private coordinates of everyone, following the principles of the agreement.*
- *Up from May 25<sup>th</sup> 2018 every end user of Anne has to receive a privacy notice with all their rights concerning the GDPR.*
- *When somebody is making software (for example Virtask) , and sells this to a third party the company is the processor responsible, and the third parties are the processors.*

The affected partners will carefully check the input, and will assess, what is valid for the project and what for the commercial rollout after the project. They will take action for implementation with highest priority. Highest goal is to protect privacy and dignity of all involved persons in this project, and to be compliant with the valid regulations and laws.



## 10 Appendix

### 10.1 Privacy Policy of HAN

Vastgesteld, met instemming van de MR, d.d. 13-3-2018/  
CvB-besluitnr. 2017/1243

#### Privacyreglement Hogeschool van Arnhem en Nijmegen

##### Preambule

Verzameling, verwerking en opslag van persoonsgegevens is noodzakelijk voor de bedrijfsprocessen van de Hogeschool van Arnhem en Nijmegen. Uiteraard dient dit met de grootste zorgvuldigheid te gebeuren. De HAN is verantwoordelijk voor de naleving van de Algemene Verordening Gegevensbescherming (AVG) en hecht veel waarde aan het beschermen van persoonsgegevens die aan haar worden verstrekt en aan de wijze waarop persoonsgegevens worden verwerkt. In dit reglement wordt onder meer geregeld welke persoonsgegevens er bij de HAN worden verwerkt, aan wie deze persoonsgegevens eventueel mogen worden verstrekt en wat de rechten zijn van degene wiens persoonsgegeven(s) worden verwerkt.

##### *I Algemene bepalingen*

#### Artikel 1 Begripsbepaling

In dit reglement wordt in aansluiting en aanvulling op de Algemene Verordening Gegevensbescherming<sup>1</sup> verstaan onder:

- a. AP: Autoriteit Persoonsgegevens, de toezichthoudende autoriteit zoals bedoeld in artikel 51 lid 1 AVG;
- b. applicatiebeheerder: degene die ervoor zorgt dat de applicatie goed werkt binnen de HAN;
- c. AVG : Algemene Verordening Gegevensbescherming;
- d. beheerder: degene die onder verantwoordelijkheid van de verwerkingsverantwoordelijke is belast met de dagelijkse zorg voor de verwerking van persoonsgegevens, voor de juistheid van de ingevoerde gegevens, alsmede voor het bewaren, verwijderen en verstrekken van gegevens. In de bijlage is een overzicht van de beheerders opgenomen. In gevallen waarin niet duidelijk is wie de beheerder is, is de directeur Service Bedrijf de beheerder;
- e. bestand: elk gestructureerd geheel van persoonsgegevens, ongeacht of dit geheel van gegevens gecentraliseerd of gedecentraliseerd is dan wel verspreid is op functionele of geografische gronden, dat volgens bepaalde criteria toegankelijk is;
- f. betrokkene: degene op wie een persoonsgegeven betrekking heeft;
- g. bijzondere persoonsgegevens: persoonsgegevens als bedoeld in artikel 9 AVG, waaruit bijvoorbeeld ras of etnische afkomst, religieuze of levensbeschouwelijke overtuigingen blijken (foto's e.d.) of gegevens betreffende gezondheid zoals handicap, chronische ziekte;
- h. functionaris: de functionaris bescherming persoonsgegevens die binnen de HAN toezicht houdt op de toepassing en naleving van de AVG;
- i. gebruiker: degene die onder verantwoordelijkheid van de beheerder bevoegd is persoonsgegevens in te voeren, te wijzigen en/of te verwijderen, dan wel van enigerlei uitvoer van de verwerking kennis te nemen;
- j. inbreuk in verband met persoonsgegevens: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens;
- k. personeel: personen in dienst van of werkzaam ten behoeve van de verwerkingsverantwoordelijke;
- l. persoonsgegeven: elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon. Als identificeerbaar wordt beschouwd een natuurlijk persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identifier zoals een naam, een

<sup>1</sup> Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens.



- identificatienummer, locatiegegevens, een online identifier of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon;
- m. profilering: elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, met name met de bedoeling zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen.
  - n. technische werkzaamheden: werkzaamheden die verband houden met onderhoud, reparatie en beveiliging van apparatuur en programmatuur;
  - o. verstrekken van persoonsgegevens: het bekend maken of ter beschikking stellen van persoonsgegevens;
  - p. verwerker: degene die ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt;
  - q. verwerking van persoonsgegevens: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens;
  - r. verwerkingsverantwoordelijke / HAN: de Stichting Hogeschool van Arnhem en Nijmegen, in deze vertegenwoordigd door het College van Bestuur;

## **II Doelstelling en Reikwijdte**

### **Artikel 2 Doelstelling van het reglement**

Dit reglement heeft tot doel:

- a) de verwerking van persoonsgegevens conform het bepaalde in de AVG te laten verlopen;
- b) de persoonlijke levenssfeer van betrokkene van wie persoonsgegevens zijn verwerkt in één of meer bestanden, te beschermen tegen misbruik van die gegevens en tegen verwerking van onjuiste gegevens;
- c) de betrokkene te informeren wat de HAN met zijn of haar persoonsgegevens doet; en
- d) de rechten van de betrokkenen te waarborgen.

### **Artikel 3 Reikwijdte van het reglement**

Dit reglement heeft betrekking op het verwerken van persoonsgegevens van betrokkenen binnen de HAN waaronder in ieder geval alle medewerkers, studenten en externe relaties (inhuur/outsourcing) alsmede op andere betrokkenen van wie de HAN persoonsgegevens verwerkt.

Dit reglement is van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens, alsmede op de verwerking van (niet geautomatiseerde) persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn daarin te worden opgenomen.

## **III Beheer van gegevens**

### **Artikel 4 Mandaat verantwoordelijke**

De directeur Service Bedrijf neemt namens de verwerkingsverantwoordelijke, de verantwoordelijkheid voor de verwerking van de persoonsgegevens.

### **Artikel 5 Documenteren van verwerkingen**

De HAN houdt een register bij van alle verwerkingen van persoonsgegevens. In dit register van verwerkingsactiviteiten staan de volgende gegevens:

- a) de naam en contactgegevens van de verwerkingsverantwoordelijke;
- b) de verwerkingsdoeleinden;
- c) een beschrijving van de categorieën van betrokkenen en van categorieën van persoonsgegevens;
- d) de categorieën ontvangers aan wie de persoonsgegevens zijn of worden verstrekt;
- e) indien van toepassing doorgifte van persoonsgegevens aan een derde land of organisatie;
- f) de beoogde termijnen waarbinnen de verschillende categorieën van gegevens moeten worden gewist;
- g) een algemene omschrijving van technische en organisatorische beveiligingsmaatregelen.

Een geheel of gedeeltelijke geautomatiseerde verwerking van persoonsgegevens dient gemeld te worden bij de functionaris gegevensbescherming. Op het intranet van de HAN wordt aangegeven hoe gemeld kan worden. De functionaris beoordeelt steekproefsgewijs de rechtsgeldigheid van de registratie en draagt zorg voor adequate documentatie.

#### ***IV Verzamelen en verwerken van gegevens***

##### **Artikel 6 Doelbinding en dataminimalisatie**

Persoonsgegevens moeten op een transparante wijze voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden verzameld worden en mogen vervolgens niet verder op een met die doeleinden onverenigbare wijze worden verwerkt. Daarnaast moeten persoonsgegevens toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt ("minimale gegevensverwerking").

##### **Artikel 7 Rechtmatigheid van de verwerking**

Het verwerken van persoonsgegevens is gebaseerd op een van de wettelijke grondslagen zoals omschreven in artikel 6 AVG. De verwerking van persoonsgegevens van betrokkenen kan conform artikel 6 AVG noodzakelijk zijn:

- a) voor de uitvoering van een overeenkomst waarbij de betrokkene partij is;
- b) om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust;
- c) om de vitale belangen van de betrokkene te beschermen;
- d) voor de vervulling van een taak van algemeen belang of een taak in het kader van de uitoefening van het openbaar gezag aan de verwerkingsverantwoordelijke is opgedragen;
- e) voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is.

De verwerking van persoonsgegevens kan ook gebaseerd zijn op toestemming van de betrokkene zelf. De verwerkingsverantwoordelijke moet dan kunnen aantonen dat de betrokkene toestemming heeft gegeven voor de verwerking van zijn persoonsgegevens. Is de betrokkene een minderjarige dan ben je in sommige gevallen verplicht om ook toestemming van de ouder/wettelijk vertegenwoordiger te vragen. In een nadere regeling zal worden uitgewerkt in welke gevallen dit al dan niet noodzakelijk is.

De HAN kan de betrokkene in specifieke – nader te bepalen – gevallen (bijvoorbeeld) middels een toestemmingsformulier om toestemming vragen voor het verwerken van zijn of haar persoonsgegevens.

##### **Artikel 8 Procedure aanvraag om gegevens verstrekken**

Indien een aanvraag tot gegevensverstrekking wordt ingediend bij een medewerker van de HAN of bij een organisatieonderdeel van de HAN dan dient deze aanvraag in ieder geval bij de service unit ICT ingediend te

worden indien:

- a) bij de aanvraag tot gegevensverstrekking een externe op enigerlei wijze is betrokken;
- b) het verzoek om de persoonsgegevens niet tot het reguliere takenpakket/functie behoort van de HAN- medewerker of niet behoort tot de reguliere werkzaamheden behorende bij het organisatieonderdeel;
- c) indien de gegevensaanvraag niet past binnen de doelen zoals deze zijn omschreven in het register van verwerkingsactiviteiten (artikel 5 van dit reglement); of
- d) indien er twijfel bestaat of er inbreuk gemaakt wordt op de AVG.

#### **V Beveiliging, meldplicht datalekken en geheimhouding**

##### **Artikel 9 Beveiliging en meldplicht datalekken**

1. De verantwoordelijke draagt zorg voor passende maatregelen van technische en organisatorische aard ter beveiliging tegen verlies of tegen enige vorm van onrechtmatige verwerking van persoonsgegevens.
2. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.
3. Iedere inbreuk in verband met persoonsgegevens zoals omschreven in artikel 1 sub j van dit reglement zal worden gedocumenteerd. De AP wordt zonder onredelijke vertraging, en indien mogelijk binnen 72 uur na kennisname van het incident, in kennis gesteld van de inbreuk tenzij niet waarschijnlijk is dat de inbreuk risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Indien de melding aan de AP niet binnen 72 uur plaatsvindt, gaat zij vergezeld van een motivering voor de vertraging. Houdt de inbreuk waarschijnlijk een hoog risico in voor de rechten en vrijheden van natuurlijke personen, dan worden ook de betrokkene(n) onverwijld van de inbreuk in kennis gesteld.
4. De kennisgeving aan de AP en de betrokkene omvat in ieder geval:
  - a) de aard van de inbreuk;
  - b) contactgegevens van de functionaris of een ander contactpunt waar meer informatie over de inbreuk kan worden verkregen;
  - c) de waarschijnlijke gevolgen van de inbreuk; en
  - d) de aanbevolen maatregelen om de inbreuk in verband met persoonsgegevens aan te pakken waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele negatieve gevolgen daarvan.
5. De in lid 3 bedoelde mededeling aan de betrokkene is niet vereist indien:
  - a) de gegevens die getroffen zijn door de inbreuk onbegrijpelijk zijn voor onbevoegden, bijvoorbeeld vanwege versleuteling;
  - b) achteraf maatregelen getroffen zijn die maken dat het in lid 3 bedoelde hoge risico zich niet meer zal voordoen;
  - c) indien de mededeling onevenredige inspanningen vergt. In dat geval komt er in plaats daarvan een openbare mededeling of een soortgelijke maatregeling waarbij betrokkenen even doeltreffend even doeltreffend worden geïnformeerd.
6. Degene die een inbreuk in verband met persoonsgegevens, zoals omschreven in lid 3 ontdekt, meldt de inbreuk binnen één werkdag aan de Servicedesk. De Servicedesk meldt de inbreuk onverwijld aan de functionaris, die de verantwoordelijke informeert en zorgdraagt voor de meldingen als omschreven in lid 3.
7. De functionaris houdt een overzicht bij van iedere inbreuk in verband met persoonsgegevens. Het overzicht bevat in ieder geval feiten en gegevens omtrent de aard van de inbreuk, bedoeld in het derde lid, alsmede voor zover van toepassing de tekst van de kennisgeving aan de betrokkene.

##### **Artikel 10 Geheimhouding**

1. De werknemer is verplicht tot geheimhouding van hetgeen hem uit hoofde van zijn functie ter kennis komt, voor zover die verplichting uit de aard van de zaak volgt, of uitdrukkelijk schriftelijk is opgelegd. Deze verplichting geldt ook na beëindiging van de arbeidsovereenkomst.

2. Onverminderd wettelijke bepalingen is de werkgever jegens derden verplicht tot geheimhouding van persoonlijke gegevens van de werknemer, tenzij de werknemer tot het verstrekken van op zijn persoon betrekking hebbende gegevens schriftelijk toestemming geeft.

#### **VI Verwerker(s)(overeenkomst)**

##### **Artikel 11 Verwerker**

1. Indien de verwerkingsverantwoordelijke een bepaalde set verwerkingen van gegevens opgedragen heeft aan een verwerker, wordt er door de verwerkingsverantwoordelijke en de verwerker een overeenkomst opgesteld ten aanzien van de door de verwerker na te komen bescherming van betreffende persoonsgegevens. In deze overeenkomst dient onder meer het onderwerp en de duur van de verwerking, de aard en het doel van de verwerking, het soort persoonsgegevens en de categorieën van betrokkenen en de rechten en verplichtingen van verwerkingsverantwoordelijke te worden omschreven. Daarnaast draagt de verwerkingsverantwoordelijke er zorg voor dat (in deze overeenkomst) verwerker voldoende waarborgen biedt ten aanzien van technische en organisatorische beveiligingsmaatregelen met betrekking tot de te verrichten verwerkingen en ten aanzien van de melding van een inbreuk in verband met persoonsgegevens.
2. Van deze overeenkomst dient door de contracteigenaar een afschrift in Proquro te worden opgenomen. Een format voor deze verwerkersovereenkomst is op het Intranet van de HAN gepubliceerd.

#### **VII Kennisgeving**

##### **Artikel 12 Informatie aan betrokkenen**

1. De verwerkingsverantwoordelijke verstrekt bij het moment van de verkrijging van gegevens van betrokkene de volgende informatie aan de betrokkene:
  - a) zijn identiteit en contactgegevens;
  - b) de contactgegevens van de functionaris;
  - c) de verwerkingsdoeleinden en rechtsgrond van de gegevensverwerking;
  - d) de gerechtvaardigde belangen (indien de verwerking is gebaseerd op artikel 9 lid 1 sub f AVG);
  - e) de ontvangers of categorieën ontvangers van de persoonsgegevens;
  - f) waarborgen bij doorgifte van de persoonsgegevens aan een derde land of internationale organisatie;
  - g) bewaartermijnen;
  - h) rechten betrokkene (waaronder het bestaan van het recht om de verwerkingsverantwoordelijke te verzoeken om inzage van en rectificatie of wissing van persoonsgegevens te verlangen alsmede het recht om bezwaar te maken en het recht op gegevensoverdraagbaarheid);
  - i) of verstrekking door betrokkene verplicht is;
  - j) recht om een klacht in te dienen bij de AP;
  - k) informatie over profilering.

Bovenstaande is niet van toepassing wanneer en voor zover de betrokkene reeds over de informatie beschikt.

2. De informatieverstrekking van lid 1 vindt plaats door middel van een algemene kennisgeving op de website van de HAN gericht aan betrokkene en bevat met name informatie over het bestaan van de gegevensverwerkingen en van deze regeling, de wijze waarop deze kan worden ingezien en over de wijze waarop nadere informatie ter zake kan worden ingewonnen.
3. Indien de persoonsgegevens op een andere wijze worden verkregen dan bedoeld in lid 1 (d.w.z. indien de persoonsgegevens niet van de betrokkene zelf zijn verkregen maar van een derde), vindt de kennisgeving van lid 2 plaats:
  - a) binnen een redelijke termijn, doch uiterlijk binnen één maand na verkrijging van de persoonsgegevens; of
  - b) bij de eerste communicatie met de betrokkene; of

- c) uiterlijk op het moment van eerste verstrekking aan een derde.  
De kennisgeving vindt plaats door middel van een algemene kennisgeving op de website van de HAN.
- 4. De kennisgeving van lid 3 vindt niet plaats, indien de kennisgeving aan de betrokkene onmogelijk is of een onevenredige inspanning kost, de betrokkene reeds over de informatie beschikt, wettelijke plicht is, of indien de persoonsgegevens vertrouwelijk moeten blijven uit hoofde van een beroepsgeheim. In dat geval legt de verwerkingsverantwoordelijke de herkomst van de gegevens vast.
- 5. Geen kennisgeving vindt plaats indien de gegevensverwerking is voorgeschreven krachtens wettelijk voorschrift.

