# Data Privacy Act Compliance Report

**Document:** ICT Case Study.pdf

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

**Compliance Status:** NON-COMPLIANT

**Risk Level:** HIGH

## Summary Statistics

| Metric | Count |
|---|---|
| Total PII Instances | 5 |
| Sensitive PII Instances | 0 |
| Regular PII Instances | 5 |
| Total Violations | 6 |
| Consent Indicators | 1 |
| Purpose Indicators | 0 |

# Executive Summary

The document 'ICT Case Study.pdf' 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:**

- 5 instances of personal information detected
- 0 instances of sensitive personal information found
- 6 DPA violations identified
- Risk level assessed as: HIGH

**Immediate Actions Required:**

- Implement comprehensive security measures: Deploy organizational, physical, and technical safeguards to protect personal information
- Implement a Consent Mechanism: Obtain explicit consent from data subjects before collecting and processing their personal information. Ensure that the consent is freely given, specific, and informed.
- Enhance Transparency: Provide clear and accessible information about the purposes of data collection and processing. Inform data subjects about their rights and how they can exercise them.

# Personal Information Analysis

**Regular Personal Information:**

- EMAIL_ADDRESS: flcyap@usep.edu.ph (Confidence: 1.00)
- EMAIL_ADDRESS: kttd@usep.edu.ph (Confidence: 1.00)
- PERSON: STUDY Engr (Confidence: 0.85)
- PERSON: Francis Louise C. Yap OIC Director (Confidence: 0.85)
- PERSON: KTTD (Confidence: 0.85)

**Consent Indicators:**

- Found: 'consent'

**Purpose Indicators:**

- No purpose indicators found

# DPA Violations Identified

### *Violation 1: Security of Personal Information*

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

### *Violation 2: Section 11*

**Section:** Section 11
**Severity:** MEDIUM
**Description:** The document does not specify the purposes for which personal information is collected and processed. This violates the principle of transparency and legitimate purpose.
**Details:** Section 11: General Data Privacy Principles

### *Violation 3: Section 12*

**Section:** Section 12
**Severity:** HIGH
**Description:** There is no evidence that consent was obtained from the data subjects before processing their personal information. This is a critical requirement for lawful processing.
**Details:** Section 12: Criteria for Lawful Processing of Personal Information

### *Violation 4: Section 13*

**Section:** Section 13
**Severity:** CRITICAL
**Description:** The document mentions personal information that could be considered sensitive (e.g., names and email addresses of individuals). There is no indication that specific consent was obtained for processing this information.
**Details:** Section 13: Sensitive Personal Information and Privileged Information

### *Violation 5: Section 16*

**Section:** Section 16
**Severity:** MEDIUM
**Description:** The document does not provide information on how data subjects can be informed about the processing of their personal information or how they can exercise their rights.
**Details:** Section 16: Rights of the Data Subject

### *Violation 6: Section 21*

**Section:** Section 21
**Severity:** HIGH
**Description:** The document does not indicate that the personal information controller is accountable for the personal information under its control or custody.
**Details:** Section 21: Principle of Accountability

## Recommendations

### *CRITICAL Priority Actions*

**Implement a Consent Mechanism**
Description: Obtain explicit consent from data subjects before collecting and processing their personal information. Ensure that the consent is freely given, specific, and informed.
Reference: Section 12

### *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

**Enhance Transparency**
Description: Provide clear and accessible information about the purposes of data collection and processing. Inform data subjects about their rights and how they can exercise them.
Reference: Section 11, Section 16

**Implement Security Measures**
Description: Ensure that reasonable and appropriate security measures are in place to protect personal information against accidental or unlawful destruction, alteration, and disclosure.
Reference: Section 20

### *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

**Establish Accountability**
Description: Ensure that the personal information controller is accountable for the personal information under its control or custody. Implement measures to provide a comparable level of protection when information is transferred to third parties.
Reference: Section 21

# Appendix: Technical Details

**DPA Sections Referenced:**

- 20
- Section 11
- Section 11 - General Data Privacy Principles
- Section 11, Section 16
- Section 12
- Section 13
- Section 16
- Section 20
- Section 20 - Security of Personal Information
- 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