

Code Audit Report

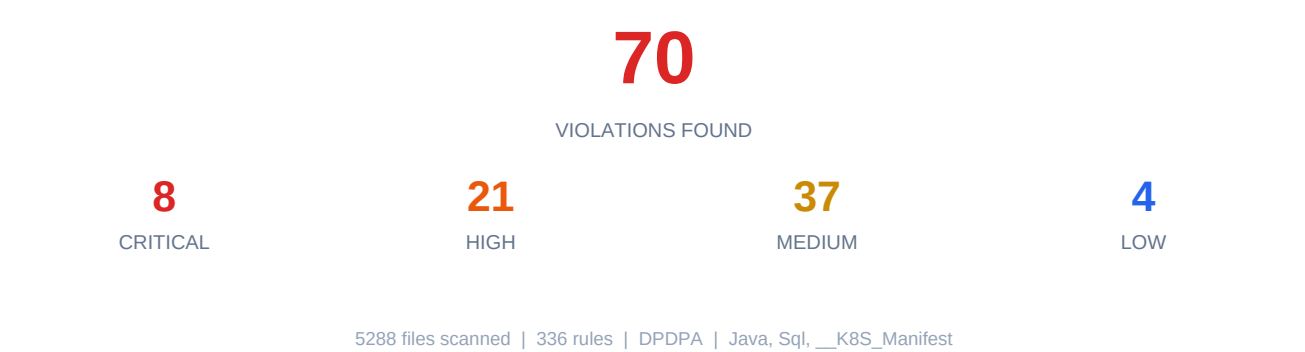
What the code does with regulated data · which controls it fails

SCRUTORA

Finract Demo

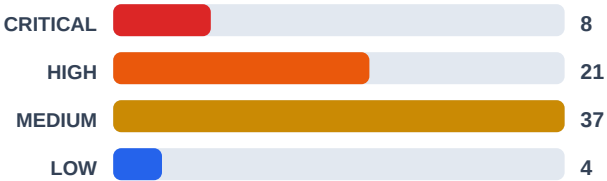
Nirvahana/fineract@develop

Generated 2026-08-20 09:27 UTC · Frameworks: DPDPA



Executive Summary

This report presents the results of an automated DPDPA compliance scan of **Nirvahana/fineract@develop**, completed on August 20, 2026. The scan analysed **5288 file(s)**, inspected **1559015 code entities**, and identified **70 violation(s)**.



Comparison with Previous Scan

Violations: 70 → 70 (0 same)

Violation Breakdown by Severity

Severity	Count	What this severity means
CRITICAL	8	Sensitive data directly exposed or unprotected
HIGH	21	Significant exposure of personal data or access control
MEDIUM	37	Control weakness with limited or indirect exposure
LOW	4	Hygiene or defence-in-depth gap
TOTAL	70	

Finding Confidence Classification

Confidence	Count	Meaning
Confirmed	16	High-certainty finding based on strong code evidence
Likely	23	Probable finding; static analysis cannot fully confirm
Needs Review	10	Possible finding requiring manual verification

The table above shows **49 unique finding(s)** after grouping similar violations that appear across multiple files. The severity breakdown counts all **70 individual occurrence(s)** before grouping.

Risk Assessment

Risk Dimension	Score	Rating	Description
----------------	-------	--------	-------------

Inherent Risk	100	High	Severity-weighted exposure before controls
Control Maturity	95%	Low	223/243 safeguards passing
Residual Risk	50	High	Remaining exposure after current controls

Reading these together: Control maturity and coverage measure *breadth* — the share of distinct safeguards implemented — and are high because most controls are in place. They count controls, not consequences: under the DPDPA an exploitable exposure of personal data is a reportable personal-data breach, so a single unresolved CRITICAL finding matters out of all proportion to its share of the control set. Both readings are true — broad coverage, with specific high-severity findings outstanding. Which of those governs your release decision is a call for your assessor, not this report.

Compliance Strengths

● **223 of 243** evaluated safeguards have no Confirmed or Likely violations | **99%** of scanned files are clean | **10** safeguards have Likely-band findings that require attention

Key Statistics

Files Scanned	Files Excluded	Entities Checked	Rules Executed	Scan Duration
5288	1906	1559015	336	952.2s

Critical Findings

- **[PCI-4.1.1]** TLS certificate verification disabled (X509TrustManager()) -- enables man-in-the-middle attacks on cardholder data (2 occurrences) (fineract-client-feign/src/main/java/org/apache/fineract/client/feign/FineractFeignClientConfig.java:177)
- **[PCI-4.1.1]** TLS certificate verification disabled (X509TrustManager()) -- enables man-in-the-middle attacks on cardholder data (fineract-client/src/main/java/org/apache/fineract/client/util/FineractClient.java:514)
- **[INPUT-001]** SQL query constructed via string concatenation/interpolation in DatatableReadServiceImpl.queryDataTableAdvanced. This is vulnerable to SQL injection attacks.
(fineract-provider/src/main/java/org/apache/fineract/infrastructure/dataqueries/service/DatatableReadServiceImpl.java:202 — queryDataTableAdvanced)
- **[INPUT-001]** SQL query constructed via string concatenation/interpolation in DatatableWriteServiceImpl.deleteDatatable. This is vulnerable to SQL injection attacks.
(fineract-provider/src/main/java/org/apache/fineract/infrastructure/dataqueries/service/DatatableWriteServiceImpl.java:536 — deleteDatatable)
- **[INPUT-001]** SQL query constructed via string concatenation/interpolation in GenericDataServiceImpl.wrapSQL. This is vulnerable to SQL injection attacks.
(fineract-provider/src/main/java/org/apache/fineract/infrastructure/dataqueries/service/GenericDataServiceImpl.java:228 — wrapSQL)
- **[INPUT-001]** SQL query constructed via string concatenation/interpolation in SavingsAccountTransactionsSearchServiceImpl.searchTransactions. This is vulnerable to SQL injection attacks.
(fineract-provider/src/main/java/org/apache/fineract/portfolio/savings/service/search/SavingsAccountTransactionsSearchServiceImpl.java:117 —

searchTransactions)

Detailed Findings

The following 49 finding(s) (consolidated from 70 total occurrences) are ordered by severity. Each card shows the offending code, root-cause analysis, and step-by-step remediation with penalty context.

#1 CRITICAL — PCI-4.1.1 [Confirmed] [Java]	
fineract-client-feign/src/main/java/org/apache/fineract/client/feign/FineractFeignClientConfig.java:177	
Applies to: [DPDPA] §8(5)	
Compliance Ref	DPDPA: §8(5)
Source	https://www.meity.gov.in/content/digital-personal-data-protection-act-2023
Location	fineract-client-feign/src/main/java/org/apache/fineract/client/feign/FineractFeignClientConfig.java:177
Method	Global scope
Operation	General
Confidence	Confirmed (90%)
Est. Fix Time	30-60 min
Complexity	MED Medium
Language	Java

■ **Finding:** TLS certificate verification disabled (X509TrustManager()) -- enables man-in-the-middle attacks on cardholder data (2 occurrences)

Why this matters: May indicate non-compliance with DPDPA requirements. Review this finding against your organization's compliance obligations.

Offending Code

177	private X509TrustManager createTrustAllManager() {
178	return new X509TrustManager() {
179	
180	@Override
181	private SSLContext createTrustAllSslContext() throws Exception {
182	TrustManager[] trustAllCerts = new TrustManager[] { createTrustAllManager() };
183	
184	SSLContext sslContext = SSLContext.getInstance("TLS");

Remediation

Enable TLS certificate verification. In Python: verify=True (default). In Go: remove InsecureSkipVerify. In Node.js: rejectUnauthorized=true. Use proper CA certificates instead of disabling validation.

#2 CRITICAL — PCI-4.1.1 [Confirmed] [Java]

fineract-client/src/main/java/org/apache/fineract/client/util/FineractClient.java:514

Applies to: [DPDPA] §8(5)

Compliance Ref	DPDPA: §8(5)
Source	https://www.meity.gov.in/content/digital-personal-data-protection-act-2023
Location	fineract-client/src/main/java/org/apache/fineract/client/util/FineractClient.java:514
Method	Global scope
Operation	General
Confidence	Confirmed (90%)
Est. Fix Time	30-60 min
Complexity	MED Medium
Language	Java

■ **Finding:** TLS certificate verification disabled (X509TrustManager()) -- enables man-in-the-middle attacks on cardholder data

Why this matters: May indicate non-compliance with DPDPA requirements. Review this finding against your organization's compliance obligations.

Offending Code

```
514
515 try {
516     X509TrustManager insecureX509TrustManager = new X509TrustManager() {
517
518     @Override
```

Remediation

Enable TLS certificate verification. In Python: verify=True (default). In Go: remove InsecureSkipVerify. In Node.js: rejectUnauthorized=true. Use proper CA certificates instead of disabling validation.

#3 CRITICAL — INPUT-001 [Likely] [Java]

fineract-provider/src/main/java/org/apache/fineract/infrastructure/dataqueries/service/DatatableReadServiceImpl.java:202

Applies to: [DPDPA] §8(5)

Compliance Ref	DPDPA: §8(5)
Source	https://www.meity.gov.in/content/digital-personal-data-protection-act-2023
Location	fineract-provider/src/main/java/org/apache/fineract/infrastructure/dataqueries/service/DatatableReadServiceImpl.java:202
Method	DatatableReadServiceImpl.queryDataTableAdvanced
Operation	General
Confidence	Likely (84%)
Est. Fix Time	30-60 min
Complexity	MED Medium
Language	Java

■ **Finding:** SQL query constructed via string concatenation/interpolation in `DatatableReadServiceImpl.queryDataTableAdvanced`. This is vulnerable to SQL injection attacks.

Why this matters: May indicate non-compliance with DPDPA requirements. Review this finding against your organization's compliance obligations.

Offending Code

```
202 String countQuery = "SELECT COUNT(*)" + from + where;
```

Remediation

Use parameterized queries instead of string concatenation. Python: `cursor.execute('SELECT * FROM users WHERE id = %s', (user_id,))`. JS: `connection.query('SELECT * FROM users WHERE id = ?', [userId])`. Java: use `PreparedStatement` with `?` placeholders.

#4 CRITICAL — INPUT-001 [Likely] [Java]

fineract-provider/src/main/java/org/apache/fineract/infrastructure/dataqueries/service/DatatableWriteServiceImpl.java:536

Applies to: [DPDPA] §8(5)

Compliance Ref	DPDPA: §8(5)
Source	https://www.meity.gov.in/content/digital-personal-data-protection-act-2023
Location	fineract-provider/src/main/java/org/apache/fineract/infrastructure/dataqueries/service/DatatableWriteServiceImpl.java:536
Method	DatatableWriteServiceImpl.deleteDatatable
Operation	General
Confidence	Likely (75%)
Est. Fix Time	30-60 min
Complexity	MED Medium
Language	Java

■ **Finding:** SQL query constructed via string concatenation/interpolation in DatatableWriteServiceImpl.deleteDatatable. This is vulnerable to SQL injection attacks.

Why this matters: May indicate non-compliance with DPDPA requirements. Review this finding against your organization's compliance obligations.

Offending Code

536	final String deleteColumnCodeSql = "delete from x_table_column_code_mappings where column_alias_name like'" + datatab...
-----	--

Remediation

Use parameterized queries instead of string concatenation. Python: cursor.execute('SELECT * FROM users WHERE id = %s', (user_id,)). JS: connection.query('SELECT * FROM users WHERE id = ?', [userId]). Java: use PreparedStatement with ? placeholders.

#5 CRITICAL — INPUT-001 [Likely] [Java]

```
fineract-provider/src/main/java/org/apache/fineract/infrastructure/dataqueries/service/GenericDataServiceImpl.java:228
```

Applies to: [DPDPA] §8(5)

Compliance Ref	DPDPA: §8(5)
Source	https://www.meity.gov.in/content/digital-personal-data-protection-act-2023
Location	fineract-provider/src/main/java/org/apache/fineract/infrastructure/dataqueries/service/GenericDataServiceImpl.java:228
Method	GenericDataServiceImpl.wrapSQL
Operation	General
Confidence	Likely (75%)
Est. Fix Time	30-60 min
Complexity	MED Medium
Language	Java

■ **Finding:** SQL query constructed via string concatenation/interpolation in GenericDataServiceImpl.wrapSQL. This is vulnerable to SQL injection attacks.

Why this matters: May indicate non-compliance with DPDPA requirements. Review this finding against your organization's compliance obligations.

Offending Code

```
228 return "select x.* from (" + sql + ") x";
```

Remediation

Use parameterized queries instead of string concatenation. Python: `cursor.execute('SELECT * FROM users WHERE id = %s', (user_id,))`. JS: `connection.query('SELECT * FROM users WHERE id = ?', [userId])`. Java: use PreparedStatement with ? placeholders.

#6 CRITICAL — INPUT-001 [Likely] [Java]

```
finract-provider/src/main/java/org/apache/finract/portfolio/savings/service/search/SavingsAccountTransactionsSearchServiceImpl.java:117
```

Applies to: [DPDPA] §8(5)

Compliance Ref	DPDPA: §8(5)
Source	https://www.meity.gov.in/content/digital-personal-data-protection-act-2023
Location	finract-provider/src/main/java/org/apache/finract/portfolio/savings/service/search/SavingsAccountTransactionsSearchServiceImpl.java:117
Method	SavingsAccountTransactionsSearchServiceImpl.searchTransactions
Operation	General
Confidence	Likely (84%)
Est. Fix Time	30-60 min
Complexity	MED Medium
Language	Java

■ **Finding:** SQL query constructed via string concatenation/interpolation in SavingsAccountTransactionsSearchServiceImpl.searchTransactions. This is vulnerable to SQL injection attacks.

Why this matters: May indicate non-compliance with DPDPA requirements. Review this finding against your organization's compliance obligations.

Offending Code

```
117 String countQuery = "SELECT COUNT(*) " + tm.from() + where;
```

Remediation

Use parameterized queries instead of string concatenation. Python: `cursor.execute('SELECT * FROM users WHERE id = %s', (user_id,))`. JS: `connection.query('SELECT * FROM users WHERE id = ?', [userId])`. Java: use PreparedStatement with ? placeholders.

#7 CRITICAL — INPUT-001 [Likely] [Java]

```
fineract-provider/src/main/java/org/apache/fineract/portfolio/savings/service/search/SavingsAccountTransactionsSearchServiceImpl.java:269
```

Applies to: [DPDPA] §8(5)

Compliance Ref	DPDPA: §8(5)
Source	https://www.meity.gov.in/content/digital-personal-data-protection-act-2023
Location	fineract-provider/src/main/java/org/apache/fineract/portfolio/savings/service/search/SavingsAccountTransactionsSearchServiceImpl.java:269
Method	SavingsAccountTransactionsSearchServiceImpl.queryAdvanced
Operation	General
Confidence	Likely (84%)
Est. Fix Time	30-60 min
Complexity	MED Medium
Language	Java

■ **Finding:** SQL query constructed via string concatenation/interpolation in SavingsAccountTransactionsSearchServiceImpl.queryAdvanced. This is vulnerable to SQL injection attacks.

Why this matters: May indicate non-compliance with DPDPA requirements. Review this finding against your organization's compliance obligations.

Offending Code

```
269 String countQuery = "SELECT COUNT(*)" + from + where;
```

Remediation

Use parameterized queries instead of string concatenation. Python: `cursor.execute('SELECT * FROM users WHERE id = %s', (user_id,))`. JS: `connection.query('SELECT * FROM users WHERE id = ?', [userId])`. Java: use PreparedStatement with ? placeholders.

#8 HIGH — TRANSFER-001 [Confirmed] [Java]

fineract-client-feign/src/main/java/org/apache/fineract/client/feign/FineractFeignClientConfig.java:194

Applies to: [DPDPA] §16(1)

Compliance Ref	DPDPA: §16(1)
Source	https://www.meity.gov.in/content/digital-personal-data-protection-act-2023
Location	fineract-client-feign/src/main/java/org/apache/fineract/client/feign/FineractFeignClientConfig.java:194
Method	Global scope
Operation	General
Confidence	Confirmed (85%)
Est. Fix Time	30-60 min
Complexity	MED Medium
Language	Java

■ Finding: Insecure SSL/TLS configuration — certificate verification disabled (2 occurrences)

Why this matters: DPDPA §16 restricts transfer of personal data outside India to countries notified by the Central Government. Unauthorized cross-border transfers may result in significant penalties.

Offending Code

```
194 TrustManager[] trustAllCerts = new TrustManager[] { createTrustAllManager() };
195 sslContext.init(null, trustAllCerts, new java.security.SecureRandom());
```

Remediation

Do not disable SSL certificate verification. This allows man-in-the-middle attacks on data transfers. Remove verify=False, rejectUnauthorized: false, or similar certificate bypass settings.

#9 HIGH — NOTICE-001 [Likely] [Java]

fineract-db/old-schema-files/0002-mifosx-base-reference-data-utf8.sql:291

Applies to: [DPDPA] §5(1)

Compliance Ref	DPDPA: §5(1)
Source	https://www.meity.gov.in/content/digital-personal-data-protection-act-2023
Location	fineract-db/old-schema-files/0002-mifosx-base-reference-data-utf8.sql:291
Method	Global scope
Operation	General
Confidence	Likely (70%)
Est. Fix Time	30-60 min
Complexity	MED Medium
Language	Java

■ **Finding:** Strong PII ('Passport') collected in a project with no notice artefact (no /privacy or /notice route, NOTICE_URL config, or privacy-notice surface). DPDPA §5(1) requires the notice to accompany or precede the consent request.

Why this matters: May indicate non-compliance with DPDPA requirements. Review this finding against your organization's compliance obligations.

Offending Code

291	select mc.id, 'Passport', 1
-----	-----------------------------

Remediation

Add a /privacy or /notice surface (or NOTICE_URL) returning the §5(1) notice, linked from the signup flow.

#10 HIGH — STORE-001 [Likely] [Java]

```
fineract-loan/src/main/java/org/apache/fineract/portfolio/loanaccount/service/GLIMAccountInfoWritePlatformServiceImpl.java:40
```

✓ **Data-flow confirmed** — taint analysis traced a real source→sink path (3-step trace); highest-confidence finding.

Applies to: **[DPDPA]** §8(5)

Compliance Ref	DPDPA: §8(5)
Source	https://www.meity.gov.in/content/digital-personal-data-protection-act-2023
Location	fineract-loan/src/main/java/org/apache/fineract/portfolio/loanaccount/service/GLIMAccountInfoWritePlatformServiceImpl.java:40
Method	createGLIMAccount
Operation	General
Confidence	Likely (80%)
Est. Fix Time	2-4 hours
Complexity	MED Medium
Language	Java

■ **Finding:** Sensitive data flows from pii field access at line 33 to storage at line 40 without encryption. Note: ORM storage operations are commonly backed by database-level encryption at rest

Why this matters: DPDPA §8(5) requires reasonable security safeguards including encryption of personal data at rest. Unencrypted storage increases breach severity and may lead to penalties under §33.

Offending Code

```
40  Data Flow Trace (STORE-001):
41  Line 33 → parameter: accountNumber [SOURCE: accountNumber]
42  Line 37 → GroupLoanIndividualMonitoringAccount glimAccountInfo =
    GroupLoanIndividualMonitoringAccount.getInstanc...
43  Line 40 → return this.glimAccountRepository.save(glimAccountInfo); [SINK: accountNumber]
```

Remediation

Encrypt accountNumber before writing to storage at line 40. Use AES-256-GCM for symmetric encryption or bcrypt/Argon2 for passwords. Note: if your database uses encryption at rest (e.g., AWS RDS, Azure SQL TDE, GCP Cloud SQL), this finding may already be mitigated at the infrastructure level.

Current Code (Before)

```
1  // Current: personal data written without verified encryption
2  Data Flow Trace (STORE-001):
```

Fixed Code (After)

```
1  // Option A: JPA @Convert with encryption
2  @Convert(converter = PHIEncryptor.class)
```

```
3 private String STORE;  
4  
5 // Option B: Hibernate @ColumnTransformer  
6 @ColumnTransformer(  
7   read = "pgp_sym_decrypt(STORE, 'key')",  
8   write = "pgp_sym_encrypt(?, 'key')")
```

#11 HIGH — PII-001 [Needs Review] [Java]

fineract-provider/src/main/java/org/apache/fineract/infrastructure/security/service/OidcAppUserResolutionServiceImpl.java:71

✓ **Data-flow confirmed** — taint analysis traced a real source→sink path (4-step trace); highest-confidence finding.

Applies to: **[DPDPA]** §6(1), §8(5)

Compliance Ref	DPDPA: §6(1), §8(5)
Source	https://www.meity.gov.in/content/digital-personal-data-protection-act-2023
Location	fineract-provider/src/main/java/org/apache/fineract/infrastructure/security/service/OidcAppUserResolutionServiceImpl.java:71
Method	resolveOrCreate
Operation	General
Confidence	Needs Review (55%)
Est. Fix Time	30-60 min
Complexity	MED Medium
Language	Java

■ **Finding:** PII flows from pii field access at line 56 to log statement at line 71 without masking

Manual Review Recommended This finding has lower certainty due to limitations of static analysis. Verify whether the identified pattern constitutes an actual compliance violation in your deployment environment.

Why this matters: DPDPA §4(2) limits processing to stated purposes. Personal data in logs exceeds the stated purpose of processing and may constitute uncontrolled disclosure.

Offending Code

71	Data Flow Trace (PII-001):
72	Line 56 → parameter: email [SOURCE: email]
73	Line 61 → AppUser user = appUserRepository.findAppUserByName(username); [PROPAGATION: user]
74	Line 69 → user = appUserRepository.findActiveUserByEmail(email); [PROPAGATION: user]
75	Line 71 → log.debug("OIDC user resolved by email: '{}'", email); [SINK: email]

Remediation

Mask or redact email before logging. Replace the log statement at line 71 with a version that masks PII fields: e.g., `maskEmail(user.email)` or `redact(data, ['email', 'phone'])`.

#12 HIGH — STORE-001 [Likely] [Java]

```
finract-provider/src/main/java/org/apache/finract/infrastructure/security/service/TwoFactorServiceImpl.java:104
```

✓ **Data-flow confirmed** — taint analysis traced a real source→sink path (6-step trace); highest-confidence finding.

Applies to: **[DPDPA]** §8(5)

Compliance Ref	DPDPA: §8(5)
Source	https://www.meity.gov.in/content/digital-personal-data-protection-act-2023
Location	finract-provider/src/main/java/org/apache/finract/infrastructure/security/service/TwoFactorServiceImpl.java:104
Method	createNewOTPToken
Operation	General
Confidence	Likely (80%)
Est. Fix Time	2-4 hours
Complexity	MED Medium
Language	Java

■ **Finding:** Sensitive data flows from pii field access at line 93 to storage at line 104 without encryption. Note: ORM storage operations are commonly backed by database-level encryption at rest

Why this matters: DPDPA §8(5) requires reasonable security safeguards including encryption of personal data at rest. Unencrypted storage increases breach severity and may lead to penalties under §33.

Offending Code

```
104 Data Flow Trace (STORE-001):
105 Line 93 → parameter: user: AppUser [SOURCE: user]
106 Line 96 → OTPDeliveryMethod smsDelivery = getSMSDeliveryMethodForUser(user); [PROPAGATION: smsDelivery]
107 Line 100 → final OTPRequest request = generateNewToken(smsDelivery, extendedAccessToken); [PROPAGATION: request]
108 Line 101 → final String smsText = configurationService.getFormattedSmsTextFor(user, request); [PROPAGATION: smsText]
109 Line 102 → SmsMessage smsMessage = SmsMessage.pendingSms(null, null, null, user.getStaff(), smsText, user.getStaff())
110 Line 104 → this.smsMessageRepository.save(smsMessage); [SINK: user]
```

Remediation

Encrypt cannot_change_password, email, firstname before writing to storage at line 104. Use AES-256-GCM for symmetric encryption or bcrypt/Argon2 for passwords. Note: if your database uses encryption at rest (e.g., AWS RDS, Azure SQL TDE, GCP Cloud SQL), this finding may already be mitigated at the infrastructure level.

Current Code (Before)

```
1 // Current: personal data written without verified encryption
2 Data Flow Trace (STORE-001):
```

Fixed Code (After)

```
1 // Option A: JPA @Convert with encryption
2 @Convert(converter = PHIEncryptor.class)
3 private String STORE;
4
5 // Option B: Hibernate @ColumnTransformer
6 @ColumnTransformer(
7   read = "pgp_sym_decrypt(STORE, 'key')",
8   write = "pgp_sym_encrypt(?, 'key')")
```

#13 HIGH — STORE-001 [Likely] [Java]

finract-provider/src/main/java/org/apache/finract/infrastructure/security/service/TwoFactorServiceImpl.java:146

✓ **Data-flow confirmed** — taint analysis traced a real source→sink path (9-step trace); highest-confidence finding.

Applies to: **[DPDPA]** §8(5)

Compliance Ref	DPDPA: §8(5)
Source	https://www.meity.gov.in/content/digital-personal-data-protection-act-2023
Location	finract-provider/src/main/java/org/apache/finract/infrastructure/security/service/TwoFactorServiceImpl.java:146
Method	createAccessTokenFromOTP
Operation	General
Confidence	Likely (80%)
Est. Fix Time	2-4 hours
Complexity	MED Medium
Language	Java

■ **Finding:** Sensitive data flows from pii field access at line 126 to storage at line 146 without encryption. Note: ORM storage operations are commonly backed by database-level encryption at rest

Why this matters: DPDPA §8(5) requires reasonable security safeguards including encryption of personal data at rest. Unencrypted storage increases breach severity and may lead to penalties under §33.

Offending Code

```
146 Data Flow Trace (STORE-001):
147 Line 126 → parameter: user: AppUser [SOURCE: user]
148 Line 131 → OTPRequest otpRequest = otpRequestRepository.getOTPRequestForUser(user); [PROPAGATION:
otpRequest]
149 Line 136 → otpRequestRepository.deleteOTPRequestForUser(user); [CALL: ]
150 Line 47 → → enters OTPRequestRepository.deleteOTPRequestForUser() [CROSS_FILE_CALL:
deleteOTPRequestForUser]
151 Line 138 → String token = accessTokenGenerationService.generateRandomToken(); [PROPAGATION: token]
152 Line 139 → int liveTime; [PROPAGATION: liveTime]
153 Line 141 → liveTime = configurationService.getAccessTokenExtendedLiveTime(); [PROPAGATION: liveTime]
154 Line 145 → TFAccessToken accessToken = TFAccessToken.create(token, user, liveTime); [PROPAGATION:
accessToken]
155 Line 146 → tfAccessTokenRepository.save(accessToken); [SINK: user]
```

Remediation

Encrypt cannot_change_password, email, firstname before writing to storage at line 146. Use AES-256-GCM for symmetric encryption or bcrypt/Argon2 for passwords. Note: if your database uses encryption at rest (e.g., AWS RDS, Azure SQL TDE, GCP Cloud SQL), this finding may already be mitigated at the infrastructure level.

Current Code (Before)

1	// Current: personal data written without verified encryption
2	Data Flow Trace (STORE-001):

Fixed Code (After)

1	// Option A: JPA @Convert with encryption
2	@Convert(converter = PHIEncryptor.class)
3	private String STORE;
4	
5	// Option B: Hibernate @ColumnTransformer
6	@ColumnTransformer(
7	read = "pgp_sym_decrypt(STORE, 'key')",
8	write = "pgp_sym_encrypt(?, 'key')")

#14 HIGH — STORE-001 [Likely] [Java]

fineract-provider/src/main/java/org/apache/fineract/infrastructure/security/service/TwoFactorServiceImpl.java:172

✓ **Data-flow confirmed** — taint analysis traced a real source→sink path (6-step trace); highest-confidence finding.

Applies to: **[DPDPA]** §8(5)

This card summarises 9 occurrence(s) across 7 file(s). The 3 most severe occurrences are shown as individual cards above.

All 9 Occurrence(s) across 7 file(s)

File	Line	Method	Conf.
fineract-loan/src/main/java/org/apache/fineract/portfolio/loanaccount/service/GLIMAccountInfoWritePlatformServiceImpl.java	40	createGLIMAccount	Likely
fineract-provider/src/main/java/org/apache/fineract/infrastructure/accountnumberformat/domain/AccountNumberFormatRepositoryWrapper.java	45	save	Needs Review
fineract-provider/src/main/java/org/apache/fineract/infrastructure/security/service/TwoFactorServiceImpl.java	104	createNewOTPToken	Likely
fineract-provider/src/main/java/org/apache/fineract/infrastructure/security/service/TwoFactorServiceImpl.java	146	createAccessTokenFromOTP	Likely
fineract-provider/src/main/java/org/apache/fineract/infrastructure/security/service/TwoFactorServiceImpl.java	172	invalidateAccessToken	Likely
fineract-provider/src/main/java/org/apache/fineract/portfolio/client/domain/ClientRepositoryWrapper.java	62	save	Likely
fineract-provider/src/main/java/org/apache/fineract/portfolio/client/service/ClientWritePlatformServiceJpaRepositoryImpl.java	402	extractAndCreateClientNonPerson	Likely
fineract-provider/src/main/java/org/apache/fineract/portfolio/savings/service/GroupSavingsIndividualMonitoringWritePlatformServiceImpl.java	47	addGSIMAccountInfo	Likely
fineract-provider/src/main/java/org/apache/fineract/useradministration/domain/JpaUserDomainService.java	62	generateKeyUsedForPasswordSalting	Likely
Compliance Ref	DPDPA: §8(5)		
Source	https://www.meity.gov.in/content/digital-personal-data-protection-act-2023		
Location	fineract-provider/src/main/java/org/apache/fineract/infrastructure/security/service/TwoFactorServiceImpl.java:172		
Method	invalidateAccessToken		

Operation	General
Confidence	Likely (80%)
Est. Fix Time	2-4 hours
Complexity	MED Medium
Language	Java

■ **Finding:** Sensitive data flows from pii field access at line 159 to storage at line 172 without encryption. Note: ORM storage operations are commonly backed by database-level encryption at rest (+6 more across 6 file(s): AccountNumberFormatRepositoryWrapper.java, TwoFactorServiceImpl.java, ClientRepositoryWrapper.java, ClientWritePlatformServiceJpaRepositoryImpl.java, GroupSavingsIndividualMonitoringWritePlatformServiceImpl.java, ... +1 more)

Why this matters: DPDPA §8(5) requires reasonable security safeguards including encryption of personal data at rest. Unencrypted storage increases breach severity and may lead to penalties under §33.

