A GDPR friendly Guider

Written by: Bianca Daltri, Olivier de Wijs, Emilie Mellbye Rytter-Ingebrigtsen and Wenhan Feng

Words: 11891

Dear Simen,

Below you can find our report concerning how GDPR applies to your robotic guider "Guider". The use of Guider is so wide that we chose to limit the scope to the Faculty of Law of the University of Bergen. We found that it is possible to have a GDPR compliant Guider, but that there is a need for some changes in how Guider interacts with users, what data Guider receives from the customer and some technical adjustments to ensure collection of less data.

Table of contents

1. Introduction

<u>What is Guider?</u>

Guider is a robot which aims to help a person navigate with ease to where they want to go within a building[1]. The problem the creator tried to solve was that in many big buildings, such as large university buildings, it is easy to get lost and difficult to find your wanted destination. The creator had experienced this himself using 15 minutes trying to locate where room 305 was in the university he exchanged to and ending up being late to his appointment[2]. This is especially a problem in places where there are new people all the time. To solve this problem the creator thought that a map often is not sufficient and that people would come to the right place more easily if they were guided there by a robot.

In the creation of Guider the creator evolved the initial thought. He thought about different places where Guider could be useful such as offices and hospitals.[3] In addition, Guider could be used in other ways than just guiding. Guider could have more of the role of a receptionist, such as giving the person information about their next meeting and making coffee to the user if it is connected to a coffee machine.

The user of Guider would be anyone who wants to be guided or use the personalised assistance that Guider can offer.

<u>Does GDPR apply to Guider?</u>

The question of whether GDPR applies or not depends on the use of Guider. As written below we have chosen a layered approach. This enables the customer to choose a Guider that does not process any personal data, by only giving Guider room numbers, and the user the possibility to type in a room number.[4] But if Guider is to have any more functions than that the GDPR applies because Guider will "[process] personal data wholly or partly by automated means" see GDPR Article 2 (1). The details concerning what types of processing will be described later in the paper.

As long as Guider processes information and is set in the EU or the customer is set in the EU, the GDPR applies according to GDPR Article 3 (1) and (2) (a) (b). The only possible exception for the material scope is if Guider is bought by the Union where the Regulation (EC) No 45/2001 applies according to GDPR Article 2 (3).

---

[1] Johansen, S. L., *Guider - a robotic guider*, MIX301 Essay at University of Bergen, p.4.
[2] Simen Larsen Johansens pitch on 16 March 2021 to the Privacy and Data protection: GDPR class on zoom.
[3] *Ibidem*.
[4] See illustration in part 3.

<u>Our approach</u>

The aim of our report is to assess if Guider is GDPR compliant and if not demonstrate how this can be done. To achieve this we will first go through the initial proposal and then go through how we think Guider could be made GDPR compliant.

We have chosen to place Guider at the Faculty of Law in a non-pandemic scenario, to make the report a manageable size and to make concrete assessments. At the same time we have thought of different possible customers and locations when choosing our approach and will thus comment on the fit for other scenarios along the way. However the assessments concerning the legal basis may be different in other locations as the data may for example be special categories of data. In the Faculty scenario we have chosen a non-pandemic scenario because a pandemic is not the normal state, and because the need for guiding is smaller when there is less happening at the Faculty. The Faculty of law is a potential place for Guider because there are new students coming all the time, for example exchange students or students from other faculties who have lectures there. In addition some rooms are rented out to for example norwegian classes or debates. The Faculty is also publicly accessible in the main opening hours.

In our report we will distinguish between the user and the data subject. The user is the person that uses Guider while the data subject is defined in GDPR Article 4 (1) as "an identified or identifiable natural person". These definitions may overlap, but not necessarily. For example the user is also a data subject if the person used his/her voice to speak in order to get help and Guider processes his/her voice. There are also scenarios where Guider does not process any personal data and thus there will be no data subjects, but there will be a user. Guider could also accidentally process the voice of people in the room and would then process the personal data of data subjects, but not users.

We have also chosen to focus on the aspects of GDPR that are especially relevant and challenging with Guider. Therefore we will be focusing on the question of which role Guider and the customer should have, the legal basis assessment, the risk assessments, the principles and the design of the information to the data subjects. We will not assess a scenario in which Guider is established in an area outside the EU/EEA and the transfer of personal data to third countries. Concerning the principles we have actively used the principles in GDPR Article 5 during our assessments and will therefore not have a separate part concerning the principles.

2. The initial proposal of the creator

The creator of Guider initially envisioned that all users would speak to Guider and therefore Guider would process the users voice[5]. However, it is possible and easy for the user to type in their wanted destination as the primary use is not in accordance with the principle of data minimisation in GDPR Article 5 (c). In addition, in the initial proposal Guider would recognise faces to keep track of the user[6]. This would not be in accordance with data minimisation as the purpose of keeping track of the user could be done by cameras with filters.[7] Furthermore Guider would recognise faces to identify when a user used Guider again[8]. This would be processing of special categories of data according to Article 9 because the face is biometric data after Article 4 (14) and it would be used "for the purpose of uniquely identifying a natural person". Our assessment is that there would be no legal grounds for processing special categories of data of every person using Guider with no exceptions.

Thus we quickly realised that Guider was not GDPR compliant. To make a GDPR compliant version of Guider we identified the different purposes Guider has and from there evaluated how those could be reached in a GDPR compliant way. This way we 'started again' and were thus able to implement data protection by design in accordance with GDPR Article 25.

3. The layered approach

In short the layered approach entails that the amount of personal data gathered will depend on the purposes the customer wants Guider to fulfil and the functions users want to utilise.

In our project it means for example that the user can choose between writing in their wanted destination and saying it with their voice. This is in accordance with data minimisation[9] because it entails that the user can choose to use Guider in a way that no personal data will be processed. This is important both for the principle of fairness as some users may wish to use Guider without their personal data being processed. In addition to being fair it makes Guider available also to persons who do not wish their personal data to be processed.

Consequently, the customer can for example choose between giving Guider a map with numbers and a map with names of the persons in the different offices. This means that the customer can choose to not

---

[5] Johansen, S. L., *Guider - a robotic guider*, cit., p. 5.
[6] *Ivi*, p. 6.
[7] See part 6 of this report.
[8] Johansen, S. L., *Guider - a robotic guider*, cit., p. 6.
[9] Regulation (EU) 2016/679 of the European Parliament and 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), Article 5 (1) (c).

put in any personal data. This way the customer can limit the function to the purposes they need[10] and it is transparent which choices involve what data and which processes.[11] It is also important because the wishes and risk assessments of the customers will be very different based on where Guider will be. For example it may be helpful and balanced that Guider has all its functions in an office building, but that might not be the case in a hospital.

One can ask if it is possible for Guider to perform certain functions without personal data, should Guider stop there? But for Guider to guide people and help them in an effective way it is important for Guider to be more easily available with voice command or to be able to guide the person not only based on room numbers, but also names.

The functions that were are going to assess

The list of functions can be found in the table of contents. We have found that it can be a bit confusing and therefore we have chosen to make these illustrations to demonstrate the differences.
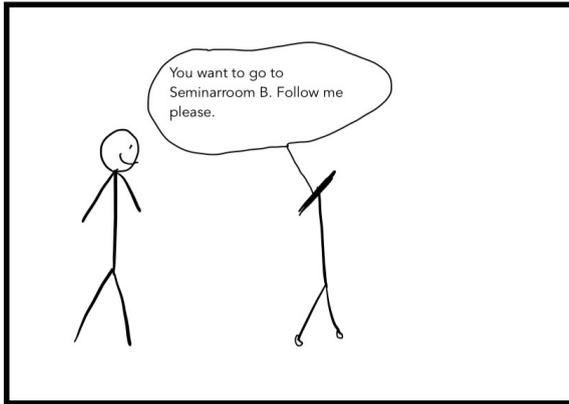

Ways for the user to communicate with Guider

___
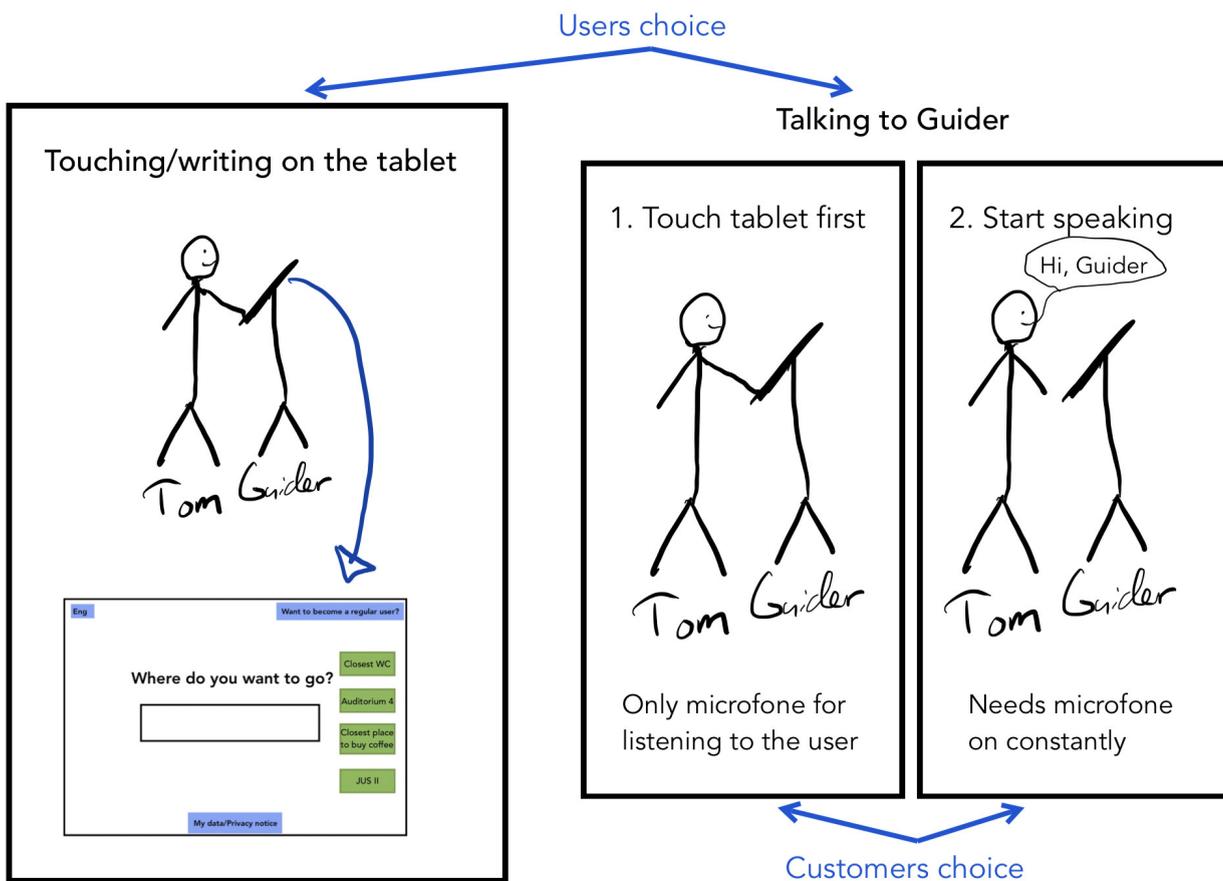
[10] GDPR Article 5 (1) (b).
[11] GDPR Article 5 (1) (a).
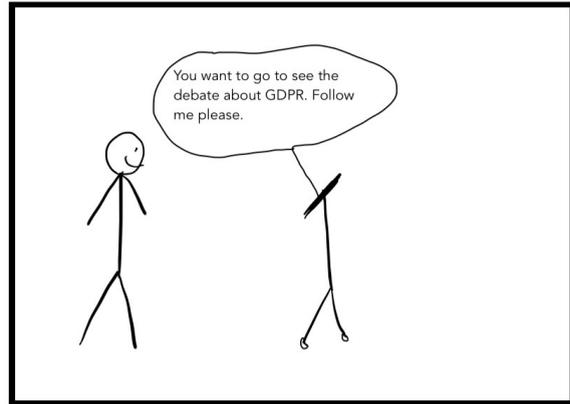
What Guider can help the ordinary user with
Guiding the way to a place by knowing

Room number

You want to go to Seminarroom B. Follow me please.

