

DataGuardian Pro

GDPR Compliance Certification Report

Repository: java-design-patterns

Full Path: <https://github.com/iluwatar/java-design-patterns>

Scan Date:	2025-05-20 22:36:16 UTC
Scan ID:	repo_ac79c7b7
Branch:	main
Report Generated:	2025-05-20 22:36:17

Executive Summary

This report presents the results of a GDPR compliance scan conducted on the repository. The scan analyzed 387 files out of a total of 467 files in the repository. The scan identified 46 instances of potential personal data or compliance issues:

- 6 high-risk findings
- 28 medium-risk findings
- 12 low-risk findings

Overall GDPR Compliance Score



out of 100

Files Scanned	PII Instances	High Risk Findings
387	46	6

Requires Immediate Action

Detailed Findings

High Risk Findings

Type	Location	Description
DATABASE_CREDENTIALS	.../views/EmailControllerRole.sql (Line 139)	Database credentials detected, posing potential security risks.
PASSWORD	.../controllers/PasswordSessionMessageController.java (Line 167)	Password text detected. This is a security vulnerability.
CREDIT_CARD	app/views/Util.java (Line 138)	Credit card number detected. This is sensitive financial data.

Medium Risk Findings

Type	Location	Description
CONFIGURATION	lib/StorageService.html (Line 53)	Sensitive configuration data detected, which should be properly secured.
CONFIGURATION	lib/StorageService.html (Line 176)	Sensitive configuration data detected, which should be properly secured.
IP_ADDRESS	.../controllers/PasswordCustomerProfileController.java (Line 102)	IP address detected, which can be considered personal data under GDPR.
IP_ADDRESS	.../controllers/PasswordCustomerProfileController.java (Line 107)	IP address detected, which can be considered personal data under GDPR.
IP_ADDRESS	.../controllers/PasswordCustomerProfileController.java (Line 167)	IP address detected, which can be considered personal data under GDPR.
PHONE_NUMBER	app/controllers/Security.java (Line 13)	Phone number detected, which constitutes personal data under GDPR.
EMAIL	.../models/PasswordApiConverter.html (Line 110)	Email address pattern detected, which constitutes personal data under GDPR.
EMAIL	.../models/PasswordApiConverter.html (Line 55)	Email address pattern detected, which constitutes personal data under GDPR.
EMAIL	.../models/PasswordApiConverter.html (Line 103)	Email address pattern detected, which constitutes personal data under GDPR.
PHONE_NUMBER	lib/Formatter.java (Line 65)	Phone number detected, which constitutes personal data under GDPR.
PHONE_NUMBER	lib/Formatter.java (Line 109)	Phone number detected, which constitutes personal data under GDPR.
CONFIGURATION	scripts/MessageToken.sql (Line 65)	Sensitive configuration data detected, which should be properly secured.
ADDRESS	.../java/UtilRepository.css (Line 174)	Physical address detected, which constitutes personal data under GDPR.
ADDRESS	.../java/UtilRepository.css (Line 78)	Physical address detected, which constitutes personal data under GDPR.

Low Risk Findings

Type	Location	Description
NAME	.../resources/TaskProfileRepository.js (Line 187)	Person name detected, which constitutes personal data under GDPR.
NAME	.../resources/TaskProfileRepository.js (Line 187)	Person name detected, which constitutes personal data under GDPR.

NAME	src/services/Message.java (Line 23)	Personal name detected, which constitutes personal data under Art. 4(1).
NAME	config/Helper.java (Line 19)	Personal name detected, which constitutes personal data under Art. 4(1).
LOG_SETTINGS	app/views/Email.java (Line 23)	Logging configuration detected, which should be adjusted to meet GDPR requirements.

... and 1 more low-risk findings.

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 transparent manner.
Purpose Limitation	Art. 5(1)(b)	✓ Compliant	Personal data must be collected for specified, explicit and legitimate purposes.
Data Minimization	Art. 5(1)(c)	■ Affected	Personal data must be adequate, relevant and limited to what is necessary for the purposes.
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 for no longer than is necessary.
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 demonstrate, compliance with the principles.

Recommendations for Compliance

- Implement data retention policies to ensure data is not stored longer than necessary.
- Use secure storage and transmission methods for all personal data.
- 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.

Dutch GDPR (UAVG) Requirements

Requirement	Description	Legal Basis
BSN Processing	Dutch Citizen Service Number (BSN) may only be processed where explicitly authorized by law.	UAVG Article 46
Medical Data	Medical data requires explicit consent and additional safeguards.	UAVG Article 30

Minors Consent	Parental consent required for children under 16 years (higher than Article 45 countries).	UN Convention
Data Breach	The Dutch DPA (AP) requires notification within 72 hours for significant breaches.	GDPR Article 33