#### **Artikel 13 Opt-in / Opt-out<sup>2</sup>**

Voor het ongevraagd verzenden van e-mailberichten voor commerciële, ideële of charitatieve doeleinden dient voorafgaande toestemming worden gevraagd (opt-in). De ontvanger moet daarbij ook altijd de mogelijkheid hebben om zich uit te kunnen schrijven (opt-out). Voorafgaand toestemming vragen is niet vereist indien het e-mailbericht geen commerciële, ideële of charitatieve doeleinden heeft, de betrokkene zijn e-mailadres voor deze doeleinden heeft verstrekt of in het geval het e-mailadres is verkregen in het kader van verkoop van een product of dienst en het e-mailadres wordt gebruikt voor eigen gelijksoortige producten of diensten. Het e-mailbericht dient dan wel een opt-out mogelijkheid te bevatten.

#### **VIII Bewaring van gegevens**

##### **Artikel 14 Bewaring en termijnen**

Persoonsgegevens moeten worden bewaard in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren dan voor de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is. Persoonsgegevens mogen voor langere perioden worden opgeslagen louter met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden dan wel op grond van een wettelijk voorschrift mits passende technische en organisatorische maatregelen worden getroffen om de rechten en vrijheden van de betrokkene te beschermen. Voor de bewaring van persoonsgegevens zijn bewaartermijnen vastgesteld. Bewaartermijnen kunnen wettelijk zijn bepaald maar kunnen ook door de HAN zelf zijn vastgelegd. Zie hiervoor het HAN-Bestandsoverzicht.<sup>3</sup>

#### **IX Recht van informatie, inzage, afschrift, rectificatie, verwijdering, overdracht en bezwaar**

##### **Artikel 15 Algemeen**

- 1. Iedere betrokkene heeft het recht met betrekking tot zijn persoonsgegevens een verzoek in te dienen bij de beheerder tot:
  - a. verkrijging van informatie;
  - b. inzage, correctie (rectificatie, aanvulling, verwijdering en/of afscherming) en overdracht van gegevens.
- 2. Aan het uitoefenen van die rechten zijn voor de betrokkene geen kosten verbonden.
- 3. Betrokkene kan zich bij het uitoefenen van die rechten – op eigen kosten - laten bijstaan.
- 4. De beheerder wijst betrokkenen op de mogelijkheden van rechtsbescherming en toezicht en op de rol daarin van de AP.

##### **Artikel 16 Recht van bezwaar**

- 1. Indien de rechtmatige grondslag voor een bepaalde verwerking:
  - a. noodzakelijk is voor de goede invulling van een publiekrechtelijke taak; of
  - b. noodzakelijk is voor het gerechtvaardigde belang van de verwerkingsverantwoordelijke, kan de betrokkene bij de beheerder te allen tijde bezwaar aantekenen tegen die verwerking in verband met zijn bijzondere persoonlijke omstandigheden.

<sup>2</sup> Conform artikel 11.7 Telecommunicatiewet

<sup>3</sup> Dit overzicht is op te vragen bij de ServiceDesk van de HAN.



2. Betrokkene heeft het recht niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking, waaronder profilering, gebaseerd besluit waaraan voor hem rechtsgevolgen zijn verbonden of hem anderszins in aanmerkelijke mate treft. Betrokkene kan hier dan bij beheerder bezwaar tegen maken. Dit geldt niet indien het besluit noodzakelijk is voor de totstandkoming of uitvoering van een overeenkomst tussen de betrokkene en verwerkingsverantwoordelijke of indien dit is toegestaan bij de wet die voorziet in passende maatregelen.
3. Binnen vier weken na ontvangst van het bezwaar beoordeelt de verwerkingsverantwoordelijke of het bezwaar gerechtvaardigd is.
4. Indien de gegevens worden verwerkt in verband met de totstandbrenging of de instandhouding van een directe relatie tussen verantwoordelijke of een derde en de betrokkene met het oog op werving voor commerciële of charitatieve doelstellingen (direct marketing), kan de betrokkene daartegen bij de verantwoordelijke te allen tijde bezwaar aantekenen.
5. Wanneer betrokkene bezwaar maakt tegen verwerking ten behoeve van direct marketing, worden de persoonsgegevens niet meer voor deze doeleinden verwerkt.
6. Bezwaar tegen de verwerking voor commerciële of charitatieve doelen is altijd gerechtvaardigd.
7. De beheerder beëindigt de verwerking ter stond, indien de verwerkingsverantwoordelijke het bezwaar gerechtvaardigd acht.

#### ***X Rechtsbescherming en toezicht***

##### **Artikel 17 Klachtenprocedure**

1. De betrokkene kan bij de functionaris een klacht in te dienen:
  - a. tegen een beslissing op een verzoek als bedoeld in artikel 15;
  - b. tegen een beslissing naar aanleiding van de aantekening van bezwaar als bedoeld in artikel 16;
  - c. tegen de wijze waarop de verwerkingsverantwoordelijke, de beheerder of de verwerker de in dit reglement opgenomen regels uitvoert.Elke betrokkene heeft het recht een klacht in te dienen bij de AP.
2. De functionaris reageert zo spoedig mogelijk, maar uiterlijk binnen zes weken na ontvangst, schriftelijk en met redenen omkleed op de klacht.
3. Betrokkene kan zich bij de indiening en behandeling van zijn klacht laten bijstaan.
4. De functionaris kan het advies van de AP inwinnen.
5. De functionaris kan tot het oordeel komen dat de klacht onterecht is dan wel geheel of gedeeltelijk terecht.
6. Indien de functionaris de klacht niet of slechts gedeeltelijk honoreert, kan de betrokkene een klacht indienen bij de AP. De verwerkingsverantwoordelijke informeert de betrokkene, van wie hij de klacht niet of slechts gedeeltelijk honoreert, over die mogelijkheid en over het adres van de AP.
7. Indien de functionaris oordeelt dat de klacht geheel of gedeeltelijk terecht is, beslist hij om:
  - a. indien de klacht zich richt tegen een beslissing als bedoeld in lid 1 onder a, het verzoek van betrokkene alsnog geheel of gedeeltelijk te honoreren;
  - b. indien de klacht zich richt tegen een beslissing als bedoeld in lid 1 onder b, het bezwaar van betrokkene alsnog te honoreren;
  - c. indien de klacht zich richt tegen de wijze van uitvoering als bedoeld in lid 1 onder c, alsnog uitvoering te geven aan de in dit privacyreglement opgenomen regels.
8. De functionaris maakt zijn oordeel schriftelijk aan betrokkene kenbaar.

#### ***XI Functionaris gegevensbescherming***

##### **Artikel 18 Functionaris gegevensbescherming**

1. De functionaris gegevensbescherming wordt benoemd door de verwerkingsverantwoordelijke.
2. De functionaris kan wat betreft de uitoefening van zijn functie geen aanwijzingen ontvangen van verwerkingsverantwoordelijke.

3. De functionaris heeft gelijke bevoegdheden als de toezichthouder van Titel 5.2 van de Algemene wet bestuursrecht.
4. Ieder die werkzaam is bij de HAN is verplicht de inlichtingen te verschaffen en de medewerking te verlenen die in het kader van het vorige lid van hem wordt verlangd.
5. De functionaris is verplicht:
  - a. jaarlijks verslaggeving te doen van zijn werkzaamheden en bevindingen als onderdeel van het jaarverslag van de HAN;
  - b. integraal beleid met betrekking tot privacy te voeren.
6. De functionaris gegevensbescherming heeft als taak:
  - a. toezien op naleving privacywetgeving;
  - b. toezien op eigen interne beleid inclusief bewustwording en opleiding;
  - c. voorlichten en adviseren over privacyvraagstukken;
  - d. samenwerken met de AP;
  - e. optreden als contactpunt voor de AP;
  - f. de behandeling van klachten van betrokkenen;
  - g. de behandeling van verzoeken van betrokkenen voor zover niet geheel aan de wensen van verzoeker tegemoet gekomen wordt;
  - h. het doen van de meldingen, zoals omschreven in artikel 9 lid 3, aan de AP en betrokkene(n) en de verantwoordelijke hierover informeren;
  - i. een overzicht bij te houden, zoals omschreven in artikel 9 lid 7 van dit privacyreglement.
7. De functionaris gegevensbescherming heeft als zodanig slechts toegang tot persoonsgegevens en maakt van de persoonsgegevens waarvan hij in zijn functie kennis krijgt slechts gebruik voor zover het de uitoefening van zijn taak als functionaris betreft.
8. De functionaris kan aanbevelingen doen aan de verwerkingsverantwoordelijke die strekken tot een betere bescherming van de gegevens die worden verwerkt.
9. De verwerkingsverantwoordelijke draagt er zorg voor dat aan de functionaris alle medewerking wordt verleend die deze nodig heeft voor de uitoefening van zijn functie.
10. De functionaris is verplicht tot geheimhouding.

#### **Artikel 19 Toezicht op de naleving**

De AP is op grond van de AVG bevoegd toe te zien op de naleving van de in dit privacyreglement krachtens de AVG opgenomen bepalingen.

#### **XII Overige bepalingen**

##### **Artikel 20 Scholing**

De verwerkingsverantwoordelijke draagt zorg voor een regelmatige scholing van de beheerders en de gebruikers om te verzekeren dat ze de processen van persoonsgegevensverwerking, de daarvoor geldende regels en hun eigen rol daarin begrijpen.

##### **Artikel 21 Onvoorzien**

In gevallen waarin het privacyreglement niet voorziet beslist de verwerkingsverantwoordelijke, nadat deze advies heeft ingewonnen bij de functionaris.

##### **Artikel 22 Bekendmaking en inzage**

Dit privacyreglement wordt opgenomen op het Intranet van de HAN en op [www.han.nl](http://www.han.nl).

##### **Artikel 23 Wijzigingen en aanvullingen**

1. Wijzigingen in het doel van de verwerking en in soort van inhoud, gebruik en wijze van verkrijging van de persoonsgegevens kunnen leiden tot wijziging van dit privacyreglement.
2. Wijzigingen en aanvullingen van het privacyreglement behoeve de instemming van de medezeggenschapsraad.

**Artikel 24 Inwerkingtreding en citeertitel**

1. Dit privacyreglement treedt in werking op [.....].
2. Dit privacyreglement kan worden aangehaald als 'Privacyreglement Hogeschool van Arnhem en Nijmegen'.



## 10.2 Data Protection Policy of HAN

# Informatiebeveiligingsbeleid Hogeschool van Arnhem en Nijmegen

Versie: 2.0 d.d. 17-10-2017

Op basis van:

**Model beveiligingsbeleid uit het  
Framework Informatiebeveiliging Hoger Onderwijs**

V2.0 d.d. 1 mei 2015

Vastgesteld, met instemming van de MR, d.d. 13-3-2018/  
CvB-besluitnr. 2017/1243

Het Model Informatiebeveiligingsbeleid is opgesteld door SURFibo en is  
gepubliceerd onder de licentie Creative Commons  
(<http://creativecommons.org/licenses/by/3.0/nl/>)



Informatiebeveiligingsbeleid HAN

Inhoudsopgave

0. Management Samenvatting .....	3
1. Inleiding .....	5
1.1. Algemeen .....	5
1.2. Doelgroep .....	6
1.3. Reikwijdte van het beleid .....	6
2. Doelstelling .....	7
3. Beleidsprincipes informatiebeveiliging .....	8
3.1. Beleidsuitgangspunten en principes .....	8
4. Wet- en regelgeving .....	10
C.1. Algemene Verordening Gegevensbescherming (AVG) .....	10
C.2. Archiefwet .....	10
C.3. Telecommunicatiewet .....	10
C.4. Wet Computercriminaliteit .....	10
5. Governance informatiebeveiligingsbeleid .....	10
5.1. Afstemming met samenhangende Risico's .....	11
5.2. Inpassing in I-governance .....	11
5.3. Documenten informatiebeveiliging .....	13
5.4. Controle, naleving en sancties .....	14
5.5. Bewustwording en training .....	15
5.6. Organisatie van de informatiebeveiligingsfunctie .....	15
5.7. Overleg .....	17
6. Melding en afhandeling van incidenten (CERT) .....	17
7. Referenties .....	19
8. Vaststelling & Wijziging .....	19
Bijlage A – Classificatie .....	20
Bijlage B Logisch toegangsbeleid digitale voorzieningen HAN .....	22
WACHTWOORDBELEID .....	25
Bijlage C – Responsible Disclosure .....	26

Informatiebeveiligingsbeleid HAN

## 0. Management Samenvatting

Informatie technologie (IT) en informatie management (IM) zijn niet meer weg te denken anno nu. Bijna alle processen zijn afhankelijk van een goede en ongestoorde werking van IM en IT. Dat geldt net zozeer voor het primaire proces, alsook voor secundaire processen en ondersteunende processen als financieel management of personeelszaken. Zonder werkende IT geen research, geen onderwijs, geen productie, geen facturering, geen uitbetaalde salarissen, geen werkende toegangscontrole, enzovoorts.

Daarom is evident dat het hoogste management zich verantwoordelijk moet weten voor IM en IT. Niemand anders dan het bestuur heeft die eindverantwoordelijkheid. Het bestuur is dan ook niet alleen verantwoordelijk voor de inrichting en de *governance* van IM en IT, maar ook voor de ongestoorde en veilige werking ervan. We hebben het dan over informatiebeveiliging of IB. Dit is het onderwerp van dit beleid.

IB is direct gerelateerd aan de missie en prioriteiten van de organisatie. De mate waarin aandacht besteed wordt aan IB is afgeleid van de business impact die inbreuken op de informatiebeveiliging kunnen veroorzaken: er ligt dus altijd een *business case* aan ten grondslag. Het middel van de risicoanalyse bestaat ervoor om een inschatting van de risico's en business cases te maken, om daar vervolgens een passende IB-structuur en -maatregelen op te kunnen baseren.

Informatiebeveiliging gaat over alle IT- en informatiemiddelen en -processen, waarbij met name 3 aspecten van belang zijn:

1. **Beschikbaarheid:** werken de middelen/processen, zijn ze "in de lucht"?
2. **Integriteit:** is de inhoud van de informatiestromen beveiligd, dat wil zeggen is het zeker dat er niet mee geknoeid is of kan worden?
3. **Vertrouwelijkheid:** hebben alleen die mensen toegang tot bepaalde informatie die daartoe gemachtigd zijn, en is het voor anderen ontoegankelijk c.q. onleesbaar?

Een aanvullend aspect dat voor alle drie van belang is, is *controleerbaarheid*: niet alleen "weten" of iets in orde is, maar dat ook achteraf kunnen "verifiëren".

Ten overvloede: IB is géén primair of secundair proces, géén *core business*, maar als je er niets aan doet gaat het wel ten koste van de *core business*: IB is dus een *business enabler* van de eerste categorie. Het bestuur van de organisatie moet dan ook zorgen voor een goede *governance*, inclusief *auditing* en *feedback*. We noemen deze *I-governance*. Deze is cruciaal en management *commitment* is daarbij essentieel.

Dit IB beleid is daarom door het College van Bestuur van de Hogeschool van Arnhem en Nijmegen vastgesteld en gedragen en geldt voor de gehele organisatie, en allen die daarbij betrokken zijn in wat voor functie dan ook.

3

#### Informatiebeveiligingsbeleid HAN

Betrokkenheid van het bestuur is dus noodzakelijk, maar niet voldoende. IB is namelijk nadrukkelijk **ieders** verantwoordelijkheid binnen de HAN. Dit zal worden uitgedragen zowel langs formele weg, als via bewustwordingscampagnes. Een speciale plek is er daarbij voor het lijnmanagement: die hebben de taak om randvoorwaardelijk en curatief toe te zien op goede IB.

Kortom, informatiebeveiliging zal het best werken wanneer de **hele** organisatie participeert. Dit is een continu proces. Dit beleid is daarvoor het uitgangspunt. Beschreven worden niet alleen de voornoemde aspecten, maar ook welke rollen ingevuld moeten worden, hoe IB onderdeel is van de *Planning & Control* cyclus, hoe beveiligingsincidenten aangepakt worden (en hoe ze beter te voorkómen), welke wettelijke randvoorwaarden bestaan, enzovoorts.