Offending Code

172	Data Flow Trace (STORE-001):
173	Line 159 → parameter: user: AppUser [SOURCE: user]
174	Line 164 → final String token = command.stringValueOfParameterNamed("token"); [PROPAGATION: token]
175	Line 165 → final TFAccessToken accessToken = fetchAccessTokenForUser(user, token); [PROPAGATION: accessToken]
176	Line 171 → accessToken.setEnabled(false); [CALL:]
177	Line 43 → → enters ExternalEventConfiguration.setEnabled() [CROSS_FILE_CALL: setEnabled]
178	Line 172 → tfAccessTokenRepository.save(accessToken); [SINK: user]

Remediation

Encrypt cannot_change_password, email, firstname before writing to storage at line 172. Use AES-256-GCM for symmetric encryption or bcrypt/Argon2 for passwords. Note: if your database uses encryption at rest (e.g., AWS RDS, Azure SQL TDE, GCP Cloud SQL), this finding may already be mitigated at the infrastructure level.

Current Code (Before)

1	// Current: personal data written without verified encryption
2	Data Flow Trace (STORE-001):

Fixed Code (After)

1	// Option A: JPA @Convert with encryption
2	@Convert(converter = PHIEncryptor.class)
3	private String STORE;
4	
5	// Option B: Hibernate @ColumnTransformer
6	@ColumnTransformer(
7	read = "pgp_sym_decrypt(STORE, 'key')",
8	write = "pgp_sym_encrypt(?, 'key')")

Shared Remediation — applies to all 9 occurrence(s)

Encrypt cannot_change_password, email, firstname before writing to storage at line 172. Use AES-256-GCM for symmetric encryption or bcrypt/Argon2 for passwords. Note: if your database uses encryption at rest (e.g., AWS RDS, Azure SQL TDE, GCP Cloud SQL), this finding may already be mitigated at the infrastructure level.

#15 HIGH — AUTH-001 [Likely] [Java]

fineract-provider/src/main/java/org/apache/fineract/organisation/staff/api/StaffApiResource.java:102

Applies to: [DPDPA] §8(5)

Compliance Ref	DPDPA: §8(5)
Source	https://www.meity.gov.in/content/digital-personal-data-protection-act-2023
Location	fineract-provider/src/main/java/org/apache/fineract/organisation/staff/api/StaffApiResource.java:102
Method	StaffApiResource.retrieveOne
Operation	General
Confidence	Likely (75%)
Est. Fix Time	4-8 hours
Complexity	HIGH High
Language	Java

■ **Finding:** Method 'retrieveOne' in controller class 'StaffApiResource' accesses PHI without an authorization or access-control check.

Why this matters: DPDPA §8(5) requires Data Fiduciaries to implement reasonable security safeguards including access controls. Missing access controls may result in penalties up to ₹250 crore under §33.

Offending Code

```
102 @GET
103 @Path("/{staffId}")
104 @Operation(summary = "Retrieve a Staff Member", operationId = "retrieveOneStaff", description = ""
105 Returns the details of a Staff Member.
106
107 Example Requests:
108
109 - /staff/1
110 "")
111 @AlternativeOperationId("retrieveOne_8")
112 public StaffData retrieveOne(@PathParam("staffId") @Parameter(description = "staffId") final Long staffId,
113 @DefaultValue("false") @QueryParam("template") @Parameter(description = "temp
```

Remediation

Add @PreAuthorize or @Secured to 'retrieveOne': @PreAuthorize("hasRole('DOCTOR') or hasRole('NURSE')") public T retrieveOne(..) { ... } Or apply @Secured at class level on StaffApiResource. Record every PHI access in an audit trail.

Current Code (Before)

```
1 // Before: no access control check
2 @GetMapping("/patient/{id}")
3 public Patient getPatient(@PathVariable Long id) {
```

```
4   return repository.findById(id);  
5   }
```

Fixed Code (After)

```
1   // After: verify authorization before access  
2   @PreAuthorize("hasRole('PROVIDER')")  
3   @GetMapping("/patient/{id}")  
4   public Patient getPatient(@PathVariable Long id) {  
5       return repository.findById(id);  
6   }
```

#16 HIGH — PII-001 [Needs Review] [Java]

fineract-provider/src/main/java/org/apache/fineract/useradministration/service/ForgotPasswordServiceImpl.java:50

✓ **Data-flow confirmed** — taint analysis traced a real source→sink path (3-step trace); highest-confidence finding.

Applies to: **[DPDPA]** §6(1), §8(5)

Compliance Ref	DPDPA: §6(1), §8(5)
Source	https://www.meity.gov.in/content/digital-personal-data-protection-act-2023
Location	fineract-provider/src/main/java/org/apache/fineract/useradministration/service/ForgotPasswordServiceImpl.java:50
Method	requestPasswordReset
Operation	General
Confidence	Needs Review (55%)
Est. Fix Time	30-60 min
Complexity	MED Medium
Language	Java

■ **Finding:** PII flows from pii field access at line 45 to log statement at line 50 without masking

Manual Review Recommended This finding has lower certainty due to limitations of static analysis. Verify whether the identified pattern constitutes an actual compliance violation in your deployment environment.

Why this matters: DPDPA §4(2) limits processing to stated purposes. Personal data in logs exceeds the stated purpose of processing and may constitute uncontrolled disclosure.

Offending Code

50	Data Flow Trace (PII-001):
51	Line 45 → parameter: email [SOURCE: email]
52	Line 48 → final AppUser user = this.appUserRepository.findActiveUserByEmail(email); [PROPAGATION: user]
53	Line 50 → log.debug("Password reset requested for non-existent or inactive email: {}", email); [SINK: email]

Remediation

Mask or redact email before logging. Replace the log statement at line 50 with a version that masks PII fields: e.g., `maskEmail(user.email)` or `redact(data, ['email', 'phone'])`.

#17 HIGH — PII-002 [Needs Review] [Java]	
fineract-security/src/main/java/org/apache/fineract/infrastructure/security/api/AuthenticationApiResource.java:96	
Applies to: [DPDPA] §8(5)	
Compliance Ref	DPDPA: §8(5)
Source	https://www.meity.gov.in/content/digital-personal-data-protection-act-2023
Location	fineract-security/src/main/java/org/apache/fineract/infrastructure/security/api/AuthenticationApiResource.java:96
Method	AuthenticationApiResource.authenticate
Operation	General
Confidence	Needs Review (55%)
Est. Fix Time	30-60 min
Complexity	MED Medium
Language	Java

■ **Finding:** PII field 'username' exposed in error response in AuthenticationApiResource.authenticate

Manual Review Recommended This finding has lower certainty due to limitations of static analysis. Verify whether the identified pattern constitutes an actual compliance violation in your deployment environment.

Why this matters: DPDPA §8(5) requires reasonable security safeguards. Exposing personal data in error responses violates confidentiality requirements and may be intercepted by intermediaries.

Offending Code

96	throw new IllegalArgumentException("Username or Password is null in JSON (see FINERACT-726) of POST to /authentication...
----	---

Remediation

Return generic error messages to clients. Never include personal data like 'username' in HTTP error responses or exception messages visible to users.

#18 HIGH — IAC-K8S-NETPOL-001 [Confirmed] [Java]

kubernetes/fineract-mifoscommunity-deployment.yml:1

Applies to: [DPDPA] §8(5)

Compliance Ref	DPDPA: §8(5)
Source	https://www.meity.gov.in/content/digital-personal-data-protection-act-2023
Location	kubernetes/fineract-mifoscommunity-deployment.yml:1
Method	Global scope
Operation	General
Confidence	Confirmed (85%)
Est. Fix Time	30-60 min
Complexity	MED Medium
Language	Java

■ **Finding:** K8s workloads declared but no NetworkPolicy anywhere in the manifest set. CIS K8s 5.3.2 — without NetworkPolicy, all pods can talk to all pods.

Why this matters: May indicate non-compliance with DPDPA requirements. Review this finding against your organization's compliance obligations.

Offending Code

1	(no NetworkPolicy declared)
---	-----------------------------

Remediation

Add a default-deny NetworkPolicy in every namespace that holds personal data, then allow specific traffic via additional NetworkPolicy resources.

#19 HIGH — IAC-K8S-RUN-ROOT-001 [Confirmed] [Java]

kubernetes/fineract-mifoscommunity-deployment.yml:76

Applies to: **[DPDPA]** §8(5)

Compliance Ref	DPDPA: §8(5)
Source	https://www.meity.gov.in/content/digital-personal-data-protection-act-2023
Location	kubernetes/fineract-mifoscommunity-deployment.yml:76
Method	Global scope
Operation	General
Confidence	Confirmed (90%)
Est. Fix Time	30-60 min
Complexity	MED Medium
Language	Java

■ **Finding:** K8s container 'mifos-community' in Deployment 'Deployment/default/mifos-community' is configured to run as root. CIS K8s 5.2.6 requires runAsNonRoot = true.

Why this matters: May indicate non-compliance with DPDPA requirements. Review this finding against your organization's compliance obligations.

Offending Code

76	container "mifos-community" runAsUser=None runAsNonRoot=None
----	--

Remediation

Set securityContext.runAsNonRoot = true and securityContext.runAsUser to a non-zero UID. Build the image with a non-root USER directive (see IAC-DOCKER-ROOT-001).

#20 HIGH — IAC-K8S-RUN-ROOT-001 [Confirmed] [Java]

kubernetes/fineract-server-deployment.yml:37

Applies to: **[DPDPA]** §8(5)

Compliance Ref	DPDPA: §8(5)
Source	https://www.meity.gov.in/content/digital-personal-data-protection-act-2023
Location	kubernetes/fineract-server-deployment.yml:37
Method	Global scope
Operation	General
Confidence	Confirmed (90%)
Est. Fix Time	30-60 min
Complexity	MED Medium
Language	Java

■ **Finding:** K8s container 'fineract-server' in Deployment 'Deployment/default/fineract-server' is configured to run as root. CIS K8s 5.2.6 requires runAsNonRoot = true.

Why this matters: May indicate non-compliance with DPDPA requirements. Review this finding against your organization's compliance obligations.

Offending Code

37	container "fineract-server" runAsUser=None runAsNonRoot=None
----	--

Remediation

Set securityContext.runAsNonRoot = true and securityContext.runAsUser to a non-zero UID. Build the image with a non-root USER directive (see IAC-DOCKER-ROOT-001).

#21 HIGH — IAC-K8S-RUN-ROOT-001 [Confirmed] [Java]

kubernetes/fineractmysql-deployment.yml:68

Applies to: **[DPDPA]** §8(5)

Compliance Ref	DPDPA: §8(5)
Source	https://www.meity.gov.in/content/digital-personal-data-protection-act-2023
Location	kubernetes/fineractmysql-deployment.yml:68
Method	Global scope
Operation	General
Confidence	Confirmed (90%)
Est. Fix Time	30-60 min
Complexity	MED Medium
Language	Java

■ **Finding:** K8s container 'mysql' in Deployment 'Deployment/default/fineractmysql' is configured to run as root. CIS K8s 5.2.6 requires runAsNonRoot = true.

Why this matters: May indicate non-compliance with DPDPA requirements. Review this finding against your organization's compliance obligations.

Offending Code

68	container "mysql" runAsUser=None runAsNonRoot=None
----	--

Remediation

Set securityContext.runAsNonRoot = true and securityContext.runAsUser to a non-zero UID. Build the image with a non-root USER directive (see IAC-DOCKER-ROOT-001).

#22 MEDIUM — DPDPA-SVC-001 [Confirmed] [Java]

custom/acme/event/externalevent/src/main/java/com/acme/fineract/event/externalevent/AcmeExternalEventSourceProviderConfig.java:28

Compliance Ref	DPDPA
Source	https://www.meity.gov.in/content/digital-personal-data-protection-act-2023
Location	custom/acme/event/externalevent/src/main/java/com/acme/fineract/event/externalevent/AcmeExternalEventSourceProviderConfig.java:28
Method	Global scope
Operation	General
Confidence	Confirmed (85%)
Est. Fix Time	30-60 min
Complexity	MED Medium
Language	Java

■ **Finding:** DPDPA §8(10) requires a grievance redressal mechanism. No GrievanceController / grievance endpoint found anywhere. (2 occurrences)

Why this matters: May indicate non-compliance with DPDPA requirements. Review this finding against your organization's compliance obligations.

Offending Code

28	(missing: Grievance redressal)
29	(missing: Breach notification)

Remediation

Add a GrievanceController with POST /grievance that records Data-Principal complaints and routes them to the Data Protection Officer within the statutory SLA.

#23 MEDIUM — DPDPA-SDF-001 [Needs Review] [Java]

custom/acme/event/externalevent/src/main/java/com/acme/fineract/event/externalevent/AcmeExternalEventSourceProviderConfig.java:28

Compliance Ref	DPDPA
Source	https://www.meity.gov.in/content/digital-personal-data-protection-act-2023
Location	custom/acme/event/externalevent/src/main/java/com/acme/fineract/event/externalevent/AcmeExternalEventSourceProviderConfig.java:28
Method	Global scope
Operation	General
Confidence	Needs Review (55%)
Est. Fix Time	30-60 min
Complexity	MED Medium
Language	Java

■ **Finding:** Project shows Significant-Data-Fiduciary signals (lending/insurance/health/telecom) but no DPIA / independent-auditor reference. DPDPA §10(2) requires a DPO in India, an independent data auditor and periodic DPIAs.

Manual Review Recommended This finding has lower certainty due to limitations of static analysis. Verify whether the identified pattern constitutes an actual compliance violation in your deployment environment.

Why this matters: May indicate non-compliance with DPDPA requirements. Review this finding against your organization's compliance obligations.

Remediation

Ship a DPIA artefact and engage an independent data auditor, or set an explicit IS_SIGNIFICANT_DF=false if not notified under §10(1).

#24 MEDIUM — RETENTION-001 [Likely] [Java]

```
fineract-command-jdbc/src/main/java/org/apache/fineract/command/jdbc/store/domain/CommandEntity.java:33
```

Applies to: [DPDPA] §8(7)(a), §8(7)(b)

Compliance Ref	DPDPA: §8(7)(a), §8(7)(b)
Source	https://www.meity.gov.in/content/digital-personal-data-protection-act-2023
Location	fineract-command-jdbc/src/main/java/org/apache/fineract/command/jdbc/store/domain/CommandEntity.java:33
Method	CommandEntity (class-level)
Operation	General
Confidence	Likely (60%)
Est. Fix Time	30-60 min
Complexity	MED Medium
Language	Java

■ **Finding:** PII data model found but no scheduled deletion/cleanup job detected — GDPR Article 5(1)(e) requires data minimization with defined retention periods

Why this matters: DPDPA §8(7) requires erasure of personal data when consent is withdrawn or the specified purpose is fulfilled. Models without deletion mechanisms violate data erasure requirements.

