GDPR Compliance Document

Name: Tony Jiang

Semester 6

Introduction

This document outlines how I, as the developer of the Music Trivia web-based game, have ensured the privacy and protection of personal data in accordance with the General Data Protection Regulation (GDPR).

Personal data

This section applies to all personal data collected from users of this application. The data being stored includes user email address, username, password, and user roles.

Data protection principles

I adhere to the following data protection principles.

Lawfulness, fairness, and transparency

I process personal data lawfully by ensuring that the processing is necessary to perform a contract with the user, specifically to authenticate and authorize them to use the application. I ensure fairness by informing users about how their data will be used and respecting their individual rights. Additionally, I provide transparency through a detailed privacy notice and clear communication about the use of their personal data within the application.

Purpose limitation

The personal data is collected to authenticate users in the application, authorize users in the application.

Data minimization

I collect only the personal data that is adequate, relevant, and limited to what is necessary for the purposes of user authentication and authorization in our application. Specifically, we collect the following data:

- Email address
- Username
- Password

This information is essential for creating and managing user accounts and ensuring secure access to the application.

Accuracy

I ensure personal data is accurate and up-to-date by periodically confirming user information through the application every six months.

Storage limitation

Personal data is retained only for as long as necessary for authentication and authorization purposes. Data will be deleted if the user remains inactive for 12 months.

Integrity and confidentiality

I implement appropriate security measures to protect personal data by following the top 10 OWASP guidelines and regularly assessing the security risks of the application.

User rights

The users have right to the following personal data. These are the rights I have consider on how to implement it in the application.

Right to be informed

Users have the right to be informed about the data that is collected through the application and how it is being used. This obligation is fulfilled by providing a privacy policy at the signup form and making it easily accessible throughout the application.

Right of access

Users have the right to access their personal data. They can view their personal profile page within the application to see the personal data we have collected, including their email address, username, and any other relevant information. For security reasons, passwords are not displayed, as they are encrypted. However, users can change their password by providing their current password and a new password.

Right to rectification

Users can request the correction of inaccurate data by accessing their personal information and making changes. They can update their username, email, and password directly within the application.

Right to erasure

Users can request the deletion of their data. They can delete their account information directly within the application.

Data security

I validate risk analyses and regularly follow the top 10 OWASP security mitigation strategies to ensure the effectiveness of our security measures. Personal data can only be accessed by authenticated and authorized personnel. Additionally, data is encoded during transit.

Third-Party Processors

I do not share data with third parties without explicit user consent. Any third-party processors that require access to personal data will be required to comply with GDPR regulations and adhere to strict data protection standards.

Conclusions

This outlines how I ensure compliance with GDPR regulations. It allows me to consider how to secure my data effectively, determine which data is essential, and maintain transparency with users of this application. These are the foundational regulations I have covered, with more to come as the application is developed.