DELIVERABLE 1.5
ETHICAL, PRIVACY AND LEGAL CONSIDERATIONS

	NAME	CONSORTIUM PARTNER
Prepared by:	Donaat Van Eynde Tony Lam	Familiehulp NetUnion
Approved by:	Cathal Gurrin Maher Ben Moussa	DCU UNIGE

Disclaimer

Acknowledgements

Thank you to all end-users across sites who took the time to participate in this research. We appreciate your time and effort.

National funding agencies

COUNTRY	FUNDING AGENCY FUL NAME
Switzerland	State Secretariat for Education, Research and Innovation
Ireland	Enterprise Ireland
Belgium	Agentschap Innoveren & Ondernemen

Document history

REV.	APPROVAL DATE	DESCRIPTION
V0.1	12/07/2017	Draft Version
V1.0	31/08/2017	Final Version
V1.1	20/07/2018	GDPR Data added
V1.2	25/07/2018	Release of D1.4b after peer review

Table of contents

Table of Figures

List of Tables

N/A

List of Abbreviations

ABBREVIATION	FULL	DESCRIPTION
WP	Work Package	Category of tasks which details the description of work
IoT	Internet of things	inter-networking of devices which enable the collection and exchange data.

1 Introduction

Vizier develops a technological solution for the elderly home environment gathering and sharing information from different sources, including sensitive personal information and information related to operational processes of enterprise software.

This report reflects on the related ethical and legal issues and evaluates the solutions in which way they comply with applicable legislation for personal data protection in the pilot countries and internal organization rules of the two organizations offering the pilot infrastructure (Myhomecare and Familiehulp vzw). This report examines ethical, legal and privacy requirements when using the Vizier solution by (older) end users.

The ethical aspects concern who has access to what information, and whether it should be access on different levels. The project has initiated discussions with respective data inspectorates while creating detailed definitions of the solution.

The technology chosen is respectful of human dignity. Vizier system respects the integrity of its users such that the data collected about its users is not directly used for making a profit by any individual though allowing for commercial services driven by the use of personal data (after users have given their consent for the usage in this way). All elderly information will be erased after the project's end. Vizier includes involvement and observation of older adults, whose privacy is subject to extensive formal regulation. It will be ensured that subjects included in the trial group are adults in full control of their faculties, and they must give a written informed consent to participate in the final test. Participants will be able to withdraw the consent (and consequently withdraw from the project) at any time and without the need to give a reason. An information brochure, written in a simple, understandable local language, documenting the objective of the project, what kind of personal data is collected and the principles on how the data is shared, stored and protected will be developed in three languages and used as information to the trial group. The project will ensure that all aspects related to possible privacy issues are understood by the participants before the written consent is collected.

To perform trials related to treatment of personal sensitive information there were already several directives at European level (European directives: Directive 95/46/EC on protection of personal data, Directive 97/66EC concerning the processing of personal data, Directive 2002/58/EC directive on privacy and electronic communications). However, more recently the paradigm of the protection of natural persons has changed largely by the publication of the REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Official Journal of the European Union, 2016).

The new regulation is applied from 25 May 2018. This Regulation is binding in its entirety and directly applicable in all Member States and repeals Directive 95/46/EC on the same date.

2 General Data Protection Regulation and Vizier

Data Protection is the means by which the privacy rights of individuals are safeguarded in relation to the processing of their personal data.

The 'new' General Data Protection Regulation (GDPR) is a set of rules to better protect European citizens' data. The legislation was approved in 2016 and consists of two parts: the Regulation, which applies to the business world, and the Directive, for public services such as police and justice.

The General Data Protection Regulation has been enforceable since 25th May 2018, replacing the existing data protection framework under the EU Data Protection Directive:

- address organisations involved in data processing of any sort;
- emphasises TRANSPARANCY, SECURITY and ACCOUNTABILTY;
- before gathering any personal data, it is necessary to communicate to individuals the legal basis for processing the data, retention periods, the right of complaint where customers are unhappy;
- all information has to be provided in concise, easy to understand and clear language.

2.1 Principles relating to processing of personal data[1]

Personal data shall be:

- lawfulness, fairness and transparency: processed lawfully, fairly and in a transparent manner in relation to the data subject;
- purpose limitation: collected for specified, explicit and legitimate purposes;
- data minimisation: adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accuracy: accurate and, where necessary, kept up to date;
- storage limitation: kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
- integrity and confidentiality: processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

1 GDPR: Chapter II, Article 5 – 'Principles relating to processing of personal data'

2.2 Lawfulness of processing[2]

Processing shall be lawful only if and to the extent that at least one of the following applies:

- the data subject has given consent to the processing of his or her personal data for one or more specific purposes: applies in Vizier!
  → Vizier attaches great importance to the active permission that participants give in the different steps of the project
  → already in the pre-trial, a preliminary version of a statement that shall be signed by participants in participating in the effective test was made;
- processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- processing is necessary for compliance with a legal obligation to which the controller[3] is subject;
- processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party.

2.3 Vizier using Customer Consent as grounds to process data

Essentially, the users of the Vizier Platform cannot be forced into consent, or be unaware that they are consenting to processing of their personal data. They must know exactly what they are consenting to and there can be no doubt that they are consenting → Vizier needs a positive indication of agreement.

The data subject has to give consent to the processing of his or her personal data for one or more Vizier-purposes

- is freely given;

2 GDPR: Chapter II, Article 6 – 'Lawfulness of processing'

3 GDPR: The controller is the party who determines 'why' the personal data will be processed (i.e. the purpose of the processing) and, where the controller appoints a processor, the processor determines 'how' the personal data will be processed (i.e. the method of the processing). Typically, an IT services provider will be a 'processor' and its customer will be the 'controller'

- is specific;
- is informed;
- is unambiguous.

2.4 Pre-Trial Vizier.

Vizier has presented his first prototype to a number of potential end users during the period February - March 2018 in the three participating countries. In Flanders, Ireland and Switzerland about thirty people were invited to meet with the Vizier solution.

2.4.1 Protocol Pre-Trial Vizier.

The scripted protocol has been developed by the Vizier consortium

Setup:

- Upon arrival the participants will be introduced to the team present for the pre-trial;
- Prior to pre-trial participants will be given a Plain Language Statement and an Informed Consent Form to complete (although this pre-trial does not process personal data, the informed consent is important as the first step in the development of a complete informed consent for the pilot);
- They will be asked for the necessary information to setup the Vizier system;
- They will logged into Memory Club;

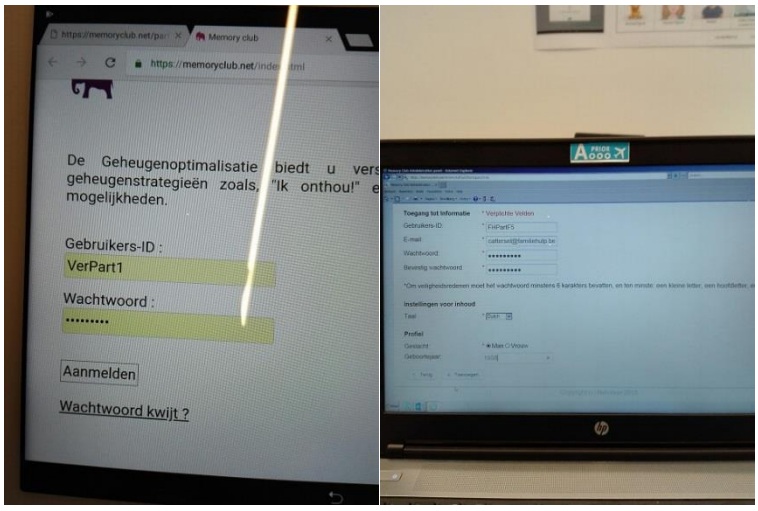

FIGURE 1 LOGGING IN ON MEMORY CLUB AND ACCOUNT DATA (PRE-TRIAL KRUIBEKE)

- They will be fitted with the FitBit activity tracker and given the “keys” with presence sensor for attached to have on their person for the evaluation;

FIGURE 2 FITBIT INSTALLATION (PRE-TRIAL KRUIBEKE)

- If they have not already completed the pre-questionnaire, they will be invited to do so;
- The will be notified of the whereabouts of the fixed sensors;
- We will execute a test voice command/response to see that they understand this element;

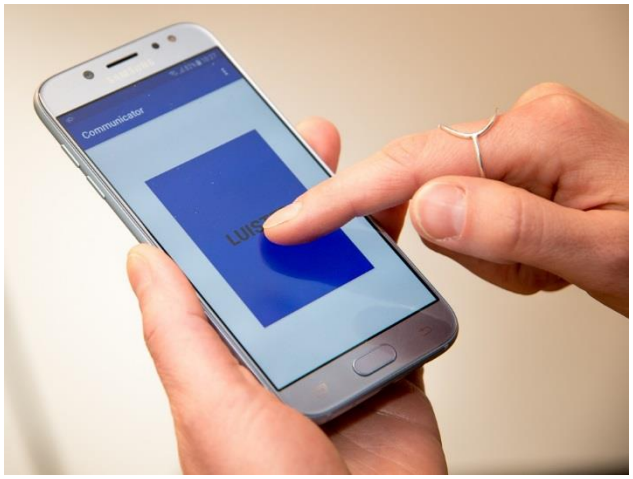

FIGURE 3 VOICE COMMAND WITH COMMUNICATOR (PRE-TRIAL KRUIBEKE)

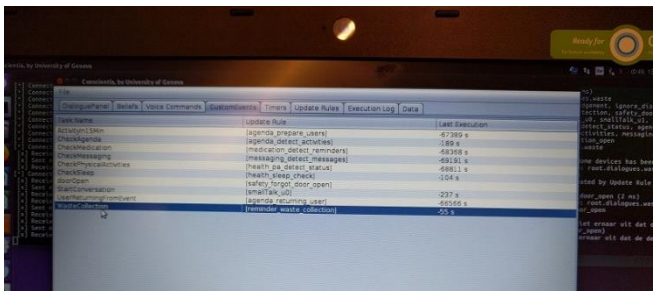

FIGURE 4 CUSTOM EVENTS (PRE-TRIAL KRUIBEKE)

Demonstration:

- User sits at the breakfast table;
- Vizier greets him and reminders him of his agenda for today and asks if he wants to view the items (StartConversation and CheckSleep);
- On the tablet is one recommendation for a local activity later this week. The user can schedule it in his agenda (CheckAgenda);
- The user takes out the trash and forgets to close the door. The system detects the door has been opened for a long time (a few minutes) and alerts the user (doorOpen);
- A family member sent a message. The user writes a short message back (CheckMessaging);
- The user gets a medication reminder (voice + pop-up on tablet) and can confirm that he took the medication (CheckMedication);
- The user takes place in the couch and works with the Memory Club (gamified memory training application) on the tablet. The program can be jump started with pre-made user accounts. The user will watch the video for the first module and do the quiz (this will take max. 15 minutes);

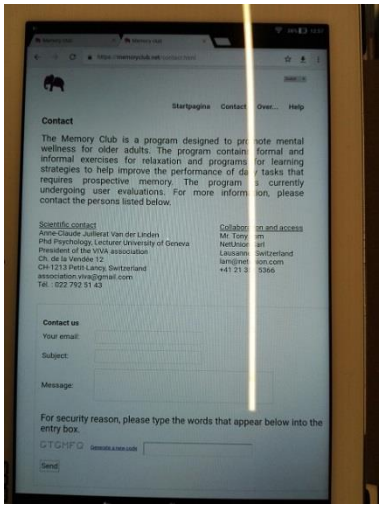

FIGURE 5 MEMORY CLUB (PRE-TRIAL KRUIBEKE)

- After a while the system notes he's been sedentary for a long time and invites him to do start the daily physical exercises. This will be a walk. The user will take a short 10-minute walk at an easy pace– accompanied by one of the research team around the mall. This activity will be detected by the activity tracking wristwatch (CheckPhysicalActivities, and then ActivityIn15Min);
- Once returned from the walk the technical evaluation will be complete (UserReturnFromEvent).

Post-pretrial interview:

- The participant will be invited to complete an exit interview about the system and give their feedback

3 Rights of the data subject

3.1 Right of access by the data subject (Article 15)

The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

- the purposes of the processing;
- the categories of personal data concerned;
- the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
- where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
- the right to lodge a complaint with a supervisory authority;
- where the personal data are not collected from the data subject, any available information as to their source;
- the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

3.2 Right to rectification (to have inaccuracies corrected)

The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

Data controllers are those who, either alone or with others, control the contents and use of personal data. Data controllers can be either legal entities such as companies, Government Departments or voluntary organisations, or they can be individuals such as pharmacists or care professionals.

For example: the data controller in Familiehulp (Flanders) is Sophie Bongaerts (in Dutch we translate ‘ the data controller into ‘Functionaris voor gegevensbescherming’).

3.3 Right to erasure (to have information erased)

The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

- the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;
- the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);
- the personal data have been unlawfully processed;
- the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
- the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

3.4 Right to restriction of processing (to restrict the processing of their information)

The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:

- the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;
- the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
- the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;
- the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.

A data subject who has obtained restriction of processing shall be informed by the controller before the restriction of processing is lifted.

3.5 Notification obligation regarding rectification or erasure of personal data or restriction of processing

The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16, Article 17(1) and Article 18 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.

3.6 Right to data portability

The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:

- the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1);
- the processing is carried out by automated means.

4 Responsibilities of non-members of the European Union

Compared with the previous data protection legislation of the EU, the GDPR substantially extends the territorial scope of organisation who have to comply. "The GDPR applies to 'controllers' who are established in the
EU, as well as those organisations who are not established in the EU but offer goods or services to, or monitor the behaviour of, data subjects within the EU" (Ridley, 2017). So it does not matter where the organisation or where the equipment is located, any organisation that provides good or services, or monitoring their activity must comply.

4.1 Participants in Switzerland

Participant no.*	Participant organisation name	Participant short name	Organisation type	Country
1 (Coordinator)	University of Geneva	UniGe	Research Organisation	CH
4	NetUnion sàrl	NetUnion	SME	CH
8	VIVA Association	Viva	End Users	CH

In this case, our partners in Switzerland are involved in the rules concerning transfers outside the EU and Vizier has to ensure that Switzerland offers an adequate level of protection.

4.2 Transfers outside the EU with adequate protection

Any controller wishing to transfer personal data outside the European Union must first ensure that the country of final destination offers an adequate level of protection. If the destination country's level of protection can be considered adequate, there can be transfers as if they took place between two Belgian controllers or to another EU country.

Nevertheless, the general principles of the Privacy Act (including legitimacy, compatibility of the communication of data to a third party with the original processing, information to data subjects) must always be observed.

The adequacy of the level of protection of countries outside the EU is assessed on the basis of a number of criteria, including general and sector legislation of the country in question and its professional rules.

Pursuant to article 21, § 2 of the Privacy Act, the King has the power to establish for which categories of personal data processing operations and in which circumstances the transfer of personal data outside the EU is not authorised, but he has not used this possibility yet. The evolution of the decisions made by the European Commission and EU member states shows, however, that not third countries nor certain processing operations not offering and adequate level of protection are listed

("black list"), but those who do offer such protection ("white list").

Which countries offer an adequate level of protection?

The European Commission is authorised to establish whether a country offers an adequate level of protection, and has done so for the following countries: Switzerland, Canada (for processing operations subject to the Canadian Personal Information Protection and Electronic Documentation Act and for airline passenger data), Andorra, Argentina, the United States (for airline passenger data), Guernsey, the Isle of Man, the Faroe Islands de Faeröereilanden, Jersey, Australia (for airline passenger data), Israel, New Zealand and Uruguay.

So Switzerland offers an adequate level of protection!

For all additional information or for the last updates of the list of countries offering an adequate level of protection, it is strongly recommended to consult the European Commission's website (Adequacy of the protection of personal data in non-EU countries) (EU , n.d.)

4.3 Swiss data protection laws

The Swiss Federal Council adopted a draft revision of the Swiss Federal Data Protection Act (“DPA”) on 15 September 2017. The revision aims at strengthening aligning the DPA with the new EU rules on data protection, the GDPR. This will also allow Switzerland to maintain its status as a country providing adequate protection of personal data from an EU perspective. While the goal of the revised DPA is to align itself with the European GDPR, some differences do exist. For example, the revised DPA does not provide data portability rights, limited sanctions (relative to scope of the offences and levels of fines), etc. The draft is expected to enter into force by August 1, 2018. (Staehelin, 2017)

At the time of writing, the Federal Data Protection Act appears to be the most current legal basis for data protection. It is more current than the Loi sur l’information du public (LIPAD) of the Canton of Geneva from 2010, and the Loi sur la protection des données personnelles (LPrD) of the Canton of Vaud (Lausanne) from 2007.

During the project period, the Vizier partners in Switzerland will strive to implement the GDPR guidelines and the DPA guidelines that applies to our project activities.

4.3.1 Genevan law

The Genevan law regarding personal data protections (Loi sur l’information du public, l’accès aux documents et la protection des données personnelles, LIPAD) clearly states that: “The collection of personal data is authorized by LIPAD (art. 38.1) as long as the collection is done in a way that is clearly recognizable by the concerned person.”

The transfer of personal data to other entities or persons is governed by LIPAD art. 39, where all cases and rules under which the data transfer can take place are described. LIPAD defines different

rules for the transmission of personal data, depending on the receiving entity. It distinguishes the following entities that can receive personal data and defines the rules that govern the transfer:

- a) Another public institution - that is falls under the data protection law
- b) A Swiss corporation or public law entity that is not under the data protection law
- c) A foreign corporation or foreign public law entity
- d) A third person or entity which is under private law

4.4 Viva Association

Viva (www.association-Viva.org). Association "Valorizing and Integrating for an Alternative Aging" is a non-profit association based in Lancy (Switzerland). This association is financed by the city of Lancy and it is devoted to promote and enhance knowledge and projects dedicated to favor well-being and active aging in the community. Viva runs programs promoting prevention, measures for community dwelling and institutionalized seniors, as well as interventions set to enhance the autonomy, dignity, sense of purpose, and identity of the elderly.

Viva is in Vizier in the third condition, and the LIPAD states that such a transmission of personal data can be done (Article 39.6)

- if the data treatment is done with a sufficient level of data protection (which is the case, as the results are anonymous, and do not provide information allowing a personal identification)
- the data transmission is not done against a law or a rule (which is also the case within the Vizier project)

At Viva, the end users are only involved at the level of the needs definition, and the prototype's appreciation, through anonymous questionnaires, and after the completion of an informed consent form. No personal data will be made available to the other partners of the project.

LIPAD also defines how the personal data can be used after the completion of the task for which they had been collected (art 41). For that, LIPAD defines that the data are either destroyed or anonymized for the purposes of research, planning and statistics. In addition, the publication of the data must be done in such a manner that the data subjects may not be identified.

According to LIPAD (art 44) any person has the right to ask at any time the responsible entities holding their personal data to be informed by whom their information is handled (art 44.1), ask that their information is destroyed, corrected or restrict access to others (art 47.1).

Also, it has been confirmed that there is no need for an ethical approval (for this project, as the cantonal law is clear: since we only collect data, there is an informed consent form, and the data is anonymised (and there are no medical ingredients, no invasive technology, no genome no ....), the cantonal ethics committee is not required.

4.5 NetUnion sarl

NetUnion, is an SME located in Lausanne Switzerland. The company is dedicated to the development of applications for promoting behavior change, healthy lifestyle, healthy aging and independent living. The main task of the company in Vizier is the development and exploitation of the Memory Club along with the VIVA association.

NetUnion will implement the GDPR guidelines and the DPA guidelines (as well as the guidelines for the data protection law of the Vaud Canton) that applies to our project activities. As the company conducts business with European partners, the GDPR will be the focus of our data and privacy protection policies.

In general the GDPR applies to all companies regardless of size. “However, there are some areas where it is acknowledged that SMEs have fewer resources, or that they process lower volumes of non-sensitive data….For this reason, an SME may be exempt from some of the more rigorous steps (such as the need
to appoint a data protection officer – see section 2.9)” (Ridley, 2017). Additional information regarding SMEs, rules for business and organisations is available on the European Commission’s Law portal. (EU Law, n.d.)

A detailed description of the GDPR compliance for the Memory Club is provided in the section: MClub Data Inventory and GDPR Compliance at the end of this document.

5 Application of the basic principles of the GDPR in Belgium and Ireland

5.1 Which data are protected?

Personal data in Belgium and Ireland (EU partners) are all data that identify or can identify an individual directly, or at least that is how the Privacy Act defines them. This Act provides for specific protection if these data are processed.

Personal data include: a person's name, a picture, a phone number (even a professional number), a code, a bank account number, an e-mail address, a fingerprint, …

Personal data reveal information about an identified or identifiable natural person (called the "data subject"). In other words, personal data are all data allowing for the identification of an individual.

They do not only include data having to do with individuals' privacy, but also data having to do with an individual's professional or public life.

Only data about a natural (physical) person are taken into account, excluding data about a legal person or an association (civil or commercial corporations or non-profit organisations).

The reference to personal data includes fingerprint data. Dactyloscopic data is biometric data and where used for the purpose of uniquely identifying a natural person is Special Category Personal data. Whilst the reference is correct; it is personal data it may be helpful to distinguish personal data from SCPD. Further it may be helpful to give examples of personal data collected as part of the project and also examples of SCPD collected as part of the project.

5.2 Definition in Belgium

Since 25 May 2018, the Commission for the protection of privacy (CPP) has given way to the new Data Protection Authority. We therefore invite you to visit the website of the Data Protection Authority:

www.dataprotectionauthority.be

- In general (Belgium)
  - What are personal data?
  - What is data processing?
  - Who is the controller?
  - The purpose of a data processing operation

5.3 Definition in Ireland

- What are personal data?

"personal data" means information relating to

(a) an identified living individual, or

(b) a living individual who can be identified from the data, directly or indirectly, in particular by reference to

(i) an identifier such as a name, an identification number, location data or an online identifier, or

(ii) one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual;

(Data Protection Act, 2018)

- What is data processing?

"processing", of or in relation to personal data, means an operation or a set of operations that is performed on personal data or on sets of personal data, whether or not by automated means, including

(a) the collection, recording, organisation, structuring or storing of the data,

(b) the adaptation or alteration of the data,

(c) the retrieval, consultation or use of the data,

(d) the disclosure of the data by their transmission, dissemination or otherwise making the data available,

(e) the alignment or combination of the data, or

(f) the restriction, erasure or destruction of the data;

- Who is the controller?
- The purpose of a data processing operation?

5.4 Sensitive data

Some data are so delicate they can only be processed in specific cases. A name and address are rather innocent data, contrary to an individual's race, health, political views, philosophical beliefs (religious or atheist, etc.), sexual preference or legal past.

The processing of personal data relating revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited (*Article 9 GDPR*).

5.5 Automated individual decisionmaking, including profiling

Some tools on the Vizier platform are also linked to automated individual decision-making, including profiling. It is our opinion that the processing may also profile the participants as well as make automated decisions. For example, it is well known that a Fitbit™ or other similar device can collect data on movement and or health related data amongst other things.

Article 22.1(GDPR): The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

- This shall not apply if the decision: (a) is necessary for entering into, or performance of, a contract between the data subject and a data controller; (b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or (c) is based on the data subject's explicit consent.

5.6 Regulation in Belgium

The Data Protection Authority regulates the registration and use of sensitive data very strictly.

In principle it is prohibited to collect, register or ask for the disclosure of the abovementioned sensitive data. Nevertheless, there are a few exceptions to this rule. Controllers may process sensitive data (excluding judicial data) if:

- the data subjects have given their written consent;
- it is necessary to provide care to the data subject;
- it is compulsory under employment law or with a view to the application of social security;
- the data subjects themselves have made the data public;
- it is necessary to establish, exercise or defend a right;
- it is necessary for scientific research.

Political parties, congregations, trade unions, healthcare institutions and other bodies may obviously register and use their members' data. They must not transmit the data to others, however, without the data subjects' consent.

Judicial data (regarding suspicions, prosecutions and sentences) may be processed by a public body if this is necessary for its missions. Such data may also be processed if it is allowed by legislation or regulations, or if the controllers need them to manage their litigations.

Furthermore, there are a few additional measures controllers have to observe when processing sensitive data.

- Information security (Belgium)
  - So precious!
  - An information security policy
  - Security counsellor
  - The risks when processing personal data and who is responsible
  - Reference Measures

5.7 Regulation in Ireland

EU law and National Irish law allows for the processing of data or statistical and scientific or historical research purposes, provided that appropriate safeguards for the rights and freedoms of the data subjects are in place. National law may provide for derogations from the rights of data subjects. The Data Protection Commissioner of Ireland has issued guidelines published in May 2018 available at: https://www.dataprotection.ie/docs/EN/19-06-2018-Limiting-Data-Subject-Rights-and-the-Application-of-Article-23-of-the-GDPR/m/1746.htm

Data collected for statistical, scientific or historical research purposes may not be used for any other purpose.

Data collected legitimately for any purpose may be further used for statistical, scientific or historical research purposes, provided that adequate safeguards are in place. For this purpose, anonymization or pseudonymisation before transmission of data to third parties can provide these safeguards. See also section 5.8.

My Homecare.ie (Servisource Healthcare LTD) has implemented appropriate technical and organizational measures to ensure that the processing of personal data is performed in accordance with the GDPR.

The six principles of data protection relating to the processing of personal data has been incorporated into our practices and procedures as follows;

1. Lawfulness, Fairness and Transparency

Personal data shall be processed in a manner that is lawful, fair and transparent.

2. Purpose limitation

Data is collected for specified, explicit and legitimate purposes.

3. Data minimisation

The data processed shall be adequate, relevant and limited to what is necessary in relation to the purpose for which it is processed.

4. Accuracy

The data shall be accurate and up to date. All reasonable steps shall be taken to ensure that inaccurate data is erased or rectified without delay.

5. Storage limitation

The data shall only be kept in a form which permits identification of the data subjects for no longer than is necessary.

6. Integrity and confidentiality

Data shall be processed in such a way that ensures appropriate security of the data, including protection against unauthorised or unlawful processing. Data security measures include encryption, authentication and authorisation mechanisms.

The eight rights of the data subject as set out below are incorporated into our GDPR policy;

- The right to be informed
- The right of access to personal data
- The right to rectification of personal data
- The right of erasure
- The right to object
- The right to restrict processing
- The right to data portability
- The individual's rights with regard to automated decision making and profiling

We are currently working toward accreditation under the ISO 27000 series standard for information security management system.

5.8 Anonymisation and pseudonymisation

5.8.1 Processing of anonymous information

The principles of data protection do not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.

5.8.2 Pseudonymisation

The principles of data protection apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments.

The application of pseudonymisation to personal data can reduce the risks to the data subjects concerned and help controllers and processors to meet their data-protection obligations. The explicit introduction of 'pseudonymisation' in this Regulation is not intended to preclude any other measures of data protection.

In Ireland PT.5 S.69 [No. 7.] of the Data Protection Act 2018 defines pseudonymisation as the following:

"pseudonymisation" means the processing of personal data in such a way that the data

can no longer be attributed to a specific data subject without the use of additional

information, provided that—

(a) such additional information is kept separately from the data, and

(b) is subject to technical and organisational measures to ensure that the data are not

attributed to an identified or identifiable individual;

About Vizier: natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other

identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.

5.9 Guidelines in case of breaches

A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned. Therefore, as soon as the controller becomes aware that a personal data breach has occurred, the controller should notify the personal data breach to the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the controller is able to demonstrate, in accordance with the accountability principle, that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where such notification cannot be achieved within 72 hours, the reasons for the delay should accompany the notification and information may be provided in phases without undue further delay.

6 Inventory of all personal data in Vizier

Vizier has to make an inventory of all personal data Vizier is holding with key questions:

- Why is Vizier holding this data?
- How did Vizier obtain it?
- Why was it originally gathered?
- How long will Vizier retain it?
- How secure is it, both in terms of encryption and accessibility?
- Does Vizier ever share it with third parties and on what basis?

6.1 Vizier architecture and data flow

The current Vizier architecture can be described in terms of data flows between 4 main architecture components:

1. End user devices which communicates with the Vizier Cloud Server (VCS) (Flow 1), the Memory Club (Flow 3) and other online services (Flow 3). The Memory Club and the VCS are maintained by Vizier partners. Other online services could include widely available applications and services, e.g. Google, Skype, etc.

2. The VCS communicates with the whole ecosystem, i.e. User devices (Flow 1), Memory Club and other online services (Flow 2), and Carer and administrators in support organisations (Flow 4)

3. The Memory Club communicates with the Vizier cloud server (Flow 2) for some processes, directly with the End user devices, e.g. tablet, (Flow 3) and devices used by support organisations (Flow 4).

4. Other online services communicates directly with End User Devices (Flow 3) , or with the Vizier cloud server (Flow 3)

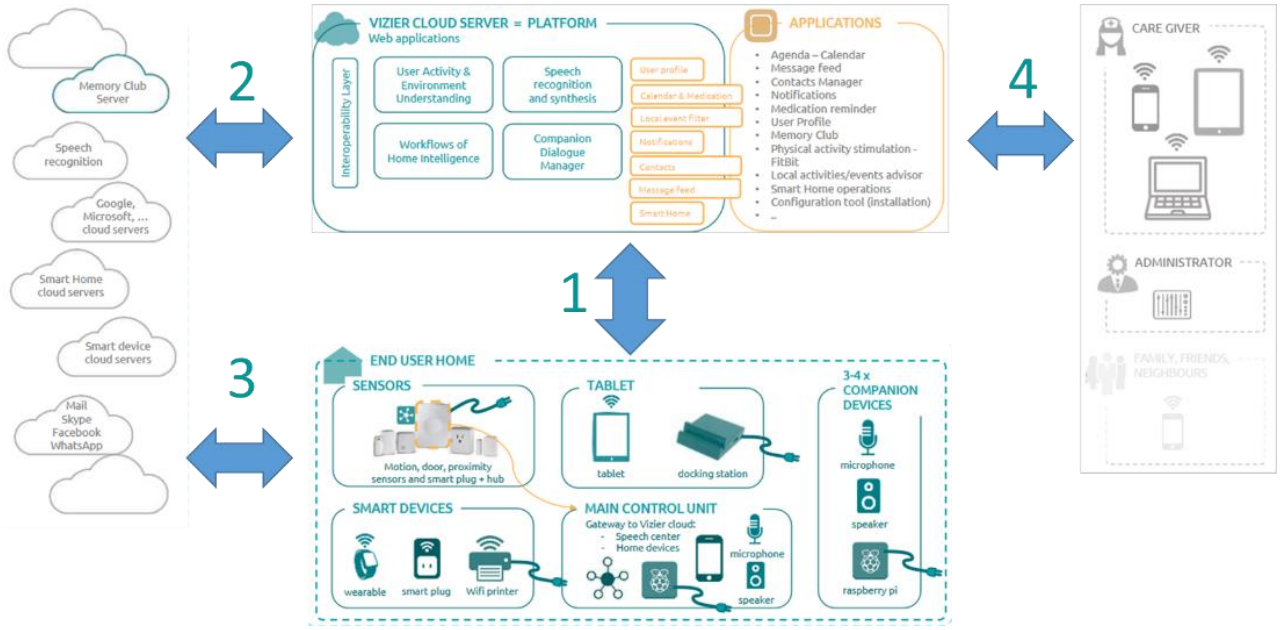

FIGURE 6 VIZIER ARCHITECTURE AND 4 DATA FLOWS

6.2 General overview of Vizier data inventory and processing

The Vizier processes data collected from different sources: 1. End user devices and main controller unit, 2. Vizier Cloud Server (VCS), 3. Formal and informal support organisations, 4. the Memory club, and 5. other online services.

1. As a general principle, all end user accounts are created with a pseudonym and a unique user id code. (We are checking on the feasibility of using first names instead of pseudonym).
2. The matching list between pseudonym, end user real name, contact information, and other user information is kept separately, outside of the Vizier platform, by the user organisations, e.g. Myhomecare, Familiehulp, and VIVA.
3. Information collected by the applications and services provided by Vizier partners are stored on the application servers. Information is exchanged between Vizier partner applications only when it is required for providing a richer user experience or personalized applications. This information is usually stored in the Vizier cloud server.
4. Information collected by other third party online services or devices are stored on the third party servers. Some of this information is extracted to the Vizier cloud server.

The section Vizier data processing inventory and their management below gives further details on the how and where data is collected and the documents used to establish the basis for data processing under the GDPR

6.3 Vizier data processing inventory and their management

The table below gives an overview how and where data is collected and processed, and the documents (Privacy statements, informed consent or user terms and conditions) to comply with the GDPR requirements for processing and management of this data by Vizier partners. These document should include a clear statement (warning) to End Users when, as a result of or in conjunction to using Vizier applications, features, and services, any of their data is collected, managed or controlled by non-Vizier partners, e.g. Google, Fitbit, etc. In this case, the documents should also recommend that the End Users review the Privacy and use policies of non-Vizier applications or services.

TYPE OF DATA	HOW DATA IS COLLECTED AND STORED	HELD BY	INFORMED CONSENT / PRIVACY STATEMENTS
Matching list End user real name and Unique User Ids, or Pseudonyms	Collected during account creation Stored at local premise of End User Organisations only	End Users: Myhomecare, Familiehulp, VIVA	Vizier informed consent and privacy statement. (Should cover all Vizier partner apps, including cloud platforms used the apps, e.g. AWS)
User Id, profile information, user activity, preferences, contacts, calendar, medication schedule, MClub data, etc.	Collected by the Vizier Main Controller Unit and the Vizier Cloud Server (VCS). Stored and processed by the VCS. Used by the online services, Vizier Behavioural Change program, and the MClub.	End users : Myhomecare, Familiehulp, VIVA Support Staff : DCU, UNIGE, Salaso	Vizier informed consent and privacy statement. Replace Vizier documents with appropriate terms and conditions during exploitation.
User Id, basic profile information, quiz results	Collected by the Memory Club. Selected information can be exchange and stored in the VCS to enable personalization and interoperability.	End Users : Myhomecare, Familiehulp, VIVA Support Staff: NetUnion	Vizier informed consent and privacy statement.

			Replace Vizier documents with appropriate terms and conditions during exploitation.
Third party devices and applications	Data collected by 3rd party devices, i.e. fitbit, sensors, etc. Collected and managed by non-Vizier partners. Data extracted by Vizier apps and stored and processed by the VCS.	End users : Myhomecare, Familiehulp, VIVA Third party platforms Support Staff : DCU, UNIGE, Salaso	Vizier informed consent and privacy statement. (Include clear statement regarding data storage and used by 3rd party platforms, and reference to their privacy policies, e.g. read the policy when they popup..?) Replace Vizier documents with appropriate terms and conditions during exploitation.

6.4 Vizier Cloud Server (VCS) Data Inventory and GDPR Compliance

6.4.1 VCS data inventory and how they are used in the pre-trial version

APPLICATION	TYPE OF DATA	WHEN COLLECTED	ENCRYPTION	THIRD PARTIES
Agenda	Appointment description, date, hour, location, other invitees	Own input Or Acceptation invite / proposed activity	Encryption of all data from device to host server. Encryption from the host server to the Vizier platform. Encryption on the Vizier platform.	(Google Calendar → not implemented at this stage: local tablet calendar)
Personal preferences (user profile)	Hobbies, fields of interest, ... (tick boxes in a list)	Setup of the Vizier account Or Change settings	Encryption on the vizier platform.	none

Home sensor data	Door open / closed, Movement in the room, indoor tracking, smart socket on/off, window open / closed, fridge open/closed, smoke alarm.	All the time, on a continual basis.	Encryption of all data from device to host server. Encryption from the host server to the Vizier platform. Encryption on the Vizier platform.	Samsung, potentially other home sensor sources later, if they are compliant.
Personal sensor data	Step count, heart rate, sleep pattern, time in bed, distance, calories burned, floors climbed, hours of active and stationary, hourly activity, weight, body fat percentage , BMI	All the time, when the fitness watch is worn & Beddit sensor is in place.	Encryption of all data from device to host server. Encryption from the host server to the Vizier platform. Encryption on the Vizier platform.	Fitbit, potentially other biometric sensor sources later, if they are compliant.

Messaging	Message body, sender, receiver, metadata (date, etc.)	Upon sending or receiving a message	Encryption of all data from device to host server. Encryption from the host server to the Vizier platform. Encryption on the Vizier platform.	Supports the integration of various 3rd party tools, from providers such as Google, Facebook.
Various reminders	Reminder-focused information (.e.g time, reminder message, reoccurrence details)	When setting-up or changing the reminder.	Encryption of all data from device to host server. Encryption from the host server to the Vizier platform. Encryption on the Vizier platform	(Google Calendar → not implemented at this stage: local tablet calendar)

6.4.2 Compliance and todo list for VCS related to the GDPR Rights

RIGHTS	VCS COMPLIANCE DURING THE PROJECT	COMMENTS / TODO BEFORE TRIAL OR SUBSEQUENT STEPS
Right of data access	The data of the user is accessible via the Vizier interface mechanisms. Should a data be requested by the user, it can be made available in raw from the database.	Provide the ability for an administrator of the system to be able to export the data related to any user and make it available to that user. This will require the development of additional SQL statements that can be run by administrators or data access request operators.
Right to rectification (to have inaccuracies corrected)	The data in the Vizier Cloud Server is coming from sensors and as such is expected to be valid. It is unlikely that there will be any requests to update such sensor data, however if this does occur, the data can be directly updated on the server database.	All data in the vizier platform must be updatable and provision for this must be made in the database. By its nature as a database system, any data in the Vizier database on the VCS is updatable.
Right to erasure (to have information erased)	Any participant in the Vizier project can have their data deleted at any point in time. This is supported by direct deletion of the relevant data from the database.	The platform must be able to support the deletion of all data related to a given user ID.
Right to restrict processing	Should any participant in the Vizier project wish to pause or stop their involvement, or otherwise restrict the processor of their data, this is supported by the system. Should a participant wish to halt or restrict the processing of a component of their Vizier data (e.g. activity only) then this will be supported.	It must be possible for the platform to turn on / off certain components or features, such as the environmental sensing, activity sensing, communication modules, etc. This functionality must be included for subsequent trials.
Notification of rectification or erasure of personal data	Should any personal data be erased or rectified/updated during the Vizier project, then the user will be given information about such data updates or deletions.	Ensure that any data deletion or direct modification to existing sensor or personal data is followed up with appropriate notices.