Offending Code

```

33  @Getter
34  @Setter
35  @ToString
36  @FieldNameConstants
37  @Table("m_command")
38  public class CommandEntity implements Serializable {
39
40      @Serial
41      private static final long serialVersionUID = 1L;
42
43      @Id
44      @Column("id")
45      private Long id;
46
47      @Column("created_at")
48      private Instant createdAt;
49
50      @Col

```

Remediation

Add a scheduled task (e.g. Celery beat, @Scheduled cron, node-cron) that periodically purges or anonymizes expired personal data. This is required for GDPR Article 5(1)(e) storage limitation compliance.

#25 MEDIUM — RETENTION-001 [Needs Review] [Java]

fineract-core/src/main/java/org/apache/fineract/commands/domain/CommandSource.java:41

Applies to: [DPDPA] §8(7)(a), §8(7)(b)

Compliance Ref	DPDPA: §8(7)(a), §8(7)(b)
Source	https://www.meity.gov.in/content/digital-personal-data-protection-act-2023
Location	fineract-core/src/main/java/org/apache/fineract/commands/domain/CommandSource.java:41
Method	CommandSource (class-level)
Operation	General
Confidence	Needs Review (50%)
Est. Fix Time	30-60 min
Complexity	MED Medium
Language	Java

■ **Finding:** Data model 'CommandSource' has PII fields but no retention/deletion mechanism

Manual Review Recommended This finding has lower certainty due to limitations of static analysis. Verify whether the identified pattern constitutes an actual compliance violation in your deployment environment.

Why this matters: DPDPA §8(7) requires erasure of personal data when consent is withdrawn or the specified purpose is fulfilled. Models without deletion mechanisms violate data erasure requirements.

Offending Code

```
41 @Entity
42 @Getter
43 @Setter
44 @Builder
45 @NoArgsConstructor
46 @AllArgsConstructor
47 @Table(name = "m_portfolio_command_source")
48 public class CommandSource extends AbstractPersistableCustom<Long> {
49
50     @Column(name = "action_name", nullable = true, length = 100)
51     private String actionName;
52
53     @Column(name
```

Remediation

Add soft-delete (deleted_at) and retention period (retention_expires_at) fields to 'CommandSource'. This supports GDPR Article 17 (right to erasure) and Article 5(1)(e) (storage limitation). Note: retention may be handled at the application layer.

#26 MEDIUM — PII-001 [Needs Review] [Java]

```
fineract-core/src/main/java/org/apache/fineract/infrastructure/core/filters/CallerIpTrackingFilter.java:62
```

Applies to: [DPDPA] §6(1), §8(5)

Compliance Ref	DPDPA: §6(1), §8(5)
Source	https://www.meity.gov.in/content/digital-personal-data-protection-act-2023
Location	fineract-core/src/main/java/org/apache/fineract/infrastructure/core/filters/CallerIpTrackingFilter.java:62
Method	CallerIpTrackingFilter.getClientIpAddress
Operation	General
Confidence	Needs Review (55%)
Est. Fix Time	30-60 min
Complexity	MED Medium
Language	Java

■ Finding: PII field 'remoteaddr' logged without masking in CallerIpTrackingFilter.getClientIpAddress

Manual Review Recommended This finding has lower certainty due to limitations of static analysis. Verify whether the identified pattern constitutes an actual compliance violation in your deployment environment.

Why this matters: DPDPA §4(2) limits processing to stated purposes. Personal data in logs exceeds the stated purpose of processing and may constitute uncontrolled disclosure.

Offending Code

```
62 log.trace("getRemoteAddr method : {}", request.getRemoteAddr());
```

Remediation

Remove or mask the 'remoteaddr' field before logging. Use anonymized identifiers (e.g. user ID) instead of PII.

#27 MEDIUM — PII-001 [Needs Review] [Java]

```
fineract-core/src/main/java/org/apache/fineract/infrastructure/core/filters/CallerIpTrackingFilter.java:82
```

Applies to: [DPDPA] §6(1), §8(5)

Compliance Ref	DPDPA: §6(1), §8(5)
Source	https://www.meity.gov.in/content/digital-personal-data-protection-act-2023
Location	fineract-core/src/main/java/org/apache/fineract/infrastructure/core/filters/CallerIpTrackingFilter.java:82
Method	CallerIpTrackingFilter.handleClientIp
Operation	General
Confidence	Needs Review (55%)
Est. Fix Time	30-60 min
Complexity	MED Medium
Language	Java

■ Finding: PII field 'ipaddress' logged without masking in CallerIpTrackingFilter.handleClientIp

Manual Review Recommended This finding has lower certainty due to limitations of static analysis. Verify whether the identified pattern constitutes an actual compliance violation in your deployment environment.

Why this matters: DPDPA §4(2) limits processing to stated purposes. Personal data in logs exceeds the stated purpose of processing and may constitute uncontrolled disclosure.

Offending Code

```
82 log.trace("Found Client IP in header : {}", clientIpAddress);
```

Remediation

Remove or mask the 'ipaddress' field before logging. Use anonymized identifiers (e.g. user ID) instead of PII.

#28 MEDIUM — RETENTION-001 [Needs Review] [Java]

fineract-core/src/main/java/org/apache/fineract/organisation/staff/domain/Staff.java:33

Applies to: [DPDPA] §8(7)(a), §8(7)(b)

Compliance Ref	DPDPA: §8(7)(a), §8(7)(b)
Source	https://www.meity.gov.in/content/digital-personal-data-protection-act-2023
Location	fineract-core/src/main/java/org/apache/fineract/organisation/staff/domain/Staff.java:33
Method	Staff (class-level)
Operation	General
Confidence	Needs Review (50%)
Est. Fix Time	30-60 min
Complexity	MED Medium
Language	Java

■ **Finding:** Data model 'Staff' has PII fields but no retention/deletion mechanism

Manual Review Recommended This finding has lower certainty due to limitations of static analysis. Verify whether the identified pattern constitutes an actual compliance violation in your deployment environment.

Why this matters: DPDPA §8(7) requires erasure of personal data when consent is withdrawn or the specified purpose is fulfilled. Models without deletion mechanisms violate data erasure requirements.

Offending Code

```
33 @Getter
34 @Setter
35 @Entity
36 @Table(name = "m_staff", uniqueConstraints = { @UniqueConstraint(columnNames = { "display_name" }, name =
    "display_na...
37 @UniqueConstraint(columnNames = { "external_id" }, name = "external_id_UNIQUE"),
38 @UniqueConstraint(columnNames = { "mobile_no" }, name =
```

Remediation

Add soft-delete (deleted_at) and retention period (retention_expires_at) fields to 'Staff'. This supports GDPR Article 17 (right to erasure) and Article 5(1)(e) (storage limitation). Note: retention may be handled at the application layer.

#29 MEDIUM — GRIEVANCE-001 [Likely] [Java]

fineract-db/old-schema-files/0002-mifosx-base-reference-data-utf8.sql:291

Applies to: [DPDPA] §8(10)

Compliance Ref	DPDPA: §8(10)
Source	https://www.meity.gov.in/content/digital-personal-data-protection-act-2023
Location	fineract-db/old-schema-files/0002-mifosx-base-reference-data-utf8.sql:291
Method	Global scope
Operation	General
Confidence	Likely (60%)
Est. Fix Time	30-60 min
Complexity	MED Medium
Language	Java

■ **Finding:** Strong PII ('Passport') collected by a Data Fiduciary with no grievance/redressal mechanism or published contact (no /grievance, /complaint, /contact-us route, grievance-officer, or grievance/privacy mailbox). DPDPA §8(10) requires a readily-available means of redress for Data Principal grievances.

Why this matters: May indicate non-compliance with DPDPA requirements. Review this finding against your organization's compliance obligations.

Offending Code

291	select mc.id, 'Passport', 1
-----	-----------------------------

Remediation

Expose a public grievance/redressal endpoint (e.g. POST /grievance) with a response SLA and publish the grievance officer's business contact in the privacy notice.

#30 MEDIUM — CONSENT-001 [Likely] [Java]

```
fineract-loan/src/main/java/org/apache/fineract/portfolio/loanaccount/service/GLIMAccountInfoWritePlatformServiceImpl.java:40
```

✓ **Data-flow confirmed** — taint analysis traced a real source→sink path (3-step trace); highest-confidence finding.

Applies to: **[DPDPA]** §6(1), §6(3), §6(10), §7

Compliance Ref	DPDPA: §6(1), §6(3), §6(10), §7
Source	https://www.meity.gov.in/content/digital-personal-data-protection-act-2023
Location	fineract-loan/src/main/java/org/apache/fineract/portfolio/loanaccount/service/GLIMAccountInfoWritePlatformServiceImpl.java:40
Method	createGLIMAccount
Operation	General
Confidence	Likely (75%)
Est. Fix Time	30-60 min
Complexity	MED Medium
Language	Java

■ **Finding:** No consent mechanism exists anywhere in this codebase, yet personal data is collected and stored (first seen at GLIMAccountInfoWritePlatformServiceImpl.java:40). DPDPA §6(1) requires free, specific, informed and unambiguous consent before processing, and §6(4)-(6) require a record of it and a means to withdraw.

Why this matters: DPDPA §6 requires valid consent from the Data Principal before processing personal data. Functions that process personal data without verifying consent violate fundamental DPDPA requirements.

Offending Code

40	Data Flow Trace (CONSENT-001):
41	Line 33 → parameter: accountNumber [SOURCE: accountNumber]
42	Line 37 → GroupLoanIndividualMonitoringAccount glimAccountInfo = GroupLoanIndividualMonitoringAccount.getInstanc...
43	Line 40 → return this.glimAccountRepository.save(glimAccountInfo); [SINK: accountNumber]

Remediation

Verify consent before processing personal data at line 40. Call a consent verification function (e.g., `hasConsent(userId, 'data_processing')`) before the data operation.

#31 MEDIUM — RETENTION-001 [Needs Review] [Java]

fineract-provider/src/main/java/org/apache/fineract/adhocquery/domain/AdHoc.java:35

Applies to: [DPDPA] §8(7)(a), §8(7)(b)

This card summarises 8 occurrence(s) across 8 file(s). The 3 most severe occurrences are shown as individual cards above.

All 8 Occurrence(s) across 8 file(s)

File	Line	Method	Conf.
fineract-command-jdbc/src/main/java/org/apache/fineract/command/jdbc/store/domain/CommandEntity.java	33	?	Likely
fineract-core/src/main/java/org/apache/fineract/commands/domain/CommandSource.java	41	?	Needs Review
fineract-core/src/main/java/org/apache/fineract/organisation/staff/domain/Staff.java	33	?	Needs Review
fineract-provider/src/main/java/org/apache/fineract/adhocquery/domain/AdHoc.java	35	?	Needs Review
fineract-provider/src/main/java/org/apache/fineract/infrastructure/campaigns/email/domain/EmailMessage.java	41	?	Needs Review
fineract-provider/src/main/java/org/apache/fineract/infrastructure/creditbureau/domain/CreditReport.java	32	?	Needs Review
fineract-provider/src/main/java/org/apache/fineract/portfolio/client/domain/ClientFamilyMembers.java	31	?	Needs Review
fineract-provider/src/main/java/org/apache/fineract/portfolio/loanaccount/guarantor/domain/Guarantor.java	42	?	Needs Review
Compliance Ref	DPDPA: §8(7)(a), §8(7)(b)		
Source	https://www.meity.gov.in/content/digital-personal-data-protection-act-2023		
Location	fineract-provider/src/main/java/org/apache/fineract/adhocquery/domain/AdHoc.java:35		
Method	AdHoc (class-level)		
Operation	General		
Confidence	Needs Review (50%)		
Est. Fix Time	30-60 min		
Complexity	MED Medium		
Language	Java		

■ **Finding:** Data model 'AdHoc' has PII fields but no retention/deletion mechanism (+5 more across 5 file(s): AdHoc.java, EmailMessage.java, CreditReport.java, ClientFamilyMembers.java, Guarantor.java)

Manual Review Recommended This finding has lower certainty due to limitations of static analysis. Verify whether the identified pattern constitutes an actual compliance violation in your deployment environment.

Why this matters: DPDPA §8(7) requires erasure of personal data when consent is withdrawn or the specified purpose is fulfilled. Models without deletion mechanisms violate data erasure requirements.

Offending Code

```
35  @Getter
36  @Setter
37  @NoArgsConstructor
38  @Accessors(chain = true)
39  @Entity
40  @Table(name = "m_adhoc")
41  public class AdHoc extends AbstractAuditableCustom {
42
43      @Column(name = "name", length = 100)
44      private String name;
45
46      @Column(name = "query", length = 2000)
47      private String query;
48
49      @Column(name
```

Remediation

Add soft-delete (`deleted_at`) and retention period (`retention_expires_at`) fields to 'AdHoc'. This supports GDPR Article 17 (right to erasure) and Article 5(1)(e) (storage limitation). Note: retention may be handled at the application layer.

Shared Remediation — applies to all 8 occurrence(s)

Add soft-delete (`deleted_at`) and retention period (`retention_expires_at`) fields to 'AdHoc'. This supports GDPR Article 17 (right to erasure) and Article 5(1)(e) (storage limitation). Note: retention may be handled at the application layer.

#32 MEDIUM — LOG-001 [Confirmed] [Java]

```
fineract-provider/src/main/java/org/apache/fineract/cob/loan/CheckDueInstallmentsBusinessStep.java:58
```

Applies to: [DPDPA] §8(5), §6(1)

Compliance Ref	DPDPA: §8(5), §6(1)
Source	https://www.meity.gov.in/content/digital-personal-data-protection-act-2023
Location	fineract-provider/src/main/java/org/apache/fineract/cob/loan/CheckDueInstallmentsBusinessStep.java:58
Method	CheckDueInstallmentsBusinessStep.run
Operation	General
Confidence	Confirmed (95%)
Est. Fix Time	1-2 hours
Complexity	LOW Low
Language	Java

■ **Finding:** Personal data [accountNumber] detected in logging call 'log.debug' in CheckDueInstallmentsBusinessStep.run. Personal data must never appear in application logs.

Why this matters: DPDPA §4(2) limits processing to stated purposes. Logging personal data exceeds the stated purpose and violates the purpose limitation principle.

