



Template for Reporting a Personal Data Breach to the PDPC

How to use this template:

This template is intended for data controllers and data processors that have experienced a personal data breach and need to report it to the PDPC. Please refrain from including any personal data involved in the breach, such as the names of affected individuals, when filling out this form. If such information is required, we will request it at a later stage. Please ensure the information you provide is as accurate and detailed as possible.

Data Controller/Processor details

Organization Name	
Registration Number	
Address	
Name of Data Protection Officer (DPO)	
Job Title	
Email Address	
Phone Number	
Date	

1. Data Breach Summary

Date of discovery of the personal data breach:

Date when the personal data breach is believed to have occurred:

- 1.1. Brief description of the personal data breach incident including, What happened?, How did it happen?, When did it happen?, Who was involved?:

- 1.2. Type of personal data affected (e.g., names, addresses, social security numbers, financial information, health data):

- 1.3. Special categories of personal data (if applicable): [Specify if any sensitive data, such as health, genetic, biometric data, or data about racial or ethnic origin, was compromised.]

- 1.4. Number of data subjects (individuals) affected:

1.5. Categories of data subjects affected (e.g., customers, employees, suppliers):

1.6. Extent of personal data compromised: [Describe the scope, e.g., the volume and scale of data records affected.]

1.7. Source of personal data: [Describe the source of the affected data, e.g., database, server, website, etc.]

2. Assessment of the Breach

2.1. Risk Assessment: [Describe the potential risks and adverse effects on the data subjects whose data was compromised, e.g., identity theft, financial loss, discrimination, reputational damage, etc.]

2.2. Immediate Impact: [Describe any immediate harm or consequences identified.]

2.3. Containment: [Describe the immediate steps taken to contain the breach and prevent further damage.]

2.4. Recovery: [Outline any actions taken to recover the data or rectify the situation.]

2.5. Mitigation:

Steps Taken to Contain the Breach: [List the steps taken to contain the breach, e.g., securing affected systems, isolating compromised data, notifying relevant authorities, etc.]

Steps Taken to Mitigate the Impact: [List the steps taken to mitigate the impact of the breach, e.g., providing credit monitoring services, offering identity theft protection, etc.]

Forensic Investigation: [Indicate whether a forensic investigation was conducted, and if so, provide details of the findings]

3. Notifications and Communications

3.1. Notification to Data Subjects

Date of Notification:

Describe the steps taken to notify affected data subjects about the data breach, Communication channels used (e.g., email, SMS, phone, post), Information provided to data subjects (e.g., nature of the breach, steps taken to mitigate harm) and Timeline for notifying data subjects.

3.2. Other Authorities Notified

Date of Notification:

Law Enforcement: [Indicate whether law enforcement agencies were notified and provide details if applicable.]

Other Regulatory Bodies: [Specify any other regulatory bodies or entities notified about the breach.]

4. Root Cause Analysis

Describe the initial investigation into the causes of the personal data breach [Identify the factors that contributed to the breach. Outline the remedial actions planned to prevent recurrence e.g., patching vulnerabilities, implementing new security controls, etc.]

5. Technical and Organizational Measures

5.1. Pre-Breach Measures

Personal Data Protection Policies: [Outline the data protection policies and procedures in place before the breach occurred.]

Security Controls: [Describe the technical and organizational security measures in place, e.g., encryption, access controls, regular audits, etc.]

Staff Training: [Mention any personal data protection training provided to staff and the frequency of such training.]

5.2. Post-Breach Measures

Corrective Actions: [Detail any steps taken to improve security and prevent future breaches, e.g., revising policies, enhancing encryption, additional staff training.]

Ongoing Monitoring: [Describe any monitoring or audit activities planned to ensure the effectiveness of the corrective actions.]

6. Lessons Learned

Describe the lessons learned from the data breach incident (Identify areas for improvement in data protection practices, Outline the steps taken to strengthen personal data security measures, Detail any changes made to existing policies, procedures, or processes as a result of this breach)

7. Supporting Documentation

Attach any relevant documentation, such as Incident reports, Logs of system activities, Evidence of notification to data subjects and Proof of remedial actions taken:

List them here and then attach.

8. Declaration

We hereby confirm that the information provided in this report is accurate to the best of our knowledge. We understand our responsibilities under the Personal Data Protection Act of Tanzania and commit to cooperating fully with the PDPC in addressing this incident.

Signature: _____

Name of Signatory:

Title of Signatory:

Date: