# Data Privacy Act Compliance Report

**Document:** 494822324_1820085335440790_7594477358422312941_n (3).jpg

**Analysis Date:** 2025-05-30

**Compliance Status:** NON-COMPLIANT

**Risk Level:** HIGH

## Summary Statistics

| Metric | Count |
|---|---|
| Total PII Instances | 1 |
| Sensitive PII Instances | 0 |
| Regular PII Instances | 1 |
| Total Violations | 3 |
| Consent Indicators | 0 |
| Purpose Indicators | 0 |

# Executive Summary

The document '494822324_1820085335440790_7594477358422312941_n (3).jpg' 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:**

• 1 instances of personal information detected
• 0 instances of sensitive personal information found
• 3 DPA violations identified
• Risk level assessed as: HIGH

**Immediate Actions Required:**

• Implement proper consent mechanisms: Establish clear, specific, and informed consent procedures before collecting personal information
• Implement comprehensive security measures: Deploy organizational, physical, and technical safeguards to protect personal information

# Personal Information Analysis

**Regular Personal Information:**
• LOCATION: US (Confidence: 0.85)

**Consent Indicators:**
• No consent indicators found

**Purpose Indicators:**
• No purpose indicators found

# DPA Violations Identified

## *Violation 1: Criteria for Lawful Processing of Personal Information*

**Section:** 12
**Severity:** HIGH
**Description:** Personal information appears to be processed without clear consent from data subjects
**Details:** No details available

## *Violation 2: Security of Personal Information*

**Section:** 20
**Severity:** HIGH
**Description:** Document does not demonstrate adequate security measures for personal information
**Details:** No details available

## *Violation 3: Section 16*

**Section:** Section 16
**Severity:** MEDIUM
**Description:** The document does not provide the data subject with information about their rights, including the right to be informed, the right to access, and the right to correct any inaccuracies in their personal information.
**Details:** Section 16 of the DPA requires that data subjects be informed of their rights before their personal information is entered into a processing system.

# Recommendations

## *CRITICAL Priority Actions*

**Implement proper consent mechanisms**
Description: Establish clear, specific, and informed consent procedures before collecting personal information
Reference: Section 12 - Criteria for Lawful Processing

## *HIGH Priority Actions*

**Implement comprehensive security measures**
Description: Deploy organizational, physical, and technical safeguards to protect personal information
Reference: Section 20 - Security of Personal Information

## *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

**Include Data Subject Rights Information**
Description: Provide the data subject with information about their rights, including the right to be informed, the right to access, and the right to correct any inaccuracies in their personal information, before their personal information is entered into a processing system.
Reference: Section 16 of the DPA

**Implement Visible Security Indicators**
Description: Include visible security warnings or indicators that personal information is being protected against accidental or unlawful destruction, alteration, and disclosure.
Reference: Section 20 of the DPA

# Appendix: Technical Details

**DPA Sections Referenced:**
• 12
• 20
• Section 11 - General Data Privacy Principles
• Section 12 - Criteria for Lawful Processing
• Section 16
• Section 16 of the DPA
• Section 20 - Security of Personal Information
• Section 20 of the DPA

**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