Offending Code

58	log.debug("Starting custom snapshot event processing for loan with id [{}], account number [{}], external Id [{}].",
59	loan.getId(), loan.getAccountNumber(), externalId)

Remediation

Under the DPDPA, 'accountNumber' may constitute personal data and should not be logged in plain text. Remove personal data from log messages. Recommended fixes: (1) Replace personal data values with opaque surrogate keys (UUID / DB primary key): `logger.info('Record updated: id={}', record.id)` — never log 'accountNumber' directly. (2) Hash the value if correlation is needed for debugging: `logger.debug('accountNumber_hash={}', sha256(accountNumber)[:8])`. (3) Use structured logging with a redaction filter in the logging pipeline. (4) If the context is required for auditing, write to a dedicated access-controlled audit log rather than the application/error log. (5) Use a masking library (scrubadub, fast-redact, pino-noir, Serilog.Enrichers.Sensitive) to automatically redact personal data before logging.

Current Code (Before)

1	// PHI in log – 'accountNumber' must not be logged
2	log.debug("Starting custom snapshot event processing for loan with id [{}], account number [{}], external Id [{}].",

Fixed Code (After)

1	// Log only opaque identifiers – never log 'accountNumber'
---	--

2	<code>logger.info("Operation completed: record_id=%s", record.id)</code>
---	--

#33 MEDIUM — LOG-001 [Confirmed] [Java]

```
fineract-provider/src/main/java/org/apache/fineract/cob/loan/CheckDueInstallmentsBusinessStep.java
:80
```

Applies to: [DPDPA] §8(5), §6(1)

Compliance Ref	DPDPA: §8(5), §6(1)
Source	https://www.meity.gov.in/content/digital-personal-data-protection-act-2023
Location	fineract-provider/src/main/java/org/apache/fineract/cob/loan/CheckDueInstallmentsBusinessStep.java:80
Method	CheckDueInstallmentsBusinessStep.run
Operation	General
Confidence	Confirmed (95%)
Est. Fix Time	1-2 hours
Complexity	LOW Low
Language	Java

■ **Finding:** Personal data [accountNumber] detected in logging call 'log.error' in CheckDueInstallmentsBusinessStep.run. Personal data must never appear in application logs.

Why this matters: DPDPA §4(2) limits processing to stated purposes. Logging personal data exceeds the stated purpose and violates the purpose limitation principle.

Offending Code

```
80 log.error(
81 "Received [{}] exception while processing custom snapshot event for loan with Id [{}], ac...
82 re.getMessage(), loan.getId(), loan.getAccountNumber(), externalId, re)
```

Remediation

Under the DPDPA, 'accountNumber' may constitute personal data and should not be logged in plain text. Remove personal data from log messages. Recommended fixes: (1) Replace personal data values with opaque surrogate keys (UUID / DB primary key): `logger.info('Record updated: id={}', record.id)` — never log 'accountNumber' directly. (2) Hash the value if correlation is needed for debugging: `logger.debug('accountNumber_hash={}', sha256(accountNumber)[:8])`. (3) Use structured logging with a redaction filter in the logging pipeline. (4) If the context is required for auditing, write to a dedicated access-controlled audit log rather than the application/error log. (5) Use a masking library (scrubadub, fast-redact, pino-noir, Serilog.Enrichers.Sensitive) to automatically redact personal data before logging.

Current Code (Before)

```
1 // PHI in log - 'accountNumber' must not be logged
2 log.error(
```

Fixed Code (After)

```
1 // Log only opaque identifiers - never log 'accountNumber'
```

2	<code>logger.info("Operation completed: record_id=%s", record.id)</code>
---	--

#34 MEDIUM — LOG-001 [Confirmed] [Java]

```
fineract-provider/src/main/java/org/apache/fineract/cob/loan/CheckDueInstallmentsBusinessStep.java
:90
```

Applies to: [DPDPA] §8(5), §6(1)

Compliance Ref	DPDPA: §8(5), §6(1)
Source	https://www.meity.gov.in/content/digital-personal-data-protection-act-2023
Location	fineract-provider/src/main/java/org/apache/fineract/cob/loan/CheckDueInstallmentsBusinessStep.java:90
Method	CheckDueInstallmentsBusinessStep.execute
Operation	General
Confidence	Confirmed (95%)
Est. Fix Time	1-2 hours
Complexity	LOW Low
Language	Java

■ **Finding:** Personal data [accountNumber] detected in logging call 'log.debug' in CheckDueInstallmentsBusinessStep.execute. Personal data must never appear in application logs.

Why this matters: DPDPA §4(2) limits processing to stated purposes. Logging personal data exceeds the stated purpose and violates the purpose limitation principle.

Offending Code

```
90 log.debug(
91 "Ending custom snapshot event processing for loan with Id [{}], account number [{}], external Id [{}]...
92 loan.getId(), loan.getAccountNumber(), externalId, duration.toMillis())
```

Remediation

Under the DPDPA, 'accountNumber' may constitute personal data and should not be logged in plain text. Remove personal data from log messages. Recommended fixes: (1) Replace personal data values with opaque surrogate keys (UUID / DB primary key): `logger.info('Record updated: id={}', record.id)` — never log 'accountNumber' directly. (2) Hash the value if correlation is needed for debugging: `logger.debug('accountNumber_hash={}', sha256(accountNumber)[:8])`. (3) Use structured logging with a redaction filter in the logging pipeline. (4) If the context is required for auditing, write to a dedicated access-controlled audit log rather than the application/error log. (5) Use a masking library (scrubadub, fast-redact, pino-noir, Serilog.Enrichers.Sensitive) to automatically redact personal data before logging.

Current Code (Before)

```
1 // PHI in log - 'accountNumber' must not be logged
2 log.debug(
```

Fixed Code (After)

```
1 // Log only opaque identifiers - never log 'accountNumber'
```

2	<code>logger.info("Operation completed: record_id=%s", record.id)</code>
---	--

#35 MEDIUM — LOG-001 [Confirmed] [Java]

fineract-provider/src/main/java/org/apache/fineract/cob/loan/SetLoanDelinquencyTagsBusinessStep.java:67

Applies to: [DPDPA] §8(5), §6(1)

This card summarises 12 occurrence(s) across 7 file(s). The 3 most severe occurrences are shown as individual cards above.

All 12 Occurrence(s) across 7 file(s)

File	Line	Method	Conf.
fineract-provider/src/main/java/org/apache/fineract/cob/loan/CheckDueInstallmentsBusinessStep.java	58	run	Confirmed
fineract-provider/src/main/java/org/apache/fineract/cob/loan/CheckDueInstallmentsBusinessStep.java	80	run	Confirmed
fineract-provider/src/main/java/org/apache/fineract/cob/loan/CheckDueInstallmentsBusinessStep.java	90	execute	Confirmed
fineract-provider/src/main/java/org/apache/fineract/cob/loan/SetLoanDelinquencyTagsBusinessStep.java	67	run	Confirmed
fineract-provider/src/main/java/org/apache/fineract/cob/loan/SetLoanDelinquencyTagsBusinessStep.java	87	run	Confirmed
fineract-provider/src/main/java/org/apache/fineract/cob/loan/SetLoanDelinquencyTagsBusinessStep.java	98	execute	Confirmed
fineract-provider/src/main/java/org/apache/fineract/infrastructure/campaigns/email/service/EmailCampaignWritePlatformCommandHandlerImpl.java	217	insertDirectCampaignIntoEmailOutboundTable	Needs Review
fineract-provider/src/main/java/org/apache/fineract/infrastructure/security/service/OidcAppUserResolutionServiceImpl.java	71	resolveOrCreate	Needs Review
fineract-provider/src/main/java/org/apache/fineract/portfolio/client/domain/ClientRepositoryWrapper.java	87	getClientByAccountNumber	Likely
fineract-provider/src/main/java/org/apache/fineract/useradministration/service/ForgotPasswordServiceImpl.java	50	requestPasswordReset	Needs Review
fineract-working-capital-loan/src/main/java/org/apache/fineract/cob/workingcapitalloan/businessstep/WorkingCapitalLoanDelinquencyClassificationBusinessStep.java	48	execute	Confirmed
fineract-working-capital-loan/src/main/java/org/apache/fineract/cob/workingcapitalloan/businessstep/WorkingCapitalLoanDelinquencyClassificationBusinessStep.java	57	setDelinquencyBucketTags	Confirmed

Compliance Ref	DPDPA: §8(5), §6(1)
Source	https://www.meity.gov.in/content/digital-personal-data-protection-act-2023
Location	fineract-provider/src/main/java/org/apache/fineract/cob/loan/SetLoanDelinquencyTagsBusinessStep.java:67
Method	SetLoanDelinquencyTagsBusinessStep.run
Operation	General
Confidence	Confirmed (95%)
Est. Fix Time	1-2 hours
Complexity	LOW Low
Language	Java

■ **Finding:** Personal data [accountNumber] detected in logging call 'log.debug' in

SetLoanDelinquencyTagsBusinessStep.run. Personal data must never appear in application logs. (+9 more across 6 file(s): SetLoanDelinquencyTagsBusinessStep.java, EmailCampaignWritePlatformCommandHandlerImpl.java, OidcAppUserResolutionServiceImpl.java, ClientRepositoryWrapper.java, ForgotPasswordServiceImpl.java, ... +1 more)

Why this matters: DPDPA §4(2) limits processing to stated purposes. Logging personal data exceeds the stated purpose and violates the purpose limitation principle.

Offending Code

67	log.debug("Starting delinquency tag processing for loan with Id [{}], account number [{}], external Id [{}]",
68	loan.getId(), loan.getAccountNumber(), externalId)

Remediation

Under the DPDPA, 'accountNumber' may constitute personal data and should not be logged in plain text. Remove personal data from log messages. Recommended fixes: (1) Replace personal data values with opaque surrogate keys (UUID / DB primary key): `logger.info('Record updated: id={}', record.id)` — never log 'accountNumber' directly. (2) Hash the value if correlation is needed for debugging: `logger.debug('accountNumber_hash={}', sha256(accountNumber)[:8])`. (3) Use structured logging with a redaction filter in the logging pipeline. (4) If the context is required for auditing, write to a dedicated access-controlled audit log rather than the application/error log. (5) Use a masking library (scrubadub, fast-redact, pino-noir, Serilog.Enrichers.Sensitive) to automatically redact personal data before logging.

Current Code (Before)

1	// PHI in log – 'accountNumber' must not be logged
2	log.debug("Starting delinquency tag processing for loan with Id [{}], account number [{}], external Id [{}]",

Fixed Code (After)

1	// Log only opaque identifiers – never log 'accountNumber'
2	logger.info("Operation completed: record_id=%s", record.id)

Shared Remediation — applies to all 12 occurrence(s)

Under the DPDPA, 'accountNumber' may constitute personal data and should not be logged in plain text. Remove personal data from log messages. Recommended fixes: (1) Replace personal data values with opaque surrogate keys (UUID / DB primary key): `logger.info('Record updated: id={}', record.id)` — never log 'accountNumber' directly. (2) Hash the value if correlation is needed for debugging: `logger.debug('accountNumber_hash={}', sha256(accountNumber)[:8])`. (3) Use structured logging with a redaction filter in the logging pipeline. (4) If the context is required for auditing, write to a dedicated access-controlled audit log rather than the application/error log. (5) Use a masking library (scrubadub, fast-redact, pino-noir, Serilog.Enrichers.Sensitive) to automatically redact personal data before logging.

#36 MEDIUM — DATA-ACCURACY-001 [Likely] [Java]

```
fineract-provider/src/main/java/org/apache/fineract/portfolio/shareaccounts/domain/ShareAccount.java:431
```

Applies to: [DPDPA] §8(3)

Compliance Ref	DPDPA: §8(3)
Source	https://www.meity.gov.in/content/digital-personal-data-protection-act-2023
Location	fineract-provider/src/main/java/org/apache/fineract/portfolio/shareaccounts/domain/ShareAccount.java:431
Method	Global scope
Operation	General
Confidence	Likely (60%)
Est. Fix Time	30-60 min
Complexity	MED Medium
Language	Java

■ **Finding:** Decision-driving function 'reject' has no input validation. DPDPA §8(3) requires completeness, accuracy and consistency of personal data used in decisions affecting the Data Principal.

Why this matters: May indicate non-compliance with DPDPA requirements. Review this finding against your organization's compliance obligations.

Offending Code

```
431 public void reject(final LocalDate rejectedDate, final AppUser rejectedUser) {
```

Remediation

Validate inputs (schema / DTO / explicit guards on PAN, Aadhaar, DOB, income) before they reach the decision.

#37 MEDIUM — IAC-K8S-RO-FS-001 [Confirmed] [Java]

kubernetes/fineract-mifoscommunity-deployment.yml:76

Applies to: [DPDPA] §8(5)

Compliance Ref DPDPA: §8(5)

Source <https://www.meity.gov.in/content/digital-personal-data-protection-act-2023>

Location kubernetes/fineract-mifoscommunity-deployment.yml:76

Method Global scope

Operation General

Confidence Confirmed (85%)

Est. Fix Time 30-60 min

Complexity MED Medium

Language Java

■ **Finding:** K8s container 'mifos-community' in Deployment 'Deployment/default/mifos-community' does not set `readOnlyRootFilesystem = true`. CIS K8s 5.7.4.

Why this matters: May indicate non-compliance with DPDPA requirements. Review this finding against your organization's compliance obligations.

Offending Code

76	container "mifos-community" RO-FS unset
----	---

Remediation

Set `securityContext.readOnlyRootFilesystem = true`. If the container needs writeable temp space, mount an `emptyDir` volume.

#38 MEDIUM — IAC-K8S-CAPS-001 [Likely] [Java]

kubernetes/fineract-mifoscommunity-deployment.yml:76

Applies to: [DPDPA] §8(5)

Compliance Ref	DPDPA: §8(5)
Source	https://www.meity.gov.in/content/digital-personal-data-protection-act-2023
Location	kubernetes/fineract-mifoscommunity-deployment.yml:76
Method	Global scope
Operation	General
Confidence	Likely (80%)
Est. Fix Time	30-60 min
Complexity	MED Medium
Language	Java

■ **Finding:** K8s container 'mifos-community' in Deployment 'Deployment/default/mifos-community' does not drop ALL capabilities. CIS K8s 5.7 best practice is `drop: [ALL]` then add back the minimum set.

Why this matters: May indicate non-compliance with DPDPA requirements. Review this finding against your organization's compliance obligations.

Offending Code

76	capabilities.drop missing ALL
----	-------------------------------

Remediation

Add `securityContext.capabilities.drop: [ALL]` and explicitly add only the caps the workload uses.

#39 MEDIUM — IAC-K8S-RESOURCES-001 [Likely] [Java]

kubernetes/fineract-mifoscommunity-deployment.yml:76

Applies to: [DPDPA] §8(5)

Compliance Ref DPDPA: §8(5)

Source <https://www.meity.gov.in/content/digital-personal-data-protection-act-2023>

Location kubernetes/fineract-mifoscommunity-deployment.yml:76

Method Global scope

Operation General

Confidence Likely (80%)

Est. Fix Time 30-60 min

Complexity MED Medium

Language Java

■ **Finding:** K8s container 'init-myservice' in Deployment 'Deployment/default/mifos-community' has no resources.limits/requests. CIS K8s 5.7.3.

Why this matters: May indicate non-compliance with DPDPA requirements. Review this finding against your organization's compliance obligations.

