Personal Data Breach Reporting Procedure

Introduction

This procedure outlines the process to be followed for suspected or actual breach of personal data. The procedure must be read in conjunction with the ICT Policy, IT Policies Standard Operating Procedure, and the Data Protection Standard Operating procedure.

Purpose and scope

The purpose of this procedure is to provide a framework within which AUDA – NEPAD will ensure compliance with its obligations in respect of incidents on data breach on the data that its keeps.

This procedure applies to all staff, consultants, volunteers, contractors and third-party agents who process data for or on behalf of AUDA – NEPAD and it must be complied with in the event of a suspected or actual personal data breach.

AUDA – NEPAD is required to keep a record of all personal data breaches. Some of these breaches must be reported to the Chief Executive Officer or anybody established by African Union at the latest, within 72 hours of detection. It may also need to notify individuals affected by the breach.

It is important that all mentioned above should report a suspected or actual personal data breach, irrespective of its gravity, as soon as possible after discovery so that the Data Protection Office can commence investigations promptly.

Definition

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is accidentally lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

Why should data breaches be reported?

1.1. The loss or breach of personal data is an infringement of the Protection of Personal Information Act of 2013 and may result in criminal or civil action. The loss or breach of confidentiality of contractually assured information may result in the loss of business, financial penalties and criminal or civil action. Therefore, it is crucial that all officers handling personal data adhere to the personal data protection procedure, Information Security Policy, and its supporting policies,

1.2. The longer an incident goes unreported, the harder it gets to resolve any vulnerabilities. Impacted data subjects have a right to know that their data may have been compromised and that they could take steps that could minimise an adverse impact on them such as informing their bank that their bank details have been compromised,

1.3. The lengthier a breach goes without being noticed or reported, the longer a susceptibility remains unacted reading to escalation of the incident and more occurrences. Visibility of any incident leading to data breach, alerts AUDA – NEPAD to take corrective actions.

1.4. The Data Protection Procedure places a duty on data subjects and data protection officer to report data breach without undue delay from the time of becoming aware of the breach.

1.5. Delay in reporting on data breach, reduce the time that AUDA – NEPAD would take to investigate and understand and provide a timely response to meet the data protection privacy,

1.6. Any security breach is handled in accordance with all relevant AUDA – NEPAD policies, including the Conditions of Use of ICT Facilities at the AUDA – NEAPAD and the appropriate disciplinary policies.

Common data breaches

The following are some of the common forms of data breaches:

1.7. Loss or theft of equipment/tools that has personal data in it, for example loss of paper record, laptop, phones, or storage banks such as USB, etc,

1.8. Unauthorised access, controls occasioned by sharing of login details intentionally or not (hacked) resulting in changes to personal data or information systems,

1.9. Error/mistake where an email containing personal data is sent to a wrong recipient

1.10. Cybersecurity breaches resulting in hacking attack leading to a breach of confidentiality and integrity of personal data or its availability

1.11. Insecure disposal of paperwork containing personal data,

1.12. Use of shared facilities such as printers, scanners where sensitive documents are left to the access of unauthorised staff.

Procedure

The responsibility to report a breach or suspected breach lies the person who has the knowledge about the breach. Once the breach has been noticed, the person should report without any delays. The report can be made verbally or written. A verbal submission must be followed by a written description of the event using the standardised forms developed for this purpose.

AUDA – NEPAD will investigate the occurrence and where necessary take immediate correction actions, notify the relevant division/unit where the breach occurred. All data breaches must be reported to the data protection officer, withing 48 hours.

Notifying the data subject

The data subject must be notified where the breach is likely to result in a high risk of harm, or personal reputation.