6.5 MClub Data Inventory and GDPR Compliance

The Memory Club is a service provided to local organisation (Health care service provider, associations, etc.), who in turn provide access to people who want to use the Memory Club (Participants). When a participant wants to use the Memory Club they ask an authorized representative of the organisation (Staff) to open an account for them. The Staff opens an account using a pseudonym or an id code and monitors the participant during the use of the program. Real name, address and phone number of the Participants are not used for opening the account.

6.5.1 MClub terms and GDPR matching terms and concepts

GDPR	MCLUB TERMS	GDPR DEFINITION (RIDLEY, 2017)	COMMENTS/ VIZIER AND MCLUB CONTEXT
Personal Data	**Personal Data**	The GDPR defines 'personal data' as: '...any information relating to an identified or identifiable nature person ('data subject). The GDPR definition of 'personal data' is broader than under the DPA and includes IP addresses, device IDs, location data and genetic and biometric data.	
Data subject	**Participants, end users**	Participants, end users, are terms used in this document to indicate Identifiable nature person ('data subjects'). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person'.	

Controller	**Organisation**	The 'controller' is the party who determines 'why' the personal data will be processed (i.e. the purpose of the processing) and, where the controller appoints a processor, the processor determines 'how' the personal data will be processed (i.e. the method of the processing).	In Vizier, the controllers are typically the end user organisation, e.g. **MyhomeCare, FamilieHulp, VIVA**. During the exploitation phase, the role of controller depends on the exploitation model.
Processor	**APP, service or platform provider**	Typically, an IT services provider will be a 'processor' and its customer will be the 'controller'.	In Vizier the Processors are typically the technical partners who provides the systems and applications. **For the MClub NetUnion is the processor**.
Employee	**Staff, Researchers, Support staff**	No explicit GDPR definition observed for now.	For the Memory Club: Staff users = employee of end user organisations Researchers = employee of Universities. Support staff = employee of SMEs
Consents and agreements, fair processing statements	**Multiple documents**	Informed consent is used during the trial period Users terms and condition is used during exploitation For simplification purpose, fair processing statement contents are in included in Privacy Statements	

6.5.2 MClub Inventory of data collected and how they are used

TYPE OF DATA	HOW IT IS COLLECTED AND USED	WHEN COLLECTED	ENCRYPTION	THIRD PARTIES
Participant account profile information	User code: This is a code number, or a pseudonym. The real name of the participant is not used. Matching list between real name and contact information is kept by the organisation. Email address: The e-mail address is encrypted with a one way hash before storage. It is only used to send temporary passwords, or other messages. Password: Stored encrypted. Language: (required to deliver the right language version) Gender (could be optional) Year of birth (Optional)	Collected when the account is created by a Staff member. Participants cannot create their own accounts directly.	TLS encryption of all data transmitted over the internet. e-mail address and password are stored as an encrypted one-way hash using a secured hash algorithm (SHA).	Relevant data could be used by third parties as follows: Enabling access and tailored delivery of other services on the Vizier platform, e.g. single sign on, message exchange, etc. For research and statistical purpose to improve the program. No third party use for commercial purposes. The MClub server is physically located in the EU (Germany) and the Processors and Researchers located in Switzerland, which is included in the EU list of countries with adequate data protection compliance.
Quiz data: **Scores, levels,**	Answers to multiple choice questions are used : as triggers for displaying feedback, next questions, or access to next level.	During use	TLS encryption of all data transmitted over the internet.	Same as above.

	to display scores, progress through the levels and achievement to the Staff and participants.			
Logs, location, or device data	Logs, timestamps, last log in, etc. No location or device data, i.e. IP addresses, device IDs, genetic or biometric data are collected.	During use	N/A	Same as above if data is transmitted, shared or otherwise processed.

6.5.3 Compliance and todo list for Memory Club related to the GDPR principles

PRINCIPLES	MCLUB COMPLIANCE DURING THE PROJECT	COMMENTS / TODO BEFORE TRIAL OR SUBSEQUENT STEPS
Lawfulness of processing	A signed Informed Consent form, accompanied by a Privacy statement, will be used as the legal basis for processing of MClub data. Acceptance of a user terms and conditions (T&C), accompanied by a Privacy Statement will serve as the legal basis for data process during the exploitation stage. The informed consent, T&C, and Privacy Statement should comply with prevail ethical standards for research activity and provisions outlined by the EU GDPR, e.g. stored, purpose for processing, etc. will be included in the a easy to understand privacy statement.	Update informed consent statement and reference privacy statement. Attach privacy statement to informed consent if necessary. (a) Make privacy statement in 3 languages and include on website. (b) Implement explicit consent features as necessary, e.g. click to accept use of cookies. (c) Include Risk Impact analysis and rectification procedure in the PS?

PRINCIPLES	MCLUB COMPLIANCE DURING THE PROJECT	COMMENTS / TODO BEFORE TRIAL OR SUBSEQUENT STEPS
	Check boxes will be included in the informed consent form or as part of the account creation process to collect explicit consent when necessary.	(d) Identify other legal basis for data processing for the exploitation stage, e.g. Acceptance of user terms and conditions providing a contractual (legal) basis for data processing.
Purpose limitation:	Data is collected and processed, explicitly, for legitimate research purpose, specific: For optimal delivery of program features as listed in the section above.	(a) Include purpose limitation in the privacy statements or terms and condition of use as the program evolves over time. (b) Update purpose limitation section statement as the use of data by other applications running on the Vizier platform or other third party applications evolves over time.
Data minimization:	Use of personal information is kept to a strict minimum as descripted in the section above.	
Storage limitation:	The platform will retain the collected data in accordance to the data retention policy of the Organisations using the platform.	(a) Confirm the following with Vizier Partners, then update relevant documents. (b) Data collected will be deleted 1 year after the end of the project? (c) Anonymized data collected for research will be destroyed after research has been completed. The data should not be kept for more than 1 years after the end of the project?
Integrity and confidentiality:	Access to processed data is limited to the following: Participants, Staff from health care organisation or community associations (VIVA)	Check if this is covered elsewhere and streamline next version of document.