Offending Code

76	container "init-myservice" no limits/requests
----	---

Remediation

Set both resources.requests (minimum reserved) and resources.limits (maximum allowed) for cpu + memory.

#40 MEDIUM — IAC-K8S-RO-FS-001 [Confirmed] [Java]

kubernetes/fineract-server-deployment.yml:37

Applies to: [DPDPA] §8(5)

Compliance Ref	DPDPA: §8(5)
Source	https://www.meity.gov.in/content/digital-personal-data-protection-act-2023
Location	kubernetes/fineract-server-deployment.yml:37
Method	Global scope
Operation	General
Confidence	Confirmed (85%)
Est. Fix Time	30-60 min
Complexity	MED Medium
Language	Java

■ **Finding:** K8s container 'fineract-server' in Deployment 'Deployment/default/fineract-server' does not set `readOnlyRootFilesystem = true`. CIS K8s 5.7.4.

Why this matters: May indicate non-compliance with DPDPA requirements. Review this finding against your organization's compliance obligations.

Offending Code

37	container "fineract-server" R0-FS unset
----	---

Remediation

Set `securityContext.readOnlyRootFilesystem = true`. If the container needs writeable temp space, mount an `emptyDir` volume.

#41 MEDIUM — IAC-K8S-CAPS-001 [Likely] [Java]

kubernetes/fineract-server-deployment.yml:37

Applies to: [DPDPA] §8(5)

Compliance Ref DPDPA: §8(5)

Source <https://www.meity.gov.in/content/digital-personal-data-protection-act-2023>

Location kubernetes/fineract-server-deployment.yml:37

Method Global scope

Operation General

Confidence Likely (80%)

Est. Fix Time 30-60 min

Complexity MED Medium

Language Java

■ **Finding:** K8s container 'fineract-server' in Deployment 'Deployment/default/fineract-server' does not drop ALL capabilities. CIS K8s 5.7 best practice is `drop: [ALL]` then add back the minimum set.

Why this matters: May indicate non-compliance with DPDPA requirements. Review this finding against your organization's compliance obligations.

Offending Code

37	capabilities.drop missing ALL
----	-------------------------------

Remediation

Add `securityContext.capabilities.drop: [ALL]` and explicitly add only the caps the workload uses.

#42 MEDIUM — IAC-K8S-RESOURCES-001 [Likely] [Java]

kubernetes/fineract-server-deployment.yml:37

Applies to: [DPDPA] §8(5)

Compliance Ref	DPDPA: §8(5)
Source	https://www.meity.gov.in/content/digital-personal-data-protection-act-2023
Location	kubernetes/fineract-server-deployment.yml:37
Method	Global scope
Operation	General
Confidence	Likely (80%)
Est. Fix Time	30-60 min
Complexity	MED Medium
Language	Java

■ **Finding:** K8s container 'init-mydb' in Deployment 'Deployment/default/fineract-server' has no resources.limits/requests. CIS K8s 5.7.3.

Why this matters: May indicate non-compliance with DPDPA requirements. Review this finding against your organization's compliance obligations.

Offending Code

37	container "init-mydb" no limits/requests
----	--

Remediation

Set both resources.requests (minimum reserved) and resources.limits (maximum allowed) for cpu + memory.

#43 MEDIUM — IAC-K8S-IMG-LATEST-001 [Confirmed] [Java]

kubernetes/fineract-server-deployment.yml:37

Applies to: [DPDPA] §8(5)

Compliance Ref	DPDPA: §8(5)
Source	https://www.meity.gov.in/content/digital-personal-data-protection-act-2023
Location	kubernetes/fineract-server-deployment.yml:37
Method	Global scope
Operation	General
Confidence	Confirmed (90%)
Est. Fix Time	30-60 min
Complexity	MED Medium
Language	Java

■ **Finding:** K8s container 'fineract-server' in Deployment 'Deployment/default/fineract-server' uses image 'apache/fineract:latest' — :latest or no tag, no digest pin. CIS K8s 1.5.2.

Why this matters: May indicate non-compliance with DPDPA requirements. Review this finding against your organization's compliance obligations.

Offending Code

37	image: apache/fineract:latest
----	-------------------------------

Remediation

Pin to a specific tag AND digest: `image: myorg/myapp:v1.4.2@sha256:<digest>`.

#44 MEDIUM — IAC-K8S-RO-FS-001 [Confirmed] [Java]

kubernetes/fineractmysql-deployment.yml:68

Applies to: [DPDPA] §8(5)

Compliance Ref	DPDPA: §8(5)
Source	https://www.meity.gov.in/content/digital-personal-data-protection-act-2023
Location	kubernetes/fineractmysql-deployment.yml:68
Method	Global scope
Operation	General
Confidence	Confirmed (85%)
Est. Fix Time	30-60 min
Complexity	MED Medium
Language	Java

■ **Finding:** K8s container 'mysql' in Deployment 'Deployment/default/fineractmysql' does not set readOnlyRootFilesystem = true. CIS K8s 5.7.4.

Why this matters: May indicate non-compliance with DPDPA requirements. Review this finding against your organization's compliance obligations.

Offending Code

68	container "mysql" RO-FS unset
----	-------------------------------

Remediation

Set securityContext.readOnlyRootFilesystem = true. If the container needs writeable temp space, mount an emptyDir volume.

#45 MEDIUM — IAC-K8S-CAPS-001 [Likely] [Java]

kubernetes/fineractmysql-deployment.yml:68

Applies to: [DPDPA] §8(5)

Compliance Ref	DPDPA: §8(5)
Source	https://www.meity.gov.in/content/digital-personal-data-protection-act-2023
Location	kubernetes/fineractmysql-deployment.yml:68
Method	Global scope
Operation	General
Confidence	Likely (80%)
Est. Fix Time	30-60 min
Complexity	MED Medium
Language	Java

■ **Finding:** K8s container 'mysql' in Deployment 'Deployment/default/fineractmysql' does not drop ALL capabilities. CIS K8s 5.7 best practice is `drop: [ALL]` then add back the minimum set.

Why this matters: May indicate non-compliance with DPDPA requirements. Review this finding against your organization's compliance obligations.

Offending Code

68	capabilities.drop missing ALL
----	-------------------------------

Remediation

Add `securityContext.capabilities.drop: [ALL]` and explicitly add only the caps the workload uses.

#46 LOW — DPO-001 [Needs Review] [Java]

fineract-db/old-schema-files/0002-mifosx-base-reference-data-utf8.sql:291

Applies to: **[DPDPA]** §8(9), §10

Compliance Ref	DPDPA: §8(9), §10
Source	https://www.meity.gov.in/content/digital-personal-data-protection-act-2023
Location	fineract-db/old-schema-files/0002-mifosx-base-reference-data-utf8.sql:291
Method	Global scope
Operation	General
Confidence	Needs Review (55%)
Est. Fix Time	30-60 min
Complexity	MED Medium
Language	Java

■ **Finding:** Significant-Data-Fiduciary vertical collecting strong PII ('Passport') with no published DPO / data-protection contact (no /dpo or /privacy-contact route, DPO designation, or dpo/privacy mailbox). DPDPA §8(9) requires publishing a contact; §10 requires a Significant Data Fiduciary to appoint an India-based DPO.

Manual Review Recommended This finding has lower certainty due to limitations of static analysis. Verify whether the identified pattern constitutes an actual compliance violation in your deployment environment.

Why this matters: May indicate non-compliance with DPDPA requirements. Review this finding against your organization's compliance obligations.

Offending Code

291	select mc.id, 'Passport', 1
-----	-----------------------------

Remediation

Publish the DPO / contact-person details (designation, email, address) on a stable surface (e.g. /dpo or /privacy-contact) and, if a Significant Data Fiduciary, appoint an India-based DPO reporting to the board.

#47 LOW — CONSENT-001 [Likely] [Java]

fineract-provider/src/main/java/org/apache/fineract/portfolio/account/domain/AccountTransferDetails.java:132

Applies to: [DPDPA] §6(1), §6(3), §6(10), §7

Compliance Ref	DPDPA: §6(1), §6(3), §6(10), §7
Source	https://www.meity.gov.in/content/digital-personal-data-protection-act-2023
Location	fineract-provider/src/main/java/org/apache/fineract/portfolio/account/domain/AccountTransferDetails.java:132
Method	AccountTransferDetails.addAccountTransferTransaction
Operation	General
Confidence	Likely (65%)
Est. Fix Time	30-60 min
Complexity	MED Medium
Language	Java

■ **Finding:** No consent verification found before data processing in

AccountTransferDetails.addAccountTransferTransaction. Note: consent may be handled at the API gateway, middleware, or integration agreement level.

Why this matters: DPDPA §6 requires valid consent from the Data Principal before processing personal data. Functions that process personal data without verifying consent violate fundamental DPDPA requirements.

Offending Code

```
132 public void addAccountTransferTransaction(AccountTransferTransaction accountTransferTransaction) {  
133     this.accountTransferTransactions.add(accountTransferTransaction);  
134 }
```

Remediation

Verify that consent is checked before processing personal data. This may be handled at the middleware or API gateway level. If consent is already verified upstream, this finding is a false positive and can be suppressed via .scrutoraignore.

#48 LOW — CONSENT-001 [Likely] [Java]

```
fineract-provider/src/main/java/org/apache/fineract/portfolio/shareaccounts/domain/ShareAccount.java:390
```

Applies to: [DPDPA] §6(1), §6(3), §6(10), §7

Compliance Ref	DPDPA: §6(1), §6(3), §6(10), §7
Source	https://www.meity.gov.in/content/digital-personal-data-protection-act-2023
Location	fineract-provider/src/main/java/org/apache/fineract/portfolio/shareaccounts/domain/ShareAccount.java:390
Method	ShareAccount.addShareAccountCharge
Operation	General
Confidence	Likely (65%)
Est. Fix Time	30-60 min
Complexity	MED Medium
Language	Java

■ **Finding:** No consent verification found before data processing in ShareAccount.addShareAccountCharge. Note: consent may be handled at the API gateway, middleware, or integration agreement level.

Why this matters: DPDPA §6 requires valid consent from the Data Principal before processing personal data. Functions that process personal data without verifying consent violate fundamental DPDPA requirements.

Offending Code

```
390 public void addShareAccountCharge(ShareAccountCharge charge) {
391     charge.update(this);
392     this.charges.add(charge);
393 }
```

Remediation

Verify that consent is checked before processing personal data. This may be handled at the middleware or API gateway level. If consent is already verified upstream, this finding is a false positive and can be suppressed via .scrutornignore.

#49 LOW — CONSENT-001 [Likely] [Java]

```
fineract-provider/src/main/java/org/apache/fineract/portfolio/shareaccounts/domain/ShareAccountTransaction.java:184
```

Applies to: [DPDPA] §6(1), §6(3), §6(10), §7

Compliance Ref	DPDPA: §6(1), §6(3), §6(10), §7
Source	https://www.meity.gov.in/content/digital-personal-data-protection-act-2023
Location	fineract-provider/src/main/java/org/apache/fineract/portfolio/shareaccounts/domain/ShareAccountTransaction.java:184
Method	ShareAccountTransaction.addShareAccountChargePaidBy
Operation	General
Confidence	Likely (65%)
Est. Fix Time	30-60 min
Complexity	MED Medium
Language	Java

■ **Finding:** No consent verification found before data processing in `ShareAccountTransaction.addShareAccountChargePaidBy`. Note: consent may be handled at the API gateway, middleware, or integration agreement level.

Why this matters: DPDPA §6 requires valid consent from the Data Principal before processing personal data. Functions that process personal data without verifying consent violate fundamental DPDPA requirements.

Offending Code

```
184 public void addShareAccountChargePaidBy(final ShareAccountChargePaidBy chargePaidBy) {
185     this.shareAccountChargesPaid.add(chargePaidBy);
186 }
```

Remediation

Verify that consent is checked before processing personal data. This may be handled at the middleware or API gateway level. If consent is already verified upstream, this finding is a false positive and can be suppressed via `.scrutornignore`.

Software Composition (Dependencies)

79 dependencies inventoried; 52 checked against known-vulnerability data (OSV / NVD). **7 known vulnerabilities** found in 4 components — 0 critical, 2 high, 5 medium, 0 low.

27 dependencies could not be checked. The build file names them without a version — it is supplied at build time by a dependency BOM, a version catalog or a parent POM. They are listed in the inventory below, but no vulnerability conclusion is possible for them from source alone.

Scope. This analysis covers the dependencies your build files declare directly. No resolved dependency tree (lock file or SBOM) was present, so transitively-pulled packages — which carry the majority of known vulnerabilities — were not inventoried and are not represented above. Providing a lock file or a resolved CycloneDX SBOM for your build system would extend this analysis to the full tree.

Highest-severity findings

- **GHSA-j92g-9f8w-j867** in postgresql (maven) — High → upgrade to 42.7.12
- **GHSA-5568-6qcg-g7fx** in activemq-client (maven) — High → upgrade to 5.19.4

The complete Software Bill of Materials (CycloneDX / SPDX) and the full dependency inventory are available in the Scrutora dashboard under Dependencies.

Remediation Roadmap

The following prioritised action plan groups violations by severity and provides specific remediation steps. Address CRITICAL items immediately to eliminate immediate risk of regulatory non-compliance.

Item counts below are **grouped findings** — each may consolidate several occurrences of the same issue across files. The severity totals on the cover and executive summary count every individual occurrence, so those figures are higher.

■ CRITICAL — 7 item(s) | Target: Immediately

1. [PCI-4.1.1] TLS certificate verification disabled (X509TrustManager()) -- enables man-in-the-middle attacks on cardholder data (2 occurrences)

(fineract-client-feign/src/main/java/org/apache/fineract/client/feign/FineractFeignClientConfig.java:177) [Confirmed]

→ Enable TLS certificate verification. In Python: verify=True (default). In Go: remove InsecureSkipVerify. In Node.js: rejectUnauthorized=true. Use proper CA certificates instead of disabling validation.

2. [PCI-4.1.1] TLS certificate verification disabled (X509TrustManager()) -- enables man-in-the-middle attacks on cardholder data (fineract-client/src/main/java/org/apache/fineract/client/util/FineractClient.java:514) [Confirmed]

→ Enable TLS certificate verification. In Python: verify=True (default). In Go: remove InsecureSkipVerify. In Node.js: rejectUnauthorized=true. Use proper CA certificates instead of disabling validation.

3. [INPUT-001] SQL query constructed via string concatenation/interpolation in DatatableReadServiceImpl.queryDataTableAdvanced. This is vulnerable to SQL injection attacks.

(fineract-provider/src/main/java/org/apache/fineract/infrastructure/dataqueries/service/DatatableReadServiceImpl.java:202 — queryDataTableAdvanced) [Likely]

→ Use parameterized queries instead of string concatenation. Python: cursor.execute('SELECT * FROM users WHERE id = %s', (user_id,)). JS: connection.query('SELECT * FROM users WHERE id = ?', [userId]). Java: use PreparedStatement with ? placeholders.