Schedule of rooms

Optional for the customer

You want to go to see the debate about GDPR. Follow me please.

Name

You want to go to Tom Smiths office. Follow me please.

Schedule of persons
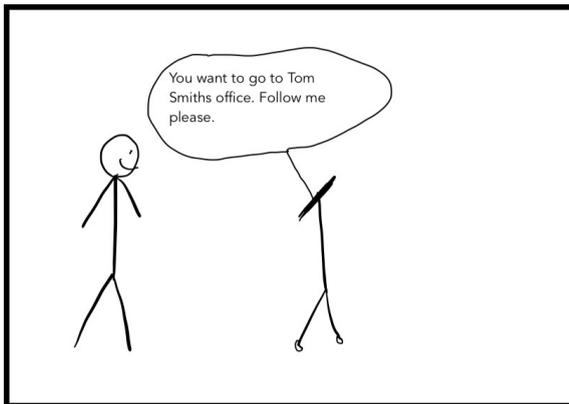
Tom is busy right now, but he will be available in 30 minutes.
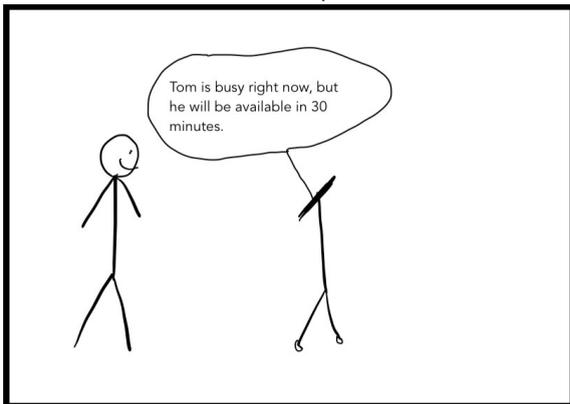
The personalised experience for the regular user of Guider

Optional both for the customer and the user

Hi, guider
Where and when is my next meeting?

Yes, please.

Good morning, Tom! Hope you're having a great day so far.
You're next meeting is in seminarroom A in 10 minutes.
Would you like a macchiato before you go up?
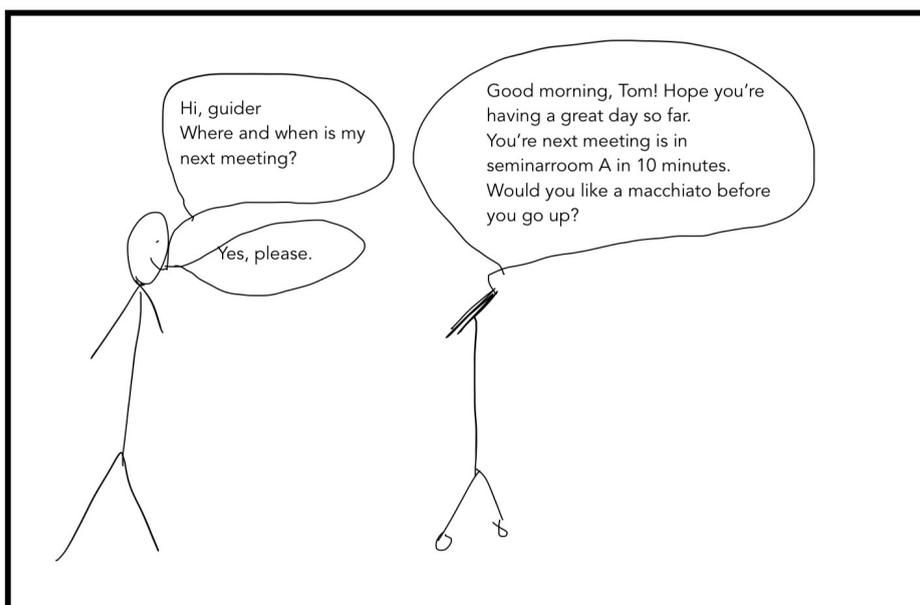
4. Controller and Processor: who is who?

To determine the rights and obligations of various actors involved in Guider it is important to clearly distinguish them at this stage. Under the GDPR the concepts of 'controller' and 'processor' are functional concepts that are used to allocate responsibilities according to the actual roles they have in the processing of personal data.[12] Most relevant information on the interpretation of the concepts of controller and processors and on their respective roles can be found in the GDPR under chapters 1 to 4 and in the European Data Protection Board Guidelines 07/2020 on the concepts of controller and processor in the GDPR. In this chapter we start by giving a brief theoretical overview of the different players and their legal obligations towards the data subject. Then we can apply this to the relationship of the different players within Guider and focus on the legal obligations that are most relevant to this project.

The controller will be the most important actor vis-à-vis the data subject. The controller is "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data".[13] In other words the controller is the one that determines how and why personal data will be processed. The importance of the controller is not limited to accountability for the lawful processing of data but will also determine the liability[14] and potential fines.[15] Under GDPR Article 5 the controller has the obligation that the processing of personal data complies with the principles of lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality. Additionally, the controller is obliged to demonstrate compliance with all these principles (accountability).[16]

The protection of the data subject under the principles of the GDPR and the security of processing will for a large part depend on using the right processor. Therefore the controller has a duty to only use processors that are able to provide sufficient guarantees to implement appropriate technical and organisational measures, in particular "in terms of expert knowledge, reliability and resources, to implement technical and organisational measures which will meet the requirements of this Regulation, including for the security of processing".[17] This will be a form of risk assessment that will depend on the nature, scope, context and purposes of processing as well as the risks for the rights and freedoms

---

[12] European Data Protection Board, *Guidelines 07/2020 on the concepts of controller and processor in the GDPR. Version 1.0*, 02 September 2020, p. 9, https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf (last accessed 19/05/2021).
[13] GDPR Article 4 (7).
[14] GDPR Article 82 (2).
[15] GDPR Article 83.
[16] GDPR Articles 5 (1) and 5 (2).
[17] GDPR Article 28 (1) and Recital 81.

of natural persons.[18] The relationship between the controller and the processor and their respective rights and obligations under the GDPR has to be put in writing, in a contract or other legal act under Union or Member State law.

The GDPR also sets out some minimum requirements for this contract with regards to the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, and the obligations and rights of the controller.[19] The controller is also under an obligation to make certain information available to the data subject. We will discuss some of the content of this information when we look at the different rights and obligations of the actors involved in Guider.

The 'processor' is defined as "the natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller".[20] The two basic conditions for qualifying as processor are: being a separate entity in relation to the controller and processing personal data on the controller's behalf. There is a definite subordinate relationship with the controller. Processing "on behalf of" means the processor serves the controllers' interest and recalls the legal concept of "delegation".[21] The relationship between the controller and the processor is determined by the already mentioned contract or other legal act.[22] The GDPR also imposes some direct obligations on the processor. These are: maintaining a record of all categories of processing activities[23], implementing appropriate technical and organisational measures[24], designating a data protection officer (under certain conditions)[25] and notifying the controller without undue delay after becoming aware of a personal data breach.[26]

The GDPR aims to protect data subjects in relation to the processing of personal data.[27] Therefore, the rights of the data subject mirrors to a large degree the obligations of the controller. In order to effectively exercise their rights the data subject will need to be aware of their rights and to have information regarding the processing of its personal data. Chapter III of the GDPR deals with the rights of data subjects. At the time when personal data are obtained there is a right to information that mirrors the obligation of the controller to provide information.[28] In addition to this the data subject has a right of access to personal data. This means the data subject has the right to obtain confirmation on

---

[18] European Data Protection Board, *Guidelines 07/2020*, cit., pp. 29-30.
[19] GDPR Article 28.
[20] GDPR Article 4 (8).
[21] European Data Protection Board, *Guidelines 07/2020*, cit., p. 24.
[22] GDPR Article 28 (3).
[23] GDPR Article 30 (2).
[24] GDPR Article 32.
[25] GDPR Article 37.
[26] GDPR Article 33 (2).
[27] GDPR Recital 1.
[28] GDPR Articles 13 and 14.

whether or not personal data concerning him is being processed, in other words to ask the controller if they are a data subject. If this is the case the controller has an obligation to give certain information.[29] When personal data that is being processed is inaccurate or incomplete the data subject has the right to rectification, within undue delay.[30] Under certain circumstances the data subject has the right to obtain erasure from the controller of personal data concerning him. This right applies for example to the storing of certain data that is no longer necessary in relation to the purpose for which it was collected or when consent is withdrawn and there is no other legal basis for processing.[31] Under some circumstances the data subject has the right to object to processing of personal data to receive the personal data concerning him, which he or she has provided to a controller, in order to transmit that data to another controller.[32]

The involvement of Guider in the processing of personal data will vary according to the services its customers want Guider to provide. Both parties are free to allocate their roles and responsibilities, as long as they are in accordance with the GDPR. They will have to decide who is controller and who is processor, which has to be reflective of the reality of day-to-day working. When Guider is listed as the processor, but behind the scenes it decides on the means and purpose of the processing it will be considered as the controller in respect of that processing.[33] This will affect its obligations, liability and potential fines. The contract between Guider and its customers, that determines their respective roles and responsibilities, should not just restate what is set in the provisions of the GDPR but it should set out specific tasks and responsibilities of the controller and processor. The contract will therefore have to be drafted on a case-by-case basis. The negotiations and the stipulation are an opportunity to specify the details on the responsibilities relevant to the specific processing.[34]

Under the most basic configuration the customer will be the controller and Guider the processor. This scenario requires that the customer decides on the purpose and means of the processing. This does not mean that Guider cannot give advice or suggestions on the purpose and means, but it will be the customer that is the ultimate decision-maker. The customers' instructions can leave a degree of discretion to Guider as to how best serve its interest. This can allow Guider to choose the most suitable technical and organisational solution. This scenario has some advantages for the customer. In the first place, as the controller, they have the final say in how the data Guider processes is being used. This doesn't mean the company has to have direct access to the data themselves.[35] This also means they can precisely decide the involvement of Guider in the contract, within the limits of its

---

[29] GDPR Article 15.
[30] GDPR Article 16.
[31] For a full overview see: GDPR Article 17.
[32] GDPR Articles 20 and 21.
[33] GDPR Article 28 (10).
[34] European Data Protection Board, *Guidelines 07/2020*, cit., pp. 32-33.
[35] *Ivi*, pp. 3 and 24-25.

obligations as a processor. This makes it the best solution for companies without sufficient experience or resources for the processing of personal data.

When Guider is used in bigger companies or companies that have access to special categories of data[36], they might prefer to process personal data entirely by themselves, without keeping Guider on board as a processor. This is how personal data is currently being processed by the University of Bergen (including for the Faculty of Law). The Rector[37] is designated the role of controller and delegates the processing to the line of managers.[38] The processing of personal data concerning employees is delegated to the HR department and the personal data of students is delegated to the Director of the Department for Student Administrative Department. If the controller wants to employ a processor it has to do a risk-assessment whether the processor is capable of giving sufficient guarantees to comply with the GDPR and with regards to data security.

Due to these obligations a lot of good arguments can be made for processing all this potentially sensitive data within the company, without the need for Guider to be in the chain of processing. The companies that want to use Guider might simply come to the conclusion that their own department is better suited as the processor than Guider itself is. They would evidently still be customers of the services of Guider but all the personal data would be handled in-house. To do this they could create a separate legal identity that acts as a processor, or simply delegate the processing to one of their departments, like UIB has done. For the University processing the personal data that is needed for the purpose by these departments would mean that they have to make minimum changes to their operational level. For Guider this would also have advantages in terms of obligations, liability and potential fines. It is important to note that for the specific purpose of the storage for improvement Guider would be considered the controller, because it is the one deciding on the means and purpose for this specific processing. It is important that the role and responsibilities of Guider for this purpose are also specifically delineated within the contract.

The controller has an obligation to provide certain information to the data subject at the time when the data is being obtained.[39] We would advise the controller to make this information available before this moment, on their website or on Guider's website. It is important that this website contains detailed information on what to do when something goes wrong. There would be a contact point[40] that data

---

[36] As an example of the processing of sensitive data we thought about Guider being used by a hospital. Guider could lead patients directly to their doctor's appointment. To do this, Guider would need access to their medical records. This is data concerning health in the sense of GDPR Article 14 (15), a special category of data under GDPR Article 9 (1).

[37] Dag Rune Olsen is the Rector of UIB.

[38] University of Bergen (2020), *Privacy policy for the University of Bergen*, https://www.uib.no/en/personaldata/130126/privacy-policy-university-bergen (last accessed 19/05/2021).

[39] GDPR Article 13 (1).

[40] For the Faculty of Law this would be the privacy ombudsman of UIB, namely Janecke Helene Veim.

subjects can reach out to regarding information or the enforcement of their rights. Additionally the contact details of the data protection authority[41] has to be provided when customers wish to not contact the designated contact point but directly file a complaint to the competent data authorities[42]. Some important obligatory information are the identity and contact details of the processor and the purposes of the processing for which the personal data are intended, as well as the legal basis for the processing. As explained above this will vary according to the functions of Guider and the specific needs of the customer. Depending on which legal grounds the processing is based the controller has to provide a different kind of information. We have identified three different legal bases for the lawful processing by Guider: necessity for the performance of a contract, legitimate interest and consent. It is important that the controller provides information regarding which legal basis is used for which processing. Additionally when the processing is based on legitimate interest the grounds for the legitimate interest have to be provided and the data subject has to be informed about the right to object to the processing of its personal data.[43] When the legal basis for processing is consent the data subject has to be made aware of the existence of the right to withdraw consent at any time.[44]

5. Guider's functions: how can Guider help the user?

In the following part of the report, Guider different functions will be assessed. Indeed, in accordance with the layered approach guiding the report, Guider may have different functions depending on how sophisticated the customer wants its performance to be. Consequently, the different functions entail a different quality and quantity of personal data being processed.

5.1 Guider's basic function: maps with rooms name or number

- Purpose: Guide the user to their wanted destination.
- Function: Guider leads users to the wanted destination based on room number.
- Personal data: none
- Legal basis: Since there is no processing of personal data, GDPR does not apply and there is no need for a legal basis to perform this function.
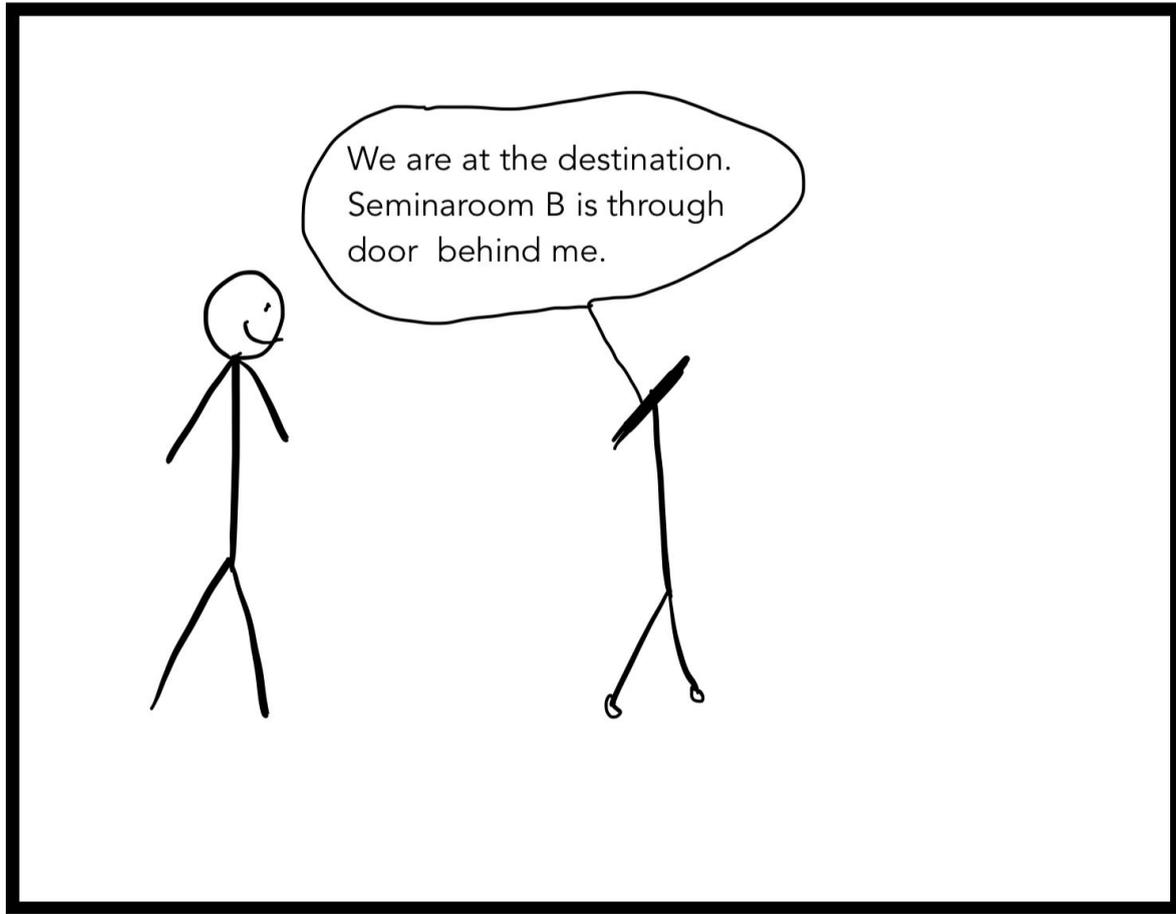- Example:

---

[41] For our project this is the Norwegian Data Protection Authority (Datatilsynet).
[42] GDPR Article 13 (2) (d).
[43] GDPR Article 21.
[44] GDPR Article 13 (2) (c).

5.2 Guider's additional functions

In addition to the aforementioned basic function of Guider, the customer might also decide to implement additional functions to be performed by Guider. However, differently from the previous one, these functions all entail collection and processing of personal data and thus, the GDPR is applicable in the following scenarios.

5.2.1 Map with names

- Purpose: easier for the user to ask for direction.
- Function: Guider leads users to the wanted destination based on the name of the person working in the office.

- Example:
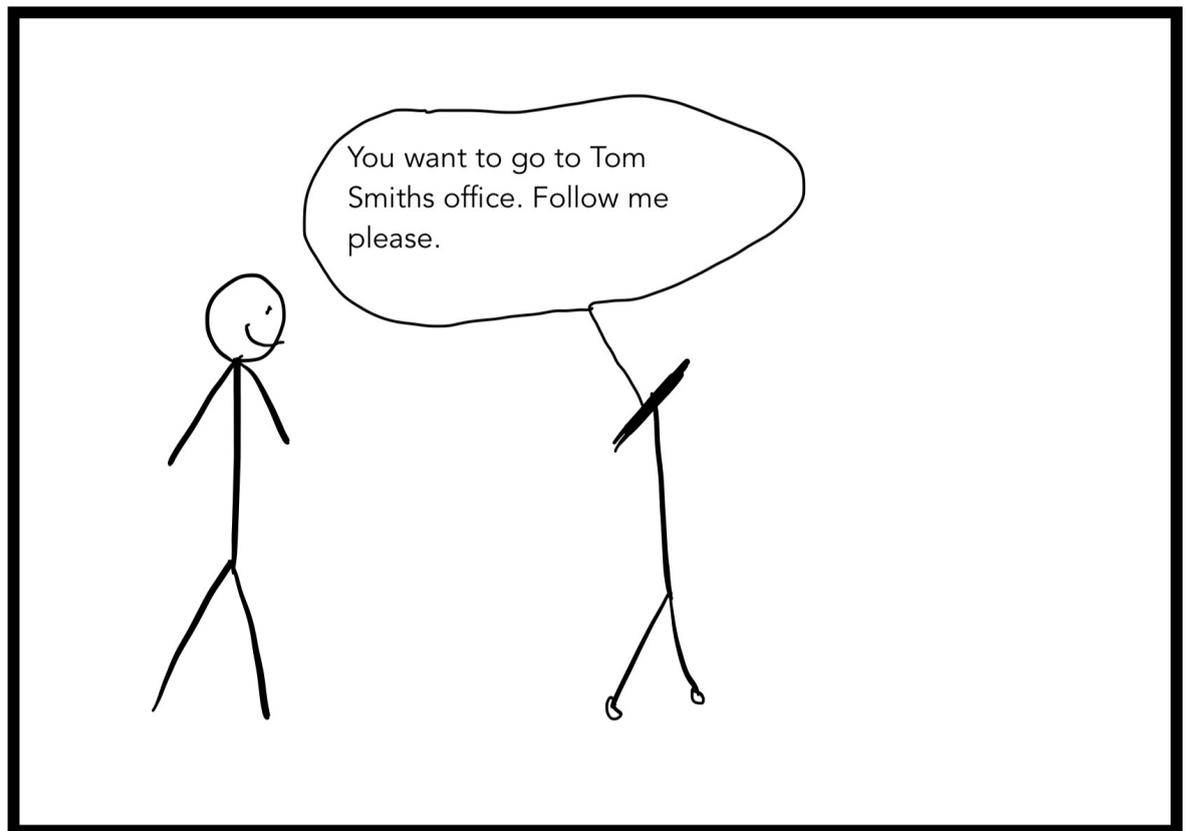
- Personal data: names and office location data.
- Processing: storage of or access to the data[45], organisation of the data for Guider to use it, retrieval to use the information to move to the right location.
- Storage time: as long as Guider is used to lead users to locations by using the name of the person.

Legal basis:

To provide this function, Guider will process personal data from the people working in the different spaces, in our case from employees in offices in the Faculty of Law. As a part of the employment contract with its staff, the University provides daily working space to keep the normal running of academic and institutional procedures. Students and visitors can have a reasonable expectation to have access to the offices of the Faculty and be in contact with its staff members with relative ease. For this purpose, Guider will need to have access to maps of the rooms with the names of the people who

---

[45] This will depend on how this information is stored. If it is stored in a way where Guider can use the information only with access this will be used because the information is then more likely to keep being accurate in accordance with GDPR Article 5 (d).

work in the offices. Therefore the legal basis for the processing of the room numbers with names follows from the performance of the employment contract between the University and its employees.[46]

5.2.2 Schedule of the rooms

- Purpose: easier to find events happening in the Faculty.
- Function: Guider leads users to the wanted destination based on schedules of rooms.
- Example:
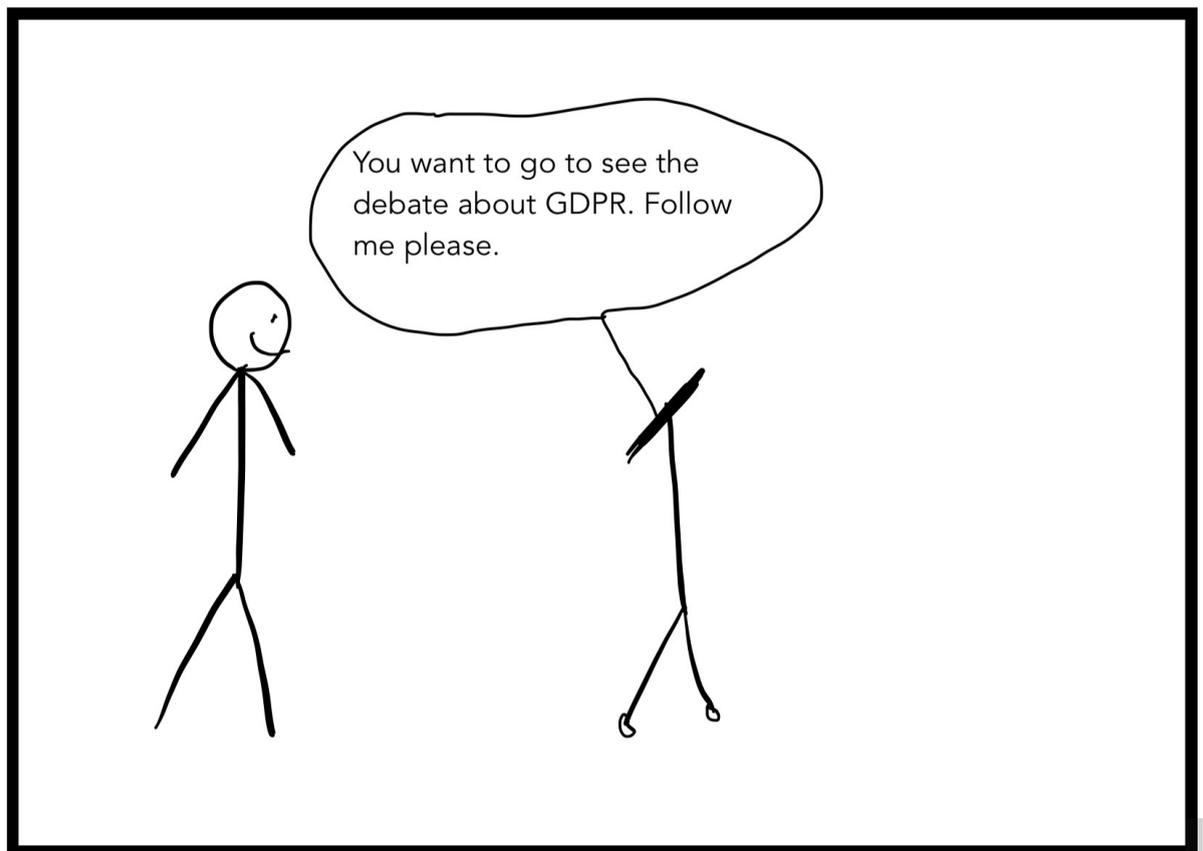
- Personal data: possible names in titles of events.
- Processing: storage of or access to the data[47], organisation of the data for Guider to use it, retrieval to use the information to move to the right location.
- Storage time: one month in advance and one week after the event happened. This enables Guider to give information about rescheduled events and past events while keeping data for no longer than the purpose requires[48].

Legal basis:

---

[46] GDPR Article 6 (1) (b).
[47] See footnote 45.
[48] GDPR Article 5 (1) (b).

The legal basis for processing the data of lecturers' names linked to schedules of rooms works similarly as for the employee using the office, namely pursuant to the employment contract under GDPR Article 6 (1) (b). The controller should process the data only when it's necessary, and erase, delete or update the schedule at a regular and reasonable frequency, not only in compliance with the obligation for personal data protection but also to provide precise information for Guider to offer better service.

5.2.3 Schedule of people

- Purpose: easier to find out if someone is busy or to find the location of your appointment.
- Function: Guider gives the user information regarding the schedule of a person.
- Example:
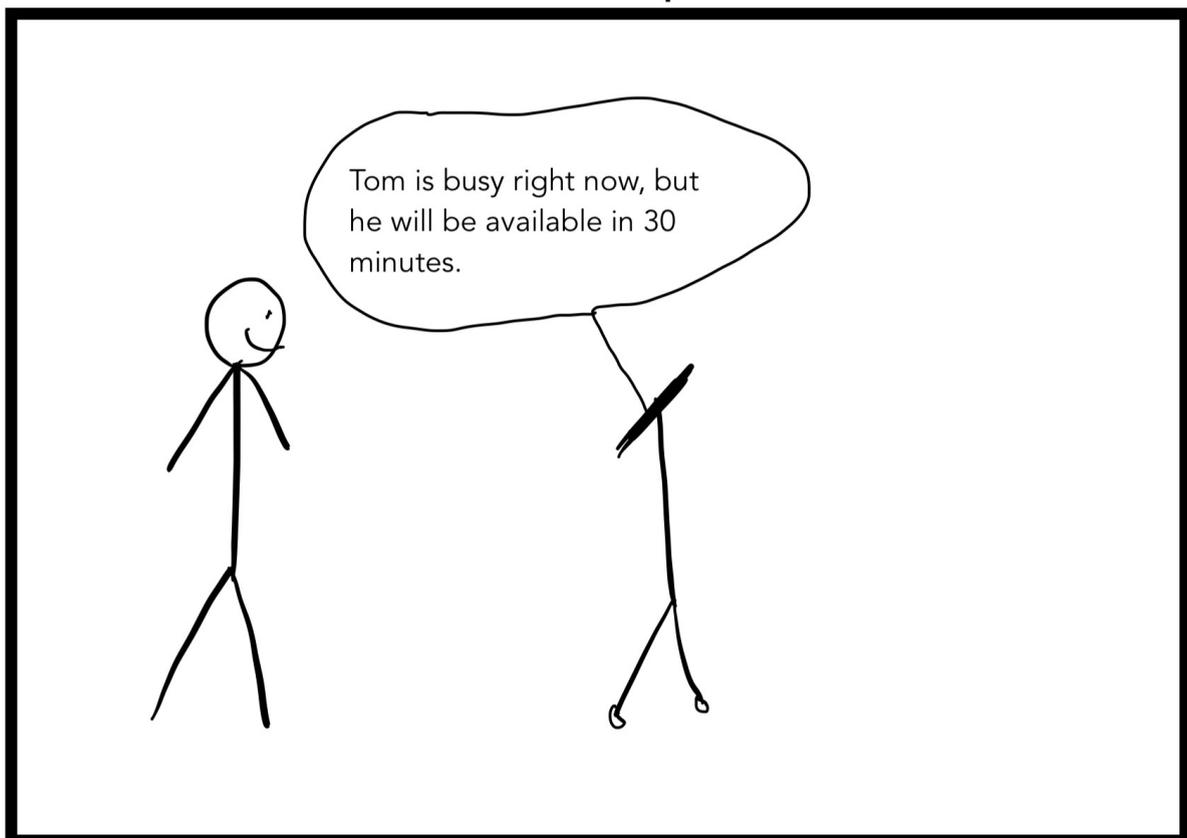
- Personal data: names combined with schedule, schedule might involve other names and information the data subject wants to show regarding his schedules.

- Processing: storage of or access to the data[49], organisation of the data for Guider to use it, disclosure of the information to the user.

- Storage time: one week ahead and behind. This enables Guider to give information about people's schedules while keeping data for no longer than the purpose requires[50].

Legal basis:

For example, Guider can directly remind the user if the professor to be visited has a schedule conflict now and suggest the visitor to come later, or help the student who wants to join a discussion held by a specific professor but has no idea which seminar room such a discussion is in. To realize this function, personal data of the names and personal schedules have to be provided.

Similar to the function of schedule of the rooms, processing of such personal data basis its lawfulness on the necessary of performance of the contract pursuant to GDPR Article 6 (1) (b) between the controller and data subjects, including both the employees using the offices and students or staffs who use the room-booking service, etc. Differently, instead of presenting the schedule information of a specific room, the whole schedules of a specific person will all be stored, retrieved, and disclosed in realization of this function, sometimes it may even imply the schedule of other names and personal schedules. So it's significant to make sure that the data subjects have initiated the contract.[51] Furthermore, the data subjects may put more sensitive information in the schedule, which concerns special categories of personal data. For example, the staff may put his or her personal daily appointments with the dentist inside the working calendar, which concerns health information and may be collected by Guider. In this circumstance, consent and explicit consent pursuant to Article 6 (1) (a) and 9 (2) (a) apply.[52]

6. How Guider can move and communicate

Tablet

Guider can use its tablet to give the user information, enable the user to become a regular user and show the person where to go.

Motion camera

The most simple way for Guider to navigate would be by using a camera. The customer that will use Guider can upload a virtual map, where specific rooms would be indicated and a number of landmarks

[49] *Ibidem*.
[50] GDPR Article 5 (1) (b).
[51] GDPR Recital 44.
[52] See how this may be done in practice in part 9.3 of this report.

that Guider could avoid. Guider would then use its built-in camera to avoid moving things, such as people.[53] In light of the principle of data minimisation and data protection by design we would advise Guider to include a filter on its cameras.[54] This would be done in order to prevent Guider from collecting data, in the form of video, that could be used to identify a person.

Guiders voice

- Purpose: Guider to be more user-friendly by communicating more actively with the users.
- Function: for being able to answer the user, Guider needs to have its own voice. This will probably be a voice that is bought like Siri or Alexa.
- Personal data: voice.
- Processing: storage of or access to the data[55], disclosure to speak to the user.
- Storage time: as long as Guider is put into use.

Legal basis:

To provide a user-friendly service, Guider should be able to "speak" by pre-installing a voice to "communicate" with the users. There are two possible sources from where the voice is made. On the one hand, the voice of Guider can be an electronic sound synthesized by artificial technology, which does not concern any personal data. On the other hand, Guider may have a more human-like voice by recording specific sentences spoken by someone in advance and playing the recordings in different scenarios. By specific technology, the voice which still allows "the unique identification of that natural person"[56] is recorded, stored, used[57] in support of the normal operation of Guider, resulting in the processing of biometric data. However, since the voice is used to enable Guider to "speak" instead of "uniquely identifying a natural person"[58], GDPR Article 9 does not apply. Instead, the controller should make a contract with the voice provider to get authorization of using the voice data, gaining lawfulness pursuant to GDPR Article 6 (1) (b).

7. Possible interactions data subjects can have with Guider

7.1 Obligatory for the customer and user

---

[53] This idea was inspired by the technology behind Roomba, for further information see: https://homesupport.irobot.com/app/answers/detail/a_id/19541/~/how-does-my-robot-navigate%3F#:~:text=Rob ots%20that%20use%20iAdapt%C2%AE%201.0%20Navigation%20Technology%20utilize%20a,then%20move s%20in%20another%20direction (last accessed 19/05/2021).
[54] See part 7.2.1 of this report.
[55] In this case the benefit of access rather than storage is improvements in the product and not accuracy.
[56] GDPR Article 4 (14).
[57] Such an operation on personal data is a kind of processing. See GDPR Article 4 (2).
[58] GDPR Article 9 (1).

Use of tablet

- Purpose: for Guider to operate without any processing of personal data.
- Function: to ask Guider for directions by using a tablet without the processing of personal data if the user does not want to say out loud where they want to go or if Guider has misunderstood where the user wants to go.
- Personal data: none.

7.2 Voluntary

7.2.1 Voice command

- Purpose: easier for the user to communicate with Guider.
- Function: the user can ask Guider for directions in an easier way by speaking to it.
- Example:

IMAGE

- Personal data: voice.
- Processing[59]: recording of the voice of the user with a filter to avoid the recording of surrounding voices, analysis to check if it is a regular user[60] and to understand the demand of the user.
- Storage time: storage throughout the interaction between Guider and the user[61].

Legal basis:

First of all, to realize this function, the processing of voice is only for getting the command information without personal identification. In addition, there is a technologically possible way for Guider to extract pure valid textual information. By extraction, the voice data lose the possibility to "allow or confirm the unique identification"[62] as "biometric data", released from the special categories of personal data. What's more, since such extraction of voice has no "purpose of uniquely identifying a natural person"[63], GDPR Article 9 does not apply.[64]

Practically, if Guider is supposed to be user-friendly, it is easier to just say "Hi, Guider" instead of having to read the terms and give consent first, the legal basis for processing the voice of the users

---

[59] Storage of the recordings are assessed separately in part 8 of this report.
[60] The assessment of the recognition is in part 7.2.3 of this report.
[61] See part 8 of this report for information on further storage.
[62] GDPR Article 4 (14).
[63] GDPR Article 9 (1).
[64] Similar logic referring to GDPR Recital 51.

talking to Guider can not be consent. Additionally, speaking to Guider is much more convenient for people who cannot reach up to Guider, for example, the disabled sitting in a wheelchair or small children, the criteria for legitimate interest under GDPR Article 6 (1) (f) are met. This article can be used even though the university is a "public authority" and thus cannot use GDPR Article 6 (1) (f) for processing "in the performance of their task". Guiding visitors is not a 'task' they have as public authority and thus the exception does not apply.[65]

Different from the concept of purpose, which is "the specific reason why the data are processed", an interest is "the broader stake that a controller may have in the processing, or the benefit that the controller derives, or that society might derive, from the processing".[66] As long as it is "acceptable under the law", the Faculty can demonstrate the interest of being user-friendly as legitimate.[67] Besides, such interest must be real and present, corresponding "with current activities or benefits that are expected in the very near future".[68] Firstly, as a public university in the second largest city of Norway, the University of Bergen has campuses all over the city where most attractions are within walking distance.[69] There are also residential areas nearby, leading the Faculty to a popular destination for both travelers and citizens to visit, walk, exercise, etc. Besides, the academic and administrative staff in different ages lead to the need for elder and younger friendly infrastructure in the Faculty. In this case, it's reasonable to pursue the legitimate interest of providing user-friendly service for all visitors through Guider. Secondly, with technological processing, the extraction of voice into simply textual information does not override "the interests or fundamental rights and freedoms of the data subject"[70]. Thirdly, "taking into consideration the reasonable expectations of data subjects based on their relationship with the controller"[71], the elderly and people with disabilities might want to go straight to the destination without detours while the staff hopes their visiting children find parents as soon and safely as possible, which all provides strong arguments for such legitimate interest of the Faculty.

In addition, when assessing whether there is a legitimate interest it is relevant to note that it is voluntary for the user to use voice command. Based on GDPR Article 6 (1) (f), the function of voice

---

[65] See GDPR Recital 47: "Given that it is for the legislator to provide by law for the legal basis for public authorities to process personal data, that legal basis should not apply to the processing by public authorities in the performance of their tasks". This limits the scope of the 'task' of public authorities into an area where the legislator provides law and the public authorities have to follow. If there is no such existing law regulating a task for the authority the public authority can apply GDPR Article 6 (1) (f) where necessary.
[66] Article 29 Data Protection Working Party, *Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller Under Article 7 of Directive 95/46/EC*, 9 April 2014, p. 24, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf (last accessed 19/05/2021).
[67] See Article 29 Data Protection Working Party, *Opinion 03/2013 on Purpose Limitation*, 2 April 2013, p. 19, https://ec.europa.eu/justice/article-29/ (last accessed 19/05/2021).
[68] Article 29 Data Protection Working Party, *Opinion 06/2014*, cit., p. 24.
[69] University of Bergen (2016), *History and location*, https://www.uib.no/en/jur/22981/history-and-location (last accessed 19/05/2021).
[70] GDPR Article 6 (1) (f).
[71] GDPR Recital 47.

command gains its lawfulness of the processing. But as the controller, the Faculty is still obligated to keep an eye on whether the original voice data is erased timely.

7.2.2 Microphone on

In order to recognize the signal of "Hi, Guider", there are two possible ways. One is that the users have to turn on the microphone and activate the voice command function by taping Guider before saying something. By doing this, Guider avoids automatically collecting the voices nearby all the time and processes less data. However, it is also less accessible to wheelchair users or small children.

Another solution is keeping Guider processing all the voice in close proximity so that every potential signal of "Hi, Guider" can be recognized immediately, making it react more intelligently and efficiently. The following is the assessment for the second solution:

- Purpose: Guider to be more user friendly and available to more people.
- Function: To understand when someone is talking to Guider.
- Personal data: voices nearby.
- Processing: analysis of the surrounding voices with a filter in order to listen to the word "Guider", erasure of the recording.
- Storage time: no storage of voices.

Legal basis:

Since the processing of the surrounding voices will go through the voice extraction and purification as it is for the voice command, there is no extra type except the ordinary personal data under processing. However, with the microphone on all the time, the data subjects are not only the users, but also the surrounding individuals who do not have an interest in Guider processing their voice. Taking the balance between legitimate interest and the impact on the data subjects into consideration, it's reasonable that Guider puts the interest of providing the users with voice command service as required over the processing of surrounding voices who have no interest in using Guider. Besides, the recording will be deleted right after Guider has analysed and concluded that the individual did not say "Guider". Thus there will be no storage of the recording and the processing is still within the legal basis of the legitimate interest pursuant to GDPR Article 6 (1) (f) .

7.2.3 The personalised experience

- Purpose: to provide users with a more personalised experience.
- Function: Guider can recognise the use, access to users' schedules and know their preferences based on previous interactions.

- Example:
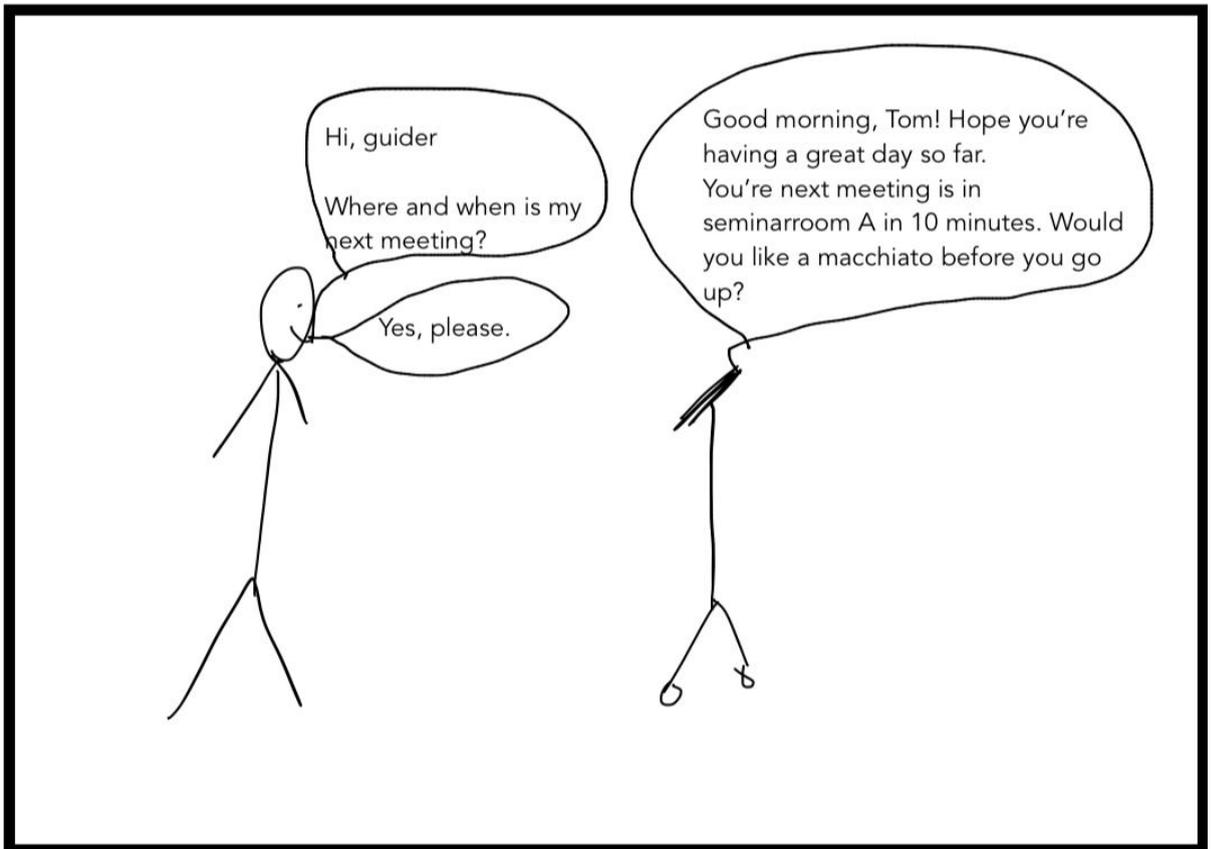
- Personal data: voice in connection with names, schedules and preferences.
- Processing: recording of the user's voice with a filter to avoid recording surrounding voices, analysis to recognise regular users, their demands and previous interactions to personalise the communication with users. storage to remember the interactions of the user with Guider,
- Storage time: As long as there is consent/contract.

Legal basis:

The users may want Guider to provide more personalised service,[72] including voice recognition, schedule reminding, hobby recommendation, etc.

On the one hand, since the purpose of the personalised experience is to connect certain names with voices, schedules, and even preferences of unique people, Guider will process special categories of personal data pursuant to GDPR Article 9 (1). Furthermore, Guider needs to analyse on "personal data resulting from specific technical processing"[73] relating to vocal characteristics of natural people, resulting in the processing of biometric data pursuant to GDPR Article 4 (14). Besides, face recognition[74] works with the same logic because they are both essentially used as biometric data to

---

[72] Johansen, S. L., *Guider - a robotic guider*, cit., p.6:
[73] GDPR Article 4 (14).
[74] Johansen, S. L., *Guider - a robotic guider*, cit., p.6.

uniquely identify the user. In fact, either voices or faces provide enough data for Guider to process and personalise service. Given that the voice data has been collected under the voice command function, according to the principle of data minimization, using voice recognition instead of facial one asks for less personal data with more functional possibilities. And it's also necessary if Guider wants to be more friendly to recognize the regular users by voice than asking the users to write down their names.[75] Consequently, the processing should be based on both GDPR Article 6 and 9, precisely explicit consent of GDPR Article 9 (2) (a).

For the legal basis of explicit consent, the elements of specification pursuant to GDPR Article 4 (11) should be underlined. Due to the different purposes of the processing, the explicit consent should be given technically by the data subjects to maintain the granularity of consent[76]. By storing and analyzing personalised experience, Guider can "evaluate certain personal aspects relating to a natural person, in particular, to analyze or predict aspects concerning that person's performance"[77] in the Faculty, resulting in the profiling of personal data. It's the controller's responsibility to demonstrate that the data subjects have a clear understanding of the profiling and give explicit consent. Besides, it should also be taken into consideration that when collecting a user's voice, the recording might contain others' voice from background, which is not necessary for the voice recognition of such a user. Therefore, Guider should also "consider technologies filtering the unnecessary data and ensuring that only the user's voice is recorded."[78]

On the other hand, to "act as an interface between users and their computing devices", Guider is providing a virtual voice assistant (VVA) service at the requirement of the users, which accesses it "to a huge amount of personal data including all users' commands and answers."[79] In this case, beside the explicit consent,[80] an extra legal basis should be provided for the purpose of storage for personalised experience pursuant to GDPR Article 6. Since the user takes the decision to use the voice assistant service with initiative, Guider has to ask the user to "register an account to activate the VVA"[81], resulting in a contractual relationship between the registered user and the controller, which can be the legal basis for the purpose of storage for personalised experience pursuant to GDPR Article 6 (1) (b).

---

[75] *Ivi*, p. 6: as it is mentioned in the report, "if Guider sees a user regularly returning, Guider would address the person by name or ask for the name if it is unknown".
[76] When the processing has multiple purposes, consent should be given for all of them. See GDPR Recital 32.
[77] GDPR Article 4 (4).
[78] European Data Protection Board, *Guidelines 02/2021 on Virtual Voice Assistants. Version 1.0*, 9 March 2021, p.3, https://edpb.europa.eu/system/files/ (last accessed 19/05/2021).
[79] *Ivi*, p. 2.
[80] *Ivi*, p. 22.
[81] Ivi, p. 21.

Besides, since "the voice data is processed in order to execute the user's requests"[82], the controller is exempted from the requirement of prior consent.[83]

Furthermore, the assessment becomes more complicated when there are children using Guider with personalised service. Besides GDPR Article 6 (1) (b) and 9 (2) (a), if a child says "Hi, Guider" to activate the voice recognition function, GDPR Article 8 applies.

The service provided by Guider is a kind of "information society service", which is "normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services".[84] Firstly, though the child does not pay Guider for such service, Guider itself has received the payment when originally bought by the Faculty from the inventor or producer. Secondly, Guider provided the at-a-distance service "without the parties being simultaneously present".[85] Thirdly, the voice data of children will be "sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data"[86], with Guider itself provided as a supporter to exercise the electronic means. Fourthly, it's the child users who raise the request with initiative.[87] Consequently, when the data subjects are children, the processing of voice data with the purpose of identification should be pursuant to GDPR Article 8, and such consents from both children and parents should also meet the requirements of both Article 6 (1) (a) and Article 9 (2) (a) of GDPR.

Article 8 (1) allows for Member States to provide a lower age of consent to processing of personal data for information society services. In our project we have placed Guider in the Faculty of Law, so the Norwegian law on data protection applies. Norway has made use of this possibility and put the valid age of consent to 13.[88] To offer information society services directly to a child under 13 years old, the processing shall be lawful "only if and to the extent that consent is given or authorized by the holder of parental responsibility"[89].

---

[82] *Ibidem*.
[83] Directive (EU) 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ 2002/L 201/37, Article 5(3): "[relative storage or access] is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information […] This shall not prevent any technical storage or access […] as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user".
[84] Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (codification), OJ 2015/L 241/1, Article 1 (1) (b).
[85] Directive 2015/1535 Article 1 (1) (b) (i).
[86] Directive 2015/1535 Article 1 (1) (b) (ii).
[87] Directive 2015/1535 Article 1(1) (b) (iii).
[88] The Personal Data Act (Norway, Act of 15 June 2018 on the processing of personal data) (Personopplysnigsloven), § 5.
[89] GDPR Article 8 (1).

On the one hand, if the child becomes a regular user of Guider who activates voice recognition and gets personalised experience, there must be somewhere the child frequently visits in the Faculty building. Under these circumstances, it's easy for the Faculty to get in touch with parents to get consent or authorization. As the controller, the Faculty shall also "make reasonable efforts to verify" that the consents are given or authorized by parental responsibility holders by "taking into consideration available technology.[90] However, before the consents are given by the parents, Guider should strictly limit its function within impersonalised service since no legal basis for the processing of special categories of personal data of the children applies, which also encourages Guider to confirm whether the person visited by the child has parental responsibility when it provides common service for a child at the first time so that the explicit consents from parents can be gained as soon as possible to activate the personalised service for the children.

On the other hand, if the child is not a regular user it's difficult for the Faculty to get consent from the holders of parental responsibility. Without voice recognition and personalised experiences, Guider can still provide basic guiding service for the child with all the functions and legal basis mentioned above, resulting in no need for further consent from parents. In this circumstance, Guider should only provide child users with common service without personalisation to keep the processing legal.

8. Storage for self-improvement

- Purpose: Guider becomes better at understanding the user and finding the most efficient route
- Function: improve Guider through technology for example machine learning[91]
- Example: Guider will learn different pronunciations for Seminarroom B.
- Personal data: voice recording combined with decoding of the recording and the route taken
- Processing: storage for analysis, analysis through machine learning for improvement
- Storage time: Until the purpose has been achieved[92]

Legal basis:

Though the storage for improvement helps Guider to provide better personalised experience service, "the training of the machine learning model and human review and labelling of voice transcriptions"[93] aim at more than the purpose of storage for personalised experience,[94] which come

---

[90] GDPR Article 8 (2).

[91] There are different ways of achieving this and it is not specified in Johansen, S. L., Guider - a robotic guider, cit.

[92] How long this is will depend on what technology is used and how. When this is decided the creator and controller should establish specific "time limits [...] for erasure of for periodic review" in accordance with GDPR recital 39. This is also important because of the principle of purpose limitation in GDPR Article 5 (1) (b).

[93] European Data Protection Board, *Guidelines 02/2021 on Virtual Voice Assistants*, cit., p. 20.

[94] *Ivi*, p. 21.

out as not "necessary for the performance of a contract".[95] Therefore, the processing of personal data for self-improvement requires another legal basis.

For the regular users, the personal data has been processed for the purpose of providing personalised experience, while registering an account leads to a contractual relationship between the data subject and the controller.[96] Hence the storage for self-improvement should be regarded as a subsequent processing with further purpose following the initial one of personalised experience pursuant to Article 6 (4). Since explicit consent has been given in the former step, "no legal basis separate from that which allowed the collection of the personal data is required."[97] Besides, with respect to the granularity rule, the controller should also make sure that the data subject has a distinguishable understanding that the purpose of such storage is specifically for the improvement of machine learning.

For the occasional users, there is no former processing with the purpose of providing personalised experience. The storage itself is an initial process with the specific purpose of machine learning improvement, which needs a respective legal basis. To keep in contact with the data subjects, Guider may still store at least the email addresses or phone numbers, leading to the potential of identification. With technical measures of pseudonymisation, Guider can process personal data in "a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information"[98], in the meantime it would keep the additional information separate. By undergoing pseudonymisation, voice recordings could still "be attributed to a natural person by the use of additional information"[99] which is "personal data", more precisely, biometric data. But the absence of the purpose of identification releases it from GDPR Article 9. In the end, the legitimate interest under Article 6 (1) (f) applies.

Unlike it is for the purpose of voice command or microphone on, the nature of legitimate interest varies. Besides producing user-friendly service while taking the social status and public prestige of the Faculty into consideration, the legitimate interest does not always need to be "compelling and beneficial to society at large", instead, it may also be "less pressing for society as a whole, or at any rate, the impact of their pursuit on society may be more mixed or controversial".[100] In this case, Guider stores personal data only for the improvement of machine learning, which benefits itself. As a robotic helper for human beings, Guider reasonably serves the legitimate interest of being able to

---

[95] Ivi, p. 22.
[96] GDPR Article 6 (4) (a) and (b).
[97] GDPR Recital 50.
[98] GDPR Article 4 (5).
[99] GDPR Recital 26.
[100] Article 29 Data Protection Working Party, *Opinion 06/2014*, cit., p. 24.

distinguish different pronunciations or other references among its users.[101] In the meantime, the controller should always keep in mind that "the existence of a legitimate interest would need careful assessment"[102].

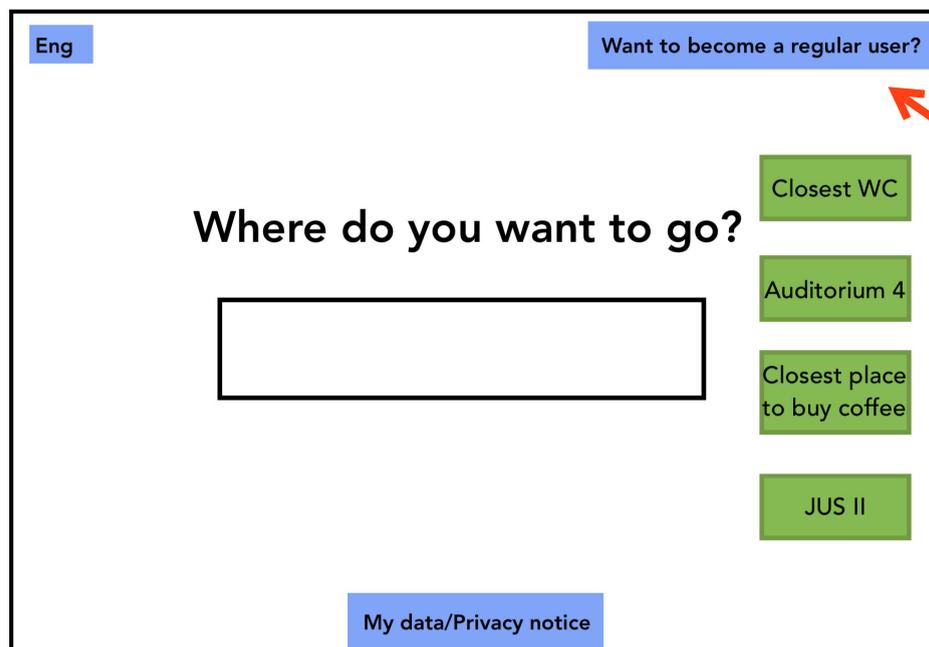# 9. Our suggestion for applying GDPR for the user in practice

There are several ways of applying GDPR for the user in practice. In this part we have made one suggestion to illustrate how this can be done.

9.1 The regular user process

The steps for the regular user:

1. Register on Guider
2. Confirmation email
3. If the user does not use Guider for 6 months they will get the reminder email
4. Ways of withdrawing/leaving the contract:
   a. Link on email
   b. On Guider
   c. On website

The consent would be given to Guider like this:

---

[101] *Ivi*, p. 25: The example given by the Working Party has similar logic that "controllers may have a legitimate interest in getting to know their customers' preferences so as to enable them to better personalise their offers, and ultimately, offer products and services that better meet the needs and desires of the customers".
[102] GDPR Recital 47.

Do you want to become a regular user?

If you become a regular user you will get a personalised experience. I will recognise you and for example remember what you usually need help with and your coffee preference.

To be able to perform these functions I need to collect, analyse and store information about you. The information will be our interactions from beginning to end including what you said and where we went. This includes analysing and storing your voice to be able to recognise you. Identifying you by your voice requires me to get your explicit consent as it is a special category of data according to GDPR.

Your consent can be withdrawn at any time. If you withdraw the information about you will be pseudonomised. This will happen by your name being deleted and your personal data no longer being grouped together. The information will still be stored for improvement. Click on this link for more information about storage for improvement. Click on this link to withdraw your consent.
Here are the terms & conditions.

