GetawayGo

GDPR Implementation

Fontys University of Applied Sciences

Anna Kadurina
15/01/2025

Table of Contents

Introduction

The purpose of this document is to outline GetawayGo's implementation of the General Data Protection Regulation (GDPR). The GDPR ensures that individuals' personal data is collected, processed, and stored responsibly, while respecting their privacy and providing them with rights regarding their personal information.

Implementation of GDPR Measures

Data Collection and Usage

GetawayGo collects only the personal data necessary for its services, including full name, email address, phone number, date of birth, and hashed password as you can see in the screenshot below.
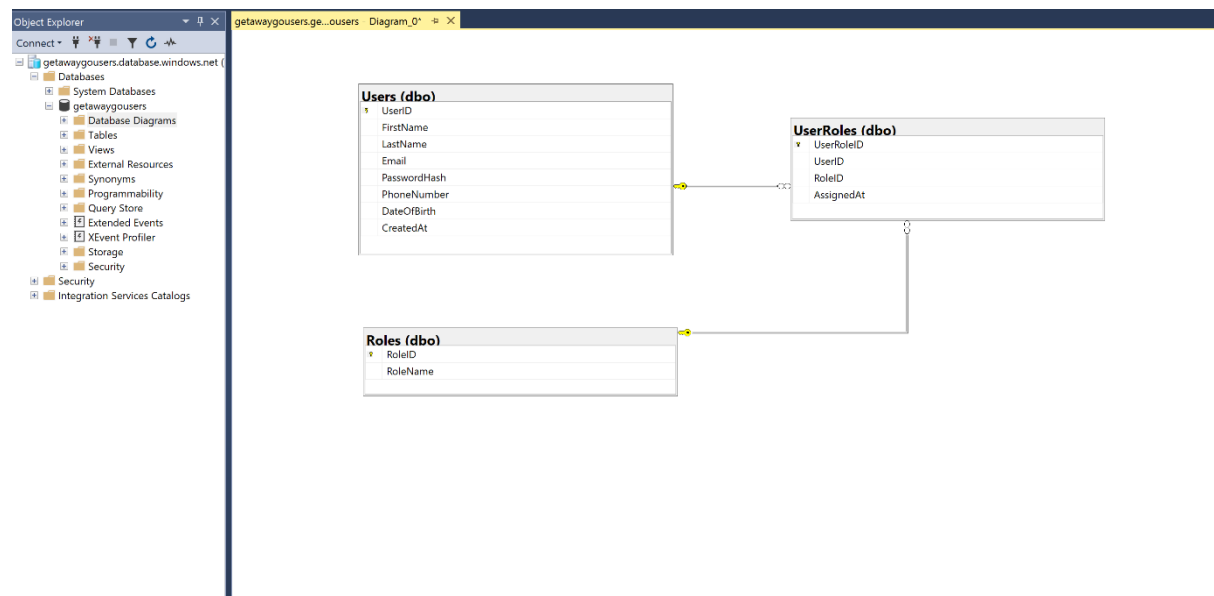

Figure 1 – Users database structure

Payments are handled by Stripe, a GDPR-compliant third party platform. No sensitive information is stored directly on GetawayGo servers.
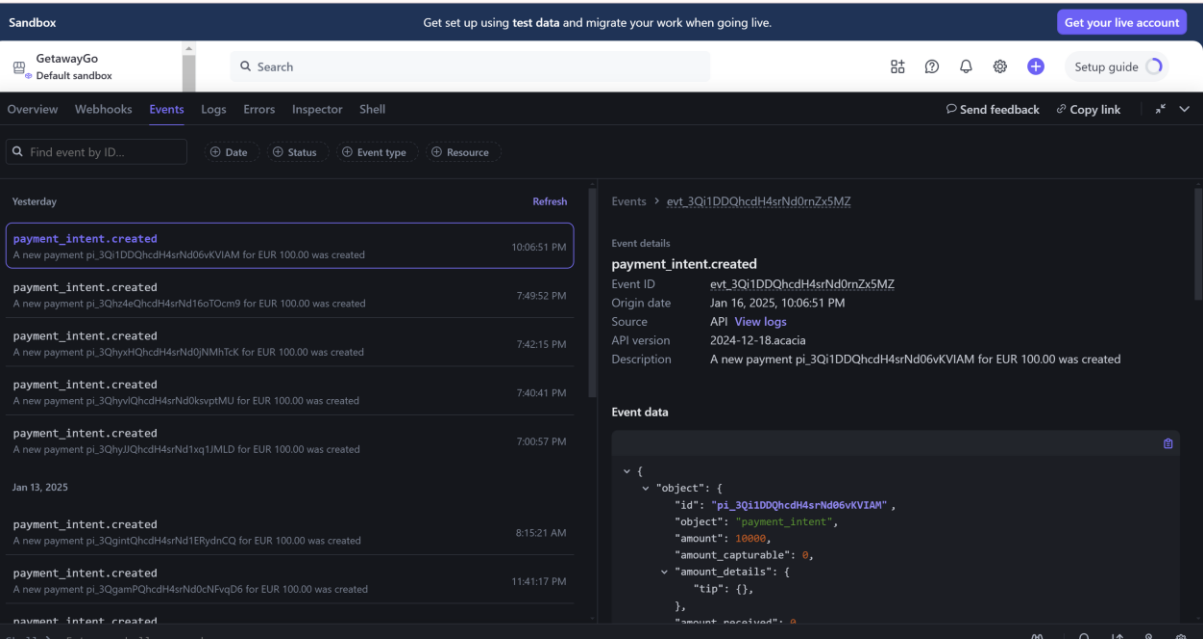

