

GDPR Compliance Document

Name: Tony Jiang

Semester: 6

Introduction

This document outlines how I, as the developer of Song Snippets, have ensured the privacy and protection of personal data in accordance with the General Data Protection Regulation (GDPR). Song Snippets is a web-based game platform where users can enjoy the challenge of guessing song names.

Data We Collect

We collect the following types of data to provide and improve our services:

1. Personal Information:
 - User ID
 - Email address
 - Username
 - Password (stored securely)
2. Activity Data:
 - Actions you take within the game (e.g., creating a song playlist, making song guesses)
 - Your guesses and game progress.
3. Preference Data:
 - show preferences, such as favorite songs and genres, based on your accuracy in guessing songs and other interactions within the game.
4. Advertising Data:
 - We may collect data related to your preferences and interactions with the songs to display more relevant advertisements based on overall user preferences.

This information is collected to enhance your experience, personalize the game, and display relevant ads (if applicable), as well as to analyze game performance and improve the service.

Purpose of Data Collection

We collect your data to enhance your experience on our website and to tailor the advertisements you see. This helps us to:

- Provide a personalized game experience.
- Display relevant advertisements based on general interests, helping us generate revenue to keep the game free to play.

Your data will only be used for these purposes, and we will not share it with third parties without your consent unless required by law.

Legal Basis for Processing

We process your personal data based on the following legal grounds:

Consent: When you sign up for our game, you give us permission to collect and use your email, username, and password to create and manage your account. We also seek your consent if we use tracking cookies for ad purposes or for sharing data with third-party advertisers where required by law.

Contract: By creating an account, you enter into an agreement with us, and we process your data to fulfill our contract with you, such as by providing game access and support.

Legitimate Interests: We use your data to maintain the game's functionality and security, to improve our game experience, and to display ads. We only process the minimum amount of data necessary and ensure that our legitimate interests do not infringe on your privacy rights.

Legal Obligations: In some cases, we may be required to retain or disclose certain data to comply with laws or regulations, such as for tax or security purposes, or to respond to valid legal requests from authorities.

Your right

Under the GDPR, you have several rights regarding your personal data:

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

We implement strong security measures to protect your personal data from unauthorized access, loss, or destruction. This includes:

- Regular risk analyses and adherence to industry-standard security practices, such as the OWASP Top 10 security mitigation strategies.
- Access to personal data is restricted to authenticated and authorized personnel only.
- All personal data is encrypted during transmission using secure protocols (e.g., HTTPS).

We continuously monitor and update our security practices to safeguard your information.

Data Retention

We retain personal data only for as long as necessary to fulfill the purposes for which it was collected, including:

- Authentication and authorization
- Song guessing and playlist creation
- Storing user preferences and using user preferences for displaying relevant ads.

If a user remains inactive for 12 months, their personal data will be deleted.

Data Sharing and Third-Party Disclosure

We may share your personal data with third parties for the following purposes:

- Third-Party Login/Signup Services: To facilitate account creation and login through third-party services.
- Targeted Advertising: To use your preferences to display relevant ads on the website through advertising partners.

We ensure that any third parties with access to your data adhere to appropriate security standards and comply with applicable data protection laws.

Conclusion

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.