GDPR research document

TwitterV2

Daniil Blagoev

Contents

[Introduction 2](#_Toc169513589)

[Research questions and methods 2](#_Toc169513590)

[Answers 2](#_Toc169513591)

[What is the GDPR? 2](#_Toc169513592)

[What are the guidelines of the GDPR for web applications? 2](#_Toc169513593)

[Does TwitterV2 meet the GDPR requirements? 3](#_Toc169513594)

[Conclusion 3](#_Toc169513595)

[Sources 5](#_Toc169513596)

# Introduction

The purpose of this document is to investigate the GDPR and what it entails for TwitterV2. TwitterV2 is an application which would ideally be available to users in the whole world. For it to be usable in the whole world, GDPR is something it must comply with.

# Research questions and methods

Main research question:

* How can I make TwitterV2 compliant with GDPR?

Sub-questions

* What is the GDPR?
  + Literature study
    - Google what the GDPR is.
* What are the GDPR guidelines for web applications?
  + Literature study
    - Google what the guidelines for web applications are.
* Does TwitterV2 meet the GDPR requirements?
  + Guideline conformity analysis
    - Analyze if TwitterV2 conforms to the GDPR guidelines.

# Answers

## What is the GDPR?

GDPR compliance is required by the General Data Protection Regulation, an EU law that is binding on both EU member states and those countries that trade in the EEA (European Economic Area). The GDPR contains many principles for processing, collecting, accessing, rectifying, erasing, and transferring personal data. But it is its specific regulations on securing and protecting data that concern those responsible for organizational information and data security.[[1]](#footnote-1)

## What are the guidelines of the GDPR for web applications?

1. Obtain explicit consent: You must obtain clear and affirmative consent from users before collecting and processing their personal data (usernames and passwords). This consent should be freely given, specific, informed, and unambiguous.
2. Provide transparency: You must inform users about what data you collect, how it is processed, for what purposes, and with whom it may be shared. This information should be provided in a clear and easily accessible manner, such as in a privacy policy.
3. Implement data protection by design and default: You must build data protection measures into your application from the ground up, ensuring that only the minimum necessary data is collected and processed, and that data is secured by default.
4. Respect data subject rights: Users have the right to access, rectify, erase their personal data. Your application should have mechanisms to facilitate these rights.
5. Ensure data security: You must implement appropriate technical and organizational measures to protect personal data against unauthorized access. This includes measures like encryption and regular security testing.
6. Report data breaches: If a data breach occurs that poses a risk to individuals' rights and freedoms, you must report it to the relevant supervisory authority within 72 hours and notify affected individuals without undue delay.[[2]](#footnote-2) [[3]](#footnote-3)

## Does TwitterV2 meet the GDPR requirements?

TwitterV2 does not meet requirement 1 and 2.

In regard to point 3, I collect only usernames and passwords of users, they are encrypted and stored within Azure’s CosmosDB. Additionally, whenever my messaging service sends data around, the content of the messages is encrypted.

For point 4, if users want to access/edit/delete their data (accounts), they can do so at any given time, as endpoints for those functionalities exist.

For point 5, data security is ensured by my implementation of authorization & authentication and the encryption of user data in the database and while being transported through messaging.

# Conclusion

In order for TwitterV2 to be compliant with the GDPR, a privacy policy page must be implemented. Inside of the privacy policy page, it needs to be stated what data TwitterV2 collects, users’ rights regarding their data. The screenshots below depict the implementation of what was mentioned so far:

A blue line with a white background

Description automatically generated with medium confidence

Figure 1 The registration screen with a link to the privacy policy

A screenshot of a computer

Description automatically generated

Figure 2 The privacy policy of TwitterV2

# Sources

*What is GDPR Compliance in Web Application and API Security?* (2023, January 11). https://probely.com/blog/what-is-gdpr-compliance-in-web-application-and-api-security

*How To Meet GDPR Requirements In Mobile And Web Applications*. (2023, November 28). https://selleo.com/blog/how-to-meet-gdpr-requirements-in-mobile-and-web-applications

*How to make your website GDPR compliant in 8 Steps*. (n.d.). Vanta. https://www.vanta.com/resources/8-steps-to-make-your-website-gdpr-compliant

1. *What is GDPR Compliance in Web Application and API Security?* (2023, January 11). https://probely.com/blog/what-is-gdpr-compliance-in-web-application-and-api-security [↑](#footnote-ref-1)
2. *How to make your website GDPR compliant in 8 Steps*. (n.d.). Vanta. https://www.vanta.com/resources/8-steps-to-make-your-website-gdpr-compliant [↑](#footnote-ref-2)
3. *How To Meet GDPR Requirements In Mobile And Web Applications*. (2023, November 28). https://selleo.com/blog/how-to-meet-gdpr-requirements-in-mobile-and-web-applications [↑](#footnote-ref-3)