Quantified Student smart watch –   
GDPR compliancy

Niels van der Burg

Contents

[Revisions](#_heading=h.gjdgxs) **3**

[Executive summary](#_heading=h.30j0zll) **4**

[Introduction](#_heading=h.1fob9te) **4**

[Research questions](#_heading=h.3znysh7) **4**

[What does the GDPR law say on personal health data?](#_heading=h.2et92p0) **5**

[Literature study](#_heading=h.tyjcwt) 5

[Expert interview](#_heading=h.3dy6vkm) 8

[Conclusion](#_heading=h.1t3h5sf) 9

[How should the data be collect, saved, changed and deleted to be GDPR compliant?](#_heading=h.4d34og8) **10**

[Sources](#_heading=h.2s8eyo1) **11**

# Revisions

| ID | Date | Author | Change |
| --- | --- | --- | --- |
| 0.0 | 12/4/2022 | Niels van der Burg | origin |

# Executive summary

# Introduction

Quantified student is a project which aims to help students achieve better results by providing them insight in their own data. This would provide students with the necessary reflection to change their own behavior. One aspect that the QS project focusses on is health monitoring. Because the QS project will collect, safe and load user health data. A GDPR compliancy analysis was started to establish how QS could legally do this.

# Research questions

The main question for this research is as follows:

How can Quantified Student be GDPR compliant while collecting health data of FHICT students the volunteer to the project.

To answer the main question, the following sub questions were made:

* What does the GDPR law say on personal health data?
* How should the data be collect, saved, changed and deleted to be GDPR compliant?

To answer these questions, the ICT dot framework was used to setup the research. The following methods were used to research the sub questions:

| Question | Method | Approach |
| --- | --- | --- |
| What does the GDPR law say on personal health data? | Literature study | Reading the literature and specifying the impact of it on the QS project |
|  | Expert interview (maartje) | Talking to experts how they handle the GDPR, validating conclusion |
| How should the data be collect, saved, changed and deleted to be GDPR compliant? | Guideline conformity analysis | What guidelines should QS follow |
|  | Expert interview | To confirm that the guidelines followed are in fact correct and GDPR compliant |

After completing this project, there should be a better understanding how to act upon the collected and processing of the data.

# What does the GDPR law say on personal health data?

To establish a proper foundation for further research. It must first be understood what the GDPR law says about health data.

## Literature study

Our project benefits of the fact that we are not building an application to identify users. But rather assist the user in identifying their own patterns.

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

*- GDPR art 9.1*

Processing does not describe the calculation or obtaining information from it. It describes the handling of data in any shape or form.

*‘processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;*

*- GDPR art 4.2*

For further research the checklist at <https://gdpr.eu/checklist/?cn-reloaded=1> is used. We must abide by the following standards:

1. Provide information and impact analysis on what we produce.
2. Has a lawful reason for processing the data.
3. Must be clear what the goal is and activities done on the data.
4. Must safely be stored taken into consideration the best possible way to secure the data.
5. Data must be anonymized or pseudo anonymized as much as possible
6. Security guidance to ensure that the weakest link is not in the organization
7. In the case that the data could infringe on a persons freedom a Data Protection Impact Assessment must be done.
8. In case of a breach contact this countries authority.
9. Somebody must be accountable for GDPR compliance.
10. In case that the data is processed by a third party, a data processing agreement must be made.
11. When processing data from a member state, we need to have a representative from that state.
12. A data protection officer (DPO) if needed (https://gdpr.eu/checklist/?cn-reloaded=1) .
13. Users should be able to easily get access to their data.
14. We must be able to allow the user to update their info.
15. We must be able to identify the user prior to providing them data.
16. The provision of a users data to a user should take less than 1 month.
17. A right to be forgotten. A user must be able to delete all data collected about them.
18. Data must be easily transferable via an excel sheet or similar methods.
19. If collection of data is for marketing purposes. A user can request an immediate stop of the processing of data which must be obliged.
20. If automated processing are at play that influence legal or similar effects. Activities must be taken to ensure the rights of these users.

Beyond the GDPR, we need to mainly comply with the AVG (the Dutch interpretation of the GDPR). For this the following source was used <https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/checklist_houd_grip_op_persoonsgegevens_def.pdf>.

In the first of the checklist we need a ground for obtaining the data. For this I recommend going with permission. Since the ground work of the project focusses on a volunteer basis. For collection of data based of permission, we need to abide by the following principles. (<https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/mag-u-persoonsgegevens-verwerken#wanneer-mag-u-zich-baseren-op-de-grondslag-toestemming-6331>)

1. *Vrijelijk gegeven*  
   U mag iemand niet onder druk zetten om toestemming te geven. Bijvoorbeeld door iemand te benadelen als hij of zij geen toestemming geeft. Let daarbij op machtsverhoudingen: een werknemer kan een vraag van zijn werkgever bijvoorbeeld moeilijk weigeren.