Figure 2 –Stripe payment system dashboard

All data collection is purpose-driven, ensuring no unnecessary information is retained.

Data Security

Sensitive information such as passwords are encrypted.

Figure 3 – Example of a hashed password of a user

Data is stored on Azure servers in the West Europe region, ensuring compliance with GDPR data residency requirements. Each microservice has its own server and database, minimizing cross-service data vulnerabilities.
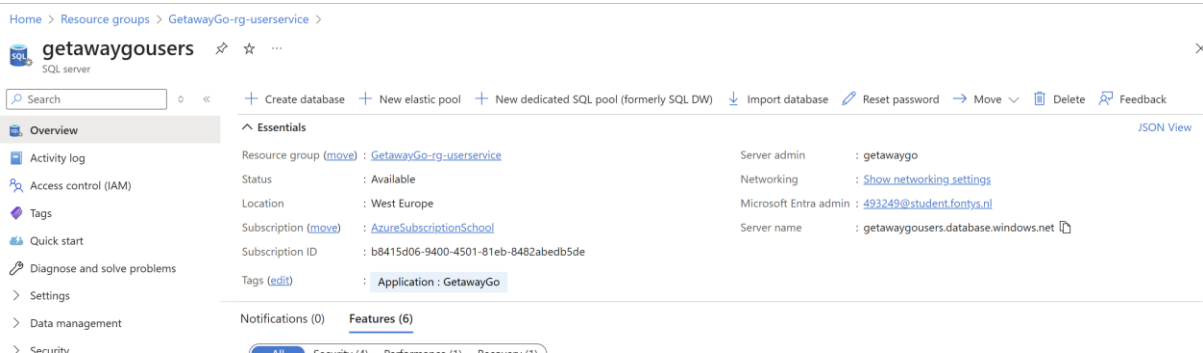

Figure 4 – Users SQL Server

Services communicate securely with Azure managed identities, eliminating the needs for hardcoded credentials. Access to user data is restricted through role-based permissions (as you saw in the database schema the roles tables).