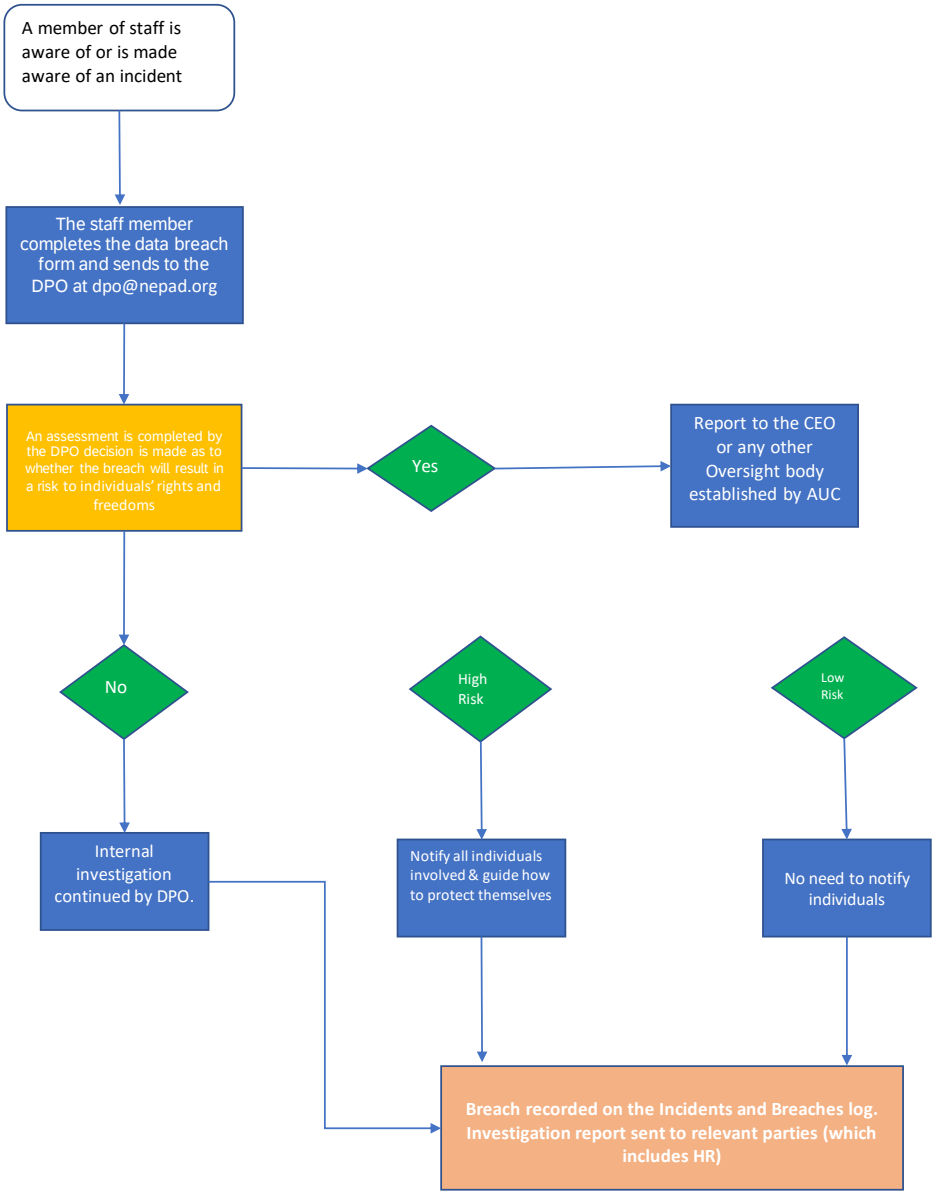
Enforcement

Members of staff will be subjected to the disciplinary procedure for failing to report suspected or actual breach.

Review

This procedure will be reviewed annually or where significant changes have occurred.

Process Flow – Data Breach



Personal Data Breach/Suspected Breach Notification Form	Breach Status			
	Actual	Suspected	Near Miss	

This form provides a means of reporting all data breaches/suspected breaches and 'near misses' across AUDA – NEPAD
Notification of any data breaches involving personal data have to be made within 72 hours of becoming aware (where a breach is likely to result in a risk to the rights and freedoms of natural persons).

It is essential that all breaches are reported as soon as they occur.
FILL IN AS MUCH AS POSSIBLE AND RETURN ASAP - EMAIL TO dpo@nepad.org.

Date of Breach	Time of Breach	Overview	How Discovered	Person reporting	No. of records	People Affected	Systems/Applications/Databases Involved	Type of data, data fields		Root cause	Action taken