

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | |
|  | | SpendSence | | | | |  | |
|  |  | | | | | | |  |
|  | | | |  |  | | | |
|  | | | | Load Test Report |  | | | |
|  | | | | May, 2025—Viktoria Todorova—First Draft |  | | | |
|  | | |  | | |  | | |

# Overview

SpendSense is a modular, containerized web application designed to help users manage their personal or organizational finances. The system is composed of several microservices that handle distinct responsibilities, including budget management, expense tracking, user authentication and authorization, and GDPR compliance orchestration. Each microservice runs in its own Docker container, ensuring modularity, scalability, and ease of deployment.

The architecture is orchestrated using Docker Compose, which provisions and networks multiple services such as MySQL databases, RabbitMQ (message broker), Traefik (reverse proxy and TLS termination), and Prometheus/Grafana (for observability and metrics visualization). The system supports secure access and monitoring through HTTPS and exposes metrics for performance analysis and alerting.

Authentication and identity management are handled by Keycloak, an open-source identity and access management solution. Keycloak connects to a dedicated MySQL database and is integrated with OAuth2 Proxy to secure access to internal services. This allows SpendSense to enforce access policies and secure APIs while maintaining a single sign-on experience.

The application also includes a GDPR Orchestrator Service, which is responsible for coordinating the deletion process across microservices to comply with the user’s right to be forgotten.

Overall, the system is built with privacy and observability in mind, allowing for performance monitoring, secure communication, and identity management across services.

# GDPR Compliance Analysis

##### Personal Data Flow Analysis

On *Fig. 1* you can see how each part of the SpendSense system uses personal data, what it's used for, and why it’s allowed under GDPR rules. Keycloak handles login details like names, emails, and passwords so users can sign in securely. The budget-service and expense-service store and manage user budget and spending information. The gdpr-orchestrator helps the system follow GDPR rules by handling user requests to delete their data. OAuth2 Proxy manages login sessions and cookies to keep services secure. RabbitMQ sends messages between services. All personal data is saved in MySQL databases, which are needed for the system to work. Overall, each part has a clear reason for using personal data and follows the legal rules set by GDPR.

|  |  |  |  |
| --- | --- | --- | --- |
| Component | Data Involved | Purpose | GDPR Legal Basis |
| Keycloak | Name, Email, Credentials, Roles | User Authentication and Authorization | Consent / Contractual |
| budget-service | Budget records (linked to users) | Budget management | Legitimate interest / Consent |
| expense-service | Expense records (linked to users) | Expense management | Legitimate interest / Consent |
| gdpr-orchestrator | User data discovery, access, deletion requests | GDPR compliance orchestration | Legal obligation |
| oauth2-proxy | Session tokens, cookies | Secure access to protected services | Legitimate interest |
| RabbitMQ | Event messages (may include user IDs) | Event-driven architecture | Legitimate interest |
| MySQL Instances | Persistent storage of personal data | Data storage for individual services | Contractual necessity |

*Fig. 1: Table with personal data flow analysis*

Terms explained

Consent - the user has clearly said "yes" to let you use their data for a specific purpose

Contractual - the data is needed to provide a service the user asked for, like when they create an account or use the app

Legitimate Interest - the system uses the data in a way that’s necessary for the business to function, but it doesn’t harm the user’s rights or privacy

Legal Obligation - required by law to collect or keep the data

Contractual Necessity - similar to "Contractual" and, but the data must be processed to fulfill a contract with the user.

##### Data Storage & Encryption

SpendSense stores personal and financial data in MySQL databases, which are used by the budget, expense, and Keycloak services. All communication between services and users is protected using TLS encryption, which is enabled through Traefik's websecure entry point. HTTPS is secured using TLS certificates (fullchain.pem and privkey.pem), ensuring that data is encrypted while in transit. However, there is no explicit encryption configured for data at rest in the MySQL containers. It is strongly recommended to enable MySQL at-rest encryption, such as Transparent Data Encryption (TDE), to better protect stored data from unauthorized access in case of a breach or physical compromise.

##### Data Access Control

SpendSense controls access to data through secure authentication and simple role-based authorization. User authentication is handled by Keycloak, using the OpenID Connect (OIDC) protocol to verify users during login. Although the system currently uses only a single role for all users, this role helps restrict access to protected services and APIs. Session security is maintained by setting cookies with SameSite and Secure attributes, and by scoping them to trusted domains. In addition, OAuth2 Proxy is configured to prevent Cross-Site Request Forgery (CSRF) attacks, helping to ensure that session-based access remains safe and trustworthy.

##### Data Retention & Deletion

Currently, there is no explicit data retention policy defined within the SpendSense stack. The gdpr-orchestrator service is responsible for ensuring that when a user requests data deletion, all their personal data stored across the various microservices’ databases is deleted consistently and simultaneously. This orchestration helps maintain compliance by coordinating the removal of data from budgetand expense services at once. Deletion can be triggered manually or via API calls handled by the service logic. To improve accountability, it is recommended to implement automated logging and auditing of all deletion requests and actions.

##### Data Subject Rights

SpendSense supports several rights that users have over their personal data. Users can access their data through various APIs. They can also correct any mistakes in their data within the application. The right to erase data (also known as the “right to be forgotten”) is fully supported and managed through the dedicated gdpr-orchestrator service. However, the system currently does not support exporting data in a portable format, which means users can’t easily download their data. Additionally, SpendSense does not offer restrictions on how data is processed, and users cannot object to certain data processing without extra features or user interface elements being added.

##### Third Parties and Transfers

SpendSense does not explicitly use any external third-party services that handle personal data based on the current configuration. While Keycloak is a third-party product, it is deployed internally within my own environment as a container I control, so it is treated as an internal service rather than an external third party. However, some components like OAuth2 Proxy or monitoring tools might send data outside the application—for example, to external services such as Grafana Cloud—if configured to do so. There are no identified transfers of personal data across international borders in the current setup.

##### Logging and Monitoring

SpendSense collects logs and monitoring data to track system performance and troubleshoot issues. Keycloak writes logs both to the console and to files, while Traefik runs with debug-level logging to capture detailed information. For monitoring, Prometheus collects metrics from services, and Grafana provides dashboards to visualize these metrics. To protect user privacy, it is recommended to ensure that any personal data is masked or excluded from logs and monitoring metrics. This helps prevent accidental exposure of sensitive information during troubleshooting or analysis.

##### Security Measures

SpendSense implements several important security measures to protect data and services. All communication is secured using HTTPS/TLS, managed by Traefik with custom certificates. The application uses network segmentation through the spendsense-net Docker network to isolate internal services and limit access. Role-based access control is handled by Keycloak to manage user permissions. Containers are isolated from each other using Docker’s built-in features and named networks. However, there is currently no rate limiting or web application firewall (WAF) configured, so it is recommended to consider adding middleware to protect against abuse or attacks.

# Recommendations

To improve data protection and follow GDPR rules, it is important to encrypt MySQL data stored on disk. There should be a clear policy explaining how long personal data is kept and how deletions are recorded. Adding features that let users download their personal data (export or portability) is also needed. Logs and monitoring data should be checked regularly to make sure no sensitive information is exposed. The process for deleting user data should be well documented and tested to ensure it works properly. Running security tests on the whole system can help find and fix weaknesses. Finally, using environment variables stored in a secure vault instead of plain-text passwords will better protect sensitive settings.

# Conclusion

While the SpendSense application demonstrates strong foundational practices in secure microservice architecture and uses tools like Keycloak and OAuth2 Proxy to handle user identity and access management, some GDPR-specific practices (like data export, consent logging, and at-rest encryption) should be improved for full compliance.