Qua rolverdeling springen een aantal cruciale rollen eruit:

- De ISO, de *Information Security Officer*: een rol op strategisch niveau. De ISO heeft direct toegang tot het bestuur en is zelf geen lijnverantwoordelijke. Zijn taak is te waken over IB, lastige vragen te stellen, auditing voor te bereiden en beleid en aanbevelingen te formuleren.
- ISM's: *Information Security Managers* die op tactisch (en operationeel) niveau opereren en daarmee de verbindende schakel vormen tussen het strategische niveau waarop de ISO opereert, en de dagelijkse inrichting en uitvoering van IB.
- CERT: het *Computer Emergency Response Team*, de brandweer van de IB, die net als de "gewone" brandweer zowel preventief als curatief opereert.

## Informatiebeveiligingsbeleid HAN

### 1. Inleiding

#### 1.1. Algemeen

Onder informatiebeveiliging wordt verstaan: het treffen en onderhouden van een samenhangend pakket aan maatregelen om de kwaliteitsaspecten beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening te waarborgen.

De kwaliteitsaspecten:

- **Beschikbaarheid:** werken de middelen/processen, zijn ze “in de lucht”?
- **Integriteit:** is de inhoud van de informatiestromen beveiligd, dat wil zeggen is het zeker dat er niet mee geknoeid is of kan worden?
- **Vertrouwelijkheid:** hebben alleen die mensen toegang tot bepaalde informatie die daartoe gemachtigd zijn, en is het voor anderen ontoegankelijk c.q. onleesbaar?

Hierbij gaat het ook om de controleerbaarheid<sup>1</sup> van de maatregelen die genomen zijn om deze kwaliteitsaspecten te borgen.

Informatiebeveiliging is een beleidsverantwoordelijkheid van het bestuur van de HAN. Zoals overal in de maatschappij is ook bij de HAN sprake van toenemende afhankelijkheid van informatie en computersystemen, waardoor nieuwe kwetsbaarheden en risico's kunnen optreden. Het is van belang hiertegen adequate maatregelen te nemen. Immers, onvoldoende informatiebeveiliging kan leiden tot onacceptabele risico's voor het bedrijfsproces van de HAN. Incidenten en inbreuken in deze processen kunnen leiden tot financiële schade en imagoschade.

Informatiebeveiliging zelf is géén primair of secundair proces, géén *core business*, maar als je er niets aan doet gaat het wel **ten koste van** de *core business*: informatiebeveiliging is een *business enabler* van de eerste categorie.

De HAN heeft de ambitie om met het onderhavige beleidsdocument informatiebeveiliging structureel naar een hoog niveau te brengen en daar te houden door de aspecten *governance* (inclusief *auditing* en *feedback*), wet- en regelgeving, de organisatie van de beveiligingsfunctie en het informatiebeveiligingsbeleid – ook in hun onderlinge relatie – duidelijk te beschrijven en vast te stellen.

<sup>1</sup> Controleerbaarheid: de mate waarin het mogelijk is om achteraf parameters die van belang zijn voor beschikbaarheid, integriteit of vertrouwelijkheid te verifiëren. Zulke parameters zijn bijvoorbeeld *downtime*, toegang en transacties.

## Informatiebeveiligingsbeleid HAN

### 1.2. Doelgroep

Het informatiebeveiligingsbeleid bij de HAN richt zich primair op bestuur en hoger management, de beveiligingsorganisatie en leidinggevenden. Het is van toepassing op alle medewerkers, studenten en derden. Kortom, op iedereen die - intern dan wel extern - op enige manier te maken heeft met (aspecten van) het bedrijfsproces van de HAN.

### 1.3. Reikwijdte van het beleid

Bij de HAN wordt informatiebeveiliging breed geïnterpreteerd. Informatiebeveiliging betreft dus alle vormen van informatie waar de HAN voor verantwoordelijk is. Het betreft hier niet alleen digitale informatie, maar bijvoorbeeld ook informatie op papier.

Er bestaat een belangrijke relatie en een gedeeltelijke overlap met zaken als sociale veiligheid, fysieke beveiliging en bedrijfscontinuïteit. Op strategisch niveau wordt aandacht geschonken aan deze raakvlakken en wordt zowel planmatig als inhoudelijk afstemming gezocht. Vaak wordt daarvoor de term "integrale veiligheid" gebruikt.

Informatiebeveiligingsbeleid HAN

## 2. Doelstelling

Als *mission statement* geldt:

**Het informatiebeveiligingsbeleid bij de HAN heeft als doel het waarborgen van de continuïteit van het bedrijfsproces<sup>2</sup>, het minimaliseren van de schade door het voorkómen van beveiligingsincidenten en het minimaliseren van eventuele gevolgen van deze incidenten.**

Daarmee is informatiebeveiligingsbeleid direct ondersteunend aan de missie en het proces van de instelling als geheel. De eindverantwoordelijkheid ligt derhalve bij het bestuur van de HAN.

Uit dit *mission statement* komen de volgende afgeleide doelstellingen voort:

- Kader: het beleid biedt een kader om (toekomstige) maatregelen in de informatiebeveiliging te toetsen aan een vastgestelde best practice (of norm) en om de taken, bevoegdheden en verantwoordelijkheden in de instelling te beleggen.
- Normen: de basis voor de inrichting van het informatiebeveiligingsmanagement is dit beleidsdocument, waarvoor ISO 27001 als inspiratie diende. Formele certificering conform ISO 27001 acht het bestuur niet wenselijk, omdat dat niet past bij de gewenste cultuur van de HAN.
- Maatregelen: maatregelen worden genomen op basis van *best practices* in de SURF doelgroep, waarbij het op ISO 27002 gebaseerde *Baseline Informatiebeveiliging* en het *Normenkader SURFaudit* als uitgangspunt wordt genomen.
- Expliciet vastgestelde beveiligingsorganisatie: uitgangspunten en organisatie van informatiebeveiligingsfuncties zijn vastgelegd en worden gedragen door het bestuur, en afgeleid daarvan, door de hele instelling.
- Daadkrachtige procesbenadering: duidelijke keuzes in maatregelen, actieve controle op beleidsmaatregelen en de uitvoering daarvan.
- *Compliance*: het beleid biedt de basis om te voldoen aan wettelijke voorschriften.

<sup>2</sup> Onderwijs en onderzoek worden nadrukkelijk als onderdelen van het bedrijfsproces gezien.

Informatiebeveiligingsbeleid HAN

### 3. Beleidsprincipes informatiebeveiliging

#### 3.1. Beleidsuitgangspunten en principes

Informatiebeveiligingsmanagement wordt als proces ingericht. De HAN kiest ervoor om de jaarlijkse planning en controlecyclus te baseren op "Plan, Do, Check, Act" (zie nevenstaande figuur). Hierin worden jaarlijks planningen gemaakt en uitgevoerd. De resultaten ervan worden geëvalueerd en vertaald naar nieuwe jaarplanningen.



De beleidsuitgangspunten bij de HAN zijn:

- De HAN acht een goede informatiebeveiliging en privacybescherming en de bijbehorende bewustwording van groot belang.
- De HAN is een instelling met een open karakter: Adequate informatiebeveiliging is daarbij wel een randvoorwaarde. Er wordt van medewerkers, studenten en derden verwacht dat ze zich qua techniek en ook qua houding 'fatsoenlijk' gedragen (eigen verantwoordelijkheid). Niet acceptabel is dat door al dan niet opzettelijk gedrag onveilige situaties ontstaan die leiden tot schade en/of imagoschade. Het is om deze reden dat er gedragscodes zijn geformuleerd en geïmplementeerd.
- Het succes van beveiliging staat of valt met goede communicatie. Goede communicatie wordt daarom actief bevorderd, op en tussen alle niveaus in de instelling.
- De informatiebeveiliging dient de volgende aspecten te waarborgen:
  - Beschikbaarheid
  - Integriteit
  - Vertrouwelijkheid.
- Bij elke informatie-inrichting wordt ter bevordering van informatiebeveiliging en privacybescherming het principe van *least privileges* gehanteerd, wat wil zeggen dat er naar wordt gestreefd om steeds niet meer dan die rechten te verlenen die nodig zijn voor adequate functie- en bedrijfsuitoefening.

De HAN hanteert de volgende beleidsprincipes:

- Informatiebeveiliging is ieders verantwoordelijkheid. Verwachtingen t.a.v. individuen: communiceer met medewerkers, studenten en derden dat er van hen verwacht wordt dat ze actief bijdragen aan de veiligheid van geautomatiseerde systemen en de daarin opgeslagen informatie. Dat gebeurt bij indiensttreding, met een gedragscode, met periodieke bewustwordingscampagnes, in contracten met tijdelijk personeel en leveranciers, enzovoorts. Het zo nodig opleggen van sancties na overtredingen maakt het geheel geloofwaardig.

8



#### Informatiebeveiligingsbeleid HAN

- Informatiebeveiliging is een lijnverantwoordelijkheid: dat betekent dat de leidinggevenden de verantwoordelijkheid dragen voor een goede informatiebeveiliging in hun groep, afdeling, instituut, faculteit, enzovoorts. Dit omvat ook de keuze van maatregelen en de uitvoering en handhaving ervan binnen de gestelde kaders.
- Informatiebeveiliging is een procesverantwoordelijkheid: dat betekent dat de procesverantwoordelijken de primaire verantwoordelijkheid dragen voor een goede beveiliging van de gegevens die in hun proces verwerkt worden. Dit omvat ook de keuze van maatregelen en de uitvoering en handhaving ervan.
- Informatiebeveiliging is een continu proces. Regelmatige herijking van beleid is nodig evenals audits: technologische en organisatorische ontwikkelingen binnen en buiten de HAN maken het noodzakelijk om periodiek te bezien of men nog wel op de juiste wijze bezig is de beveiliging te waarborgen. De audits maken het mogelijk het beleid en de genomen maatregelen te controleren op effectiviteit en efficiëntie.
- Eigendom van informatie: de HAN is in beginsel eigenaar van de informatie die onder haar verantwoordelijkheid wordt geproduceerd. Daarnaast beheert de HAN informatie, waarvan het (intellectueel) eigendom toebehoort aan derden. Medewerkers, studenten en derden dienen goed geïnformeerd te zijn over het (her)gebruik van deze informatie.
- Waardering van informatie: iedereen behoort de waarde van informatie te kennen en daarnaar te handelen. Deze waarde wordt bepaald door de schade als gevolg van verlies van beschikbaarheid, integriteit en vertrouwelijkheid. Classificatie kan hierbij behulpzaam zijn.
- De HAN streeft ernaar om alle gegevens en systemen waarop dit informatiebeveiligingsbeleid van toepassing is te classificeren. Daarbij wordt gekeken naar de aspecten beschikbaarheid, integriteit en vertrouwelijkheid. Voor elk van deze aspecten wordt een klein aantal klassen gedefinieerd. Het niveau van de beveiligingsmaatregelen is afhankelijk van deze klassen. De huidige stand van zaken qua classificatie is te vinden in Bijlage A - Classificatie.
- Bij elke mutatie, zoals infrastructurele wijzigingen, (IT)projecten of de aanschaf van nieuwe systemen wordt reeds in het vroegst mogelijke stadium rekening gehouden met informatiebeveiliging.

Informatiebeveiligingsbeleid HAN

#### 4. Wet- en regelgeving

Bij de HAN wordt op de volgende wijze omgegaan met relevante wet- en regelgeving:

##### C.1. Algemene Verordening Gegevensbescherming (AVG)

De HAN heeft de wettelijke *privacy* vereisten met betrekking tot beveiliging ingebed in dit beleid. Handelen conform dit beleid leidt in beginsel tot voldoen aan de beveiligingsvereisten uit de wet.

##### C.2. Archiefwet

De HAN houdt zich aan de wettelijke voorschriften ten aanzien van bewaartermijnen, zoals die bijvoorbeeld in de Archiefwet zijn vastgelegd.

##### C.3. Telecommunicatiewet

Zolang het netwerk van de instelling niet openbaar is, is de Telecommunicatiewet niet van toepassing. Wanneer wel (ten dele) een openbaar netwerk wordt aangeboden, dan moet aan de Telecommunicatiewet worden voldaan en dus de bijbehorende maatregelen (separaat) worden geïmplementeerd. Voorbeeld: de HAN hoeft geen toestemming te vragen voor het opslaan van cookies voor heb.han.nl, maar wel voor www.han.nl.

##### C.4. Wet Computercriminaliteit

De Wet Computercriminaliteit richt zich op de strafrechtelijke probleemgebieden in relatie tot het computergebruik. De wet bestaat uit artikelen die op diverse plekken zijn toegevoegd aan het WvS. De extra artikelen houden zich bezig met:

- Vernieling en onbruikbaar maken
- Aftappen van gegevens
- *Denial of service*, verstikkingsaanval
- Computervredebreek
- Diensten afnemen zonder betalen
- Malware, kwaadaardige software

Evenwel zorgen het naleven van dit informatiebeveiligingsbeleid en het implementeren van basismaatregelen ervoor dat de HAN een basisniveau van beveiliging heeft. Indien er aanvallen op de HAN plaatsvinden die die beveiliging significant doorbreken en die vallen onder de Wet Computercriminaliteit, zal de HAN in beginsel aangifte doen.

#### 5. Governance informatiebeveiligingsbeleid

Het goed, efficiënt en verantwoord leiden van een instelling wordt aangeduid met de term *governance*. Het omvat vooral ook de relatie met de belangrijkste belanghebbenden van de HAN, zoals de proceseigenaren, medewerkers, studenten, klanten en derden. Een goede *governance* zorgt er voor dat alle

10

## Informatiebeveiligingsbeleid HAN

belanghebbenden hun rechten en plichten kennen.

In dit hoofdstuk worden diverse rollen onderscheiden. Het aantal rollen is als regel groter dan het aantal personen dat die rollen vervult.

### 5.1. Afstemming met samenhangende Risico's

Onderdeel van *governance* is dat aan alle soorten risico's en hun onderlinge verwevenheid passende aandacht geschonken wordt. Het is om die reden dat bij de HAN op strategisch niveau zowel aandacht geschonken wordt aan informatiebeveiliging, als aan zaken als sociale veiligheid, fysieke beveiliging en bedrijfscontinuïteit. Immers, samenwerking op het gebied van deze risico's is een noodzakelijke voorwaarde voor goede *governance*. Dit wordt bevorderd door de planningscyclus voor deze gebieden zo veel mogelijk parallel te laten verlopen. Daardoor kan de gewenste kruisbestuiving optreden. Waar mogelijk en nodig wordt deze afstemming ook vertaald naar het tactische en operationele niveau.

In dit hoofdstuk wordt verder ingegaan op de *governance* van de informatiehuishouding (verder *I-governance* te noemen) en de positionering van informatiebeveiliging daarin.

### 5.2. Inpassing in *I-governance*

In deze paragraaf wordt beschreven hoe informatiebeveiliging als onderdeel van *I-governance* is georganiseerd en wie waarvoor verantwoordelijk is. Van belang daarbij is om onderscheid te maken naar richtinggevend of strategisch, sturend of tactisch en uitvoerend niveau. Wat betreft de benaming van rollen wordt zoveel mogelijk aangesloten bij een landelijke beschrijving van die rollen<sup>3</sup>.

<sup>3</sup> Volgens "Functies in de informatiebeveiliging", Platform voor Informatiebeveiliging (PvIB), 2006

## Informatiebeveiligingsbeleid HAN

De governance structuur samengevat in een tabel:

Niveau	Wat?	Wie?	Overleg	Documenten
<b>Richtinggevend</b>	Bepalen IB strategie. Organisatie t.b.v. IB inrichten, IB planning en control vaststellen.  Communicatie naar management en organisatie.	Bestuur, in het bijzonder de portefeuillehouder IB, op basis van advies ISO en hoofd Service Unit ICT.	Bestuur stelt vast. I-Klankbord groep adviseert.	Beleidsplan Baselines (basismaatregelen).
<b>Sturend</b>	Planning & Control IB: <ul style="list-style-type: none"> <li>• voorbereiden normen en wijze van toetsen,</li> <li>• evalueren beleid en maatregelen,</li> <li>• begeleiding audits</li> </ul> Communicatie naar proceseigenaren.	ISO, ISM's, Proces- en systeemeigenaren, Leidinggevenden.	Tactisch IB overleg.	Interne audits en SURFaudit, Jaarplan en -verslag.
<b>Uitvoerend</b>	Implementeren IB maatregelen, Registreren, afhandelen en evalueren incidenten, Communicatie richting eindgebruikers.	Beheerders in samenwerking met ISM, CERT.	Operationeel beheerders overleg, CERT overleg.	Overeenkomsten industrieel SLA's, Incidentregistratie ind. evaluatie.