4. [INPUT-001] SQL query constructed via string concatenation/interpolation in DatatableWriteServiceImpl.deleteDatatable. This is vulnerable to SQL injection attacks.

(fineract-provider/src/main/java/org/apache/fineract/infrastructure/dataqueries/service/DatatableWriteServiceImpl.java:536 — deleteDatatable) [Likely]

→ Use parameterized queries instead of string concatenation. Python: cursor.execute('SELECT * FROM users WHERE id = %s', (user_id,)). JS: connection.query('SELECT * FROM users WHERE id = ?', [userId]). Java: use PreparedStatement with ? placeholders.

5. [INPUT-001] SQL query constructed via string concatenation/interpolation in GenericDataServiceImpl.wrapSQL. This is vulnerable to SQL injection attacks.

(fineract-provider/src/main/java/org/apache/fineract/infrastructure/dataqueries/service/GenericDataServiceImpl.java:228 — wrapSQL) [Likely]

→ Use parameterized queries instead of string concatenation. Python: cursor.execute('SELECT * FROM users WHERE id = %s', (user_id,)). JS: connection.query('SELECT * FROM users WHERE id = ?', [userId]). Java: use PreparedStatement with ? placeholders.

6. [INPUT-001] SQL query constructed via string concatenation/interpolation in**SavingsAccountTransactionsSearchServiceImpl.searchTransactions. This is vulnerable to SQL injection attacks. (****fineract-provider/src/main/java/org/apache/fineract/portfolio/savings/service/search/SavingsAccountTransactionsSearchServiceImpl.java:117 — searchTransactions) [Likely]**

→ Use parameterized queries instead of string concatenation. Python: `cursor.execute('SELECT * FROM users WHERE id = %s', (user_id,))`. JS: `connection.query('SELECT * FROM users WHERE id = ?', [userId])`. Java: use `PreparedStatement` with `?` placeholders.

7. [INPUT-001] SQL query constructed via string concatenation/interpolation in**SavingsAccountTransactionsSearchServiceImpl.queryAdvanced. This is vulnerable to SQL injection attacks. (fineract-provider/src/main/java/org/apache/fineract/portfolio/savings/service/search/SavingsAccountTransactionsSearchServiceImpl.java:269****— queryAdvanced) [Likely]**

→ Use parameterized queries instead of string concatenation. Python: `cursor.execute('SELECT * FROM users WHERE id = %s', (user_id,))`. JS: `connection.query('SELECT * FROM users WHERE id = ?', [userId])`. Java: use `PreparedStatement` with `?` placeholders.

■ HIGH — 14 item(s) | Target: Within 30 days**1. [TRANSFER-001] Insecure SSL/TLS configuration — certificate verification disabled (2 occurrences)****(fineract-client-feign/src/main/java/org/apache/fineract/client/feign/FineractFeignClientConfig.java:194 — ?) [Confirmed]**

→ Do not disable SSL certificate verification. This allows man-in-the-middle attacks on data transfers. Remove `verify=False`, `rejectUnauthorized: false`, or similar certificate bypass settings.

2. [NOTICE-001] Strong PII ('Passport') collected in a project with no notice artefact (no /privacy or /notice route, NOTICE_URL config, or privacy-notice surface). DPDPA §5(1) requires the notice to accompany or precede the consent request. (fineract-db/old-schema-files/0002-mifosx-base-reference-data-utf8.sql:291) [Likely]

→ Add a /privacy or /notice surface (or NOTICE_URL) returning the §5(1) notice, linked from the signup flow.

3. [STORE-001] Sensitive data flows from pii field access at line 33 to storage at line 40 without encryption. Note: ORM storage operations are commonly backed by database-level encryption at rest**(fineract-loan/src/main/java/org/apache/fineract/portfolio/loanaccount/service/GLIMAccountInfoWritePlatformServiceImpl.java:40 — createGLIMAccount) [Likely] ~2-4 hours**

→ Encrypt `accountNumber` before writing to storage at line 40. Use AES-256-GCM for symmetric encryption or `bcrypt/Argon2` for passwords. Note: if your database uses encryption at rest (e.g., AWS RDS, Azure SQL TDE, GCP Cloud SQL), this finding may already be mitigated at the infrastructure level.

4. [PII-001] PII flows from pii field access at line 56 to log statement at line 71 without masking**(fineract-provider/src/main/java/org/apache/fineract/infrastructure/security/service/OidcAppUserResolutionServiceImpl.java:71 — resolveOrCreate) [Needs Review]**

→ Mask or redact email before logging. Replace the log statement at line 71 with a version that masks PII fields: e.g., `maskEmail(user.email)` or `redact(data, ['email', 'phone'])`.

5. [STORE-001] Sensitive data flows from pii field access at line 93 to storage at line 104 without encryption. Note: ORM storage operations are commonly backed by database-level encryption at rest**(fineract-provider/src/main/java/org/apache/fineract/infrastructure/security/service/TwoFactorServiceImpl.java:104 —**

createNewOTPToken) [Likely] ~2-4 hours

→ Encrypt cannot_change_password, email, firstname before writing to storage at line 104. Use AES-256-GCM for symmetric encryption or bcrypt/Argon2 for passwords. Note: if your database uses encryption at rest (e.g., AWS RDS, Azure SQL TDE, GCP Cloud SQL), this finding may already be mitigated at the infrastructure level.

6. [STORE-001] Sensitive data flows from pii field access at line 126 to storage at line 146 without encryption. Note: ORM storage operations are commonly backed by database-level encryption at rest

(fineract-provider/src/main/java/org/apache/fineract/infrastructure/security/service/TwoFactorServiceImpl.java:146 —

createAccessTokenFromOTP) [Likely] ~2-4 hours

→ Encrypt cannot_change_password, email, firstname before writing to storage at line 146. Use AES-256-GCM for symmetric encryption or bcrypt/Argon2 for passwords. Note: if your database uses encryption at rest (e.g., AWS RDS, Azure SQL TDE, GCP Cloud SQL), this finding may already be mitigated at the infrastructure level.

7. [STORE-001] Sensitive data flows from pii field access at line 159 to storage at line 172 without encryption. Note: ORM storage operations are commonly backed by database-level encryption at rest (+6 more across 6 file(s): AccountNumberFormatRepositoryWrapper.java, TwoFactorServiceImpl.java, ClientRepositoryWrapper.java, ClientWritePlatformServiceJpaRepositoryImpl.java, GroupSavingsIndividualMonitoringWritePlatformServiceImpl.java, ... +1 more)

(fineract-provider/src/main/java/org/apache/fineract/infrastructure/security/service/TwoFactorServiceImpl.java:172 —

invalidateAccessToken) [Likely] ~2-4 hours

→ Encrypt cannot_change_password, email, firstname before writing to storage at line 172. Use AES-256-GCM for symmetric encryption or bcrypt/Argon2 for passwords. Note: if your database uses encryption at rest (e.g., AWS RDS, Azure SQL TDE, GCP Cloud SQL), this finding may already be mitigated at the infrastructure level.

8. [AUTH-001] Method 'retrieveOne' in controller class 'StaffApiResource' accesses PHI without an authorization or access-control check. (fineract-provider/src/main/java/org/apache/fineract/organisation/staff/api/StaffApiResource.java:102 —

retrieveOne) [Likely] ~4-8 hours

→ Add @PreAuthorize or @Secured to 'retrieveOne': @PreAuthorize("hasRole('DOCTOR') or hasRole('NURSE')")
public T retrieveOne(...) { ... } Or apply @Secured at class level on StaffApiResource. Record every PHI access in an audit trail.

9. [PII-001] PII flows from pii field access at line 45 to log statement at line 50 without masking

(fineract-provider/src/main/java/org/apache/fineract/useradministration/service/ForgotPasswordServiceImpl.java:50 —

requestPasswordReset) [Needs Review]

→ Mask or redact email before logging. Replace the log statement at line 50 with a version that masks PII fields: e.g., maskEmail(user.email) or redact(data, ['email', 'phone']).

10. [PII-002] PII field 'username' exposed in error response in AuthenticationApiResource.authenticate

(fineract-security/src/main/java/org/apache/fineract/infrastructure/security/api/AuthenticationApiResource.java:96 — authenticate) [Needs Review]

→ Return generic error messages to clients. Never include personal data like 'username' in HTTP error responses or exception messages visible to users.

11. [IAC-K8S-NETPOL-001] K8s workloads declared but no NetworkPolicy anywhere in the manifest set. CIS K8s 5.3.2 — without NetworkPolicy, all pods can talk to all pods. (kubernetes/fineract-mifoscommunity-deployment.yml:1)

[Confirmed]

→ Add a default-deny NetworkPolicy in every namespace that holds personal data, then allow specific traffic via additional NetworkPolicy resources.

12. [IAC-K8S-RUN-ROOT-001] K8s container 'mifos-community' in Deployment

'Deployment/default/mifos-community' is configured to run as root. CIS K8s 5.2.6 requires runAsNonRoot = true.

(kubernetes/fineract-mifoscommunity-deployment.yml:76) [Confirmed]

→ Set securityContext.runAsNonRoot = true and securityContext.runAsUser to a non-zero UID. Build the image with a non-root USER directive (see IAC-DOCKER-ROOT-001).

13. [IAC-K8S-RUN-ROOT-001] K8s container 'fineract-server' in Deployment 'Deployment/default/fineract-server' is configured to run as root. CIS K8s 5.2.6 requires runAsNonRoot = true. (kubernetes/fineract-server-deployment.yml:37)

[Confirmed]

→ Set securityContext.runAsNonRoot = true and securityContext.runAsUser to a non-zero UID. Build the image with a non-root USER directive (see IAC-DOCKER-ROOT-001).

14. [IAC-K8S-RUN-ROOT-001] K8s container 'mysql' in Deployment 'Deployment/default/fineractmysql' is configured to run as root. CIS K8s 5.2.6 requires runAsNonRoot = true. (kubernetes/fineractmysql-deployment.yml:68)

[Confirmed]

→ Set securityContext.runAsNonRoot = true and securityContext.runAsUser to a non-zero UID. Build the image with a non-root USER directive (see IAC-DOCKER-ROOT-001).

■ MEDIUM — 24 item(s) | Target: Within 90 days

1. [DPDPA-SVC-001] DPDPA §8(10) requires a grievance redressal mechanism. No GrievanceController / grievance endpoint found anywhere. (2 occurrences) (custom/acme/event/externalevent/src/main/java/com/acme/fineract/event/externalevent/AcmeExternalEventSourceProviderConfig.java:28) [Confirmed]

→ Add a GrievanceController with POST /grievance that records Data-Principal complaints and routes them to the Data Protection Officer within the statutory SLA.

2. [DPDPA-SDF-001] Project shows Significant-Data-Fiduciary signals (lending/insurance/health/telecom) but no DPIA / independent-auditor reference. DPDPA §10(2) requires a DPO in India, an independent data auditor and periodic DPIAs. (custom/acme/event/externalevent/src/main/java/com/acme/fineract/event/externalevent/AcmeExternalEventSourceProviderConfig.java:28) [Needs Review]

→ Ship a DPIA artefact and engage an independent data auditor, or set an explicit IS_SIGNIFICANT_DF=false if not notified under §10(1).

3. [RETENTION-001] PII data model found but no scheduled deletion/cleanup job detected — GDPR Article 5(1)(e) requires data minimization with defined retention periods

(fineract-command-jdbc/src/main/java/org/apache/fineract/command/jdbc/store/domain/CommandEntity.java:33 — ?) [Likely]

→ Add a scheduled task (e.g. Celery beat, @Scheduled cron, node-cron) that periodically purges or anonymizes expired personal data. This is required for GDPR Article 5(1)(e) storage limitation compliance.

4. [RETENTION-001] Data model 'CommandSource' has PII fields but no retention/deletion mechanism

(fineract-core/src/main/java/org/apache/fineract/commands/domain/CommandSource.java:41 — ?) [Needs Review]

→ Add soft-delete (deleted_at) and retention period (retention_expires_at) fields to 'CommandSource'. This supports GDPR Article 17 (right to erasure) and Article 5(1)(e) (storage limitation). Note: retention may be handled at the application layer.

5. [PII-001] PII field 'remoteaddr' logged without masking in CallerIpTrackingFilter.getClientIpAddress

(fineract-core/src/main/java/org/apache/fineract/infrastructure/core/filters/CallerIpTrackingFilter.java:62 — getClientIpAddress) [Needs Review]

→ Remove or mask the 'remoteaddr' field before logging. Use anonymized identifiers (e.g. user ID) instead of PII.

6. [PII-001] PII field 'ipaddress' logged without masking in CallerIpTrackingFilter.handleClientIp

(fineract-core/src/main/java/org/apache/fineract/infrastructure/core/filters/CallerIpTrackingFilter.java:82 — handleClientIp) [Needs Review]

→ Remove or mask the 'ipaddress' field before logging. Use anonymized identifiers (e.g. user ID) instead of PII.

7. [RETENTION-001] Data model 'Staff' has PII fields but no retention/deletion mechanism

(fineract-core/src/main/java/org/apache/fineract/organisation/staff/domain/Staff.java:33 — ?) [Needs Review]

→ Add soft-delete (deleted_at) and retention period (retention_expires_at) fields to 'Staff'. This supports GDPR Article 17 (right to erasure) and Article 5(1)(e) (storage limitation). Note: retention may be handled at the application layer.

8. [GRIEVANCE-001] Strong PII ('Passport') collected by a Data Fiduciary with no grievance/redressal mechanism or published contact (no /grievance, /complaint, /contact-us route, grievance-officer, or grievance/privacy mailbox). DPDPA §8(10) requires a readily-available means of redress for Data Principal grievances.

(fineract-db/old-schema-files/0002-mifosx-base-reference-data-utf8.sql:291) [Likely]

→ Expose a public grievance/redressal endpoint (e.g. POST /grievance) with a response SLA and publish the grievance officer's business contact in the privacy notice.

9. [CONSENT-001] No consent mechanism exists anywhere in this codebase, yet personal data is collected and stored (first seen at GLIMAccountInfoWritePlatformServiceImpl.java:40). DPDPA §6(1) requires free, specific, informed and unambiguous consent before processing, and §6(4)-(6) require a record of it and a means to withdraw.

(fineract-loan/src/main/java/org/apache/fineract/portfolio/loanaccount/service/GLIMAccountInfoWritePlatformServiceImpl.java:40 — createGLIMAccount) [Likely]

→ Verify consent before processing personal data at line 40. Call a consent verification function (e.g., hasConsent(userId, 'data_processing')) before the data operation.

10. [RETENTION-001] Data model 'AdHoc' has PII fields but no retention/deletion mechanism (+5 more across 5 file(s): AdHoc.java, EmailMessage.java, CreditReport.java, ClientFamilyMembers.java, Guarantor.java)

(fineract-provider/src/main/java/org/apache/fineract/adhocquery/domain/AdHoc.java:35 — ?) [Needs Review]

→ Add soft-delete (deleted_at) and retention period (retention_expires_at) fields to 'AdHoc'. This supports GDPR Article 17 (right to erasure) and Article 5(1)(e) (storage limitation). Note: retention may be handled at the application layer.

