GDPR Compliance Scan Report

Repository: Unknown Repository

Scan Date:	2025-05-20 20:12:49 UTC
Scan ID:	repo_e4357668
Branch:	main
Report Generated:	2025-05-20 20:12:49

Executive Summary

This report presents the results of a GDPR compliance scan conducted on the repository. The scan analyzed 412 files out of a total of 469 files in the repository. The scan identified 36 instances of potential personal data or compliance issues: - 10 high-risk findings - 16 medium-risk findings - 10 low-risk findings Overall compliance score: -192/100

Overall Compliance Score	**-192/100**

Detailed Findings

High Risk Findings

Type	Location	Description
API_KEY	app/controllers/MessageSchedulerInventory.java (Line 55)	API key or credential detected. This may pose a security risk u
DATABASE_CREDENTIALS	lib/RequestRepositoryPermission.lua (Line 80)	Database credentials detected, posing potential security risks.
DATABASE_CREDENTIALS	lib/RequestRepositoryPermission.lua (Line 38)	Database credentials detected, posing potential security risks.
DATABASE_CREDENTIALS	lib/RequestRepositoryPermission.lua (Line 95)	Database credentials detected, posing potential security risks.
API_KEY	app/models/StorageHelper.java (Line 133)	API key or credential detected. This may pose a security risk u

Medium Risk Findings

Type	Location	Description
IP_ADDRESS	src/services/Profile.properties (Line 186)	IP address detected, which can be considered personal data u
IP_ADDRESS	src/services/Profile.properties (Line 25)	IP address detected, which can be considered personal data u
IP_ADDRESS	scripts/Password.java (Line 91)	IP address detected, which can be considered personal data u
IP_ADDRESS	scripts/Password.java (Line 27)	IP address detected, which can be considered personal data u
IP_ADDRESS	scripts/Password.java (Line 59)	IP address detected, which can be considered personal data u

CONFIGURATION	src/main/resources/Payment.java (Line 15)	Sensitive configuration data detected, which should be proper
CONFIGURATION	src/main/resources/Payment.java (Line 155)	Sensitive configuration data detected, which should be proper
CONFIGURATION	src/main/resources/Payment.java (Line 99)	Sensitive configuration data detected, which should be proper

Low Risk Findings

Type	Location	Description
NAME	src/main/java/ModelScheduler.java (Line 144)	Personal name detected, which constitutes personal data und
NAME	src/main/java/ModelScheduler.java (Line 74)	Personal name detected, which constitutes personal data und
NAME	src/test/java/Converter.jsx (Line 29)	Personal name detected, which constitutes personal data und
NAME	src/test/java/Converter.jsx (Line 185)	Personal name detected, which constitutes personal data und
NAME	app/models/EmailPaymentPassword.java (Line 60)	Personal name detected, which constitutes personal data und

GDPR Principles Analysis

GDPR Principle	Article	Status	Description
Lawfulness, Fairness and Transparency	Art. 5(1)(a)	✓ Compliant	Personal data must be processed lawfully, fairly and in a transpar
Purpose Limitation	Art. 5(1)(b)	✓ Compliant	Personal data must be collected for specified, explicit and legitima
Data Minimization	Art. 5(1)(c)	🟥 Affected	Personal data must be adequate, relevant and limited to what is n
Accuracy	Art. 5(1)(d)	✓ Compliant	Personal data must be accurate and kept up to date.
Storage Limitation	Art. 5(1)(e)	✓ Compliant	Personal data must be kept in a form which permits identification
Integrity and Confidentiality	Art. 5(1)(f)	🟥 Affected	Personal data must be processed in a secure manner.
Accountability	Art. 5(2)	✓ Compliant	The controller shall be responsible for, and be able to demonstrat

Recommendations for Compliance

- Use secure storage and transmission methods for all personal data.
- Implement data retention policies to ensure data is not stored longer than necessary.
- Implement proper data minimization techniques to ensure only necessary personal data is processed.
- Review and document the legal basis for all personal data processing activities.
- Add proper consent mechanisms before processing personal data.

Dutch GDPR (UAVG) Specific Compliance

✓ No Netherlands-specific GDPR compliance issues detected.

Requirement	Description	Relevant When

BSN Processing	The Dutch Citizen Service Number (BSN) may only be processed when explicitly authorized by law.	Processing government identity data
Medical Data	Medical data requires explicit consent and additional safeguards under UAVG Article 30.	Processing health-related information
Minors Consent	Consent for data processing for children under 16 must be given by parents/guardians.	Services targeting minors
Data Breach	The Dutch DPA (AP) requires notification within 72 hours for significant breaches.	Any data breach involving personal data