Op instellingsniveau is het bestuur juridisch gezien eindverantwoordelijk voor informatiebeveiliging. Deze verantwoordelijkheid wordt in de instelling verder belegd.

De *Information Security Officer* of ISO is een rol op strategisch (en tactisch) niveau. Hij adviseert aan het bestuur. De ISO bewaakt de uniformiteit ten aanzien van informatiebeveiliging binnen de instelling en dient gevraagd zowel als ongevraagd het bestuur van advies. Vanwege de grote samenhang tussen informatiebeveiliging en bescherming persoonsgegevens combineert de HAN deze rol met die van Functionaris Gegevensbescherming.

De rol van *Information Security Manager* of ISM is vormgegeven op het stafniveau van instituten, faculteiten en service units. De ISM vervult een rol bij de vertaling van de strategie naar tactische (en operationele) plannen. Dit doet hij samen met de ISO (vanwege de uniformiteit) en de proceseigenaren. Er is één ISO en er kunnen meerdere *Information Security Managers* (ISM's) zijn.

Op operationeel niveau overleggen de ISM's met de functionele beheerders en relevante IT-functionarissen met als belangrijkste onderwerp de implementatie van de informatiebeveiligingsmaatregelen.

#### Informatiebeveiligingsbeleid HAN

De financiering van informatiebeveiliging wordt bij de HAN geregeld conform hieronder beschreven.

Algemene zaken, zoals het opstellen van een informatiebeveiligingsplan voor de instelling of een externe audit, worden uit de algemene middelen betaald. Algemene instellingsbrede bewustwordingscampagnes en trainingen worden eveneens uit deze middelen betaald.

De beveiliging van informatiesystemen, inclusief de kosten daarvan, zijn integraal onderdeel van verantwoord beheer van het betreffende informatiesysteem. Beveiligingskosten van werkplekken maken integraal onderdeel uit van de werkplekkosten. Voorlichting en training voor specifieke toepassingen of doelgroepen worden uit decentrale middelen betaald.

#### 5.3. Documenten informatiebeveiliging

Voor informatiebeveiliging wordt bij de HAN dezelfde managementcyclus gevolgd, die doorgaans voor andere onderwerpen geldt: visie/idee, beleid, analyse, plan implementatie, uitvoering, controles en evaluatie.

In het kader van informatiebeveiliging hanteert de HAN de volgende documenten:

1. Dit Informatiebeveiligingsbeleid:  
Het Informatiebeveiligingsbeleid ligt ten grondslag aan de aanpak van informatiebeveiliging door de HAN. In het Informatiebeveiligingsbeleid worden de randvoorwaarden en uitgangspunten vastgelegd en wordt richting gegeven aan de vertaling van het beleid in concrete maatregelen. Om er voor te zorgen dat het beleid gedragen wordt binnen de instelling en die er ook naar handelt wordt het uitgedragen door (of namens) het bestuur. Het informatiebeveiligingsbeleid wordt opgesteld door de ISO en vastgesteld door het bestuur.
2. Jaarplan/verslag:  
Elk jaar levert de ISO een jaarverslag en een jaarplan voor het volgende jaar in bij het bestuur. Het jaarplan is mede gebaseerd op de resultaten van de periodieke controles / audits. Er wordt o.a. ingegaan op incidenten, resultaten van risicoanalyses (incl. genomen maatregelen) en andere initiatieven die het afgelopen jaar hebben plaatsgevonden. Dergelijke verslagen kunnen geconsolideerd worden in de bestuurlijke Planning & Control-cyclus. Waar nodig wordt apart aandacht besteed aan specifieke systemen/applicaties.
3. Baseline van IT informatiebeveiligingsmaatregelen (basisniveau maatregelen):  
De baseline van beveiligingsmaatregelen wordt per gegevensgroep of informatiesysteem vastgesteld en volgt uit de betreffende interne audit. De baseline is daarmee geen vooraf vastgesteld document.
4. Policies:  
Gedragscodes en richtlijnen voor medewerkers, studenten en derden, al dan niet voor specifieke doelgroepen, op het gebied van informatiebeveiliging. Met name:

13

## Informatiebeveiligingsbeleid HAN

- Reglement omgaan met gegevens en informatievoorzieningen (gepubliceerd op Insite);
- Privacyreglement (gepubliceerd op Insite);
- Richtlijn classificatie (bijlage A);
- Logisch toegangsbeleid digitale voorzieningen HAN (richtlijn voor authenticatie en autorisatie; bijlage B);
- Richtlijn responsible disclosure (bijlage C);
- RFC-2350 voor de lokale CERT (gepubliceerd op [www.han.nl](http://www.han.nl))

Met opmerkingen [JG1]: Nog naar stuk van de VU kijken

Daarnaast is informatiebeveiliging een vast onderdeel van de volgende documenten:

5. Overeenkomsten met leveranciers van informatiesystemen (waaronder ook SLA's: Service Level Agreements), inhuur- en uitbestedingscontracten: Bij de inhuur van personeel, maar ook bij de inkoop van middelen (met name hardware, software en applicatie- / cloudplatforms), wordt expliciet aandacht aan informatiebeveiliging besteed, onder andere door dit beleid ook toe te passen op externen en door beveiliging standaard onderdeel van de inkoopvoorwaarden te maken. Afspraken worden in een contract met de leverancier vastgelegd. In deze contracten zijn de verantwoordelijkheden van de leverancier opgenomen. Als basis hiervoor dient het SURF Juridisch Normenkader Cloudservices Hoger Onderwijs.

### 5.4. Controle, naleving en sancties

Bij de HAN is de ISO verantwoordelijk voor de interne audits en voor de uitvoering van het informatiebeveiligingsjaarplan. De ISM's ondersteunen daarbij.

De bedrijfskritische informatiesystemen van de HAN worden intern geaudit, in samenhang met de processen die van deze systemen gebruikmaken. Deze audits richten zich op de classificatie van de in het informatiesysteem vastgelegde gegevens, op de inventarisatie van de risico's, op de genomen beveiligingsmaatregelen en op de samenhang tussen deze drie onderwerpen. De audits richten zich zowel op informatiebeveiliging als op de bescherming van persoonsgegevens.

De interne audit vindt tenminste eens per twee jaar plaats. Indien een informatiesysteem wordt vervangen of indien zich significante wijzigingen voordoen in de implementatie van de beveiliging wordt op dat moment een audit uitgevoerd. De externe controle wordt eens in de twee jaar uitgevoerd middels SURFaudit. De HAN wordt dan geaudit door "peers" uit het Hoger Onderwijs.

Het Normenkader SURFaudit is het kader voor zowel interne als externe controles.

De bevindingen van de interne en externe controles, evenals mogelijke externe ontwikkelingen rond beveiliging, zijn input voor de nieuwe informatiebeveiligingsjaarplannen van de HAN. Deze kunnen ook tot wijziging van dit beleid

## Informatiebeveiligingsbeleid HAN

leiden.

De naleving bestaat uit concreet toezicht op de dagelijkse praktijk van de informatiebeveiliging. Van belang hierbij is dat mensen elkaar aanspreken in geval van tekortkomingen.

Mocht de naleving ernstig tekort schieten, dan kan de HAN de betrokken medewerkers of studenten een sanctie opleggen, binnen de kaders van arbeids- en studieovereenkomsten en de wettelijke mogelijkheden. Dit is primair een verantwoordelijkheid van de betrokken leidinggevenden en het bestuur.

### 5.5. Bewustwording en training

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van informatiebeveiliging uit te sluiten. De mens zelf creëert de grootste risico's. Daarom wordt bij de HAN het bewustzijn voortdurend aangescherpt, zodat kennis van risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd.

Onderdeel van het beleid zijn regelmatig terugkerende bewustwordingscampagnes voor medewerkers, studenten, derden en met name operationele beheerders. Verhoging van het beveiligingsbewustzijn is zowel een verantwoordelijkheid van de leidinggevenden, als de ISO en de ISM('s); uiteindelijk is hiervoor het bestuur verantwoordelijk. Dit alles laat onverlet dat elke beveiliging faalt als deze niet gedragen wordt door de medewerkers – elke medewerker is mede verantwoordelijk voor goede beveiliging. Dit is een cruciaal onderdeel van bewustwording en wordt randvoorwaardelijk ondersteund in het personeelsbeleid.

### 5.6. Organisatie van de informatiebeveiligingsfunctie

Om informatiebeveiliging gestructureerd en gecoördineerd op te pakken onderkent de HAN een aantal rollen die aan functionarissen in de bestaande instelling zijn toegewezen.

#### **Bestuur**

Het bestuur is verantwoordelijk voor de informatiebeveiliging bij de HAN en stelt het beleid en de basismaatregelen op het gebied van informatiebeveiliging vast. Informatiebeveiliging komt zo vaak als nodig en minimaal 3x per jaar op de agenda van het bestuur. Het bestuur wijst één van haar leden aan als portefeuillehouder informatiebeveiliging.

De inhoudelijke verantwoordelijkheid voor informatiebeveiliging is door de portefeuillehouder gemandateerd aan de ISO. Deze heeft de opdracht om op de informatiebeveiliging van de gehele instelling toe te zien.

#### **Information Security Officer (ISO)**

De ISO is een rol op strategisch (en tactisch) niveau. Hij adviseert aan het bestuur. De ISO formuleert het beveiligingsbeleid, helpt bij een juiste vertaling daarvan

15



#### Informatiebeveiligingsbeleid HAN

naar instellingsonderdelen, ziet toe op de (uniforme) naleving ervan en rapporteert over lacunes, inconsistenties en onvolkomenheden. Hij heeft de bevoegdheid om onderzoek te doen of laten doen (audits) en informatie op te vragen en in principe ook te krijgen, tenzij privacy in het geding is – in alle bijzondere gevallen beslist het bestuur. De ISO kan zowel gevraagd als ongevraagd van advies dienen.

#### **Information Security Manager (ISM)**

De ISM vervult een rol bij de vertaling van de strategie naar tactische (en operationele) plannen. Dit doet hij samen met de ISO (vanwege de uniformiteit) en met de proces- en systeemeigenaren. Tevens adviseert de ISM over specifieke informatiebeveiligingsmaatregelen in projecten – variërend van allerhande staande projecten tot acquisities van bijvoorbeeld software of hardware.

#### **Proceseigenaar**

Een proceseigenaar is iemand die verantwoordelijk is voor een van de primaire of ondersteunende processen, al dan niet gebruikmakend van informatiesystemen.

#### **Systeemeigenaar**

Een systeemeigenaar is iemand die verantwoordelijk is voor een informatie-systeem, waarmee een of meerdere processen worden ondersteund.

#### **Leidinggevende**

Naleving van het informatiebeveiligingsbeleid is onderdeel van het integrale bedrijfsproces. Iedere leidinggevende heeft de taak om:

- er voor te zorgen dat hun medewerkers c.q. studenten op de hoogte zijn van (de voor hen relevante aspecten van) het beveiligingsbeleid;
- toe te zien op de naleving van het beveiligingsbeleid door medewerkers en studenten;
- periodiek het onderwerp informatiebeveiliging onder de aandacht te brengen in werkoverleggen;
- als aanspreekpunt beschikbaar te zijn voor alle personeel gerelateerde informatiebeveiligingszaken.

De leidinggevende kan hierin ondersteund worden door de ISO.

#### **Interne auditor**

De interne auditor controleert jaarlijks het goed en betrouwbaar functioneren van de interne processen. Dit omvat o.a.: de structuur en verantwoordelijkheden van de organisatie, de hardware, de software, het interne- en externe netwerk, veiligheids- en calamiteitensystemen.

De interne auditor rapporteert aan de ISO.

#### **Functionaris Gegevensbescherming**

De FG houdt binnen de HAN toezicht op de toepassing en naleving van de AVG. De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie in de instelling.

## Informatiebeveiligingsbeleid HAN

### CERT-coördinator

De CERT-coördinator bij de HAN wordt benoemd door het bestuur op advies van de ISO. Hij is verantwoordelijk voor *information security incident management* binnen de instelling, en is in dat kader ook bevoegd het tijdelijk isoleren van computersystemen of netwerksegmenten te gelasten. De CERT-coördinator werkt voor het uitvoeren van deze taken samen met andere, formeel benoemde, CERT-leden.

### 5.7. Overleg

Om de samenhang in de organisatie van de informatiebeveiligingsfunctie goed tot uitdrukking te laten komen en de initiatieven en activiteiten op het gebied van informatiebeveiliging binnen de verschillende onderdelen op elkaar af te stemmen overlegt de HAN gestructureerd over het onderwerp informatiebeveiliging op diverse niveaus.

Op **strategisch** niveau wordt richtinggevend gesproken over *governance* en *compliance*, alsmede over doelen, scope en ambitie op het gebied van informatiebeveiliging. Dit gebeurt in het bestuur, geadviseerd door de ISO.

Op **tactisch** niveau wordt de strategie vertaald naar plannen, te hanteren normen, evaluatiemethoden, e.d. Deze plannen en instrumenten zijn sturend voor de uitvoering. Dit tactisch overleg wordt uitgevoerd door de ISO en ISM('s) in overleg met betrokken functionarissen zoals de CERT-coördinator en proceseigenaren.

Op **operationeel** niveau worden de zaken besproken die het dagelijkse bedrijfsproces aangaan in de zin van uitvoering en implementatie.

## 6. Melding en afhandeling van incidenten (CERT)

Incidentbeheer en -registratie hebben betrekking op de wijze waarop geconstateerde dan wel vermoede inbreuken op de informatiebeveiliging door medewerkers, studenten en derden gemeld worden en de wijze waarop deze worden afgehandeld.

Het is van belang om te leren van incidenten. Incidentregistratie en periodieke rapportage over opgetreden incidenten horen thuis in een volwassen informatiebeveiligingsomgeving. De HAN maakt daartoe gebruik van een CERT-meldpunt en heeft bekend gemaakt hoe dat is te benaderen.

Elke medewerker, student en derde is zelf verantwoordelijk voor het signaleren en melden van incidenten en inbreuken op informatiebeveiliging. Incidenten en inbreuken dienen direct gemeld te worden bij de ServiceDesk.

De incidenten worden afgehandeld en worden in het relevante operationeel overleg besproken en, als bedrijfsproces, financiën of goede naam in gevaar zijn, ook in het bestuur. Bij constatering van verontrustende trends kan hierop meteen

17

#### Informatiebeveiligingsbeleid HAN

worden ingespeeld, bijvoorbeeld door het nemen van extra maatregelen of een bewustwordingscampagne.

Het CERT houdt zich ook bezig met beveiligingsincidenten buiten de HAN als daar eigen medewerkers of studenten in enige rol bij betrokken zijn. In zulke gevallen wordt in principe gebruik gemaakt van de diensten van SURFcert, die wereldwijd in verbinding staat met andere CERT's.

De leden van het CERT zijn in die rol benoemd door de ISO en opereren in haar opdracht.

Het CERT heeft een document opgesteld waarin doelgroep, opdracht, bevoegdheden, escalaties, werkwijze (inclusief omgang met vertrouwelijkheid) en samenstelling zijn uitgewerkt. Daarin wordt o.a. vastgesteld wordt dat het CERT voor de HAN als geheel werkzaam is en haar opdracht direct van het bestuur van de HAN krijgt. Tevens worden directe escalaties naar het bestuursniveau (via de ISO) vastgelegd, evenals directe contacten met de afdelingen c.q. personen die binnen de HAN zorg dragen voor contacten met de pers, en voor juridische kwesties.

Het CERT is gerechtigd het tijdelijk isoleren van systeem/netwerkgebruikers, computersystemen of netwerksegmenten te gelasten ten einde haar taak uit te kunnen voeren.

Informatiebeveiligingsbeleid HAN

## 7. Referenties

HORA: Toolbox Hoger Onderwijs Referentie Architectuur  
<http://www.wikixl.nl/wiki/hora>

ISO 27001 : NEN-ISO/IEC 27001:2017  
<http://www.nen.nl>

ISO 27002 : NEN-ISO/IEC 27002:2017  
<http://www.nen.nl>

Normenkader SURFaudit:  
<http://www.surf.nl/diensten-en-producten/surfaudit/normenkader-surfaudit/index.html>

Juridisch Normenkader Cloudservices Hoger Onderwijs:  
<https://www.surf.nl/kennisbank/2013/surf-juridisch-normenkader-cloudservices.html>

## 8. Vaststelling & Wijziging

Het Informatiebeveiligingsbeleid wordt jaarlijks geëvalueerd op initiatief van de ISO van de Hogeschool van Arnhem en Nijmegen.

Dit beleid, versie **%versienummer%**, is vastgesteld door het bestuur van de Hogeschool van Arnhem en Nijmegen op **%datum%**.