*Translated:  
A user must give permission and can revoke it. Keeping in mind power dynamic such as employer to employee or in our case teacher to student.*

1. *Ondubbelzinnig*  
   Er moet sprake zijn van een duidelijke actieve handeling. Bijvoorbeeld een (digitale) schriftelijke of een mondelinge verklaring. Het moet in elk geval volstrekt helder zijn dát er toestemming is verleend. U mag niet uit gaan van het principe ‘wie zwijgt, stemt toe’. Het gebruik van voor-aangevinkte vakjes is dus niet toegestaan.  
   *Translation:  
   The action of giving consent must be given. It cannot be if you use this service you agree to the collection of data.*
2. *Geïnformeerd*

U moet mensen vooraf informeren over:

* + - * 1. de identiteit van u als organisatie;
        2. het doel van elke verwerking waarvoor u toestemming vraagt;
        3. welke persoonsgegevens u verzamelt en gebruikt;
        4. het recht dat zij hebben om de toestemming weer in te trekken.

*Translation:  
A user must be aware of the identity of the organization, the goal of the data processing, which data is collected and the rights the users have to revoke their permission.*

1. *Specifiek*  
   Toestemming moet steeds gelden voor een specifieke verwerking en een specifiek doel. Heeft u meerdere doeleinden om gegevens te verwerken? Dan moet u de betrokkene hierover informeren en voor elk doel afzonderlijk toestemming vragen. Het doel mag niet gaandeweg veranderen.  
   *Transtlation:  
   Consent must apply for specific processing and goals. If there are multiple goals from data collection a user must be made aware of them.*

Beyond this, all employees or future employees must be made aware of the privacy laws.

A user also has a set of rights, which must be made accessible to them. These are:

* Recht op inzage. Dat is het recht van mensen om onder meer een kopie te ontvangen van de persoonsgegevens die u van hen verwerkt. De Autoriteit Persoonsgegevens (AP) biedt u een voorbeeldoverzicht.  
  *Translotion  
  Right of insight. The user has the right to obtain a copy of the data processed.*
* Recht op vergetelheid. Mensen hebben het recht om ‘vergeten’ te worden. Maar wist u dat u vaak niet alle persoonsgegevens kunt wissen?  
  *Translation:  
  Right to be forgotten. The user has the right to request deletion of their data. This applies when:*
  + *Not needed anymore*
  + *Permission is revoked*
  + *Objection*
  + *Unlawfull processing*
  + *It passed the legal storage time*
  + *Kids are using it*
* Recht op rectificatie en aanvulling. Het recht om de persoonsgegevens die u verwerkt te laten wijzigen.  
  *Translation:  
  The user has the right to edit or add data personal data.*
* Het recht op dataportabiliteit. Het recht om persoonsgegevens over te laten dragen aan een andere partij.  
  *Translation:  
  The user has the right for data to be portable between platforms.*
* Het recht op beperking van de verwerking: Het recht om minder gegevens te laten verwerken.  
  *Translation:  
  The user has the right to limit data processing.*
* Het recht met betrekking tot geautomatiseerde besluitvorming en profilering. Oftewel: het recht op een menselijke blik bij besluiten.  
  *Translation:  
  A user must be provided a human readable export of the information.*
* Het recht om bezwaar te maken tegen de gegevensverwerking.  
  *Translation:  
  A user has the right to revoke or block data if laws apply.*
* Ten slotte hebben mensen recht op duidelijke informatie over wat u met hun persoonsgegevens doet. Onder de AVG moet u aan een aantal specifieke eisen voldoen.  
  *Translation:  
  The user has the right to gain insight into how their data is used.*

## Expert interview

To confirm the findings of this research. An expert was interviewed to verify these findings.

## Conclusion

Based of the previously stated requirements we must:

1. Enforce user consent per data source.
2. Request consent for the usage and for each data source added.
3. Must be able to provide an export for other services and as an export (csv or similar)
4. Set a limit for data storage (probably 365 days)
5. Provide the possibility to revoke and add data.
6. Set a specific usage for the data. We cannot add new usages later.

In the case of smart watch the data must also be encrypted since it could identify users.

# How should the data be collect, saved, changed and deleted to be GDPR compliant?

Based of the previously stated GDPR law. We must abide by the following laws:

* An impact analysis (how the usage of this data impacts our users)
* Reason for processing the data.
* Goal and activities done on the data relevant to the end user.
* Data must be safely stored.
* Data must be anonymized, pseudonymization or encrypted as much as possible.
* Security guidance and processes as much as possible.
* Proper awareness and training for individuals handling the data.
* Date Impact Analysis prior to handling the data.
* In case of a data breach, authorities and the individual affected must be alerted within 72 hours.
* Since there FHICT and Fontys have more than 250+ employees, a person needs to be accountable for GDPR compliance.
* Users must be able to request their data in an easily understood format within a month
* Users must be able to keep personal data up-to-date and gain easy insight.
* The user must be verified as the actual person updating and requesting their own data.
* The user has the right to be forgotten. Which means that all data must be removed from the services.
* The user, in case of unlawful actions, must be able to put a halt to the processing of data.

Quantified Student must oblige by these standards to lawfully operate within the Netherlands.

# Sources

<https://gdpr.eu/checklist/>

<https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/checklist_houd_grip_op_persoonsgegevens_def.pdf>

<https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/mag-u-persoonsgegevens-verwerken#wanneer-mag-u-zich-baseren-op-de-grondslag-toestemming-6331>

<https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/rechten-van-betrokkenen>