

Data Privacy Act Compliance Report

Document: Digi-AMS-Final_V2_LPChecked (2).docx

Analysis Date: 2025-05-30

Compliance Status: NON-COMPLIANT

Risk Level: CRITICAL

Summary Statistics

Metric	Count
Total PII Instances	405
Sensitive PII Instances	9
Regular PII Instances	396
Total Violations	6
Consent Indicators	6
Purpose Indicators	10

Executive Summary

The document 'Digi-AMS-Final_V2_LPChecked (2).docx' has been analyzed for compliance with the Republic Act No. 10173 (Data Privacy Act of 2012). The analysis indicates that the document is **NON-COMPLIANT** with DPA requirements and requires immediate attention.

Key Findings:

- 405 instances of personal information detected
- 9 instances of sensitive personal information found
- 6 DPA violations identified
- Risk level assessed as: CRITICAL

Immediate Actions Required:

- Implement a Consent Mechanism: Develop and implement a robust consent mechanism to ensure that data subjects give their explicit, informed, and freely given consent for the collection and processing of their personal information.
- Enhance Transparency: Ensure that the purposes for which personal information is collected, processed, and used are clearly communicated to the data subjects.
- Protect Sensitive Personal Information: Obtain specific consent from data subjects before processing sensitive personal information, such as religious information.

Personal Information Analysis

Regular Personal Information:

- EMAIL_ADDRESS: ejrcalingasan03118@usep.edu.ph (Confidence: 1.00)
- EMAIL_ADDRESS: Cmldeasis02769@usep.edu.ph (Confidence: 1.00)
- EMAIL_ADDRESS: kbomblero03456@usep.edu.ph (Confidence: 1.00)
- LOCATION: Calingasan (Confidence: 0.85)
- PERSON: Edwin James R. De Asis (Confidence: 0.85)
- PERSON: Crist Mar L. Omblero (Confidence: 0.85)
- PERSON: Kobe Bryan K. Adviser (Confidence: 0.85)
- PERSON: Pelias (Confidence: 0.85)
- PERSON: Leah O. (Confidence: 0.85)
- DATE_TIME: May 2025 (Confidence: 0.85)

Sensitive Personal Information:

- PH_PHONE: 09915517362 (Confidence: 1.00)
- RELIGIOUS_INFO: Religion (Confidence: 1.00)
- RELIGIOUS_INFO: Catholic (Confidence: 1.00)
- PH_PHONE: 09949530454 (Confidence: 1.00)
- RELIGIOUS_INFO: Religion (Confidence: 1.00)
- RELIGIOUS_INFO: Catholic (Confidence: 1.00)
- PH_PHONE: 09538907413 (Confidence: 1.00)
- RELIGIOUS_INFO: Religion (Confidence: 1.00)
- RELIGIOUS_INFO: Catholic (Confidence: 1.00)

Consent Indicators:

- Found: 'consent'
- Found: 'allow'
- Found: 'allow'
- Found: 'allow'
- Found: 'approve'

Purpose Indicators:

- Found: 'purpose'
- Found: 'purpose'
- Found: 'purpose'
- Found: 'purpose'
- Found: 'purpose'

DPA Violations Identified

Violation 1: Section 11

Section: Section 11

Severity: MEDIUM

Description: The document does not specify the purposes for which personal information is collected, processed, or used. This violates the principle of transparency required by Section 11.

Details: Section 11: General Data Privacy Principles

Violation 2: Section 12

Section: Section 12

Severity: HIGH

Description: There is no evidence that the data subjects have given their consent for the collection and processing of their personal information. This is a critical requirement under Section 12.

Details: Section 12: Criteria for Lawful Processing of Personal Information

Violation 3: Section 13

Section: Section 13

Severity: CRITICAL

Description: The document includes religious information, which is considered sensitive personal information. There is no indication that consent was obtained from the data subjects for processing this information.

Details: Section 13: Sensitive Personal Information and Privileged Information

Violation 4: Section 16

Section: Section 16

Severity: MEDIUM

Description: The document does not provide the data subjects with information about the personal information to be processed, the purposes of processing, and their rights as data subjects.

Details: Section 16: Rights of the Data Subject

Violation 5: Section 20

Section: Section 20

Severity: HIGH

Description: The document does not specify the security measures implemented to protect personal information against accidental or unlawful destruction, alteration, and disclosure.

Details: Section 20: Security of Personal Information

Violation 6: Section 21

Section: Section 21

Severity: HIGH

Description: There is no clear indication of who is responsible for the personal information under the control or custody of the system, nor any mention of contractual or other means to ensure a comparable level of protection.

Details: Section 21: Principle of Accountability

Recommendations

CRITICAL Priority Actions

Implement a Consent Mechanism

Description: Develop and implement a robust consent mechanism to ensure that data subjects give their explicit, informed, and freely given consent for the collection and processing of their personal information.

Reference: Section 12

Protect Sensitive Personal Information

Description: Obtain specific consent from data subjects before processing sensitive personal information, such as religious information.

Reference: Section 13

HIGH Priority Actions

Enhance Transparency

Description: Ensure that the purposes for which personal information is collected, processed, and used are clearly communicated to the data subjects.

Reference: Section 11

Implement Security Measures

Description: Ensure that reasonable and appropriate security measures are implemented to protect personal information against accidental or unlawful destruction, alteration, and disclosure.

Reference: Section 20

Establish Accountability

Description: Clearly define the roles and responsibilities of the personal information controller and ensure that accountability measures are in place.

Reference: Section 21

MEDIUM Priority Actions

Conduct data protection impact assessment

Description: Evaluate the risks and implement appropriate measures for personal data processing

Reference: Section 11 - General Data Privacy Principles

Inform Data Subjects of Their Rights

Description: Provide data subjects with information about their rights, including the right to be informed, the right to access, and the right to rectify their personal information.

Reference: Section 16

Appendix: Technical Details

DPA Sections Referenced:

- Section 11
- Section 11 - General Data Privacy Principles
- Section 12
- Section 13
- Section 16
- Section 20
- Section 21

Analysis Methodology:

This analysis was conducted using automated tools that: 1. Extract text from uploaded documents (PDF, DOCX, images) 2. Detect personal information using pattern recognition and NLP 3. Identify Philippine-specific PII (TIN, SSS, PhilHealth numbers) 4. Check for consent and purpose indicators 5. Apply DPA compliance rules to identify violations 6. Generate risk assessments and recommendations