Informatiebeveiligingsbeleid HAN

### Bijlage A – Classificatie

Bij de HAN zijn alle gegevens waarop dit informatiebeveiligingsbeleid van toepassing is geclassificeerd. Het niveau van de beveiligingsmaatregelen is afhankelijk van de klasse.

De classificatie van informatie is afhankelijk van de gegevens in het informatiesysteem en wordt bepaald op basis van risicoanalyses. Hierbij zijn de volgende aspecten van belang:

B = Beschikbaarheid	Is de informatie/functie aanwezig/buikbaar/leesbaar?
I = Integriteit	Is de informatie/functie betrouwbaar/compleet/onaangetast?
V = Vertrouwelijkheid	Hebben alleen rechthebbenden toegang tot de informatie/functie?

Ten aanzien van de beschikbaarheidseisen (B) worden de volgende klassen onderscheiden:

Classificatie B	Definitie
HOOG	Een uitval van meer dan 2 uur (in werktijd) heeft ernstige gevolgen voor de organisatie en is onacceptabel. Veel lessen vallen uit, mensen kunnen naar huis, Mogelijk slechte publiciteit, grote vervolgschade.
MIDDEN	Een uitval van maximaal 1 dag is acceptabel. Langere uitval heeft nadelige gevolgen. Sommige mensen kunnen hun werk niet meer doen, maar dit levert geen grote schade op.
LAAG	Het is niet erg als de voorziening een paar dagen niet beschikbaar is. Dit heeft weinig of geen gevolgen. Niemand merkt hier iets van of uitstel van het gebruik wordt geaccepteerd. Eventueel zijn er alternatieven beschikbaar.

Informatiebeveiligingsbeleid HAN

Voor integriteit (I) wordt de volgende indeling gevolgd:

Classificatie I	Definitie
HOOG	Onbetrouwbare (onjuiste, onvolledige, onrechtmatige of niet tijdig verwerkte) informatie is onacceptabel, of hooguit gedurende twee uur en een enkele keer in een aantal jaren.
MIDDEN	Onbetrouwbare (onjuiste, onvolledige, onrechtmatige of niet tijdig verwerkte) informatie is acceptabel, maar hooguit gedurende twee uur tot één dag, en niet meer dan een enkele keer per jaar.
LAAG	Onbetrouwbare (onjuiste, onvolledige, onrechtmatige of niet tijdig verwerkte) informatie is acceptabel, gedurende één of meerdere dagen en meerdere keren per jaar.

Voor vertrouwelijkheid (V) wordt de volgende indeling gevolgd:

Classificatie V	Definitie
HOOG	Kennisname van informatie door onbevoegden is onacceptabel, of hooguit een enkele keer in een aantal jaren.
MIDDEN	Kennisname van de informatie door onbevoegden is acceptabel, maar alleen als het gaat om HAN-medewerkers, of anders een enkele keer per jaar.
LAAG	De informatie is niet vertrouwelijk / het betreft publieke informatie.

Ten aanzien van alle aspecten BIV kunnen in bijzondere gevallen, bijvoorbeeld als gevolg van externe eisen, zwaardere klassen worden vastgesteld door het bestuur. De ISO zorgt ervoor dat zulke bijzondere klassen als uitzondering worden aangemerkt en behandeld.

Informatiebeveiligingsbeleid HAN

## Bijlage B Logisch toegangsbeleid digitale voorzieningen HAN

Versie: 28 november 2013, een eerdere versie is goedgekeurd in de STIB van 22 oktober 2013, in deze versie is het commentaar van KPMG verwerkt (mail van Wout van Kessel van 15/11/13)

### Inleiding

Een toegangsbeleid tot digitale voorzieningen kent twee componenten, een logische en een fysieke. De logische regelt de "virtuele" toegang tot de digitale middelen, de fysieke de toegang tot de ruimtes waarin en de apparatuur waarop de digitale voorzieningen fysiek draaien.

Het fysieke toegangsbeleid van de HAN is gebaseerd op hoofdstuk 9 "Fysieke beveiliging en beveiliging van de omgeving" van de Code voor Informatiebeveiliging (ISO 27002). Dit beleid wordt gevormd en uitgevoerd door de Service Unit ICT, in samenwerking met de Service Unit Facilitaire Zaken. De HAN hanteert een logisch toegangsbeleid, dat is gebaseerd op hoofdstuk 11 "Toegangsbeveiliging" van de Code voor Informatiebeveiliging (ISO 27002). In deze notitie wordt het voor veel systemen al bestaande toegangsbeleid geformaliseerd en gestandaardiseerd. Dit is nodig omdat uit de interne audits en uit het onderzoek van het CBP is gebleken, dat de HAN het toegangsbeleid onvoldoende beschreven heeft.

### Logisch toegangsbeleid

Uitgangspunt van dit beleid is dat elke aan de HAN verbonden persoon (student, medewerker, relatie) toegang heeft tot die applicaties en gegevens, die hij voor zijn activiteiten voor de HAN nodig heeft. Verder dient dit beleid aan wettelijke eisen te voldoen, met name aan de Wet Bescherming Persoonsgegevens (WBP). Tenslotte speelt de classificatie van de applicaties en de daarin vastgelegde gegevens op de aspecten Integriteit en Vertrouwelijkheid een bepalende rol, in combinatie met de geïnventariseerde risico's op beide aspecten.

Er wordt een onderscheid gemaakt tussen authenticatie en autorisatie. Authenticatie houdt in dat vastgesteld wordt dat als een persoon zich digitaal "meldt" dit ook werkelijk die persoon is. Authenticatie staat in beginsel los van applicaties. Authenticatie is de eerste stap, daarna volgt autorisatie. Autorisatie houdt in dat voor elke functie geregeld is wat een persoon met die functie in een applicatie mag doen: welke gegevens hij mag raadplegen en welke gegevens hij mag invoeren, wijzigen en / of verwijderen. Autorisatie wordt in beginsel per applicatie geregeld.

Het beleid puntsgewijs:

- Het toegangsbeleid geldt voor alle applicaties waarvan de HAN eigenaar is, en alle applicaties waarvan de HAN geen eigenaar is, maar middels een overeenkomst gebruik maakt
- Het al bestaande wachtwoordbeleid maakt deel uit van het toegangsbeleid (zie bijlage)
- De HAN stelt een HAN-account beschikbaar, waar nodig aangevuld met andere accounts

22



#### Informatiebeveiligingsbeleid HAN

- Voor authenticatie wordt het HAN-account gebruikt, tenzij dat onvoldoende beveiliging biedt. Het beheer van het HAN-account is beschreven en wordt conform de beschrijving uitgevoerd.
- Waar mogelijk wordt gebruik gemaakt van Single Sign On (SSO) en SURFconext, tenzij deze onvoldoende beveiliging bieden.
- Het autorisatiebeleid en -beheer worden per applicatie (in enkele gevallen per groep van applicaties) expliciet beschreven en op basis van de beschrijving geïmplementeerd. In de beschrijving komende de volgende onderwerpen aan de orde:
  - Hoe verloopt de authenticatie?
  - Welke autorisaties zijn er? Vaak zijn deze in de vorm van autorisatie rollen gedefinieerd.
  - Voor zo ver niet in het voorgaande punt geregeld: hoe wordt afgebakend welke gegevens toegankelijk zijn, bijvoorbeeld de afbakening in de organisatiestructuur. Hierna wordt dit "afbakening" genoemd.
  - Hoe worden autorisaties en afbakeningen gekoppeld aan functies en personen? Geef bijvoorbeeld in een matrix aan welke functie welke autorisatie en welke afbakening heeft.
  - Hoe worden autorisaties en afbakeningen uitgereikt, gewijzigd en ingetrokken?
  - Hoe worden autorisaties en afbakeningen geregistreerd en hoe houdt men die registratie bij?
  - Hoe en met welke periodiciteit wordt gecontroleerd of de actuele autorisaties en afbakeningen juist zijn en hoe wordt deze controle vastgelegd?
    - Voor applicaties die als Hoog op Integriteit en / of Vertrouwelijkheid geclassificeerd zijn is de periodieke controle minimaal eens per drie maanden.
    - Voor applicaties die als Midden op Integriteit en / of Vertrouwelijkheid geclassificeerd zijn (en op geen van beide als Hoog) is de periodieke controle minimaal eens per zes maanden.
    - Voor de overige applicaties is de periodieke controle minimaal eens per jaar
  - Hoe wordt het wachtwoordbeleid toegepast?
  - Bij elk van de voorgaande punten: wie is verantwoordelijk en wie voert uit?
  - Hoe wordt dit gecommuniceerd met de gebruikers
- De autorisaties van beheerders (functioneel beheer, applicatiebeheer en technisch beheer) worden apart beschreven. Het gaat hierbij niet alleen om toegang tot de applicatie, maar ook, indien van toepassing, om toegang buiten de applicatie om, bijvoorbeeld rechtstreekse toegang tot de database. In de beschrijving komende de volgende onderwerpen aan de orde:
  - Hoe verloopt de authenticatie?
  - Welke autorisaties zijn er? Vaak zijn deze in de vorm van autorisatie rollen gedefinieerd.

23

#### Informatiebeveiligingsbeleid HAN

- Voor zo ver niet in het voorgaande punt geregeld: hoe wordt afgebakend welke gegevens toegankelijk zijn, bijvoorbeeld de afbakening in de organisatiestructuur. Hierna wordt dit "afbakening" genoemd.
- Hoe worden autorisaties en afbakeningen gekoppeld aan functies en personen? Geef bijvoorbeeld in een matrix aan welke functie welke autorisatie en welke afbakening heeft.
- Hoe worden autorisaties en afbakeningen uitgereikt, gewijzigd en ingetrokken?
- Hoe worden autorisaties en afbakeningen geregistreerd en hoe houdt men die registratie bij?
- Hoe wordt het wachtwoordbeleid toegepast?
- Hoe en met welke periodiciteit wordt gecontroleerd of de actuele autorisaties en afbakeningen juist zijn en hoe wordt deze controle vastgelegd?
  - Voor applicaties die als Hoog op Beschikbaarheid, Integriteit en / of Vertrouwelijkheid geclassificeerd zijn is de periodieke controle minimaal eens per drie maanden.
  - Voor applicaties die als Midden op Beschikbaarheid, Integriteit en / of Vertrouwelijkheid geclassificeerd zijn (en op geen van drieën als Hoog) is de periodieke controle minimaal eens per zes maanden.
  - Voor de overige applicaties is de periodieke controle minimaal eens per jaar
- Bij elk van de voorgaande punten: wie is verantwoordelijk en wie voert uit?
- Voor die applicaties waarvan de Integriteit geclassificeerd is als Midden of Hoog is in het autorisatiebeleid in detail beschreven wie er gegevens mogen invoeren, wijzigen of verwijderen en welke gegevens dat zijn. Indien de classificatie Laag is hoeft dat niet (maar mag het wel).
- Voor die applicaties waarvan de Vertrouwelijkheid geclassificeerd is als Midden of Hoog is in het autorisatiebeleid in detail beschreven wie er gegevens mogen raadplegen en welke gegevens dat zijn.
- Als voor een beperkt deel van de gegevens in een applicatie een hogere classificatie op Integriteit en/of Vertrouwelijkheid geldt dan voor de overige gegevens kan daarvoor een restrictiever toegangsbeleid beschreven en geïmplementeerd worden om te voorkomen dat dat restrictieve beleid voor de gehele applicatie dient te gelden. Voorbeeld: SLB-notities in Alluris.
- De authenticatie is standaard op basis van account en wachtwoord (1-factor authenticatie). In de afweging tussen de classificatie van de Integriteit en / of de Vertrouwelijkheid enerzijds en de Risicoanalyse anderzijds kan gekozen worden voor extra beveiliging (met name 2-factor authenticatie dmv een SMS-code, een token en dergelijke). Die keuze ligt voor de hand in de combinatie van enerzijds classificatie Hoog op Vertrouwelijkheid en / of Integriteit en anderzijds grote beveiligingsrisico's.
- Het toegangsbeleid per applicatie wordt vastgesteld door de eigenaar van de informatievoorziening

24

Informatiebeveiligingsbeleid HAN

## **WACHTWOORDBELEID**

*Hogeschool van Arnhem en Nijmegen*

Versie: 1.0  
Datum: 25 augustus 2011

### **WACHTWOORDBELEID**

Alle gebruikers dienen het advies te krijgen om:

- a) wachtwoorden geheim te houden;
- b) wachtwoorden niet vast te leggen (bijvoorbeeld op papier of in bestand), tenzij deze registratie veilig kan worden opgeslagen en de methode van opslag is goedgekeurd;
- c) een wachtwoord te wijzigen zodra er aanwijzingen zijn dat onbevoegden dit wachtwoord weten;
- d) een wachtwoord te kiezen dat:
  - 1) een minimumlengte heeft van 8 tekens;
  - 2) gemakkelijk te onthouden is;
  - 3) iemand anders niet gemakkelijk kan raden;
  - 4) geen woord is dat in een woordenboek voorkomt;
  - 5) geen opeenvolgende gelijke tekens bevat en niet uitsluitend uit numerieke of alfabetische tekens bestaat;
- e) wachtwoorden met regelmatige tussenpozen te wijzigen;
- f) hergebruik van oude wachtwoorden te voorkomen;
- g) tijdelijk ingestelde wachtwoorden direct te wijzigen;
- h) geen individuele gebruikerswachtwoorden met anderen te delen;
- i) niet hetzelfde wachtwoord te gebruiken voor zakelijke en particuliere doeleinden.

Waar nodig (en mogelijk) kan de HAN besluiten één of meer van bovenstaande adviezen af te dwingen. Dit geldt in ieder geval voor:

- Wachtwoord van het HANaccount: minimaal 8 karakters en een verplichte jaarlijkse wijziging voor medewerkers.
- Wachtwoord van het beheeraccount: minimaal 8 karakters.

25

Informatiebeveiligingsbeleid HAN

## Bijlage C – Responsible Disclosure

De Hogeschool van Arnhem en Nijmegen vindt de veiligheid van haar systemen erg belangrijk. Ondanks de zorg voor de beveiliging van de systemen kan een zwakke plek voorkomen. Iedereen mag deze zwakke plekken bij ons melden.

Als je een zwakke plek in een van onze systemen vindt, dan horen wij dit graag. We kunnen dan zo snel mogelijk maatregelen treffen. Wij werken graag met je samen om onze gebruikers en systemen beter te kunnen beschermen.

### **Geen uitnodiging tot actief scannen**

Ons zogenoemde responsible disclosure beleid is geen uitnodiging om ons netwerk of onze systemen uitgebreid actief te scannen op zwakke plekken. Wij monitoren namelijk zelf ons bedrijfsnetwerk. De kans bestaat dat we je scan oppikken en onderzoeken, wat mogelijk leidt tot ongewenste gevolgen.

### **Strafrechtelijke vervolging**

Het is mogelijk dat je tijdens je onderzoek handelingen uitvoert die volgens het strafrecht strafbaar zijn. Heb je je aan onderstaande voorwaarden gehouden, dan ondernemen wij geen juridische stappen tegen je. Het Openbaar Ministerie heeft echter altijd het recht om zelf te beslissen of het je strafrechtelijk vervolgt.

### **Verzoek aan jou**

- Mail je bevindingen zo snel mogelijk naar [servicedesk@han.nl](mailto:servicedesk@han.nl). Wil je je bevindingen liever versleuteld aanleveren, stem dan vooraf de procedure af.
- Misbruik de gevonden zwakheid niet door bijvoorbeeld meer data te downloaden dan nodig is om het lek aan te tonen, of de gegevens te veranderen of verwijderen.
- Wees extra terughoudendheid bij persoonsgegevens.
- Deel de zwakheid niet met anderen totdat deze is opgelost.
- Maak geen gebruik van aanvallen op fysieke beveiliging of applicaties van derden, van social engineering, (distributed) denial-of-service attacks of spam.
- Geef voldoende informatie om de zwakheid te reproduceren, zodat wij deze zo snel mogelijk kunnen oplossen. Meestal zijn het IP-adres of de URL van het getroffen systeem en een omschrijving van de kwetsbaarheid en de uitgevoerde handelingen voldoende, maar bij complexere kwetsbaarheden kan meer nodig zijn.

### **Onze belofte**

- Wij reageren binnen 3 werkdagen met onze beoordeling van de melding en een verwachte datum voor een oplossing.
- Wij behandelen je melding vertrouwelijk en zullen je persoonlijke gegevens niet zonder je toestemming met derden delen, tenzij dat noodzakelijk is om een wettelijke verplichting na te komen.

26

#### Informatiebeveiligingsbeleid HAN

- Wij houden je op de hoogte van de voortgang van het oplossen van de zwakheid.
- Je kunt anoniem of onder een pseudoniem melden. Wij kunnen dan echter geen contact met je opnemen over bijvoorbeeld de vervolgstappen, voortgang van het dichten van het lek, publicatie of de eventuele beloning voor de melding.
- In berichtgeving over de gemelde zwakheid zullen wij, als je dit wilt, je naam vermelden als de ontdekker van de kwetsbaarheid.
- Wij kunnen je een beloning geven voor je onderzoek, maar zijn hiertoe niet verplicht. Je hebt dus niet zonder meer recht op een vergoeding. De vorm van deze beloning staat niet van tevoren vast en wordt door ons per geval bepaald. Of we een beloning geven en de vorm waarin dat gebeurt, hangen af van de zorgvuldigheid van je onderzoek, de kwaliteit van de melding en de ernst van het lek.

Wij streven ernaar om alle problemen zo snel mogelijk op te lossen en alle betrokken partijen op de hoogte te houden. Wij zijn graag betrokken bij een eventuele publicatie over de zwakheid, nadat deze is opgelost.

Deze responsible disclosure valt onder een Creative Commons Naamsvermelding 3.0-licentie. Het beleid is gebaseerd op het voorbeeldbeleid van [Floor Terra](#).

## 10.3 Data and system usage of HAN

Reglement voor medewerkers, vastgesteld door het CvB op 13-3-2018



Reglement omgaan met gegevens en informatiesystemen

Registratienummer: 2017/1243  
Vaststelling door CvB: 13-3-2018  
Instemming MR: 8-3-2018  
Inwerkingtreding: 13-3-2018

Dit reglement bevat voorschriften ten aanzien van het gebruik van HAN-gegevens en HAN-informatiesystemen door medewerkers van de Stichting Hogeschool van Arnhem en Nijmegen ("de HAN"), en dient in samenhang te worden gelezen met andere binnen de HAN geldende reglementen en beleidsdocumenten, waaronder in ieder geval:

- het Privacyreglement
- de Integriteitcode
- gouden HAN-regels voor informatiebeveiliging en privacy
- archiefbeheersregeling en Selectielijst Hogescholen
- klokkenluiderregeling

Deze documenten zijn te vinden op Insite.

### Artikel 1. Begripsbepaling

In dit reglement wordt verstaan onder:

#### *Gezagdrager*

Een lid van het College van Bestuur ("CvB"), een faculteitsdirecteur, de directeur van het Service Bedrijf, een instituutdirecteur of het hoofd van een Service Unit of een andere persoon die, of ingevolge de Wet op het Hoger onderwijs en Wetenschappelijk onderzoek, of middels een besluit of regeling van het CvB als bevoegd gezagdrager is aangewezen.

#### *Medewerker*

Een persoon die op basis van een arbeidsovereenkomst, overeenkomst van opdracht, detacheringsovereenkomst, uitzendovereenkomst of anderszins bij of voor de HAN werkzaam is.

#### *HAN-gegevens*

Alle gegevens, in welke verschijningsvorm dan ook, die voor of namens de HAN zijn aangemaakt (e-mail, documenten, afbeeldingen, video's, databases, etc.).

#### *HAN-informatiesystemen*

De door of namens de HAN ter beschikking gestelde digitale diensten en computer-, communicatie- en netwerkvoorzieningen, inclusief (maar niet uitsluitend) laptops, telefoons, printers, opslagsystemen en internettoegang.

## Artikel 2. Gebruik algemeen

2.1 De medewerker is gerechtigd gebruik te maken van de HAN-gegevens en HAN-informatiesystemen welke noodzakelijk zijn voor het uitvoeren van zijn of haar taken.

2.2 Indien de HAN voor bepaalde doeleinden HAN-informatiesystemen beschikbaar stelt (bijvoorbeeld voor e-mail of opslag), dan dient de medewerker deze HAN-informatiesystemen te gebruiken.

2.3 Het is de medewerker niet toegestaan de HAN-gegevens en HAN-informatiesystemen te gebruiken voor andere doeleinden dan voor het uitvoeren van zijn of haar werkzaamheden, met uitzondering van het bepaalde in artikel 2.4.

2.4 Privégebruik van HAN-informatiesystemen is buiten werktijd, of voor zover het werk er niet onder lijdt toegestaan. Beperkte opslag van privégegevens op HAN-informatiesystemen is toegestaan. Ook bij privégebruik dient de medewerker zich te houden aan de voorschriften in dit reglement.

2.5 De medewerker dient te allen tijde zorgvuldig om te gaan met zijn of haar persoonlijk inloggegevens en eventuele aanvullende authenticatiemiddelen (zoals sms, authenticatie-apps en tokens). Persoonsgebonden inloggegevens en aanvullende authenticatiemiddelen mogen niet worden overgedragen of gedeeld.

2.6 Het is niet toegestaan andermans inloggegevens te gebruiken of een ingelogd HAN-informatiesysteem achter te laten, zodanig dat anderen in de gelegenheid worden gesteld hiervan gebruik te maken. Bij een vermoeden van misbruik van inloggegevens behoudt de HAN zich het recht voor om direct het betrokken account te blokkeren.

2.7 Bij het beëindigen van de overeenkomst op basis waarvan de medewerker bij de HAN werkzaam is, dient uiterlijk op de dag van beëindiging de aan de medewerker in bruikleen gegeven HAN-gegevens en HAN-informatiesystemen door de medewerker te worden teruggegeven aan de HAN. De HAN zal na vertrek alle persoonlijke gegevens van de medewerker vernietigen, tenzij er een wettelijke plicht is deze gegevens te bewaren.

2.8 De medewerker dient vermoedelijke of gevonden onvolkomenheden in de beveiliging van HAN-informatiesystemen te melden bij de ServiceDesk (telefoon 024 – 353 16 66 of e-mail [servicedesk@han.nl](mailto:servicedesk@han.nl)).

## Artikel 3. Handelingen en gedragingen

3.1 Het is de medewerker niet toegestaan HAN-gegevens en HAN-informatiesystemen te gebruiken voor handelingen en/of gedragingen die in strijd zijn met de wet, de goede zeden, de openbare orde of dit reglement. Hieronder vallen onder meer, maar niet uitsluitend, de volgende handelingen en gedragingen:

- a. inbreuk plegen op auteursrechtelijk beschermde werk(en) of het anderszins handelen in strijd met (intellectuele eigendoms)rechten van de HAN of derden;
- b. bekijken, bewaren en/of verspreiden van pornografie of ander aanstootgevend beeldmateriaal;
- c. intimideren of op andere wijze lastig vallen van personen;
- d. online gokken;
- e. verspreiden van schadelijke software;
- f. het (pogen tot) binnendringen van een HAN-informatiesysteem of het (pogen tot) onbevoegd toegang verschaffen tot HAN-gegevens;
- g. je identiteit verhullen of je voordoen als iemand anders;
- h. het onnodig bezet houden of onnodig belasten van HAN-informatiesystemen;
- i. het opzettelijk berichten of mededelingen verzenden, te plaatsen of toegankelijk maken waarvan de medewerker wist of behoorde te weten dat de inhoud ongewenst of niet juist is.



#### Artikel 4. Omgaan met HAN-gegevens

4.1 Van de medewerker wordt zorgvuldigheid verwacht bij de omgang met HAN-gegevens. De medewerker dient alle redelijke maatregelen te nemen om te voorkomen dat onbevoegden toegang krijgen tot HAN-gegevens, ook wanneer deze HAN-gegevens zich niet op HAN-informatiesystemen bevinden. De medewerker houdt zich tenminste aan de "gouden HAN-regels voor informatiebeveiliging en privacy".

4.2 HAN-gegevens dienen te worden opgeslagen op HAN-informatiesystemen. Het tevens opslaan van HAN-gegevens op een niet door de HAN ter beschikking gesteld informatiesysteem is toegestaan, mits het niet gaat om (privacy)gevoelige, vertrouwelijke of bedrijfskritische informatie.

4.3 De medewerker dient privacygevoelige informatie (waaronder persoonsgegevens) die hij in het kader van het werk te weten komt, strikt vertrouwelijk te behandelen. Voor de verwerking van persoonsgegevens zijn aanvullende regels opgesteld die zijn vastgelegd in het Privacyreglement van de HAN.

4.4 De medewerker is op de hoogte van de geldende minimale en maximale bewaartermijnen van HAN-gegevens en houdt zich hieraan. Deze bewaartermijnen zijn te vinden in de HAN Archiefbeheersregeling en Selectielijst Hogescholen.

4.5 In geval van (tijdelijke) onbereikbaarheid dan wel nalatigheid van de medewerker, is de gezagdrager gerechtigd een vervanger toegang te verschaffen tot de bestanden en/of mailbox van de medewerker, doch uitsluitend indien aangetoond kan worden dat toestemming van de medewerker verkrijgen onmogelijk is en er een zwaarwegende reden van bedrijfsbelang is. De vervanger mag zich alleen toegang verschaffen tot de bestanden of mails die een relatie hebben met de zwaarwegende reden van bedrijfsbelang, doch echter niet tot als privé gemarkeerde mappen, bestanden of mails, of mails verzonden naar dan wel afkomstig van een vertrouwenspersoon, bedrijfsarts, medezeggenschap, HR of vakbond.

#### Artikel 5. Omgaan met communicatiemiddelen

5.1 De HAN ondersteunt de open dialoog en de uitwisseling van ideeën en het delen van kennis van de medewerker met collega's, studenten en derden via sociale media. De HAN verwacht van de medewerker professionaliteit in het communiceren, in welke vorm dan ook, zoals via e-mail of sociale media. Wanneer men zich als medewerker van de HAN presenteert op sociale media doet men dat op persoonlijke titel.

5.2 De medewerker dient privé en zakelijke communicatie zoveel mogelijk gescheiden te houden.

5.3 De medewerker plaatst geen gegevens, foto's, video's en dergelijke van andere medewerkers, studenten of HAN-relaties op sociale media zonder uitdrukkelijke toestemming van de betrokkene(n).

#### Artikel 6. Monitoring en controle

6.1 De HAN is gerechtigd om informatie over HAN-gerelateerde activiteiten te verzamelen voor controle ter voorkoming van schade, alsook voor controle in het kader van kosten- en capaciteitsbeheersing.

6.2 De in artikel 6.1 genoemde verzamelde informatie is alleen toegankelijk voor de verantwoordelijke beheerders. Bij vermoedens of constatering van misbruik kan hiervan worden afgeweken (zie artikel 7).

6.3 Verboden gebruik van de HAN-informatiesystemen, of specifiek gedrag dat tot grote kosten leidt of overlast veroorzaakt, wordt zoveel mogelijk beperkt of verhinderd.

## Artikel 7. Procedure bij misbruik

7.1 Vermoedens of constatering van misbruik van HAN-gegevens of HAN-informatiesystemen moeten bij de ServiceDesk worden gemeld. Melden kan via een e-mail naar [servicedesk@han.nl](mailto:servicedesk@han.nl) of via telefoonnummer 024 – 353 16 66. Anoniem melden bij de ServiceDesk is ook mogelijk via telefoonnummer #31#0243531666. Ontvangst van de melding wordt direct en vertrouwelijk geregistreerd en, indien mogelijk, per e-mail bevestigd. Als alternatief kan men zich tot een vertrouwenspersoon wenden, gebruik maken van de Klokkenuiderregeling of melding maken bij het meldpunt Integriteitcode.

7.2 De ServiceDesk wijst, zo nodig in overleg met de systeemeigenaar, een behandelaar toe die het vermoeden of de constatering van misbruik zal onderzoeken. Bij dit onderzoek is de behandelaar bevoegd om, indien hij dit voor het onderzoek noodzakelijk acht, bewijsmateriaal veilig te stellen en maatregelen te nemen om verder misbruik te voorkomen.

7.3 In geval van misbruik zal de behandelaar, afhankelijk van de situatie, de identiteit van de vermoedelijke misbruiker achterhalen en de betreffende gezagdrager inlichten. Tevens wordt de eigenaar van het betreffende HAN-informatiesysteem en/of de betreffende HAN-gegevens ingelicht over het gemelde misbruik.

7.4 De gezagdrager kan de behandelaar verzoeken het incident nader te onderzoeken. Uiterlijk twee weken na dit verzoek brengt de behandelaar schriftelijk rapport uit aan de gezagdrager over de uitkomsten van dit onderzoek.

7.5 De behandelaar is bevoegd om, indien hij dit voor de uitoefening van zijn werkzaamheden noodzakelijk acht, alle betrokken informatie over HAN-gerelateerde activiteiten en gegevens in te zien en hiervan kopieën te maken, met inachtneming van de geldende wetgeving en HAN-regelgeving.

7.6 Na het uitbrengen van het onderzoeksrapport door de behandelaar informeert de gezagdrager de medewerker schriftelijk en met redenen omkleed over de uitkomsten van het onderzoek, waarna de medewerker in de gelegenheid wordt gesteld zijn zienswijze te geven.

## Artikel 8. Maatregelen bij misbruik

8.1 Tegen de medewerker die in strijd handelt met de voorschriften uit dit reglement, alsmede tegen degene met wiens inloggegevens in strijd wordt gehandeld met dit reglement, kan de gezagdrager (disciplinaire) maatregelen treffen, conform hetgeen is opgenomen in de cao respectievelijk de overeenkomst op basis waarvan de medewerker bij de HAN werkzaam is.

8.2 Daarnaast kan de gezagdrager op basis van dit reglement onverwijld informatie (laten) verwijderen, blokkeren of andere (technische) maatregelen treffen indien dit noodzakelijk wordt geacht ter schadebeperking.

## Artikel 9. Rehabilitatie

Indien een klacht na onderzoek ongegrond blijkt en indien dit onderzoek de medewerker heeft benadeeld, dan volgt een passende rehabilitatie van de medewerker, tenzij de medewerker te kennen geeft geen rehabilitatie te wensen.

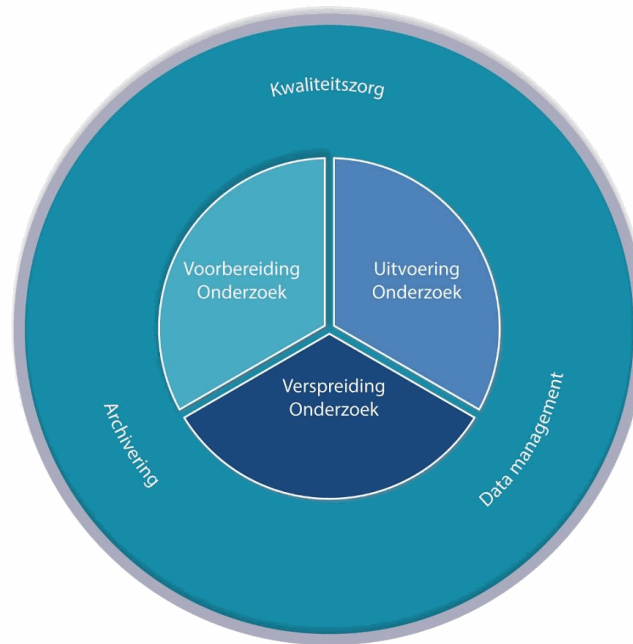
### Artikel 10. Onvoorziene gevallen

In die gevallen waarin dit reglement niet voorziet, beslist het College van Bestuur.

## 10.4 Data Management Plan of HAN

### Datamanagementplan HAN

*(ter ondersteuning van onderzoekers bij een professioneel databeheer)*



*Datamanagement, archivering en kwaliteitszorg ondersteunen onderzoek(ers) niet alleen tijdens een enkele onderzoeksfase maar gedurende het gehele onderzoeksproces.*

Datum:	12 februari 2018
Versie:	Versie 2.2
Aanvullingen in versie 2.0	<p>In versie 2.1:</p> <ul style="list-style-type: none"> <li>- beleid en regelgeving uit het document gehaald en in plaats daarvan naar de beleidspagina op Insite verwezen</li> <li>- hoofdstukken en toelichtingen beter op elkaar afgestemd</li> </ul> <p>In versie 2.2:</p> <ul style="list-style-type: none"> <li>- stappenplan en duidelijker introductie</li> <li>- mappen structuur R-schijf herzien</li> </ul>
Opdrachtgever:	Nanske Wilholt (programmamanager Onderzoek)
Auteur(s):	Imke Adams (beleidsmedewerker onderzoek SU00), Liesbeth Hoogkamp (projectleider SU FAZ/ICT), Yvonne van Wanrooij (archivaris SU FAZ/ICT),
Ondersteuning:	Ondersteuning bij het invullen van het datamanagement kunt u aanvragen via <a href="mailto:onderzoeksondersteuning@han.nl">onderzoeksondersteuning@han.nl</a>

## Inhoudsopgave

Introductie .....	3
Datamanagement stappen bij de HAN .....	5
1. Administratieve informatie .....	6
2. Financiële informatie en eigenaarschap .....	8
3. Data verzamelen en analyseren .....	10
4. Data opleveren: projectproducten (kennisdisseminatie) .....	12
5. Dataopslag tijdens en na het project .....	13
Bijlage 1 Dataopslag tijdens en na het project .....	16
Specificaties R-schijf bij de HAN .....	16
Surfdrive bij de HAN .....	18
HAN-Scholar en #OnderwijsOnline .....	19
Duurzame formaten .....	19

## Introductie

Datamanagement is het gestructureerd beheren van de onderzoeksdata die verzameld worden.<sup>1</sup> Welk type onderzoeksdata brengt een onderzoeksproject op? Wie heeft er toegang tot de data? Hoe sla je data veilig en duurzaam op? Door in een vroeg stadium over dit soort vragen na te denken en antwoorden te documenteren, voorkom je als onderzoeker problemen in een latere fase.

