General Data Protection Regulation

Research into GDPR based on the Care web-application

Name: Victoria C. A. Fong

Student number: 488384

Introduction

This document is based on research into the GDPR (General Data Protection Regulation) to what it is and how to apply it to the Care web-application. It is important to stick to these regulations for privacy and legal issues that can come fort when handling personal data of users.

Table of Contents

What is the GDPR

The GFPR is a European privacy regulation that ensures that personal data is carefully processed by business and organizations. These rules apply across the EU/EEA which protects the privacy rights of user’s personal data based on a set of rules.

Data Requirements

Here are some non-functional requirements that are important in an enterprise environment based on the Care web-application.

- **Privacy**:
    - Collecting data of the users to get a grasp to what medicines they take and when they take it so that the system can help monitor their medicine. No one should have access to the user's data besides the system for privacy rights.
- **Security**:
    - Access to data where only the user has and strangers.
- **Reliable, scalable infrastructure:**
    - The platform is designed for a large audience of users. Scalability and reliability is needed for users to have access of keeping track of their medicine and if the correct information is displayed.
- **Processing speed of data:**
    - The speed of the system has to be fast enough where it does not take 1 min for the data to be updated for the user.
    - Real time data helps the user to feel at ease with using trusting the application.

Privacy sensitive data stored in the web-application

Context

Here we will be touching down on data that is stored in the system and seeing if there any privacy sensitive data and planning functionalities to comply with the GDPR and other regulations.

Personal Data stored

- User’s name
- Password
- Email
- Dose intake of the user for a specific medicine
- Time of intake for the user to take in the medicine
- The name of the medicine the user is taking
- Personal feedback written by the user of taking the medicine

Functionalities to comply with the GDPR

- Personal data that is stored by the user is only used for the assistance of the user to track their medicine intake and for nothing more.
- Personal data will be secured with password and email as authentication as long with other tools for higher security to protect for data breaches.
- Personal data that the user has stored on the web-application can always be fully deleted/removed by the user’s request.

Evaluating MongoDB data storage

The data storage that is used for each microservice of the Care web-application is the MongoDB database. We will be evaluating the database with the use of the CAP theorem based on the set data requirements.

CAP theorem

The CAP theorem is based on representing three different kinds of guarantees developers aim to provide in their distributed data system. It is stated that developers must choose two out of the three guarantees because it is impossible to promise all three. The three guarantees are:

- **Consistency**: All nodes in the system have the same view of the data at any time.
- **Availability**: the system is responsive to requests.
- **Partition tolerance**: they system can remain operational when problems occur, or a service needs to be down.

Evaluation / patterns to enhance architecture

The web-application top picks which are important to the system are Consistency and Partition Tolerance. Based on the requirements that the data has to be constituent and able to be updated when parts are down is important to the project.

To implement this, the application uses a message broker (RabbitMQ + Mass transit) to be able to update other service that were down and needed information of new data of other services with using publish and subscribe. This make sure that the data is consistent withing the system and that services are not reliant on other services and that the application can always be running.

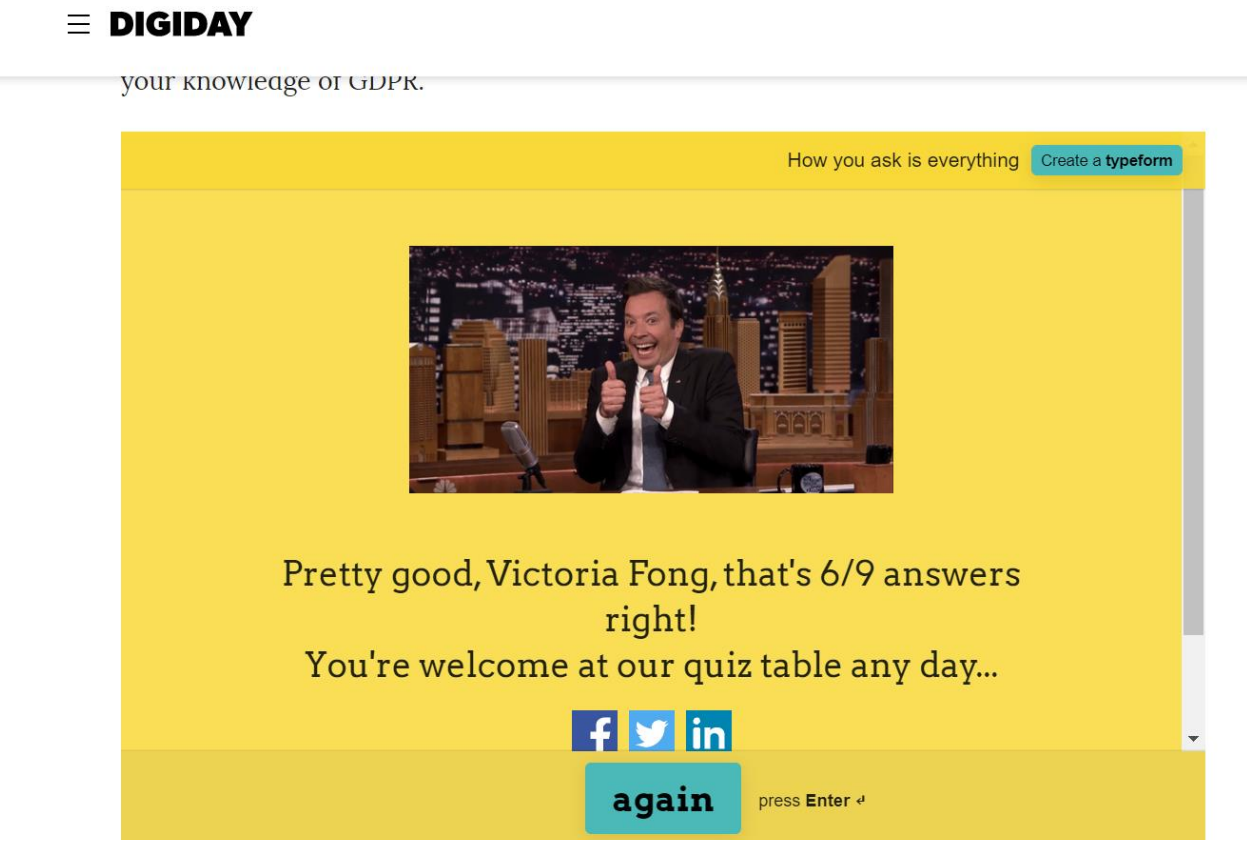
Practical approaches

Context

To have a better understanding of the law regarding the GDPR, I have also taken upon some practical approaches such as:

- Testing my knowledge by taking the GDPR test.
- Going through the practical GDPR checklist.

GDPR Test results



your knowledge of GDPR.

Pretty good, Victoria Fong, that's 6/9 answers right!
You're welcome at our quiz table any day...

GDPR checklist for data controllers

The checklist has been made by the GDPR.EU to get some useful information on terminology and basic structure of the law for starting a business that uses personal data of users. I have through it for myself to be more aware regarding applying GDRP to the application.

Sources

Netherlands Enterprise Agency, RVO. (2022a, September 27). *How to make your business GDPR compliant*. business.gov.nl. https://business.gov.nl/running-your-business/business-management/administration/how-to-make-your-business-gdpr-compliant/

GDPR Checklist. (n.d.). *The GDPR Checklist - Your GDPR compliance checklist*. https://gdprchecklist.io/

Koch, R. (2019, April 11). *Everything you need to know about GDPR compliance*. GDPR.eu. https://gdpr.eu/compliance/