Do you consent?*
☐ Yes   ☐ No
What would you like me to call you?   [   ]
Your email*:   [   ]

Confirm that you are above 13 years old: ☐
In addition, I can help you with your daily appointments if you give me access to your schedule. To do this login through Feide here.

This page will appear if a regular user clicks to withdraw their consent.

Your consent to Guider has been withdrawed.

In five minutes your information will be pseudonomised. This will happen by your name being deleted and your personal data no longer being grouped together. The information will still be stored for improvement. Click on this link for more information about storage for improvement and your rights as a data subject.

If you clicked on the link by mistake and do not wish to withdraw your consent click here.

9.2 Consent from employees for their schedule

As written in part 5.2.3 staff may put his or her personal daily appointments which may include health information and thus consent and explicit consent pursuant to GDPR Article 6 (1) (a) and 9 (2) (a) applies.

An employee adding their personal appointments to their work calendar is voluntary since there is no requirement for the employees to do so. The faculty can give their employees the option to make their schedule available online to the public. This serves the purpose of users being able to know if a person is available or not and to find the location of events based on the name of a person.

Personal view — Week 15

	Monday	Tuesday	Wednesday	Thursday	Friday
07.00					
08.00					
09.00	Doctors appointment	GDPR conference Online			Busy writing
10.00					
11.00					
12.00	GDPR lecture Auditorium 2			GDPR lecture Auditorium 2	
13.00					
14.00					
15.00					
16.00			GDPR debate Straffbar		
17.00					
18.00					

Public view — Week 15

	Monday	Tuesday	Wednesday	Thursday	Friday
07.00					
08.00					
09.00	Busy	Busy			Busy
10.00					
11.00					
12.00	GDPR lecture Auditorium 2			GDPR lecture Auditorium 2	
13.00					
14.00					
15.00					
16.00			GDPR debate Straffbar		
17.00					
18.00					

9.3 The information about the users data and rights

This information will be available on the website and on Guiders tablet. It will be linked in the emails sent to the regular user.

Your data and your rights

Your rights

Regular user - you can withdraw your consent here

Concerning your data you have the right to:

- Access
- Rectification
- Erasure
- Restriction of processing
- Object to processing
- Data portability

To find out more about your rights and how you can exercise them click on the links above and. You will be directed to the Norwegian Data Protection Authority's page about the rights.

How to exercise your rights

You can exercise your rights by contacting

1. The privacy ombudsman of UiB is currently Janecke Helen Veim

   Email: personvernombud@UiB.no

2. The Norwegian Data Protection Authority (Datatilsynet)

   Send a written inquiry to:

   Datatilsynet

   PO Box 458 Sentrum

   0105 Oslo

   Norway

Information concerning Guiders processing of personal data

Purpose	Type of processing	Data subject	Personal data	Legal basis	Storage time
Easier for the user to ask for direction.	storage of or access to the data, organisation of the data for Guider to use it, retrieval to use the information to	Employee	names and office location data.	Contract	as long as Guider is used to lead users to locations by using the name of the person.

	move to the right location.				
easier to find events happening in the Faculty.	storage of or access to the data, organisation of the data for Guider to use it, retrieval to use the information to move to the right location.	employee	possible names in titles of events.	Contract	one month in advance and one week after the event happened.
easier to find out if someone is busy or to find the location of your appointment.	storage of or access to the data, organisation of the data for Guider to use it, disclosure of the information to the user.	employee	names combined with schedule, schedule might involve other names and information the data subject wants to show regarding his schedules.	Contract, consent and explicit consent	one week ahead and behind.
Guider to be more user-friendly by communicating more actively with the users.	storage of or access to the data, disclosure to speak to the user.	Individual who has sold voice recordings for resale	voice	contract	as long as Guider is put into use.
easier for the user to communicate with Guider.	recording of the voice of the user with a filter to avoid the recording of surrounding voices, analysis to check if it is a regular user and to understand the demand of the user.	user	voice	legitimate interest	storage throughout the interaction between Guider and the user.

Guider to be more user friendly and available to more people.	analysis of the surrounding voices with a filter in order to listen to the word "Guider", erasure of the recording.	Individuals nearby	voices	legitimate interest	no storage of voices.
to provide users with a more personalised experience.	recording of the user's voice with a filter to avoid recording surrounding voices, analysis to recognise regular users, their demands and previous interactions to personalise the communicatio n with users, storage to remember the interactions of the user with Guider	regular user	voice in connection with names, schedules and preferences.	contract and explicit consent	As long as there is consent and contract.

10. Risk assessment

According to the principle of accountability, the controller is responsible to demonstrate compliance.[103] To that end, under GDPR Article 24, the controller shall implement "appropriate technical and organisational measures to ensure and demonstrate that the processing of personal data he is carrying out is compliant with GDPR".[104] Particularly, the controller, in fulfilling this obligation, must take into account the risks that the processing operations might have on the rights and freedoms of those whose data are being processed ("varying likelihood and severity for the rights and freedoms of natural persons"[105]).[106] In that respect, the notion of rights and freedoms of the data subject mainly refers to the right to protection of personal data, the right to respect for private and family life, the freedom of expression, the freedom of thought, conscience and religion, the freedom of movement and the prohibition of discrimination.[107] In addition, the risks connected to such rights and freedom can range from personal data being stolen, being used for unknown purposes or inadvertently released.[108]

Therefore, the controller has to carry out - before and after their implementation - a risk assessment of its processing operations in order to adopt the necessary measures. Indeed, as stated in GDPR Article 25, the controller must implement:

a. measures "designed to implement data-protection principles [...] in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of [the] Regulation and protect the rights of data subjects"[109] ('data protection by design'); and

b. "measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed"[110] ('data protection by default').

In addition, the controller and the processor must also implement appropriate measures to ensure a level of security appropriate to the risk envisaged by the various types of processing involved, such as the pseudonymisation and encryption of personal data.[111] Particular attention when assessing the appropriate level of security must be devoted to risks such as the "accidental or unlawful destruction,

---

[103] GDPR Article 5 (2).
[104] GDPR Article 24 (1).
[105] *Ibidem*.
[106] European Data Protection Supervisor, *Accountability on the ground Part I: Records, Registers and when to do Data Protection Impact Assessments*, February 2018, p. 6, https://edps.europa.eu/sites/default/files/publication/19-07-17_accountability_on_the_ground_part_i_en.pdf (last accessed 19/05/2021).
[107] Article 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA)*, https://ec.europa.eu/newsroom/article29/items/611236 (last accessed 19/05/2021).
[108] An Coimisiún um Chosaint Sonraí (Data Protection Commission), *Guidance Note: Guide to Data Protection Impact Assessments (DPIAs)*, October 2019, p. 3, https://www.dataprotection.ie/ (last accessed 19/05/2021).
[109] GDPR Article 25 (1).
[110] GDPR Article 25 (2).
[111] GDPR Article 32 (1).

loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed".[112]

Taking the aforementioned into consideration, controllers must design processing operations in a way that ensures their compliance with the GDPR and in that respect, they might also use codes of conduct or approved certification mechanisms to demonstrate such compliance.[113]

In addition, in case the risk assessment carried out by the controller leads to the conclusion that a type of processing is likely to result in a high risk to the rights and freedoms of natural persons, the controller - prior to the implementation of the concerned processing - must carry out a Data Protection Impact Assessment (DPIA).[114] Consequently, controllers are under an obligation to undertake a DPIA only in those cases the processing is "likely to result in a high risk". Particularly, GDPR Article 35 (3) lists certain types of processing for which a DPIA is certainly required, such as in case of systematic monitoring of a publicly accessible area on a large scale.[115] However, the latter list is not exhaustive of all kinds of processing that can lead to a high risk. Therefore, the European Data Protection Supervisor adopted - pursuant to GDPR Article 35 (4) - in 2019 a decision setting forth a further list of types of processing operations that have to be subject to a DPIA[116]. Particularly, the processing connected to high risks might be:

- "Systematic and extensive evaluation of personal aspects or scoring";
- "Automated-decision making with legal or similar significant effect";
- "Systematic monitoring";
- "Sensitive data or data of a highly personal nature", for example revealing ethnic or racial origin, political opinions, genetic data, biometric data for uniquely identifying a natural person, data of highly personal nature, etc;
- "Data processed on a large scale";
- "Datasets matched or combined from different data processing operations performed for different purposes and/or by different data controllers";
- "Data concerning vulnerable data subjects" (e.g. children, asylum seekers);
- "Innovative use or applying technological or organisational solutions that can involve novel forms of data collection and usage" (e.g. machine learning);
- "Preventing data subjects from exercising a right or using a service or a contract".[117]

---

[112] GDPR Article 32 (2).
[113] GDPR Articles 24, 25, 32, 40 and 42.
[114] GDPR Article 35 (1).
[115] GDPR Article 35 (3).
[116] Decision of the European Data Protection Supervisor Of 16 July 2019 on DPIA Lists issued under Articles 39(4) and (5) ff Regulation (EU) 2018/1725, https://edps.europa.eu/data-protection/ (last accessed 19/05/2021).
[117] *Ibidem*.

It is general agreement that if two or more of these kinds of processing apply, the controller should carry out a DPIA. Notwithstanding that, if the controller is of the opinion that its processing operations do not entail a high risk even in the presence in the specific case of more than one type of processing listed, it still has to explain and justify its decision not to carry out a DPIA.[118]

Finally, GDPR Article 35 (7) sets forth the elements that a DPIA should contain, namely (a) a systematic description of the processing operations and their purposes; (b) an assessment of their necessity and proportionality; (c) an assessment of the risks to the rights and freedoms of data subjects; and (d) the measures envisaged to address those risks.[119]

Once the framework of the risk assessment procedure within the GDPR has been established, it is necessary to carry out an assessment of the risks connected to Guider and to the various processing operations it is performing in order to help the controller to comply with its obligations. As already said, the degree of involvement of Guider in the processing of personal data might vary according to the services its customers want Guider to provide and thus, the controller has to be established on a case-by-case basis. However, if Guider is located in the Faculty of Law of the University of Bergen, the role of controller is held by the Rector who is accordingly responsible to carry out the risk assessment. Notwithstanding that, Guider would still be responsible to carry out the risk assessment with reference to the processing regarding storage for self-improvement since in the latter case it would be the controller.

In order to fulfil the aforementioned task, this report will use tables within its analysis in line with the approach and guidelines given by the various data protection entities.[120] Since the risk assessment has to be carried out only for those processing operations dealing with personal data, this part will focus only on those Guider's functions that fall within the scope of the GDPR. In addition, it should be recalled that the goal of the DPIA is not to eliminate all possible risks but rather to identify and minimise those risks.[121]

The first question that has to be answered within a risk assessment procedure is: Which of Guider's data processing operations require a DPIA?

Table 1. *Assessment of the necessity of a DPIA for different Guider's data processing operations.*

Guider's data processing operations	Criteria for processing 'likely to result in high risk'	Applicability of DPIA

---

[118] *Ibidem.*
[119] GDPR Article 35 (7).
[120] Article 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA)*, cit.
[121] An Coimisiún um Chosaint Sonraí (Data Protection Commission), *Guidance Note*, cit., p. 2.