Het gestructureerd beheren van onderzoeksdata is ook van belang zodat je als onderzoeker transparant kan zijn over je dataverzameling, data analyse en data opslag. Fraudezaken in de afgelopen jaren hebben de noodzaak hiervan duidelijk naar voren gebracht (KNAW, 2012). Belangrijke thema's bij financiers en beleidsmakers in de onderzoeksweld zijn dan ook transparantie en verificerbaarheid van studies en het hergebruik van onderzoeksgegevens. Dit zal uiteindelijk leiden tot beter en efficiënter onderzoek. Voortbouwen op bestaande gegevens kan onderzoek immers versnellen en hergebruik van data kan leiden tot minder financiële kosten.

### Wat is een datamanagementplan?

Een hulpmiddel om gestructureerd na te denken over je datamanagement is een datamanagementplan (DMP). Soms stellen financiers een DMP als verplichting maar ook zonder dat, is het vooral een middel om onderzoekers te helpen de risico's te inventariseren ten aanzien van het beheer van onderzoeksdata gedurende het hele onderzoeksproces en daarna. Het draagt bij aan een efficiënt en effectief beheer, met oog voor risico's van verlies van data of andere bedreigingen waardoor de data onleesbaar en onbruikbaar worden, bijvoorbeeld door veroudering van software.

### Verantwoordelijkheden

Het is de verantwoordelijkheid van de onderzoeker zelf om een DMP (dit DMP óf op verzoek van een subsidieverstrekker een ander DMP) in te vullen en bij te houden. De HAN stimuleert het invullen van een DMP aan het begin van een onderzoeksproject. Omdat niet alles vooraf te voorzien is, is het aan te raden om het DMP als een "levend document" periodiek te herzien en nader aan te vullen. Ondersteuners van het studiecentrum kunnen hierbij helpen ([onderzoeksondersteuning@han.nl](mailto:onderzoeksondersteuning@han.nl)).

Een DMP kan in het verlengde van een Plan van Aanpak of projectplan gemaakt worden. Het is geenszins de bedoeling informatie dubbel te administreren. Verwijzen over en weer en naar informatie die elders al is vastgelegd is prima.

---

<sup>1</sup> Het beheren van onderzoeksdata, Marnix van Berchum en Marjan Grootveld, [www.iwabase.nl](http://www.iwabase.nl) december 2016

### Open Science

Waarom is Open Science goed voor de HAN? Het is voor de HAN, mede in het kader van het IP 16/20 relevant om de overgang naar Open Science te maken, omdat het ten goede komt aan:

- de onderzoekers zelf, en aan de vindbaarheid van hun producten
- de HAN in de profilering op zwaartepunten
- de omgeving voor wie resultaten makkelijker vindbaar zijn, en de kleur van de HAN inzichtelijker is
- de toegankelijkheid van onderzoek van elders
- vormgeving van peer review en andere vormen van kwaliteitszorg

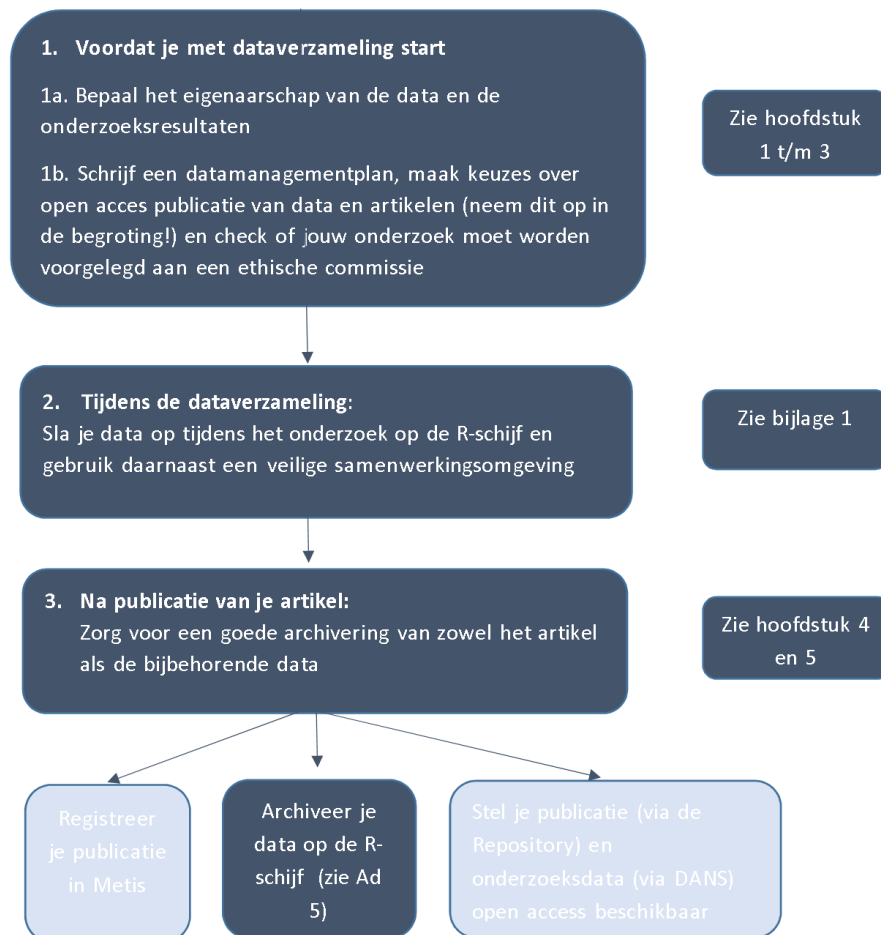
De FAIR-principes van *Findable, Accessible, Interoperable* en *Reusable* data zijn in 2014 geïntroduceerd en worden vaak in één adem met Open Science genoemd. Op de weg naar FAIR data zijn er nog wel uitdagingen bijvoorbeeld op het gebied van het toekennen van metadata of de inzet van duurzame software. De HAN beschikt nu over opslag op een eigen server (de R(earch)-schijf), naar verwachting een tussenstation op weg naar een gecertificeerd data-archief.

### Vragen?

Heb je na het lezen van dit document nog vragen of extra ondersteuning nodig? Kijk dan op <http://specials.han.nl/sites/studiecentra/onderzoek/> of mail naar [onderzoeksondersteuning@han.nl](mailto:onderzoeksondersteuning@han.nl)



## Datamanagement stappen bij de HAN



In lichtblauw zie je activiteiten die nu nog niet mogelijk zijn maar waaraan gewerkt wordt.

1. Administratieve informatie		
1.1	<b>Projectnummer</b> Bij voorkeur zoals bekend in DAX.	
1.2	<b>Projectnaam</b> De naam van het project.	
1.3	<b>Startdatum project</b>	
1.4	<b>(Beoogde) einddatum project</b>	
1.5	<b>Projectbeschrijving</b> Vat kort het type onderzoek (of onderzoeken) samen om anderen het doel van de dataverzameling uit te leggen. <i>Max. 50 woorden.</i>	
1.6	<b>Oprichtgever</b>	Naam:  Functie:  Organisatie(onderdeel):  Telefoon:  E-mailadres:

1.7	<b>Hoofdonderzoeker</b>	Naam:  Functie:  Organisatie(onderdeel):  Telefoon:  E-mailadres:
1.8	<b>Medewerkers onderzoek</b>	Naam:  Functie:  Organisatie(onderdeel):  Telefoon:  E-mailadres: <hr/> Naam:  Functie:  Organisatie(onderdeel):  Telefoon:  E-mailadres: <hr/> Naam:  Functie:  Organisatie(onderdeel):  Telefoon:  E-mailadres: <hr/> Naam:  Functie:  Organisatie(onderdeel):  Telefoon:  E-mailadres:

1.9	<b>Onderzoekseenheid</b> Kies uit: <ul style="list-style-type: none"> <li>• Business Development &amp; Co creation</li> <li>• Kwaliteit van Leren</li> <li>• Duurzame Zorg</li> <li>• Revalidatie, Arbeid, Sport</li> <li>• HAN Sociaal</li> <li>• Publieke Zaak</li> <li>• Technologie &amp; Samenleving</li> </ul>	
1.10	<b>Lectoraat (facultatief)</b>	

<h2 style="color: #4F81BD;">2. Financiële informatie en eigenaarschap</h2>		
2.1	<b>Onderzoeksfinanciering</b> Door wie wordt het onderzoek gefinancierd? Noem hierbij ook eventuele co-financiers.	
2.2	<b>Subsidie</b> Zijn er voor dit project mogelijkheden voor externe financiering en loopt dit <a href="#">via het Centrum voor Valorisatie en Ondernemerschap (CVVO)</a> ? Wanneer er afspraken zijn over externe financiering: zijn er specifieke afspraken met de subsidieverstrekker over toegankelijkheid van de data tijdens en na het onderzoek gemaakt?	
2.3	<b>Eigenaarschap data / onderzoeksgegevens (en Auteursrecht publicatie)</b> Wie is de eigenaar van de onderzoeksgegevens en waar ligt het auteursrecht van de publicatie c.q. het onderzoeksrapport of ander type resultaat? Zijn hierover afspraken gemaakt met opdrachtgever en/of subsidieverstrekker c.q. werkgever? Denk aan een contract, samenwerkingsovereenkomst, consortiumagreement, non-disclosure	

	<p>agreement. (In principe is de HAN eigenaar van de data (!), tenzij hier andere afspraken over zijn gemaakt). Neem voor meer informatie contact op met het Auteursrecht Informatiepunt via <a href="mailto:auteursrecht@han.nl">auteursrecht@han.nl</a></p>	
2.4	<p>Zijn er partners betrokken bij dit onderzoeksproject? Welke contactgegevens (naam, functie, organisatie) horen hierbij?</p>	<p>Naam:</p> <p>Functie:</p> <p>Organisatie(onderdeel):</p> <p>Telefoon:</p> <p>E-mailadres:</p> <hr/> <p>Naam:</p> <p>Functie:</p> <p>Organisatie(onderdeel):</p> <p>Telefoon:</p> <p>E-mailadres:</p> <hr/> <p>Naam:</p> <p>Functie:</p> <p>Organisatie(onderdeel):</p> <p>Telefoon:</p> <p>E-mailadres:</p>

3. Data verzamelen en analyseren				
3.1 Bestaande data hergebruiken				
		Ja	Nee	n.v.t.
3.1.1	Ik ga bestaande onderzoeksgegevens of datasets hergebruiken. Zo nee, ga verder bij 3.2. Zo ja, specificeer:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.1.2	Ik heb toestemming gekregen om deze onderzoeksgegevens of datasets te gebruiken. Zo nee, specificeer hoe dat opgelost gaat worden:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.2 Nieuwe data verzamelen				
3.2.1	Is er sprake van tot personen herleidbare data? Zo nee, ga verder bij 3.3. Zo ja, specificeer:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.2.2	Is er sprake van vertrouwelijke data? Zo nee, ga verder bij 3.3. Zo ja, specificeer:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.2.3	Ik verkrijg de onderzoeksgegevens van deelnemers met toestemming (informed consent). Zo ja, specificeer:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.2.4	Is er sprake van een externe partij, die namens jou gegevens verzamelt (of opslaat)? Heb je hiervoor een <a href="#">bewerksvereenkomst</a> afgesloten?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.3 Gevoelige gegevens beschermen				
3.3.1	<u>Ik heb gecheckt of er aparte geheimhoudingsverklaringen moeten worden getekend.</u> Toelichting: Een ieder die betrokken is bij de verwerking van persoonsgegevens tekent een geheimhoudings-verklaring. Indien het om een project gaat met externe partijen kan het zo zijn dat er reeds een (samenwerkings)overeenkomst is getekend waarin afspraken staan over geheimhouding. Dan is een afzonderlijke geheimhoudings-verklaring veelal niet (meer) nodig. Gaat het enkel om het binnen de HAN verwerken van persoonsgegevens en is er geen derde bij	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

	<p>betrokken dan is dit gedekt door onze Cao, behalve bij studentonderzoekers. Zij moeten dus wel een geheimhoudingsverklaring tekenen. Gaat het om het verwerken van persoonsgegevens van medewerkers of studenten van de HAN door een derde, dan is er op grond van de WBP of AVG een bewerkersovereenkomst vereist (zie 3.2.4).</p>			
3.3.2	<p>In het geval van een wetenschappelijk onderzoek met mensen: ik heb gecheckt of het project moet worden voorgelegd aan de Adviescommissie Praktijkgericht Onderzoek GGM of aan een andere Medisch Ethische Toetsingscommissie, zie de beslisboom in de <a href="#">Gedragscode voor onderzoek met mensen</a>.</p>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.3.3	<p>Moet ik mijn onderzoek melden bij de functionaris gegevensbescherming HAN (Jaap Gall)?</p> <p>Toelichting: Elke verwerking van persoonsgegevens moet in principe worden gemeld bij de functionaris gegevensbescherming HAN. Voor (praktijkgericht) wetenschappelijk onderzoek wordt een uitzondering gemaakt. Persoonsgegevens die een onderzoeker verzamelt in het kader van onderzoek hoeven niet te worden gemeld. Daarvoor geldt wel een aantal voorwaarden:</p> <ul style="list-style-type: none"> <li>• de persoonsgegevens moeten uitsluitend worden verzameld, verwerkt en gecontroleerd ten behoeve van het onderzoek of een bepaalde statistiek;</li> <li>• de persoonsgegevens mogen niet langer worden bewaard dan voor het desbetreffende onderzoek noodzakelijk is;</li> <li>• de persoonsgegevens (met uitzondering van sekse, woonplaats en geboortjaar) mogen niet langer worden bewaard dan zes maanden nadat ze van de desbetreffende deelnemer zijn verkregen.</li> </ul> <p>Voldoet een onderzoeker niet aan deze voorwaarden, dan dient hij/zij dit te melden bij de functionaris gegevensbescherming HAN.</p>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>



3.3.4	Ik anonimiseer/ pseudonimiseer (privacygevoelige) onderzoeksgegevens. Zo ja, specificeer:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.3.5	Ik controleer zelf de naleving van de maatregelen die genomen zijn om de privacy van personen en de niet-herleidbaarheid van de onderzoeksgegevens te waarborgen.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

4. Data opleveren: projectproducten (kennisdisseminatie)				
4.1	Geef een overzicht van de verwachte types onderzoeksdata, softwarekeuzes en -groei.			
	<b>Data stadium (volgens indeling mappen R-schijf)</b>	<b>Specificatie van het type onderzoeksdata</b>	<b>Software keuze</b>	<b>Data grootte/groei</b>
	Ruwe data sets			
	Half bewerkte data sets			
	Data sets voor analyse			
	Gepubliceerde data			
4.2	Ik bied beschrijvende informatie aan bij de verschillende projectproducten zodat de data in de toekomst te lezen en te interpreteren zijn. Zo ja, bijvoorbeeld benodigde software om bestanden te lezen Zo nee, leg uit waarom niet:	<input type="checkbox"/> Ja	<input type="checkbox"/> Nee	

5. Dataopslag tijdens en na het project				
5.1 Dataopslag gedurende het onderzoek.				
		Ja	Nee	n.v.t.
5.1.1	Voor opslag van mijn gegevens maak ik gebruik van de standaardvoorzieningen van de HAN waarbij er aandacht is voor een goede back-up van gegevens (zie toelichting Dataopslag tijdens en na het project). Zo ja, ga naar 5.1.3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.1.2	Voor opslag van mijn gegevens maak ik gebruik van voorzieningen van een andere onderwijsinstelling of bijvoorbeeld DANS (dit zijn opslagmogelijkheden die kennisdeling met derden mogelijk maken (zie bijlage 1)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.1.3	Ik weet bij benadering wat de omvang en eventuele groei van de data zijn. Zo ja, specificeer:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.1.4	Ik neem de volgende technische en organisatorische maatregelen ter beveiliging van onderzoeksgegevens. Denk qua technische maatregelen aan het gebruik van duurzame bestandsformaten (zie bijlage 1) en qua organisatorische maatregelen aan een zorgvuldige afweging wie toegang krijgt tot de onderzoeksdata (zie bijlage 1)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.1.5	Ik heb voor ogen volgens welke structuur ik mijn data wil gaan opslaan (voor de geprefereerde structuur op de R-schijf en voorbeelden zie bijlage 1).	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

5.1.6 Maak hier een overzicht van jouw mappenstructuur:

Empty box for drawing the folder structure.