PRINCIPLES	MCLUB COMPLIANCE DURING THE PROJECT	COMMENTS / TODO BEFORE TRIAL OR SUBSEQUENT STEPS
	Access to anonymized data is limited to: the platform provider (NU), other applications using these data to personalize service delivery.	
Data protection by design	Data and privacy protection concepts are an integral part of Staff training and end user orientation. Data transmitted over the internet using standard TSL protocol. All user password and e-mail address encrypted with one way hash (SHA) before storing in database. Matching list between Enduser real name and contact information and pseudonym used to open the account is kept by the Controller (Health care organisation and community associations). Processors, and 3rd party organisations cannot access this information.	How does Vizier encrypt data transmission over the internet?
Sensitive Data, and pseudonymisation	The most sensitive information for the MClub (and Vizier) is the matching list between and anonymous id, or the pseudonym (whichever is used), with the end user's real name and contact information. This information is not stored in the Organization's premises, separate from the MClub platform. Financial data of individual users are not collected on the MClub for payment or e-commerce purposes.	Find out if we can use first names to open accounts.
Risk analysis and impact of data breach.	The MClub collects data on user responses and user activities that are specific to the program functions. This data would not have a high enough financial value to attract potential hacking.	See if risk analysis is required for official reporting or inclusion into privacy statement.

PRINCIPLES	MCLUB COMPLIANCE DURING THE PROJECT	COMMENTS / TODO BEFORE TRIAL OR SUBSEQUENT STEPS
	Financial risk is minimum or payment information is not collected on the MClub web. Risk to personal reputation is also minimal as the results are just right or wrong answers to multiple choice questions about daily activities of fictitious scenarios.	
Data breach definition and notification guidelines	The most critical data breach in the MClub is when the both the following events happens: The matching list is exposed and access to the MClub is compromised. If a critical data breach occurs, the Staff should inform the EndUsers and give them the option to delete their collected data or their account.	Verify if this policy is adequate for the small data set involved.

6.5.4 Compliance and todo list for Memory Club related to the GDPR Rights

RIGHTS	MCLUB COMPLIANCE DURING THE PROJECT	COMMENTS / TODO BEFORE TRIAL OR SUBSEQUENT STEPS
Right of data access	Participants will have access to the Data Inventory described in this document showing: the purpose of the processing; categories of personal data concerned; third parties, etc. can see their information in their account page They can see their process in the progress page	Privacy / Fair processing statement actions: (a) Integrate data inventory information into MClub Privacy Statement (b) Include statements specifying that requests should be reasonable, e.g. data that is available without extra programming or special scripts.

RIGHTS	MCLUB COMPLIANCE DURING THE PROJECT	COMMENTS / TODO BEFORE TRIAL OR SUBSEQUENT STEPS
Right to rectification (to have inaccuracies corrected)	The participant can request their Organisation to rectify incorrect data within reason. The Organisation then requests the platform administrator to perform the deletion. Given the nature of the information collected by the MClub, e.g. answers to multiple choice questions, where the correct answer is displayed in case of error, and where no monetary prizes or rewards are given based on the score, we do not foresee significant rectification requests.	Privacy / Fair processing statement actions: Include statement on: who to contact, what can be rectified by themselves, and what should be rectified by Staff or Support Staff. Internal Process actions: Include process to improve Accuracy in operation and training documents. Researchers and staff users should check accuracy of the following information and update them as necessary. Participant account information, especially, before creating the account. The participant contact information that are kept, locally, and not on the Memory Club platform, in case you need to contact them by phone or other means. During the exploitation stage, the program might need to include systematic checks, e.g. periodically asking the user to update their contact information, etc.
Right to erasure (to have information erased)	The MClub conforms to the right to erasure outlined in section the Right to erasure (to have information erased) in this document The participant can request the managing Organisation to delete their account at any time. The platform will delete a Participant's data upon request by the Organisation managing the participant's account.	(a) Implement new program functions for erasing End User account or collected data, with or without, deleting profile and account information. (b) Implement access control, e.g. who can delete accounts, who can delete information.

RIGHTS	MCLUB COMPLIANCE DURING THE PROJECT	COMMENTS / TODO BEFORE TRIAL OR SUBSEQUENT STEPS
	The Platform will delete a User's account and all collected date upon request in the case of a data breach. (See Data breach definition and notification guidelines in section Compliance and todo list for Memory Club related to the GDPR principles)	
Right to restrict processing	The MClub will adhere to the Right to restriction of processing rights as described in the section Right to restriction of processing above.	(a) State a definitive date for data erasure e.g. 1 year after project completion? (b) Verify whether there is a conflict with right of restricted use where "the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defense of legal claims;"
Notification of rectification or erasure of personal data	During the trial, Staff users who have direct contact with the data subjects (end users) will correspond directly with end user regarding rectification, erasures and data breach.	Investigate adding features for automatic notifications of specific rectification or erasure notices as necessary.

6.6 Conclusions

The application of the GDPR gives a great responsibility to the developers of the VIZIER platform, especially since several countries are involved and because personal data include both more innocent data and sensitive data.

In Vizier's final report, it is necessary to attribute a separate chapter to Vizier's concrete implementation of the GDPR and the difficulties and recommendations that result from this for current and future AAL projects.

7 Bibliography

EU . (n.d.). *Adequacy of the protection of personal data in non-EU countries*. Retrieved from https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en

EU Law. (n.d.). *EU Law portal data protection*. Retrieved from EU Law: https://ec.europa.eu/info/law/law-topic/data-protection_en

Official Journal of the European Union. (2016, April 27). Retrieved from EUR-Lex: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG

Ridley, S. (2017, November 03). *GDPR guide for SMEs – everything a small business needs to know.* Retrieved from https://www.hiscox.co.uk/business-blog/gdpr-guide-smes-everything-small-business-needs-know/: https://www.hiscox.co.uk/business-blog/wp-content/uploads/2017/11/Hiscox-UK-GDPR-Guide.pdf

Staehelin, L. &. (2017, September 26). *Revision of Swiss Federal Data Protection Act* . Retrieved from https://www.lexology.com: https://www.lexology.com/library/detail.aspx?g=9002396d-cfc5-4267-b84e-caaa846aff05