11. [LOG-001] Personal data [accountNumber] detected in logging call 'log.debug' in CheckDueInstallmentsBusinessStep.run. Personal data must never appear in application logs.

(fineract-provider/src/main/java/org/apache/fineract/cob/loan/CheckDueInstallmentsBusinessStep.java:58 — run) [Confirmed] ~1-2 hours

→ Under the DPDPA, 'accountNumber' may constitute personal data and should not be logged in plain text. Remove personal data from log messages. Recommended fixes: (1) Replace personal data values with opaque surrogate keys

(UUID / DB primary key): `logger.info('Record updated: id={}', record.id)` — never log 'accountNumber' directly. (2) Hash the value if correlation is needed for debugging: `logger.debug('accountNumber_hash={}', sha256(accountNumber)[:8])`. (3) Use structured logging with a redaction filter in the logging pipeline. (4) If the context is required for auditing, write to a dedicated access-controlled audit log rather than the application/error log. (5) Use a masking library (scrubadub, fast-redact, pino-noir, Serilog.Enrichers.Sensitive) to automatically redact personal data before logging.

12. [LOG-001] Personal data [accountNumber] detected in logging call 'log.error' in

CheckDueInstallmentsBusinessStep.run. Personal data must never appear in application logs.

(fineract-provider/src/main/java/org/apache/fineract/cob/loan/CheckDueInstallmentsBusinessStep.java:80 — run) [Confirmed] ~1-2 hours

→ Under the DPDPA, 'accountNumber' may constitute personal data and should not be logged in plain text. Remove personal data from log messages. Recommended fixes: (1) Replace personal data values with opaque surrogate keys (UUID / DB primary key): `logger.info('Record updated: id={}', record.id)` — never log 'accountNumber' directly. (2) Hash the value if correlation is needed for debugging: `logger.debug('accountNumber_hash={}', sha256(accountNumber)[:8])`. (3) Use structured logging with a redaction filter in the logging pipeline. (4) If the context is required for auditing, write to a dedicated access-controlled audit log rather than the application/error log. (5) Use a masking library (scrubadub, fast-redact, pino-noir, Serilog.Enrichers.Sensitive) to automatically redact personal data before logging.

13. [LOG-001] Personal data [accountNumber] detected in logging call 'log.debug' in

CheckDueInstallmentsBusinessStep.execute. Personal data must never appear in application logs.

(fineract-provider/src/main/java/org/apache/fineract/cob/loan/CheckDueInstallmentsBusinessStep.java:90 — execute) [Confirmed] ~1-2 hours

→ Under the DPDPA, 'accountNumber' may constitute personal data and should not be logged in plain text. Remove personal data from log messages. Recommended fixes: (1) Replace personal data values with opaque surrogate keys (UUID / DB primary key): `logger.info('Record updated: id={}', record.id)` — never log 'accountNumber' directly. (2) Hash the value if correlation is needed for debugging: `logger.debug('accountNumber_hash={}', sha256(accountNumber)[:8])`. (3) Use structured logging with a redaction filter in the logging pipeline. (4) If the context is required for auditing, write to a dedicated access-controlled audit log rather than the application/error log. (5) Use a masking library (scrubadub, fast-redact, pino-noir, Serilog.Enrichers.Sensitive) to automatically redact personal data before logging.

14. [LOG-001] Personal data [accountNumber] detected in logging call 'log.debug' in

SetLoanDelinquencyTagsBusinessStep.run. Personal data must never appear in application logs. (+9 more across 6 file(s): SetLoanDelinquencyTagsBusinessStep.java, EmailCampaignWritePlatformCommandHandlerImpl.java, OidcAppUserResolutionServiceImpl.java, ClientRepositoryWrapper.java, ForgotPasswordServiceImpl.java, ... +1 more) (fineract-provider/src/main/java/org/apache/fineract/cob/loan/SetLoanDelinquencyTagsBusinessStep.java:67 — run) [Confirmed]

~1-2 hours

→ Under the DPDPA, 'accountNumber' may constitute personal data and should not be logged in plain text. Remove personal data from log messages. Recommended fixes: (1) Replace personal data values with opaque surrogate keys (UUID / DB primary key): `logger.info('Record updated: id={}', record.id)` — never log 'accountNumber' directly. (2) Hash the value if correlation is needed for debugging: `logger.debug('accountNumber_hash={}', sha256(accountNumber)[:8])`. (3) Use structured logging with a redaction filter in the logging pipeline. (4) If the context is required for auditing, write to a dedicated access-controlled audit log rather than the application/error log. (5) Use a masking library (scrubadub, fast-redact, pino-noir, Serilog.Enrichers.Sensitive) to automatically redact personal data before logging.

15. [DATA-ACCURACY-001] Decision-driving function 'reject' has no input validation. DPDPA §8(3) requires completeness, accuracy and consistency of personal data used in decisions affecting the Data Principal.

(fineract-provider/src/main/java/org/apache/fineract/portfolio/shareaccounts/domain/ShareAccount.java:431) [Likely]

→ Validate inputs (schema / DTO / explicit guards on PAN, Aadhaar, DOB, income) before they reach the decision.

16. [IAC-K8S-RO-FS-001] K8s container 'mifos-community' in Deployment 'Deployment/default/mifos-community' does not set readOnlyRootFilesystem = true. CIS K8s 5.7.4. (kubernetes/fineract-mifoscommunity-deployment.yml:76)

[Confirmed]

→ Set securityContext.readOnlyRootFilesystem = true. If the container needs writeable temp space, mount an emptyDir volume.

17. [IAC-K8S-CAPS-001] K8s container 'mifos-community' in Deployment 'Deployment/default/mifos-community' does not drop ALL capabilities. CIS K8s 5.7 best practice is `drop: [ALL]` then add back the minimum set.

(kubernetes/fineract-mifoscommunity-deployment.yml:76) [Likely]

→ Add `securityContext.capabilities.drop: [ALL]` and explicitly add only the caps the workload uses.

18. [IAC-K8S-RESOURCES-001] K8s container 'init-myservice' in Deployment 'Deployment/default/mifos-community' has no resources.limits/requests. CIS K8s 5.7.3.

(kubernetes/fineract-mifoscommunity-deployment.yml:76) [Likely]

→ Set both resources.requests (minimum reserved) and resources.limits (maximum allowed) for cpu + memory.

19. [IAC-K8S-RO-FS-001] K8s container 'fineract-server' in Deployment 'Deployment/default/fineract-server' does not set readOnlyRootFilesystem = true. CIS K8s 5.7.4. (kubernetes/fineract-server-deployment.yml:37) [Confirmed]

→ Set securityContext.readOnlyRootFilesystem = true. If the container needs writeable temp space, mount an emptyDir volume.

20. [IAC-K8S-CAPS-001] K8s container 'fineract-server' in Deployment 'Deployment/default/fineract-server' does not drop ALL capabilities. CIS K8s 5.7 best practice is `drop: [ALL]` then add back the minimum set.

(kubernetes/fineract-server-deployment.yml:37) [Likely]

→ Add `securityContext.capabilities.drop: [ALL]` and explicitly add only the caps the workload uses.

21. [IAC-K8S-RESOURCES-001] K8s container 'init-mysdb' in Deployment 'Deployment/default/fineract-server' has no resources.limits/requests. CIS K8s 5.7.3. (kubernetes/fineract-server-deployment.yml:37) [Likely]

→ Set both resources.requests (minimum reserved) and resources.limits (maximum allowed) for cpu + memory.

22. [IAC-K8S-IMG-LATEST-001] K8s container 'fineract-server' in Deployment 'Deployment/default/fineract-server' uses image 'apache/fineract:latest' — :latest or no tag, no digest pin. CIS K8s 1.5.2.

(kubernetes/fineract-server-deployment.yml:37) [Confirmed]

→ Pin to a specific tag AND digest: `image: myorg/myapp:v1.4.2@sha256:<digest>`.

23. [IAC-K8S-RO-FS-001] K8s container 'mysql' in Deployment 'Deployment/default/fineractmysql' does not set readOnlyRootFilesystem = true. CIS K8s 5.7.4. (kubernetes/fineractmysql-deployment.yml:68) [Confirmed]

→ Set securityContext.readOnlyRootFilesystem = true. If the container needs writeable temp space, mount an emptyDir volume.

24. [IAC-K8S-CAPS-001] K8s container 'mysql' in Deployment 'Deployment/default/fineractmysql' does not drop ALL capabilities. CIS K8s 5.7 best practice is `drop: [ALL]` then add back the minimum set.

(kubernetes/fineractmysql-deployment.yml:68) [Likely]

→ Add `securityContext.capabilities.drop: [ALL]` and explicitly add only the caps the workload uses.

■ LOW — 4 item(s) | Target: Within 6 months

1. [DPO-001] Significant-Data-Fiduciary vertical collecting strong PII ('Passport') with no published DPO / data-protection contact (no /dpo or /privacy-contact route, DPO designation, or dpo/privacy mailbox). DPDPA §8(9) requires publishing a contact; §10 requires a Significant Data Fiduciary to appoint an India-based DPO.

(fineract-db/old-schema-files/0002-mifosx-base-reference-data-utf8.sql:291) [Needs Review]

→ Publish the DPO / contact-person details (designation, email, address) on a stable surface (e.g. /dpo or /privacy-contact) and, if a Significant Data Fiduciary, appoint an India-based DPO reporting to the board.

2. [CONSENT-001] No consent verification found before data processing in AccountTransferDetails.addAccountTransferTransaction. Note: consent may be handled at the API gateway, middleware, or integration agreement level.

(fineract-provider/src/main/java/org/apache/fineract/portfolio/account/domain/AccountTransferDetails.java:132 —

addAccountTransferTransaction) [Likely]

→ Verify that consent is checked before processing personal data. This may be handled at the middleware or API gateway level. If consent is already verified upstream, this finding is a false positive and can be suppressed via .scrutornignore.

3. [CONSENT-001] No consent verification found before data processing in ShareAccount.addShareAccountCharge. Note: consent may be handled at the API gateway, middleware, or integration agreement level.

(fineract-provider/src/main/java/org/apache/fineract/portfolio/shareaccounts/domain/ShareAccount.java:390 — addShareAccountCharge)

[Likely]

→ Verify that consent is checked before processing personal data. This may be handled at the middleware or API gateway level. If consent is already verified upstream, this finding is a false positive and can be suppressed via .scrutornignore.

4. [CONSENT-001] No consent verification found before data processing in ShareAccountTransaction.addShareAccountChargePaidBy. Note: consent may be handled at the API gateway, middleware, or integration agreement level.

(fineract-provider/src/main/java/org/apache/fineract/portfolio/shareaccounts/domain/ShareAccountTransaction.java:184 —

addShareAccountChargePaidBy) [Likely]

→ Verify that consent is checked before processing personal data. This may be handled at the middleware or API gateway level. If consent is already verified upstream, this finding is a false positive and can be suppressed via .scrutornignore.

Next Steps: After remediating the above findings, re-run the Scrutora scanner to obtain an updated DPDPA compliance report. Consider integrating the scanner into your CI/CD pipeline to catch violations before they reach production.

Appendix

A. DPDPA Control Checklist

Control Area	DPDPA Ref	Status	Description
Access Control	§8(5)	ATTENTION	Reasonable security safeguards for access control
Transmission Security	§8(5)	PASS	Encryption of personal data during transmission
Encryption at Rest	§8(5)	ATTENTION	Encryption of stored personal data
Cryptographic Standards	§8(5)	PASS	Use of approved cryptographic algorithms
Session Management	§8(5)	PASS	Automatic logoff and session timeout
Authentication	§8(5)	PASS	Password strength and authentication controls
Key Management	§8(5)	PASS	Encryption key lifecycle and secure storage
Backup & Recovery	§8(5)	PASS	Data backup and disaster recovery
Purpose Limitation	§4(2)	FAIL	Limit data processing to stated purpose
Consent Management	§6, §7	ATTENTION	Obtain and manage data principal consent
Breach Notification	§8(5)	PASS	Audit controls for breach detection and notification
Data Erasure	§8(7)	ATTENTION	Erase personal data when no longer needed
Cross-Border Transfer	§16, §17	FAIL	Safeguards for data transfer outside India
PII in Logs	§4(2), §8(5)	REVIEW	No personal data in application logs
PII in Errors	§8(5)	REVIEW	No personal data in error responses
SQL Injection Prevention	§8(5)	ATTENTION	Parameterized queries for data protection
XSS Prevention	§8(5)	PASS	Output encoding to prevent cross-site scripting
CSRF Prevention	§8(5)	PASS	CSRF tokens on state-changing operations
Secure Development	§8(5)	PASS	Secure software development practices
Error Handling	§8(5)	PASS	Secure error handling without data leakage

B. Scan Metadata

Property	Value
Scanner	Scrutora
Scan Date	2026-08-20 09:27:55 UTC
Target	Nirvahana/fineract@develop
Frameworks	DPDPA
Files Scanned	5288

Files Excluded	1906
Entities Checked	1559015
Rules Executed	336
Scan Duration	952.2 seconds
Languages	._k8s_manifest (4), .java (5270), .sql (14)
Violations Found	70

C. Control Coverage Summary

DPDPA: 223 of 243 controls passed (92% coverage)

D. Scope & Limitations

What this report evaluates: Static analysis of source code for DPDPA technical controls. Covers encryption at rest, transmission security, access controls, audit logging, session management, password policies, key management, and backup procedures. Additionally evaluates consent management, purpose limitation, data erasure, breach notification, and cross-border transfer controls.

What this report does NOT evaluate: Runtime behaviour, network configuration, physical safeguards, administrative policies, workforce training, or breach notification procedures. Infrastructure-level controls (firewall rules, VPN, IDS/IPS) are outside scope.

Methodology: Multi-phase static analysis using tree-sitter AST parsers (12 programming languages) with interprocedural taint tracking, cross-file data flow analysis, and context-aware false positive reduction. Includes SBOM generation (CycloneDX / SPDX), policy-as-code custom rules, auto-fix suggestions, and sensitive-data flow mapping.

Disclaimer: This report is generated by automated tooling and should not be considered a substitute for a comprehensive DPDPA compliance assessment performed by a qualified security professional. A clean scan does not guarantee regulatory compliance.

E. References & Resources

DPDPA 2023 Full Text: The Digital Personal Data Protection Act, 2023 — published by the Ministry of Law and Justice

MeitY Draft Rules 2025: Draft Digital Personal Data Protection Rules (Ministry of Electronics and Information Technology)

Data Protection Board: Notifications, guidelines, and orders issued by the Data Protection Board of India under §40

OWASP Top 10 / ASVS: OWASP Application Security Verification Standard and Top 10 — application-security baselines

Scrutora Docs: Visit scrutora.com for scanner documentation and best practices

F. Report Integrity

SHA-256 Digest: c13c68dec76dc791c0c86510167adcc4910847fcc1cc4357f834f32c65d1cc10

This cryptographic hash covers the scan metadata and results. Any modification to the report content will produce a different hash, enabling tamper detection.