5.2 Dataopslag na afloop van het onderzoek				
		Ja	Nee	n.v.t.
5.2.1	Ik archiveer de data in het archief op de R-schijf van de HAN (geprefereerde plaats - zie bijlage 1) of elders binnen de HAN (specificeer waar).	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.2.2	Voor archivering van mijn gegevens maak ik gebruik van voorzieningen van een andere onderwijsinstelling of bijvoorbeeld DANS. Zo ja, specificeer:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.2.3	Ik wil mijn publicaties digitaal op laten slaan en vrij beschikbaar maken via de HAN repository. Zie <a href="http://specials.han.nl/sites/studiecentra/onderzoek/">http://specials.han.nl/sites/studiecentra/onderzoek/</a> en check of dit voor jouw publicatie mogelijk is via <a href="http://www.sherpa.ac.uk/romeo/index.php?la=nl">http://www.sherpa.ac.uk/romeo/index.php?la=nl</a>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.2.4.	Ik wil mijn onderzoeksdata, of een gedeelte hiervan, na afloop van het project open access beschikbaar stellen voor hergebruik. Zo ja, geef concreet aan wanneer en op welke wijze de data beschikbaar gesteld wordt. Zo nee, geef aan waarom (een deel van) de data niet geschikt is voor hergebruik.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.2.5	Worden er voorwaarden gesteld aan het hergebruik van de data? Indien van toepassing: zijn deze vastgesteld in een consortium agreement?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

## Bijlage 1 Dataopslag tijdens en na het project

Het is belangrijk om onderzoeksdata van de HAN op een eenduidige manier op te slaan. Daarom is de preferente manier van opslaan op de R-schijf. Daarnaast stimuleert de HAN het open access beschikbaar stellen van (een deel van) onderzoeksdata. Een goede manier om dit te doen is via DANS, maar hieronder geven we andere mogelijke opties.

En als je kiest voor een niet door de HAN beheerde opslag of samenwerkingsomgeving, maak dan vooraf een plaatje van de gewenste opslagstructuur zoals bijvoorbeeld die van de R-schijf en een autorisatiematrix, waarin je aangeeft wie, wanneer, waar bij mag. Houd er ook rekening mee dat aan externe opslag onvoorziene kosten verbonden kunnen zijn. Neem voor advies altijd contact op met [Onderzoeksondersteuning@han.nl](mailto:Onderzoeksondersteuning@han.nl)

### Opties voor **Dataopslag tijdens een project:**

- R-schijf, op netwerk van de HAN en centraal beheerd door de HAN, zie verder
- Surfdrive, zie verder
- HAN Scholar, zie verder
- #OnderwijsOnline
- Dutch Dataverse Network <https://www.dataverse.nl/dvn/>
- SURFsara (grootschalig) <https://www.surfsara.nl/>
- Target (grootschalig) <http://www.rug.nl/science-and-society/target/>
- Parelsnoer Instituut <http://catalogus.parelsnoer.org/catalogus/>

### Opties voor **Dataopslag na afloop van een project:**

- ICT-afdeling van de HAN – R-schijf, zie verder
- DANS (voor o.a. tekst, databases, spreadsheets, audio, audiovisuele data, XML) <http://dans.knaw.nl/>
- 3TU.Datacentrum <http://datacentrum.3tu.nl/>
- SURFsara (grootschalig) <https://www.surfsara.nl/>
- CentERdata (m.n. surveydata) <http://www.centerdata.nl/>
- Target (grootschalig) <http://www.rug.nl/science-and-society/target/>
- Nederlands Instituut voor Beeld en Geluid <http://www.beeldengeluid.nl>

### Specificaties R-schijf bij de HAN

Voor de opslag en archivering van onderzoeksdata biedt de HAN de R-schijf (voor Research data). De centrale opslag van onderzoeksdata is stap 1, het invullen van een datamanagementplan en het toekennen van metadata is stap 2. Vervolgens kunnen we aan de slag met verdere implementatie van de FAIR-principes van *Findable*, *Accessible*, *Interoperable* en *Reusable* data onder het motto: *Open als het kan, beschermd als het moet*.

### Kenmerken van de R-schijf:

- Per faculteit of per kenniscentrum of lectoraat is er een supervisor (de lector) en een vervanger (secretariaat) om het beheer van de mappen op de R-schijf te regelen.
- De supervisor en de vervanger hebben toegang tot alle mappen van een faculteit/kenniscentrum/lectoraat.

- Voor een nieuwe omgeving of map op de R-schijf, is een akkoord nodig van de supervisor (of vervanger) van de faculteit/het kenniscentrum/het lectoraat.
- Het is aan de onderzoeker in overleg met de supervisor of vervanger om te bepalen wie – naast de onderzoeker zelf - verder nog toegang tot de betreffende onderzoeksomgeving moet hebben. Toegang is voornamelijk voorbehouden aan HAN medewerkers.
- In iedere onderzoeksomgeving is er een vaste mappenstructuur (om de structuur te waarborgen) gebaseerd op de fasen in een lopend onderzoek.
- In map 'd. Publicaties' komt de informatie te staan zoals deze openbaar gedeeld kan worden met collega-onderzoekers en bijv. de subsidiegever. Gegevens in deze map zijn geanonimiseerd of gepseudonimiseerd.
- Binnen de standaard mappen, kunnen gebruikers zelf submappen maken. Voor map 'c. Data sets voor analyse', 'd. Publicaties' en 'e. Contact en contract' hebben we een geprefereerde indeling laten zien bij punt 5.
- Er gelden geen quota of limieten, je krijgt zoveel ruimte als voor je onderzoek nodig is. De kosten van de opslag worden naar verbruik doorbelast aan de faculteiten.
- Verwacht je extreem grote hoeveelheden data, dan is wellicht een andere omgeving dan de R-schijf beter. ICT kan adviseren/bemiddelen bij andere opties.

Per project: Projectnummer-projectnaam

- Ruwe data sets
- Halfbewerkte data sets
- Data sets voor analyse
  - Uiteindelijke dataset(s) voor analyse
  - Syntax en bijbehorende output
- Publicaties
  - Publicatie (zowel de opgemaakte versie van het tijdschrift/uitgever (PDF) als de laatste eigen versie)
  - Openbare data sets (bijv. voor DANS)
  - Datamanagement plan
  - Goedkeuring ethische commissie
- Contact en contract
  - Toestemmingsformulieren deelnemers
  - Samenwerkingsovereenkomsten (o.a. eigenaarschap data)
  - Subsidie aanvragen en toekenningen

Per project: Projectnummer-sleutelgegevens

- Sleutelgegevens

#### Aanvraagprocedure R-schijf

1. De onderzoeker stemt af binnen lectoraat/kenniscentrum over het opslaan van

- onderzoeksdata bij de HAN (over wie toegang moet hebben, naamgeving, projectnummer etc.).
2. Indien de supervisor (of vervanger) van de faculteit/het kenniscentrum/het lectoraat akkoord is, stuurt de supervisor de vraag door naar ICT: [Liesbeth.Hoogkamp@han.nl](mailto:Liesbeth.Hoogkamp@han.nl)
  3. Als dit de eerste vraag is vanuit de faculteit/het kenniscentrum/het lectoraat is, kan een 'intake-gesprek' gewenst zijn.
  4. Als de aanvraag akkoord is, wordt de onderzoeksomgeving op de R-schijf ingericht.
  5. Aanvullingen/mutaties verlopen ook via de supervisor of vervanger.

### Na afloop van het project

Na afloop van een project, wordt in overleg de einddatum bepaald. Die einddatum bepaalt vervolgens hoe lang de onderzoeksgegevens bewaard moeten worden.

De mappen kunnen op de R-schijf blijven staan maar worden verplaatst naar een submap '\_Archive' (per Kenniscentrum/Lectoraat) en op read-only gezet. Bij die overgang van de dynamische onderzoeksfase naar de archieffase is het van belang bestanden te ontdebellen, te zorgen voor een betekenisvolle naam (voor zover dat nog niet was gedaan), bestanden zo mogelijk op te slaan als pdf (/A) i.p.v. Word en grote bestanden te zippen. Alleen eindrapporten/versies hoeven bewaard te worden, niet alle concepten en tussenversies.

Hieronder kun je zien hoe lang de verschillende standaard mappen bewaard blijven.

Ruwe data sets	Bewaren tot 10 jaar na einde onderzoek, data indien nodig versleuteld, mocht wet- en regelgeving bepalen dat data langer of korter bewaard moeten worden, dan geldt die wet- en regelgeving
Halfbewerkte data sets	Bewaren tot 10 jaar na einde onderzoek, data indien nodig versleuteld, mocht wet- en regelgeving bepalen dat data langer of korter bewaard moeten worden, dan geldt die wet- en regelgeving
Data sets voor analyse	Bewaren tot 10 jaar na einde onderzoek, data indien nodig versleuteld, mocht wet- en regelgeving bepalen dat data langer of korter bewaard moeten worden, dan geldt die wet- en regelgeving
Publicaties	Altijd bewaren na einde onderzoek, hierin opslaan: eindrapport, onderzoeksresultaten, projectplan, evaluatierapport, datamanagementplan, goedkeuring ethische commissie (indien van toepassing).
Contact en contract	Bewaren tot 10 jaar na einde onderzoek, hierin informed consent verklaringen en bijvoorbeeld submap subsidies
Sleutelgegevens	Bewaren tot 10 jaar na einde onderzoek, mocht wet- en regelgeving bepalen dat data langer of korter bewaard moeten worden, dan geldt die wet- en regelgeving ook voor bijbehorende sleutelgegevens

### Surfdrive bij de HAN

Voor Surfdrive moet de afdeling ICT enkele zaken regelen voordat je er gebruik van kunt maken. Stuur een mailtje naar de ServiceDesk als je toegang tot Surfdrive wilt.



Het verdere beheer van een omgeving in Surfdrive is aan de onderzoeker(s). Houd er wél rekening mee dat na afloop van een onderzoeksproject de te archiveren data naar een duurzame omgeving wordt overgezet. De betreffende HAN onderzoeker (medewerker) is daarvoor verantwoordelijk. Surfdrive is géén duurzame omgeving, de R-schijf van de HAN is dat wel net als bijvoorbeeld de opslagvoorziening van DANS.

Surfdrive heeft als voordeel dat er ook met studenten kan worden samengewerkt. Beheer en organisatie verlopen echter altijd via een medewerker van de HAN.

#### HAN-Scholar en #OnderwijsOnline

Deze beide omgevingen horen tot de standaard voorzieningen van de HAN en kunnen gebruikt worden om onderling (én met studenten) samen te werken. Maar ook hier geldt dat voor het duurzame archiveren van onderzoeksdata, de R-schijf van de HAN of de opslagvoorziening van DANS (zie ook bijlage 1) gekozen moet worden.

#### Duurzame formaten

- Data formaten met de beste kans op langdurige toegang hebben de volgende karakteristieken: Open documentatie
- Ondersteund door veel software platforms
- Wijdverbreid gebruik
- Geen compressie van data
- Geen geïntegreerde bestanden/programma's/scripts
- Geen gepatenteerde (maar juist open) formaten

Zie ook <https://dans.knaw.nl/nl/deponeren/toelichting-data-deponeren/bestandsformaten>

## 10.5 Engie GDPR and AVG Compliance Declaration

### ***MyLifeMyWay GDPR & AVG compliancy***

#### **SDO: Smart Digital Operations.**

ENGIE Netherlands consists of ENGIE Energy, ENGIE Services, ENGIE E&P, ENGIE Fabricom and ENGIE Laborelec. ENGIE Smart digital solutions is challenging the business by building a connected world towards smart solutions and big data.

Smart Digital Operations(SDO) is responsible of maintenance of diverse Enterprise networks and hybrid solutions, amongst existing networks, own data centers, virtual public and private clouds and IaaS solutions. Each of these building blocks are delivered to internal and external clients.

For SDO is GDPR is part of the daily operations. We are continuously busy with improving the infra security processes and optimisation of the information security

#### **Certification.**

ENGIE Smart Digital Operations has diverse privacy and security audits certifications in place. Our processes are based on ITIL.

- ISAE 3402 International Standard service, organisation and control (accountant declaration)
- ISO 27001 checked on GDPR and AVG;
- ENGIE ICS framework for Industrial Computer Security (in cooperation with ENGIE Laborelec)

Towards these certifications we implemented information security compliance regulations that can be found back on information security book.

#### **Security & Information security awareness within team and the organisation**

ENGIE SDO developed its own handbook for information security which is checked by an external audit company.

In that information security book there are various work instructions, forms and rules are defined. All ENGIE SDO employees are signed this handbook and trained accordingly. To observe and execute the content of the handbook on daily operational business.

Additionally ENGIE security officer holds regularly trainings with the employees to keep the employees up to date with the actual changes and practices showcases. The main goal of the trainings is to create awareness on information security.

We try as little as possible to save personal information, in case it is required to store the personal information, we have clear instructions and watertight procedures in place in line with the GDPR regulation how to protect the data.

There are several Chief Information Security officers assigned for guarding and the implementing the GDPR regulation within ENGIEs.

#### **Datacenter environment**

The SDO platform is fully endorsed with our own TIER III datacenter in Maastricht-Airport with 2500m<sup>2</sup> IT systems and has an uptime of 99.982%. The data center is compliant to highest security norms in order to be satisfactory for the high quality demand of the ENGIE Business requirements:

The data center has 24x7 monitoring, is located on a secured business industry area that is under control and safety of the Dutch Royal Military police. The data center has zoned alarm system and cam security. All space in the data center has a box in box building system which the suites are not

The authorized personnel receives an entree badge that gives access to their own responsible suite. Every visit to the data center and to a specific suite is registered per event.

Geautoriseerde personen krijgen vervolgens een persoonlijke toegangsbadge, die ze toegang verleent tot hun suite. Ieder bezoek en iedere suite toetreden wordt dus geregistreerd en bewaakt.

The data center quality is in line with the certifications that are in place: e.g. ISAE 3402 type II, ISO 27001, 9001, 55001 and ENGIE ICS. Next to this ENGIE participates in diverse security and privacy interest groups such as Green Grid, EU Code of Conduct for Datacenters and the Dutch Datacenter Association.

#### **Infrastructure as a Service (IaaS)**

In our data center we offer IaaS business services.

ENGIE SDO offers data driven calculation cloud services based on CPU, memory and storage capacity.

This scalable platform offers right now more than 2000 virtual servers. For this cloud services we implemented restricted security regulations as well. The complete platform has the latest patch and development updates in place, antivirus programs and security walls, it is monitored and maintained 24\*7. Additionally a back-up service is offered, it means every 24 hours we make a snapshot of the complete environment and it is stored in our location in Amsterdam.

This business services has restricted processes, it is continuously monitored and checked.

Every employee signs an NDA document to agree on to protect the information confidentiality and security, in case of any data leakage the employee is obligated to report it immediately.

All of these regulations and the tasks are written in the security handbook.

#### **Service management**

For the Service management we implemented also regulations to be compliant for GDPR.

For every and a new client we take care of a SLA contract (full or partially) defining the offered business services in details with care. Additionally we also make a processor agreement which is based on actual country level regulation.

In this processor agreement it is written how we would process the personal information and the eventual data leakage. Additionally at country level we do inventarisation of the sensitive personal information that is stored.

We ask to our each customer which type of data is going to be stored in our platform, after than we implement the necessary procedures inlie with the type of data that will be stored.

We are busy with all of our clients at the moment for inventarisation of which personal information through SDO will be processed

As soon as this inventarisation is completed, we will be able to share the necessary information about the reason why that data will be stored by SDO and what their rights about the data are.

Above mentioned service management information(client information) will be stored in our CMDB, in order us to know by which client which type of agreement is in place for how long.

In a case of the data processing and storage involves personal information on our platform, we make also a similar agreement with the suppliers as well.