Map with names of Professors associated to their offices within the Faculty of Law	None	NO
Schedule of rooms/spaces within the Faculty of Law	None	NO
Schedule of the persons working at the Faculty of Law	None	NO
Voice command + Microphone on to understand when someone is speaking to Guider	**1. Systematic monitoring of data subjects:** Guider will continuously collect the voices and process data in close proximity to its location so that every potential signal of "Hi, Guider" can be recognized immediately. However, people visiting the Faculty of Law might not be aware of such a collection of their personal data or how they will be used. **2. New technologies:** voice command can be considered an innovative form of data collection and usage.	**YES**
Storage for Personalised Experience	**1. Systematic and extensive evaluation of personal aspects or profiling**: by analysing and storing preferences and experience of users, Guider will evaluate certain personal aspects relating to them in order to predict aspects concerning that user. This would result in the profiling of the personal data of users; **2. Processing of sensitive data or data of a highly personal nature**: Guider will process special categories of personal data pursuant to GDPR Article 9(1), namely the voice of users, amounting to biometric data, for the unique purpose of identifying the user; **3. Processing of data of vulnerable data subjects:** Guider might process personal data belonging to children; **4. New technologies:** voice recognition can be considered an innovative form of data collection and usage.	**YES**
Storage for self-improvement	**1. New technologies:** machine learning is considered a new and innovative form of data collection and usage.	**YES**

Once established that only for some of Guider's data processing operations a DPIA is required, namely voice command and microphone on, storage for personalised experience and storage for self-improvement, the following table will carry out such an assessment. Particularly, since GDPR Article 35 only provides for a very general framework to carry out a DPIA, this permits controllers to design their DPIAs with flexibility and scalability so that the assessment can be shaped on their organisations' needs.[122] Thus, the following way of proceeding represents the one appropriate for Guider.

Table 2. *DPIA for some of Guider's data processing operations.*

Processing	Voice command + Microphone	Storage for Personalised	Storage for self-improvement

---

[122] *Ivi*, p. 14.

operations	on	Experience	
Description of the processing operations (*What are we doing and how?*)	**Purpose:** easier for the user to communicate with Guider by talking to it while the latter is listening with his microphone on in its proximity. **Type of processing:** recording of the voice and analysis. **Personal data:** voice. **Legal basis:** legitimate interest under art. 6 (1)(f). **Legitimate interest:** providing a user-friendly service for all visitors at the Faculty of Law through Guider. **Storage time**: throughout the interaction between Guider and the user.	**Purpose:** to connect voices with names, schedules and preferences of people in order to give a personalised experience. **Type of processing:** recording of the user's voice with filters to avoid recording surrounding voices, analysis to recognise regular users to personalise the communication, storage of previous interactions. **Personal data:** voice (special categories under art. 9 (1)), schedule and preferences. **Legal basis:** - for recording and analysis: consent under art. 6 (1) (a) and explicit consent of art. 9 (2) (a) + for children also art. 8. - for storage: contract under ar. 6 (1) (b). **Storage time:** as long as there is consent/contract.	**Purpose:** improve Guider's functioning through machine learning. **Type of processing:** storage, analysis through machine learning for improvement. **Personal data:** voice recording, decoding of the recording, previous routes taken. **Legal basis:** - Regular users: storage for self-improvement is a further processing of personalised experience → Article 6 (4) applies and purpose is compatible → no separate legal basis = consent under art. 6 (1) (a) and explicit consent under art. 9 (2) (a). - Occasional users: legitimate interest under art. 6 (1) (f). Legitimate interest = to improve in order to be able to distinguish different pronunciations or other references among its users. Storage time: until the purpose has been achieved.
Necessity/ proportionality (*Why do we do this?*)	The Law Faculty, as a popular destination, needs friendly infrastructures making all its rooms/space easily accessible. If the data subject can interact with Guider as normal face-to-face conversation, the legitimate interest of providing user-friendly service for all visitors through Guider is considered to be appropriate and necessary, especially in the case of people with disabilities. In addition, it is proportionate since voices are processed only to extract pure valid textual information for command, without any personal identification effects. Moreover, it is voluntary for the user to use voice command.	In order to give users a personal experience, Guider needs to collect, process and store special categories of personal data – biometric data for identification purposes – and other personal data - such as personal preferences and interests - in order to recognize the users and evaluate, analyse or predict their personal aspects. Such a data processing is proportionate because it is applied only to regular users of Guider that have expressed a consent, an explicit consent and entered into a contract. Moreover, in line with the principle of data minimisation, voice recognition asks for fewer personal data and has more functional possibilities than facial recognition, since voice data has been collected under voice command.	For Guider to improve its functioning, performance and speaking skills to distinguish words, different pronunciations or other references among its users, it is necessary to store data of previous usages and voice recordings. This processing has to be considered proportionate since the data stored, such as voice, are not used for identification but only for machine learning and in addition, they can be pseudonymised.
Risks to the rights and freedoms of	1. Power imbalance between the data subject and the data controller: data subjects might	1. Breaches of confidentiality of personal data and inappropriate disclosure	1. Breaches of confidentiality of personal data and inappropriate disclosure (especially of

data subjects (*How will data subjects be affected? Can we do this?*)	not be aware of being subject to such a processing and it might be impossible for them to consent to or oppose the processing since Guider's microphone is constantly listening to sounds nearby. 2. Risk of being identified.	(especially of vulnerable data subjects such as children). 2. Personal data might be inaccurate or incomplete: decisions and actions based on inaccurate information may negatively affect data subjects.	vulnerable data subjects such as children). 2. Personal data might be inaccurate or incomplete: decisions and actions based on inaccurate information may negatively affect data subjects. 3. Storage limitation: not possible to keep personal data only as long as necessary and as short as possible.
Measures to be adopted (*What to do?*)	1. More proportionate measure: data subjects can choose to turn on Guider's microphone and activate the voice command function before talking to Guider + filter to avoid the recording of surrounding voice. 2. Technological processing leads to the extraction from voices of pure valid textual information without any identification effects.	1. Raising awareness among staff to prevent unauthorised data sharing + logging access to personal data restricted to only authorised people + procedures to automatically inform data subjects of data breaches. 2. Procedures to correct inaccurate data such as consistency checks and data quality reviews. 3. Encrypted storage devices and pseudonymisation.	1. Raising awareness among staff to prevent unauthorised data sharing + logging access to personal data restricted to only authorised people + procedures to automatically inform data subjects of data breaches. 2. Procedures to correct inaccurate data such as consistency checks and data quality reviews. 3. Encrypted storage device and pseudonymisation.

Once Guider's controller has carried out a DPIA for those types of processing entailing a high risk for the rights and freedoms of data subjects, another question should be answered, namely what should the controller do and who should it contact if something "goes wrong"? Indeed, under GDPR Article 36, the controller is obliged - before implementing its processing operations - to consult its data protection authority in case the DPIA carried out under GDPR Article 35 shows that the identified high risk or a residual risk still persists irrespective of the measures adopted by the controller.[123] In that case, the supervisory authority shall provide written advice to the controller, and, if necessary, to the processor.[124] As far as Guider is concerned, in case of persistent risks, the controller has to contact Datatilsynet, namely the relevant Norwegian data protection authority.

11. Conclusion

When we initially got assigned to this project it was evident that through the interaction with people Guider has a lot of potential to improve lives. Despite this potential, the initial project was not designed with data protection in mind. Therefore this report aims to keep the interaction between the user and Guider, as envisioned by its creator, but make it compliant with the GDPR. We have always referred to the principles of the GDPR throughout the report, but now we will evaluate whether the new Guider actually complies with the principles as a whole.

We designed the layered approach to Guider with the principles of data protection by design and data minimisation in mind. In essence, the specific purposes Guider has for a customer will influence the quality and quantity of personal data that Guider will collect. We even created a version of Guider that does not require processing of personal data. Within these specific purposes we have given data subjects the additional choice to share as little personal data as they want with Guider. For example, users can click boxes instead of using their voice to enter room numbers, or they can simply login with Feide to identify themselves for the individual user experience. This means data subjects will often have the option to choose personal data protection over user-friendliness.

---

[123] An Coimisiún um Chosaint Sonraí (Data Protection Commission), Guidance Note, cit., p. 23.
[124] GDPR Article 36 (2).

Although we feel this version of Guider is compliant with the GDPR we still have identified some future challenges for Guider with regard to the principles. Under the principle of accountability the controller is accountable for compliance under the GDPR. One of the future challenges of Guider in the start-up phase is that they will be confronted with a limited capacity for the processing of personal data relative to their potential customers. We have identified that customers of Guider might be better suited to do the processing of personal data collected in their premises entirely by themselves. This is why big customers may choose to delegate the processing to one of their departments or have a separate legal entity be the processor. It is important that, under the principle of accountability, Guider has to be forthright about this with its customers in order to mitigate possible risks for data protection.

In our report Guider may rely on artificial intelligence to improve its understanding of users' speech and to find the most efficient route. Under the principle of fairness, data subjects should be informed about the processing happening through algorithms.[125] It will be a challenge for the future developers to give meaningful information about "the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject".[126] There might be a lot of applications for the improvement of Guider through artificial intelligence that we have not identified yet in this paper. Artificial intelligence can be used to improve the service of Guider, for example to better know or predict preferences of users or to improve interaction with its surroundings. When Guider wants to implement these new forms of processing of personal data it is important that these new purposes are again identified precisely and that compliance with principles as a whole is again reviewed.

---

[125] European Data Protection Board, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, 20 October 2020, p. 18, https://edpb.europa.eu/sites/ (last accessed 19/05/2021).
[126] GDPR Article 13 (2) (f).

12. Bibliography

European Union Law sources:

- Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, OJ 1993/L 95/29.
- Directive (EU) 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995/L 281/31.
- Directive (EU) 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ 2002/L 201/37.
- Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (codification), OJ 2015/L 241/1.
- 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), OJ 2016/L 119/11.

European Union documents:

- Article 29 Data Protection Working Party, *Opinion 03/2013 on Purpose Limitation*, 2 April 2013, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf (last accessed 19/05/2021).
- Article 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA)*, 4 April 2017, https://ec.europa.eu/newsroom/article29/items/611236 (last accessed 19/05/2021).
- Article 29 Data Protection Working Party, *Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller Under Article 7 of Directive 95/46/EC*, 9 April 2014, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf (last accessed 19/05/2021).
- European Data Protection Supervisor, *Accountability on the ground Part I: Records, Registers and when to do Data Protection Impact Assessments*, February 2018, https://edps.europa.eu/sites/default/files/publication/19-07-17_accountability_on_the_ground_part_i_en.pdf (last accessed 19/05/2021).

- European Data Protection Board, *Guidelines 07/2020 on the concepts of controller and processor in the GDPR. Version 1.0*, 02 September 2020, https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf (last accessed 19/05/2021).
- European Data Protection Board, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, 20 October 2020, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf (last accessed 19/05/2021).
- European Data Protection Board, *Guidelines 02/2021 on Virtual Voice Assistants*, 9 March 2021,
  https://edpb.europa.eu/system/files/2021-03/edpb_guidelines_022021_virtual_voice_assistants_adopted-public-consultation_en.pdf, (last accessed 19/05/2021).

Other sources:

- An Coimisiún um Chosaint Sonraí (Data Protection Commission), *Guidance Note: Guide to Data Protection Impact Assessments (DPIAs)*, October 2019, https://www.dataprotection.ie/sites/default/files/uploads/2019-10/Guide%20to%20Data%20Protection%20Impact%20Assessments%20%28DPIAs%29_Oct19_0.pdf (last accessed 19/05/2021).
- Johansen, S. L., *Guider - a robotic guider*, MIX301 Essay at University of Bergen.
- The Personal Data Act (Norway, Act of 15 June 2018 on the processing of personal data) (Personopplysnigsloven).