User Rights

GetawayGo ensures that the users have the right to access their data, update it, and delete all of it. When a user requests account deletion, a message is sent to an Azure Service Bus queue. Each microservice processes this message to delete the respective data. This ensure comprehensive and synchronized data removal across the system.
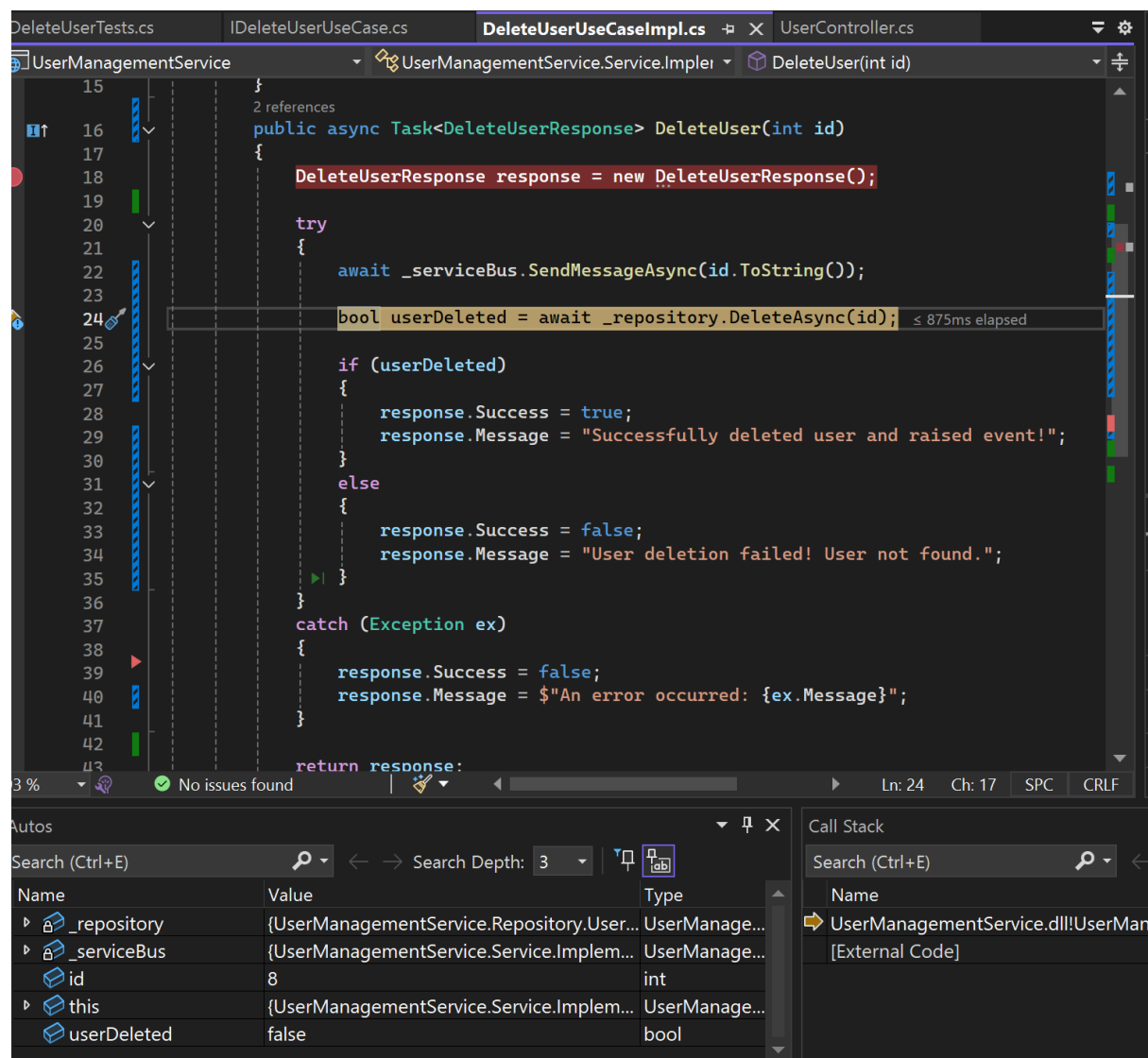

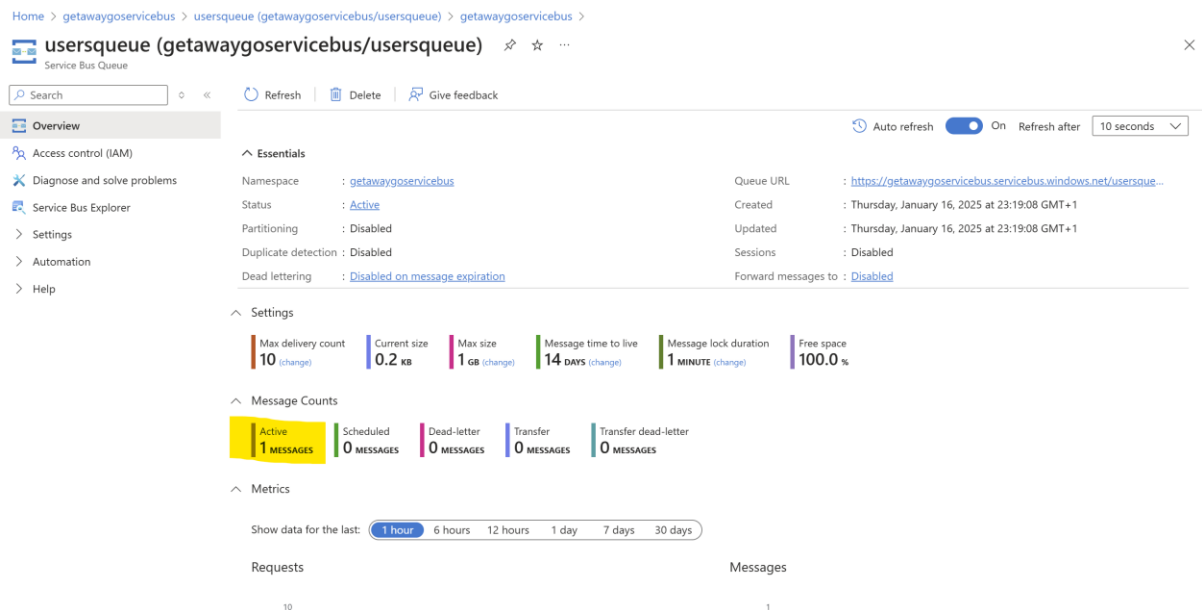*Figure 5 – Sending a message to service bus on a deletion of user*

Figure 6 – Users queue on Azure Service Bus

Conclusion

GetawayGo is fully committed to GDPR compliance, ensuring the privacy and protection of user data through robust security measures, data minimization practices, and user empowerment. By implementing encryption, secure cloud storage, managed identities, and a structured data deletion process, GetawayGo provides a secure environment for its users.